



Enzoic for Active Directory 3.6 combines real-time password policy enforcement with continuous password auditing and automated remediation to keep unsafe passwords out of Active Directory.

What distinguishes Enzoic is our unique approach to helping organizations prevent the #1 cause of a data breach while ensuring full, automated compliance with industry benchmarks like NIST, CJIS, HITRUST and other compliance standards. Our value proposition goes beyond defense; we're about maximizing resource efficiency, especially in IT and helpdesk, allowing organizations to redirect the saved time and financial resources to other areas.

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 with real-time reporting.



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.



Real-time End-User Messaging

An optional Windows Client explains password policy requirements and provides real-time feedback with every keystroke during password reset.



Broad Credential Provider Support

With Enzoic, you're not limited to the Windows default. Third-party credential providers, such as those equipped with MFA like DUO, are easily integrated.



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, with prebuilt integrations available. With your SMTP server, you can tailor the sender address for email alerts.



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, periodic password expiration, and reset guidance.
- ★ **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.