

Позицията за сигурност на Ewon

Как решението на Ewon работи и отговаря на изискването за високо защитена отдалечена индустриална свързаност.



Отдалечения достъп до индустриалното оборудване вече се подразбира като нещо обичайно.

За производителите на машини това означава по-бързо отстраняване на повредите на машините, оптимизиране ефективността на сервизните екипи и намаляване на разходите, повишаване удовлетвореността на клиентите, а вече и онлайн мониторинг, получаване на аларми и информация, и данни за интелигентни приложения.

Производствените компании използват отдалечен достъп, за да поддържат работоспособното състояние на машинния си парк, да консолидират отношенията си с доставчиците на машини, да осигурят свързаност с техния завод.

Безспорно сигурността на избраното решение за отдалечена свързаност е изключително важна и тя е в основата на решението на Ewon.

По-долу са представени различните аспекти на сигурността, свързани с решението на Ewon, за информация на потребителите, собствениците на фабрики и ИТ екипите.

С повече от 20 години опит в индустриалните приложения, Ewon на HMS Networks си сътрудничи с производители и потребители на машини и им помага в техния път към успешна дигитализация, отдалечена свързаност и индустриален интернет на нещата (IIoT). HMS Networks са известни с дългогодишния си опит в индустриалните приложения и добро разбиране на пазарните очаквания, доказали са се като доставчици на качествени продукти и услуги, на решения, подготвени за бъдещето.

Изборът и използването на решение на Ewon е гаранция за дългосрочна наличност и устойчивост. Киберсигурността

е в основата на решението на Ewon, проектирано от самото начало като осигуряващо необходимата сигурност, редовно проверявано и сертифицирано от независими организации. Решението на Ewon е цялостно сертифицирано по ISO 27001. Работи се за непрекъснато подобряване на организационните процеси и техническата експертиза на инженерните екипи, за да се гарантира най-високо ниво на сигурност за всички продукти и услуги на Ewon.

Архитектура на решението Ewon

Решението на Ewon се състои от 2 основни компонента:

1. Ewon Talk2m: глобална облачна услуга за свързаност, която централизирано управлява всички аспекти на свързаността.
2. Ewon гейтуей: хардуерен гейтуей, който обикновено се поставя в контролното табло на промишленото оборудване и се свързва с устройства за управление като PLC и HMI.

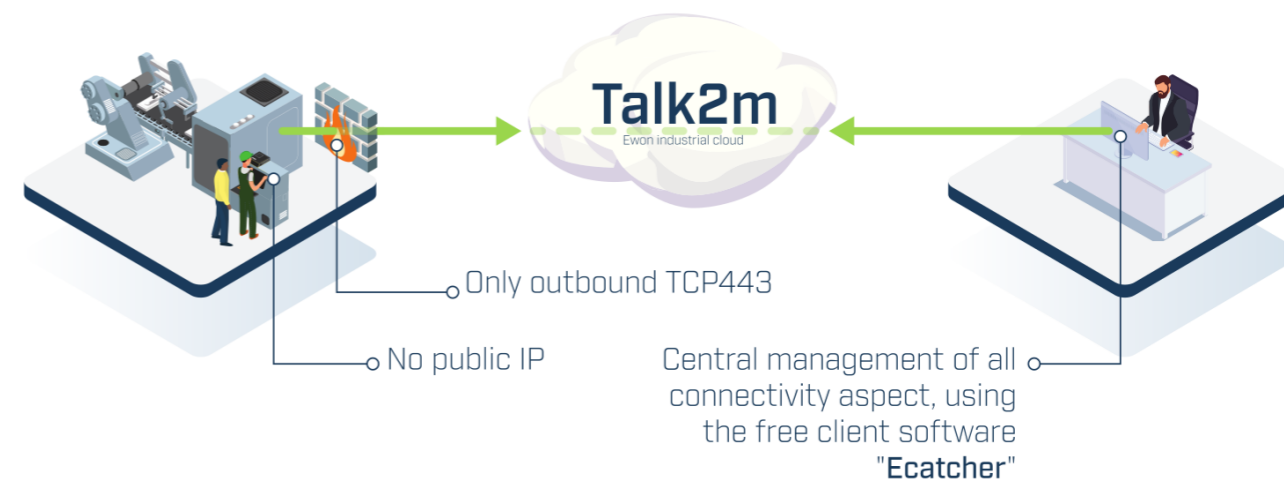
С тази структура инженерите по поддръжката, независимо от географското си местоположение или часова зона, могат да установят сигурна връзка за отдалечен достъп до оборудването от своите компютри или мобилни устройства, с няколко кликания.

