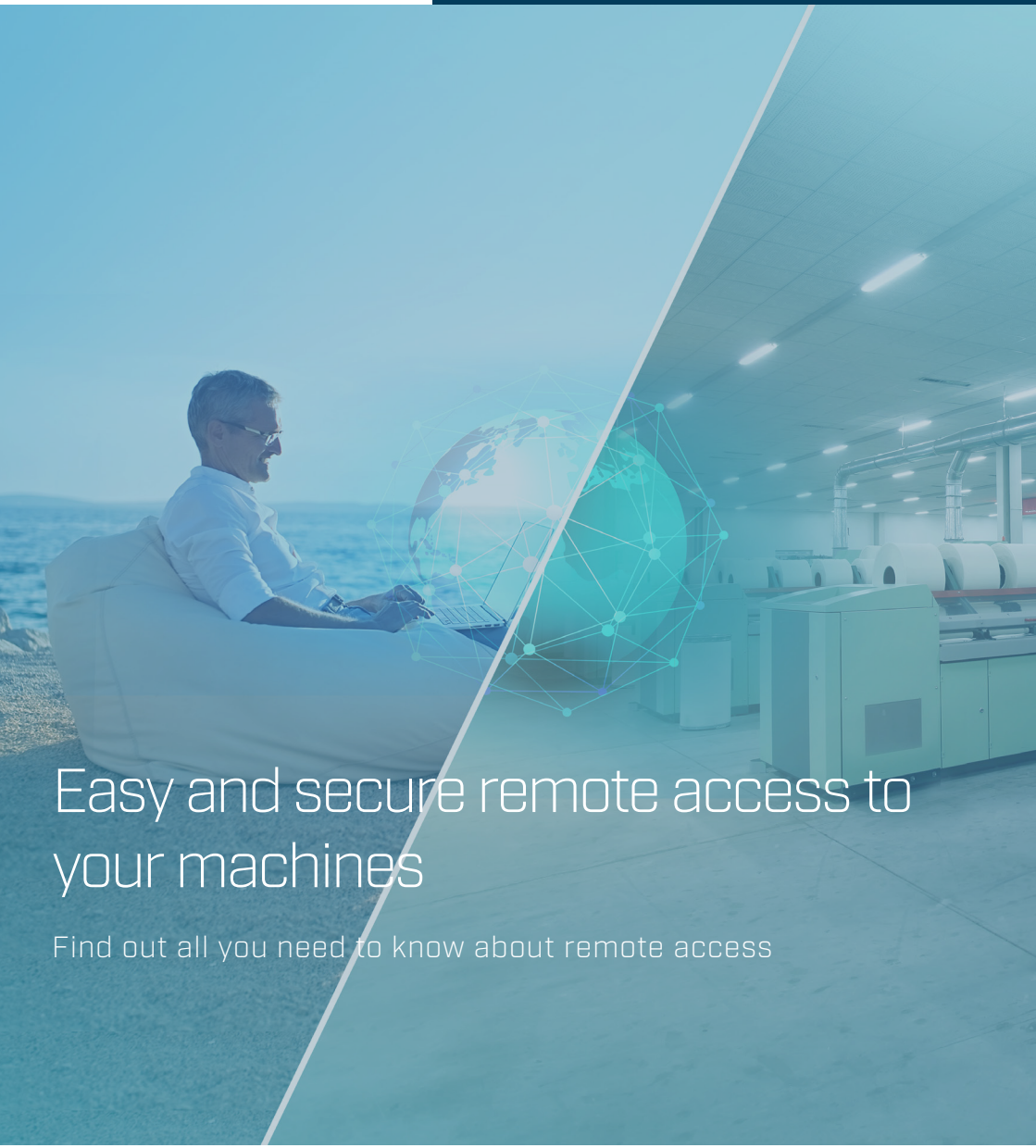
Ewon® BY HMS NETWORKS

White paper:
Get started with industrial remote access



Easy and secure remote access to your machines

Find out all you need to know about remote access

Überreicht durch:

WACHENDORFF Prozesstechnik GmbH & Co. KG

HMS

Table of contents

Introduction

In the industrial sector, after-sales engineers and technicians must regularly travel to factories to service machines and various pieces of equipment. Wouldn't it be wonderful – for the machine builder as well as the industrial company – to be able to perform these operations remotely and to solve most problems simply and securely, no matter where you are?

Assumptions

We assume that you work in the field of manufacturing and/or automation. So while you may be perfectly familiar with the machines and their PLCs that you market, build, maintain or use, you may be less comfortable with technologies such as remote access, the Internet, security, cloud computing and the use of the data provided by your machines.

Icons used in this white paper

Throughout this white paper we use special icons to draw attention to important information. These are as follows:

This icon indicates important information to keep in mind.

This icon indicates technical content.

This symbol indicates useful information.

Pay attention to this advice and you will avoid making potentially costly mistakes.

Beyond the white paper

For your convenience, we limit ourselves here to an introduction to industrial remote access. If you wish to explore the subject in more detail, we invite you to visit our website: **https://www.ewon.biz**

What is industrial remote access and what are the advantages?

In this chapter we will ask the following questions:

- Why has remote access become more necessary than ever?
- What are the options for remote access to your machines?
- What are the advantages of remote access?

Definition of the need for remote access

Industrial machine builders have always dreamed of being able to connect remotely to their machines. Indeed, for original equipment manufacturers (OEMs) with fleets of machines installed at many distant customer sites, as well as for companies manufacturing at multiple sites, being able to remotely view the functioning of equipment offers a clear competitive advantage.


Advice

Common use cases for remote access to industrial machinery include:

- Troubleshooting and remote programming of programmable logic controllers (PLCs)
- Remote viewing and control from your human-machine interface (HMI)
- Connection to a webcam for help
- Assistance to field technicians for commissioning

Advantages of remote access

The ability to remotely access a machine's control system can help troubleshoot and resolve the majority of problems encountered, avoiding the need for technicians or engineers to travel to the site. These problems can often be resolved not so much by repairing the machine as by adjusting its programming or settings. They are often due, for example, to changes in raw materials, machine wear and tear or other production parameters that may have changed over time. Remote access is the first essential step towards the digitalisation and utilisation of data.

Advice

Remote access allows you to move from a reactive to a proactive support model that helps you remain competitive. Indeed, once you are remotely connected to your machine (or fleet of machines), you can, in addition to troubleshooting them and rapidly intervening, analyse the data for other purposes. For example, to:

- improve responsiveness
- reduce the impact of emergencies
- optimise the workload of engineers
- maximise machine availability and productivity
- reduce travel costs
- minimise environmental impact
- increase your sustainability
- minimise the downtime of your machines
- maximise overall equipment effectiveness (OEE)
- maximise safety

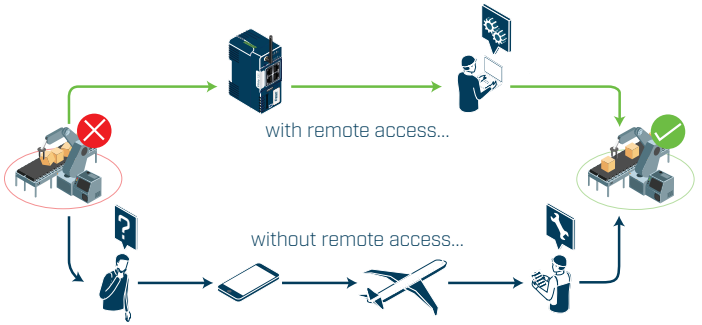
Rapid problem resolution means less downtime and a faster return to production for the end customer. In cases where physical intervention at the site is still necessary, remote access can help ensure that the person travelling to the site has the right skills, machine parts and tools - increasing the chances of correcting the problem in one visit. All this contributes to a better customer experience and minimises machine downtime.

The pressures on industrial companies to adopt remote access strategies have only intensified in recent years. The global emergence of teleworking, for example, has contributed to this. The ultimate accelerator has been the Covid-19 crisis and the fear of industrial companies that allowing outsiders to visit their facilities poses a risk of contamination for the personnel.

