Password Safe and the German IT Baseline Protection “IT-Grundschutz Compendium” 2021

MATESO
PASSWORD SAFE

Whitepaper

Introduction

Digitization is advancing rapidly in Germany, confronting companies with new tasks, challenges and opportunities time and again. The most important question is always: How can companies protect their systems and data from external attacks? For this purpose, the German Federal Office for Information Security regularly provides the "IT-Grundschutz Compendium". It contains detailed methods, instructions and recommendations for protecting a company's own IT systems, data and processes in the best possible way.

Password Safe also helps to increase the IT security of companies and make the access to information in our digital world more secure. In this whitepaper, you will find out how Password Safe can help you implement the password recommendations of the "IT-Grundschutz" in the best possible way and increase your company's IT Security.

Federal Office for Information Security

> Information is an essential asset for companies and government agencies and must therefore be adequately protected.

*Please note that the 2021 version of the IT-Grundschutz was not available in English when this Whitepaper was published.

The most important features

Password Safe offers numerous features to make the handling of passwords and other information as secure as possible and to implement the recommendations of the IT-Grundschutz.

Role-based rights system	Each employee receives the access rights required for his or her role in an automated manner.
Temporary enabling	Access to certain passwords can be temporarily enabled and then revoked.
Privacy shield	Passwords can be stored with a privacy shield so that employees can use them but cannot see them. In this way, even shared passwords remain secret.
2-factor authentication	Using a token, a smart card or a biometric scanner, Password Safe enables particularly secure 2-factor authentication.
Identity Provider	Password Safe can provide the credentials to log in to other applications in an uncomplicated way.
Login without password	The user can use a token or smart card to log in to Password Safe without a password and from there log in to other applications.
Password generator	Password Safe has a built-in password generator that can create highly secure and complex passwords according to individual policies.
App & browser extension	For secure login on the go, Password Safe offers its own app and a browser extension.
Password reset	Passwords can be reset individually, triggered by a certain action or at regular intervals without any disadvantages for the user.
End-to-end encryption	Password Safe uses the most advanced encryption technologies and algorithms: • AES 256 • PBKDF2 with 100,000 iterations for the formation of user hashes • PBKDF2 with 1,000 iterations for hashes of passwords within the database • RSA 4096 for private and public key method
Seal & multi-eye principle	With a seal, a password cannot be used or viewed until the seal has been broken by one or more authorized persons.
Emergency backup	An offline client for Windows, a WebViewer for the browser and a 2FA-protected emergency WebViewer for administrators are available for emergencies.

Password-specific recommendations of the "IT-Grundschutz"

ORP.4: Identity and authorization management

2.1 Missing or insufficient processes for identity and authorization management

> „If identity and authorization management processes are inadequately defined or implemented, there is no guarantee that access is restricted to the necessary extent, thus violating the principles of need-to-know and least privilege. The administrator may not receive information about personnel changes, so that, for example, the user IDs of employees who have left the company are not deleted. They can thus continue to access restricted information."

Password Safe has a **role-based rights system**. This means that all employees receive the authorizations for access codes stored in Password Safe depending on their role. HR employees or department heads can be authorized to assign and revoke roles and the associated accesses. This reduces the burden on IT, distributes responsibilities more effectively, and gives users more scope to take active action themselves and protect access data.

> „It may also be possible for employees who have been transferred to a new department to retain their old authorizations, thereby accumulating extensive authorizations over time."

Thanks to the **role-based rights assignment** in Password Safe, rights within a department can be easily granted and also revoked. **Temporary enabling** of a password allows temporary employees such as working students, trainees or external service providers only limited access to the stored data.

If the necessary passwords are protected through a **privacy shield**, employees can use them to log in but cannot view them in plain text. This ensures that trainees, for example, only ever receive the authorizations they currently need, even when they pass through several departments.

2.2 Lack of central deactivation option for user accesses

„In institutions, employees often have user access to many IT systems, such as production, test, quality management or project systems. These are usually located in different areas of responsibility and are often managed by different administrators. This may mean that the same and unique user ID is not used on all IT systems, and there is also no central overview of user access on the individual IT systems.“

In Password Safe, all access data can be stored centrally and managed clearly. In addition, administrators can view all users as part of user management. This gives them a central overview of the users and their authorizations for individual access data.

