ENZOIC

DETECT COMPROMISED PASSWORDS
PROTECT EMPLOYEE ACCOUNTS

AUTOMATED PASSWORD MONITORING FOR ACTIVE DIRECTORY

Enzoic for Active Directory combines real-time password policy enforcement with continuous password auditing and automated remediation to keep unsafe passwords out of Active Directory.

Enzoic's threat intelligence team acquires the latest compromised credentials from public and private sources. They go beyond the publicized data breaches with additional unsafe passwords added every day. This follows NIST password guidelines to prevent weak, commonly used, or compromised passwords. Additional policy options include checking a customizable dictionary, detecting reused password roots, and more.

COMPLETE PASSWORD FILTERING AND MONITORING IN ACTIVE DIRECTORY:

Prioritize Full Credential Exposure

Go beyond passwords to detect when an exact username and password pair is exposed and apply separate remediation rules to resolve this critical vulnerability.

Password Filtering

Password hygiene starts with preventing unsafe passwords from ever being saved. It takes just milliseconds from whenever and wherever new passwords are created or updated.

Detecting Expected Passwords & Roots

People frequently use a familiar password root with easy-to-guess variations. Block all these - plus variations on users' names and your custom dictionary entries

Continuous Password Auditing & Remediation

Good passwords become unsafe when they are leaked – even on third-party sites. Continuous screening handles detection and resolution, including optional alerting and password reset.

NIST Compliance

NIST authentication guidelines specify blocking weak, commonly used, expected, and compromised passwords. Enzoic provides a one-click confirmation option to comply with NIST 800-63B.

IMPORTANT CONSIDERATION

Quick Install
An installation wizard allows you to deploy in minutes.

Always Current
Blacklisted passwords are automatically updated every day with the latest from data breaches and Dark Web cracking dictionaries.

Designed for Security
A partial-hash (K-Anonymity) data exchange works without the password or hash leaving your environment or any customer data stored in the cloud.

End-User Messaging
An optional Windows Client explains new password policy requirements and specific validation messages when a password is blocked.

Set & Forget Automation
A configurable process handles customizable notifications, immediate and delayed password resets, or other actions.

Support for Complex Environments
Works with complex domain configurations, hybrid Azure implementations, and third-party IAM platforms that defer to policies in AD.

Integrations
Log files are stored in easy to ingest JSON to support SIEM and SOAR integration.

BENEFITS

- ★ **Prevent Credential Stuffing & Password Spraying: Set a modern password policy that protects against cyberattacks that target unsafe passwords.**
- ★ **Improve End-User Experience: Make passwords easier and stronger by removing outdated complexity requirements and periodic password expiration.**
- ★ **Reduce IT Burden: Run continuous audits and automate remediation, keeping IT administrators and helpdesk free to focus elsewhere.**
- ★ **Seamless: Strengthen an authentication layer that is already in place.**