It is clear that ecological, economic and societal aspects also play an important role. Sustainability and environmental impact are becoming increasingly important in our lifestyles. In this regard, it is clear that industrial remote access is an effective and secure way of contributing to this objective, while minimising costs and increasing equipment effectiveness (OEE).

Machine builders also recognise the opportunity offered by remote access to create new revenue-generating, proactive and preventive services that can be offered to their customers. We are referring here to the exploitation of data to facilitate predictive maintenance.

Ultimately, remote access allows greater efficiency for everyone. Machine builders can gain competitive advantages, as illustrated in Figure 1-1, so as to serve more customers and reach new markets; while machine users will see their OEE increase.



- Reduce costly visits to the site
- Live and online assistance for your customers
- Regular contact with your equipment
- Reduced environmental impact
- Reduced machine downtime
- Maximised OEE
- Increased safety
- Increased productivity

Figure 1-1: Achieve greater efficiency and a competitive advantage thanks to remote access

History of remote access

In its early stages, remote access to machines consisted of “point-to-point” management using a terminal console connected via an analogue landline telephone and a modem. These systems were slow, often difficult to install, and expensive to operate and maintain.

However, remote access via a router connection continues to be popular today, thanks to the availability of high-speed cellular networks. The main attraction of this method of remote access is the ability to access the data of the machine controller (PLC), while avoiding the use of the computer network of the customers. Wireless routers that communicate via the data networks of mobile telephony providers are available from many PLC suppliers.

This approach avoids the need for a wired telephone line or the need to tap into the company's computer network, although the availability of the wireless signal in production areas can sometimes be problematic.

That means continuous network access and user fees that can rapidly accumulate.

Leveraging the Internet

A better way to access machines remotely is to take advantage of Internet technology and cloud computing. The main challenge is to *securely* manage the machine's connection to the end-user's corporate network and, consequently, to the Internet. IT departments in most companies are reluctant to grant access to the company network to non-employees for obvious security reasons.

Remote access on demand

Machine builders do not particularly need continuous connections. Indeed, remote access for troubleshooting, maintenance or servicing of the machine can be provided by an on-demand connection, minimising costs and increasing security.
What are the advantages of access on demand? First, the end user may want to prevent continuous remote access to the machine. Disconnecting the machine from the local area network (LAN) is not essential for security, but it gives the end user physical control over when the machine is accessible and for how long. In this situation, the machine is usually disconnected from the local area network. The machine is only connected when necessary or at the request of the machine builder.
In addition, when the remote connectivity is based on a volume-based pricing option, such as cellular technology, it may be desirable to establish a connection and pay only when necessary;-).

Outbound connections

Virtual private networks (VPNs) are an excellent solution from a technical point of view. However, enabling appropriate inbound network access while ensuring security can be a complex task. Each PLC builder typically uses a different set of network ports, and defining a clear path through a customer's firewalls requires careful configuration. Moreover, this is regularly rejected by IT departments, which are reluctant to create security loopholes.
By relying on an outbound connection on the factory's local area network (LAN), you can solve many firewall problems from the outset. This is because if no inbound connections are established, no ports need to be activated in the company's firewall for inbound connections, and no IT changes are required to establish the communication; this is completely secure.This configuration allows the engineer to access authorised machines, while preventing access to the factory network (LAN).

Software-based solutions

Using the internet, a local supervising PC can be accessed and controlled remotely using Virtual Network Computing (VNC) technology or other remote access software on a PC. In this scenario, the software replies and relinquishes control of the remotely accessible operator interface computer. Although this type of solution may be acceptable for remote connection to a PC, it generally provides the user with access to the entire network, which is not acceptable from a security perspective.

This approach assumes that there is an industrial PC capable of running the application on the remote machine. This hardware and software involves additional expenses, making its total cost higher than that of a dedicated solution.

VPN solutions based on a secure industrial router

The best solution is to use an on-demand VPN connection using an industrial router and a secure cloud-based infrastructure. An SSL (Secure Sockets Layer) VPN connection generally presents few problems for a customer's IT department.

This method is even more interesting from a security perspective because it automatically adds logical network segregation between the machine and the factory LAN. Machine builders can manage fleets of machines via one simple and secure interface. End users, for their part, can use the platform to manage remote access rights.

As this is the best solution, we will deal with it in detail in the following chapters.

Chapter 2

Understanding and using the Ewon remote access solution

This is what you will find in this chapter:

- Introduction and functioning of the Ewon Cosy and the Talk2M industrial cloud
- How to connect to the Talk2M industrial cloud
- How to use eCatcher to connect to your machine via Talk2M
- How to communicate over a VPN connection
- Other solutions from Ewon

Introduction to the Ewon Cosy industrial router

The Ewon Cosy, a secure industrial router, allows secure remote connection to a machine or piece of equipment. With the Ewon Cosy, machine builders and industrial companies can troubleshoot their machines, correct PLC errors and remotely use a Human-Machine Interface (HMI) or operate an IP camera, without the need to travel. The Ewon Cosy is compatible with the vast majority of PLCs on the one hand, and with older machines ("legacy/brown field equipment") on the other hand.

This approach allows you to:

- significantly reduce costs
- improve machine efficiency
- minimise the carbon footprint
- easily upgrade older equipment

How does the Ewon Cosy work?

The Ewon Cosy establishes a secure VPN connection between you and your machine, anytime, anywhere. The connection is established via Talk2M, a highly secure industrial cloud. The Ewon Cosy allows connection via Ethernet or wirelessly (4G or Wi-Fi) for easy remote access in any situation.

The Ewon Cosy coupled with Talk2M makes it easy for users to connect to their machines via the Internet, as shown in Figure 4-1. This solution is very easy to use and does not require any special IT knowledge.

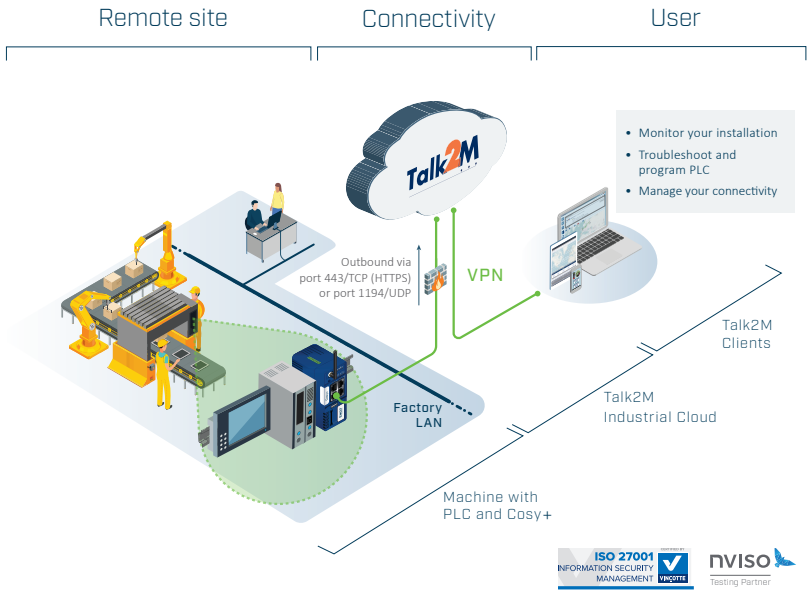


Figure 4-1: Talk2M is an industrial cloud that allows users to connect to their machines via the Internet.

Ewon offers users three solutions for connection via Talk2M to their machines:

- eCatcher: a Talk2M client software
- eCatcher Mobile: an application for smartphone
- M2Web: a dedicated Internet portal

Advice

You can also use a web browser (such as Google Chrome, Microsoft Internet Explorer / Edge or Mozilla Firefox) without installing the eCatcher application to connect to your machines (called M2Web).

Connecting your machine to the Internet using the Ewon Cosy

To connect your machines to the Internet, there are several possibilities:

Wired network (Ethernet): Most industrial sites are equipped with wired networks to connect to the Internet. This method is often preferred. An Ethernet LAN connection is usually free and provides reliable, high-speed access. In some cases, local area networks are subject to complex security policies that may restrict the connection of your machines. In these cases, wireless connections can be an alternative.

