Authlogics Password Security Management

Don’t let an Internet password breach affect your security

Password Security Management is a comprehensive real-time solution to ensure that user passwords comply with regulations and that they have not already been compromised online.

The Password Legacy

Passwords have long been the foundation for user authentication, yet passwords are not a solid security mechanism. A breach can render all other security controls useless, leaving company data and systems exposed.

Within most organisations, the user’s Active Directory password is the key to the front door and is used to access many systems, including internal documents and data stored in the Cloud. That makes it the most important password to protect and the most attractive for hackers to target.

To ensure adequate password-based security, administrators have traditionally applied various Windows complexity restrictions such as forcing minimum length, use of special characters and enforced changes every x number of days. These complexity settings have not only frustrated users for years but have increasingly been found to be unsecure.

What makes a password secure?

A ‘secure’ password is one that is both secret and not easy to guess. However, “P@ssw0rd” would appear to meet all the typical guidelines for password complexity; as a result, it is commonly used and therefore easily guessed.

There are other common techniques users use to get around complexity rules, e.g. adding a number at the end of their password to match the current month. This makes it easier to remember, meets the policy requirement of a password change every 30 days, but adds no actual security value.

Worst of all, users often share passwords across multiple unrelated websites. A breach on one compromised website is a common way that criminals gain access to online information such as documents and information stored in the Cloud or VPN’s.

Fortunately, the new Digital Identity Guidelines (Special Publication 800-63B) from the U.S. National Institute of Standards and Technology provides new best practice on how we can replace outdated password policies. These guidelines state that we no longer need complicated policy rules, and that frequent password changes are no longer required.

Instead, passwords should have a minimum length, and most importantly should be checked against a comprehensive database of previously known compromised passwords. This greatly reduces the likelihood that bad actors can use password breach data from an unrelated website or organisation to gain access to your organisation.

With the introduction of new hard-hitting data protection and legislative governance controls, such as EU General Data Protection Regulation (GDPR), companies now have to ensure that their systems are ‘secure by design’ and ‘secure by default’. Unfortunately, these regulations are vague in that although they require that companies are ‘secure’ they don’t define in detail what ‘secure’ means.

Furthermore, the legislation stipulates that single point in time compliance is not adequate. Any controls introduced must, therefore, have the ability to be continuously monitored to prove that compliance is on-going. For these reasons, Data Protection Officers charged with ensuring their organisations are compliant need to resort to best practice standards, e.g. NIST SP 800-63B, and employ modern authentication products and processes.

Features and highlights

- Analyse the risk posed by publicly available breach data
- Credential audit and reporting for Active Directory including breaches and public website sharing weaknesses
- Organisation and user level risk rating
- Real-time and retrospective scanning
- Protection from breached and shared passwords
- User self-service AD password reset via OTP with policy compliance UI.
- Continuously updated database of over 4 billion breached credentials and 1.2 billion clear text passwords
- Simplified password policy and reduced helpdesk costs
- Comply with NIST SP 800-63B, NCSC, CMMC, GDPR and other digital identity guidelines
- No desktop software required

Authlogics

Authlogics Password Security Management

Simplified passwords management across the entire enterprise

Achieve NIST SP 800-63B compliance by combining a modern password policy engine and our Password Breach Database containing over 4 billion breached credentials.

Password Security Management

Authlogics Password Security Management (PSM) has been designed to assess existing password related weaknesses, report on the current threats and risks, automatically remediate the problem and provide ongoing real-time protection and alerting from new password breaches.

It allows for a simpler password policy which reduces regular changes, lockouts and helpdesk calls for password-related problems. Users can reset their password via a One Time Pin (OTP) themselves to further reduce the helpdesk burden.

When installed with Active Directory, PSM immediately intercepts and analyses password changes as they happen, no matter where they originate from, ensuring compatibility with 3rd party IAM solutions and helpdesk management software.

There is no need to install extra software onto workstations, PSM is centrally managed and has a small footprint. All password change attempts, both accepted and declined, are logged centrally for auditing and reporting purposes.

Password Breach Database

Ensuring that compromised usernames and passwords from an unrelated security breach are not used to gain access to corporate systems is a crucial part of meeting the NIST password guidelines. Our Cloud-based Password Breach Database consists of over 4 billion breached credentials, including over 1.2 billion compromised clear text passwords, and is continually updated.

Customer privacy is important to us; hence, database lookups use *k*-anonymity technology to ensure that passwords and hashes do not leave the corporate network when checks are being done.

Password Security Portal

The Authlogics Password Security Portal proves an insightful view of the public breach data relevant to your organisation constructed using AI and BI logic from multiple data breach sources.

This allows you to view both organisation and user risk levels over time, as well as who may be sharing their corporate password on other websites.

Email notifications about newly discovered breaches relevant to your company can also be sent.

Finding weak passwords

Many corporate Active Directory databases have been in existence for decades and may contain very old and well-known passwords.

Password Security Manager can perform a detailed audit of the existing AD data and provide a detailed per-user report including accounts with breached and shared passwords within and outside of the network.

Fixing the problem

Password Security Management is able to automatically raise alerts and remediate Active Directory user accounts which have breached or shared passwords by either forcing them to be changed at next logon or by disabling the account.

When a new password is created, PSM uses a combination of a rules engine, custom blacklists, heuristic scanning and the Password Breach Database to ensure weak passwords are rejected. These rules are NIST compliant by default.

More granular policy features include restricting character repetition, month and day names, alphabetic, and character sequences based on keyboard layouts are also available.

Not just for Windows

While AD is a common directory service, many others too rely on passwords. The rules and heuristics engines and the Password Breach Database are available via a web API allowing integration with other directory services or in-house applications for stronger password security.

Regulation and Compliance

The National Institute of Standards and Technology (NIST) Special Publication 800-63B released in June 2017, and updated in December 2017, provides updated password best practice to be more reflective of dealing with modern password security problems.

Section 5.1.1.2 includes a new requirement that passwords should be checked to see if they have previously been compromised in previous data breaches; if they have they can't be used.

Enforcing these new guidelines with legacy built-in directory policies alone is simply not possible.

By deploying Authlogics Password Security Management, you can immediately benefit from enhanced password protection and comply with these regulations, all while cutting helpdesk costs and reducing the password pain for users.

NIST

Authlogics

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866