Automate Password Policy Enforcement & NIST Password Guidelines

Enzoic for Active Directory enables real-time password policy enforcement with daily password auditing and automated remediation. With compromised password detection, custom password dictionary, fuzzy matching with common character substitutions, and continuous ongoing monitoring; enterprises can easily adopt NIST password requirements and eliminate vulnerable passwords in Active Directory.

The newest version Enzoic for Active Directory follows NIST password guidelines as it screens for weak, commonly-used, expected, and compromised passwords. It checks the password at the time it is created or reset, and then monitors it daily against a real-time compromised password database.

Why Do Organizations Need Continuous Password Protection?

The average person reuses a given password at least 13 times. Most people know not to reuse passwords, but struggle to recall unique passwords for all of their personal and work accounts. Cybercriminals rely on this lax behavior and prey upon the vulnerabilities caused by password reuse. This is why compromised passwords are responsible for 81% of hacking-related breaches.

IT and Security teams are fighting back with compromised password screening. For example, some IT organizations download static password blacklists off the Internet and then periodically monitor their passwords against those lists. That is a great first step, but those lists are typically only 10-20% of the common passwords that attackers use, so they provide limited protection. Additionally, since those lists require manual updates, it doesn't protect organizations from any recent breach lists.

Screening passwords against a consistently updated list is critical. Attackers are frequently using the freshest exposures they can find because they know the more recent exposures will result in more successful outcomes. If an organization only uses old password blacklists, they are giving attackers a much larger attack window to take over an employee account.

Enzoic for Active Directory enables continuous password monitoring against a proprietary database of previous breach corpuses that is refreshed daily. It is NIST 800-63b compliant. It then continues to monitor the password daily to ensure it doesn't become unsafe while it is in use.

Why Should Organizations Screen for Commonly-Used Passwords?

Many employees use weak, common passwords and are completely unaware of it because they've satisfied password policies based on traditional algorithmic password complexity rules. For years the security industry has been trying to educate employees, yet still haven't been able to secure this vulnerability. Many organizations are now choosing to take this burden off their employees and automating password screening to account for normal human limitations and behavior when it comes to passwords.

It starts with preventing common dictionary words. Every English-language word can be found in cracking dictionaries so organizations should prevent employees from using basic dictionary words in isolation. Pairing common words with other words, special characters and numbers can be allowed with appropriate character lengths. Additionally, organizations should block repetitive characters or sequential characters (*for example: aaaaaa, 111111*). Lastly, there are the most common passwords that attackers know some people will use so organizations should be blocking common passwords (*for example: 123456, 12345678, qwerty, abc123, password1, iloveyou, etc.)*

Why Should Organizations Block Expected and Similar Passwords?

Most employees will also create or reuse passwords that are context-specific or expected. This can be expected passwords in the form of a root password that gets changed by just a few characters or even just capitalization. Once again, attackers know that this is a common practice on any system with users logging in, so organizations also need to prevent these expected passwords and their various forms.

Organizations should also deploy fuzzy password matching against the entries in their password blacklist. The reason why fuzzy matching is important is if your password is recently exposed online from another site, an attacker will choose to try patterns of that password. They will be highly successful in that endeavor because most people use patterns when selecting their passwords. Fuzzy password matching checks for multiple variants of the password, including case sensitivity as well as common substitutions such as leetspeak and password reversing.

For example: If your exposed password is "HolidayVacation1", attackers will usually try variations such as::

- *"HolidayVacationi" Leetspeak (substituting numbers for letters like leet= 1337)*
- *"1noitacaVyadiloH" reversed password*
- *"holidayvacation1" a case-sensitive change*

Another common employee password behavior that attacks exploit is using one root password and then use various iterations of it. This practice makes it easier for the employee to remember their password, but unfortunately it also makes it easy for bad actors to figure out.

With this in mind, it is important for organizations to implement password similarity blocking. With password similarity blocking, new passwords are screened by similarity to former password using the Damerau-Levenshtein distance.

For example: If your compromised password is "HolidayVacation2018" , attackers usually try iterations like:

- *"HolidayVacation2019" one-character change*
- *"HolidayVacation2020" two-character change*
- *"HolidayVacation18" two-digit change*

In Enzoic for Active Directory, the systems admin can determine the amount of difference (called distance) that will be required between the old password and the new password. With this password policy, the minimum number of differences would be 1 and the maximum number of differences would be 8. Organizations have varying opinions on how many characters should be different, including transpositions, between old and new passwords. This configurability allows them to adjust it to the right level for their business.

Why Should Organizations Screen for Context-Specific Passwords?

Savvy cybercriminals will also attempt to use context-specific passwords to gain access into Active Directory. They know that companies that have headquarters in Boston will be more likely to have employee passwords that include "*GoPatriots*" due to the New England Patriots. They know that since many organizations enforce quarterly forced password resets, many employees will include seasons in their password like "*Winter2019*" and they know that many people include their company name in their password as well. Attackers exploit context-specific passwords because they are commonly used by employees. To combat this, companies need the ability to create a filter for a custom password dictionary.

With Enzoic for Active Directory, organizations can add up to 5,000 custom passwords stored locally that will be screened and blocked at creation. These words can be local sports team, years, product names, company names, office locations, etc. Custom passwords are partially matched and case insensitive so any password that includes that word would be blocked. These can also be optionally fuzzy matched if you have fuzzy matching turned on.

For example: If your custom password dictionary includes the word "GeneralElectric"

- *Users would not be allowed to use that word in any password so a password like "ILovegeneralElectric" will be blocked.*

How Does Automation Help Save IT Team Time and Energy?

