eWON Security Paper

SECURE INDUSTRIAL AUTOMATION REMOTE ACCESS CONNECTIVITY

Using eWON routers and Talk2M connectivity platform

www.ewon.biz

Connecting Devices™

Overview

eWON®, part of HMS Industrial Networks, is a global provider of secure industrial remote access connectivity. By leveraging a combination of its cloud based, redundant infrastructure called Talk2M and its industrial eWON hardware devices, eWON created a first-to-market integrated approach to secure remote access to industrial control systems.

Since its launch in 2006, eWON's Talk2M has successfully hosted millions of encrypted VPN sessions allowing engineers to easily and securely remotely monitor and troubleshoot their machines.

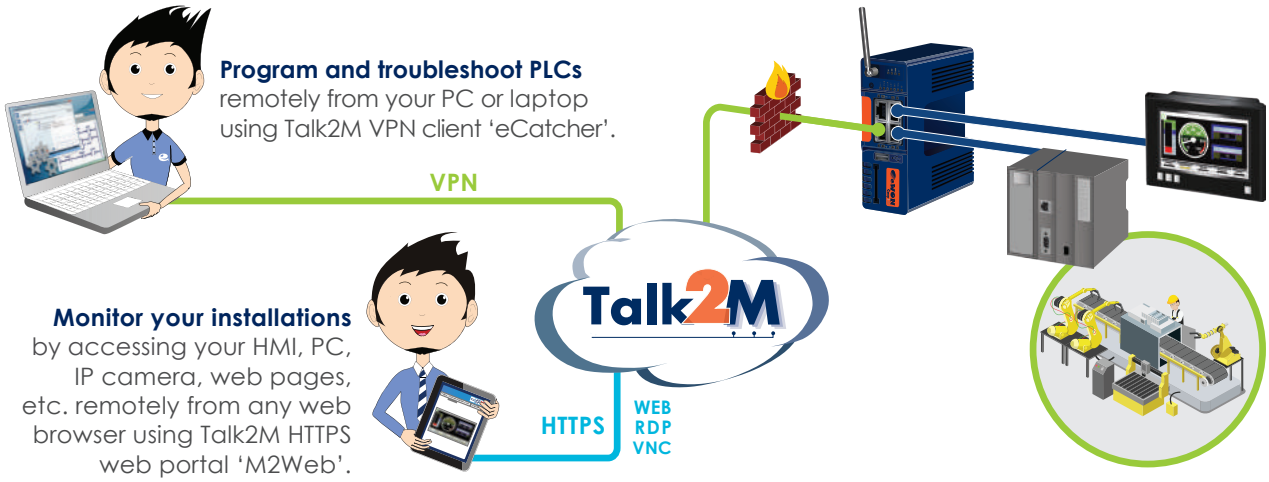
MAIN BENEFITS

The benefits of leveraging the eWON Solution include;

- Mitigating risks by improving uptime and equipment availability and efficiency with managed secure remote access, users and devices
- Reduce onsite travel
- Reducing mean-time-to-repair (MTTR)
- Lowering the total cost of ownership (TCO) of the IACS remote access approach
- Professionally managed globally redundant cloud infrastructure
- Compatible with industry standards (SSL and VPN)

HOW IT WORKS

The integrated Talk2M and eWON remote access solution was designed with simplicity and security in mind. To make the eWON and the devices behind it remotely accessible, eWON routers make an outbound connection via UDP or HTTPS to the Talk2M infrastructure. Using our VPN Client software, eCatcher, authorized users are able to log into their Talk2M account and connect to their eWON devices anywhere in the world.



