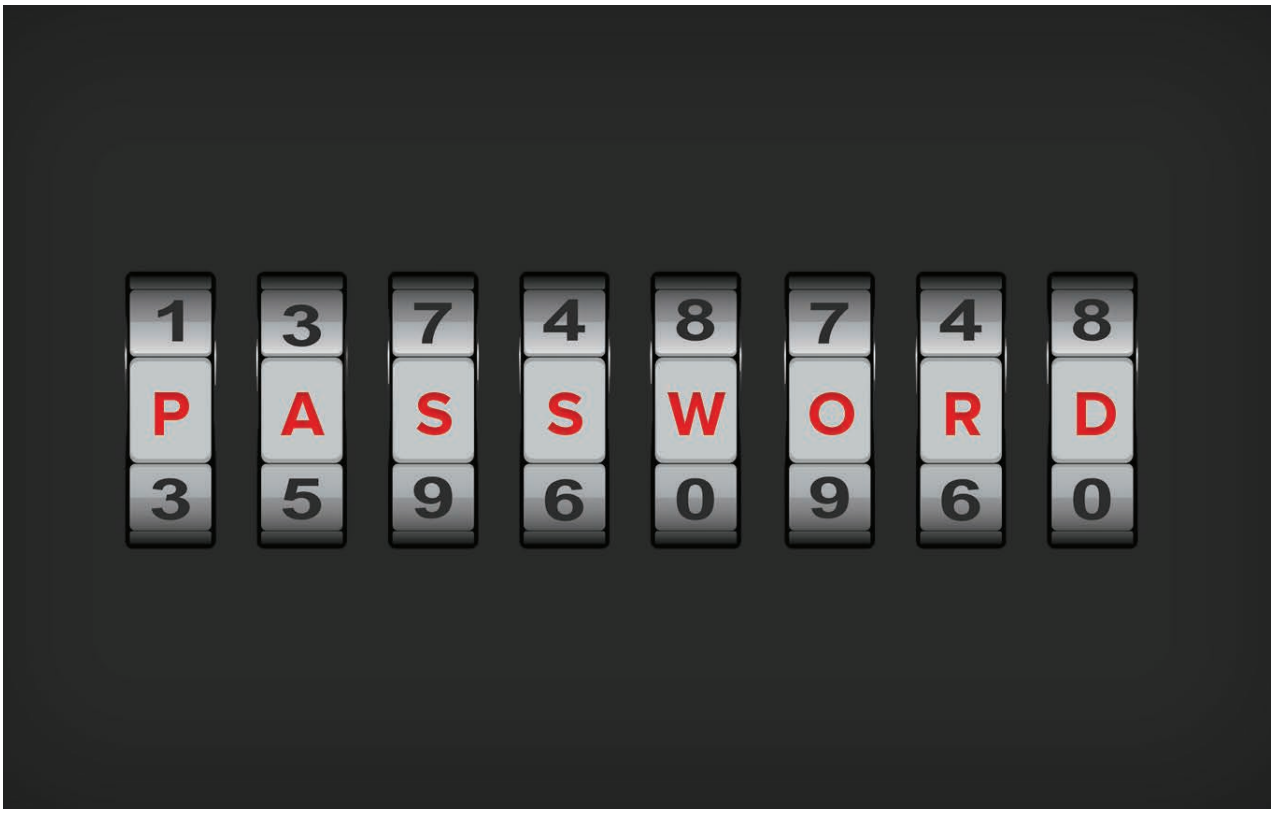
ManageEngine
ADSelfService Plus

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

www.adselfserviceplus.com

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.

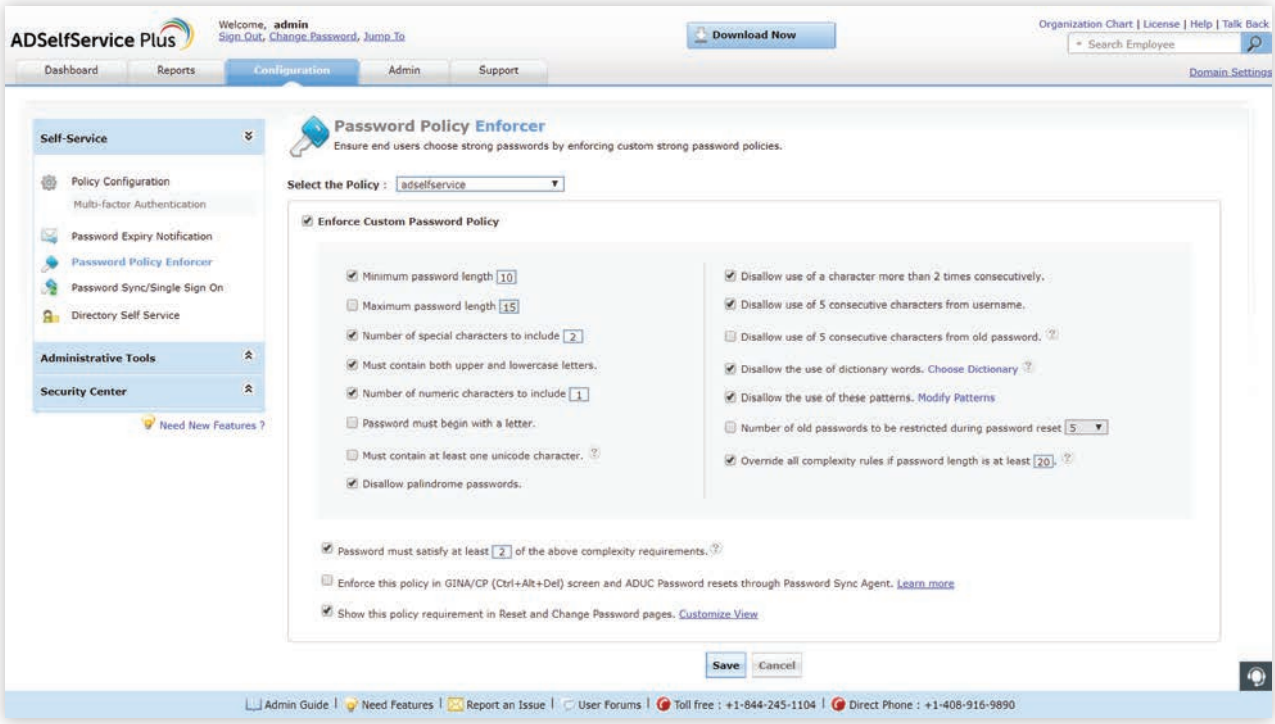
The most traditional way of gaining access to users' credentials is directly asking them. Social engineering is the process of tricking users into committing a security mistake through human interaction. For example: If a hacker pretends to be a network administrator online or over the phone, employees 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