epas

Enterprise Password Analytics Solution

Achieve compliance with “BSI IT-Grundschutz ORP 4: Identity and access management” with the help of EPAS

The German Federal Office for Information Security (“BSI”) has favored regular password change in its “Guide to basic protection based on IT-Grundschutz ” until 2020. This aspect is no longer available in the new edition, published in February 2020. In this edition BSI wrote that a password must be changed at latest in the event of suspected misuse in accordance with BSI guidelines. Alternative and secure passwords should be used for different logins and these must be changed if there is a suspicion of compromise of the corresponding account or password.

Since 2013, Detack GmbH has been offering a software solution based on its own hardware, which is installed in the customer‘s data center and it is operated by the customers‘ IT department in a secure environment. The solution works also without an internet connection. EPAS is made up of two components: EPAS Audit and EPAS Enforcer.

EPAS Audit analyzes the password quality, as promoted in the above-mentioned BSI Guide by simulating a real attack without ever disclosing or storing the passwords and without compromising the availability of the target system. EPAS provides effective quality assurance for password-based authentication using a Europe-wide and North America patented technology.

EPAS Audit extracts all password-relevant data from the target system and then uses it to assess password resilience to attacks. To protect the test objects, EPAS uses only the interfaces provided by the manufacturer for the extraction of encrypted data. This does not pose any risk to the system stability of the selected target systems.

EPAS Enforcer is a password quality improvement module that systematically prevents the use of weak, reused or shared passwords every time passwords are changed. The EPAS Enforcer checks whether the security of the newly selected password meets a centralized policy and security requirements for newly set passwords and password changes. For the end user, this means that previously allowed passwords such as “Password123” or “Secret!” are no longer accepted.

This document contains how EPAS (Audit and Enforcer) supports an organization to be in compliance with the new “Basic Protection ORP 4: Identity and Access Management” from the point of view of password security. The supporting functions of EPAS are also explained for the regulations concerned.

“ORP.4. A8 Password Usage Control [User, IT Operation] (B)”[1]

“The institution MUST regulate the use of passwords conform with the new laws (see also ORP.4. A22 regulation on password quality and ORP.4.A23 regulation for password processing applications and IT systems).”[1]

✓ Passwords are the most commonly used authentication method. EPAS Audit proves that the quality level of the passwords currently in use meets the authentication requirements of relevant security policies and standards.

“It must be checked whether passwords should be used as the sole authentication method, or whether other authentication features or procedures can be used in addition to or instead of passwords.[1]

Passwords MUST NOT be used multiple times.”[1]

“A stand-alone password MUST be used for each IT system or application.”[1]

✓ EPAS Audit technology is used to identify both weak passwords (too short, too easy, etc.) and passwords are used multiple times by a person or by multiple persons, on the same system or across multiple ones. EPAS Enforcer prevents both weak passwords and passwords shared by multiple accounts.

“Passwords that are easy to guess or are listed in shared password lists, MUST NOT be used.”[1]

✓ EPAS Audit identifies passwords that are already compromised or blacklisted (including all known leaked passwords) as well any easy to guess used passwords. EPAS Enforcer has configurable policies, one rule being the blacklisting of leaked passwords.

“Passwords MUST be kept secret. They SHOULD ONLY be personally known by the user. Passwords SHOULD ONLY be entered unobserved. Passwords MUST NOT be stored on programmable function keys of keyboards or mouse. A password IS ALLOWED ONLY to be fixed in writing for an emergency situation. It MUST then be stored safely. The use of a password manager SHOULD be checked.

A password MUST be changed if it has become known to unauthorized persons or something like this is suspected.”[1]

[1] BSI – IT-Grundschutz Kompendium 2020 ORP.4 Identitäts- und Berechtigungsmanagement: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

EPAS analyzes password quality by simulating a real attack without ever disclosing or storing the passwords, and without compromising the availability of the target system. EPAS provides effective quality assurance for password-based authentication. Consequently, the regulations of ORP.4. A22 are almost completely covered by the functions of EPAS with minimal need for additional measures or technologies.

"ORP.4.A22 Password Quality Control [IT Operation] (B)"[1]

"Depending on the purpose and protection needs, secure passwords with a suitable quality level MUST be chosen.
The password MUST be so complex that it is not easy to guess.
The password MUST NOT be too complicated, the user must be able to use the password regularly with reasonable effort."[1]

EPAS analyzes password quality by simulating a real attack without ever disclosing or storing the passwords, and without compromising the availability of the target system. EPAS provides effective quality assurance for password-based authentication. Consequently, the regulations of ORP.4. A22 are almost completely covered by the functions of EPAS with minimal need for additional measures or technologies.

