stealthINTERCEPT

StealthINTERCEPT® ENTERPRISE PASSWORD ENFORCER

Password policy enforcement for Active Directory environments

stealthbits

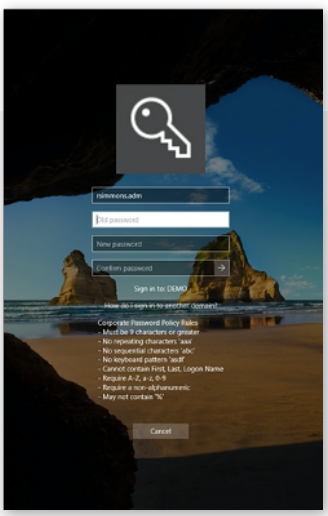
With 80% of breaches involving weak or compromised passwords and the top 10 common passwords still including '123456', 'password' and 'qwerty', organizations need to strengthen & improve password hygiene. Breach costs will only rise, further emphasizing the importance of your first line of defense...the password.

Password Policy Enforcement Users Barely Notice

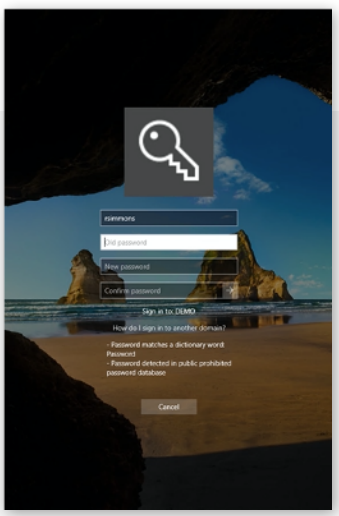
Using a dictionary of millions of collected compromised passwords, along with complexity, character substitution, and policy testing tools, Stealth-INTERCEPT Enterprise Password Enforcer safeguards your organization from credential-based attacks. We identify and prevent weak and compromised passwords from being used and can even provide user guidance on how to choose a strong(er) password.

Key Benefits

- Save helpdesk calls and costs by telling users why passwords fail and what changes need to be made to adhere.
- Avoid user frustration and unnecessary helpdesk calls by testing new or modified password policies before production rollout.
- Improve password effectiveness by controlling allowable character substitutions (e.g. "A" ≠ "@"; "S" ≠ "$").
- Increase security and ensure total enterprise systems compatibility with granular password complexity control.
- Establish strong password defenses by ensuring none of yours are found in the "Have I Been Pwned" breach dictionary of 555 million known bad ones.



Show your password policy to users



Show specifically why password rejected

KEY FEATURES

Tell Why Password Failed

Save helpdesk calls and help users choose passwords that meet policy by showing them what needs to change.

Control Character Substitutions

Attackers can easily replace an "S" with a "$", or an "A" with the "@" too. Gain control of your passwords and all possible variations.

Password Policy Testing

Before implementing modified password rules, it's advantageous to know where and what issues will arise.

Breached Password Dictionary

Check a repository of 555 million known bad passwords, HIBP, so users don't unknowingly try & use these vulnerable passwords.

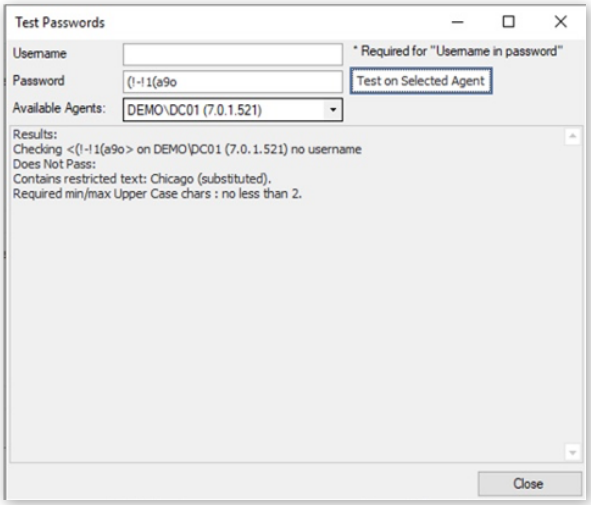
Enhance Password Complexity

Administrators gain more granular control of password requirements to ensure proper compatibility across all resources.

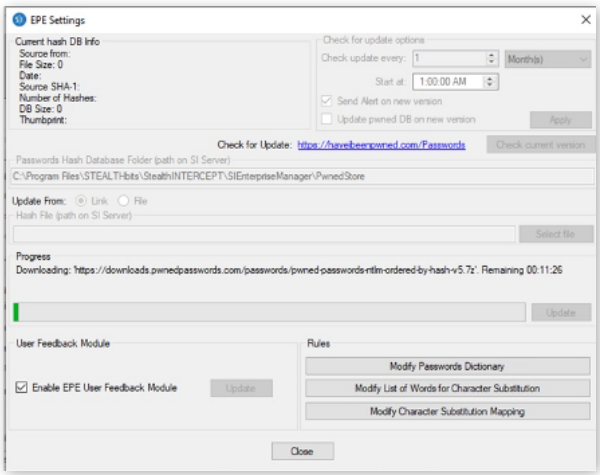
Know the Affects of a Password Policy Change BEFORE Deployment

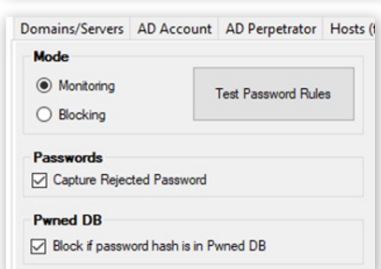
Wasted time and user & administrator frustration is often caused when organizations change password policies. Most don't know the impact until deployed. Some accept it as a necessary evil, we found a better way!

StealthINTERCEPT Enterprise Password Enforcer allows policy creators to test out any potential policy change without affecting users. We analyze the proposed policy against current environment passwords, reporting back which would fail and why. Get your policy right BEFORE engaging users.



Password policy tester





Check enterprise passwords against the Have I Been Pwned repository

Improve Passwords - Check Them Against Millions of Known Bad Ones

The password "NjHGYAPLkF2#17" complies with most common complexity standards and many would consider a strong, very hard to guess password.

BUT THIS PASSWORD WAS STOLEN IN A PAST BREACH AND IS FOR SALE ON THE DARK WEB…

60+% REUSE THE SAME PASSWORD AMONG ACCOUNTS[1] LEAVING YOU VULNERABLE!

The National Institute of Standards and Technology (NIST) recommends the restriction of "passwords obtained from previous breach corpuses" and other "commonly-used" or "expected" values for passwords. StealthINTERCEPT Enterprise Password Enforcer leverages the Have I Been Pwned breach dictionary of 555 bad/ compromised passwords.

1 - https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com