ManageEngine
ADSelfService Plus

Your insider's guide to

# why passwords are here to stay, and how IT teams can stay in control of password management.

www.adselfserviceplus.com

# Table of contents

1. History of passwords ---- 1

a. Different kinds of authentication ---- 1

2. Why passwords are here to stay ---- 1

a. Passwords are completely right or completely wrong ---- 1

b. Passwords are disposable and cannot be used to identify the person ---- 2

c. Passwords are secrets known only to the users ---- 2

3. Why passwords are going to grow in number ---- 3

4. How passwords impact productivity ---- 3

5. Staying ahead of the curve ---- 3

a. What you can do to manage passwords better ---- 3

6. The best solution that helps you stay ahead ---- 4

# 1. History of passwords

In the early 1960s, Fernando Corbató helped deploy the first known computer password. According to The Wall Street Journal, Fernando said he doesn't regret inventing the password, although it does have its flaws. These flaws prompted Bill Gates to famously say at a conference in 2004, *"Traditional password-based security is headed for extinction, because it cannot 'meet the challenge' of keeping critical information secure." However,* we're still using passwords—almost two decades later.

From their invention in the 1960s to now, passwords have come a long way. There has been a drastic yet consistent growth in both the number of passwords each person uses and the number of people who use them around the world. Besides enabling us to log into our computers, passwords today guard all of our digital identities. With so much dependency on passwords, they're far from being eradicated.

## a. Different kinds of authentication

Authentication forms fall into three broad categories:

1. Something the end user "knows"—like traditional passwords or pins.
2. Something the end user "has"—like a physical token.
3. Something the end user "is"—like the user's fingerprint.

While all three categories of authentication are used today, the first is the most commonly used. The second and third categories of authentication usually compliment the first type to provide added security. In this e-book, we discuss why authentication through passwords is here to stay, how organizations will be impacted by the growth of passwords, and how they can strike the right balance between password management, efficiency, and security.

# 2. Why passwords are here to stay

## a. Passwords are completely right or completely wrong

"Password" may seem identical to "pa$sw0rd," but to a computer, they are completely different. This is true for all computers—both a legacy system and the latest supercomputer have difficulty distinguishing between two similar-looking passwords.

The same cannot be said for biometric authentication mechanisms like voice recognition modules, fingerprint readers, or iris scanners. These systems have to account for some margin of error, because biology is not binary in being right or wrong. That is, a finger print or facial structure only has to be good enough to fool the scanner.

For example, the first generation fingerprint readers on smartphones weren't as good as the ones we have today. Their margins of error were a lot higher, and a close-enough fingerprint could still fool the system. Although, the technology has come a long way, fingerprints are still used as a secondary form of authentication rather than the sole form. For example, when users can't use their fingerprints to unlock their phones, they can still log in using their passwords. The fact that password authentication acts as a fail-safe mechanism for fingerprint authentication shows the reliability of the this older process.

## b. Passwords are disposable and cannot be used to identify the person

In 2014, hackers working for the Chinese government broke into computer systems at the Office of Personnel Management and stole the sensitive personal data of more than 22 million Americans—including the fingerprints of 5.6 million people. When biometric passwords are stolen, the security of the end users is compromised for life. There's no way for users to change their fingerprints.

Now, if the authentication method used was passwords, this would cause less damage if stolen, because no personally identifiable information would be falling into the wrong hands. With data regulation laws like GDPR on the rise, companies would much rather have passwords that can be disposed of than rely only on biometric or physical authentication tokens that could prove disastrous if they fall into the wrong hands.

## c. Passwords are secrets known only to the users

In theory, nobody except the end user is supposed to know their password. The same is not the case with authentication tokens or biometrics. After all, anybody could borrow an authentication token, and a fake fingerprint or an illegitimate user's facial structure only has to be good enough to trick the system.

The level of security relies on the quality of the hardware. However, passwords offer the same level of security whether they're entered in a Windows 2000 system or a Windows 10 system. Even if there is a breach, users can easily change the password and move on.

## 3. Why passwords are going to grow in number

According to a report by Cybersecurity Ventures, the total number of passwords belonging to Fortune 500 employees will be 5.4 billion in 2020. On top of this, with the Internet of Things (IoT) becoming increasingly important, the number of passwords is only going to multiply and, in turn, increase many business' attack surface.

While employees have their own login credentials, there's a small number of privileged users (typically IT and system administrators) who have access to hundreds, and sometimes thousands, of login IDs and passwords. A compromised administrator account might give hackers the required ammunition to wreak substantial havoc.