SECURITY, CONVENIENCE AND ACCEPTANCE

One of the key challenges with remote connections to industrial control systems is balancing the needs of an engineer or PLC technician with the mandate by the IT department to ensure network security, integrity and reliability. Finding a solution that is readily accepted by both business groups has been a challenge for many years and a source of frustration and inefficiency for all stakeholders. Maintaining network security is essential for IT acceptance. At the same time, users will never use solutions that are complex, difficult or interrupt productivity. By balancing both the security and ease of use, eWON has created a best-in-class Remote Access solution that works for both end users and IT managers.

eWON layered security approach

Understanding the challenges associated with securely deploying and managing remote access within an IACS, eWON developed a solution compatible with industry accepted open standards that addresses the following key areas related to secure remote access in a defense-in-depth layered approach;

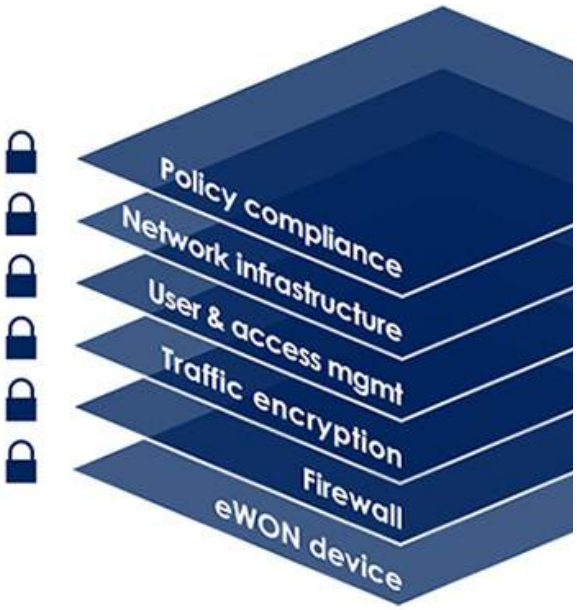
- Policy compliance
- Network Infrasctructure
- User and access management
- Traffic encryption
- Firewall
- eWON Device

While ease of use is important, security remains the priority.

eWON ensures high security using the "Layered security approach", also called "Defense in Depth Approach", based on guidelines set forth by ISO27001 and NIST Cyber security Framework 1.0 and other publications, guidelines and industry best practices (e.g. OSSTMM and OWASP).

This managed, hybrid, layered cyber security approach preserves information integrity and confidentiality along with information system availability and resiliency.

From the hardware devices to the policies & procedures, security is a core competency fully integrated at every level within the framework of eWON solutions.



EWON DEVICE

Network segregation, local device authentication, physical switch for enabling/disabling access.

Network segregation

The eWON industrial routers are typically installed in the machine control panel with the machine connected on one side(LAN) and the factory 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 first configured for VPN access, security settings on the device restrict traffic between its two network interfaces. This network segregation limits remote access to only the devices connected to the LAN of the eWON. Access to the rest of the network is prevented.

Device authentication

The eWONs themselves have user-level access rights separate from the Talk2M login. Only users with appropriate credentials and access rights can change the security settings on the eWON. Similarly, for the devices with data services, only authorized users can view or modify the data.

Physical key switch

All of our hardware devices feature a digital input. A switch can be connected to this input and the state of the switch can enable or disable the WAN port. This allows the end user to keep full local control of whether or not the device is remotely accessible.

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, plus any optional proxy settings). Since the eWON can act as a DHCP client, it can be configured to receive those settings automatically. However, the eWON also can be set up to use a static IP address that is assigned and controlled by the IT department if preferred.

FIREWALL

IP, port, and protocol filtering/firewalling available. Restricted access based on user, group, site for all or single devices.

Within the eCatcher application, Talk2M account administrators can set filtering and firewalling rules about which devices behind the eWON are remotely accessible and even over which ports and with which protocols they are accessible. Talk2M provides four different firewall setting rules based on declared devices IP, ports, gateways and eWON services (FTP server, HTTP server…) access.

From least restrictive to most secure firewall levels;

- Standard
- High
- Enforced
- Ultra

When combined with Talk2M's user rights management, administrators have the ability to tailor the remote access rights to selected groups of users.

TRAFFIC ENCRYPTION

Communications are transmitted through end-to-end encrypted tunnels using OpenVPN and SSL-TLS protocol.

Communications between the remote user and the eWON are fully encrypted using the SSL/TLS protocol, thereby ensuring data authenticity, integrity & confidentiality.