- **Wireless network (Wi-Fi)**: Wi-Fi networks are becoming increasingly common in factories. Like LAN connections, Wi-Fi access is usually free and offers high-speed connectivity. Many factories provide “guest” Wi-Fi networks that are logically separate from the company's LAN. This solution allows machine builders and users to access the Internet without the need for firewall configuration changes.

- **Cellular network (4G)**: When no LAN or Wi-Fi connection is available, cellular technologies are a good alternative. The cellular service is generally available worldwide at various speeds, but signal coverage may be limited or unreliable in some areas. Moreover, the costs of using data on a cellular network can be high and cellular technology is not the same everywhere, potentially requiring the installation of different SIM modules in the machine's routers. This is the reason why LAN or Wi-Fi connections are generally preferred if available.

Connecting of the machine to Talk2M

Once you are connected to the Internet, the Ewon tries to connect to Talk2M in three phases:

1. The Ewon connects to a central access server (AS) and authenticates itself via a Hyper Text Transfer Protocol Secure (HTTPS) session.
2. The Ewon requests the IP address of the VPN server to be used (VPN server addresses can change from connection to connection) via an HTTPS connection.
3. The Ewon establishes a VPN tunnel with the VPN server.

These phases are shown in Figure 4-2.

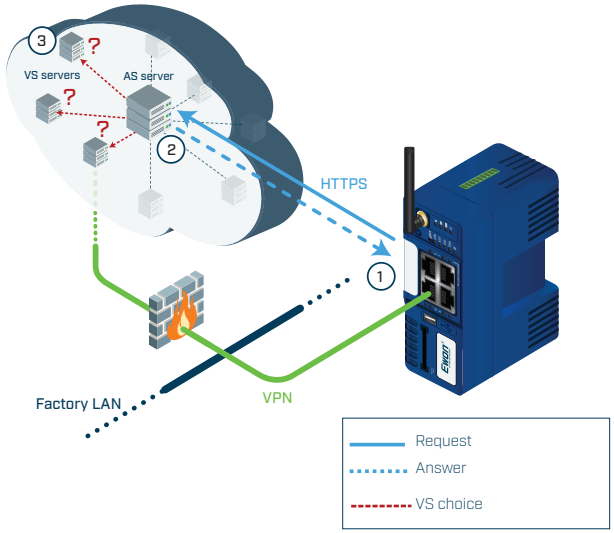


Figure 4-2: Connecting of the Ewon to Talk2M in three phases.

Connecting of the user to Talk2M

When the user starts the eCatcher software, the first step is to authenticate their identity using the following information:

- **Name of account:** A Talk2M account can be created with eCatcher. An unlimited number of accounts can be created. Each account contains all users who are allowed to connect to the Ewon devices registered in that account.
- **User name:** An unlimited number of users can be registered in an account. User names in an account must be unique.
- **Password**: Each user has their own password.

Attention

After authentication, you can access the list of Ewons registered on a Talk2M account and for which you have access rights. The list provides the following items:

- The name and status of each Ewon
- A brief description of the Ewon and the connected machine
- All users currently connected to the Ewon
- All parks (groups of Ewons) connected
- The type of controller (PLC)
- The type of remote connectivity (such as LAN or cellular)
- The IP address of other pieces of equipment declared on the Ewon's network

When you click on a listed Ewon, if its connection status is indicated as “Online” (which means that a VPN connection is being executed), eCatcher creates a VPN tunnel to the assigned Ewon.

You can also perform several other actions in eCatcher, such as:

- Registering a new Ewon in the current account
- Editing and deleting information about the Ewons
- Adding, changing or deleting user or group information in the current account (a group is a set of users)
- Adding, changing or deleting parks in the current account (a park is a set of Ewons)
- Editing account information

Using the VPN connection

When a VPN connection is established, two “tunnels” are created: one between the Ewon and the VPN server, and the other between eCatcher and the VPN server. This is illustrated in Figure 4-3. Each tunnel is automatically assigned a unique VPN IP address. Although the VPN addresses are accessible on the Ewon side and the eCatcher side, they are not accessible on the VPN server side.

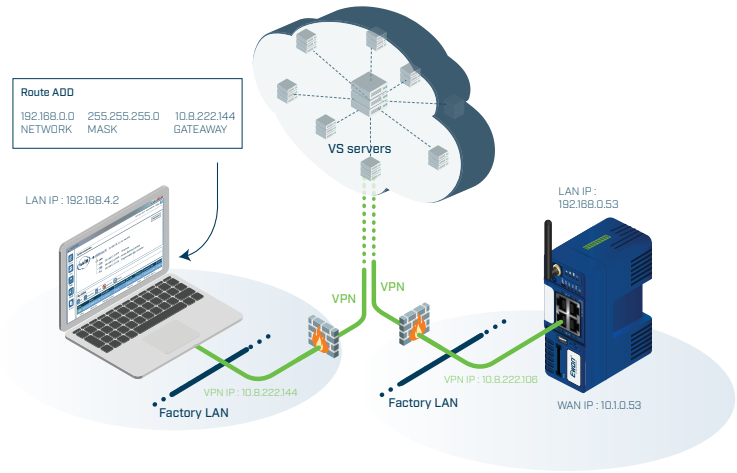


Figure 4-3: the eCatcher software automatically adds a route to the LAN IP address of the destination Ewon.

Technical Content

To reach the machine side of the Ewon, your computer/tablet/smartphone needs to know that all traffic containing a destination IP address within the IP address range of the Ewon LAN must be forwarded via its virtual interface. To enable this, eCatcher automatically adds a route when a VPN connection is opened and automatically removes the route when the VPN connection is closed, as shown in Figure 4-3. The eCatcher software knows the LAN IP address of the Ewon because it is provided when each Ewon registers in a Talk2M account. If you want to connect to another Ewon, eCatcher automatically deletes the previous route and adds a new route with the appropriate range of destination addresses.

On the machine side, traffic passing through the VPN tunnel is automatically transferred to the LAN (machine) side of the Ewon. For a machine on the LAN side to communicate with the user, you have two options:

- A network address translation (NAT) feature (also called “Plug'n Route”) can replace the Ewon LAN IP address with the user's IP address (this is the default setting in the Ewon).
- Individual machines on the LAN side of the Ewon can be manually configured to use the Ewon's LAN IP address as the default gateway.

Becoming familiar with other Ewon solutions

Remote access via the Ewon Cosy and Talk2M is a first step on the road to digitalisation. To go further, Ewon offers monitoring and data capture solutions via the Ewon Flexy and Talk2M.

The Ewon Flexy, while being a truly versatile IIoT gateway, is also an advanced industrial router. In addition to remote access, it allows you to monitor and collect key performance indicators (KPIs) that are essential for optimising effectiveness (OEE). It also allows you to feed this data back from the machine to the cloud and analyse it for the organisation of predictive maintenance.

The features of the Ewon Flexy include:

- Secure VPN remote access: The Ewon Flexy also includes a VPN compatible with Talk2M, enabling highly secure remote access for maintenance, monitoring and data capture. It enables remote connection to the PLC, the IP camera, the HMI etc.

- Expansion cards: In addition to the basic functionality, the Ewon Flexy can be adapted to your specific connectivity needs by adding expansion cards (Ethernet, Wi-Fi, 4G, USB, serial,...).

- Data acquisition: Local data acquisition is performed by the Ewon Flexy using the serial or Ethernet port. The acquisition process is built around a tagged database in which each tag is associated with an input/output (I/O) server.

- Alarm and notification management: The Ewon Flexy allows alarms and notifications to be triggered and tracked. Alarm thresholds and parameters can be set on each variable. The complete alarm cycle is traced and available for monitoring and analysis. Alarm notification can be done by email, SMS, or SNMP (Simple Network Management Protocol) and/or FTP (File Transfer Protocol) trap.

- Data recording and retrieval: Continuous data recording and buffering can be performed on each variable. Each variable can be recorded at a fixed interval or triggers can be changed. The Ewon stores data values and time stamps them in its internal database (up to one million time-stamped points) for statistical analysis and later review (historical recording), or to analyse recent trends (real-time recording).

