Review: Enzoic for Active Directory

Hrvoje Martincic

Senior IT Consultant

Data breaches now happen so often that we don't even pause when reading yet another headline notifying us of the latest one. We react only if the breach happened to a service we use – and maybe not even then. But we should all be aware that once one of our passwords has been compromised and exposed, it should be considered compromised forever.

By gathering and analyzing passwords leaked after many breaches, attackers may work out specific users' password-creation patterns, allowing them to easily guess their passwords. Even worse: they don't need to discover those patterns and attempt to guess passwords, since many users **don't even bother to change their passwords** after a data breach.

By using honeypots or private personas to go into places where bad actors go, Enzoic researchers are continuously investigating data breaches and credential leaks so that organizations that don't have threat researchers can take advantage of the knowledge gleaned during the investigations.

What's new in Enzoic for Active Directory?

One of the strong points of the Enzoic for Active Directory solution is that it's fully compliant with NIST's password guidelines (as set out in **NIST Special Publication 800-63b**, which has been updated in 2020) helping organizations easily achieve industry best practices for passwords.

If you look at those guidelines, you can see that NIST has moved away from old password policy recommendations and has now suggests that users should focus on password blacklists over algorithmic complexity, with an emphasis on ensuring passwords are adequately hashed and salted. Additionally, organizations should not require their employees to reset their passwords unless there is evidence of compromise, and they should monitor new passwords daily, testing them against lists of more recent compromised passwords.

Of particular note is NIST's recommendation of eliminating periodic password resets if you have a method to detect whether credentials in use have become compromised. Here is where a tool like **Enzoic for Active Directory** can come in handy, as it checks passwords when they are created but also continues to check them daily against a constantly updated database.

In its most recent release (v3.2.318.0), Enzoic for Active Directory is going beyond just checking passwords to see whether they've been compromised generally - it now also checks full

credential pairs (e.g., email address + password). And, throughout it all, it uses **k-anonymity**, a secure method using partial-hash data exchange to check passwords without the password or the hash leaving the customer's environment or cloud assets.

Installation

A setup assistant (wizard) allows for an easy installation and setup process, and helps users apply their new password policy with ease.

I installed the solution in my test environment via the domain administrator account, as elevated domain privileges are required to access Active Directory to select which users and groups will be monitored.