Indeed, all users and eWON units are authenticated using x509 SSL certificates and end-to-end traffic is encrypted using strong symmetric & asymmetric algorithms that are part of the SSL/TLS protocol cipher suite.

USER AND ACCESS MANAGEMENT

Unique user logins, configurable user rights to different devices, two-factor authentication, connection traceability.

A Talk2M account can have an unlimited number of users. For every user who needs to access equipment remotely, administrators can create unique logins. This makes it easy to grant and revoke access privileges when needed. In addition, Talk2M account administrators can restrict which remote eWONs particular users can access, which sevices behind those eWON are accessible and even the ports on those devices and the communication protocols used. For instance, an administrator might permit remote users to reach the web services in a particular device for monitoring purposes but limit the ports used for making programing changes to only specific engineers.

Every remote connection is documented on the Talk2M connection report. This report is a powerful IT auditing tool which allows account administrators to monitor the logging activities of each device.

Account administrators can see:

- **Who** has connected
- **When** the connection was established
- **How long** connection lasted

Audit trail is a useful tool when dealing with legal and security regulation compliance.

On top this, to re-inforce device access security in a world where 76% of all breaches involve weak or stolen passwords, eCatcher also offers secure authentication mechanisms, such as password enforcement and two-factor authentication (a password and a confirmation code sent to your mobile phone). Advanced configuration options (remember this PC, password expiration policy) are available for Talk2M Pro users.

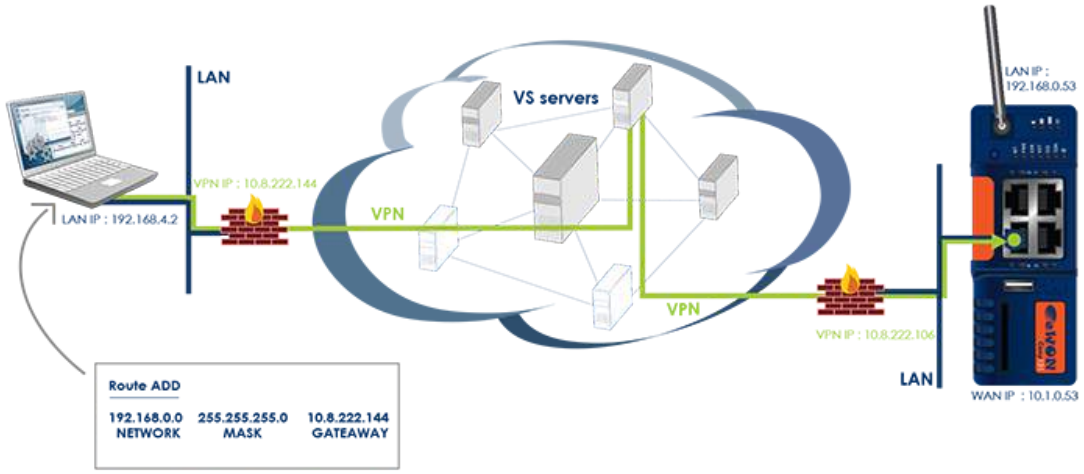
To sum up, user and access management includes:

- Advanced user and device access control with Talk2M by configuring groups of users and pools of eWON devices.
- Unique user login and customizable password policy by account administrator to guarantee compliance with corporate user identification and password policy.
- Connection audit trail
- Two-factor authentication via the user's mobile phone.
- User lockout implementation to prevent too many connection attempts from an unauthorized user trying to guess the password.

NETWORK INFRASTRUCTURE

Globally redundant Tier 1 hosting partners, 24/7 monitoring, SOC1/SSAE 16/ISAE 3402, SOC2 & ISO 27001 certified data centers, CSA members

The Talk2M infrastructure is a critical integrated element in our remote access solution. It is a fully redundant network of distributed access servers, VPN servers, and other services that act as the secure meeting place for eWONs and users.



Globally redundant Tier 1 hosting partners

To increase reliability, redundancy and reduce latency, eWON works with multiple industry leading hosting partners throughout the world to ensure best in class service.