- HMI (Human-Machine Interface) web server: The Ewon Flexy has an integrated web server for configuration and the visualisation of data, which can be viewed in any standard web browser.**- Talk2M API:**Use the API for enterprise integration of third-party software and cloud solutions (e.g. Ewon IIoT Partners: AmazonWeb Services, Microsoft Azure, Siemens MindSphere, IBMBluemix and others).

The Ewon Flexy can be used in particular for connection in the areas of cleantech, photovoltaics, building management, smart metering, water and wastewater management, energy monitoring, irrigation systems, etc.

Figure 4-4 illustrates these application areas.

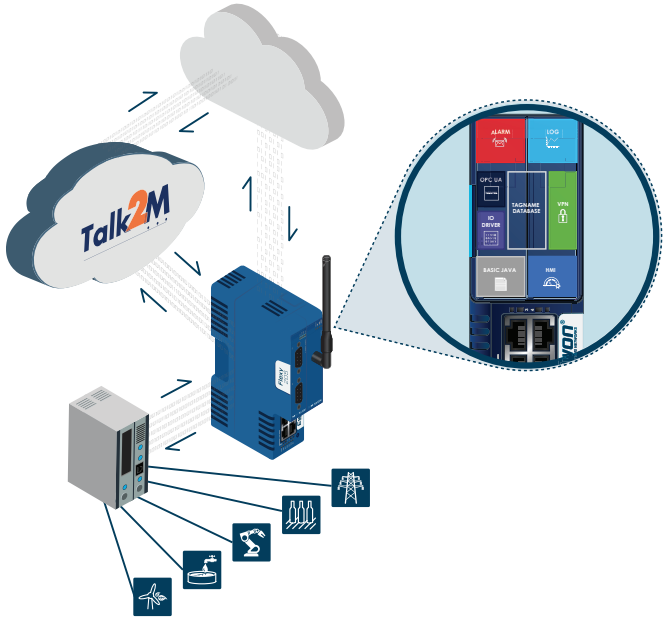


Figure 4-4: The Ewon Flexy connects remote pieces of equipment using different communication protocols.

Advice

For more information on the Ewon Flexy, visit **www.ewon.biz/flexy**

Ensuring secure and reliable remote access

In this chapter, you will be able to:

- discover tips for better security
- learn more about cybersecurity threats
- learn more about firewalls and VPNs
- choose a web-hosted architecture
- adopt a “multi-tiered” security approach
- discover the Ewon Cosy and its features

Tips for better security

Security is like a chain that can break at any time because of its weakest link. It is therefore essential to find the best compromise between security and ease of use. To do this, here are a few tips that can be easily verified before implementing an industrial remote access solution:

1. The factory's firewall should not be modified, so as to ensure its integrity. By using an outbound connection you minimise the risk of creating an opening in your networks. Furthermore, thanks to a key switch or an HMI button, the end user maintains physical control over remote access. “All you have to do is turn the key.”
2. Be able to audit your connections! The administrator must be able to determine who has had access, when, and to what
3. Multi-factor authentication: In addition to traditional identifiers (username/password), it is advisable to use a second layer of security with the help of multi-factor authentication. For example, by means of an identification key sent by SMS, which is different for each connection.
4. Certification: It is important that the solutions you use are professionally audited and certified. The ISO 27001 standard is of course the reference in this regard. However, it is important to be sure of the context of this certification and what exactly it certifies. For example, certification can be limited to the writing of the instructions for use, which is not very helpful. We recommend that you ensure that the cloud, the connections and the industrial router all meet the relevant standard.

5. Audit and penetration testing: Make sure your provider is properly audited by a reputable external company that updates its tests frequently. The aim is, of course, to remain in step with events and avoid repeating the same test or the same process every year or auditing a part that is too limiting.

6. Finally, let's not be naive: “all that glitters is not gold” – So choose a serious, established and specialised partner.

Cybersecurity threats

Large security breaches, usually involving the disclosure of millions of identifiers, are frequently reported in the media. However, there is a far greater and potentially more devastating threat: cyber attacks on critical infrastructure and machinery. This includes in particular utilities, emergency systems, environmental controls for buildings and industrial equipment.

Here's an example: In May 2021, Colonial Pipeline, which supplies 45% of all fuel consumed on the US East Coast, was the target of a cyber attack. The ransomware attack forced the company to close its 8,000 kilometres of pipelines for several days.

Groups of hackers, usually motivated by financial gain, but also by a political or social cause, may try to obtain ransom money or damage industrial machinery connected to the Internet. Some states are also engaged in cyber attacks to achieve various strategic objectives.

For example, the Stuxnet virus in 2010 was allegedly developed by one or more nations targeting the Iranian nuclear programme. The virus infected vulnerable PLCs and Siemens' Step7 software at Iran's Natanz nuclear facility, causing centrifuges to spin at varying speeds, inducing excessive vibration and thus destroying them.

More recently, the introduction of malicious code into the security software of the Solarwinds company is said to have infected more than 18,000 customers and allowed the exfiltration of data. Its CEO, Mr Mandia, said the attack could only have been carried out “by a country with first-class offensive capabilities”.*Security must therefore be a priority for all machine builders, original equipment manufacturers (OEMs) and system integrators looking to connect remotely to their customers' machines.*

According to a recent report by Palo Alto Networks, 98% of IoT traffic is unencrypted and nearly 60% of the devices are vulnerable to (moderate to severe) cyber attacks. It is more important than ever to protect factories against malicious attacks, which are becoming increasingly complex and sophisticated.

Understanding firewalls and virtual private networks (VPNs)

Firewalls control the flow of traffic between networks such as a local area network (LAN) and the Internet. A firewall is usually installed at the edge of the network it protects and may consist of a hardware device, software or a combination of hardware and software.

Advice

You can think of a router as the entrance to a medieval castle, and the firewall as the drawbridge at the entrance, controlling access to the castle.

Although many advanced designs and technologies exist, the basic function of a firewall is to filter all traffic coming from an unapproved network (such as the Internet) based on a set of pre-configured rules.*By default, all outbound traffic from the trusted network is allowed* (e.g. from the LAN to the Internet). Inbound traffic sent in response to an active outbound connection is also allowed. Inbound traffic from the Ewon web page www.ewon.biz will be automatically allowed through the firewall in response to the request started by a web browser.

However, any inbound traffic that is not explicitly associated with an outbound traffic request is blocked by default. To allow certain inbound traffic from the Internet, firewall rules must be configured to allow a specific type of traffic, from a specific source, and to a specific destination.

While a firewall protects the systems (including the machines) and data on the LAN from unauthorised access, it does not protect the confidentiality and integrity of Internet traffic sent and received over the LAN. *This is what makes a virtual private network, or VPN, so interesting.* VPN technology creates a tunnel between two machines or two networks. An encryption key is generated between the two ends and is used to create an encrypted “wrapper” protecting the data at the source. At the other end of the communication tunnel, the destination gateway “unpacks” the data and decrypts it.

Using a web-hosted architecture

You can choose to install a VPN solution on your PC yourself. You will then need to install and configure the software so that communication is established and is secure. This is not necessarily an easy task and incorrect configuration of the security settings would undermine the intended purpose. We believe that machine builders should only concern themselves with maintenance activities conducted on their machines, without the IT complications. That's why we designed Talk2M. Thanks to our hosted solution, there is no need for complicated configuration by the users. The VPN server configuration is outsourced from the PC to the cloud and the technical and security configurations are set up by our expert engineers. Users connect to their machines with the greatest of ease and focus on their tasks, as illustrated in Figure 3-1.

