Ewon – Security at Every Level

IT Approved

By balancing both security and ease of use, Ewon creates best-in-class remote solutions that work for both users and IT managers.

Key advantages for Factory IT Acceptance

- **Firewall Friendly**: because no incoming connections are made to the device, there is no need to change firewall settings, routing policies, open ports or add exceptions. Little to no IT involvement is required. Ewon devices initiate a VPN tunnel to our Industrial Cloud VPN Servers by making an outbound connection across the factory LAN using ports that are commonly enabled (HTTPS port 443 or UDP port 1194).
- **Key Switch**: thanks to the use of a Key Switch or HMI Button to the Ewon device's digital input, the end user keeps full local control of whether the device is remotely accessible or not.
- **Connection Audit Trail**: our solutions provide traceability. A connection report is available for account administrators to see which users were connected to which devices, where and when. This report can be a valuable tool to ensure that your corporate remote solution policies are being followed.
- **Multi-Factor Authentication**: along with the User/Password, you can add a second layer of security with a key sent by SMS that changes at each login.

What does my IT department need to do to use the Ewon router?

Typically, nothing! Talk2M tunnels are initiated by the router and use only outgoing connections. No incoming connections are made, so no ports need to be enabled in your corporate firewall for incoming connections. In addition, Talk2M is designed to be minimally intrusive by using outgoing ports that are usually already enabled (HTTPS port 443 or UDP port 1194).

How to prepare a successful installation of the Ewon connectivity in my network?

The Ewon router is typically configured as a DHCP client so it receives network settings automatically. The Ewon can also be configured to use a static IP address that is assigned and controlled by the IT department if preferred. A small utility called Talk2MConnectionChecker can be used to verify all connection parameters; available for download from Ewon website:

https://websupport.ewon.biz/support/product/download-zone/all-software

Will my network be accessible by the remote User?

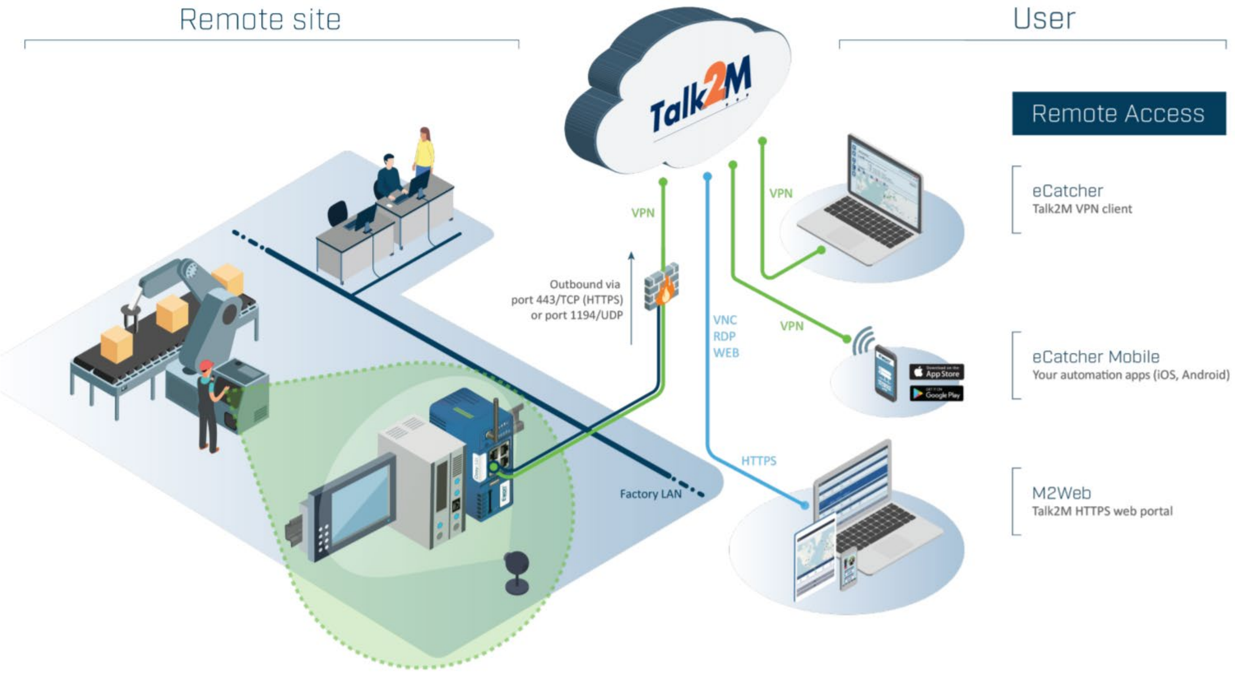
No, the Ewon router provides a segregation between WAN and the LAN machine subnet. The remote user can only reach the devices connected directly to the Ewon's LAN. The factory network cannot be accessed.