"ORP.4. A23 Control for password processing applications and IT systems [IT operation] (B)"[1]

"IT systems or applications SHOULD ONLY ask the user to change the password with a valid reason. Pure time-controlled changes should be avoided."[1]

EPAS Audit includes existing as well as regular updates of the contents of password leaks. If a password is already compromised, a password change can be enforced. EPAS Enforcer eliminates the need for a user to update the password regularly. Whenever a password change occurs, the already compromised passwords can be blacklisted.

"Measures MUST be taken to detect the compromise of passwords."[1]

EPAS Audit identifies passwords that are already compromised or blacklisted (including all known leaked passwords) as well any easy to guess used passwords. EPAS Enforcer has configurable policies, one rule being the blacklisting of leaked passwords.

EPAS Audit and EPAS Enforcer are equipped with dictionaries in multiple languages that contain the most used passwords and all publicly available exposed credentials. EPAS Audit uses these dictionaries to determine whether a password matches a dictionary entry or is similar with a dictionary entry. EPAS Enforcer uses these dictionaries to implement policies that prevent users from selecting passwords contained in dictionaries.

EPAS also includes a function that allows the recognition of passwords which are based on context-specific words (e.g. derivatives of).

"If this is not possible, it should be checked whether the disadvantages of a timed password change can be accepted, and passwords should be changed at certain intervals.

Standard passwords MUST be replaced with sufficiently strong passwords and predefined identifiers MUST be changed."[1]

EPAS Audit determines whether initial passwords are still in use, whether they are shared by multiple users, and when such passwords have been changed.

"ORP.4.M 8 Control of password use"[2]

"Basically, it is necessary to consider whether passwords should be used as the singular authentication method or whether other authentication methods or additional authentication features can be used instead of passwords, such as certificates or multi-factor authentication.

In order to create and manage passwords, there must be fixed rules. Users of IT systems must be instructed in this regard. This is how an organization has to prevent using weak passwords and mishandling of them."[2]

[2] BSI IT-Grundschutz „Umsetzungshinweise zum Baustein ORP.4: Identitäts- und Berechtigungsmanagement":
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2020/Umsetzungshinweise_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=3#download=1

EPAS Audit helps organizations through addressing the human-side risks by measuring user awareness and training based on password verification reports. The history of password check results allows measuring training effectiveness and intensifying information and training for "risky" users. Regardless of the auditing feature, EPAS provides a separate interface for voluntary password quality assessment, which is typically used by users to verify passwords before they are used. This interface is also used in awareness training.

Additionally, EPAS Enforcer provides direct feedback on password strength when changing passwords, increasing understanding of how to design a secure password. In EPAS Audit and Enforcer, different security classes with defined guidelines can be set up. Stricter rules can be defined, e.g. for mobile/teleworking regulations, for credentials quality to match the risk level of each user category.

"A password must be changed if it has become known to unauthorized persons or something like this is suspected."[2]

EPAS Audit provides instant insight into the security-related activities of accounts, such as last password change, last login, lockout status, and permissions information. This data helps to identify and remove unused accounts that are still enabled and often have sensitive permissions.

EPAS Audit identifies passwords that are already compromised or blacklisted (including all known leaked passwords) as well as any predictable passwords.

"The reuse of already used passwords should be prevented. Where appropriate, rules may be adopted that passwords may be reused after a reasonable period of time.
Pre-set passwords and identifiers, e.g. of the manufacturer when delivery of IT systems, must be replaced by individual passwords and, if possible, by identifiers.
Strength of the used factors (for the knowledge factor, see also ORP.4.M22 password quality control)."[2]

EPAS analyzes password quality by simulating a real attack without ever disclosing or storing the passwords, and without compromising the availability of the target system. EPAS provides effective quality assurance for password-based authentication.

“ORP.4.M22 Password Quality Control”[2]

“If passwords are used for authentication in an IT system or application, it is necessary to ensure that secure passwords are used. The password requirements must be designed in such a way that it represents a workable compromise between complexity and usability with reasonable effort. The number of possible passwords of an authentication proceed must be so large that a password cannot be determined in a short time by simply trying it out. The following rules on password design and use must therefore be applied.”[2]

✓ User registration in an institution involves creating an account and assigning an initial password that needs to be changed as soon as possible. EPAS Audit determines whether initial passwords are still in use, whether they are shared by users with help from multiple files, and when such passwords have been changed. EPAS Audit data can be used to correlate the registration/deregistration of accounts with the actual identities in the user repository.