## 4. How passwords impact productivity

For most users, the work day starts with logging in to their systems; entering passwords cannot be avoided. Gartner estimates that 20 to 50 percent of all help desk calls are for password resets, and Forrester Research estimates that the average cost of a single password reset done by help desk is about $70. Password reset operations not only delay the employee's work day, but they also consume a disproportionate amount of the IT team's time and effort, preventing them from investing it in more pressing matters that require their attention.

## 5. Staying ahead of the curve

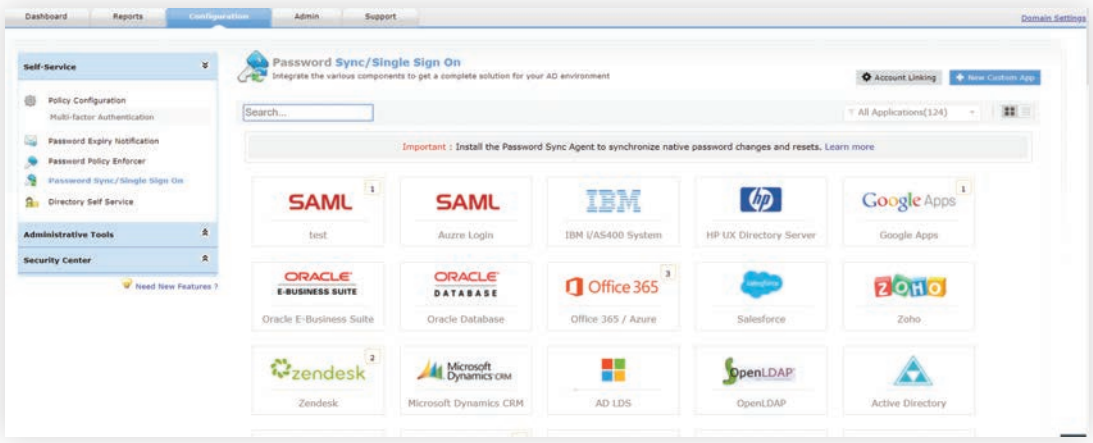
Many organizations once claimed they would go password-less. Even tech giants like Google and Microsoft wanted to kill passwords. Yet, almost two decades later, the primary form of authentication in Gmail and Outlook remains passwords. To stay ahead of the curve, organizations need to implement password best practices so they don't have to worry about their productivity plummeting due to passwords mismanagement.

### a. What you can do to manage passwords better

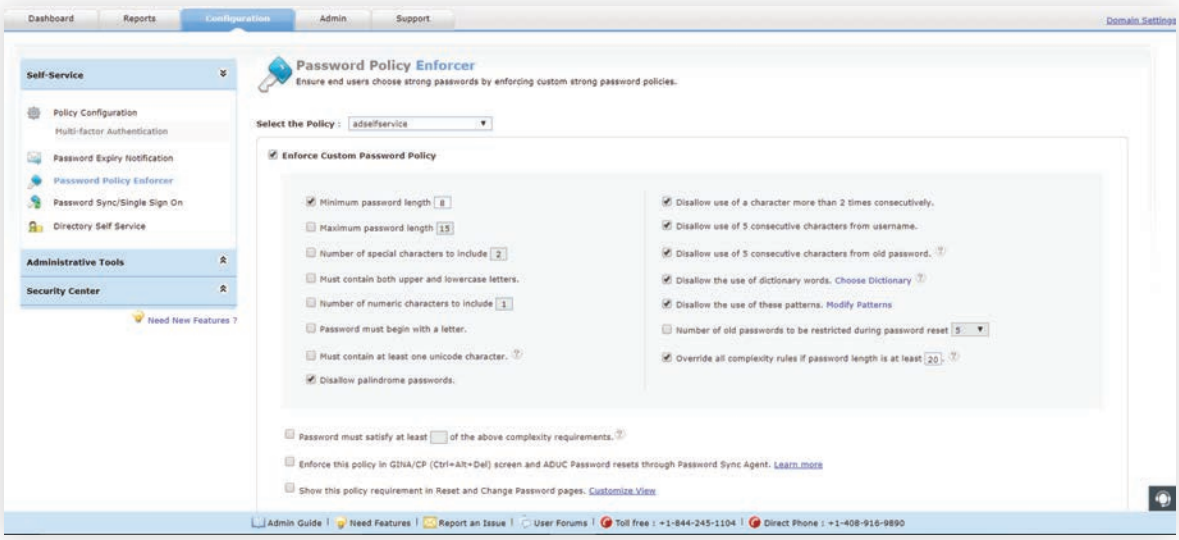
It's difficult for IT administrators to keep tabs on the overwhelming number of passwords. The best way to manage passwords is to implement an effective password self-service solution that empowers users to reset or change their passwords and unlock their accounts by themselves. The solution should establish stringent password policies, offer multi-factor authentication, and provide a good return on investment.