Key Benefits

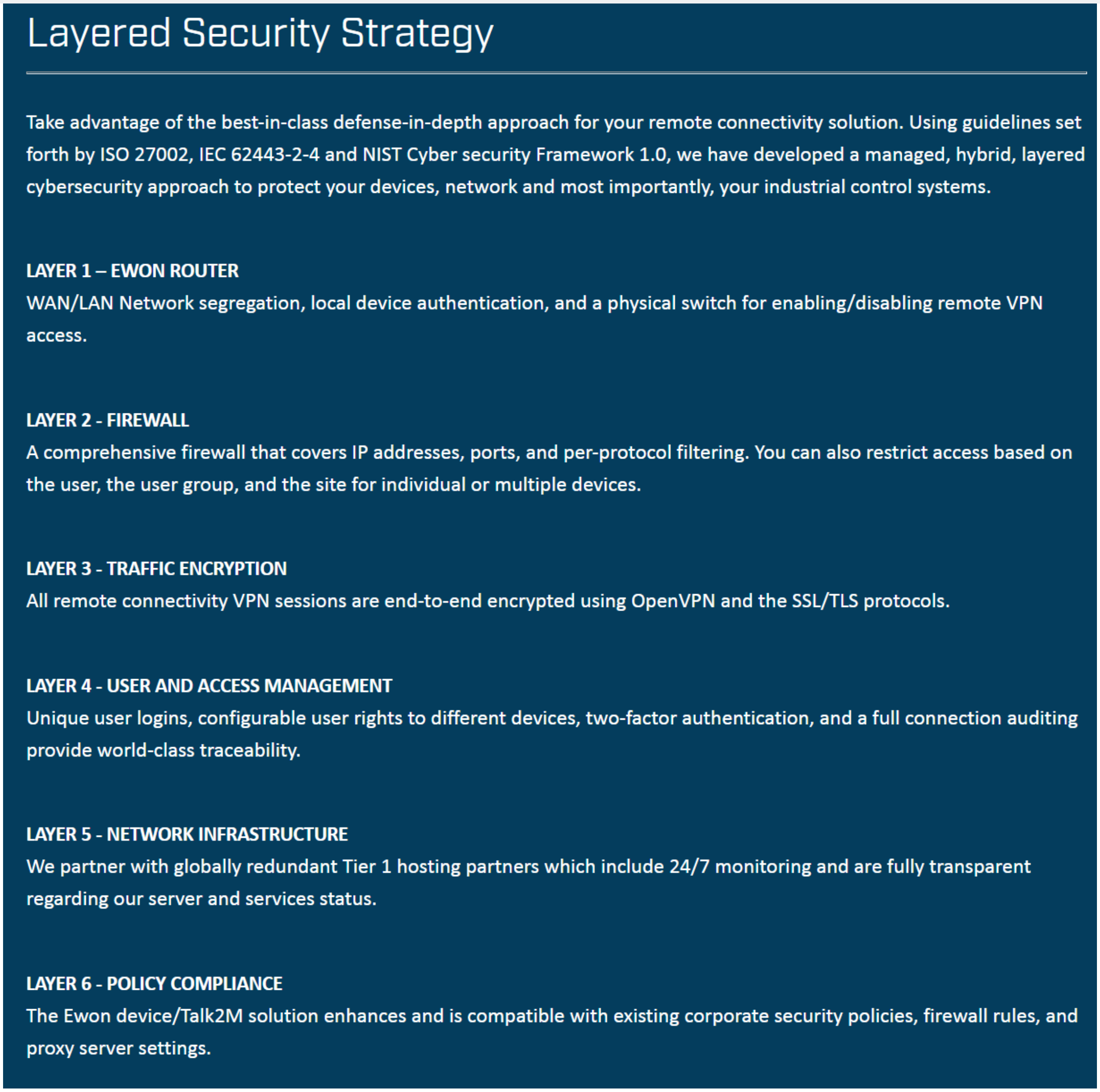
- **Eliminate downtime and travel expenses** – When problems occur, the machine's engineer can immediately analyze and resolve theissue remotely, limiting costly downtime and travel expenses. Using Ewon VPN products, you make it easy for the machine builder to setup and control a secure connection to your machines while keeping your corporate network integrity secure.
- **Integrated WiFi, Cellular connectivity for the Cosy 131** – WiFi and Cellular modems provide internet connectivity while avoiding connection to the factory/corporate LAN network. The customers have great flexibility to pick the most appropriate technology to allow secure remote connection within their operation.

How does Ewon Secured Connectivity work?

Ewon industrial routers (DIN rail mounted, 24VDC) are built to fit within the automation panel and can communicate with both Ethernet and serial devices . The Ewon device makes an outbound connection via UDP or HTTPS to HMS cloud based VPN servers called (Talk2M). Using the VPN client eCatcher, authorized users are able to log into their FREE Talk2M account and connect to their Ewon router anywhere in the world. The Talk2M server acts as a secure broker and completes the encrypted VPN tunnel between the remote user and the equipment connected to the Ewon router.



ISO 27001 Certified



Layered Security Strategy

Take advantage of the best-in-class defense-in-depth approach for your remote connectivity solution. Using guidelines set forth by ISO 27002, IEC 62443-2-4 and NIST Cyber security Framework 1.0, we have developed a managed, hybrid, layered cybersecurity approach to protect your devices, network and most importantly, your industrial control systems.

LAYER 1 – EWON ROUTER
WAN/LAN Network segregation, local device authentication, and a physical switch for enabling/disabling remote VPN access.

LAYER 2 - FIREWALL
A comprehensive firewall that covers IP addresses, ports, and per-protocol filtering. You can also restrict access based on the user, the user group, and the site for individual or multiple devices.

LAYER 3 - TRAFFIC ENCRYPTION
All remote connectivity VPN sessions are end-to-end encrypted using OpenVPN and the SSL/TLS protocols.

LAYER 4 - USER AND ACCESS MANAGEMENT
Unique user logins, configurable user rights to different devices, two-factor authentication, and a full connection auditing provide world-class traceability.

LAYER 5 - NETWORK INFRASTRUCTURE
We partner with globally redundant Tier 1 hosting partners which include 24/7 monitoring and are fully transparent regarding our server and services status.

LAYER 6 - POLICY COMPLIANCE
The Ewon device/Talk2M solution enhances and is compatible with existing corporate security policies, firewall rules, and proxy server settings.