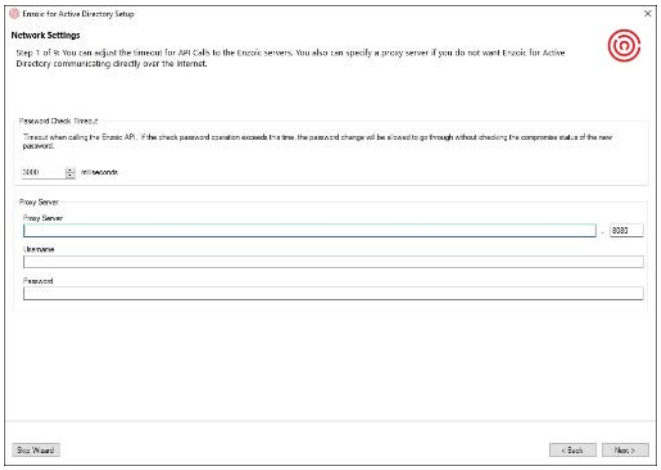


Figure 1 – Network Settings

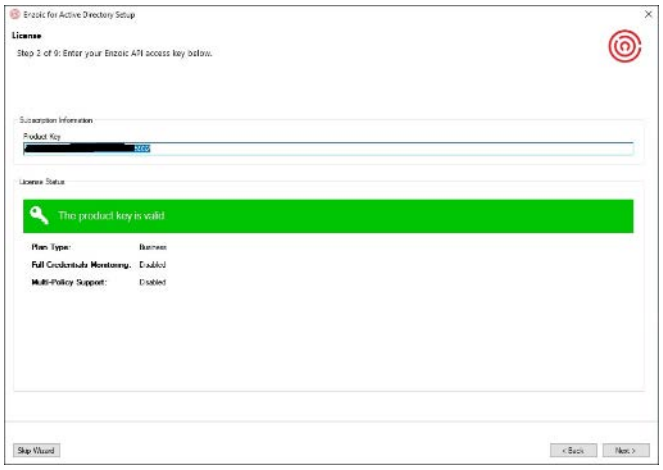


Figure 2 – Enter the product key

After entering the necessary network and license information, I was offered the option of setting up groups and users to be monitored, followed by the option of letting the solution automatically choose the right configuration to achieve NIST 800-63b compliance (alternatively, you can customize settings manually).

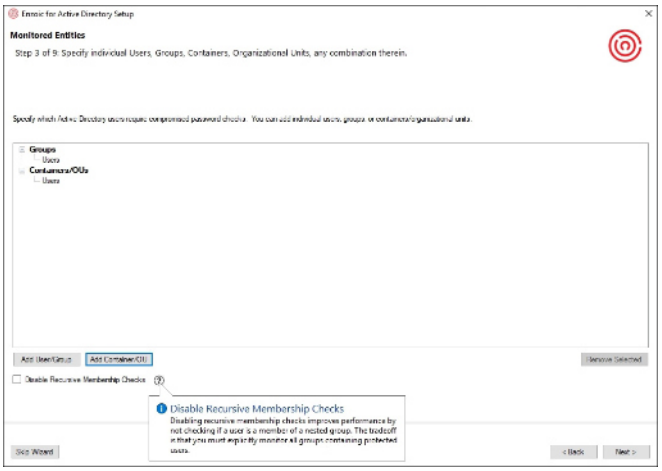


Figure 3 - Setting up groups and users to be monitored

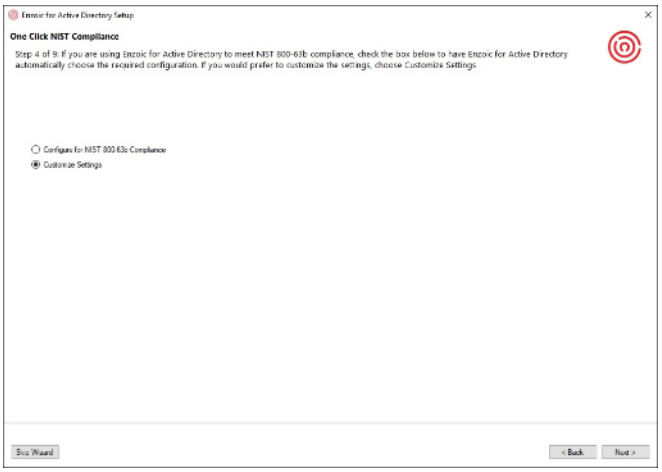


Figure 4 – One Click NIST Compliance

By choosing the "One Click NIST Compliance" option, you can set up a new, NIST-compliant password policy in mere minutes (though not with just one click).

To begin with, you'll need to add words specific to your business (e.g., company name, product name, etc.) to a list that will be used to create a local

custom password dictionary. The solution will use that local dictionary to prevent employees from creating predictable and easily guessable passwords that could be easily connected to your company. By cutting this link, you are limiting options for the attacker. All dictionary and compromised passwords are automatically handled by Enzoic, so your custom dictionary can be concise.

Figure 5 – Creating a list of words specific to your business

Next, you are given the option to enable User Password Monitoring and select the remediation actions users will have to go through if their password becomes compromised. I like the option to add a delay before automatically requiring a password change or disabling the account.