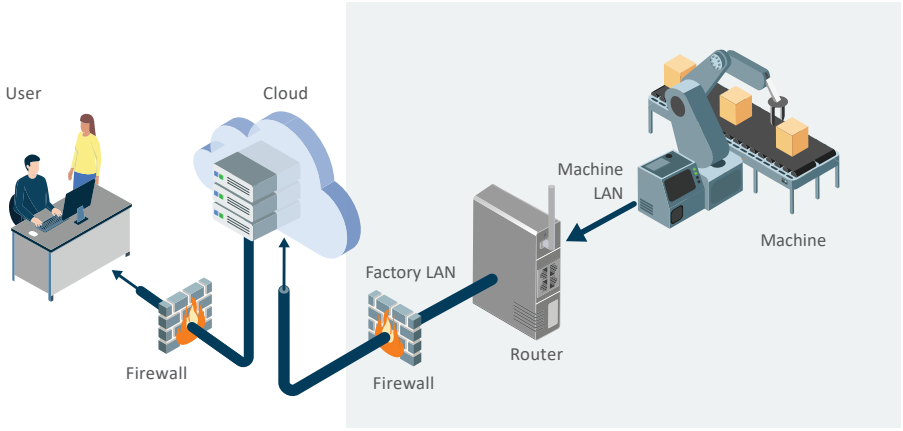


Figure 3-1: Use of a VPN server to securely connect to your remote machines.

However, if instead of being installed on a single machine (PC) the VPN server is hosted by an independent organisation in a cloud service (SaaS) offering, it can be shared between multiple machine builders, each with a private account and each able to configure their customers and machines individually. *A cloud-based architecture inherently offers better scalability than a purely physical architecture* based on hardware gateways or internal software applications.

A cloud architecture allows for load balancing by distributing the necessary connections and VPN tunnels over several servers. It also provides redundancy and thus ensures the resilience of remote access services in the event of an interruption to operations or a disaster.

Discovering Ewon's “multi-tiered” security approach

One of the main challenges of remote connections is balancing the needs of a PLC engineer or technician with the mission of an IT department, which is to ensure the security, integrity and reliability of the network. Finding a solution that is readily accepted by both entities has been a challenge for many years and a source of frustration and inefficiency for all stakeholders. Maintaining network security is essential for gaining acceptance with the IT department, but users do not want solutions that are complex, difficult to implement or that impede productivity. *By focusing on both security and ease of use, Ewon has created a remote access solution that is suitable for both end users and IT managers.*

Safety and reliability are two key aspects of Ewon solutions. They are based on a “multi-tiered security” strategy that uses several layers of security countermeasures, as shown in Figure 3-2.

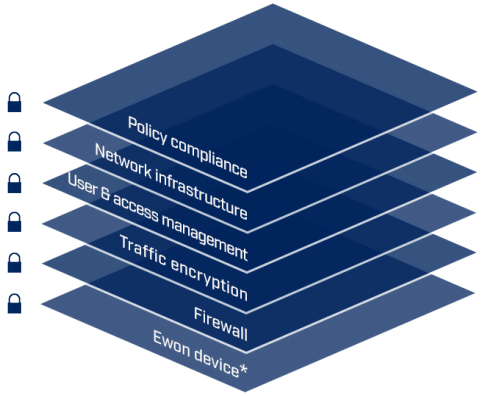


Figure 3-2: Ewon's multi-tiered defence strategy.

The objective is to protect the integrity of the Talk2M industrial cloud connectivity and information system, based on numerous publications, guidelines, best practices and established security standards, such as:

- ISO/IEC 27001 (International Organisation for Standardization and International Electrotechnical Commission)
- US National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity, Version 1.0
- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)

Reminder

From hardware to policies and procedures, security is a key component fully integrated at every level of Ewon solutions. The different layers of Ewon's defence-in-depth strategy consist of the following elements:

- **Ewon router*:*** Users must be authenticated. Traffic on the machine/LAN side is separated from the WAN/customer side and users can only access authorised devices on the LAN. The specific controls include four key aspects
  - Network segregation: Industrial routers are usually installed in the control panel of the machine, with the machine connected on one side (LAN) and the factory's network on the other (WAN). When a connection needs to be established, the Ewon device acts as a gateway through which all traffic passes. When the Ewon is initially configured, the device's security settings limit traffic between these two network interfaces. This network separation limits remote access to only those devices connected to the Ewon's local area network; it prevents access to the rest of the network.
  - Device authentication: Ewon routers have access rights that differ from those of Talk2M. Only users with the appropriate credentials and access rights can change the security settings of Ewon routers. Similarly, for devices with data services, only authorised users can view or change the data.
  - Physical switch: All Ewon hardware devices have a digital input. A physical switch can be connected to this input to enable or disable the WAN port. This allows the end user to retain full local control over whether or not the device is remotely accessed.
  - IP assignment and control:The Ewon needs the same type of settings as a PC connected to the same network (IP address, subnet mask and gateway, as well as all optional proxy settings). The Ewon can be configured to receive these settings automatically via DHCP. However, the Ewon can also be configured to use a static IP address assigned and controlled by the IT department, if desired.
- **Firewall:** In the eCatcher application, Talk2M account administrators can set filtering and firewall rules that indicate which devices behind the Ewon can be accessed remotely and even on which ports (Ethernet, USB or serial) and with which protocols they can be accessed. Talk2M provides four different firewall configurations based on the IP address, ports, gateways and access to Ewon services of the declared devices. From the least restrictive firewall level through to the most secure level, they can be described as:
  - Standard: Access to all devices connected to the Ewon network is granted.
  - High: Access only to explicitly listed devices connected to the Ewon's LAN; port restrictions are also possible.
  - Reinforced: Access to the Ewon gateway can be blocked.
  - Ultra: Access to Ewon device services such as HTTP, FTP and SNMP can be blocked.

When associated with the management of Talk2M user rights, administrators can customise remote access rights for specific user groups.

- **Encryption:**Communications between the remote user and the Ewons are fully encrypted using Transport Layer Security (TLS), ensuring data authenticity, integrity and confidentiality. All users and Ewon units are authenticated using x.509 certificates, and end-to-end traffic is encrypted using strong symmetric and asymmetric algorithms
- **User management and responsibility:** Each Talk2M account can have an unlimited number of users. For each user who needs access to the remote equipment, administrators can create unique identifiers. This makes it easier to grant and revoke access privileges when needed. In addition, Talk2M account administrators can limit which machines are accessible by each user, which services are accessible and even which ports and protocols are allowed. For example, an administrator can allow remote users to access the web services of a particular device for monitoring purposes, but limit the ports used to make changes to specific engineers only. Controls include:

- Role-Based Access Control (RBAC), which defines which users can access which machines and allows different levels of access
- Unique identifier per user and personalised password requirements (minimum length, letters, numbers, special characters, expiration time and one-time password history)
- Multi-Factor Authentication (MFA), which requires users to enter a code sent by SMS after entering their username and password
- Audit logs and connection logs for each device to see who connected, when and for how long

- **Talk2M infrastructure:**Ewon regularly evaluates the Talk2M architecture within the framework of risk management. Appropriate controls are implemented for maximum security effectiveness and compliance with applicable regulatory requirements.

Ewon has contracted several first-class hosting companies that meet the following requirements:

- Qualitative hosting providers: To increase reliability, improve redundancy and reduce latency, Ewon works with 21 leading hosting providers around the world.
- Monitoring 24/7/365: Our server network is monitored 24 hours a day to ensure maximum availability and security.
- Certified data centres: Relevant certifications include Service Organization Control (SOC) 1/2 Statements on Standards for Attestation Engagements (SSAE) 16/International Standard for Assurance Engagements (ISAE) 3402, SOC 2, and International Organization for Standardization (ISO) 27001/27002/27017/27018.
- Corporate member of the Cloud Security Alliance (CSA): Ewon works with hosting partners who are corporate members of the CSA.

- **Policies and procedures**:The Talk2M remote access solution is designed to be compatible with the existing security policies of customers. By using outbound connections on ports that are commonly open (e.g. 443 and 1194) and by being compatible with most proxy servers, the Ewon router is designed to be minimally intrusive on the network and work within existing firewall rules. Talk2M account administrators can customise password policies to bring them in line with corporate policies. They can also restrict user access. Talk2M account administrators can also view the Talk2M connection report (audit) to see which users are connecting to which devices and when, and thus check that the company's remote access policies are being followed.

