WHITE PAPER

Ewon's security posture

How the Ewon solution works and meets your needs for highly secure industrial remote connectivity.

Introduction

INDUSTRIAL REMOTE CONNECTIVITY HAS BECOME TRULY ESSENTIAL FOR MACHINE BUILDERS AND MANUFACTURING COMPANIES. MACHINE BUILDERS ARE USING IT TO IMPROVE THEIR CUSTOMERS' SATISFACTION THROUGH A FASTER TROUBLESHOOTING OF MACHINE FAILURES, TO OPTIMIZE THE EFFICIENCY OF THEIR SERVICE TEAM WHILE REDUCING COSTS, BUT ALSO, MORE RECENTLY, TO GET INSIGHTS FROM MACHINES TO ENABLE ONLINE MONITORING, ALARMING AND SMART DATA-BASED APPLICATIONS.

On their end, manufacturing companies are taking advantage of industrial remote access to support the availability of their production capacities, to structure and consolidate their relationship with their machine suppliers, as well as to secure the connectivity to their plant.

Obviously, security is an essential aspect of a remote connectivity solution and is at the heart of the Ewon solution.

In the "Secure Remote Access for Industrial Machines" guide, we underline the main concepts and benefits of a cloud-based architecture for remote access and describe the key specificities of the Ewon solution.

In the present document, we aim to explain the different security aspects related to the Ewon solution, to support its evaluation by users and help them gain its acceptance from factory owners and IT teams.
In a quick overview, the first two chapters introduce:

- Our company and its security posture,
- A high-level description of the Ewon solution and its security principles.

The following chapters will provide more details about these security concepts with:

- An introduction on how the Talk2m service allows a centralized management of all remote access activities,
- An overview of the architecture of the Talk2m cloud service,
- An explanation of the process of establishing a secure remote access connection,
- A description of the reasons why a hardware gateway is an essential element of a secure remote connectivity solution,
- A brief outline of additional services offered by the Talk2m service.

As the cybersecurity of a system is only as strong as its weakest link, we also provide recommendations and best practices to be followed by customers in order to complement the security measures provided by the Ewon solution itself. The document "Best practices for a secure usage of the Ewon solution" provides a description of these best practices.

A simplified explanation of the security of the Ewon solution is also available as a FAQ document.
This shorter description is mainly dedicated to people without expertise in IT or security, or to those who only want a brief introduction to the Ewon solution.

For more details about the Ewon solution and its features, please consult our product user manual or installation guide available on our Support website.

1. Ewon in a nutshell

1.1 Ewon by HMS Networks

Established in 2001 in Nivelles (Belgium), Ewon is one of the world's leading supplier of smart industrial remote connectivity solutions. With more than 20 years of expertise in industrial applications, Ewon collaborates with machine builders and machine users to help them in their digitalization journey towards successful remote connectivity and Industrial Internet of Things (IIoT).

Ewon is operating as a Business Unit of HMS Networks AB since 2016. HMS Networks, the leading independent manufacturer of solutions for industrial communication, is a publicly traded Swedish company with more than three decades of experience enabling connectivity. HMS Networks has over 750 employees and a worldwide presence, with offices in 17 countries and distributors in more than 50 countries. It is recognized for its strong focus on high quality products, security and sustainability.

The HMS Networks group and its Ewon brand have:

- A long expertise in industrial applications and a good understanding of the market expectations,
- A proven track record of quality products and services, with a commitment to providing future proof solutions to its customers,
- A strong highly skilled team, and the financial strength to address future challenges.

Selecting and using the Ewon solution is a guaranty of long-term availability and sustainability. Of course, cybersecurity is also at the core of the Ewon solution, designed from the start with security in mind, and regularly audited and certified by third-party organizations.

1.2 ISO 27001 certified security

ISO/IEC 27001 is an international standard on how to manage Information Security. It details requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). ISO 27001 is the most widely used and recognized security standard, well known and accepted by IT departments.

Security is at the heart of the Ewon solution. For this reason, Ewon has selected, implemented, and certified all 114 controls of the ISO 27001 Standard.

Ewon's ISO 27001 scope covers Talk2m, Ewon's industrial cloud service, and the Ewon gateways. Ewon continuously improves its organizational processes, as well as the technical expertise of its engineering teams to ensure the highest security level for all its products and services. Its Information Security Management System guarantees that all security issues and threats are identified and adequately handled.

The security of the Ewon solution is permanently monitored (24/7/365) by a team of skilled professionals and regular reviews or updates address potential vulnerabilities or provide new functionalities.

1.3 Regular security assessments

Ewon and its solution are regularly assessed by independent security experts to ensure that a good security posture is maintained and continuously improved. NVISO has been selected as the Privileged Testing Partner.

NVISO
Testing Partner

NVISO is an independent professional services firm focusing exclusively on cybersecurity and has a proven track-record in various markets such as financial and telecom services. NVISO counts among the leaders in the security industry, co-creator of OWASP project, teaching security (SANS) and presenting on new security topics at major events around the world (BruCON, DefCON,…).

NVISO is present all along the development and support processes to ensure that information security is designed and implemented within the lifecycle of Ewon's solutions, and to provide adaptive security test plans ensuring their capability to handle modern cybersecurity threats.

2. Architecture of the Ewon solution

2.1 Solution overview

The basic architecture of the Ewon remote connectivity solution relies on 2 main components:

1. **Ewon Talk2m**: A global connectivity cloud service to centrally manage all aspects of the connectivity,
2. **Ewon Gateway**: A hardware gateway usually placed inside the control panel of an industrial equipment and connected to control devices such as PLCs and HMIs.

With this setup, support engineers, regardless of geography or time zone, can establish a secure remote access connection to the equipment, from their computers or mobile devices, in a couple of clicks.

2.2 Architecture

The Talk2m cloud offers secure services to connect users to their machines via the Internet. These users are typically Service or Automation engineers, who need access to machines installed at their various customers' premises, which can be spread all over the world.

- The **Talk2m service** plays the **central role** between the Ewon gateway and the user. It is a cloud-based infrastructure composed of multiple servers, which relay communications between users and machines. The entire system operates with the prerequisite that both sides of the communication can access the Internet and reach the Talk2m servers.
  Talk2m provides a secure encrypted connectivity making it possible for the user to work on the remote equipment, as if he were physically connected to it. The Talk2m service is available in different levels, from a free version supporting fundamental needs for remote access connectivity, to a version fulfilling more advanced expectations regarding security, availability and overall management possibilities. In between, the light version meets the expectations of most users.

- On the **machine side**, an **Ewon gateway** (such as a "Cosy" or a "Flexy") is installed, typically inside the control panel, and connected to the automation devices controlling the machine, such as a PLC (Programmable Logic Controller), HMI (Human-Machine Interface) or IP camera.

This connection is possible through Ethernet, serial (RS232/RS485/RS422 or MPI) or USB. The Ewon gateway is also configured to securely connect to the Internet via Ethernet, WiFi or cellular network in order to interact with Talk2m.

- On the user side, a software application is installed on a PC running the Windows operating system. This client application, named "Ecatcher", is used to establish a secure communication link between the PC and Talk2m, through the Internet. It is also used to configure and manage the user's Talk2m account. Connections can also be established from a mobile device using the "Ecatcher Mobile" app, available for Android and iOS, or from any web-browser using the Talk2m web portal "M2web".

2.3 Benefits of a cloud-based Rendez-Vous server

Traditionally, various approaches have been used to establish connections to remote industrial equipment:

- Modem connectivity,
- Software connectivity (usually a remote desktop solution),
- Direct VPN connectivity,
- Connectivity via a private APN or private VPN server.

These methods have never managed to completely fulfill the expectations related to industrial applications, such as robust security, scalability for large deployments of equipment, immediate availability of the connectivity to enable a fast reactivity, and ease of use for any user to connect and interact with their industrial controllers, even without being IT experts.

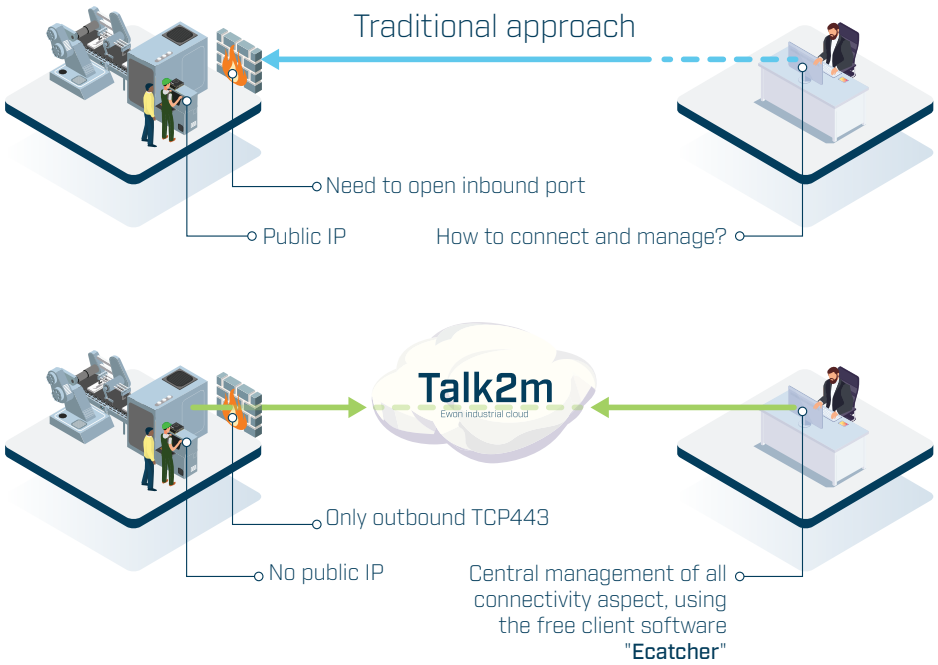
Ewon changed the game in 2006 by creating Talk2m, a Rendez-Vous server making the link between the Ewon gateways and Ecatcher, the VPN client installed on the user's computer, in a very secure and easy way.
A rendez-vous server allows two network endpoints to meet and communicate with each other.

A cloud-based Rendez-Vous server such as Talk2m brings a lot of benefit in terms of:

- Efficiency, by providing a central place to manage all aspects of the remote connectivity solution (devices, users, access rights...),
- Security, since only outbound connections are required and there is therefore no need for change in the user's company firewall,
- Scalability, availability and performance, with a platform designed to grow over time (Talk2m is an extensive and fully redundant global server infrastructure, optimizing connections between endpoints),

- Finally, HMS experts are constantly on duty to handle cybersecurity challenges, as well as to ensure the quality and reliability of the solution.

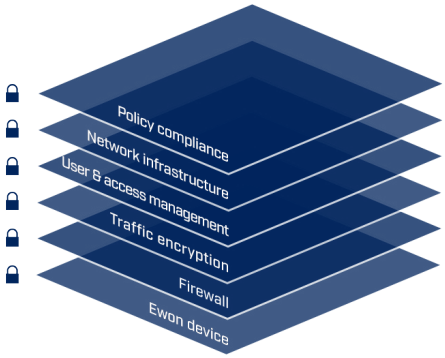
Using Talk2m significantly reduces efforts, investments and expertise required to create and maintain a professional and worldwide remote access solution.



Traditional approach versus Talk2m rendez-vous cloud approach

2.4 Security of the Ewon solution

Security is the most important aspect of the Ewon solution. To achieve a best-in-class level of security, the system is designed and built around a "Defense in Depth" approach.



Defense in Depth (or layered security) is a coordinated use of multiple types of security countermeasures spread on multiple layers of security controls. This approach ensures the protection of the whole Ewon solution, and therefore of the users' networks, devices and industrial control systems.

It is based on guidelines set forth by leading security standards like ISO 27001, IEC 62443 and NIST Cyber Security Framework, in addition to numerous other publications, guidelines and industry best practices.

Below is an overview of the different security measures implemented.

Layer	Layer Name	Security measures implemented
1	Ewon gateway	1. Ewon gateway configuration: users need to authenticate and must possess the appropriate permissions to be able to modify the configuration of the device, 2. Network segregation: traffic on the machine/LAN side is segregated from the factory/WAN side. Remote users can only access authorized devices on the LAN side. NAT 1:1 is available, 3. The gateway authenticates itself to the Talk2m platform, 4. A physical switch can be used to control the connectivity of the Ewon gateway.
2	Firewall	Filtering/firewalling: up to 4 levels are possible, allowing the filtering of a user's traffic to any Ethernet device, any USB/serial device or even any internal service of the Ewon gateway. The filtering is managed and applied on the Talk2m connectivity platform itself and not in the Ewon gateway.
3	Traffic encryption	Each user is authenticated, and all communication is encrypted using TLS protocols.
4	User & access management	1. Users & Ewon gateway access control: the purpose is to define which users can have access to which machines, through roles attributed to group of users over pools of Ewon gateways, 2. Unique user credentials with (optional): • Password policies, with: minimum length, requirement for letters/digits/special characters, expiration period, prevention of password reuse, • Double factor authentication: after regular authentication via username and password, a verification code received by SMS must be entered. 3. Connection audit trail (who connected to which gateway, when & for how long), 4. User lockout implementation to prevent too many connection attempts from an unauthorized user trying to guess a password.

5	Talk2m Network infrastructure	Ewon regularly assesses the Talk2m architecture (as well as the hardware and firmware security of the devices) as part of its ISO 27001 continuous improvement process. Appropriate measures and controls are then put in place for better effectiveness and compliance. We list below the different families of controls of this assessment. a. Security policies: to make sure that policies are in line with our security objectives, b. Organization of information security and human resources: to cover the right assignment of security responsibilities to all employees and contractors, c. Asset management: to define appropriate protection measures for each asset, d. Access control: to ensure that the "need to know" principle is enforced, e. Cryptography: to protect the confidentiality, integrity and availability of data, f. Physical and environmental security: to protect assets from physical and environmental threats, g. Operation security: to address threat of malware, cover backup, ensure logging, h. Communications security: concerns network security management, and protection of data in transit, i. System acquisition and development: address the security requirements for internal systems, j. Supplier relationship: to address the protection of assets accessible by suppliers, k. Incident management: to manage and report incident effectively, l. Business continuity management: to manage business disruption, m. Compliance: to identify relevant laws and regulations. Ewon relies on market leading hosting providers certified ISO 27001, SOC 1, SOC2 and SOC3.
6	Policy compliance	The Talk2m remote access solution is designed to be compatible with customers' existing security policies. By using outbound connections over commonly open ports (TCP 443, and optionally UDP 1194) and by being compatible with most proxy servers, the Ewon gateway is designed to be minimally intrusive on the network and work within the existing firewall rules. Talk2m account administrators can customize the password policies to force compliance to corporate password policies and can restrict which users can access which devices remotely. Talk2m account administrators can also view the Talk2m connection report to see which users are connecting to which devices and when. This report can be a valuable tool to ensure that that customer's corporate remote access policies are being followed.