Device: Ewon Cosy 131

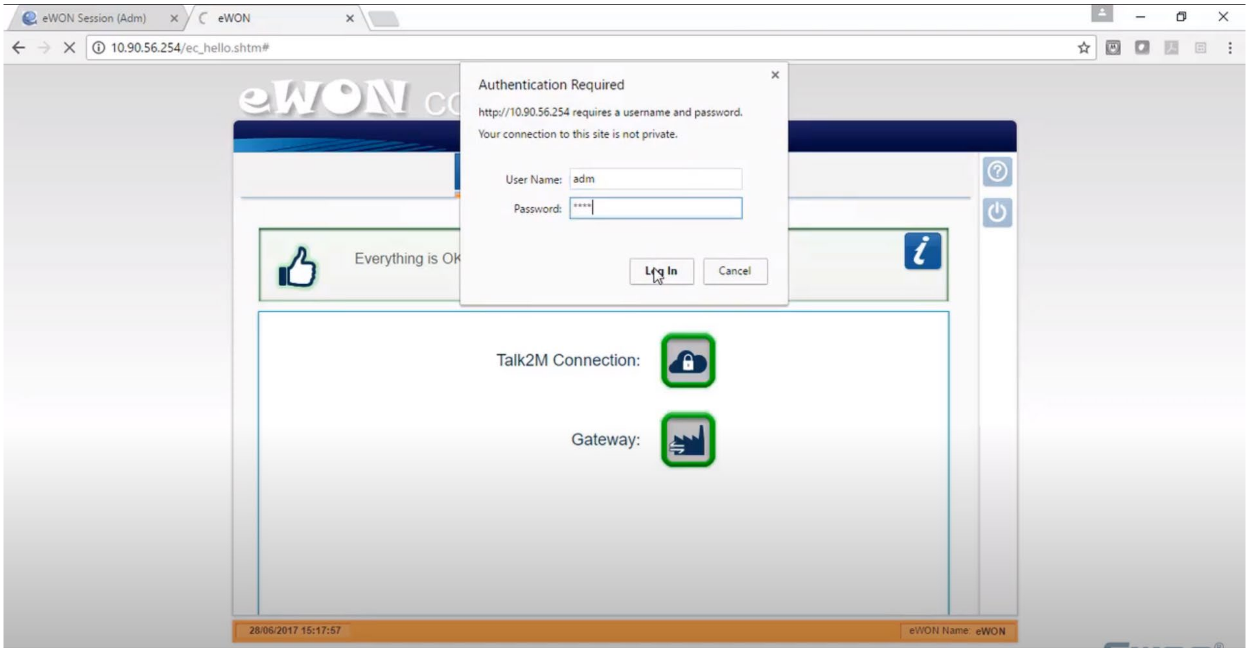
The device itself contains different layers of security in regards of user access, connection authorization.

https://www.ewon.biz/e-learning/library/cosy-131/security

Change the Default Password

The eWON comes with a default password for the administrator user "Adm". This password must be changed on first connection to the web interface of the eWON.

https://www.youtube.com/watch?v=742rL_LTFgw



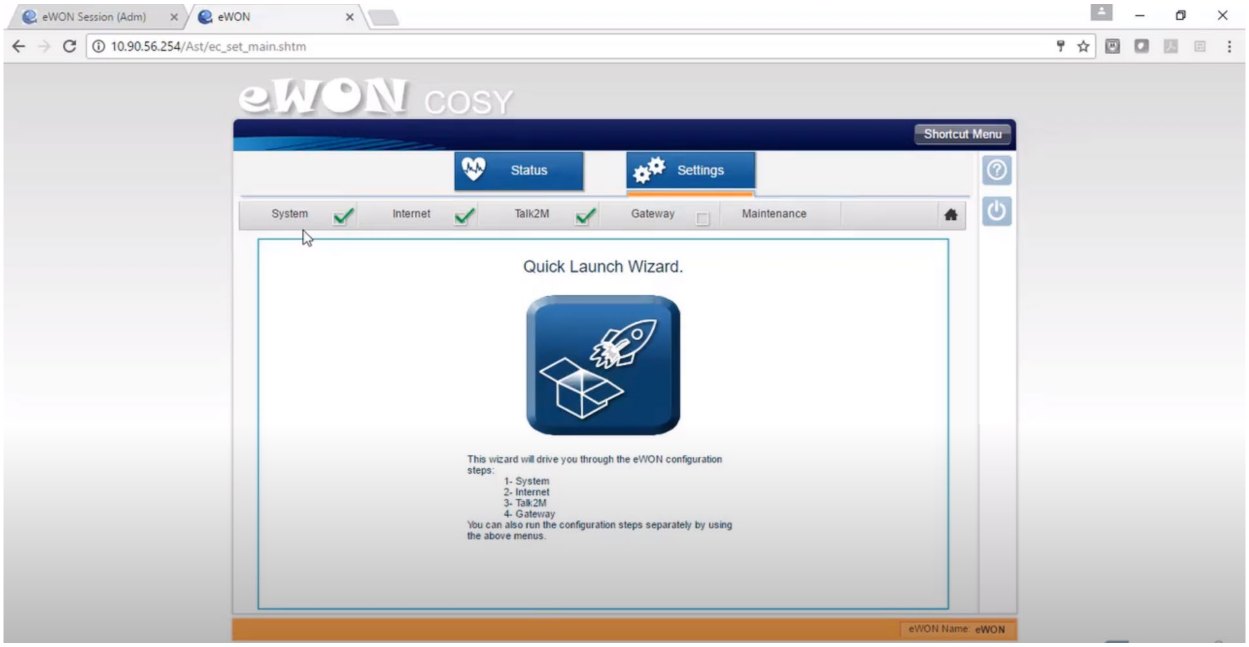
Authentication Required

http://10.90.56.254 requires a username and password.

Your connection to this site is not private.

