Have you been pwned? Try Enzoic for Active Directory compromised credentials protection

Brandon Lee Tue, Apr 5 2022 password, security 0

Have you been pwned? The new compromised credentials protection feature of Enzoic for Active Directory allows you to monitor your AD users' exact username and password combination from the latest pwned (breached) passwords available to hackers.

Author Recent Posts

Brandon Lee

Brandon Lee has been in the IT industry 15+ years and focuses on networking and virtualization. He contributes to the community through various blog posts and technical documentation primarily at Virtualizationhowto.com.

Contents

Have you been pwned? ^

A new development on the dark web is the Initial Access Broker (IAB), a group of cybercriminals dealing with pwned passwords, that is, with stolen credentials. Combined with Ransomware-as-a-Service (RaaS), these are extremely dangerous and provide even novice attackers with access to everything they need to launch a ransomware attack with compromised credentials.

Current password guidance from Microsoft and NIST, among others, now recommends checking passwords against known breached lists. This means that organizations should check passwords in use or recently created to see whether they are known to be breached. However, Active Directory Domain Services (AD DS) does not have a native way to check for breached passwords. The traditional Active Directory Password Policy found in Group Policy has not changed much over the years. It only allows controlling the basic elements of passwords chosen in the environment, such as age, length, complexity, etc. The password policy settings below are taken from a Windows Server 2022 domain controller.

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	42 days
Minimum password age	30 days
Minimum password length	Not Defined
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Not Defined

Active Directory password policy settings

What is Enzoic for Active Directory? ^

Enzoic for Active Directory is an automated tool to help level the playing field with attackers who have access to breached password lists, cracking tools, password dictionaries, and other automated tools of their own. Enzoic for Active Directory does two things to make sure a password is safe:

- When a password is created, it checks the password against billions of unsafe passwords known to the Enzoic password dictionary database. Enzoic checks for exact passwords and fuzzy logic variations that hackers also check for during brute force attempts or other types of attacks. When a password is reset, Enzoic performs the same checks.
- As part of the continuous monitoring provided by Enzoic, it also checks Active Directory passwords daily for new compromises in the environment based on newly collected data. The reality is that a password could be uncompromised today but pwned tomorrow. The automated rechecks of the Active Directory environment help discover these types of new password risks. Enzoic fully automates the alerting and remediation of password risks when password risks are found in the environment, so no manual tasks are required.

Note the following features included in Enzoic for Active Directory:

- **Easily align with modern password guidance**—Provides push-button alignment with modern password guidance from NIST and others, including all common, easy to guess and compromised passwords.
- **Security-focused architecture**—No passwords are transmitted between the domain controllers and the Enzoic cloud. It uses a partial-hash exchange that maintains the security of Active Directory passwords.
- **Intuitive messaging**—You can install an optional Windows client that provides intuitive feedback and validation messages when passwords are blocked.
- **Fully automated**—When Enzoic's continuous monitoring process detected a compromised password, Enzoic handles the automation of requiring password resets, notifications, and other actions.
- **Hybrid cloud-aware**—Enzoic works with traditional AD DS deployments, complex domain configurations, and hybrid Azure AD implementations. You can also use third-party IAM solutions that defer policies in Active Directory.
- **Rich integrations with SIEM and SOAR solutions**—Enzoic provides JSON-formatted log files that can integrate with popular SIEM/SOAR solutions on the market.
- **Up-to-date compromised and dark web password dictionaries**—Enzoic updates the password lists each day, which helps to have the most up-to-date information available for password risks in the environment.

Enzoic's added value lies in its full automation capabilities and the always up-to-date database of passwords and variations checked, which is much larger than many of its competitors. While IT admins can perform some checks via PowerShell scripts and other tools, these are manual tools and processes. In addition, the list of passwords checked is generally static or rarely updated from many open-source lists. The full compromised credentials feature, new in 3.2, steps up the protection to include both the username and password combinations found breached in the wild. We will discuss this in detail below.

When attackers use sophisticated automated tools that only need to find one compromised password in the environment to make their way "in the door," Enzoic helps businesses increase their password security posture and equal the playing field.