3. Talk2m Central management of remote access activities

Talk2m is not only used to securely and easily establish a connection between users and their remote equipment. It also enables to manage, from one central place, all the aspects of remote connectivity, including:

- Management of the account,
- Management of the users,
- Management of the devices,
- Definition of security policy,
- Monitoring of the activity.

3.1 Talk2m Account

A Talk2m account is the workspace for the management of devices, users, and all security aspects of the Ewon remote connectivity solution. There is no dependency between the different accounts existing on the Talk2m cloud, which means that no information or device registered on one account can be reached from another account.

Account administrator

The Talk2m account administrator plays a key role with extended responsibilities:

- Managing all the settings and properties of the Talk2m account such as its general parameters, password policies, credit balance and services levels aspects, contact information, etc.,
- Registering Ewon devices,
- Creating users and defining their roles and access rights,
- Accessing log files and reports to monitor the activity occurring on the account.

Note: Multiple administrators can be created, including administrators with a more limited access and the authorization to manage only parts of the Talk2m account (see section "Pools, groups & access rights management" on page 11).

Password policies and two-factor authentication

Administrators of a Talk2m account can adapt password policies for different levels of security expectations:

- Password definition rules to require strong passwords,

- Password validity period to impose regular change of passwords,
- Two-factor authentication to strengthen the security of the user login process, by forcing users to provide two different means of proving their identity.

Additionally, Talk2m implements a lockout mechanism to prevent repeated login attempts with incorrect passwords, by temporarily disabling a user for a period of time and notifying the administrators of the account, who can then take appropriate measures.

User management and identification

Users are created and defined in the Talk2m account and can interact with the account or the registered Ewon gateways according to their roles and access rights. The administrators' account can manage all user's roles and permissions, to precisely control for example who can connect, when, and to which equipment.

Ewon device management

Ewon gateways are registered to a Talk2m account and can only belong to one account.
Talk2m provides functionalities to support the management of a growing population of Ewon gateways over time:

- To simplify the onboarding of multiple gateways with similar settings, a "global registration key" can be used within a configuration file to be easily deployed on all devices via a USB drive or SD card,
- To keep the devices' population up to date with the latest security patches and firmware updates, a system for automated mass deployment of updates is available.

3.2 Pools, groups and access rights management

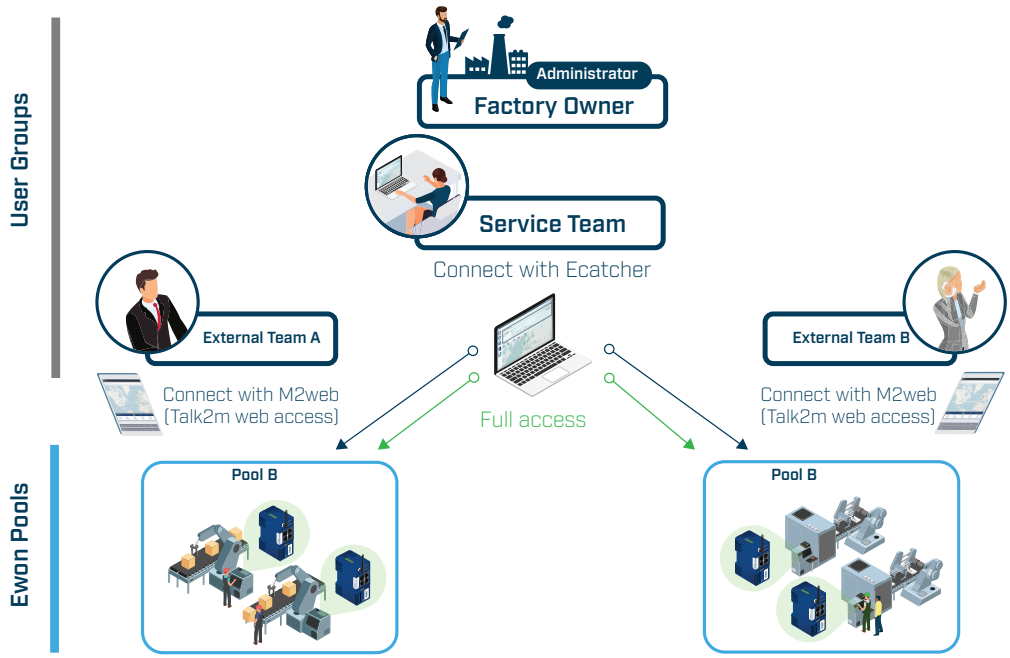
Talk2m light and Talk2m pro provide ways to simplify the management of users and devices by gathering them into pools of devices and groups of users, in order to easily define their respective roles and permissions. Defining a structure of pools and groups that reflects the organization of the company and the relation with external partners is key to optimizing the security and maintenance activities when using the Ewon solution.

Pools of Ewon devices

A pool gathers one or more Ewon gateways that will be given similar access rights properties. An Ewon gateway is assigned to one or several pools, usually during its registration on the Talk2m account.

Groups of Users

A group gathers one or more users who will be given similar roles and access rights to pools of Ewon devices. A user is assigned to one or several groups, usually during the registration process, and automatically inherits the access rights and restrictions defined for the group(s).



Access rights definition

Groups of users can be assigned different access levels to each pool of devices. For example, maintenance and service teams could be granted full VPN access to all machines on a production line, in order to be able to carry out their remote programming, troubleshooting or control. On the other hand, a limited monitoring access could be assigned for users who only need to connect to a HMI or to monitor the status and performance of the equipment using the Talk2m Live KPI service (see chapter "Talk2m Additional Services" on page 26).
Administration roles towards devices, users, pools of devices or groups of users can also be assigned to specific users, to give them the possibility to manage their respective area or team.

Device Firewall and granular equipment access level

Talk2m light and Talk2m pro allow to control, with different granularity levels, the permissions of users to access specific devices connected behind an Ewon gateway, such as PLC and HMI. Talk2m integrates firewall functionalities that can be customized for each Ewon gateway, with different levels varying from no restrictions to strictly restricted access through the definition of all accessible IP addresses, ports and even protocols.

3.2 Account activity & monitoring

Talk2m provides tools to supervise the activities and events occurring within an account and validate the compliance with the corporate security policies. For security and traceability purposes, logs listing all connections, disconnections, as well as changes of state for all users and devices are available. This information can be viewed using Ecatcher and displayed for the whole Talk2m account or for specific users or devices. It can also be displayed as monthly reports (which can be exported in various file formats and are also received by email by the account administrators).

An activity logbook is associated with each device to document operations performed during a remote session. This allows organizations using the Ewon solution to keep track of the work that has been done and share information between users of a same device.

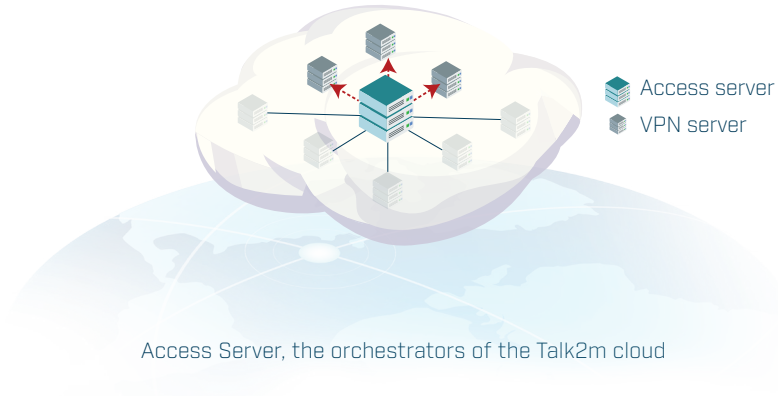
Finally, a financial report helps keeping track of the data consumption and the credit balance of the Talk2m account.

4. Talk2m cloud infrastructure

4.1 Talk2m global infrastructure and availability

The Talk2m infrastructure is mainly composed of two types of servers: Access Servers (AS) and VPN Servers (VS).Access Servers are the first ones to be solicitated when a device or user initializes a connection to Talk2m. They take care of all authentication aspects and play a role of central coordinator, controlling all permissions and orchestrating the interactions between the different Talk2m services, the users and the devices.
VPN Servers are distributed around the world and are the Rendez-Vous servers handling the actual VPN connections between users and devices.

Following security aspects, the second highest priority of the Talk2m architecture is to offer the best possible availability of its connectivity services. The Talk2m infrastructure includes more than 40 servers, distributed across the world and hosted by multiple leading hosting providers to provide worldwide coverage and redundancy for maximum business continuity.



Access Server, the orchestrators of the Talk2m cloud

Talk2m servers are currently located in Europe, the United States, Japan, China, India, Singapore, Australia, Brazil and South Africa, and the infrastructure is regularly expanded with the addition of new servers to meet network and customers' expansion. This distribution of the hosting sites allows to improve performance, reduce latency and optimize the load between the servers.

The availability of the Talk2m service is reinforced by multiple control objectives, such as:

- **Service Level Agreements (SLA)** with hosting providers: Ewon has contracts with several leading hosting providers, guaranteeing a good availability and performance of their own infrastructure. Depending on the Talk2m service, Ewon may deal with different providers,
- **Continuous system monitoring**: Ewon monitors at all time the key performance indicators of all Talk2m servers. All data acquired is displayed on monitoring dashboards and is also logged on an alarm server able to notify 24/7/365 duty service personnel,
- **Server roll-out**: with its multiple different providers, Ewon can quickly roll-out VPN connections from one VPN server to another in case of issue or when a maintenance operation is carried out.

Status of Talk2m can be checked live on:
https://www.ewon.biz/technical-support/pages/Talk2m/Talk2m-status

4.2 Talk2m Service Level Agreement

Ewon strives to provide an excellent business continuity for all users and offers three versions of the Talk2m service:

- The Talk2m free offering, provided for free and perfect for customers starting with a small number of Ewon gateways deployed **(version available on condition that you install at least one new Ewon device in Ecatcher every 12 months),**
- The Talk2m light subscription, based on enhanced hosting services, and including a comprehensive SLA and that meet the needs of most of users.
- The Talk2m pro subscription, which provides a premium service, and full functionality.

Here are the details of business continuity levels guaranteed to Talk2m pro and to Talk2m light customers for each of the Talk2m services:

Service Name	Total Service Availability per year per region	Total Unscheduled Downtime per year in hours	Max. Service Downtime in hours
Remote Access	99.6 %	35	4
M2web Portal	99.6 %	35	4
M2web APIs	99.6 %	35	4
DMweb APIs	99.5 %	44	4

Table: SLA per service

For more details, please refer to the Talk2m Terms of Use available on this page:
https://www.ewon.biz/terms-of-use/Talk2m---terms-of-use

5. Establishing a remote access connection

This chapter describes the mechanism of enabling a VPN connection between a user and a remote machine, through the Talk2m cloud service.

5.1 Connection of a user to Talk2m

To manage the Talk2m account or establish a VPN connection from a PC to a remote machine, a user uses the "Ecatcher" client software (free download available on Ewon's Support website). With Ecatcher, the user logs into the Talk2m account using their credentials: account name, username and password. A HTTPS session is initiated to the Talk2m cloud to authenticate the user, and once logged in, they can perform various actions, depending on their permissions, such as:

- Registering a new Ewon gateway on the account. This operation is described in the next paragraph. The user can also edit the information or delete the registration of an Ewon gateway,
- Adding, modifying, or deleting users or groups of the Talk2m account (a "group" is a collection of users),
- Adding, modifying, or deleting pools of the Talk2m account (a "pool" is a collection of Ewon gateways),
- Modifying the general settings of the Talk2m account and checking information about its usage,
- Establishing a VPN connection to an Ewon gateway. This operation will be described in a subsequent paragraph.

5.2 Registering an Ewon Gateway on a Talk2m Account

In a couple simple steps, an Ewon gateway installed inside the panel of a machine can be configured to connect to the Internet and be registered to the user's Talk2m account.

1. The first step is to use the Ecatcher client software to create inside the Talk2m account an entry for the Ewon gateway. A unique "activation key" is generated and will be used in the next step to authenticate the Ewon gateway and link it to its entry on the Talk2m account.

2. The second step consists in assigning the activation key to the Ewon gateway, to allow it to connect to Talk2m for the first time, authenticate to the user's account and complete the registration process. To prove that it is a genuine Ewon product and to provide a unique identification to Talk2m, the Ewon gateway will also use its "birth certificate".

Two main options are available to achieve this step:

- Launching "manually" the "Talk2m connection wizard" of the Ewon gateway from its web interface. During this wizard, the user will be asked to input the activation key retrieved in the first step,
- Configuring the Ewon gateway "automatically" by inserting into it a SD card or USB flash drive containing a configuration file that can be generated at the end of the first step and includes, among other information, the activation key.