User Name: adm

Password: ****

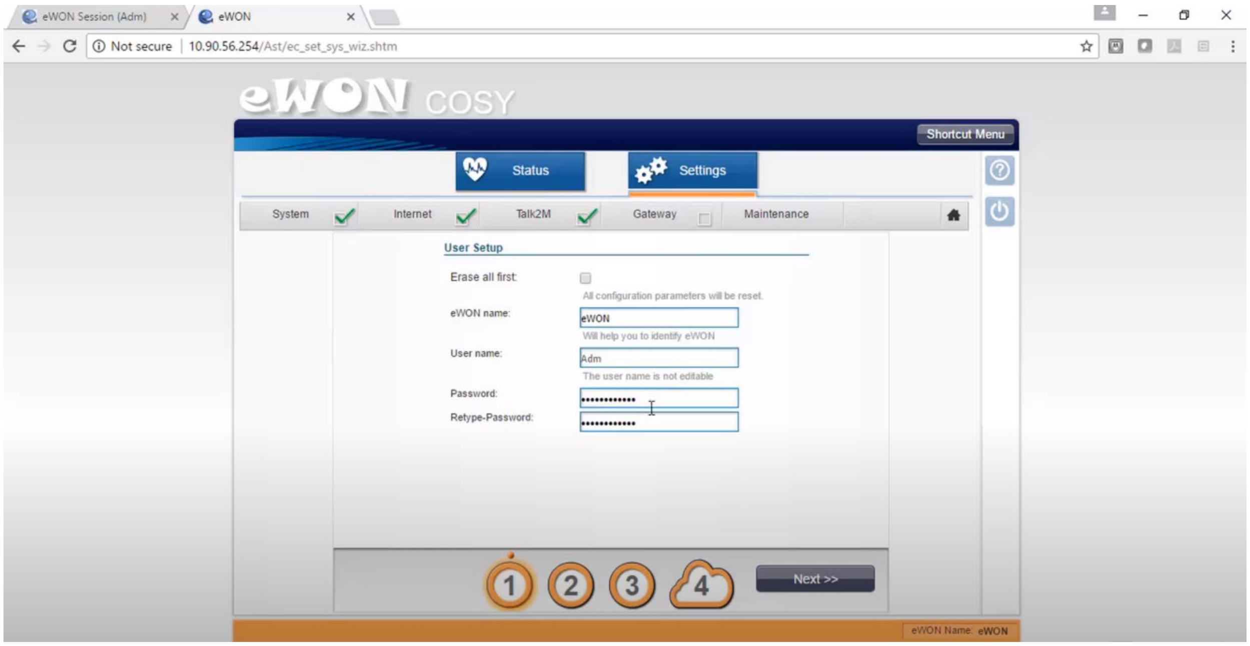


Quick Launch Wizard.

This wizard will drive you through the eWON configuration steps:

1- System
2- Internet
3- Talk2M
4- Gateway

You can also run the configuration steps separately by using the above menus.



User Setup

Erase all first: □
All configuration parameters will be reset.

eWON name: eWON
Will help you to identify eWON

User name: Adm
The user name is not editable

Password: ••••••••••••

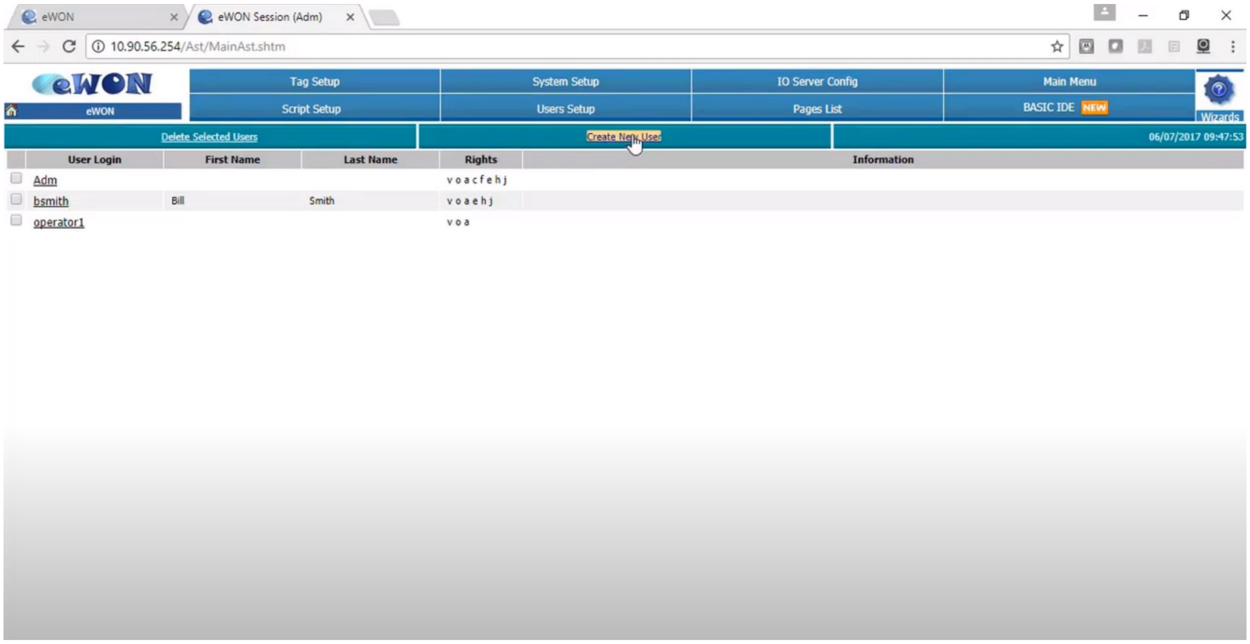
Retype-Password: ••••••••••••

User Access Rights

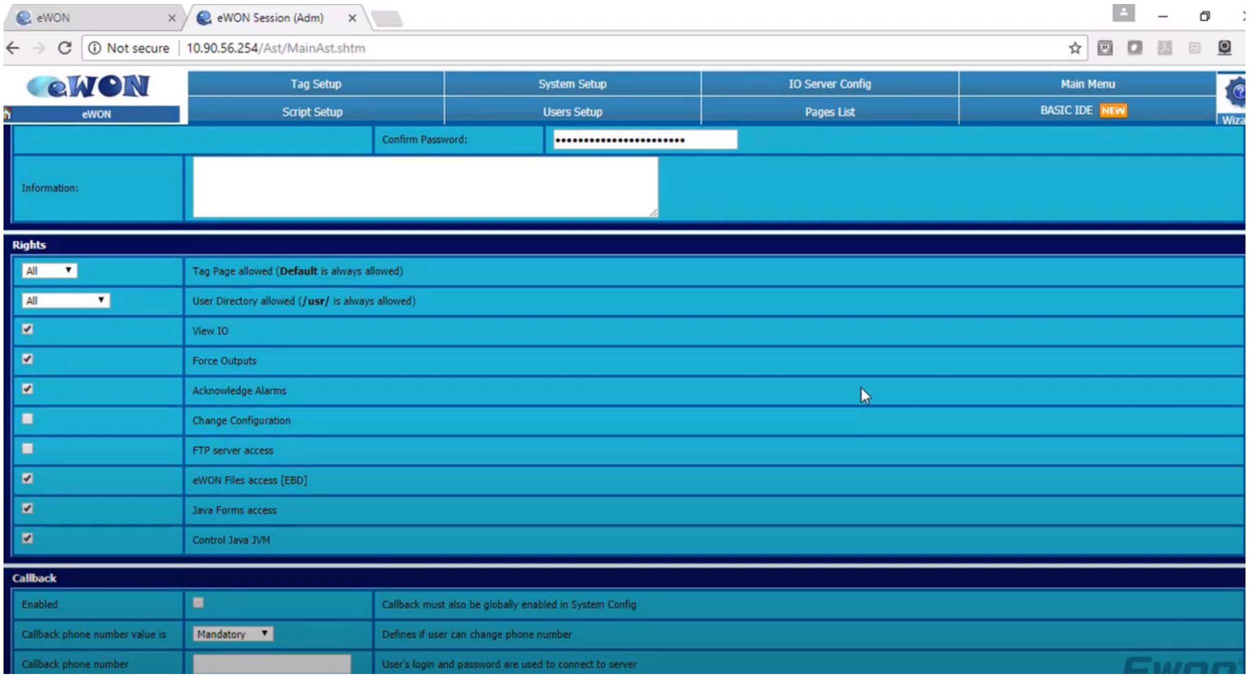
The eWON is built to be as secured as possible. One of these security measures goes through the user management.

