Insight Security - Gasmet

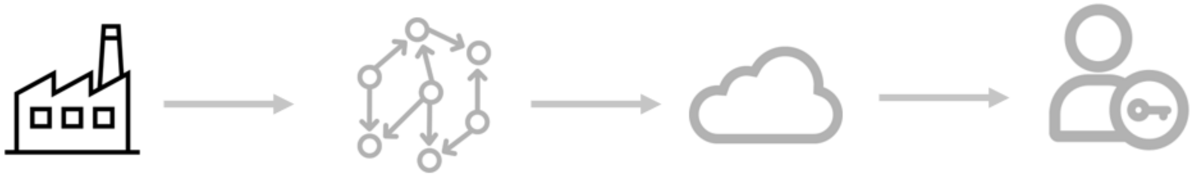
Introduction

There are two purposes of the Insight security document. The first is to guide the user how to enable the connection to the IoT platform. The second is to describe the existing security features of the solution.

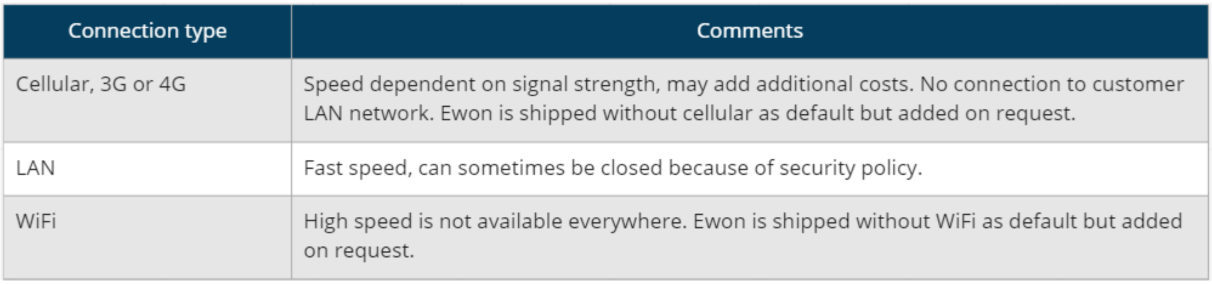
The following steps shall always be done

- Decide if the current network should be used to connect CEMS II to the IoT platform or if the Ewon router/firewall should be used.
- Decide if LAN, Wi-Fi or Cellular should be used
- Make sure the ports 53, 443 and 8883 are open for outbound traffic
- Make sure data.iot.eu-west-1.amazonaws.com is reachable

Customer site security



Connection to Insight Cloud: There are several possibilities to connect to Insight cloud. Already existing infrastructure could be used or adding a secure router/firewall to separate the networks. This will support Cellular, LAN or Wi-Fi.



Connection type	Comments
Cellular, 3G or 4G	Speed dependent on signal strength, may add additional costs. No connection to customer LAN network. Ewon is shipped without cellular as default but added on request.
LAN	Fast speed, can sometimes be closed because of security policy.
WiFi	High speed is not available everywhere. Ewon is shipped without WiFi as default but added on request.

Data sent to cloud: Insight cloud is only receiving tags, telemetry, and alarms data from sensors.

Firewall Requirements: No incoming connections are necessary.

- Outbound ports 53, 443 and 8883 are used.

Ewon router: Ewon router from HMS can be used to connect to Insight cloud. Ewon can use Cellular, LAN or Wi-Fi to connect. All modes are all disabled as default and it’s up to the customer which mode they prefer to enable. All modes are fully encrypted.

Ewon are by default configured to discard all traffic except VPN and initiated traffic.

If the customer also would like to disable the VPN option, it can be done in the Ewon router by setting all addresses to 0.0.0.0 in the VPN protection in the router.

It can also be done by a flexible option that can be toggled on and off. This is described in the section “Local VPN control”.

Ewon Cellular Connection: The following steps should be followed to setup Ewon for cellular connections.

- Install SIM card and antenna and power up Ewon. Connect Gasmet PC to Ewon LAN port 1, 2, or 3 with Ethernet cable.
- Change Gasmet PC network settings to following:
  - IP address into 10.0.0.x range
  - Subnet mask: 255.255.255.0
  - Default gateway: 10.0.0.53 (same as Ewon IP)
  - Preferred DNS server: 1.1.1.1 (What is 1.1.1.1? | Cloudflare)
- Access Ewon through browser (10.0.0.53) and do following
  - Do system setup + cellular setup using “insight.cxn” as APN. (select it as a custom APN from the dropdown list)
  - Change settings as per guide How to access the Internet via the Ewon (beside Talk2M VPN) (windows.net)
    - Uncheck the "Route all gateway traffic through VPN"
    - For the 'Apply Nat and TF to connection' field choose "NAT and TF on WAN"
    - Leave the "Enable transparent forwarding" option unchecked.
    - Allow traffic forwarding in security settings

Local VPN control: It’s possible to enable and disable the remote access manually. This is done by the use of a Key Switch or HMI physical button connected to the Ewon device’s digital input, the end user can decide whether the device is remotely accessible or not. It can manually be enabled to allow maintenance or error investigation. When remote access is no longer desirable, the user can use the switch to turn off the VPN possibility again. This functionality is not built-in by default. Ewon needs to be programmed to turn VPN on/off. The code for this is readily available.