Warning:

- Outbound access to the Talk2m domain name via outbound port TCP/443 must be opened in the End-User's network Proxy/Firewall: It is recommended to whitelist the wildcard domain *.Talk2m.com for access to all Talk2m servers, instead of using individual hostnames or IP addresses, for which failover scenarios would not be supported. For more details, please refer to the documentation "Addresses and ports used by Talk2m" :

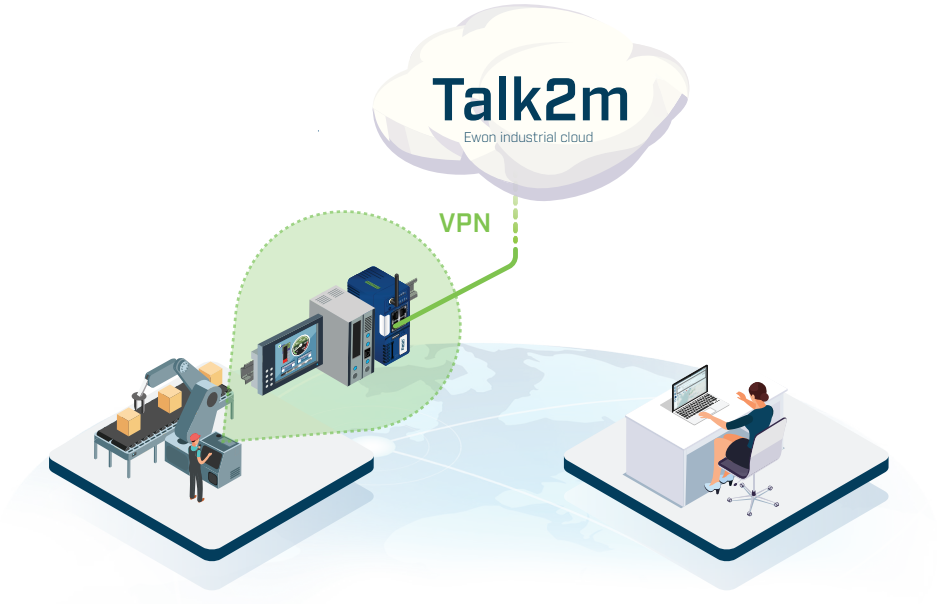
https://hmsnetworks.blob.core.windows.net/www/docs/librariesprovider10/downloads-monitored/manuals/knowledge-base/kb-0209-00-en-adresses-and-ports-used-by-Talk2m.pdf

5.3 Connecting a machine to Talk2m

Once registered on Talk2m, an Ewon gateway will automatically establish a VPN connection to the Talk2m service. This is performed in three phases:

1. An initialization process, during which the Ewon gateway will connect and authenticate to the Talk2m cloud service through a HTTPS connection, using its "birth certificate". If Talk2m recognises the certificate, the device is authorized to communicate with the cloud.
2. Then, the Ewon gateway will send a HTTPS request to ask for the most suitable VPN server it needs to connect to (this VPN server may change between connections).
3. Finally, the Ewon gateway will establish a VPN tunnel to the VPN server assigned in the previous step.

Once its VPN connection has been established, the Ewon gateway will appear on the Talk2m account with the status "online", and users with the appropriate permissions will be able to connect to it remotely.

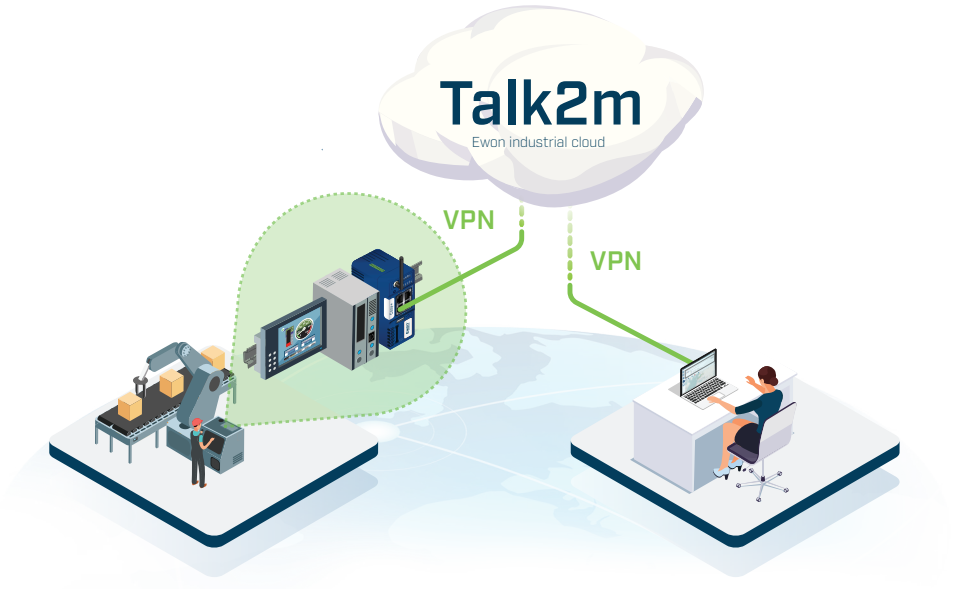


5.4 VPN connection from a user to a machine

To connect to a remote machine, a user will start by logging into its Talk2m account using Ecatcher. After successful login, a list of all the Ewon gateways for which the user possesses access rights is displayed.

To establish a VPN connection to an Ewon gateway whose status is "online", the user simply needs to select it in the list and click on the "Connect" button. Through a HTTPS request, Ecatcher will ask Talk2m to indicate the VPN server to which the Ewon gateway is already connected. Ecatcher will then also establish a VPN

to this server. Finally, the two VPN tunnels – the first one between the Ewon gateway and the VPN server, and the second one between Ecatcher and the VPN server – will be linked on the VPN server, to allow a secure communication between Ecatcher and the Ewon gateway. On the user's PC, a route is added to redirect through the VPN tunnel all the traffic whose destination IP address belongs to the range of the LAN IP of the Ewon gateway.



Once the VPN connection has been established, it is virtually as if the user's PC is directly connected to the network located on the LAN side of the Ewon gateway, through "one long secured cable". The user gets access to the devices installed inside the remote machine and can reach them by simply using their private IP address. For example, it becomes possible to connect to a PLC using its proprietary software and perform monitoring or maintenance operations remotely.

Once the work on the remote machine is completed, the user can click on the "Disconnect" button of Ecatcher to terminate the VPN connection. The route that was added on the PC is removed and it is not possible to reach the Ewon gateway or its LAN side anymore.

6. Ewon Gateway: strengthening the security of the industrial assets

6.1 Outbound VPN connection

The VPN protocol used by Talk2m is based on OpenVPN and uses OpenSSL. The authentication of an Ewon gateway or user (using the eCatcher client software) to Talk2m is done through the outbound port TCP/443 (HTTPS), and the actual VPN connection can be established either through the outbound port UDP/1194 (OpenVPN's default port) or through the outbound port TCP/443.

Since only outbound connections originating from a trusted network (such as a factory LAN on the Ewon gateway side, or an office LAN on the user side) are used, it is not necessary to open any port for inbound connections in the firewall protecting the network. Another advantage is that there is no need to use a public IP address for the Ewon gateway, which is therefore not "visible" on the Internet.

One effect of connecting to the Internet from inside a LAN is the possibility of having to pass through HTTP proxies. This will require proxy authentication settings to be provided in the Ewon gateway configuration or/and in the Ecatcher configuration. Proxies that are supported by both Ecatcher and Ewon gateways are:

- Proxy without authentication,
- Proxy with user and password authentication,
- NTLM Authorization proxy.