• Talk2m е облачна инфраструктура, състояща се от множество сървъри, които осъществяват комуникациите между потребители и машини. Цялата система работи при условие, че и двете страни в комуникацията (потребител и гейтуей/машина) имат достъп до интернет и могат да се свържат със сървърите на Talk2m. Talk2m осигурява сигурна криптирана връзка, позволяваща на потребителя

да работи по отдалеченото оборудване, сякаш е до него.

• При машината се инсталира Ewon гейтуей („Cosy“ или „Flexy“) и се свързва с автоматизираните устройства за контрол на машината, като PLC, HMI или IP камера. Тази връзка е възможна чрез Ethernet, сериен порт (RS232/RS485/RS422 или MPI) или USB. Ewon гейтуей се свързва сигурно с интернет чрез Ethernet, WiFi или мобилна мрежа, за да взаимодейства с Talk2m.

• От страна на потребителя, на компютър с OS Windows се инсталира софтуерно приложение за управление на връзката, наречено „Ecatcher“, което служи за установяване на сигурна комуникационна връзка между компютъра и Talk2m през интернет, както и за конфигуриране и управление на потребителския акаунт в Talk2m. Връзката може да се установи и от мобилно устройство посредством приложението „Ecatcher Mobile“, работещо на Android и iOS, или от всеки уеб браузър с помощта на M2web - уеб портала на Talk2m.



Предимства на облачния сървър Rendez-Vous: За установяване на връзка с отдалечено промишлено оборудване са възможни различни подходи - модемна връзка, софтуерна връзка (обикновено решение за отдалечен работен десктоп), директна VPN връзка, свързване чрез частен APN или частен VPN сървър. Тези методи никога не са успявали напълно да отговорят на очакванията, свързани с индустриални приложения, като надеждна сигурност, мащабируемост за големи промишлени инсталации с много оборудване, незабавна достъпност на свързаността за бърза реакция и лекота на използване от всеки потребител, дори без да е ИТ експерт. През 2006 г. Ewon създаде Talk2m, Rendez-Vous сървър, който свързва по много сигурен и лесен начин Ewon гейтуейте и VPN клиента Ecatcher, работещ на компютъра на потребителя. Предимства на облачния Rendez-Vous сървър Talk2m са:

• Ефективност, като предоставя централно място за управление на всички аспекти на решението за отдалечена свързаност (устройства, потребители, права за достъп...).

• Сигурност, тъй като са необходими само изходящи връзки и следователно не е необходимо да се променя фирмената защитна стена на потребителя.

• Мащабируемост, достъпност и производителност, с платформа, проектирана да се разраства с времето.

Talk2m е обширна и изцяло резервирана глобална сървърна инфраструктура, която оптимизира връзките между крайните точки. Състои се основно от два типа сървъри: за достъп (AS) и VPN (VS) сървъри. Сървърите за достъп са първите, към които се обръщат устройствата или потребителите, иницирайки връзка с Talk2m. Те се грижат за всички аспекти на удостоверяването и играят ролята на централен координатор, контролирайки всички разрешения и координирайки взаимодействията между различните услуги на Talk2m, потребителите и устройствата. VPN сървърите са разпределени по целия свят и са Rendez-Vous сървъри, които обработват действителните VPN връзки между потребителите и устройствата.

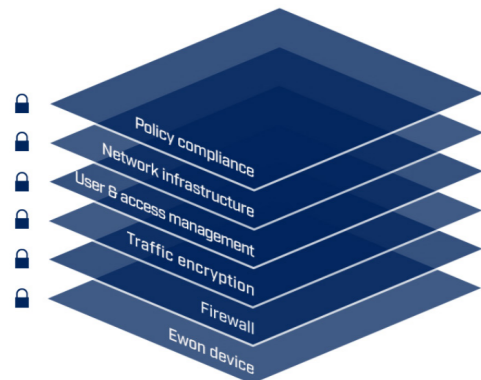
След аспектите на сигурността, вторият най-висок

приоритет на архитектурата на Talk2m е да предлага най-добрата възможна наличност на своите услуги за свързаност. Инфраструктурата на Talk2m включва повече от 40 сървъра, разпределени по целия свят и хоствани от множество водещи хостинг доставчици, за да осигурят световно покритие и резервираност за максимална непрекъснатост на бизнеса.

Използването на Talk2m значително намалява усилията, инвестициите и експертния опит, необходими за създаване и поддържане на професионално решение за отдалечен достъп в световен мащаб.

Сигурност на решението Ewon: За да се постигне най-високо ниво на сигурност, системата е проектирана и изградена на основата на подхода „Defense in Depth“ (защита в дълбочина). Това е координирано използване на различни видове мерки за сигурност, разпределени на няколко нива на контрол на сигурността. Такъв подход гарантира защитата на цялото Ewon решение и следователно на мрежите, устройствата и индустриалните системи за управление на потребителите. Той се основава

на насоките, определени от водещи стандарти за сигурност като ISO 27001, IEC 62443 и NIST Cyber Security Framework, както и най-добри практики в индустрията.



Talk2m - управление на дейностите за отдалечен достъп

Talk2m служи за сигурно и лесно установяване на връзка между потребителите и тяхното отдалечено оборудване, и за управление от едно централно място на всички аспекти на отдалечената свързаност като управление на акаунта, на потребителите и на устройствата, определяне на политиката за сигурност, мониторинг на дейността.

Акаунтът в Talk2m е работното пространство за управление на устройства, потребители и всички аспекти на сигурността на Ewon решението за отдалечена свързаност.

Администратори: Администраторът на акаунта в Talk2m има ключова роля с разширени отговорности: управлява всички настройки и свойства на акаунта в Talk2m, като общи параметри, политики за пароли, аспекти на кредитния баланс и нивата на услугите, контактна информация и др., регистрира устройства Ewon, създава потребители и определя техните роли и права за достъп, има достъп до лог файлове и доклади за мониторинг на дейността, извършвана в акаунта. (Може да има няколко администратора, включително такива с по-ограничен достъп и правомощия.)

Администраторите на акаунт в Talk2m могат да адаптират политиките за пароли за различни нива на сигурност като правила за пароли, срок на валидност на пароли, двуфакторно удостоверяване, за по-висока сигурност на процеса за влизане в системата. Talk2m има и механизъм за блокиране на повтарящи се опити за влизане с неправилни пароли, като временно деактивира потребителя и уведомява администраторите на акаунта за предприемане на подходящи мерки.

Потребители: В Talk2m акаунта се създават и дефинират потребители, които могат да взаимодействат с акаунта или регистрираните в него Ewon гейтуеи според своите роли и права за достъп. Например, на екипите за поддръжка и сервис може да бъде предоставен пълен VPN достъп до всички машини, за да могат да извършват дистанционно програмиране, отстраняване на неизправности или контрол. За мониторинг може да е достатъчен само ограничен достъп - за връзка с HMI или информация за

състоянието и производителността на оборудването.

Устройства Ewon: един Ewon гейтуей може да се регистрира в и принадлежи само на един Talk2m акаунт. Talk2m предоставя функционалности за управлението на нарастващия брой Ewon гейтуеи във времето:

- За включването на множество гейтуеи с подобни настройки може да се използва „глобален регистрационен ключ“ в конфигурационен файл, който лесно се инсталира на всички устройства чрез USB устройство или SD карта.

- Възможно е автоматизирано масово внедряване на актуализации на софтуера.

Пулове и групи: Talk2m light и Talk2m pro позволяват обединяване на устройства в пулове и на потребители в групи, с цел улесняване на управлението им.

Защитна стена на устройствата и гранулирано ниво на достъп до оборудването: Talk2m light и Talk2m pro позволяват контрол с различни нива на детайлност на разрешенията на потребителите за достъп до конкретни устройства, свързани зад Ewon гейтуея, като PLC и HMI, от липса на ограничения до строго ограничен достъп чрез определяне на всички достъпни IP адреси, портове и дори протоколи.

Активност и мониторинг на акаунта: Talk2m предоставя инструменти за наблюдение на дейностите и събитията, които се случват в рамките на даден акаунт, и за проверка на съответствието с корпоративните политики за сигурност. За целите на сигурността и проследимостта са налични логове, в които са изброени всички връзки, прекъсвания на връзката, както и промени в състоянието на всички потребители и устройства. Финансов отчет помага да се следи потреблението на данни и кредитния баланс на акаунта в Talk2m.

Споразумение за ниво на обслужване (SLA) на Talk2m: Ewon се стреми да осигури отлична непрекъснатост на бизнеса за всички потребители и предлага три варианта на услугата Talk2m:

- Безплатна услуга Talk2m, идеална за клиенти с малък брой инсталирани Ewon гейтуеи (достъпна 12 месеца след инсталиране на всяко ново устройство в акаунта),
- Абонаментен план Talk2m light, базиран на подобрени хостинг услуги, включващ всеобхватно SLA и отговарящ на нуждите на повечето потребители.
- Абонаментен план Talk2m pro, който предоставя премиум услуга и пълна функционалност.

Как работи решението на Ewon. Установяване на връзка за отдалечен достъп

Свързване на потребител с Talk2m: Потребителят влиза в акаунта си в Talk2m с помощта на клиентския софтуер Ecatcher (безплатен), използвайки идентификационните си данни: име на акаунта, потребителско име и парола. Започва HTTPS сесия към облака Talk2m за удостоверяване на потребителя и след като се впише, той може да извършва различни действия в зависимост от разрешенията си:

- Регистриране на нов Ewon гейтуей в акаунта, редактиране

или изтриване на информация за гейтуей.

- Добавяне, промяна или изтриване на потребители или групи от потребители в акаунта.
- Добавяне, промяна или изтриване на пулове от Ewon гейтуеи в акаунта.
- Модифициране на общите настройки на Talk2m акаунта, проверка на информация за неговото използване.
- Установяване на VPN връзка с Ewon гейтуей.

Регистриране на Ewon Gateway в Talk2m акаунт:

С няколко прости стъпки Ewon гейтуей, свързан към табло на машина, може да бъде конфигуриран за свързване с интернет и да бъде регистриран в Talk2m акаунта на потребителя.

1. Първо с Ecatcher се създава в Talk2m акаунта запис за Ewon гейтуея. Генерира се уникален „активационен ключ“, необходим в следващата стъпка за удостоверяване на Ewon гейтуея и свързването му със запис в акаунта Talk2m.
2. Следва присвояване на активационния ключ към Ewon гейтуея, за да може да се свърже с Talk2m за първи път, да се удостовери в акаунта на потребителя и да завърши процеса на регистрация. За да докаже, че е оригинален продукт на Ewon и да предостави уникална идентификация на Talk2m, Ewon гейтуеят ще използва своя „birth“ сертификат. Вариантите са:

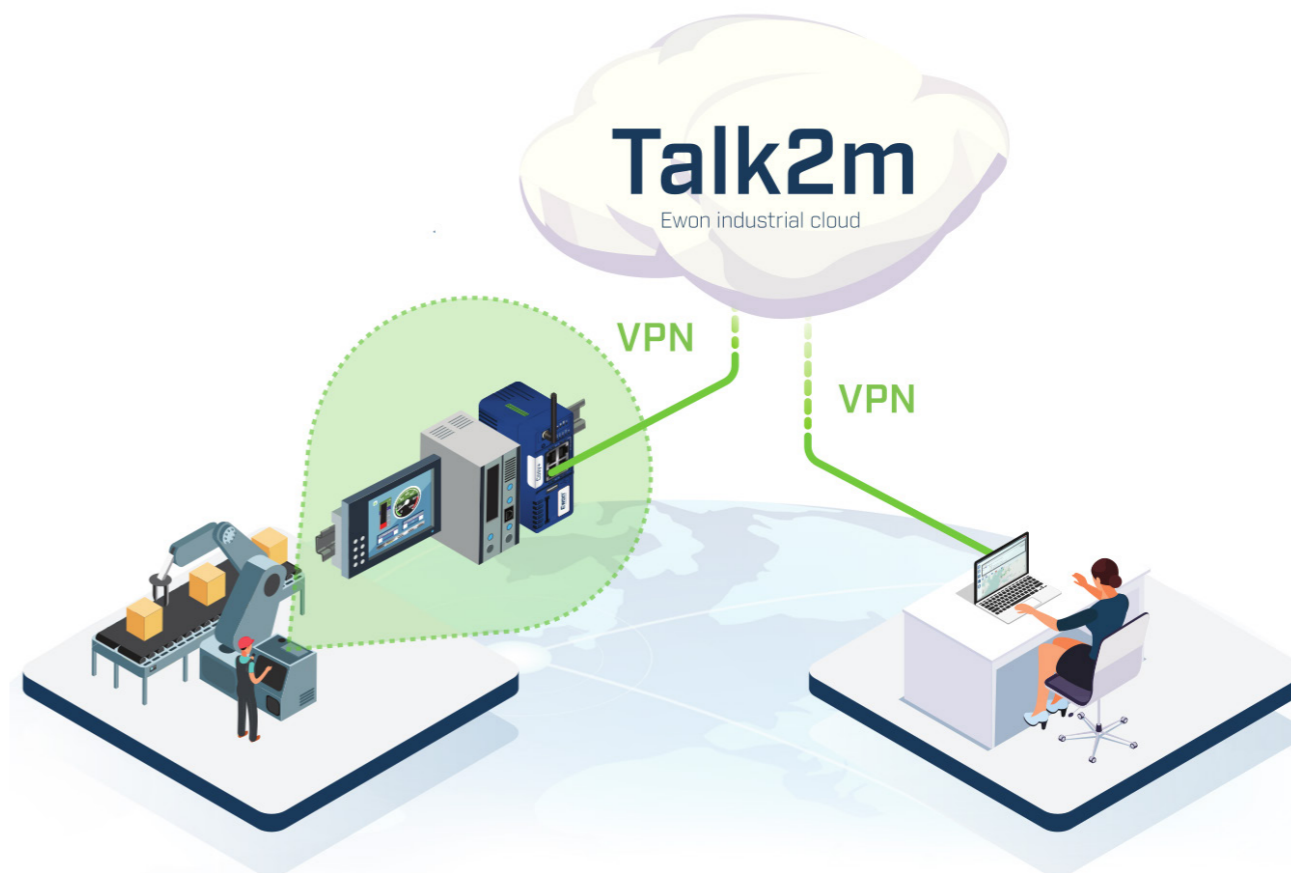
- „Ръчно“ стартиране на „Talk2m connecton wizard“ на Ewon гейтуея от неговия уеб интерфейс. По време на процеса потребителят трябва да въведе активационния ключ, получен в първата стъпка.

- „Автоматично“ конфигуриране на Ewon гейтуея с помощта на SD карта или USB флаш памет, съдържаща конфигурационен файл, който може да бъде генериран в края на първата стъпка и включва активационния ключ.

Свързване на машина с Talk2m: След като се регистрира в Talk2m, Ewon гейтуеят автоматично ще установи VPN връзка с услугата Talk2m. Това се извършва в три фази:

1. Процес на инициализация, по време на който гейтуеят ще се свърже и ще се удостовери пред облачната услуга Talk2m чрез HTTPS връзка, използвайки своя „birth“ сертификат.
2. След това Ewon гейтуеят изпраща HTTPS заявка, за да попита за най-подходящия VPN сървър, към който трябва да се свърже (VPN сървърът може да се променя между връзките).
3. Накрая, гейтуеят установява VPN тунел към VPN сървъра, назначен в предходната стъпка.

След като VPN връзката бъде установена, Ewon гейтуеят ще се появи в акаунта Talk2m със статус „онлайн“ и потребителите ще могат да се свързват с него дистанционно.



VPN връзка от потребител към машина: За да се свърже с отдалечена машина, потребителят трябва да влезе в своя Talk2m акаунт, използвайки Ecatcher. След успешно влизане се показва списък с всички Ewon гейтуеи, за които потребителят притежава права за достъп. За да установи VPN връзка с Ewon гейтуей, чийто статус е „онлайн“, потребителят просто трябва да го избере от списъка и да кликне върху бутона „Свържи (Connect)“. Чрез HTTPS заявка Ecatcher ще поиска от Talk2m да посочи VPN сървър, към който Ewon гейтуеят вече е свързан. Ecatcher ще установи VPN към този сървър. Накрая, двата VPN тунела – първият между Ewon гейтуея и VPN сървъра, и вторият между Ecatcher и VPN сървъра – ще бъдат свързани на VPN сървъра, за да позволят сигурна комуникация между Ecatcher и Ewon гейтуея. На компютъра на потребителя се добавя маршрут, за да се пренасочи през VPN тунела целият трафик, чийто IP адрес по местоназначение принадлежи към обхвата на LAN IP на Ewon гейтуея.

След като VPN връзката бъде установена, компютърът на потребителя все едно е директно свързан към мрежата, намираща се от LAN страната на Ewon гейтуея. Потребителят получава достъп до устройствата, инсталирани в отдалечената машина. Може например да се свърже с PLC и да извърши операции по мониторинг или поддръжка от разстояние.

След приключване на работата на отдалечената машина потребителят кликва върху бутона „Изключи (Disconnect)“ на Ecatcher, за да прекрати VPN връзката. Маршрутът, който е бил добавен на компютъра, се премахва.

Още за сигурността на решението на Ewon

Изходяща VPN връзка: VPN протоколът, използван от Talk2m, е базиран на OpenVPN и използва OpenSSL. Удостоверяването на Ewon гейтуей или потребител (чрез клиентския софтуер eCatcher) пред Talk2m се извършва през изходящия порт TCP/443 (HTTPS), а самата VPN връзка може да бъде установена или през изходящия порт UDP/1194 (порт на OpenVPN по подразбиране), или през изходящия порт TCP/443.

Тъй като се използват само изходящи връзки от надеждна мрежа (като фабричната LAN от страна на Ewon гейтуея или офис LAN от страна на потребителя), не е необходимо да се отварят портове за входящи връзки в защитната стена, която предпазва мрежата. Друго предимство е, че не е необходимо да се използва публичен IP адрес за Ewon гейтуея, който по този начин не е „видим“ в интернет.

При свързването с интернет от вътрешната страна на LAN може да се наложи преминаване през HTTP прокси сървъри. Прокси, които се поддържат както от Ecatcher, така и от Ewon гейтуеите, са прокси без удостоверяване, прокси с удостоверяване на потребител и парола, прокси с NTLM оторизация.

Верига на доверие по време на отдалечената връзка: Решението Ewon е проектирано да защитава всички данни, обменяни между индустриалната машина и потребителя, независимо от разстоянието, което ги разделя. Сигурността на информацията се осигурява с помощта на криптография и се основава на три основни принципа: надеждна

идентичност на устройството, поверителност на данните и цялост на софтуера, работещ на устройството. Те се изразяват в удостоверяване, криптиране и подписване на кода.

Но без механизъм за сигурно съхранение на криптографски ключове, цялата стратегия за сигурност за установяване на идентичността на устройството, гарантиране на поверителността на комуникацията и сигурно актуализиране на фърмуера от всяко място, остава с голяма празнота. Следователно за надеждно IoT решение трябва да се приложи така нареченият „корен на доверието“ („root of trust“). В новото поколение Ewon гейтуеи, като Cosy+, специален хардуерен чип, наречен Secure Element, отговаря за съхранението на поверителна информация по сигурен и немодифицируем начин, и за извършване на криптографски операции (генериране на случайни числа, криптиране, декриптиране, подписване и др.).

• **Сигурен процес на стартиране:** това е гаранцията, че при стартиране се зарежда само легитимен фърмуер, произведен от Ewon. Ако устройството открие проблем, то няма да стартира.

