Addresses & ports used by Talk2M

SOLUTION SHEET

KB-0209-00 2.2 en-US ENGLISH

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Industrial Networks of any inaccuracies or omissions found in this document. HMS Industrial Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Industrial Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Industrial Networks and is subject to change without notice. HMS Industrial Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Industrial Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

Page

This page intentionally left blank

1 Preface

1.1 About This Document

The present document details the addresses and ports used by Talk2M to establish a VPN connection to your Ewon but also to your computer.

For additional related documentation and file downloads, please visit www.ewon.biz/support.

1.2 Document History

Version	Date	Description
1.0	2015-04-22	First release
1.1	2015-07-16	Added Mumbai VPN server
1.2	2015-12-08	Added Europe VPN server
1.3	2015-12-09	Changed: VPN server info
1.4	2018-02-28	Added: access server address
1.5	2018-05-16	Added: detailed List of ortsVPN servers
1.6	2018-07-11	Added: NAP Server
1.7	2018-11-07	Changed: information inside *Ewon Connection to Talk2M, p. 9*
1.8	2018-12-05	Changed: references inside *eCatcher Connection to Talk2M, p. 8* and *Ewon Connection to Talk2M, p. 9*.
1.9	2019-05-08	Changed: General disclaimer Added: *Deep Packet Inspection of TLS/SSL Encrypted Traffic, p. 6*
2.0	2019-09-03	Changed: *eCatcher Connection to Talk2M, p. 8* Changed: *Ewon Connection to Talk2M, p. 9*
2.1	2019-10-16	Changed: general review
2.2	2020-04-15	Added: *Access Servers, p. 5* Added: *List of Talk2M VPN Servers, p. 7* Added: *VPN Servers Switch Notification, p. 7* Added: *Self-Signed Certificates, p. 6*

1.3 Related Documents

Document	Author	Document ID

1.4 Trademark Information

Ewon® is a registered trademark of HMS Industrial Networks SA. All other trademarks mentioned in this document are the property of their respective holders.

2 Introduction

Talk2M is a cloud service that provides remote connectivity to industrial equipment.

To use Talk2M, an Ewon VPN router is installed at the remote site and acts as a VPN client. The Ewon connects to one of the nearest VPN servers hosted by Talk2M.

To connect to the Ewon VPN router, remote users run eCatcher, the VPN client software, to connect to the same VPN server.

Fig. 1 Talk2M overview

The Talk2M architecture consists of multiple interconnected servers and services. This architecture permits a single rule when adding the Talk2M servers and services to a firewall: whitelist the Talk2M domain name.

The simplest solution is to whitelist the wildcard domain ***.talk2M.com** for outgoing port TCP 443 and UDP 1194.

If your firewall cannot be configured with a wildcard, additional information about specific addresses is included in this document.

You can check if the different ports and addresses needed for Talk2M connections are accessible from your network by using our Talk2M connection checker tool: Talk2M connection checker.