Certifications: The device is manufactured by HMS AB, who strictly adhere to **ISO 27001** requirements, the world's most comprehensive security standard. With its ISO 27001 certification, HMS, a leading player in Industry 4.0 and IIoT, has implemented comprehensive security programs that protect information. This provides the level of security that industrial companies are entitled to expect.

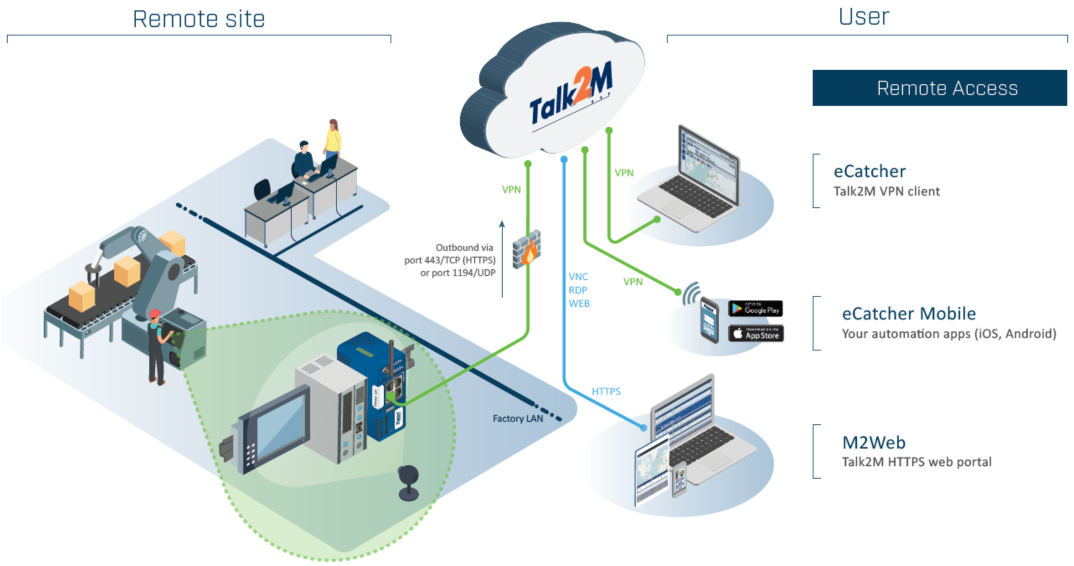
ISO 27001
INFORMATION SECURITY
MANAGEMENT
CERTIFIED BY
VINÇOTTE

The security approach on device level is based on the guidelines set by the standard **IEC 62443**, Cybersecurity for Industry. This will ensure the highest level of industrial security standards. This has been developed to address the need to design cybersecurity robustness and resilience into industrial automation control systems. It covers safety, availability, integrity, and confidentiality.

Segregation: Network segregation limits remote access only to the devices connected to the LAN of the Ewon gateway when accessing devices remotely. Access to the factory network is prevented. Additionally, when a cellular connection is used there is no need for physical access to the factory network at all.

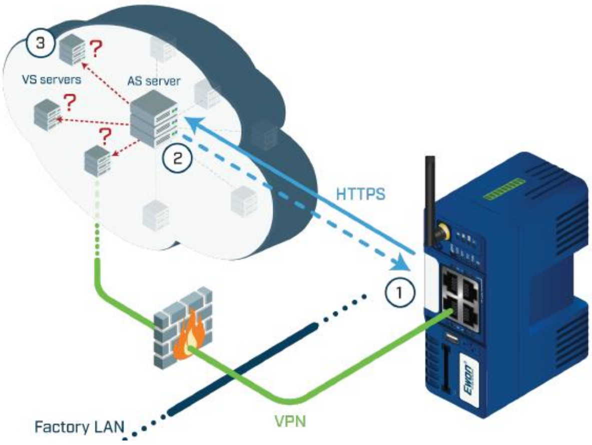
Connection Audit Trail: Ewon's solution provides traceability. A connection report is available for account administrators to check which users were connected to which devices, when and for how long.

Ewon VPN functionality: Ewon devices only communicate with Talk2M services. The clients also need to connect to the Talk2M service in order to communicate with the Ewon. This functionality can be fully disabled as described in the earlier section.



