# PASSWORD SAFE

Cybersecurity for industry

Through digitalisation and Industry 4.0, people and machines work hand in hand. Intelligent and networked industrial plants offer companies a wide range of opportunities, but at the same time this creates new security risks. Cybercrime costs the global economy over one trillion US dollars. Hackers smuggle malware into networked systems and blackmail operators into paying high ransom demands by blocking systems. This leads to delays in the value chain, competitive disadvantages, reputational damage and high costs.
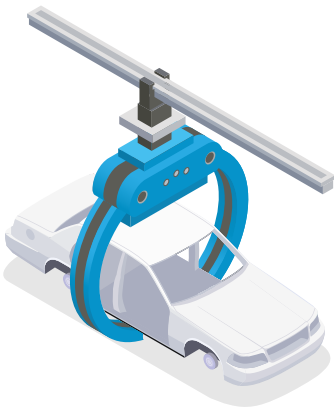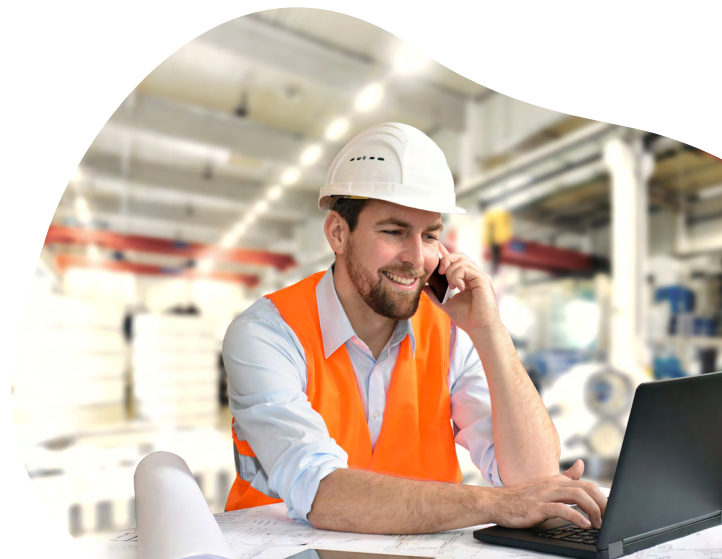
Companies need security concepts to counter increasing threat scenarios despite advancing digitalisation. Is your production already secured?

Increase your IT security now. Work with the market leader in password management right from the start - we have the expertise to secure your IT and production against cyberattacks!

Intelligent and secure solutions for industry

Password Safe supports you with a password management solution individually tailored to your company. No matter whether you are dealing with branched authorisation structures or central password management: Trust our extensive experience and long expertise in the IT security industry!

Password generator   ✕

Phonetic password   ▾

Syllables:

●—————————————————   3

Syllable separator:

Upper case letter   ▾

☐ Use LeetSpeak

Length:

●—————————————————————   12

Password preview:

ZejoMugaNume   Strong   🔒

                    Cancel   Apply

A secure lock for important data

Many employees still use passwords like „password123" to secure accounts. Passwords like these are like doors that are locked with adhesive tape. To minimise the risk of cyberattacks, business-critical data must be protected by strong encryption technologies. This is also stated in the international standard IEC62443 „IT Security for Industrial Control Systems - Network and System Protection".

Securely encrypted: With Password Safe, employees can create secure passwords at the click of a button. All data is transmitted in Password Safe using secure end-to-end encryption. The encryption takes place exclusively between the client and the server, so passwords remain secret and accesses secure.

Strong passwords, easy to use

In production, industrial machines are often used without an internet connection. Manual password transmission must also be protected and secured.