“A password must not be easy to guess, so it must not contain information from the user’s personal or professional environment, such as name, license plate number or date of birth.”[2]

✓ EPAS Audit and EPAS Enforcer are equipped with dictionaries in multiple languages that contain the most commonly used passwords and all available previous violations. EPAS Audit uses these dictionaries to determine whether a password matches a dictionary entry or is similar to a dictionary entry. EPAS Enforcer uses these dictionaries to implement policies that prevent users from selecting passwords contained in dictionaries.

EPAS also includes a function which allows the recognition of passwords based on context-specific words (e.g. derivatives of). EPAS can use „machine learning“ to understand the user‘s behavior and prevent them from using passwords associated with the user‘s public information or related to their historical passwords.

“Passwords must not be used multiple times, but a stand-alone password must be used for each IT system or application.”[2]

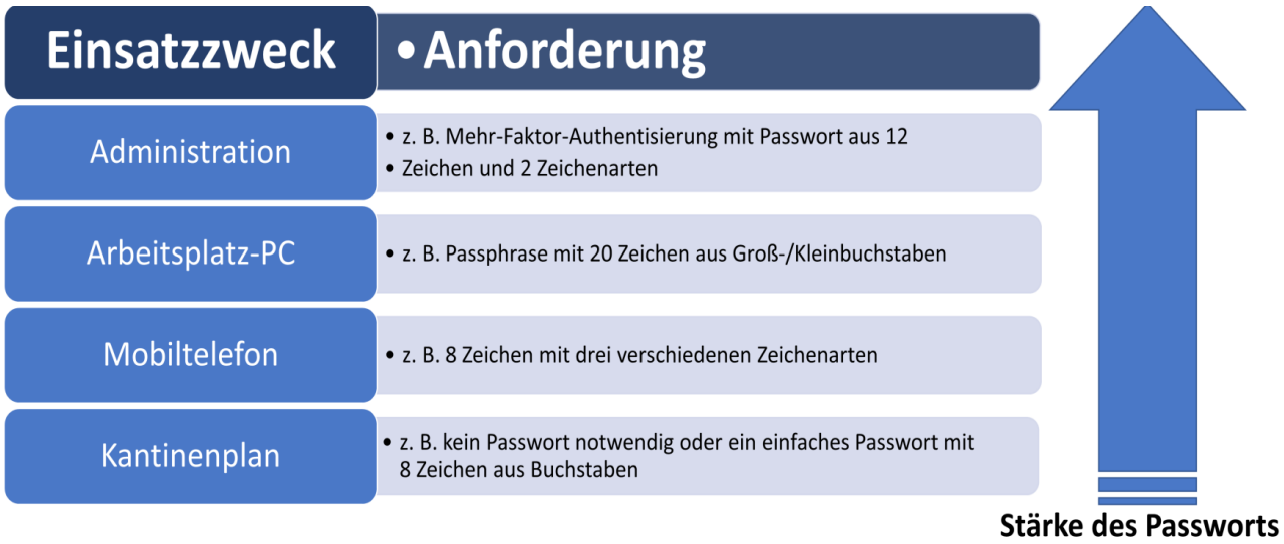
✓ EPAS Audit technology is used to identify both weak passwords (too short, too easy, etc.) and passwords are used multiple times by a person or by multiple persons, on the same system or across multiple ones. EPAS Enforcer prevents both weak passwords and passwords shared by multiple accounts, across one or multiple systems.

“To create a good password, the user should be aware of the password´s length and of number of character and also types, such as uppercase letters, lowercase letters, special characters and numbers. All this must be chosen in a reasonable combination and depending on the method used:

• e.g. 20 -25 characters in length and two used character types (less complex, longer password or passphrase)

• e.g. 8-12 characters in length and four types of characters used (complex, smaller length of password)

• e.g. for multi-factor authentication 8 characters length and three used character types
The purpose of passwords affects the security requirements of passwords, see the following figure:



Passwords used in multi-factor authentication can be less complex than if they are the individual security factor.”[2]

EPAS Enforcer is an EPAS password quality enrichment module that systematically prevents the use of weak, reused or shared passwords with each password change. EPAS Enforcer checks whether the security of the newly selected password meets a centralized policy and security requirements for newly set passwords and password changes.
If the password change is not successful, EPAS Enforcer allows users to be informed of the reasons for failed password changes (e.g.: „The password is not strong/long enough for the workstation PC guidelines“/ or „The password must not be included in a dictionary.“ The security requirements for each password are based on customer-specific and group-specific security requirements, as well as on the risk category of the data accessible by the account using the password.