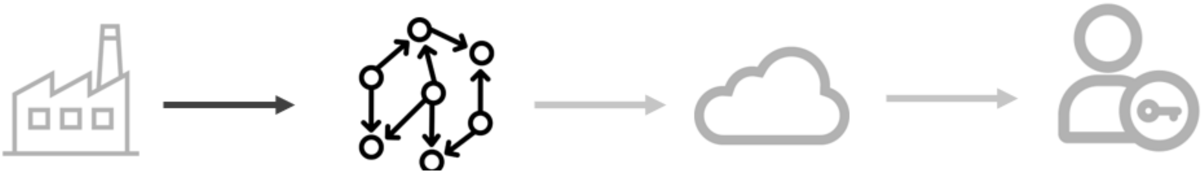
How Ewon communicates to Talk2M

1. A first and initial commissioning process where the Ewon device will connect to a central Access Server (AS) and authenticate through an HTTPS connection. It will then fetch its certificates. This operation is executed once, then the Ewon device will save its key and certificates internally.
2. Then, every time the Ewon device needs to connect to the VPN, it will first ask the AS for the Hostname of the VPN Server (VS) it needs to use (this VPN server address may change at any time from connection to connection). This request is also sent via an HTTPS connection.
3. Finally, the Ewon device will set up a VPN tunnel with the VS assigned in the previous step.



Additional information and access to a wide user community is available at HMS Networks website: https://www.hms-networks.com/

Data in transit



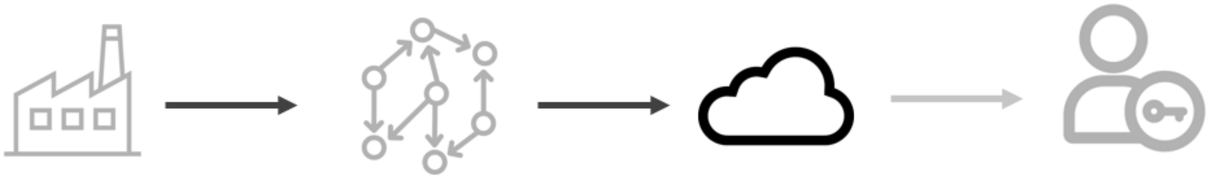
Encryption: All communication is fully encrypted. Additionally, when using cellular, the connection is completely unreachable as there are no physical wires and Insight employs a private APN.

Endpoint: Edge application uses data.iot.eu-west-1.amazonaws.com as an AWS endpoint. There is not any IP filtering done from Insight cloud.

Data availability: In case of network interruption, the Insight gateway buffers data and transmits it again once the connection is re-established.

For cellular connection type an automatic fall back to a hardwired LAN connection is available to ensure operation (primary operation via LAN with auto fall back to cellular is also available).

Data in the cloud



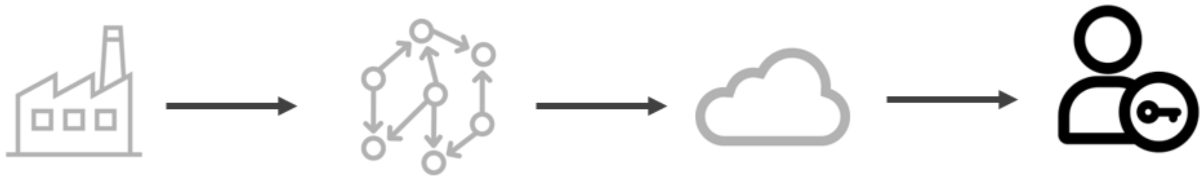
Technologies: Insight is built on the best and most advanced technologies available for reliable and secure web-based plant productivity software, IIoT, mobile and remote access. The combination of our dedication to reliability and security first and use of only the best technologies from AWS (Amazon Web Services), Microsoft and HMS provide the performance industrial applications demand.

Data availability: Data is stored in multiple database locations on separate servers for 99.99% availability once received.

Privacy: Data and its real-world description (meta-data) is stored on separate servers using different methods. It is impossible to infer the location or application of the equipment. All data is stored inside the EU.

Security: Continuous 3rd party security reviews and penetration testing assures best-in-class security. Aligned with CSA STAR Cloud Security Standards which overlaps ISO 270001.

User Access and Identity



Authentication: The Insight application uses Microsoft Azure Active Directory for user authentication. The user can use existing company credentials if using Office 365.

Security: 99.9% protection against cyber-attacks while logon is easy for Microsoft Office 365 users with a single corporate credential. Multi-factor authentication (MFA) is applied for all privileged accounts by default.

Nederman software is developed in accordance with the following security standards for Insight:

- ISO/IEC 62443
- ISO/IEC 27001
- CSA Star

Traceability: All user actions are logged, as well as connection and access attempts.

GDPR: The Insight application is GDPR compliant according to General Data Protection Regulation (EU) 2016/679.

Business continuity: The Nederman Insight Program has an established disaster recovery and business continuity plan for all levels of the IoT stack.

Auditing: Regular security tests are done by well-renowned 3rd party security companies.

Peter Blomberg

Peter Blomberg
Director, IoT Development & Operations
Nederman Insight AB