To ensure the best possible business continuity, two service offerings are available to customers:

- Talk2M Free+ provides a free, efficient service with no Service Level Agreement (SLA)
- Talk2M Pro is a more elaborate, paid service with an SLA

The Talk2M Pro service guarantees 99.6% service availability. In order to provide these two levels of service, the Talk2M architecture is reinforced by several policy and control objectives, including:

- Service Level Agreement of hosting providers: Talk2M Pro services are hosted via first-class hosting partners, guaranteeing us 99.99% availability. For Talk2M Free+ services, several hosting providers are used, usually offering an availability of over 99%.
- Key performance indicators: The performance of each server is continuously monitored.
- Redundancy of servers: The multiplicity of providers allows VPN connections to be quickly re-routed in case of problems.
- Continuous monitoring: TalK2M services are continuously monitored by on-call engineers.

Finally, to reduce network latency, the data centres are located on five continents (North America, Europe, Asia, Africa and Australia) and continue to expand into more and more regions. Indeed, low latency is required by certain PLC protocols based on very small packet sizes, which are much more sensitive to network interruptions. Ewon products connect to the geographically closest server so as to optimise connection performance.

Future solution: The Ewon Cosy+ and its further enhanced security

In the future, Ewon's Cosy+ industrial router will incorporate a multi-tiered security approach (see Figure 3-2) and will position itself as an absolute industry benchmark with an ever-increasing emphasis on security.
With the Cosy+, Ewon takes the remote access market to an unprecedented level of security. This new approach incorporates a high level of physical security as part of the chain of trust so as to meet the most stringent IoT standards. Here are just a few of the advanced security features that the Ewon Cosy+ incorporates:

- Guaranteed chain of trust, from the hardware to the cloud: The Ewon Cosy+ has a built-in Secure Element (SE) chip to protect secret information and provide a hardware Root of Trust. It also includes a root certificate to prevent cloning or counterfeiting.
- A Secure Boot (a form of controlled booting) sequence has been implemented to ensure that only code signed by Ewon is executed. Strong encryption of all communications with the T2M Cloud is also ensured.
- All operations concerning secrets related to the Ewon Cosy+ are handled via Key Ceremonies. A Key Ceremony (KC) is a session that governs how cryptographic objects are generated and stored.
- Increased security thanks to a digital output indicating an active remote connection.

Examples of remote access use

In this chapter, discover four concrete examples:

1. Manufacturer of thermoforming machines (MAAC)
2. Industrial bakery (Bakkersland)
3. Materials handling (A.G. Stacker)
4. Cyclotrons in the health sector (IBA)

1. Manufacturer of thermoforming machines

Based in Chicago, MAAC specialises in the manufacture of thermoforming machines and other complementary products. MAAC products are used worldwide and serve many industrial sectors, such as the aerospace, medical and automotive industries.

MAAC quickly realised that automation control technology would be the key to success in the machinery sector. Leslie Adams, Director of Technical Services, has long been an advocate of electronic automation. According to Adams, “the communications provided by an Ewon VPN router are simply amazing. With an Internet connection, we can connect to machines just about anywhere.”

The secure VPN connection provided by Ewon technology offers full integration of IT security standards. Ewon's unique remote access solution allows MAAC to connect to machines in the field with the same ease and flexibility as a machine on the company's shop floor.

Remote access allows the company to connect to a machine as if it were on hand, and have access to PLCs, drives and HMI devices, as well as any other device connected to the machine's subnet, including an IP camera. Prior to installing the Ewon routers, MAAC used telephone modems to connect to its machines, but the time delay was a huge problem. “I remember the frustration associated with monitoring the machines, when information took a long time to arrive via the modem connection. We were working with a machine in Australia and the delay was up to 15 seconds,” Adams recalls.

Remote maintenance, which enables rapid and efficient troubleshooting, has a positive impact on customer support costs. Leslie comments: “With Ewon, we eliminate 50-70% of our support costs, while significantly reducing the machine downtime normally associated with waiting for a service

technician. The time wasted travelling in the field represents a lot of money. Sitting in airports and driving to customer facilities is a lot of wasted time- time we'd rather our programmers spend working on new machines or refining existing systems. When these people are absent from the company, they are simply not working on the important things."

2. Industrial bakery (Bakkersland)

Bakkersland is the largest industrial bakery in the Netherlands. Bakkersland's main concern is the possible stoppage of machines in a production process. Any immobilisation situation can cause delays in the logistics process.

To avoid this type of disruption, Bakkersland undertook a project in which each of its machines would be equipped with an Ewon industrial router. Ewon routers are installed in the control room next to the PLC on the DIN rail (a metal rail used to mount circuit breakers and industrial control equipment inside equipment racks). The structure works online and can provide remote supervision of the machine to the operator via a secure VPN connection.

Bakkersland chose Ewon's Cosy router as a remote maintenance system for its machines. Dennis van Scheijndel, a technical specialist at Bakkersland, explains the advantages of the Ewon architecture: "In case of an alarm, the operator will be able to indicate that a particular sensor is dirty or that the connection is not fully secure. If necessary, the supplier will be able to make changes to the control. As a user, we are not the only ones who save time; the manufacturer of the machine no longer needs to send an engineer to the site. It is mainly suppliers located abroad who benefit from this."

3. Materials handling (A.G. Stacker)

A.G. Stacker is a manufacturer of stacking machines and auxiliary equipment. When Clarence and Helen Allen started the company in 1996, they aimed to provide innovative equipment with better customer support than anyone in the industry. Today, with innovation and customer service in mind, A.G. Stacker is working with Ewon to develop the next generation of customer interaction.

A.G. Stacker machines have been adopted by customers worldwide. Each of these machines uses a sophisticated automation system that includes drives, programmable controls and other state-of-the-art devices. Although A.G. Stacker has a team of highly qualified engineers, technicians and trainers to help customers maximise the value of the machine, customer conditions sometimes justify fine-tuning and system modifications in the field.

The automation equipment on the machines in use sometimes requires someone to travel to the customer's site to make changes, however small. With the cost of last-minute flights skyrocketing, A.G. Stacker sought a new and innovative way to solve this problem. That's when Ewon was called in to help.

Ewon provides a quick and easy, yet secure, approach to remote connectivity. Kennedy Larramore, an electrical/IT technician at A.G. Stacker, explains: "Even though we have three technicians assigned to support our customers, "mobile technicians" are expensive, both for our customers and for A.G. Stacker. Basically, the time spent travelling could be better spent by our staff and the downtimes at our customers' sites are very costly. In addition, we often encounter problems where the customer finds it difficult to describe the exact nature of the problem."

"We started by providing Ewon devices as an option on our machines. But after seeing the power of Ewon's free Talk2M solution and the devices in the field, we've integrated Ewon into all the machines we build," adds Mr Larramore.

4. Cyclotrons in the health sector (IBA)

IBA develops high-precision solutions for cancer diagnosis and treatment- for example, cyclotrons. IBA chose Ewon and Talk2M technology to provide remote after-sales service on a global scale.

"Above all, our aim is to be able to solve problems remotely for customers in the event of a breakdown or if they have any questions," explains Patrick Delcour, IBA's customer service project manager. "With Talk2M, I can log in and go from the Melbourne, Australia site to the Ghent, Belgium site in three seconds."

Faults are resolved for the customer from the control room based on the information provided by the status of indicator lights and displays. "However, the feedback information from the control room is very fragmented," said Mr Delcour. Before Ewon was used, the customer's operator had to call an IBA hotline when a problem occurred.

The Talk2M solution has revolutionised the way IBA works. Talk2M offers ease of use and connection while improving response efficiency. "Three clicks and I'm connected," declared Mr Delcour. The complexity associated with firewalls or proxies is completely hidden from the user.

Once the connection to Talk2M is established, all IP addresses on the local area network side of the Ewon become transparent and accessible to the user. With a few clicks, the user can connect to the PLC and the IP camera, or launch the remote desktop application on the control PC to control the local PC and launch the HMI.

See more examples of how Ewon is used at **www.ewon.biz/customers.**

Chapter 5

Getting the Ewon Cosy up and running in 5 easy steps

In this chapter, find out how to:

- create and set up your Talk2M account
- configure your Ewon Cosy
- connect to a remote machine

Advice

If you do not yet own an Ewon Cosy but would like to obtain one, please visit **www.ewon.biz/contact** to find a distributor in your area/country.