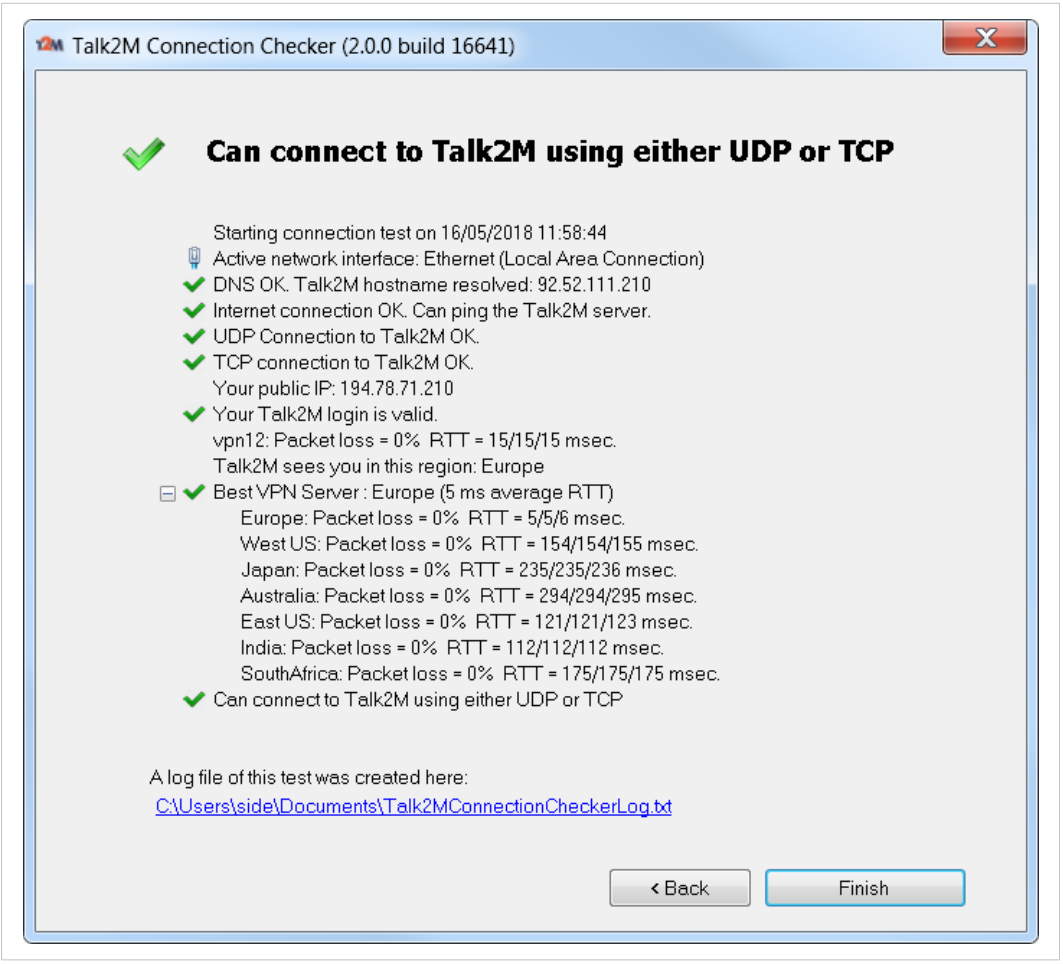

Fig. 2 Talk2M connection checker interface

2.1 Access Servers

It is important to understand why the simplest yet required rule in terms of network security must be respected.

Talk2M uses the Access Servers as first contact for the Ewons to know which Talk2M VPN servers they need to connect to.

The configuration explained in *Ewon Connection to Talk2M, p. 9* describes which rule must be applied to be sure that the connection to the Access Servers is functional.

If your Ewon can't connect to the Access Servers, then the following will might occur:

- No *bidi* communication between the Ewon and Talk2M. If no more *bidi* communnication:
  - → no more KPIs available on M2Web or eCatcher Mobile App;
  - → no more Talk2M VPN server fallback (e.g.: maintenance);
  - → Mail or DataMailbox might not work if the serial number registered in Talk2M is incorrect.

3 Firewall Configuration

The firewall rules should be as follows:

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

Under some circumstances, it is necessary to shift a Talk2M account from one VPN server to another.

If all the Talk2M servers are whitelisted using ***.talk2M.com**, shifting an account does not result in access issues.

If you don't whitelist ***.talk2M.com** (or all required servers), problems could occur such as:

- Remote access is no longer possible.
- If your Ewon VPN router uses Talk2M as a mail server or as an SMS relay, then alarm notification is no longer available
- If your Ewon VPN router uses the DataMailbox, historical data is no longer sent to the DataMailbox.

> **!** If your firewall has an option "block OpenVPN connection" (or a similar option), be sure to uncheck it as Talk2M uses the OpenVPN technology to link users to their Ewon(s).

> **i** *A server switch from one server to another one can be required during a VPN server maintenance or due to a major VPN server issue.*

3.1 Deep Packet Inspection of TLS/SSL Encrypted Traffic

Some firewalls or anti-virus software include a *Deep Packet Inspection* feature which monitors the data of encrypted traffic sent and received by an application.

With this mechanism, the firewall or the anti-virus software replaces the Talk2M HTTPS certificate by its own certificate and may be seen as a "Man in the middle" attack.

This method of replacing certificates is refused by eCatcher and the Ewon VPN routers for security reasons.

If you face this issue, an error is thrown:

- 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 issued for a different hostname, issuer is not trusted`.

The only solution is to disable the *Deep Packet Inspection* feature in the firewall / anti-virus software, at least for our URL/IP addresses (see *eCatcher Connection to Talk2M, p. 8* and *Ewon Connection to Talk2M, p. 9*).

3.2 Self-Signed Certificates

Talk2M uses a CA — a.k.a Certificate Authority — created by Ewon to sign certificates.

When the Ewon device tries to establish a secure connection to a Talk2M VPN server using the *device.api.talk2m.com* URL, it uses a certificate that is signed by Talk2M CA. This CA can be blocked or unrecognized by some firewalls as it has been created by Ewon.

If your firewall verifies the CA origins, it must accept the Talk2M CA to allow the Ewon to connect to Talk2M.

3.3 List of Talk2M VPN Servers

If the firewall responsible of the network security doesn't allow a wildcard as protection rule, you can find a list of all the Talk2M VPN servers on the Ewon support website.

This list is divided per area in the world. It provides the IP addresses and the domain names for each Talk2M VPN server.

Thanks to this list, you can set the firewall with the required IP address(es) and / or domain name(s).

3.4 VPN Servers Switch Notification

If you decide to create a rule for each specific URL – because of firewall limitation or by design – instead of using the wildcard domain, you have the opportunity to subscribe to a mailing list which will be used to send a notification when Ewon performs a Talk2M VPN server switch, thus changing the IP address of such Talk2M VPN server.

Through this notification, you will know if and when your rules inside your firewall must be updated to prevent any disconnection from Talk2M..

4 eCatcher Connection to Talk2M

If whitelisting ***.talk2m.com** is not possible, then the following section lists the servers you must grant access to.

eCatcher needs to connect to the following servers:

1. Access Server:
   - Protocol and port used: **HTTPS** (TCP port 443)
   - Addresses:
     - **as.pro.talk2m.com** (eCatcher version < 6.3.5)
     - **client.api.talk2m.com** (eCatcher version >= 6.3.5)
2. VPN servers
   - Protocols and ports used:
     - **UDP port 1194** or **TCP port 443**
   - Addresses:
     - **client.vpnX.talk2m.com**, where **X** is the VPN server number. The VPN server number can be between 1 and 50.
     - NAP server of China:
       - Primary: **sclient.vpn30.talk2m.com**
       - Backup: **sclient.vpn31.talk2m.com**

> **!** You must use the NAP server when the Ewon VPN router is located in China. If the Ewon VPN router is outside China but the user is in China, then additional URLs might be required.

We recommend whitelisting the URL ***.talk2m.com**. If whitelisting a wildcard domain is not possible, you can whitelist the URLs **client.vpn1.talk2m.com, client.vpn2.talk2m.com, ..., client.vpn50.talk2m.com**.

> *We do not use all incremental URLs. There might be gaps between "vpn1" and "vpn50".*

If the Internet connection is established through a proxy server, then eCatcher uses the TCP protocol.

> **!** Since eCatcher v4.1, if eCatcher connects through a proxy server, this proxy server must allow outbound connections on port **TCP 443** to hostname ***.talk2m.com**.

5 Ewon Connection to Talk2M

1. Access Server:
   - Protocol and port used: **HTTPS** (TCP port 443)
   - Addresses:
     - **as.pro.talk2m.com** (Ewon firmware < 12.2)
     - **device.api.talk2m.com** (Ewon firmware >= 12.2)
2. VPN servers
   - Protocols and ports used:
     - **UDP port 1194** or **TCP port 443**
   - Addresses:
     - **device.vpnX.talk2m.com**, where **X** is the VPN server number. The VPN server number can be between 1 and 50.

We recommend whitelisting the URL ***.talk2m.com**. If whitelisting a wild-card is not possible, you can whitelist the URLs **device.vpn1.talk2m.com, device.vpn2.talk2m.com, ..., device.vpn50.talk2m.com**.

We do not use all incremental URLs. There might be gaps between "vpn1" and "vpn50".

If the Internet connection is established through a proxy server, then your Ewon VPN router uses the TCP protocol.

Since Ewon firmware 6.4s6, if your Ewon connects through a proxy server, this proxy server on local site should allow outbound connections on port **TCP 443** to hostname ***.talk2m.com**.

Box 4126
300 04 Halmstad, Sweden

info@hms.se