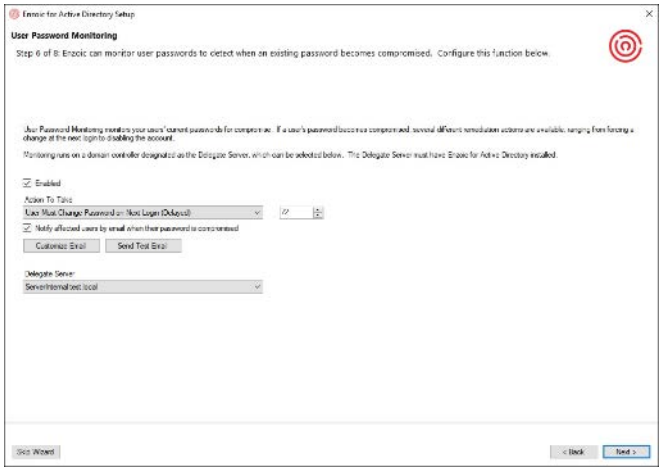


Figure 6 - Setting up User Password Monitoring

The alternative to “One Click NIST Compliance” is to choose your own settings. This includes deciding if you want to enable User Password Monitoring (as pictured above) and which individual password policy settings for your organization's policies and requirements:

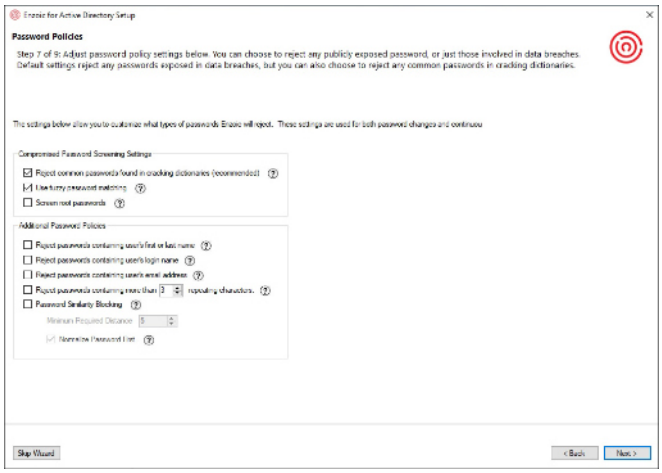
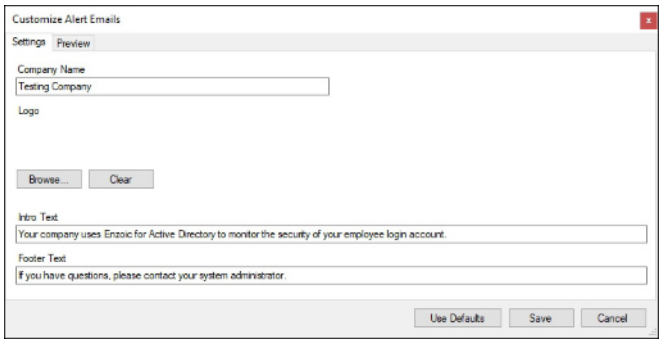


Figure 7 – Choosing specific password policies

Regardless of your installation path of choice, you can customize and preview the email alerts that will be sent to your employees if their password is no longer safe to use:



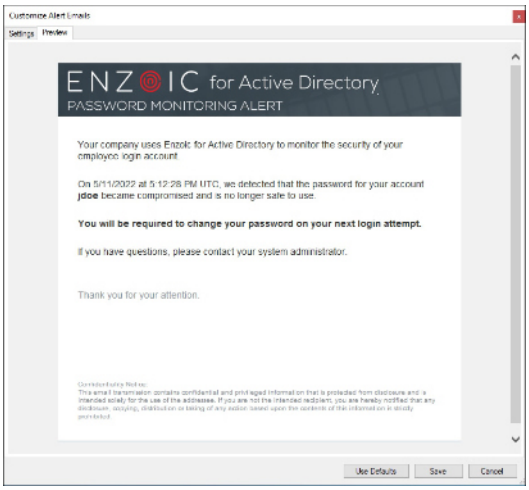


Figure 8 and 9 - Customizing and preview of email alerts

Next, you must specify which administrators will be notified when the solution has an important alert:

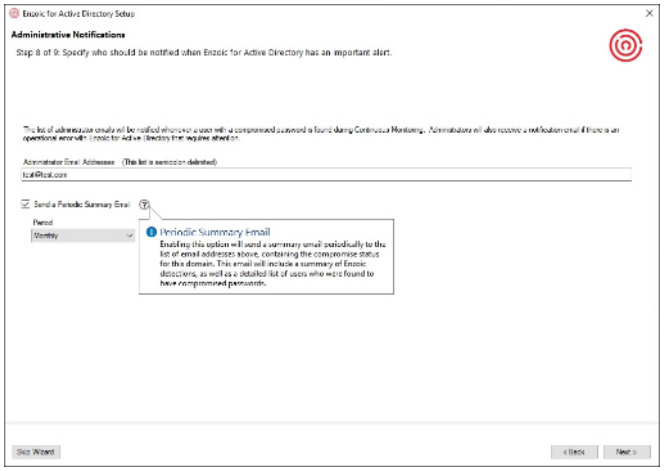


Figure 10 - Administrative Notification settings

Admins who have been added to the list to receive administrative notifications will be notified every time a monitored user with a compromised password is found in the system during Continuous Monitoring, although most organizations will set up the automatic remediation that handles requiring a password reset at noted above. Admins will also receive notifications in case of operational error with the software, as they must resolve the situation.

You can also make it so they receive a periodic summary email that will provide additional insight by delivering a compromise status for the monitored domain, a summary of Enzoic's detections and a list of users with compromised passwords in a specified time frame. This can be helpful for documenting password policy compliance for auditors.

Finally, you can test the settings configured during the installation. The test checks whether the password chosen by a specific user complies with your password policy and whether it has been compromised (by comparing it against Enzoic's database of billions of common and compromised credentials). Enzoic suggests most checks take around 250 milliseconds, and I can confirm the password check takes well under a second:

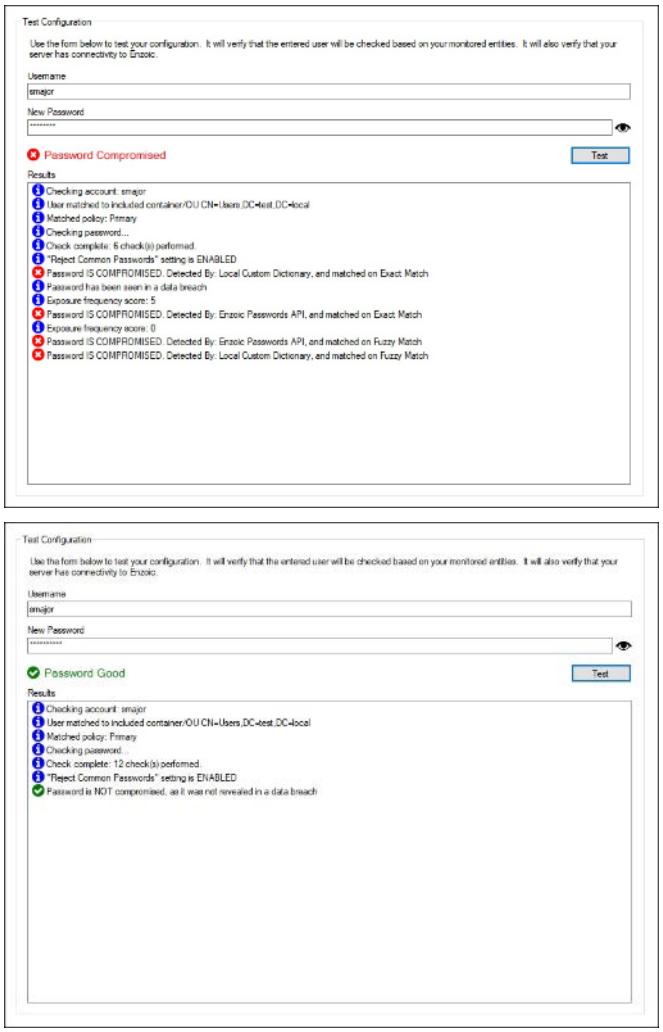


Figure 11 and 12 – Testing a password

And that's it! The software is installed, up and running, applied to a Windows domain environment, protecting monitored users right away.