Follow these steps:

1. **Download, install and start eCatcher.**
   eCatcher is a free tool used to initiate remote access on the Talk2M virtual private network (VPN) and connect to all devices connected to your Ewon. You can download eCatcher from the Ewon website at https://ewon.biz/technical-support/pages/all-downloads. After starting the installation wizard, follow the instructions to complete the setup and launch eCatcher.

2. **On the login page, create your account by clicking on "Create a free account".**
   Create a unique account name, enter your name and email address and create a password. You must also activate your account by clicking on the link sent to your email address.

Advice

Click on "Check availability" to verify that you have selected a unique account name.

3. **Log in to eCatcher and add your Ewon by clicking on the "Add" button.**
   This step is illustrated in Figure 6-1. Continue by following the setup wizard. Select your version of Ewon Cosy (Ethernet, Wi-Fi or Cellular). The configuration is done either via a pre-configured USB stick / SD card inserted in the Ewon or via the Ewon's web interface.

Advice

The Ewon's web interface can be accessed via a web browser connected to the same LAN as the Ewon (or plugged directly into the Ethernet port). The easiest way to access this web interface is to launch the "eBuddy" program, which automatically detects the Ewons connected to the same local area network. Once the Ewon has been found, simply right-click on the Ewon and select "Open in browser".

In this step you have the possibility of changing the IP address of the LAN (default 10.0.0.53) and defining the WAN via DHCP or a static IP address. When prompted, insert a USB stick / SD card into your PC to save the configuration. When you have finished, close the eCatcher application.

Figure 6.1: Adding an Ewon in eCatcher

4. **Turn on your Ewon Cosy, connect your WAN cable and insert your USB stick / SD card.**
   Plug your WAN Ethernet cable into the WAN port, as shown in Figure 6-2, which will have a glowing amber light next to the appropriate port. Each port on the Ewon has a number displayed next to it. By default, 1 is a LAN port and 4 is a WAN port.

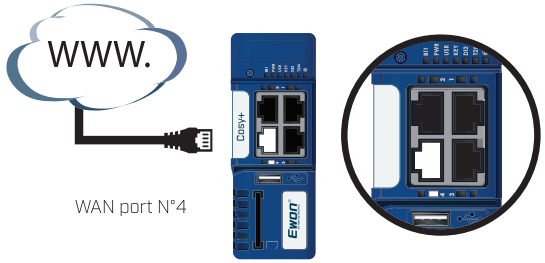


FIGURE 6-2: Identification of the WAN port on your Ewon.

When the PWR indicator light is green and the USR light is flashing green, as illustrated in Figure 6-3, insert your configured USB stick / SD card into your Ewon Cosy. The USR light will start to rapidly flash amber, indicating that a valid configuration file has been detected.

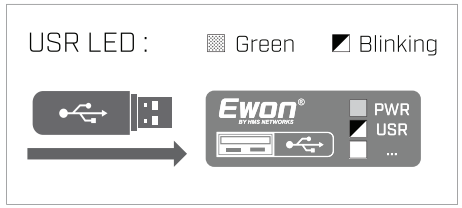


Figure 6-3: The LED pattern when you plug in the USB and the file was successful.

Once the USR indicator light turns solid green, the file has been successfully loaded. You can remove the USB stick or SD card and your Ewon Cosy will now restart. If the USR light turns red, you have an error in your configuration. These models are illustrated in Figure 6-4.

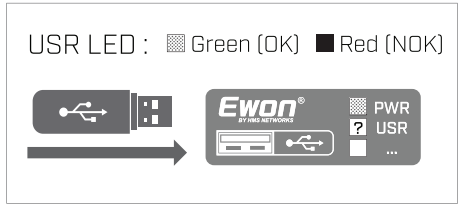


Figure 6-4: Wait until the User indicator turns solid green (successfully loaded) or red (error)

Reminder

Setting up the Talk2M connection may take several minutes. At the end of the setup process the Talk2M indicator should light up. See Figure 6-5.

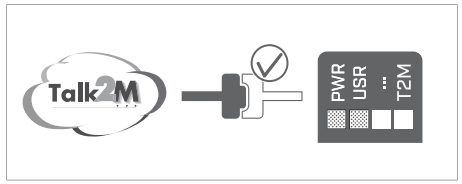


FIGURE 6-5: The Talk2M light is on, indicating that the setup process has been completed.

5. **Once your computer has been connected to the Internet, launch eCatcher.**
   The status of your Ewon Cosy must be “Online”. Simply highlight your Ewon device and click on the “Connect” button.

Once you are connected to your Ewon through eCatcher, if you have plugged an Ethernet device into the LAN port of your Ewon Cosy and in the same subnet, you should be able to ping its IP address to check connectivity.

Recommendations for the user who chooses an industrial remote access solution:

1. Pay particular attention to the security aspect (see Chapter 3).
2. Make sure you can easily manage your connections and who has access when and to which machine(s). It is also important to be able to trace previous accesses via an integrated audit system.
3. All connections must be confidential and encrypted.
4. Define your network access architecture within your factories: Machine suppliers should not have access to your entire LAN. Only accept outbound connections. You then don't need to open more ports and you shouldn't need a fixed IP address.
5. Be sure that the cloud architecture of your supplier guarantees you access via an appropriate SLA. Indeed, nothing is worse than getting stuck because your cloud system relies on a single data centre that becomes unavailable. Remember what happened in France in 2021.
6. Choose a solution developed on the basis of proven solutions that continue to evolve, preferably open-source.
7. Ensure that your supplier continues to update the firmware and programs.
   There is nothing worse than a supplier who enters the battle for purely opportunistic reasons and withdraws after a few years.
8. Stability of the group: Make sure your supplier is sound and profitable.

Glossary

2G: First released to the public in 1991 and based on GSM, the second generation of wireless telecommunications technology enabled digital data services for mobiles, including SMS text messaging. See also Global System for Mobile Communications (GSM) and Short Message Service (SMS).

3G: First released to the public in 1998, the third generation of wireless telecommunications technology offers data transfer rates of 2 megabits per second (Mbps) or more for wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calling and mobile TV technologies.

4G: First released to the public in 2008, the fourth generation of wireless telecommunications technology offers peak data transfer rates of 100 Mbps for high mobility communications (such as those from a moving vehicle) and 1 gigabit per second (Gbps) for low mobility communications (such as those of a pedestrian).

Advanced Encryption Standard (AES): A symmetric block cipher algorithm used to encrypt sensitive network traffic and data. AES is the replacement encryption algorithm for DES and 3DES. See also Data Encryption Standard (DES).

Application Programming Interface (API): A set of rules and specifications that software programs can follow to communicate with one another; serves as an interface between different software programs and facilitates their interaction.

Certification authority (CA): An entity that issues digital certificates and certifies ownership of a public key by the subject named on the certificate.

Data Encryption Standard (DES): Symmetric key encryption algorithm developed in the early 1970s, but now considered insecure due to its small key size (56 bits).

DB9: A common electrical connector used for RS232 serial computer connections and named for its characteristic D-shaped metal shielding and its two parallel rows of nine pins in total. See also RS232.

DF1: An asynchronous byte-oriented protocol used to communicate with most Allen Bradley RS232 interface modules. See also RS232.

Envelope Encryption (EVP): A high-level interface to OpenSSL cryptographic functions. See also OpenSSL.

Encapsulation of security payload (ESP): Part of the IPsec protocol suite responsible for guaranteeing the authenticity, integrity and confidentiality of original packets.

Ethernet: A network protocol that controls how data is transmitted over a local area network. Technically, this is the IEEE 802.3 protocol. This protocol has evolved and improved over time and can now transmit data at a speed of 1 GB per second.

Ethernet cable (crossover): A type of twisted pair copper cable with RJ45 connectors, used to directly connect two computer devices together.

Ethernet cable (straight through): A type of twisted pair copper cable with RJ45 connectors, used to connect computer devices together on a local area network, usually via a hub or switch. See also local area network (LAN).

File Transfer Protocol (FTP): A standard network protocol used to transfer computer files between a client and a server on a network.

Firewall : A network security system designed to prevent unauthorised access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorised users from accessing private networks connected to the Internet.

