epas

Enterprise Password Analytics Solution

EPAS for Compliance: NIST password guildeines

The NIST authentication standard

The National Institute of Standards and Technology (NIST) is one of the authorities which sets the best practices on how to secure identities and authentication of users. The updated version of NIST Special Publication 800-63 "Digital Identity Guidelines" was released in June 2017 and updated in March 2020. Various companies and organizations use NIST guidelines to establish their security practices, while US federal agencies are required to comply with NIST 800-63.

"The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions."[1]

Why is a standard like NIST useful for an organisation? Following the guidelines will not only assure compliance, but it will also prove that an organization is implementing realistic and appropriate measures to support security controls. "Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to be traceable back to a specific real-life subject. In other words, accessing a digital service may not mean that the underlying subject's real-life representation is known. Identity proofing establishes that a subject is actually who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as the one who accessed the service previously. Digital identity presents a technical challenge because it often involves the proofing of individuals over an open network and always involves the authentication of individuals over an open network. This presents multiple opportunities for impersonation and other attacks which can lead to fraudulent claims of a subject's digital identity. NIST Special Publication 800-63 provides recommendations on types of authentication processes, including choices of authenticators, that may be used at various Authenticator Assurance Levels. It also provides recommendations on the lifecycle of authenticators, including revocation in the event of loss or theft."[2]

1 Grassi, Paul, Garcia, Michael, Fenton & James. (2020, March 2). Digital Identity Guidelines. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-63/3/final

2 NIST Special Publication 800-63B. (n.d.). Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

How to achieve NIST compliance with EPAS

These guidelines follow the recommendations set out in the NIST Special Publication 800-63B. The following requirements notation and conventions are part of the aforementioned document.

We set out here a list of NIST recommendations that EPAS can help implement along with a short description of the EPAS capability, together with the recommendation it covers, as well as a short explanation. A table summarizing the NIST recommendations covered is provided at the end.

This document is intended as guidance for companies and organizations aiming to achieve compliance with NIST recommendations with the help of EPAS.

5.1.1 Memorized Secrets

"A Memorized Secret authenticator — commonly referred to as a password or, if numeric, a PIN — is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is something you know."[2]

EPAS Audit will detect the usage of memorized secrets which are not complex enough and EPAS Enforcer will force users to use memorized secrets (passwords) with a strength and complexity level sufficient for the given user category.

5.1.1.1 Memorized Secret Authenticators

"Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed."[2]

EPAS Audit identifies any already compromised or blacklisted passwords, as well as any short passwords in use. EPAS Enforcer allows blacklisting any compromised passwords and permits setting minimum password length requirements.

5.1.1.2 Memorized Secret Verifiers

"Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well."[2]

EPAS Audit detects if any of the already existing passwords are shorter than 8 characters. EPAS Enforcer forces users to choose passwords based on a minimum length policy.

"If Unicode characters are accepted in memorized secrets, the verifier SHOULD apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization. This process is applied before hashing the byte string representing the memorized secret."[2]

EPAS Audit and EPAS Enforcer support Unicode character encoding and all the normalization process used by the connected targets.

"Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets."[2]

EPAS Audit parses all data present in the identity store (e.g. comments, descriptions), accessible to authenticated and unauthenticated clients and uses this information to detect if any part of it is used by any user as password; this includes hints and expected hint replies.

"When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. The list MAY include, but is not limited to:

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

If the chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret, SHALL provide the reason for rejection, and SHALL require the subscriber to choose a different value."[2]

EPAS Audit and EPAS Enforcer are equipped with dictionaries in multiple languages that contain the most commonly used passwords, as well as all available previous breach corpuses. EPAS Audit leverages said dictionaries for detecting if any password corresponds to a dictionary entry or is similar to a dictionary entry. EPAS Enforcer uses said dictionaries to implement policies preventing users from choosing passwords found in dictionaries.

EPAS also includes derivation engines which enable the detection of passwords which are based on (i.e. derivatives of) context-specific words.

EPAS is able to understand the behavior of the user, preventing them from using passwords that are linked to user public information present in the identity store (e.g. comments, descriptions) or related to its historical passwords. EPAS Enforcer can also allow the creation of strong policies that among the others features will not allow to use consecutive characters or digits, already exposed passwords, etc.

"Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blacklists]."[2]

EPAS Audit provides a feature to allow users to check their new passwords against the EPAS policies. Each password is given a numeric score as recommended, and passwords present in blacklists are flagged.
EPAS Enforcer gives a numeric score of the chosen password, calculated analysing the password from a mathematical and logical perspective. With an explicit message, Enforcer will guide the user in choosing a strong password without negatively impacting the user experience.

"Verifiers SHOULD permit claimants to use "paste" functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."[2]

Allowed in EPAS Enforcer.

"Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."[2]

EPAS Enforcer allows the use of flexible and customizable policies, based on each organization's security requirements. Granular policies for groups or organizational units can be set as well. By default, the delivered policies are following the NIST recommendations.

"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."[2]

EPAS Audit includes regular updates of password breaches contents. If a password is identified to be already compromised, a password change can be forced. EPAS Enforcer makes superfluous the periodic update of the password by a user. Whenever a password change takes place, the already compromised passwords can be blacklisted.

"In order to assist the claimant in successfully entering a memorized secret, the verifier SHOULD offer an option to display the secret — rather than a series of dots or asterisks — until it is entered. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed."[2]

The EPAS Audit voluntary password checking feature API can be configured to either hide (default option) or display the entered password.

"Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive."[2]

EPAS Audit identifies and reports any passwords stored with weak hashes, with no salts, and passwords vulnerable to offline attacks. The actual speed of offline attacks against all audited algorithms is reported as well, allowing the definition of policies to prevent such attacks. The combination of EPAS Audit (that identifies weak passwords and the correct remediation methods) and EPAS Enforcer (the prevents the usage of weak, reusable passwords) makes it infeasible for an attacker to recover passwords offline.

NIST requirements checklist

NIST Section	Description	EPAS Coverage
5.1.1	Password secrecy and complexity	✓
5.1.1.1	Minimum length for authenticator	✓
5.1.1.2	Minimum and maximum length for verifiers	✓
5.1.1.2	Normalization of Unicode chars	✓
5.1.1.2	No hints storage	✓
5.1.1.2	Help in choosing safe passwords	✓
5.1.1.2	Password-meter evaluation	✓
5.1.1.2	Paste functionality	✓
5.1.1.2	Enforcing of flexible policies	✓
5.1.1.2	No need to change passwords frequently	✓
5.1.1.2	Password displaying	✓
5.1.1.2	Secure storage	✓

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