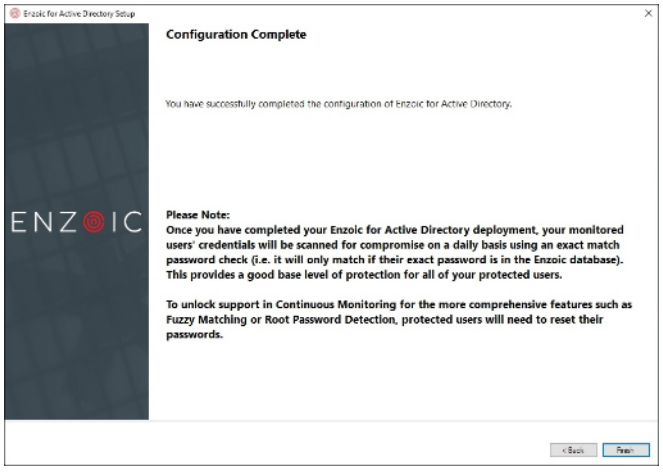


Figure 13 - Completed installation (with some limitations)

Enzoic states that to fully unlock the potential of the software – e.g., more comprehensive features such as “Fuzzy Matching” and “Root Password Detection” - a password reset is required for all monitored users. As a domain-wide user password reset is not possible in all environments nor convenient right after the installation, Enzoic made the right choice to leave these features disabled. It’s on administrators to decide if/when to enable them.

Use

Once installation and setup are complete, Enzoic for Active Directory will ask you if you want to run an initial scan of your domain to identify monitored users with compromised passwords.

This scan will reveal users with the compromised or weak passwords and accounts that share passwords, and I recommend running it right away.

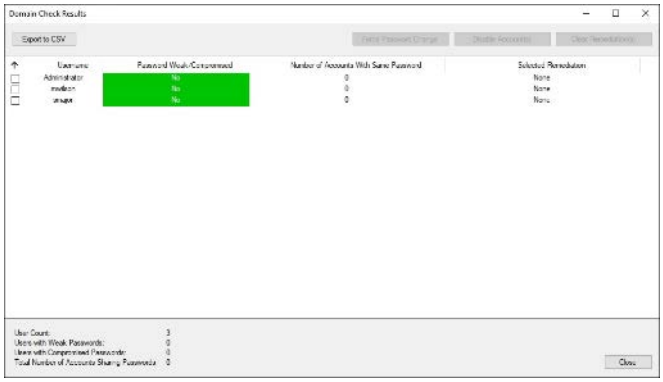


Figure 14 – The results of the initial scan of the domain

Looking at the dashboard, I can say that Enzoic tried and succeed in keeping things simple and tidy. I could argue that the color scheme could be toned down, but that’s not an issue – just a personal preference.

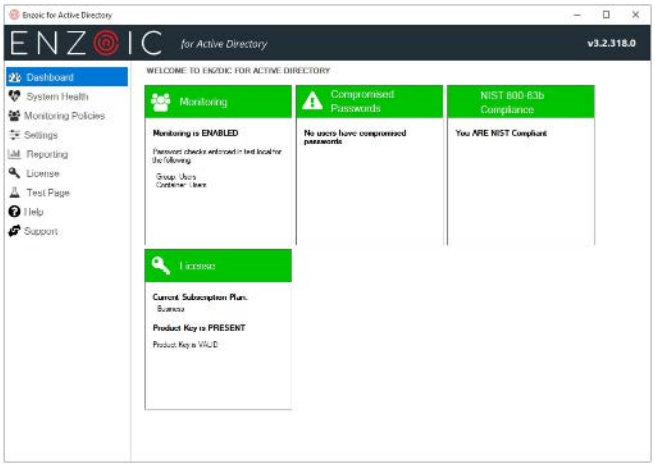


Figure 15 – The solution’s dashboard

The System Health tab provides an overview of possible issues with the Enzoic for Active Directory, enabling you to quickly detect and diagnose them.

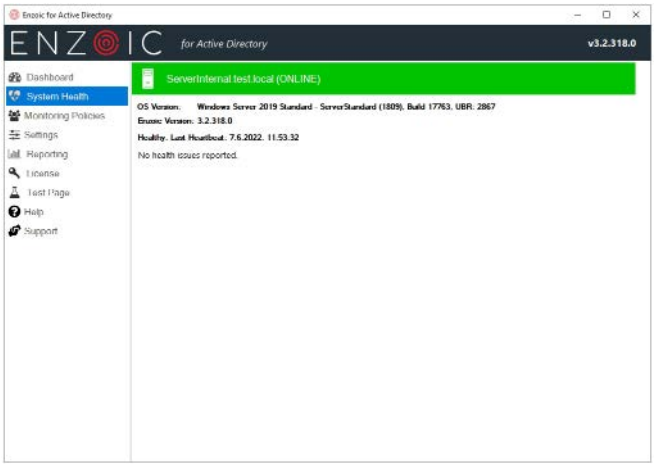


Figure 16 - System Health info

All the options you have initially chosen during the installation and setup process can be changed.

In the Monitoring Policies tab you can add additional policies (if supported by your software license), but also configure the monitoring policy to fit your needs.

• Monitored Entities – Fine tune Active Directory users and groups to be monitored

• Password Changes – Enable protection for monitored entities during password change

• Password Monitoring – Enable continuous, daily checking of how it behaves when it finds compromised user passwords

• Credentials Monitoring – Customize actions when full credentials (username + password pair) are compromised.

• Password Policies – Customize what types of passwords will be rejected

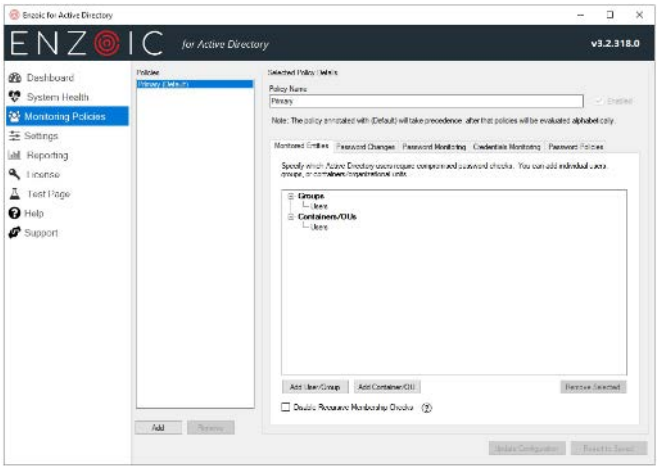


Figure 17 – Choose monitored users and groups

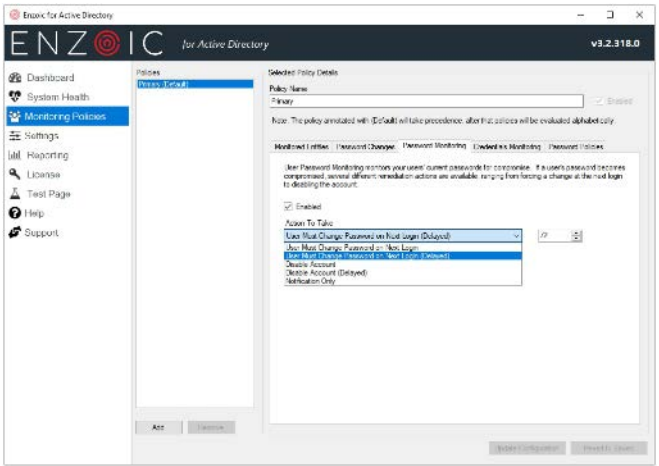


Figure 18 – Enable or disable Password Monitoring

User Credentials Monitoring

User Credentials Monitoring checks every day if the exact email/password combination has become compromised. Since this type of compromise presents a level of high risk, I would always recommend disabling the user until the situation is investigated either by admins or dedicated security team.

