ManageEngine
ADSelfService Plus

How to keep up with the **shifting landscape** of **password attacks**

www.adselfserviceplus.com

Weak passwords are the direct result of weak password policies.

Since the early 2000s, Microsoft's Active Directory and its associated applications have played a critical role in IT management. Enterprises today still rely heavily on Active Directory to manage identities in their IT environments. Despite advances in technology, Active Directory's password policy has remained unchanged for a decade. As a result, today's administrators are forced to find ways to circumvent the weaknesses in this policy.

Why Microsoft's Active Directory password policy is no longer a viable option.

- The password policy follows a "one size fits all" principle. Administrators find it challenging to set different password policies for different users based on their group or OU memberships within the domain.
- The password policy fails to restrict the use of common password patterns, like asdf, 1234, and qwerty, as well as incremental passwords like password1, password2, password3.
- The password policy cannot prevent dictionary words or usernames from being used as passwords.

Common password attack methods.

81 percent of hacking-related breaches occurred due to either stolen or weak passwords. Hackers are evolving, and apart from implementing technology to help avoid cyberthreats, personal awareness plays a big role in defending against the various mechanisms cybercriminals use to steal credentials (social engineering, phishing, etc.). When it comes to an enterprise-level network compromise, organizations end up paying dearly—both through hefty fines and negative publicity. To help enhance awareness about these issues, this white paper discusses common password theft methods used by hackers, and how simple tweaks can reduce the risk of a password compromise.

Password guessing.

The easiest way to gain access to information is by guessing an end user's password. Many hackers extensively analyze both the keywords used in an organization as well as the keywords used in competitor organizations. Hackers typically string together a set of potential keywords that may be commonly used by employees to get into a company's network. Instead of trying multiple passwords for one user, hackers try the same set of passwords for many users until they eventually get one password right. To their luck, if they happen to land an administrator-level password, the organization is doomed.

How to prevent password guessing.

So, then what's the best way to defend against password guess attacks? Use strict password policies and restrict commonly used patterns. To make it that much harder for cybercriminals to guess passwords, employees should not be allowed to use common words, set weak passwords, or leave a password unchanged for extended periods of time (passwords should be changed every 45-60 days).

Dictionary attacks.

