ManageEngine
ADSelfService Plus

Ensure business continuity with a robust password management framework

www.adselfserviceplus.com

Table of Contents

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 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 in to our computers, passwords guard all of our digital identities today. With so much dependency on passwords, they're far from being eradicated.

2. The advantages traditional passwords have over modern authentication methods

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 supercomputers have no 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 fingerprint or a person's facial structure only has to be good enough to fool the scanner.

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

In 2014, hackers working for the Chinese government broke into computer systems at the United States 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; after all, there's no way for users to change their fingerprints. Although stolen passwords could pose a similar threat, users can easily change their passwords, and will not have lost any personally identifiable information that could be traced back to them.

c. Passwords are secrets known only to their users

In theory, nobody except the end user is supposed to know their password. The same can't be said for 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.

3. Where native password policy configurations offered by directory services fall short

Since the early 2000s, Microsoft's Active Directory (AD) and its associated applications have played a critical role in IT management. Enterprises today still rely heavily on AD to manage identities in their IT environments. Despite advances in technology, AD's password policy configurations have remained unchanged for a decade.

1. 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 organizational unit memberships within the domain.
2. 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,” and “password3.”
3. The password policy cannot prevent dictionary words or usernames from being used as passwords.

4. Why password management is important for business continuity

Business operations are controlled to a significant degree by passwords. It's a balancing act between making them memorable for users and ensuring that no password abuse or theft occurs. The business continuity challenges that organizations face include weeding out passwords like “secret,” “1234,” or even just “password”; enforcing privilege-based password protection; and dealing with passwords that have been forgotten.

Why is managing passwords so important?

In theory, nobody except the end user is supposed to know their password. The same can't be said for 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.

a. Even a small breach in the security of an organization can immediately halt its operations and have a financial impact.

b. Often, these breaches are due to password-related human errors that could've easily been avoided. In fact, according to Verizon's 2019 Data Breach Investigation Report, 81 percent of data breaches leveraged either weak or stolen credentials.

While it may seem like these are basic standards that any company would follow, even popular companies like Citrix fall prey to password attacks despite so much emphasis on password security.

5. Password management best practices

a. Implement self-service password reset for end users

The combination of using too many applications and enforcing strong password policies only sets users up to forget their passwords and get locked out of their accounts. Password management solutions such as ADSelfService Plus aim to tackle this issue by securely enabling users to both reset their forgotten passwords and unlock their accounts without contacting the help desk. Users' identities are verified and established securely through:

- Security questions and answers.
- SMS or email-based ID verification.
- Google Authenticator.
- RSA SecurID.
- RADIUS auntication.
- Microsoft Authenticator
- Yubikey Authenticator

ADSelfService Plus also enables administrators to choose to exercise just one or all of these user identification methods for enhanced security.