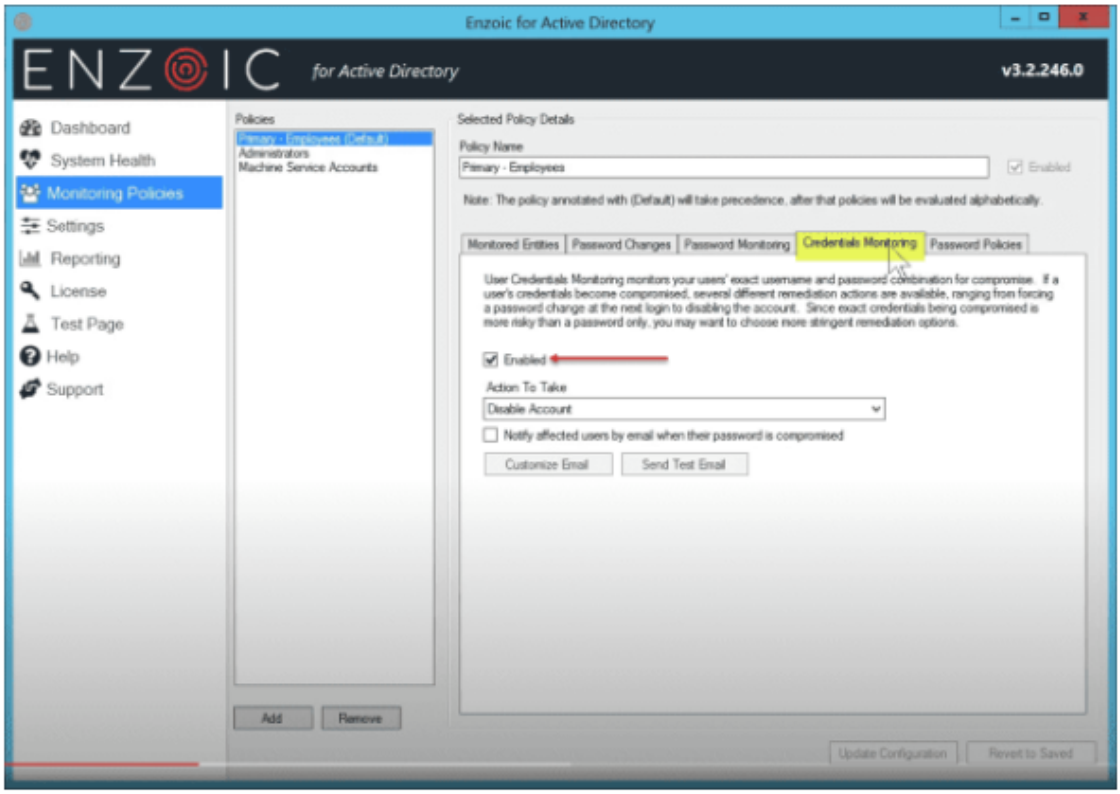
Enzoic architecture ^

The Enzoic solution comes down to a password filtering Active Directory plugin installed on each domain controller. It is a small footprint installation and has minimal requirements. These include the following:

- AD DS running a forest and domain functional level of at least Windows Server 2008 R2 or higher. Note that you need to install Enzoic on all domain controllers running in your AD DS environment.
- Microsoft .NET Framework 4.5 on each domain controller, provided as part of the Enzoic installation.
- Internet egress connections for TCP port 443 on your firewall. IT admins can use a proxy to route traffic to a designated server and scope down the egress connections, either via the IP addresses provided by Enzoic or via FQDN to Enzoic.com.

Pwned password protection ^

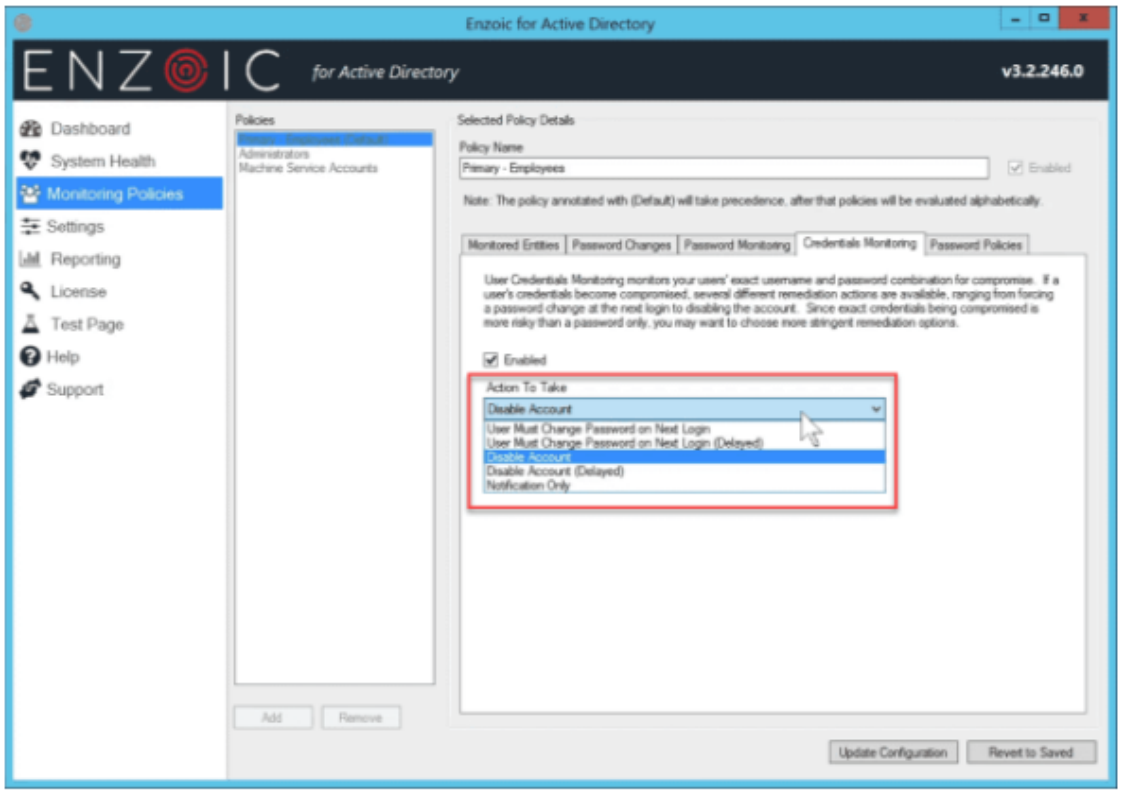
While competitors can check pwned password lists, Enzoic for Active Directory 3.2 adds monitoring your users' exact username and password combination to see whether they have been compromised. This functionality is an even more critical check than just a pwned password, since it means Enzoic has noted the exact credential pair (username and password) has been compromised.



Enzoic for Active Directory full compromised credentials functionality

Since full compromised credentials are a critical password risk, Enzoic provides many options for IT admins to remediate this condition. The options for the full compromised credentials found with Enzoic include the following:

- **User Must Change Password on Next Login**—Immediately sets the **User must change password at next logon** setting in Active Directory for this user.
- **User Must Change Password on Next Login (Delayed)**—Sets the **User must change password at next logon** setting in Active Directory for this user after the selected delay period.
- **Disable Account**—Immediately sets the **Account is disabled** setting in Active Directory for this user.
- **Disable Account (Delayed)**—Sets the **Account is disabled** setting in Active Directory for this user after the selected delay period.
- **Notification Only**—The administrators on the administrative notification list, as well as the affected user (optional), will be notified via email that the password is compromised with no other action taken.



Choosing the remediation option for Enzoic full compromised credentials

Wrapping up and impressions ^

Password security is one of the most crucial areas of focus for businesses today to bolster their overall cybersecurity posture. Using manual tools, running scripts, and relying on stagnant lists of passwords is better than not scrutinizing end user passwords at all. However, it will most likely fall short when attackers use sophisticated password crack utilities and deep dark web password intelligence to compromise businesses.