The goal of Enzoic for Active Directory is to allow IT to set it up and then just let it run. When an existing password becomes vulnerable, Enzoic automates the remediation steps that would otherwise require manual intervention by an Admin or Helpdesk.

Some organizations buy password policy enforcement tools that handle one or some of these, but the most recent version of Enzoic for Active Directory can meet all the NIST criteria. There is no additional manual work required. Enzoic for Active Directory serves as a

comprehensive, automated password blacklist that filters for weak, commonly-used, expected, and compromised passwords.

Organizations have unique needs, so the automated responses can be customized when compromised or weak passwords are found. The organization can select the appropriate automated action—ranging from prompting the user to change their password to disabling the account. These remediation steps can be set to kick-in immediately or after a predetermined delay. Alerts can also be sent to the user directly and/or an admin or helpdesk so the right individuals are kept informed.

What Visibility Is Available?

Enzoic for Active Directory has also incorporated additional insights into the product. It has enhanced usage tracking so Active Directory administrators can see the total number of detections, including the number of detections due to fuzzy matching, local dictionary or password similarity matching. With log files now stored in a JSON format, outside consumption by SIEM and log management tools can help streamline reporting.

What is Required for Installation?

Enzoic for Active Directory runs on each domain controller so it can check every password wherever it is being created; however, it only needs to be configured once. All of its configuration settings are stored in Active Directory itself and automatically shared across other domain controllers to make it easy. With the installation wizard, it is easy to install. Some customers have it fully implemented in 3 minutes, but of course, that depends on the complexity of your environment.

Daily Screening

Continuous exposed password filtering

New Exposures

Detects if a safe password becomes exposed

Automated

No extra manual work

Insightful

Enhanced dashboard and SIEM logging

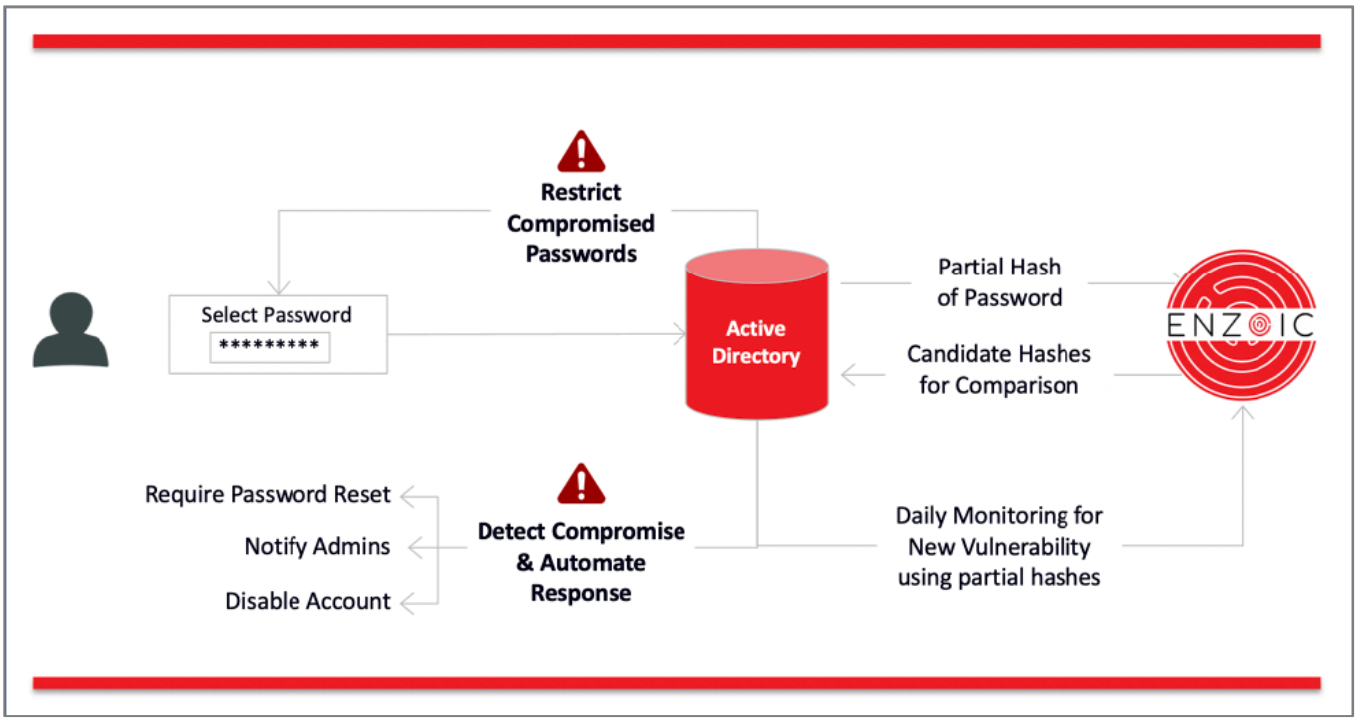
Quick and Quiet

Checks in milliseconds and only impacts employees that need to change their password.

Easy to install

Take a short amount of time to install, then you just let it run because everything is automated.

Flow chart of how it works



Enzoic for Active Directory enables quick-to-deploy password policy enforcement and daily exposed password screening. With a fully automated weak password filtering, fuzzy password matching, password similarity blocking, and custom password dictionary filtering; enterprises can easily adopt NIST password requirements and secure passwords in Active Directory.