Global System for Mobile Communications (GSM): Wireless telecommunications standard developed by the European Telecommunications Standards Institute (ETSI) for 2G protocols. See also 2G.

Hash-Based Message Authentication Code (HMAC): A message authentication code that uses a cryptographic hash function and a secret cryptographic key.

Hyper Text Transfer Protocol Secure (HTTPS): Protocol for secure communication via a web browser on the Internet that uses the Secure Sockets Layer (SSL) protocol for encryption. See also Secure Sockets Layer (SSL).

Human-Machine Interface (HMI): The user interface in a manufacturing or process control system.

Industrial Programmable Logic Controller (PLC): An industrial programmable logic controller is a special type of computer used to control industrial processes by so-called “sequential processing”. It is used to automate industrial processes. One action triggers another, which triggers another, depending on various parameters, conditions, etc. These automatons are used extensively in assembly lines and for machine control.

Internet Service Provider (ISP): An organisation that provides its customers with access to the Internet.

IP camera: A video camera that is networked via a Fast Ethernet connection. The IP camera sends its signals to the main server or the computer monitor via an Internet or network connection. It is mainly used for IP surveillance, closed circuit television (CCTV) and digital videography. IP cameras are largely replacing analogue cameras because of their digital zoom and remote monitoring capabilities via the Internet.

Internet Protocol (IP) : The main communication protocol of the TCP/IP communications suite for routing across network boundaries (routers) and the Internet. See also Transmission.

Local Area Network (LAN): A computer network that connects computers and devices (including machines) in a building, factory, laboratory, school or other relatively small area.

Machine-to-machine (M2M): Wired or wireless communication that occurs directly between two machines

Modbus: A serial communication protocol originally published by Modicon (now Schneider Electric) for use in its PLCs. See also programmable logic controller (PLC).

Multi-factor authentication (MFA): A type of access control that grants access only after providing at least two forms of authentication.

Network latency: Any type of delay that occurs in the communication of data over a network. Network connections in which small delays occur are called low latency networks. Network connections that suffer long delays are called high latency networks.

Object Linking and Embedding (OLE): A Microsoft proprietary technology that allows documents to be embedded in and linked to other objects.

OEE (Overall Equipment Effectiveness) is a measure used to estimate the effectiveness of your manufacturing operations and reduce the downtime of a production machine, thus improving productivity.

OpenSSL: An open source implementation of the SSL and TLS protocols. See also Secure Sockets Layer (SSL) et Transport Layer Security (TLS).

Original Equipment Manufacturer (OEM):A company that produces parts and equipment that can be marketed by another manufacturer.

Out-of-band management:A dedicated communication channel used for the management of networked devices, such as remote monitoring and configuration. An out-of-band communication channel is independent of an in-band communication channel and therefore does not depend on the device's operational communication channel (e.g. a network connection).

Packet switching: A method used in communication networks in which data is transmitted in packets- consisting of a header and a payload- to its destination. Using the information in the header, the networking hardware routes the individual packets to the destination via the best available path, and then reassembles the data in the correct order at the destination.

Ping:A software utility used to test the accessibility of a host (such as a device or machine on an IP network).

Process Field Bus (PROFIBUS): A standard for fieldbus communication in automation technology.

Programmable Logic Controller (PLC): A robust industrial computer that has been adapted for the control of manufacturing processes.

Public Key Infrastructure (PKI): A set of roles, policies and procedures used to create, manage, distribute, use, store and revoke digital certificates and manage public key (also known as asymmetric) encryption.

Public Switched Telephone Network (PSTN): All global circuit-switched telephone networks operated by national, regional and local telephone operators.

RJ45 : Standard telecommunications network interface ("registered jack") used to connect voice and data equipment.

Role-Based Access Control (RBAC):A method of controlling access to the resources of a computer or network based on defined roles assigned to individual users within an organisation.

RS232: A telecommunications standard for serial data transmission.

RS485: standard serial interface defined by the Telecommunications Industry Association and the Electronic Industries Alliance (EIA/TIA). Also known as TIA485 and EIA485.

Secure Hash Algorithm (SHA): Family of cryptographic hash functions published by the US National Institute of Standards and Technology (NIST).

Secure Sockets Layer (SSL): A cryptographic protocol for securing communications on a computer network.

Transmission Control Protocol (TCP): One of the main protocols of the Internet protocol suite, TCP is one of the two original components of the suite, complementing the Internet protocol (IP), and that is why the entire suite is commonly referred to as "TCP/IP". TCP ensures the reliable and orderly delivery of a byte stream from a program on one computer to another program on another computer. TCP is the protocol on which major Internet applications such as the World Wide Web, email, remote administration and file transfer are based. See also Internet protocol (IP).

Virtual private network (VPN): Technology used to securely extend a private network (such as a local area network) across a public network (such as the Internet) using an encrypted connection and data encapsulation. See also local area network (LAN).

Wide area network (WAN):A telecommunications or computer network that extends over a large geographical distance.

Wireless modem: A modem that bypasses the telephone system and connects directly to a wireless network, through which it can directly access Internet connectivity provided by an Internet service provider (ISP).

Service Level Agreement (SLA): A formal commitment between a service provider and a customer that addresses specific aspects of the service provided such as quality, performance, availability and responsibilities.

Internet Protocol security (IPsec): A suite of network protocols that authenticates and encrypts data packets sent over a network.

Network segregation: Splitting of a network into two LANs, keeping unsecured computers in the first network and moving the computers you want to protect to a second shielded network.

Short Message Service (SMS):A text messaging service.

Siemens Multi-Point Interface (MPI):A proprietary serial interface based on the EIA485 (formerly RS485) standard that is used to connect PCs, consoles and other devices to Siemens SIMATIC S7 PLCs. See also RS485 and programmable logic controller (PLC).

Simple Network Management Protocol (SNMP): Standard Internet protocol used to collect and organise information about devices managed on a network.

Subscriber Identity Module (SIM): An integrated circuit (IC) that is used to store the International Mobile Subscriber Identity (IMSI) number and its associated key, which are used to identify and authenticate subscribers on mobile devices.

Supervisory Control and Data Acquisition (SCADA) system: A control system architecture that uses computers, networked data communications and graphical user interfaces (GUIs) for high-level process supervision management.

Intrusion Detection System (IDS): A hardware device or software application that monitors a network or system for malicious activity.

Network address translation (NAT): Method of mapping an IP address to another IP address, e.g. a private IP address to a public IP address.

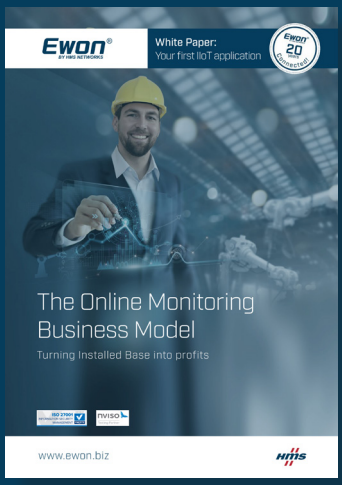
Transport Layer Security (TLS): A cryptographic protocol for securing communications on a computer network.

Universal Serial Bus (USB): An industry standard that defines cables, connectors and communication protocols for connection, communication and power between computers and peripheral devices.

Virtual Network Computing (VNC): A graphical desktop sharing system used to remotely connect to and control another PC by sending keyboard strokes and mouse movements to a remote PC.

X.509:A cryptographic standard that defines the format of public key certificates.

To find out more...



This white paper explores the advantages of remote access and monitoring for machine builders and equipment manufacturers (OEM). These capabilities enable machine builders to support their equipment with optimal organisation, while preserving the data at the local level.

This type of service is seen as a competitive differentiator, a source of customer satisfaction and often also as a profit generator.

https://www.ewon.biz/products/ewon-flexy/kpis-as-iot-application/flexy-kpis-whitepaper

This white paper presents five case studies on centralised data collection, which machine builders can implement today using an Ewon Flexy and Talk2M.

Data-driven projects can help machine builders grow their businesses by giving them better insight into the health of their machines and enabling them to understand their customers' usage patterns.

https://www.ewon.biz/products/Talk2M/talk2m-data-services/whitepaper-data-services

EN - Rev. Sept 2021