• **Подписване на код:** това е гаранцията, че на устройствата е инсталиран само легитимен фърмуер, произведен от Ewon.

• **Birth certificate:** това е гаранцията, че само легитимни устройства, произведени от Ewon, се свързват с Talk2m.

Ограничен достъп до целевото оборудване: Потребител, който се свързва дистанционно, има достъп само до целевите устройства, с които трябва да работи, като например PLC в машина. При никакви обстоятелства той няма достъп до друго оборудване в завода. Ewon гейтуеят, свързан с Talk2m, е конфигуриран да извършва разделяне между LAN страната, до която отдалеченият потребител има достъп, и WAN страната, често това е фабричната мрежа, чрез която Ewon гейтуеят е свързан с интернет, но до която отдалеченият потребител няма достъп.

Възможност за комуникация с фабрични системи: Ewon гейтуеите имат функция „NAT 1:1“, позволяваща на системата, намираща се от WAN страната на гейтуея (например фабричната мрежа), като SCADA или MES, да се свърже с устройства, намиращи се от LAN страната на гейтуея (машинната мрежа), като PLC. Функцията NAT 1:1 позволява да се асоциира IP адреса на LAN устройство с виртуален IP адрес, принадлежащ към подмрежата на WAN мрежата. Така LAN устройствата стават достъпни за фабричната система от WAN страната чрез техния виртуален IP адрес.

Възможно е вместо да се използва функция NAT 1:1, да се конфигурира Ewon „Flexy“ гейтуей да чете данни от LAN устройствата, посредством вградените си индустриални протоколи, и да публикува тези данни за фабричната система от WAN страната след преобразуването им в OPC UA.

Контрол на свързаността на Ewon гейтуей: С цел физически контрол на свързаността на място при машината е възможно да се сложи ключ, който да се използва от персонала в завода, за да активира или деактивира локално свързаността на Ewon гейтуея с Talk2m. Ewon гейтуеят може да се включва онлайн само когато е необходима

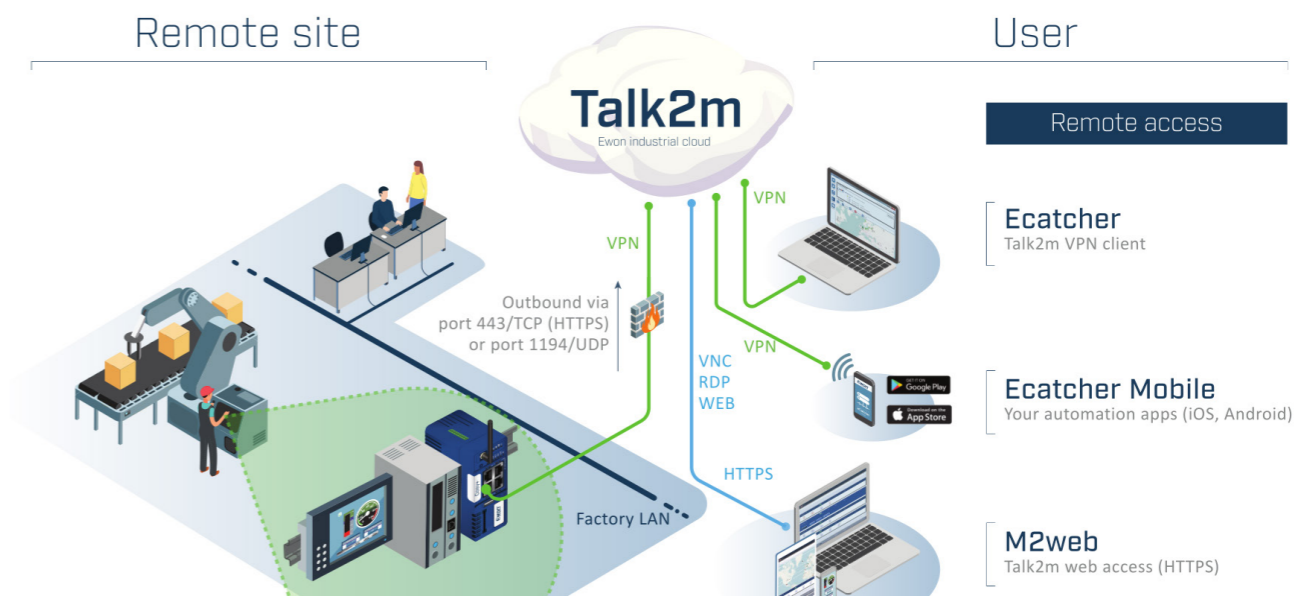
дистанционна поддръжка.

Вместо ключ може да се използва настройка на Ewon гейтуея за „triggered (задействана)“ връзка. Ewon гейтуеят ще остане офлайн и ще установи VPN връзка с Talk2m едва след като получи SMS съобщение за „събуждане“. Такъв SMS може да се изпрати от всеки мобилен телефон, като за получател се използва телефонният номер на SIM картата, инсталирана в Ewon гейтуея, или да се изпрати от Talk2m, използвайки Ecatcher.

Поддържане на устройствата и софтуера актуални:

За минимизиране на рисковете за сигурността е важно софтуерът на Ewon гейтуеите да се поддържа актуален. Ъпдейт може да се прави ръчно от потребителя, дори дистанционно чрез Talk2m VPN връзка. По-новите модели предлагат опцията за автоматична инсталация на нови версии на фърмуера - в пълната им версия или само на части, съдържащи файлове за сигурност.

Софтуерът Ecatcher също се актуализира редовно и е добре винаги да се използва най-новата версия. В eCatcher се показва съобщение за наличието на ъпдейт.



Допълнителни услуги на Talk2m

Мобилен приложение Ecatcher: За връзка с отдалеченото оборудване от смартфон или таблет е налично безплатното приложение „Ecatcher Mobile“, работещо в среда на Android и iOS.

M2web уеб портал на Ewon за отдалечено наблюдение: Потребителите могат да се свързват с оборудването си от всеки браузър, използвайки уеб портала на Talk2m „M2web“.

Ключови показатели за ефективност (KPI) в реално време, за мониторинг: Ewon Flexy гейтуеите могат да четат данни от PLC и друго оборудване за автоматизация и да съхраняват тези данни в тагове във вътрешна памет. За всеки Ewon Flexy гейтуей могат да бъдат дефинирани до 6 тага като KPI, чиито стойности в реално време ще станат видими за

потребителите, когато влязат в своя Talk2m акаунт от портала M2web или мобилното приложение eCatcher. Така може удобно от едно централно място да се следи състоянието и производителността на всички машини, оборудвани с Ewon Flexy гейтуеи.

Услуги за уведомяване: SMTP relay и SMS gateway сървъри са част от инфраструктурата на Talk2m и предоставят на потребителите лесен начин да получават имейл или SMS съобщения от оборудването си, въз основа на алармената система, налична в Ewon гейтуеите.

Talk2m API: Talk2m предоставя REST API, които позволяват на софтуер на трети страни лесно да събира данни от или да взаимодейства с отдалечени машини, оборудвани с Ewon гейтуеи. Това са:

- Услугата datamailbox (Dmweb API) за извличане на исторически данни от множество машини по лесен и надежден начин. Ewon гейтуеите могат да се конфигурират да изпращат редовно историческите записи на данните, които са събрали от машините, към Talk2m чрез VPN тунела си. Тези данни се съхраняват временно в сървърите на Talk2m datamailbox за максимален период от 10 дни, а IoT

софтуерът може да използва datamailbox API, за да извлича ефективно данните от всички Ewon гейтуеи, без загуба или дублиране, чрез HTTPS заявки към Talk2m акаунта на потребителя.

• M2web API: M2web API може да се използва от IoT софтуера за изпращане на заявки към уеб услугите на Ewon гейтуея, например за контрол или за да извлече информация на живо от отдалечената машина. Комуникацията между IoT софтуера и Talk2m се осъществява чрез HTTPS, докато комуникацията между Talk2m и Ewon гейтуея преминава през VPN тунел.

За повече информация:
<https://comicon.bg/bg/>