Access to full credentials is a treasure trove for attackers, as it greatly simplifies access to the target system. This is exactly why taking advantage of the User Credentials Monitoring option provides an additional level of protection most organizations should be using.

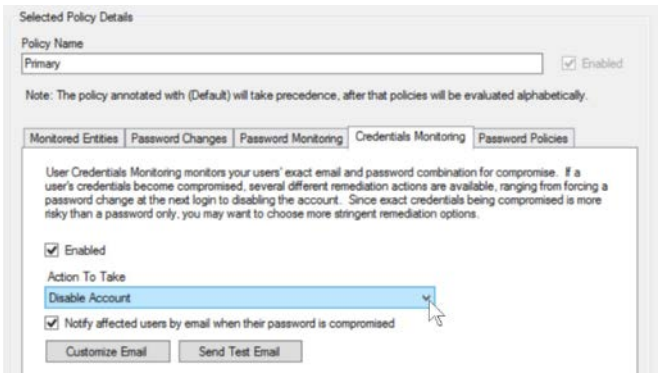


Figure 19 - Add checking of full credentials (email/password combo)

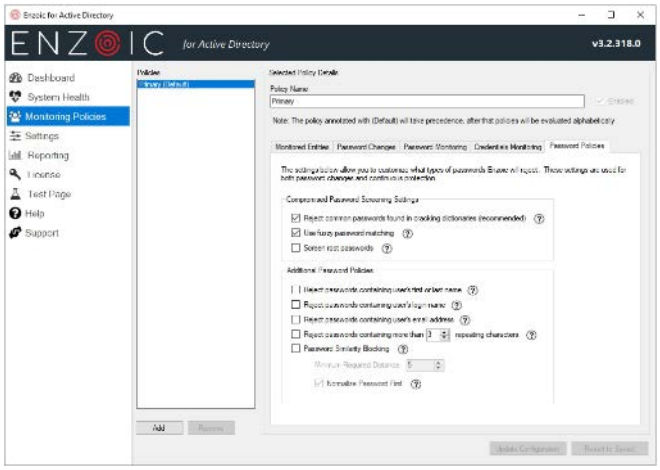


Figure 20 - Customize what types of passwords will be rejected

All Settings are configurable here in one place: You can change network settings, add new words to your custom password dictionary, change which admins will be receiving alerts, and make sure your password policies will adhere to NIST standards.

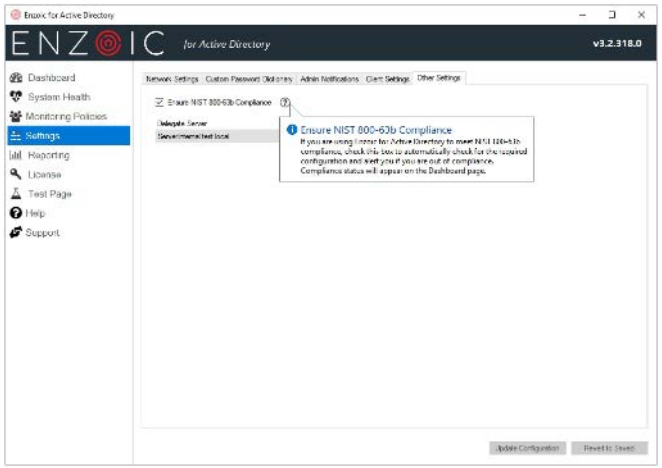


Figure 21 - General Settings

Reports based on "Monitored users," "Password Change," and "Continuous Monitoring" can be generated and exported to CSV:

Verdict

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

By using Enzoic for Active Directory organizations of all types and sizes can implement NIST 800-63b password guideline requirements in minutes and monitor and clean their AD environment of vulnerable or compromised passwords.