https://www.youtube.com/watch?v=7pK1HKVoeM4&feature=youtu.be

47



	User Login	First Name	Last Name	Rights	Information
□	Adm			v o a c f e h j	
□	bsmith	Bill	Smith	v o a e h j	
□	operator1			v o a	



Confirm Password: ••••••••••••••••••••••••

Information:

Rights

All ▾	Tag Page allowed (**Default** is always allowed)
All ▾	User Directory allowed (**/usr/** is always allowed)
☑	View IO
☑	Force Outputs
☑	Acknowledge Alarms
□	Change Configuration
□	FTP server access
☑	eWON Files access [EBD]
☑	Java Forms access
☑	Control Java JVM

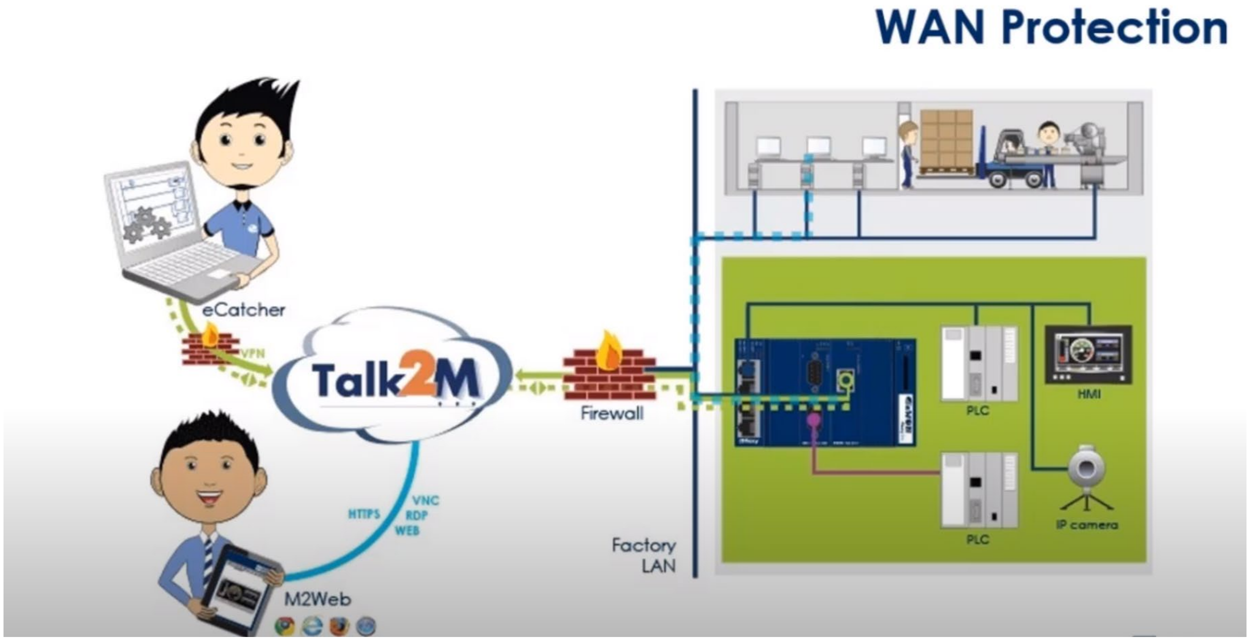
Callback

Enabled	□	Callback must also be globally enabled in System Config
Callback phone number value is	Mandatory ▾	Defines if user can change phone number
Callback phone number		User's login and password are used to connect to server

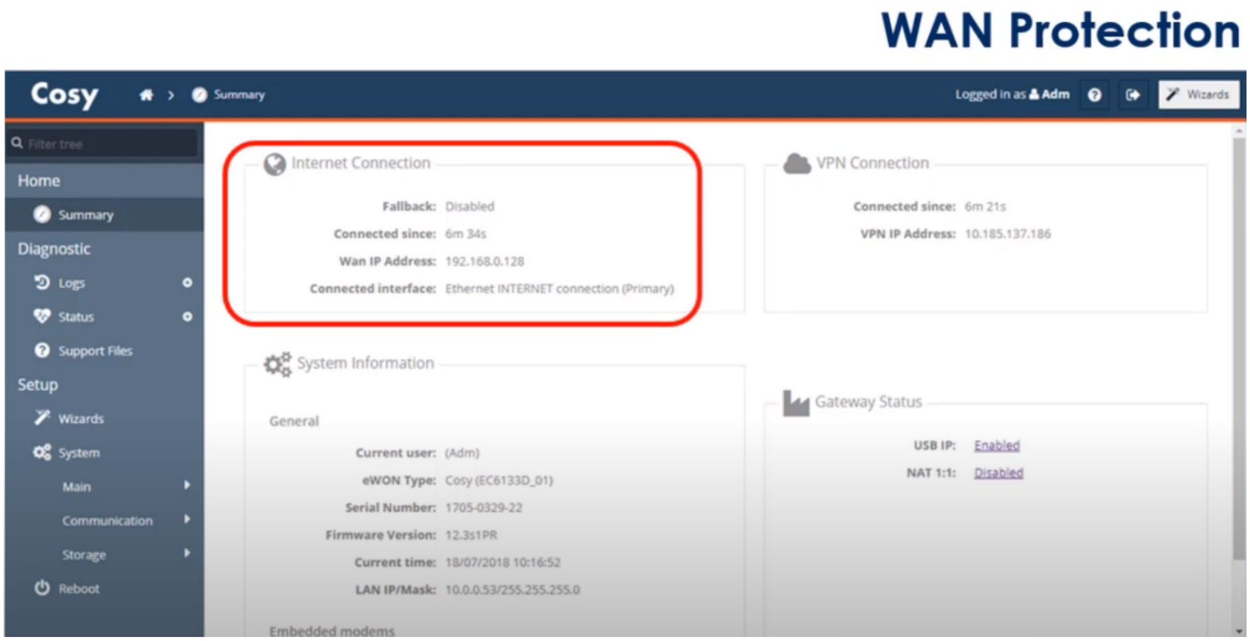
WAN Protection

You can protect the communication that goes between the WAN and LAN networks set on your Ewon.

https://www.youtube.com/watch?v=ybiY-AXJsAw&feature=youtu.be



WAN Protection



WAN Protection

Internet Connection

Fallback: Disabled
Connected since: 6m 34s
Wan IP Address: 192.168.0.128
Connected interface: Ethernet INTERNET connection (Primary)

VPN Connection

Connected since: 6m 21s
VPN IP Address: 10.185.137.186

System Information

General

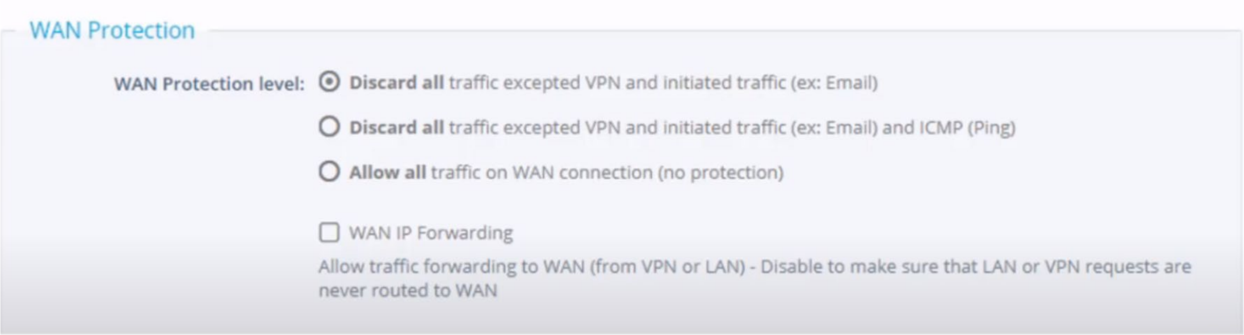
Current user: (Adm)
eWON Type: Cosy (EC6133D_01)
Serial Number: 1705-0329-22
Firmware Version: 12.3s1PR
Current time: 18/07/2018 10:16:52
LAN IP/Mask: 10.0.0.53/255.255.255.0

Embedded modems

Gateway Status

USB IP: Enabled
NAT 1:1: Disabled

WAN Protection



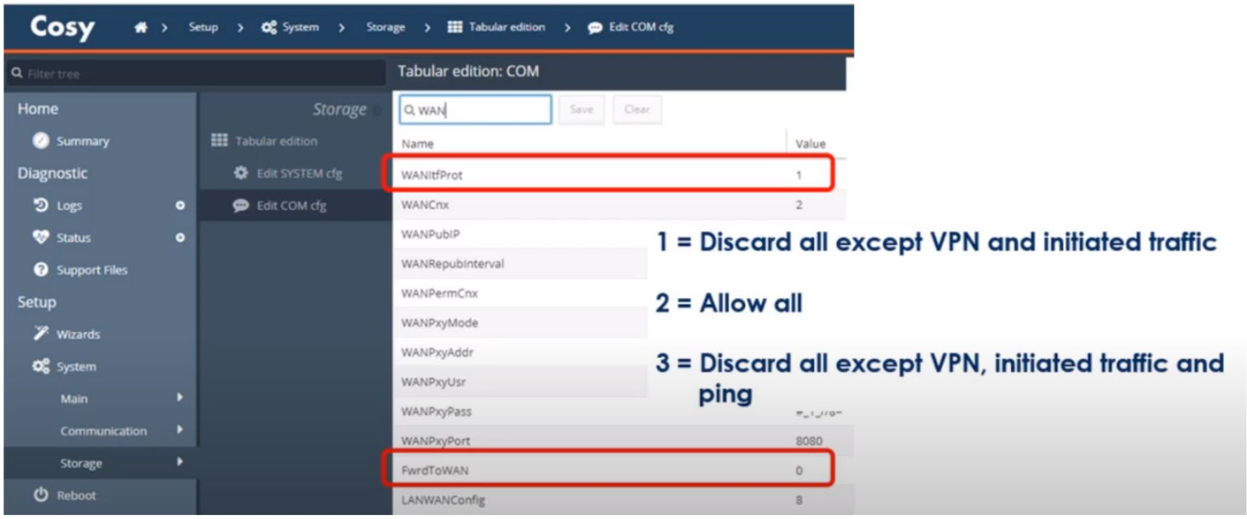
WAN Protection

WAN Protection level:
● **Discard all** traffic excepted VPN and initiated traffic (ex: Email)
○ **Discard all** traffic excepted VPN and initiated traffic (ex: Email) and ICMP (Ping)
○ **Allow all** traffic on WAN connection (no protection)

□ WAN IP Forwarding

Allow traffic forwarding to WAN (from VPN or LAN) - Disable to make sure that LAN or VPN requests are never routed to WAN

WAN Protection



Tabular edition: COM

WAN

Name	Value
WANItfProt	1
WANCnx	2
WANPubIP	
WANRepubInterval	
WANPermCnx	
WANPxyMode	
WANPxyAddr	
WANPxyUsr	
WANPxyPass	
WANPxyPort	8080
FwrdToWAN	0
LANWANConfig	8

1 = Discard all except VPN and initiated traffic

2 = Allow all

3 = Discard all except VPN, initiated traffic and ping

Talk2M Pro Account

HMS Talk2M is ISECOM STAR certified after passing an assessment performed by the company Admeritia GmbH, a vendor-independent German cybersecurity company specialized in IT Security assessment (ethical hacking) and KPI-based security measurement. The assessment was done through an OSSTMM 3.0 and OWASP audit process which included penetration tests of Talk2M targeting the cloud based infrastructure.

