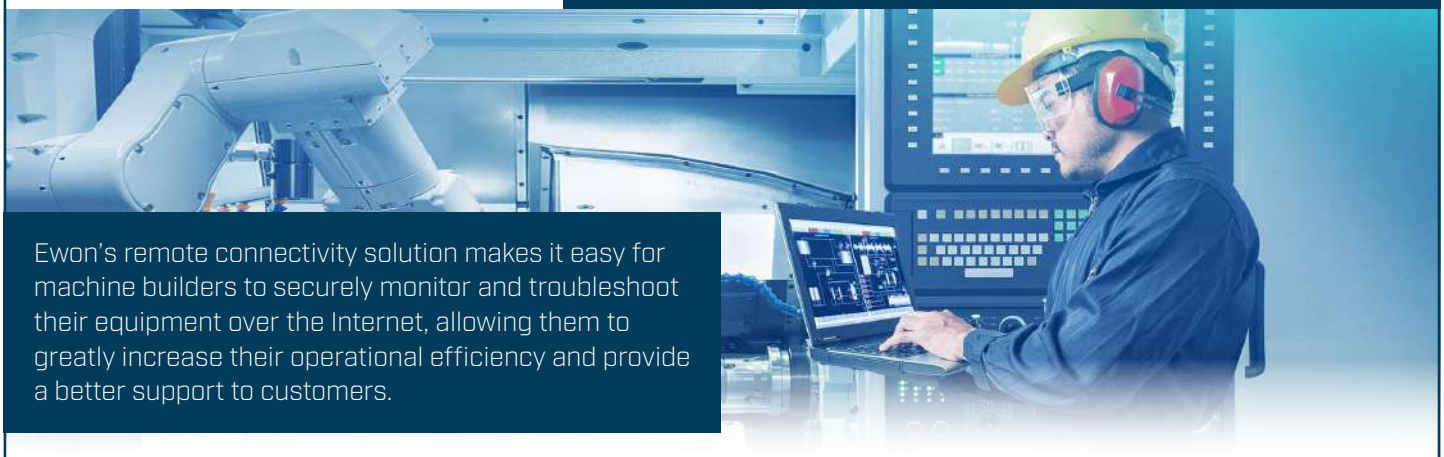
FAQ - Remote Access

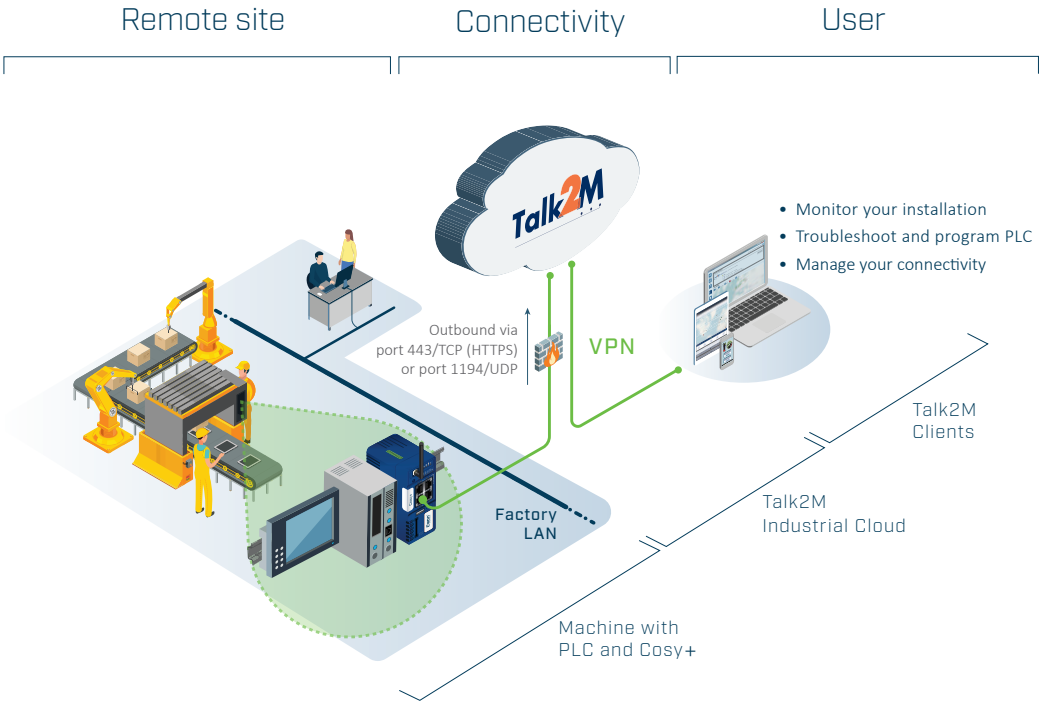


Ewon's remote connectivity solution makes it easy for machine builders to securely monitor and troubleshoot their equipment over the Internet, allowing them to greatly increase their operational efficiency and provide a better support to customers.