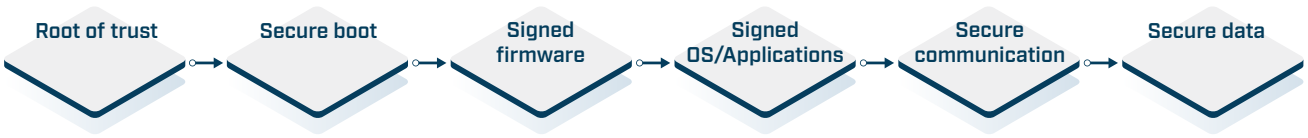
6.2 Chain of trust during the remote connection

The Ewon solution has been designed to protect all data exchanged between the industrial machine and the user, whatever the distance separating them. The security of information within the Ewon gateway is ensured thanks to cryptography and relies on three key principles: a trusted device identity, data confidentiality, and integrity of firmware running on the device. These translate into authentication, encryption and code signing.

However, without a mechanism to securely store cryptographic keys, the whole security strategy of establishing theidentity of a device, ensuring the confidentiality of communication and securely updating the firmware from any location is left with a major hole.

The foundation of a trustworthy IoT solution is therefore to implement a so-called "root of trust". In new generation Ewon gateways such as the Cosy+, a specific hardware chip called Secure Element is in charge of, on one hand, storing confidential information in a secure and non-modifiable manner, and on the other hand, performing cryptographic operations (generation of random numbers, encryption, decryption, signature, etc.).

This is the perfect starting point for the hardware root of trust. Where lines of code, an OS or a user interface may be altered, the data engraved in the silicon is resistant to change. With this security foundation in place, a whole chain of secure operations can take place.



Chain of trust

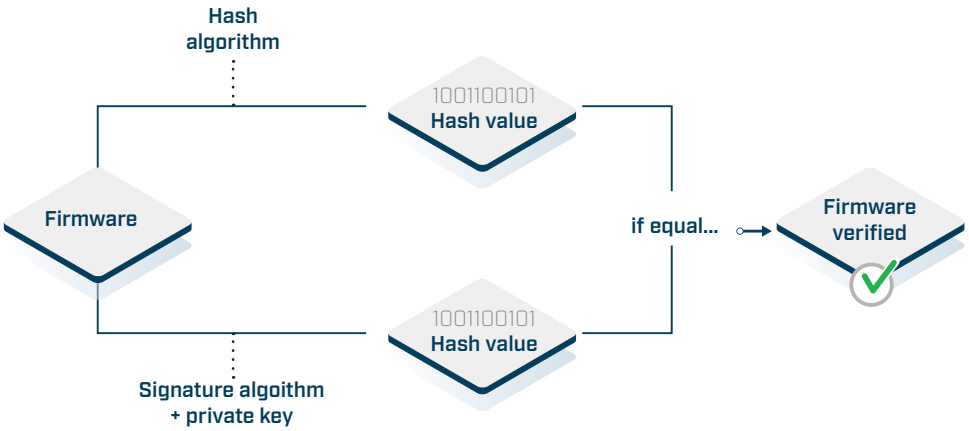
- **Secure boot process:**

  The insurance that only legitimate firmware produced by Ewon is loaded at startup.
  Secure Boot is the process ensuring that only genuine, manufacturer-validated software runs on the device. Without Secure Boot, a malicious actor could load its own Operating System or spoofed software into the device or even intercept secrets by interfering between the various stages of boot. Thanks to asymmetric cryptography and keys stored on the Secure Element, the signatures of the different pieces of code loaded during the boot are verified and only authentic ones are authorized. If the device detects a problem, it will not start.

- **Code signing:**

  The insurance that only legitimate firmware produced by Ewon is installed on devices.
  To maintain an effective security on devices and benefit from new functionalities, firmware updates are proposed regularly. To prevent installation of counterfeited firmware, the code is signed before traveling to the devices.
  The process of signing firmware is initiated through the computation of a cryptographic hash value. This value is signed with the private key of a private/public key pair before the signature is attached to the publicly released firmware image.

Before being installed on the device, the new firmware is verified. To ensure that the new firmware has not been tampered, the corresponding public key stored inside the Secure Element of the device is used to confirm that the hash value was indeed signed with the matching private key. By also computing the hash value of the firmware and comparing it to this validated hash value from the signature, the integrity of the firmware can be verified.



- **Birth certificate:**

  The insurance that only legitimate devices manufactured by Ewon can connect to Talk2m. A birth certificate is the electronic immutable device identity preventing enrollment of rogue, counterfeited devices to the Talk2m cloud. The certificate contains information such as a serial number, is signed by the Talk2m industrial cloud infrastructure and is securely stored inside the Secure Element. With this authenticated digital identity, access and permissions to Talk2m are granted and cryptographic integrity of all communication and data that the device processes is ensured.

6.3 Restricted access to the target equipment

A user connecting remotely should only be able to access to the target devices they need to work on, such as a PLC inside a machine requiring troubleshooting. Under no circumstances should they be able to gain access to other equipment inside the factory. An Ewon gateway connected to Talk2m is configured to perform a segregation between its LAN side, that the remote user will be able to reach, and its WAN side, often a factory network through which the Ewon gateway is connected to the Internet but that the remote user is strictly unable to access.

Adapting the IP subnet configuration on the LAN side of an Ewon gateway is also a way to easily limit the scope of devices reachable in a production line or a machine without specific parametrization at the Talk2m level.

6.4 Enabling communication with factory systems

Ewon gateways provide a "NAT 1:1" feature which is useful to allow a system located on their WAN side (for example a factory network), such as a SCADA or MES, to connect to devices located on their LAN side (machine network), such as a PLC. The NAT 1:1 feature makes it possible to map the IP address of the LAN devices to new virtual IP addresses belonging to the subnet of the WAN network. The LAN devices become therefore reachable by the factory system on the WAN side through their virtual IP address, as if they were on the same network.

Instead of using this NAT 1:1 feature, it is also possible to configure an Ewon "Flexy" gateway to read data from the LAN devices using its embedded industrial protocol drivers, and publish this data for the factory system on its WAN side after converting it to OPC UA.

6.5 Controlling the connectivity of the Ewon gateway

Using a connection through a factory LAN usually means that the Ewon gateway is always securely connected in VPN to the Talk2m service through the Internet. There are cases where factory owners might be reluctant to leave the Ewon gateway permanently online, if remote access is rarely needed, or if they want full control over the remote connectivity for security or safety reasons.

To allow a physical control of the connectivity on site, it is possible to wire a key switch, for example, to the digital input (DI) of the Ewon gateway. This key switch can then be mounted on the control panel of the machine and used by someone in the factory to locally enable or disable the connectivity of the Ewon gateway to Talk2m. The Ewon gateway could for instance be kept offline most of the time and only turned online when a remote maintenance operation is necessary.

In some cases, it can also be preferable to keep offline Ewon gateways equipped with modem and connecting to the Internet through a cellular network, in particular to save on SIM card data traffic costs. For isolated equipment with nobody around to manipulate a key switch, this can be achieved by configuring the Ewon gateway to use a "triggered" connection.