„In case of an attack or password theft, it is not possible to disable all user accesses of an employee in one step. Also, in this scenario, when an employee leaves the institution, it is not possible to disable all accesses in one step.“

Role-based rights assignment means that user access is managed not depending on the person, but depending on their role. This role and the associated access can be revoked at any time by authorized persons as part of the rights management. In addition, visual protection can be used to prevent employees from viewing passwords without authorization. In the event of an emergency, any compromised passwords can be replaced automatically or manually using the **password reset** function.

ORP.4.A8 Regulation of password use [user, IT operation]

„The institution SHALL regulate password use in a binding manner (...).“

In Password Safe, the use of passwords including all necessary actions (creating, saving, sharing, logging in, archiving) is regulated.

„It SHOULD be considered whether passwords should be used as the sole authentication method, or whether other authentication features or methods may be used in addition to or instead of passwords.“

Through **2-factor authentication**, Password Safe offers the option of specifying at least one other factor in addition to the password, for example using a biometric scanner or a token. Additionally, Password Safe as an **identity provider** also enables login to applications **without a password**. The login for Password Safe itself can be done without a password or by combining a master password with a FIDO-2-compliant token or smart card.

„Passwords MUST NOT be used more than once. A separate password MUST be used for each IT system or application.“

Thanks to the **password generator** integrated in Password Safe, a separate complex password can be created and stored for each application. In addition, the user does not need to remember these passwords, as they are securely stored and easily retrievable in Password Safe.

„Passwords that are easy to guess or are kept in common password lists MUST NOT be used.“

The **password generator** systematically excludes words that are easy to guess as well as words that can be found in the dictionary. In addition, individual guidelines can be created to ensure the desired complexity of passwords. Password Safe can also evaluate the security of self-created passwords.

„Passwords MUST be kept secret. They MUST ONLY be known by the user.“

In Password Safe all passwords are stored securely and are visible only to the authorized person. The additional **privacy shield** option means that the password cannot be seen in plain text by others but can still be used for login or shared securely without knowing it.

„Passwords MUST ONLY be entered unobserved.“

With the help of Password Safe, the login is automatic: it is no longer necessary to type in the password, as the access data is passed on in a concealed way for login. This ensures unobserved login at all times.

„Passwords MUST NOT be stored on programmable function keys on keyboards or mice.“

The easy login via Password Safe makes it unnecessary to resort to such insecure makeshift solutions. All access data is stored centrally and securely.

„A password MUST be written down ONLY for deposit in case of an emergency. It MUST then be stored securely.“

With Password Safe, writing down passwords is a thing of the past – in an emergency, the **emergency WebViewer** can be used, which provides the passwords in an encrypted HTML file.

„The use of a password manager SHOULD be explored.“

Nowadays, a password manager is part of every comprehensive ISMS strategy and is indispensable for companies that want to protect their passwords and secrets. Password Safe is the market leader for password management in the German speaking region:

20 of 30
DAX companies

over 10.000
corporate customers
rely on us.

„For password managers with features or plug-ins that synchronize passwords via third-party online services or otherwise transmit passwords to third parties, those features and plug-ins MUST be disabled.“

Password Safe does not transmit passwords via third-party systems and offers its own secure **app** and **browser extension**.

„A password MUST be changed if it has become known to unauthorized persons or if it is suspected.“

The **password reset** to change a password can be done manually, time-based or event-based in Password Safe. Since companies often do not know when unauthorized persons have had access to a password, it is advisable to change passwords regularly and automatically in order to deliberately exclude potential attackers. Thanks to Password Safe, there is no additional effort for the user and all changes are logged in an audit-proof manner.

ORP.4.A22 Password Quality Regulation [IT Operations]

„Depending on the intended use and protection needs, secure passwords of appropriate quality MUST be selected.“

Password Safe‘s built-in **password generator** can create phonetic, user-defined or policy-based passwords. Depending on the intended use and protection requirements, higher password requirements can be added.

„The password MUST be complex enough that it cannot be easily guessed. The password SHALL NOT be too complex for the user to be able to use the password regularly with reasonable effort.“

With the help of Password Safe, the user no longer needs to remember passwords and can therefore use highly secure and complex passwords. The complexity of the passwords can be defined in terms of minimum length, upper and lower case letters, numbers, special characters and easily confused characters. „Readable“ passwords can be put out as „phonetic password“.

ORP.4.A23 Regulation for password-processing applications and IT systems [IT operations].