Security offline and online: With Password Safe, passwords are also available offline. To simplify password entry in difficult production environments, Password Safe has a typing aid. This enlarges individual characters and highlights them in colour. In addition, phonetic passwords can be generated with the password generator. These are easy to read and pronounce, but still meet the complexity requirements of secure passwords.
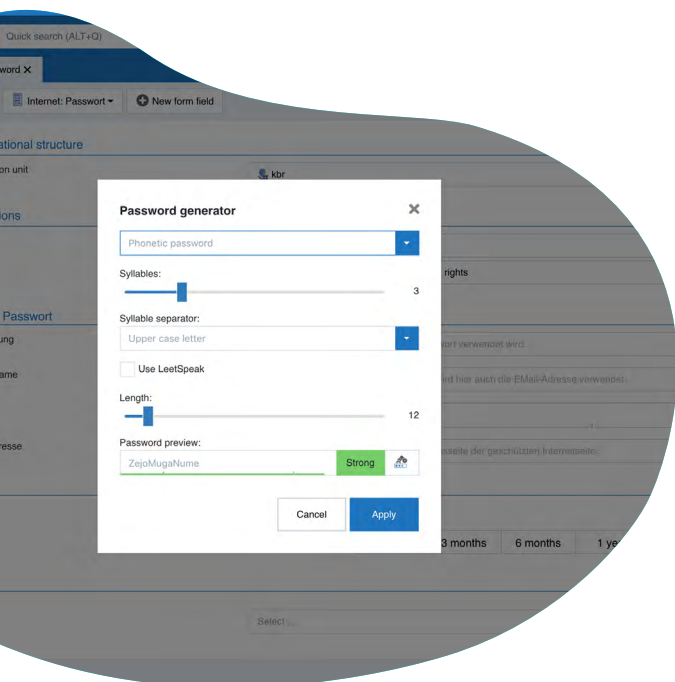
Security from A to Z

Cyberattacks bring entire production plants to a standstill. The criminals' goal: To integrate malware into industrial control elements, as these are often not holistically protected.

Security through absolute data sovereignty: Password Safe stores all information, passwords and accesses in encrypted form in the customer's environment. The data can be self-hosted either on the company's own servers, or in the private as well as private cloud. Customers can thus choose the right model depending on their security needs, and all data always remains 100% within the company. In addition, Password Safe is highly available: In the event of a server failure or other problems, all passwords and accesses can always be accessed offline.

Secure all systems - from the printer to the machine

Embedded devices (embedded systems) include industrial control components and network technologies. These are often set up by a pre-configured default password in the company and rarely changed. If these easily obtained passwords are not shared, cybercriminals can easily gain access to systems.

Secure passwords everywhere: With Password Safe, insecure passwords can be automatically and periodically replaced with highly complex ones. The storage of password guidelines by IT also increases security, because passwords such as „machine1" can thus no longer be created.

Remote maintenance - yes but secured

If a system is to be maintained or repaired remotely by external parties, the security risk for companies increases immensely. To keep this threat to a minimum, guidelines should be set up for enabling access. In addition, the VDI/VDE guideline 2182 requires that personalised accesses take place via role- or person-related authorisations.

Security through technology: With Password Safe, access data can be provided with an expiry date and users can only be authorised to it for a limited time. These authorisations are assigned on a role basis. Once the employee has been removed from the role, he or she can no longer access their passwords. For more security, it can also be preset that a new password is set after each login and that this is only used once in terms of OTP.

Caution is better than indulgence

For safety incidents, all actions should be logged for audits. It should be clear which employee was active when and on which machine. In addition, employees should only have access to passwords and accesses that are absolutely necessary for their work.

Maximum traceability for exceptional cases: In Password Safe, all actions are documented and can be traced and analysed afterwards in an audit-proof manner. In addition, authorisations to a password are assigned according to the minimum principle, so that employees only have access to the passwords that are necessary for their work. All actions in Password Safe are also DSGVO-compliant.

A holistic approach to security

An insecure password or a password written on a Post-it is enough to give hackers access to company secrets. In industry, too, it is important that employees can use and manage secure passwords across all devices, machines and applications.

With Password Safe, the management and secure handling of access data can be ensured regardless of the size of the company and the associated number of licences. Password Safe reduces the risk of cyberattacks through complex passwords and secured access. Invest in comprehensive password protection today and secure tomorrow's customers and competitive advantage.

Contact us today for advice on how Password Safe is the right solution for your business!

Warum Password Safe?

Experience

MATESO has focused on professional enterprise password management since **2006**. Over **21 of the top 40 DAX companies** and more than **10,000 users** already rely on Password Safe for password protection.

Comprehensive protection

With the influence of over **20 years of market experience**, the solution is holistically tailored to the individual security requirements and needs of companies. All passwords are protected holistically throughout the **password lifecycle** - from creation to archiving.

Made in Germany

As a member of the TeleTrust initiative „**IT-Security Made in Germany**", MATESO stands for trustworthy IT security solutions that meet the requirements of German data protection law, can be used in **compliance with the DSGVO** and do not contain any hidden accesses.

MATESO
PASSWORD SAFE