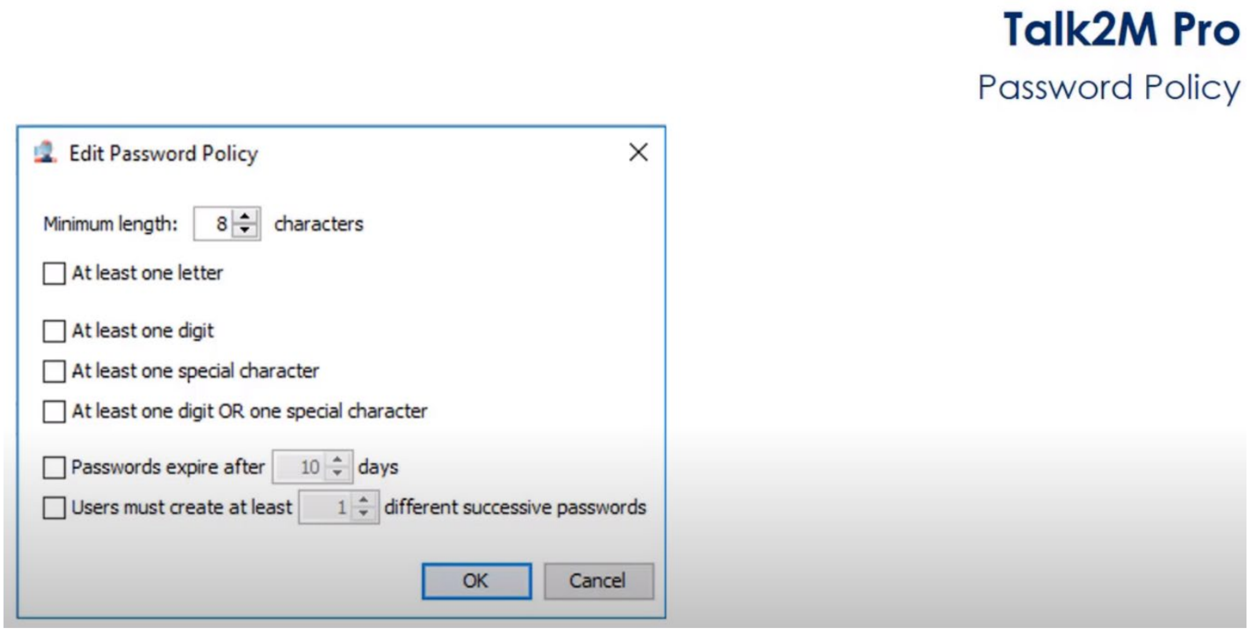
eWON solutions Security Manager Geoffrey Gobert comments: “The assessment was performed through a number of tests from the perspective of a malicious actor, and we got a snapshot of the overall security posture of the eWON Talk2M remote connectivity service. We are very satisfied to have successfully passed the ISECOM STAR security certification and are committed to continue with regular security assessments to ensure that we provide secure connectivity for our customers. We always aim to identify any technical risk can translate into business risk.”

Our ISO 27001 scope covers both Talk2M our industrial cloud solution and our gateways. Our engineers are regularly audited to ensure the highest security level of our products and services, and to offer the most secure solution with confidentiality, integrity, and availability in perfect balance.

Password Management

In a Talk2M Pro account, password settings can be modified to fit the user desire.