# 6. The best solution that helps you stay ahead

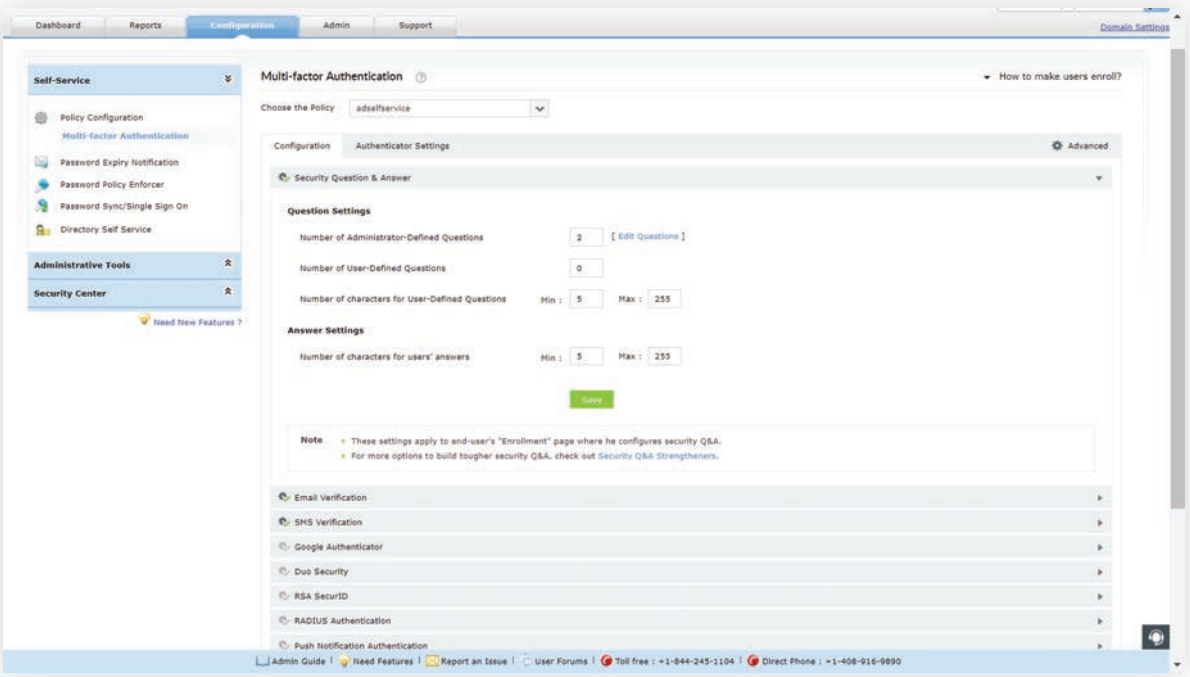
ManageEngine ADSelfService Plus, a secure end-user password management solution, is a great fit. Apart from providing password self-service capabilities, the solution features a password policy enhancer, multi-factor authentication (MFA), and single sign-on (SSO) for seamless access to more than 100 enterprise applications. With ADSelfService Plus, implementing password management best practices is a piece of cake.




Single sign-on to over 100 applications from a central dashboard.




Password policy enhancer in ADSelfService Plus.




Multi-factor authentication in ADSelfService Plus.

**With ADSelfService Plus, administrators can:**

- Empower end users with self-service password reset and account unlock even when they're working remotely.
- Remind end users about their soon-to-expire passwords and accounts, and prompt them to take relevant action.
- Implement one-click logon through single sign-on (SSO) to more than 100 enterprise applications for seamless access.
- Set stringent password policies to ensure strong passwords.
- Enforce multi-factor authentication during Windows logon and during password reset and change operations.
- Implement password policies granularly for users based on their organizational unit (OU) and group memberships.

With so many robust features and affordable pricing, ADSelfService Plus is a no brainer for your organization. No matter the number of users in your organization, ADSelfService Plus has got your covered. What's more, the solution offers a 30-day, free trial of the professional version. No credit card required. No strings attached.

Still skeptical? See for yourself the return on investment your organization can achieve utilizing ADSelfService Plus.