The Ewon gateway will then stay offline and only establish its VPN connection to Talk2m after receiving by SMS a "wake up" message. These wake up SMS messages can be sent from any mobile phone using as recipient the phone number of the SIM card installed inside the Ewon gateway, or from Talk2m using Ecatcher. Once the remote connection is not needed anymore, a "go offline" command can be sent from Ecatcher to the Ewon gateway to make it terminate its VPN connection.

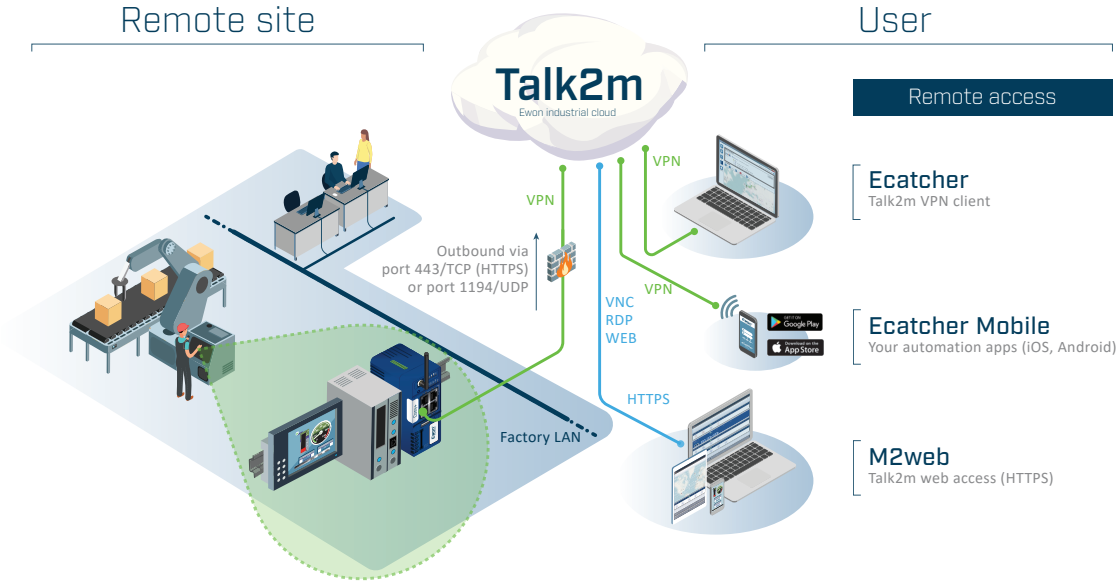
6.6 Keeping devices and software up to date

To minimize security risks, it is important to keep Ewon gateways up to date by installing new firmware versions that are made available, especially if they contain security vulnerability fixes. Ewon gateways can be updated manually by a user, even remotely through a Talk2m VPN connection. Newer models even offer the option of automatically installing new firmware releases, either in their full version or only by applying parts containing security fixes.

Similarly, the Ecatcher software is also regularly updated, and some updates might contain vulnerability patches. It is good practice to always use the latest version and a message is displayed in eCatcher to notify users of the availability of a new release.

HMS Networks publishes on its website cybersecurity advisories whenever one of its products is concerned by a vulnerability. It also has a responsible disclosure program and welcomes reports from the community on potential vulnerabilities in its solutions.

7. Talk2m Additional Services

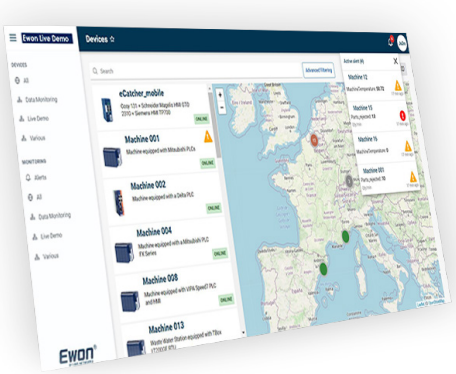


7.1 Ecatcher Mobile app

Users who wish to connect to their remote machines from a smartphone or tablet can use the "Ecatcher Mobile" app, available for free on Android and iOS. This app allows to establish a VPN connection through Talk2m, using the same principle as the Ecatcher client software for Windows, described in a previous chapter. Connecting in VPN from a mobile device is especially useful for users who want to access to a remote automation device using its proprietary app (for example: connecting to an HMI using the mobile app provided by the HMI manufacturer).

7.2 M2web: Ewon's web portal for remote monitoring

Users can connect to their equipment from any browser using the Talk2m web-portal, "M2web". This allows to establish a HTTPS connection to Talk2m servers from any device, without the need to install a specific application or software.



M2web URL: https://m2web.Talk2m.com

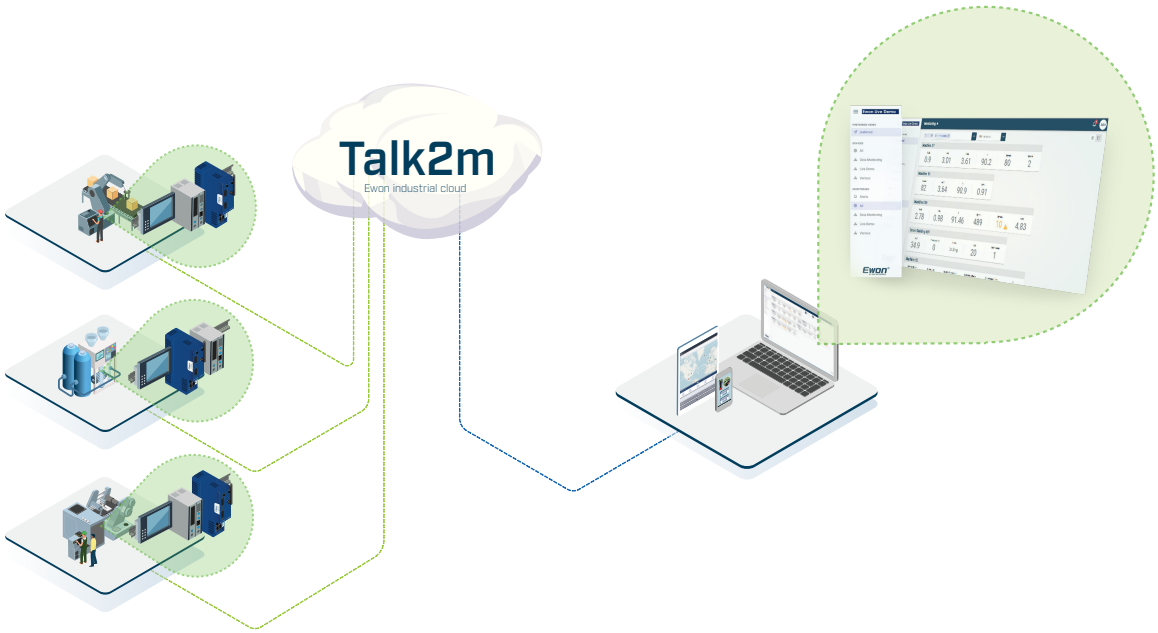
On the M2web portal, the HTTPS traffic originating from the user is redirected to the appropriate Ewon gateway through its VPN tunnel. M2web is used to connect to any automation device running:

- A web server (HTML5), such as an Industrial PC or an IP camera,
- A VNC server (Virtual Network Computing), such as an HMI (Human Machine Interface),
- A RDP server (Remote Desktop Protocol), such as a Windows device.