In my humble opinion: If you're searching for such a service or if you're looking for a password policy tool that offers protection from leaked credentials with daily updates, Enzoic for Active Directory is a candidate you should strongly consider.

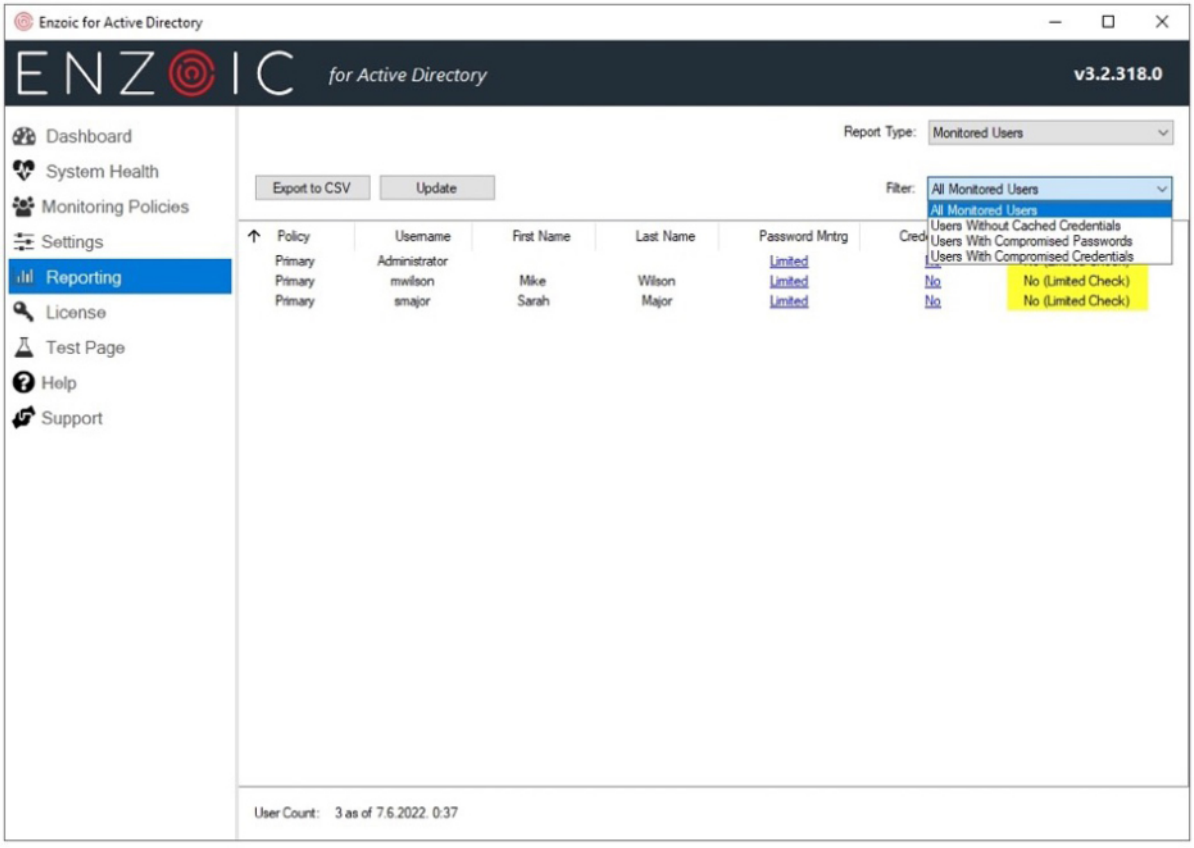


Figure 22 - Reporting options