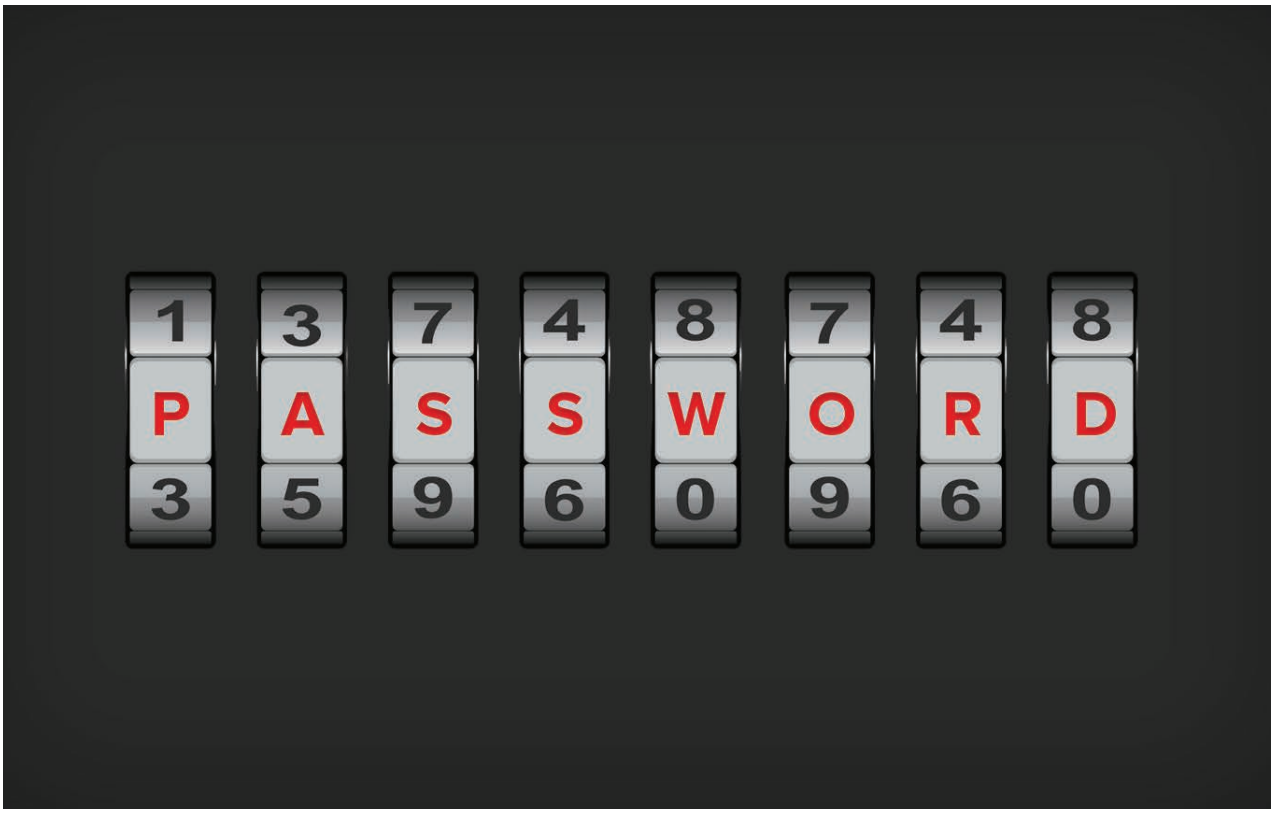
This attack is similar to the password guessing technique. However, in this method, hackers don't have to guess the password. Over the years, thousands of common passwords comprised of dictionary words like letmein, iamadmin, superman, etc. have been consolidated into dictionaries that can be easily accessed by hackers. All they have to do is pick a potential username and automate a script to try each word in the dictionary as the password. With enough time and a strong enough computer, hackers can easily gain access to passwords this way.

How to prevent dictionary attacks.

Restrict common dictionary words and patterns in password policies. If common dictionary words and patterns cannot be used in the password itself, hackers aren't going to find a match from online repositories.

Brute force attacks.

Hackers can gain access to passwords by brute-forcing their way in. That is, they can try millions of password combinations comprised of uppercase letters, lowercase letters, numerals, and special characters. Although this technique is time-consuming and requirers greater computational power, the chance of success is far greater.



How to prevent brute force attacks.

Create stringent password policies. An increase in the length and complexity of passwords by mandating stringent password policies drastically increases the time taken and the computational power required for an attack, rendering brute-force attacks nearly impossible.

Phishing.

An extremely easy way to gain both usernames and passwords is to trick users into giving them up freely. Hackers shoot out clickbait emails with links that look exactly like a popular website, for example a bank site's login page. Without paying heed to the minor change in the URL, users tend to confidently enter their usernames and passwords, sending this sensitive information directly to the hacker. And since most users set the same username and password for many of their applications, once a hacker has one set of credentials, they can easily cause havoc.

How to prevent phishing.

Use Active Directory single sign-on. Hackers can't trick users into entering their credentials in wrong portals if users don't have to enter their credentials at all!

Social engineering.