An M2web connection to these devices allows the user to remotely monitor and control the equipment in a very easy way.

7.3 Live KPIs for monitoring

Ewon Flexy gateways can read data from PLCs and other automation equipment and store this data into internal memory tags. For each Ewon Flexy gateway, up to 6 of these tags can be defined as KPIs (Key Performance Indicators), whose live values will then become visible to users (with appropriate permissions) when they log in to their Talk2m account from the M2web portal or the eCatcher Mobile app. The transfer of these KPI live values is carried out through the VPN tunnels connecting the Ewon gateways to the Talk2mm VPN server, and only starts when a user logs in to their account. The data transfer stops when the user logs out and no data is stored on the Talk2m server. This feature allows users to conveniently monitor in one central place the status and performance of all their machines equipped with an Ewon Flexy gateway.



Talk2m live KPIs

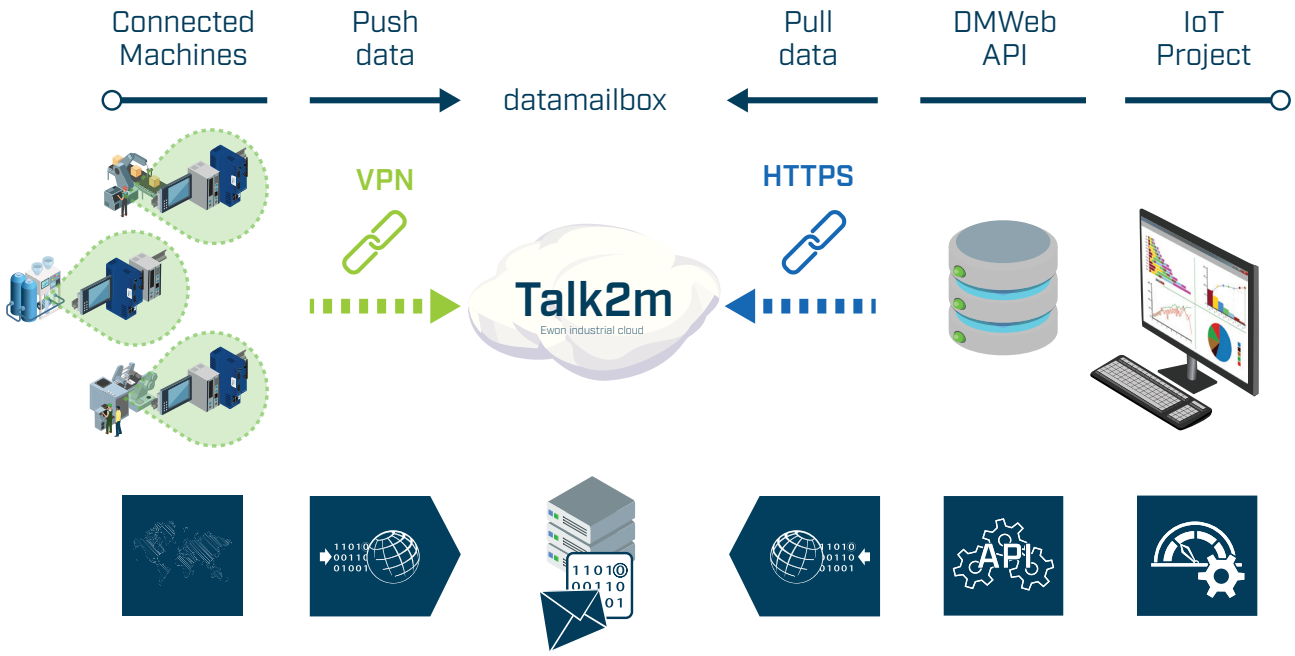
7.4 Notification services: SMTP relay, SMS gateway

Talk2m also offers other services in addition to remote access. SMTP relay and SMS gateway servers are also part of the Talk2m infrastructure and provide users with easy way to receive email or SMS notifications from their equipment, based on the alarm system available in the Ewon gateways. Indeed, data gathered from a PLC or other industrial device connected to an Ewon gateway can be used to trigger alarm messages, which can be forwarded to Talk2m through the machine VPN tunnel. When these messages reach the Talk2m platform, they can be relayed on the Internet as an email and/or SMS.

7.5 Talk2m APIs

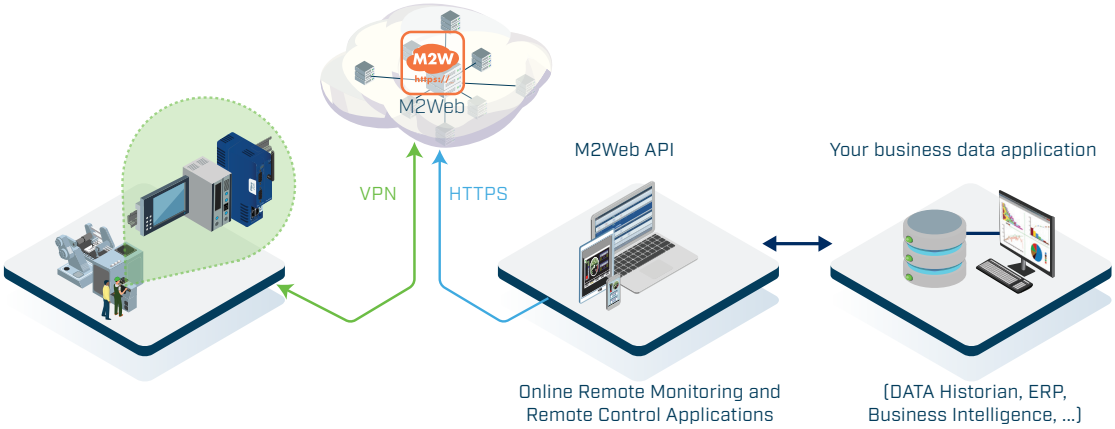
Talk2m provides REST APIs, which allow a third-party software to easily collect data from, or interact with remote machines equipped with an Ewon gateway. These APIs are:

- The datamailbox service (Dmweb API), which allows the retrieval of historical data from multiple machines in an easy and reliable way. Ewon gateways can be configured to regularly push the historical logging of the data they have collected from machines to Talk2m through their VPN tunnel. This data is temporarily buffered on the Talk2m datamailbox servers for a maximum of 10 days, and IoT software can use the datamailbox API to efficiently retrieve the data of all the Ewon gateways, without any loss or duplicate, via HTTPS queries to the user's Talk2m account.



datamailbox service for collection and integration of historical data into IoT software

- The **M2web API**: The M2web API can be used by IoT software to send queries to the web services of an Ewon gateway, for example to control it or a device connected to its LAN side, or to retrieve live information from the remote machine. The communication between the IoT software and Talk2m is made through HTTPS, while the communication between Talk2m and the Ewon gateway goes through the VPN tunnel.



Work with HMS Networks. The number one choice for industrial communication and IIoT.

Anybus® BY HMS NETWORKS

Ewon® BY HMS NETWORKS

Intesis™ BY HMS NETWORKS

Ixxat® BY HMS NETWORKS

www.hms-networks.com