https://www.youtube.com/watch?v=0Qa0tDcUVJ4



Talk2M Pro

Password Policy

Edit Password Policy

Minimum length: 8 characters

□ At least one letter

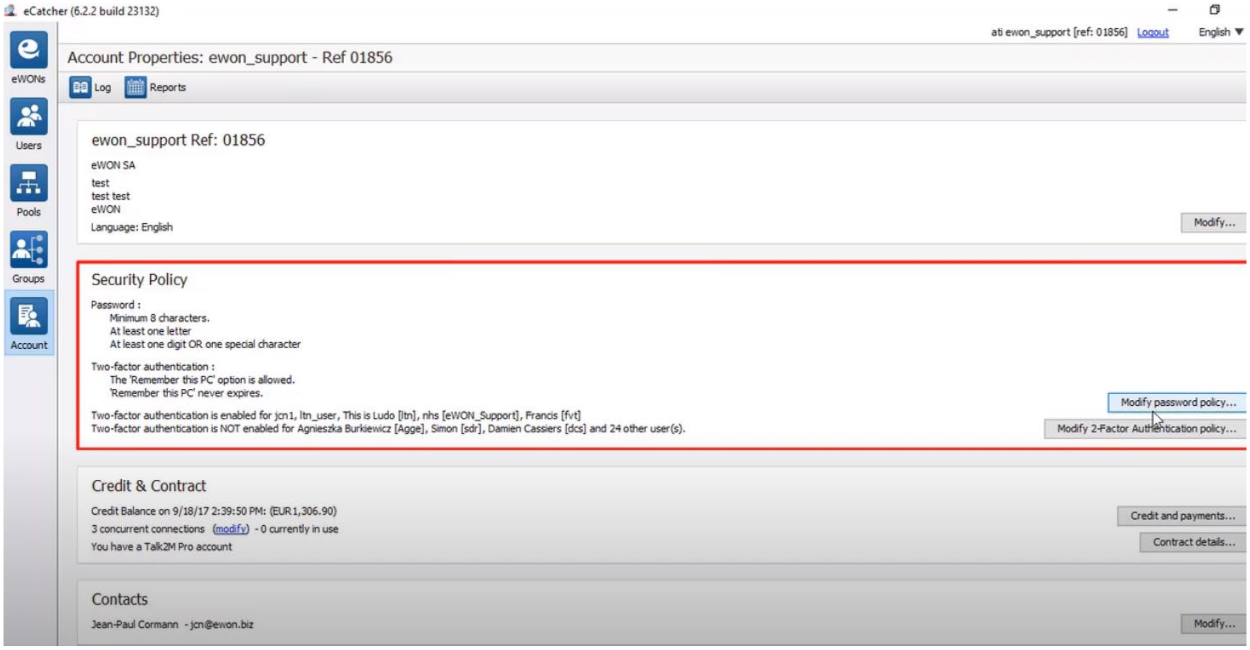
□ At least one digit

□ At least one special character

□ At least one digit OR one special character

□ Passwords expire after 10 days

□ Users must create at least 1 different successive passwords


eCatcher (6.2.2 build 23132)
ati ewon_support [ref: 01856] Logout
English ▼
eWONs
Users
Pools
Groups
Account
Log
Reports
Modify...
Modify password policy...
Modify 2-Factor Authentication policy...
Credit and payments...
Contract details...
Modify...

Account Properties: ewon_support - Ref 01856

ewon_support Ref: 01856

eWON SA

test
test test
eWON

Language: English

Security Policy

Password :
Minimum 8 characters.
At least one letter
At least one digit OR one special character

Two-factor authentication :
The 'Remember this PC' option is allowed.
'Remember this PC' never expires.

Two-factor authentication is enabled for jcn1, ltn_user, This is Ludo [ltn], nhs [eWON_Support], Francis [fvt]
Two-factor authentication is NOT enabled for Agnieszka Burkiewicz [Agge], Simon [sdr], Damien Cassiers [dcs] and 24 other user(s).

Credit & Contract

Credit Balance on 9/18/17 2:39:50 PM: (EUR1,306.90)
3 concurrent connections (modify) - 0 currently in use
You have a Talk2M Pro account

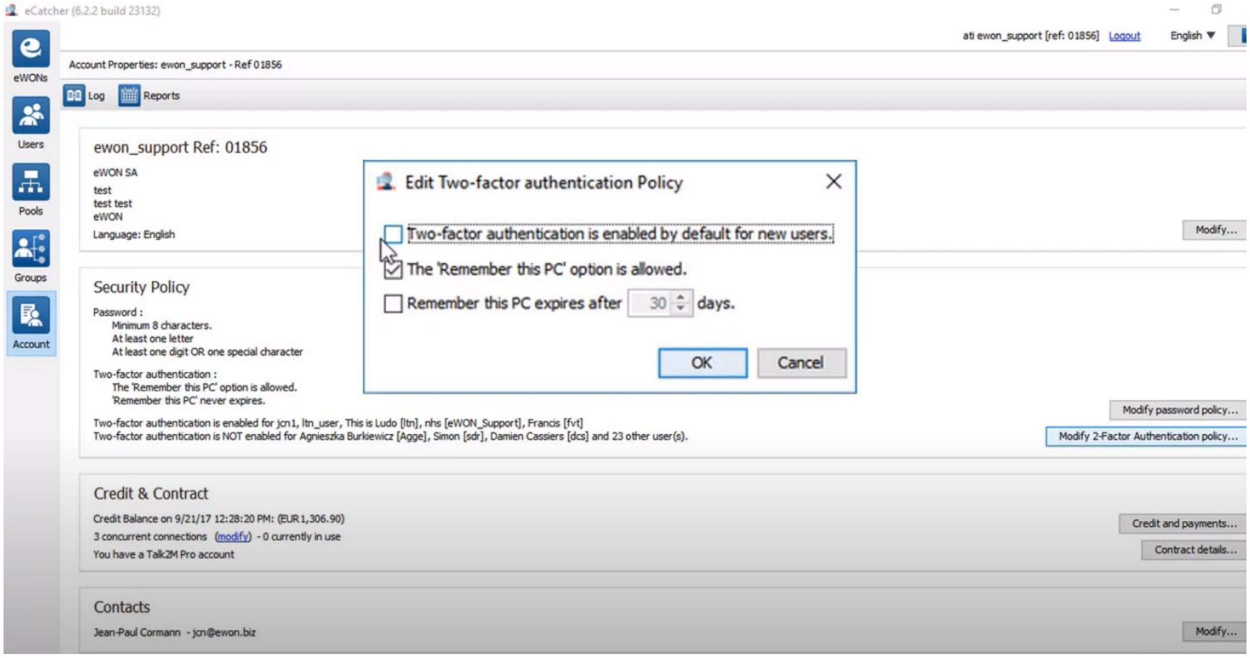
Contacts

Jean-Paul Cormann - jcn@ewon.biz

Two-Factor Authentication (2FA)

The Talk2M account can be combined with the 2-factor authentication for an extra layer of security in regards of account access.

https://www.youtube.com/watch?v=NdOCZtm20C0



eCatcher (6.2.2 build 23132)
ati ewon_support [ref: 01856]
Logout
English ▼
eWONs
Users
Pools
Groups
Account
Log
Reports
Modify...
Modify password policy...
Modify 2-Factor Authentication policy...
Credit and payments...
Contract details...
Modify...

Account Properties: ewon_support - Ref 01856

ewon_support Ref: 01856

eWON SA
test
test test
eWON
Language: English

Security Policy

Password :
Minimum 8 characters.
At least one letter
At least one digit OR one special character

Two-factor authentication :
The 'Remember this PC' option is allowed.
'Remember this PC' never expires.

Two-factor authentication is enabled for jcn1, ltn_user, This is Ludo [ltn], nhs [eWON_Support], Francis [fvt]
Two-factor authentication is NOT enabled for Agnieszka Burkiewicz [Agge], Simon [sdr], Damien Cassiers [dcs] and 23 other user(s).

Credit & Contract

Credit Balance on 9/21/17 12:28:20 PM: (EUR 1,306.90)
3 concurrent connections (modify) - 0 currently in use
You have a Talk2M Pro account

Contacts

Jean-Paul Cormann - jcn@ewon.biz

Edit Two-factor authentication Policy

□ Two-factor authentication is enabled by default for new users.
☑ The 'Remember this PC' option is allowed.
□ Remember this PC expires after 30 days.

OK Cancel