- 3 different hosting providers geographically distributed in a way to maximize resilience.
- Separated access servers and VPN servers for an optimized roll out mechanism.
- Best server location selection to minimize latency.
- Hosting sites spread among different regions of the world: Europe, North America, Japan, China, Australia, India, South Africa…

24/7/365 monitoring

The network of servers is monitored 24/7 to ensure maximum availability and security using intrusion detection systems (IDS), in addition to an array of alerting mechanisms.

- Supervised 24/7/365 by on duty engineers.
- Based on KPI (key performance indicators) gathered from all servers.
- With proven and effective monitoring software (i.e. Munin).

SOC1/SSAE 16/ISAE 3402, SOC2 & ISO 27001 certified Data Centers

Talk2M is hosted in SOC1/SSAE 16/ISAE 3402, SOC2 & ISO 27001 certified data centers.

Cloud Security Alliance (CSA)

eWON is working with hosting partners, members of the CSA (Cloud Security Alliance) such as Rackspace and Softlayer.

POLICY COMPLIANCE

The eWON/Talk2M solution enhances and is compatible with existing corporate security policies, firewall rules, and proxy server.

The Talk2M remote access solution is designed to be compatible with customers' existing security policies. By using outbound connections over commonly open ports (443 and 1194) and by being compatible to most proxy servers, the eWON is designed to be minimally intrusive on the network and work within the existing firewall rules. Within eCatcher, Talk2M account administrators can customize the password policies to force compliance to corporate password policies and can restrict which users can access which devices remotely. Talk2M account administrators can also view the Talk2M Connection report (see user and access management) which can be a valuable tool to ensure that your corporate remote access policies are being followed.

To sum up, eWON solution is compliant with:

- Existing corporate security policies
- Firewall rules
- Proxy servers

AUDITS AND CERTIFICATIONS

Our Talk2M security environment is regularly tested in order to ensure our customers' high security level, and has been successfully audited by cyber security companies such as NVISO and admeritia.

In this context, Talk2M has got the ISECOM STAR certificate by going through an OSSTMM 3.0 and OWASP audit process (see certificate below). The assessment has been performed by the company admeritia.

For more info, visit www.isecom.com.

SUMMARY

A combination of unique hardware and globally redundant cloud infrastructure creates a robust, secure and convenient method to enable encrypted remote access to machines, panels and other industrial automation devices.

The key added-value of Talk2M is the full integration of IT security standards by allowing an Internet communication tunnel between the user and the remote machine while still following the existing firewall rules and security policies of each network. This means little or no IT changes required and gives organizations the ultimate solution to manage their Remote Access needs with maximum control, visibility and security.

Technical contact information:

Email: ewonsecurity@hms-networks.com

eWON BU - HMS Industrial Networks
Avenue Robert Schuman, 22
1400 Nivelles
Belgium (GMT+1)

Worldwide offices:

HMS - Sweden (HQ)
Tel : +46 35 17 29 00 (Halmstad HQ)
E-mail: sales@hms-networks.com

HMS - Belgium (eWON)
Tel: +32 67 895 800
E-mail: ewon@hms-networks.com

HMS - China
Tel : +86 010 8532 3183
E-mail: cn-sales@hms-networks.com

HMS - France
Tel: +33 (0)3 67 88 02 50 (Mulhouse office)
E-mail: fr-sales@hms-networks.com

HMS - Germany
Tel: +49 721 989777-000
E-mail: ge-sales@hms-networks.com

HMS - India
Tel: +91 83800 66578
E-mail: in-sales@hms-networks.com

HMS - Italy
Tel : +39 039 59662 27
E-mail: it-sales@hms-networks.com

HMS - Japan
Tel: +81 45 478 5340
E-mail: jp-sales@hms-networks.com

HMS - Switzerland
Tel: +41 61 511342-0
E-mail: sales@hms-networks.ch

HMS - UK
Tel: +44 1926 405599
E-mail: uk-sales@hms-networks.com

HMS - United States
Tel: +1 312 829 0601
E-mail: us-sales@hms-networks.com

www.ewon.biz