For 20 years, Ewon has been a pioneer and leader of remote access for industrial machines. The combination of Talk2M, the first industrial cloud connectivity service, and the Ewon gateways enables machine builders and system integrators to securely connect to their equipment through the Internet, from anywhere in the world, in just a few clicks.

How does the Ewon Remote Access solution work?

Ewon gateways are designed to fit inside the control panel of a machine (DIN rail mounted, 24VDC) and be connected to automation devices such as PLCs and HMIs, through Ethernet, serial or USB interfaces. They also connect to the Internet via an Ethernet, WiFi or cellular network, to establish a secure outbound VPN connection to Talk2M, Ewon's cloud-based remote connectivity service. Authorized users can then log in to their Talk2M account using the eCatcher client software, and remotely connect to their Ewon gateways to gain access to the automation devices behind them, for monitoring or maintenance. The Talk2M service acts as a secure broker which completes the encrypted VPN tunnel between the user and the remote equipment connected to the Ewon gateway.



What does the IT department of the remote site need to do?

Typically, nothing! Talk2M VPN tunnels are initiated by the gateway and use only outbound connections. Since no inbound connection is made, no inbound port needs to be opened in the firewall, and no public IP address is required. In addition, Talk2M is designed to be minimally intrusive by using outbound ports that are usually already enabled (TCP port 443 and - optionally - UDP port 1194). If connection through a local network is not possible, WiFi or cellular connectivity is also available to achieve internet connection.

How to prepare for the successful installation of an Ewon gateway on a network?

By default, the Ewon gateway is configured as a DHCP client and can therefore receive its network settings automatically. Alternatively, it can be configured to use a static IP address, which will be assigned and managed by the IT department. Connection through a proxy server is also possible. A tool called "Talk2M Connection Checker" can be used to verify from a PC if an Ewon gateway will be able to connect through the network. It is available at: https://ewon.biz/technical-support/pages/all-downloads

Will the whole factory network become accessible to the user?

No, the Ewon gateway provides a segregation between its WAN side (used to connect to the Internet through the factory network) and its LAN side (where the target equipment is connected). Users of the solution can only reach the devices connected to the LAN side of the Ewon gateway, for example the PLC or HMI of the machine. The factory network, on the WAN side, cannot be accessed.

ADDITIONAL SECURITY INFORMATION

Compatible with existing factory networks – the solution uses only outbound connections across the factory network, through TCP port 443 (HTTPS) or UDP port 1194, which are typically available. In most cases, there is no need to change any firewall or proxy setting.

Built-in Hardware security – The new generation of Ewon gateways includes a dedicated secure element chip, which is certified CC EAL6+ and serves as a root-of-trust to deliver state-of-the-art, end-to-end security.

Secure communication – SSL/TLS session authentication certificates using 2048-bit key exchange ensure that each Ewon gateway only communicates with your Talk2M account. This guarantees that only authorized users can connect to the Ewon gateways. All the communication occurs within an encrypted VPN tunnel.

The local customer keeps control – Connect a key switch or HMI button to the digital input of the Ewon gateway to manually enable or disable its VPN connectivity on-site. The digital output of the gateway can also be used to notify when a remote user is connected.

Device and user management – The administrator of the Talk2M account can at any time manage the Ewon gateways, users and permissions, to precisely control who can connect, when and to which device.

Connection Audit Trail – Detailed connection logs and reports allow to monitor all the remote activity occurring through the Talk2M account.

LAN Firewalling – Control which devices connected to the Ewon gateway are accessible to the user.

Two factor authentication –The security of your Talk2M account can be strengthened by enabling the 2-factor authentication on user login.

Ewon's security is regularly audited by 3rd party organizations and certified **ISO27001**: https://ewon.biz/about-us/security

KEY BENEFITS

- Provide a better, faster support and reduce downtime
- Avoid service trips to save time and money
- Monitor your equipment at any time, from anywhere

WHY MACHINE BUILDERS CHOOSE EWON

- Over 20,000 customers and voted No. 1 remote access solution for 6 years in a row
- Very easy to setup and use, even without IT knowledge
- No recurring cost: the Talk2M service and its clients (desktop, web, mobile) are available for free
- Global and reliable infrastructure, with more than 35 servers worldwide
- ISO27001 certified security
- NEW! Ewon Cosy+ gateway, with built-in hardware security!

www.ewon.biz