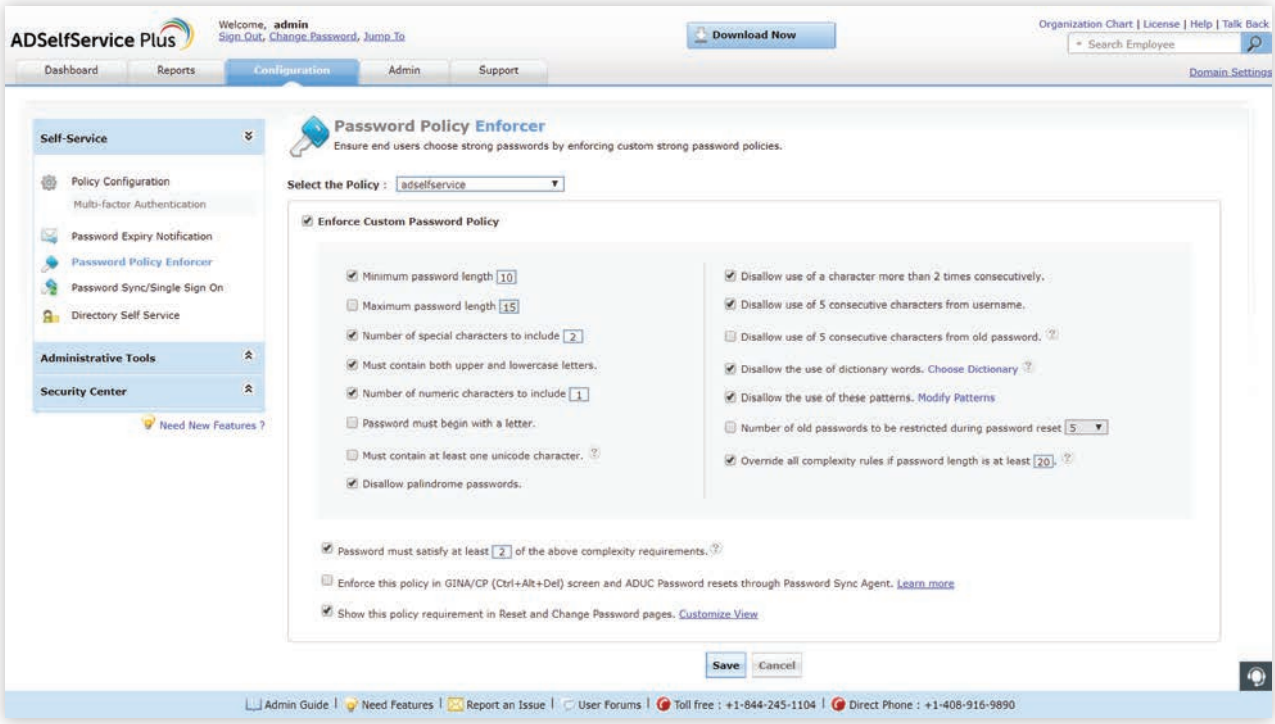
The most traditional way of gaining access to users' credentials is directly asking them. Social engineering is the process of tricking users into committing a security mistake through human interaction. For example: If a hacker pretends to be a network administrator online or over the phone, employees are likely to share their password when asked. Why do people still fall for this? Because even today, end users predominantly have to depend on the help desk to get their password issues resolved.

How to prevent social engineering.

Liberate end users with password self-service. If they can reset their passwords and unlock their accounts themselves, there's no reason they'd feel obliged to share their credentials with administrators.

Using the right tool for implementing these prevention mechanisms.

As we've already established, Active Directory lacks the granular password controls needed to thwart today's hackers, which leaves administrators searching for another way to prevent the use of weak passwords. That search ends now!



ManageEngine ADSelfService Plus is a secure, end user self-service password management solution. It has a wide range of features, allowing administrators to:

- Implement stringent password policies.
- Prevent common dictionary patterns.
- Enable single sign-on for end users.
- Facilitate real-time password synchronization.

Get started with a free trial.

Get started with ADSelfService Plus now, and experience its various value-adding features for yourself. Download your free, 30-day trial.

For small businesses with less than 50 users, ADSelfService Plus is completely free to use—no restrictions.

ManageEngine
ADSelfService Plus

ADSelfService Plus is an integrated Active Directory self-service password management and SSO solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications. ADSelfService Plus supports IT help desks by reducing password reset tickets and spares end users the frustration caused by downtime.

For more information, please visit www.manageengine.com/products/self-service-password.

$ Get Quote Download