“ORP.4.M23 Control for password processing applications and IT systems”[2]

“Password-processing applications and IT systems must, if technically possible, comply with the following boundary conditions:
The choice of trivial passwords and common strings, such as “123456”, “password”, names, dates of birth, and keyboard patterns such as “asdf”, must be avoided. This can be prevented, for example, by checking passwords against lists of trivial passwords or lists of publicly known passwords.”[2]

EPAS Audit analyzes password quality by simulating a real attack without ever disclosing or storing the passwords, and without compromising the availability of the target system. EPAS provides effective quality assurance for password-based authentication.
For newly set passwords and password changes, EPAS Enforcer checks whether the security of the newly selected password meets a centralized policy and security requirements. For the end user, this means that previously allowed passwords such as “Password123” or “Secret!” are no longer accepted.

“Users should be supported in changing a password by providing password goodness instructions that meet these requirements.”[2]

For newly set passwords and password changes, EPAS Enforcer checks whether the security of the newly selected password meets a centralized policy and security requirements.

“Only software should be used that actually uses all user input for the password. If there is a maximum number of characters, the user should be made aware of this.”[2]

If the password change is not successful, EPAS Enforcer allows users to be informed of the reasons for failed password changes (e.g.: „The password is not strong/long enough for the workstation PC guidelines“/ or „The password must not be included in a dictionary.“ The security requirements for each password are based on customer-specific and group-specific security requirements, as well as on the risk category of the data accessible by the account using the password.

“IT systems or applications should only ask users to change passwords for a valid reason, pure timed switching is not recommended.”[2]

EPAS Audit includes existing as well as regular updates of the contents of password leaks. If a password is already compromised, a password change can be enforced. EPAS Enforcer eliminates the need for a user to update the password regularly. Whenever a password change occurs, the already compromised passwords can be blacklisted.

"Measures must be taken to detect password compromise, e.g. parallel logins from different systems or locations, accumulation of incorrect entries, etc. If sufficient measures are not possible to detect password compromise, it is necessary to consider whether the disadvantages of, a timed password change can be accepted in this case and whether passwords should be changed at certain intervals, e.g. every 6 months."[2]

The EPAS Audit includes regularly updated compromised/leaked passwords that occur due to known security incidents. These are also updated regularly. This data is used by the audit process to determine whether any of the accounts are using disclosed/compromised information/passwords. These accounts are immediately marked for remediation.

"The passwords must not be stored in plain text in the IT system, they should be protected, for example, by means of a secure one-way function (hash functions with Salt and possibly Pepper)."[2]

EPAS detects and reports plain text passwords, passwords with reversible encryption, and passwords stored with weak/insecure hashing algorithms. Metrics, about all password algorithms used by an identity, can be found in the report.

"The IT system must prevent the repetition of old passwords when changing passwords (password history)."[2]

EPAS Enforcer can completely block the repetition of old passwords, with a configurable number of historical passwords compared, whenever passwords are changed.

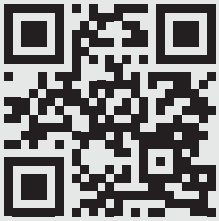
“Passwords for services or technical users, most of which are stored in configuration files on a system, must be stored as securely as possible. For example, configuration files can be secured by access rights. Initial passwords should be assigned for the first time of new users, which must be changed after a single use. For the first login, an individual password must be used for each new user and this must be changed after the single use.”[2]

EPAS Audit can define stricter classes of password strength for privileged accounts. Automatic notifications of violations and continuous metrics are used to improve the authentication security of privileged accounts.
EPAS Enforcer defines stricter policies to enforce for privileged accounts. EPAS components - Audit and Enforcer - are either used independently or to complement PAM (Privileged Access Management) solutions.

EPAS reports contain detailed information about group and organizational unit membership, including mixed groups. This allows the organization to quickly identify sensitive user rights along with password security metrics for all accounts, including technical and hard-to-identify accounts.

EPAS reports provide instant insight into account security-related activities, such as last password change, last login, lock out status, and permissions information. This data helps to detect and remove unused accounts that are still enabled and often have sensitive permissions.

User registration in an institution involves creating an account and assigning an initial password that needs to be changed as soon as possible. EPAS Audit determines whether initial passwords are still in use, whether they are shared by users with multiple files, and when such passwords have been changed. EPAS Audit data can be used to correlate the registration/deregistration of accounts with the actual identities in the user repository.



DETACK GmbH
Königsallee 43
71638 Ludwigsburg, Germany
Phone: +49 7141 69 62 65 0
Fax: +49 7141 69 62 65 5
info@detack.de
www.epas.de

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig