

FAQ Talk2M

Frequently Asked Questions about Talk2M



Machine Builders/OEM, Systems & ICT Integrators



1

What is Talk2M?

Talk2M comprises connectivity services based on a hosted web application designed to connect users to their machines via the Internet. This hosted application acts as a broker and relays the communications originated by the users to their machines. It is intended to be used in the industrial automation sector.

2

How does Talk2M work?

Talk2M uses virtual private networks (VPNs) and tunneling. Talk2M accepts connections from users as well as from their machines, so both parties can exchange data using tunneling technology.

3

What are VPN and tunneling?

VPN (virtual private network) and **tunneling** are techniques that allow you to encrypt data links between yourself and another (remote) computer. This computer might belong to your organization, a trusted person or organization, or a commercial VPN service. Tunneling encapsulates a specific stream of data within an encrypted protocol, making everything that travels through the tunnel unreadable to anyone along the transmission path. Using a VPN or other form of tunneling to encrypt data can be a good way to ensure that it will not be seen by anyone other than you and people you trust.

4

The Talk2M service is hosted on the Internet. This means that anyone in the world can access the machine in my factory.

Each eWON connected to your machine connects exclusively to the Talk2M server. An authentication mechanism ensures that each eWON talks to the Talk2M server that has the same key. A similar mechanism ensures that each user can only communicate with a specific eWON. All data exchanged via the Talk2M server and the Internet is encrypted, so the data remains secure.

5

The Talk2M service allows connections to be made from the Internet to my factory. This means I need to reconfigure my firewall to enable a port, but I don't intend to do this.

Talk2M tunnels are initiated by eWONs and use only outgoing connections. No incoming connections are made (in other words, the Talk2M server does not initiate tunnels), so no ports need to be enabled in your corporate firewall for incoming connections.

In addition, Talk2M is designed to be minimally intrusive. This means that it tries to use outgoing ports that are already enabled, which are usually the HTTP port (80) and the related secure HTTPS port (443).

6

What are the VPN protocols used in Talk2M?

The Talk2M VPN protocols are Open SSL and Open VPN Version 2.

7

The Talk2M system does not use the IPSec protocol, which is the ICT standard for VPN security. Why not?

They are two reasons why the IPSec protocol was not chosen for implementing VPNs and tunneling with Talk2M.

Design reason: The IPSec protocol is based on OSI layer 3, the network layer. It is designed to protect IP packets exchanged between remote networks or hosts and an IPSec gateway located on the edge of your private network.

The Open VPN protocol is based on OSI layer 7, the application layer. It protects application streams sent from remote users to an SSL gateway.

In other words, IPSec connects hosts to complete private networks, while SSL VPNs connect users to services and applications inside these networks,

which is the usual situation for accessing machines remotely via local networks.

Technical reason: One of the goals with Talk2M was to design a minimally intrusive architecture, which means that the VPN protocol needs to be able to adapt easily to existing outgoing open ports available in the firewall. The Open VPN protocol makes it easy to switch to different IP ports, and it typically uses the HTTPS port (443).

IPSec uses predefined IP ports (UDP 500 and 4500). Using IPSec would require machine builders and OEMs who want to use Talk2M to be much more involved in the configuration of their customers' network protection systems in order to ensure that the Talk2M system works properly.

8 The eWON is connected to the factory LAN. This means that the machine manufacturer can access all the PLCs and IP devices in the factory.

The point-to-point Talk2M tunnel links the Talk2M user to a specific eWON device attached to the machine control panel.

The eWON can be configured so that only devices connected to the (green) LAN ports of the eWON device can be accessed remotely.

9 A Talk2M tunnel can be configured to be always on. This means that the machine builder can access the PLC and make changes without my knowledge.

It is possible to configure the eWON with a switch connected to the eWON digital input so the VPN connection can be enabled or disabled. A digital output is also available to control a relay that can be used to physically decouple the Ethernet port from the corporate network.

10 There are some devices connected to the (green) LAN ports of the eWON which I do not want to be remotely accessible, for security reasons. How can I manage this?

Each device connected to the green VPN ports of the eWON is configured with an IP address, a subnet mask, and a gateway address.

If the gateway address configured for a device matches the IP address of the eWON, this device will be accessible. If the gateway address does not

match the IP address of the eWON or is blank, the device will not be accessible.

11 What happens if the Talk2M services are discontinued?

The Talk2M services are owned and operated by eWON, which produces the gateway devices.

The Talk2M Free service can be used at no charge and is financed by sales of eWON units.

For customers that require operational continuity of service, Talk2M Pro (which is based on a mission critical host architecture) ensures 99.6% operational continuity over one year with a maximum out-of-service interval of 4 hours.

12 I always install a PC on the machine and use software on this PC, such as PCAnywhere, to access the machine. Why is Talk2M better?

Talk2M only needs an eWON unit at the machine instead of a fully functional Windows PC.

An eWON unit is more reliable than a PC, since it has no moving parts and no hard disk, and it is less likely to be tampered with by engineers. A Windows PC also has a higher total cost of ownership (TCO), estimated to be three to five times greater than an eWON.

In addition, a PC is vulnerable to viruses and thus needs antivirus protection, further increasing the TCO.

An eWON can also communicate with the machine and send alarms and data back to headquarters.

13 What do I need at the machine site in order to use the Talk2M system?

All you need is a Talk2M compatible eWON unit and Internet access via your LAN or a dedicated line with a built-in modem (ADSL, GPRS/EDGE/3G, or PSTN).

If you use a LAN, it should allow users to browse on the Internet from their network (in other words, using HTTP and HTTPS).

14 What factory network information is needed on site to allow an eWON to be fitted to a machine?

If the eWON uses the customer LAN to connect to the Talk2M system, it needs the same settings as a PC connected to the same network (IP address, subnet mask and gateway, plus any proxy settings). The eWON is also a DHCP client, so it can be assigned an address automatically.

15 How often does Talk2M go offline for maintenance or upgrades?

Talk2M service is subject to occasional planned maintenance. Users are informed of these activities in advance by e-mail.

16 What security protocols or level of security does Talk2M technology provide?

Talk2M uses several levels of security. Users and eWON units are authenticated by the Talk2M server using SSL/TLS for session authentication and the IPSec ESP protocol for secure tunnel transport over UDP.

Talk2M supports the X509 PKI (public key infrastructure) for session authentication, the TLS protocol for key exchange, the cipher-independent EVP (DES, 3DES, AES, BF) interface for encrypting tunnel data, and the HMAC-SHA1 algorithm for authenticating tunnel data

17 Are there any HTTP proxies that may not be compatible with Talk2M or supported by Talk2M ?

There are presently some proxies that may not be supported due to their authentication mechanisms. The known proxies in this category are:

- Kerberos authentication
- Digest access authentication

18 If I decide to use Talk2M, what ports do I need to open if all my firewall outgoing ports are closed?

Talk2M is designed to be minimally intrusive. It is based on the Open SSL/Open VPN protocol, so its base port is UDP 1194. However, eCatcher and eWON check to see whether the UDP 1194 port is open in outgoing mode before they connect to the

Talk2M server. It is usually closed, so Talk2M technology is designed to use the HTTPS port (TCP 443) as an alternative, since it is considered to be more widely used than the Open VPN port.

This means that if no outgoing communication ports are open on your company firewall, you need to open at least the HTTPS port (TCP 443) in outgoing mode.