„IT systems or applications SHOULD ONLY prompt for password change with a valid reason. Purely interval-based changes SHOULD be avoided. Measures SHALL be taken to detect password compromise. If this is not possible, consideration SHOULD be given to accepting the disadvantages of interval-based password changes.“

Where Password Safe is in use, secure scheduled password resets offers no disadvantages. The end user is freed from manual password reset and does not have to remember passwords. In this way, the security in the company can be increased.

„Default passwords MUST be replaced with sufficiently strong passwords and predefined identifiers MUST be changed.“

Password Safe detects new as well as insecure passwords that do not comply with internal policies and creates a secure value using the **password generator**.

„It SHOULD be ensured that the possible password length is also checked to the full extent by processing IT systems.“

Password Safe evaluates the quality of the stored passwords. In addition, minimum password length requirements can be created in Password Safe to exclude passwords that fall short of these criteria.

„After a password change, old passwords MUST NOT be used.“

Password Safe can replace old, insecure passwords with new, automatically created passwords using the **password generator**. Due to the complexity of the values created by the generator, it is virtually impossible to use an old password more than once.

„Passwords MUST be stored as securely as possible.“

Password Safe offers the highest possible protection thanks to modern **end-to-end encryption**.

„For identifiers for technical users, service accounts, interfaces, or the like, password changes SHOULD be carefully planned and, if necessary, coordinated with application owners.“

With Password Safe, changing passwords is straightforward and does not require any additional effort on the part of the user. Therefore, long-term planning for **password resets** is not necessary. Nevertheless, the password change can also be set and coordinated individually.

„When authenticating in networked systems, passwords SHOULD NOT be transmitted unencrypted via insecure networks. When passwords are transmitted via intranet, they SHOULD be encrypted.“

Password Safe offers modern **end-to-end encryption** and thus meets the highest security requirements.

„For unsuccessful login attempts, the system SHOULD not give any indication if the password or user ID is incorrect.“

If the login to Password Safe itself is unsuccessful, no indication of incorrectly entered credentials is given.

ORP.4.A11 Password Reset [IT operations]

„An appropriate secure procedure SHOULD be defined and implemented for resetting passwords. Support staff who can reset passwords SHOULD be trained accordingly. For higher password protection needs, a policy SHOULD be defined in case a support staff member cannot take responsibility due to lack of secure means of transmitting the password.“

The **password reset** in Password Safe allows resetting passwords to a new and unknown value according to freely definable triggers. Such a trigger can be either a definable interval or a specific action of the user, such as login or changing the password. To reset passwords, appropriate rights are required. The password reset is documented as an action in the logbook and can thus be traced.

ORP.4.A24 Four-eyes principle for administrative activities [IT operations]

„Administrative activities SHOULD only be able to be performed by two people. For this purpose, in case of multi-factor authentication, the factors SHOULD be distributed among the two persons. When passwords are used, they SHOULD be split into two parts and each of the two people enters one part.“

Password Safe offers the **multi-eye principle** through the **seal** function: enabling a password must first be requested and approved by the required persons. In addition, the user can request a reason for the action, which is logged in the history. Particularly security-critical actions are secured through live notifications to the responsible persons.

CON.8.A5 Secure system design

„If passwords are stored for authentication, they MUST be stored using a secure hash method."

Password Safe offers PBKDF2 as a hashing method with 1,000 integrations and 100,000 for the user password hash.

OPS.1.1.2.A2 Substitution arrangements and emergency procedures

„It SHALL be ensured that designated representatives can access the IT systems to be managed. Emergency users with administrative rights SHOULD be established for emergencies."

With the help of **role-based rights assignment**, employees can easily be authorized to access IT systems in an emergency. An **offline client** for Windows, a **WebViewer** for the browser, and a 2FA-protected **emergency WebViewer** for administrators are available for emergencies.

OPS.1.1.2.A4 Termination of employment as IT administrator [Human Resources Department]

„When administrators are relieved of their duties again, all personal administration IDs assigned to them SHALL be locked. In addition, it SHALL be checked which passwords are known by the departing employees. Such passwords MUST be changed."

Role-based access control means that rights can be revoked immediately when employees change. It is documented which passwords the user had access to. These can be reset to a new value. In addition, Password Safe works on the minimal principle, so the user only knows as many passwords as necessary. These can be additionally secured by the visual protection.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE