E-BOOK

Using NIST Guidelines for Secure Passwords

ENZOIC

The Compromised Credential Crisis: What's Happening?

Due to ongoing data breaches, billions of credentials are available on the Dark Web. They represent a major vulnerability in contemporary cybersecurity. They're responsible for everything from destructive ransomware attacks to individual account takeovers, which can be an entry point into an entire network.

Designing and implementing a password policy that responds directly to NIST guidelines is a crucial step in locking down your company's security. Enzoic for Active Directory achieves password security in line with NIST by enabling real-time password policy enforcement and daily password auditing with automated remediation.

What are the NIST Guidelines?

NIST (National Institute of Standards and Technology) is a neutral, data-driven body that provides guidelines for improved security postures.

Since 2017 NIST password guidelines have recommended eliminating traditional password complexity requirements.

NIST now recommends the following:

- No longer requiring the use of character complexity
- Instead of character complexity, screening passwords against a blacklist
- Allowing users free reign of all Unicode characters (including spaces)
- Requiring at least eight characters per password, the more the better
- Allowing copy/pasting of passwords to facilitate the use of password managers
- Getting rid of the periodic password reset

Why has NIST made these recommendations?

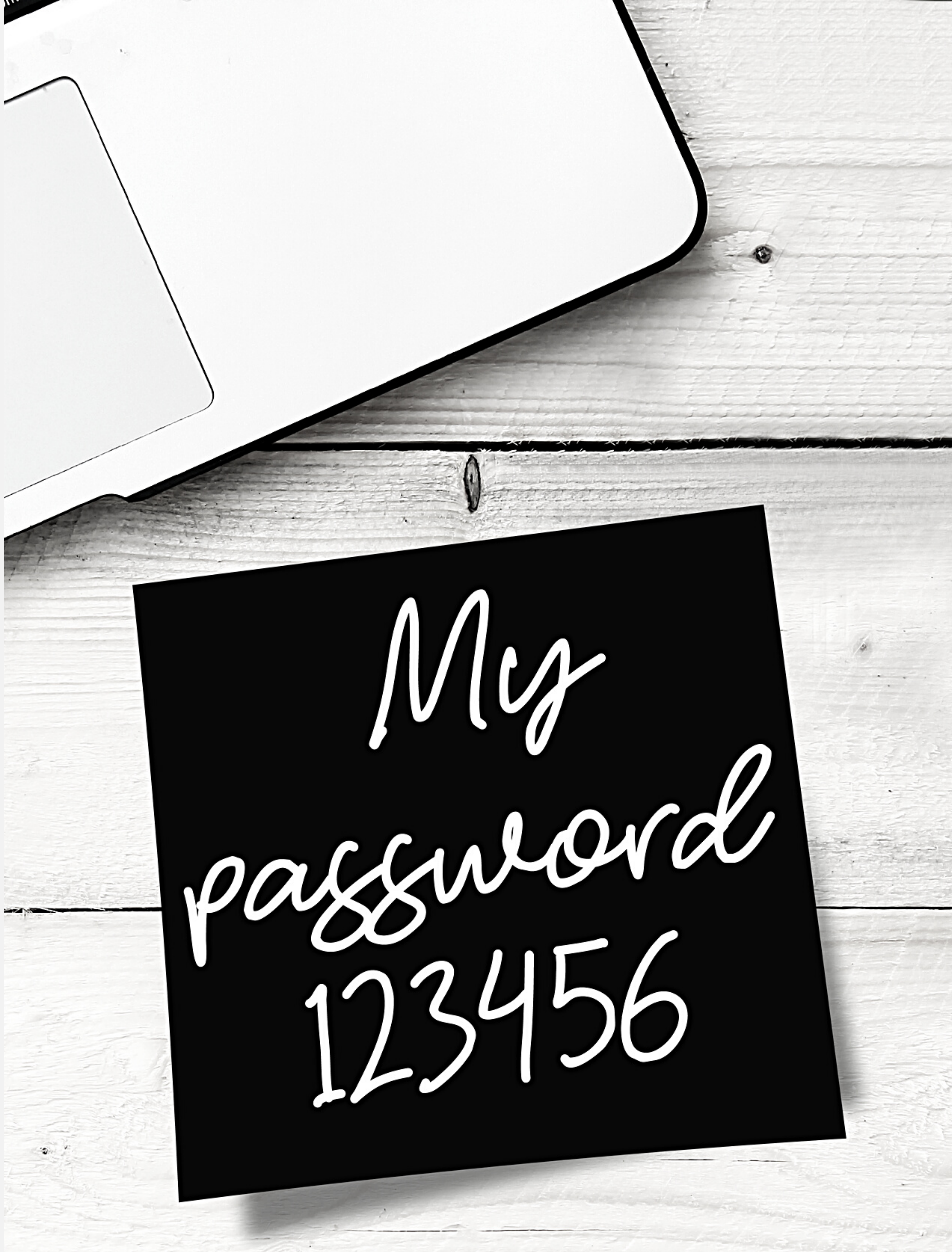
Years of academic and industry research showed that previous password recommendations did not result in more secure passwords. Passwords requiring character complexity (combination of alpha, numeric, and symbols) made selecting a memorable password more difficult for users. However, the predictable patterns people followed made passwords easier for bad actors to guess. What's more, recent surveys from Google and Verizon DBIR Reports revealed that password reuse is a perennial issue across industries. The human desire to remember our passwords means that most people reuse their passwords across personal and professional accounts blending boundaries. This habit creates a significant additional vulnerability for organizations.

Screening Passwords: How Many and When?

It's essential to think about what passwords should be screened and at what point screening should occur.

The reality of cyberattacks is that threat actors are not sitting around painstakingly guessing individuals' passwords. Instead, their dedicated programs and bots can guess hundreds of thousands of passwords a second—and there are many methods attackers use to commit cyberattacks, like credential stuffing.

Since bots can guess so many combinations, blocking the most common passwords (like '123456' or 'Password123') is a starting place, but it's nowhere near enough. As a result, organizations need to expand their understanding of just how wide threat actor's nets are.



Humans are highly predictable, and threat actors know the typical patterns people use to satisfy complexity requirements. For example, a user might want to choose a password like 'baseball' but see that they are also required to have a digit and special character, so they might slightly alter it to 'Baseball1990!' and think they've created something untouchable. But these slight variations, known as leetspeak, are just as easy for threat actors to guess. Therefore, organizations must find a way to screen against these root passwords and fuzzy matched and similar passwords.

When thinking about their security posture, enterprises should approach the issue like an attacker. Threat actors will certainly go the extra steps of paying attention to company-specific details, from an organizations' name to location. For example, if your organization is in New York City, employees are more likely to choose passwords like 'GoGiants2021'. Attackers will exploit these context-specific passwords because they know they are more likely to be used by employees.

Compiling a contextual list of terms, including product names and location details, into a custom dictionary is crucial in developing an effective password blacklist.

What's the difference between static and dynamic blacklists?

When first encountering the password blacklist concept, some might want to search for a free option. There are many static lists online. Some are never updated, and others are only updated a few times a year. Cybercriminals are typically using the most recent data breaches.

A static list means your blacklist will not include the most recent credentials leaked. However, a dynamic blacklist grows and constantly changes in response to the data breaches occurring every day.

What does 'dynamic' really mean?

Be wary of 'continuous monitoring' claims. For example, some services might call themselves dynamic but only update several times per year with those free lists. Unfortunately, that isn't good enough. Organizations need true continuous protection because, in the cyber landscape, things move quickly. Therefore, companies need to find a password blacklist that is updated multiple times per day.

Timeliness also ties back to the NIST guideline recommendation to eliminate periodic password resets. While eliminating password resets is currently only a recommendation and not a requirement, many organizations are starting to recognize the simple logic and real-world evidence behind this change.

While designed to take unsafe credentials out of circulation, periodic password expiration encouraged users to select weaker passwords because they knew they would be temporary. When faced with this situation, users often just make incremental changes to previously used passwords.

At the same time, a compromised password kept in circulation until the next periodic reset provides far too much time for bad actors to apply their craft.

As for 'when' to screen passwords, the short answer is 'continuously.' Doing so is easy through Enzoic for Active Directory, which checks at least once per day against the latest data breaches.

Are there NIST policies already in Active Directory?

Microsoft relies on third parties to deliver the capabilities necessary for Active Directory to comply with NIST requirements.

Creating a NIST-approved password policy within Active Directory for your organization is not only possible, but it's also an excellent idea for making the password policy effective and user-friendly.

Organizations of all sizes use Active Directory. This popularity means that cybercriminals frequently target AD. Organizations need something additional to boost their security because the policies within AD don't adhere to the recent NIST guidelines. Enzoic's Active Directory plugin complies with the NIST standards with the additional benefit of fitting seamlessly into the user experience with minimal user friction.

With Enzoic for Active Directory, an organization can tailor several aspects of the plugin to their needs. For example, for organizations looking to satisfy the NIST requirements, a single checkbox can apply all of the password policy options. In addition, once enabled, a dashboard component can highlight if settings are changed, alerting the IT Team.

Checking for Compromised Credentials... Constantly

One of the most critical abilities the tool provides is checking if a password is already compromised when a user creates it.

Given that users tend to re-use passwords between personal sites and business logins, it's highly possible that a password they use on a non-work site has been compromised and is now a risk to the organization.

Additionally, Enzoic for AD will monitor all approved credentials on an ongoing basis so that when a user's username or password is detected and determined to have been compromised, appropriate action can be taken immediately.

The blacklist database that powers Enzoic for Active Directory is updated daily with the latest breach data, and passwords are rescanned every 24 hours. When users' passwords are found to be vulnerable, the remediation steps are fully automated. Organizations can also tailor which steps they would like to take, from alerting the user or forcing a password reset to flagging the compromise internally for the IT team to monitor.

Unexpected Benefits

Unlike other products, Enzoic for AD doesn't add a burden to the organization. Adopting a NIST password policy does the opposite:

1

It improves the user experience by eliminating password complexity rules and reducing frequent password reset

2

and it lowers administrative costs with fewer password resets calls and automated remediation.

Prevention is critical when it comes to cybersecurity. Enzoic for Active Directory will help prevent additional breaches, ransomware attacks, and account takeover.

What's Next

Enzoic for Active Directory was specifically designed to satisfy NIST password policy requirements. It is based on Enzoic's proprietary compromised credentials threat research. The blacklist database that powers Enzoic for Active Directory is updated daily with the latest breach data.

When an enterprise invests time and effort into strong defensive security, it will find many positive ramifications. With Enzoic for Active Directory, both detection and remediation are automatic, meaning that the screening happens passively and constantly in the background and only impacts the users' experience to protect them. As a result, the journey to cyber hygiene has never been easier.

» Free Trial

Email Address
info@enzoic.com

Website
www.enzoic.com

ENZOIC