Best practices for a secure usage of the Ewon solution

This document contains recommendations to help you take advantage of the Ewon solution in a very secure and efficient way.

The Ewon Remote Connectivity Solution has been designed with two strategic commitments in mind: security and ease of use. This document introduces a list of best practices to follow when configuring and using the Ewon remote access solution, in order to achieve optimal security and efficiency, as well as to complement the measures that HMS has already implemented in the solution.

We strongly suggest to use this document as a basis to define or improve your internal processes related to the management of the solution. This will contribute to increase the quality of your security posture, as well as the acceptance by customers and partners.[1]

On the final page of this document, you will find a table summarizing our recommended best practices. Feel free to use this list to describe your implementation and to demonstrate to your own customers that you have solid security processes in place. This will make it easier for you to get the remote solution accepted.

1. Governance

Consistency of the solution

In addition to contributing to increase your competitiveness, defining remote connectivity as a key element for your company allows to involve people, create a structured and consistent solution, and also establish a solid security posture.

- Involve your company management to define a remote maintenance strategy, as well as adequate expectations and tools.
- Use a dedicated hardware for industrial remote connectivity. This adds a physical layer of security protecting your equipment and reduces the risk of impacting the operation of your industrial control systems.

[1]This document assumes the usage of a "Talk2M Pro" account. Some features may not be available in the "Talk2M Free+" version.

- Harmonize your remote access activities to one solution. This reduces the complexity of administration, security risks and number of attack vectors.

2. Account creation and structure

A Talk2M account is used for the management of the devices, users, and all security aspects of the Ewon remote connectivity solution.

Structure of the account

Your company activities, requirements and organization should be reflected in the structure of your account.

- Define a clear structure for your maintenance activities within your organization and for the collaboration with your external partners. Use the Talk2M device pools and user groups to simplify the management of users' permissions and access rights over various groups of Ewon devices.

Account consolidation

Managing multiple accounts reduces efficiency by requiring redundant efforts.

- Consolidate all your Ewon devices into as few Talk2M accounts as possible (ideally only one account), to reduce your maintenance efforts and increase your security posture. Minimizing the number of elements (such as users, groups and pools) to create and manage also allows to decrease the probability of mistakes and oversights.

Account management resilience

The owner of the Talk2M account (main administrator) should take responsibility for ensuring that best practices are implemented on the account.

- Create at least two users with administrator privilege to limit the risk of having a single point of failure, in case of departure of a unique administrator.
- Use the "custom fields" that can be defined for registered devices and users of your Talk2M account, by filling them with useful information. This makes it possible to sort and filter based on a larger number of criteria and therefore increases efficiency by making the retrieval of a device or user easier while also reducing the possibility of mistake.

  - *Examples of custom fields for devices: equipment model, customer name, country, city, site.*
  - *Examples of custom fields for users: team, function, qualifications, region.*

3. User creation and management

User identification

Shared user accounts should be avoided under all circumstances, as they prevent accountability and lead to major security issues when an employee leaves the company.

- Create a unique user for each person interacting with the Ewon solution.

Authentication

Talk2M allows you to configure password policies that will force all users to define strong passwords.

- Define minimum password security requirements.
- Configure a password validity period, after which passwords will expire and will need to be changed
- Enable two-factor authentication for all users' accounts.
  Usernames and passwords are not anymore recognized as a sufficient method of authentication. A better security level is provided by two-factor authentication, in which not only knowledge (example: a password), but also ownership (example: a phone number) must be proven. If a user account login information (username/password) has been compromised in a data breach, having two-factor authentication enabled will allow to keep the account safe.

Segregation of duties

Users should only have access to information or permissions necessary to undertake their duties, on a need-to-know basis.

- Most users should be defined as standard users with limited permissions.
- Use the «user group» feature of the Talk2M account to define user profiles to which specific permissions, access rights and/or management roles are attributed. For example, it is possible to restrict the access rights of a group of users to only specific Ewon gateways, or even to specific devices connected behind these Ewon gateways.
- Administrators have the responsibility of managing the rights and permissions of other users and as such, this duty should be limited to highly trusted personnel within the organization.
- Limited administrative roles can be attributed to some users, with the authority to manage specific groups of users or pools of devices.

User temporary activation

To further strengthen security, administrators of the Talk2M account can keep users disabled by default.

- Enable users of your Talk2M account only when they need to perform a task, such as a remote maintenance operation on a machine, and disable them once their task is done.

4. Device deployment

Planning the device installation

Combined with Talk2M, Ewon gateways enable remote access to equipment installed on their LAN side. The installation and configuration of an Ewon gateway must be done according to the range of equipment expected to be accessed remotely.

- Install one Ewon gateway per machine or system (with same ownership) for an easy and granular management of access rights.
- Avoid creating an access to a whole factory network, as it is not optimal from a security point of view and would open access to a very large area that would require the management of complex user access rights.
- To simplify the management of user access rights, create a coherent structure of pools of Ewon gateways (example: pools of devices by region, customer or type of equipment) and always assign an Ewon gateway to the appropriate pool(s).

Consistent configuration of devices

The registration and configuration of devices is a first and important step to a secure setup. In case of large deployments, manually configuring each device individually can be inconvenient and might lead to mistakes.

- Do not use default credentials and define a strong password for the access to the configuration web-page of the Ewon gateways.
- Consider using the Global Registration Key of your Talk2M account to create a common configuration file that can be used to set up each new device with limited efforts and reduced risk of error. This common configuration file can be copied on a USB flash drive or SD card and used for the first initialization of your Ewon gateways. A Talk2M Administrator will then need to approve the registration of the new device on the account.

5. Remote connection to machines

Remote connectivity control

The control of the remote connectivity of the Ewon gateway and of the external access to production equipment is key to guarantee the security and safety of operations.

- Connect the digital input of an Ewon gateway to a key switch or similar device, which can then be used to locally enable or disable the VPN connection.
- Alternatively, the connectivity of an Ewon gateway or of a user can also be controlled at the cloud level, by disabling or enabling it through your Talk2M account.
- To improve on-site operators' awareness and safety, use the digital output of the Ewon gateway (new product generation) to connect an indicator light or another signaling equipment. The indicator will light up when a remote connection is active.

Establishment of a remote connection

Some good practices before establishing a remote connection to a device:

- Verify if another user is not already connected by checking the “User connected” field in eCatcher.
- If necessary, reserve one or several connections to prioritize a certain group of users.

Closing of a remote connection

Some good practices when the remote operation has been completed:

- Do not leave unattended a computer with an active remote connection, to prevent unauthorized people from performing any operation or seeing confidential information.
- Close the connection when the VPN tunnel is not needed anymore.
- Document the remote activity that has been performed, for example by using the logbook feature of eCatcher. This is useful to keep track of your work and to share information with other users.

6. Maintenance strategy

Software updates

In all information systems, vulnerabilities can be discovered and then patched accordingly by the software or hardware providers. Assets that are not patched provide potential security entries for hackers. Mitigating risks can be achieved by following a few simple recommendations:

- Keep the firmware of your Ewon gateways up to date.
- Keep the version of your Ewon software, such as the Talk2M client eCatcher, up to date.
- More generally, keep your equipment (computers, mobile devices) up to date.
- Use an antivirus application on your PC.

Monitoring of remote access usage

Regularly consulting the connection reports and logs gives you good insights on the remote activity occurring on your Talk2M account.

- Monitor the utilization patterns in your team.
- Identify equipment needing more attention.
- Compare traffic usage month-to-month to detect important variations.

Removal or adjustment of access rights

It is essential that you have efficient processes in place to systematically adjust users’ registrations and access rights.

- Immediately delete the user account of an employee leaving your company.

- Review regularly users, devices, and permissions (groups and pools assignations) and remove excessive or unused rights.

Verification of remote access availability

When an issue requiring support occurs, the highest reactivity is needed to immediately start the remote troubleshooting activity.

- Setup routines to regularly verify your capacity to connect to your equipment, in particular for Ewon gateways that do not have a permanent connection to Talk2M (example: VPN is disabled by default and enabled via a key switch).

7. Organizational measures

Documentation of remote access management

The Ewon Remote Connectivity Solution is an essential tool in your organization and shall be described and managed in a professional manner. Successful deployment and customer acceptance can be facilitated with comprehensive processes and materials for communication towards partners and customers.

- Document your Talk2M account, list of devices and user organization.
- Create processes and guidelines for internal / external users of the solution.

Control measures

- Regularly review that your documentation is up-to-date and that your guidelines are followed within your organization.

Training and awareness

Employees should be aware of the importance of information security and of the risks resulting from a poor implementation of security measures.

- Educate your employees regarding security, and train them to follow the best practices.

For more details about how to configure a Talk2M account, please refer to the Ewon Support website:
https://www.ewon.biz/technical-support/pages/talk2m/talk2m-service?ordercode=talk2m

Application of best practices

Enclosed is a list of the best practices implemented by our organization to guarantee the efficient and secure usage of the Ewon solution:

#	Topic		Implementation comments
1	Governance	• Consistency of the solution	
2	Account creation and structure	• Structure of the account • Account consolidation • Account management resilience	
3	User creation and management	• User identification • Authentication • Segregation of duties • User temporary activation	
4	Device deployment	• Planning the device installation • Consistent configuration of devices	
5	Remote connection to machines	• Remote connectivity control • Establishment of a remote connection • Closing of a remote connection	
6	Maintenance strategy	• Software updates • Monitoring of remote access usage • Removal or adjustment of access rights • Verification of remote access availability	
7	Organizational measures	• Documentation of remote access management • Control measures • Training and awareness	