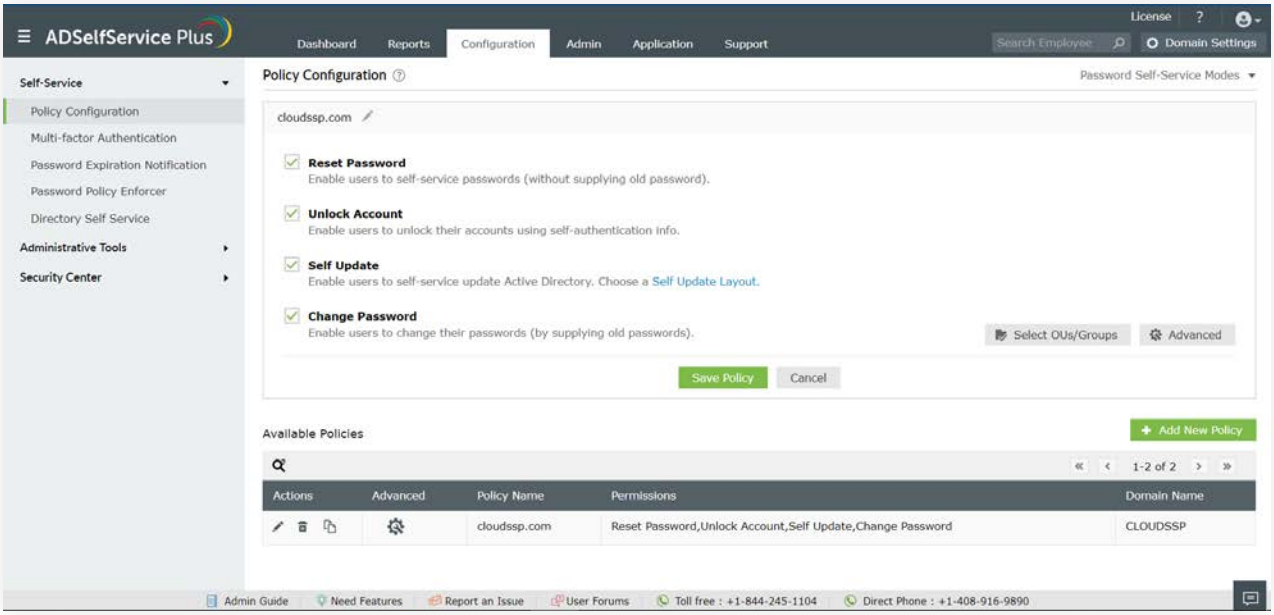

Fig 1: The Policy Configuration tab for self-service password reset in ADSelfService Plus.

Moreover, to reduce the number of passwords in use, IT admins can enable single sign-on to over 100 enterprise applications for end users. Thanks to ADSelfService Plus Administrators also have the flexibility to decide the applications accessible to each user based on their privilege.

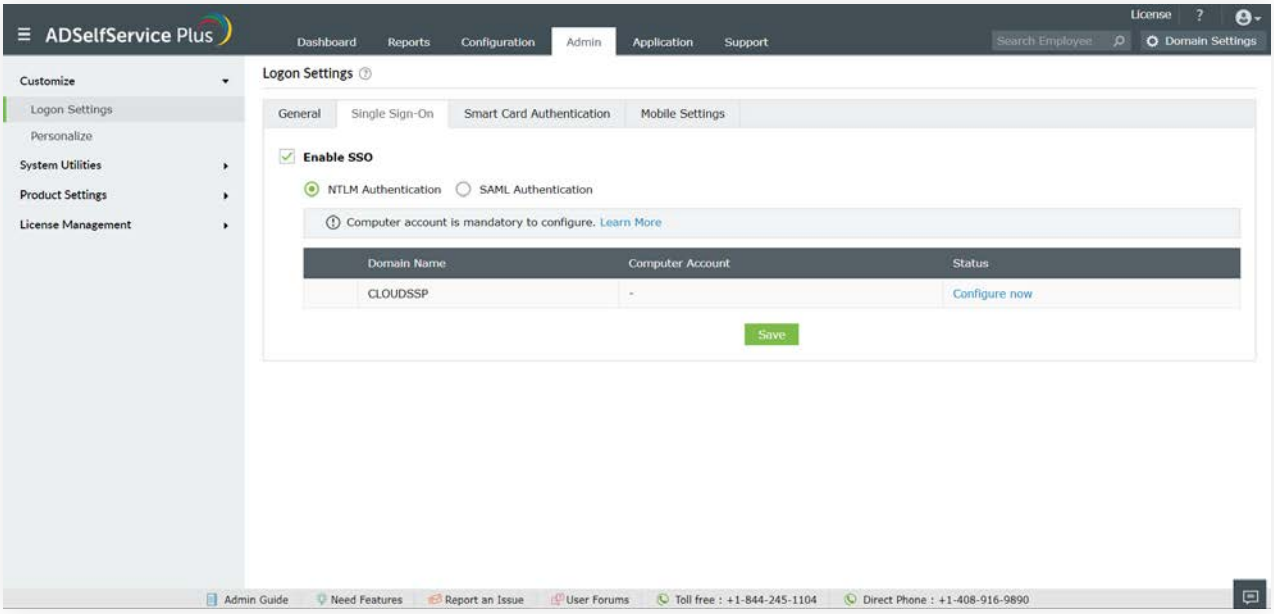

Fig 2: The Logon Settings tab for Single Sign-on in ADSelfService Plus

b. Enforce stringent password policies

AD password policies haven't undergone any major changes in the last two decades, and fall short in all the ways discussed earlier in the e-book. Today's daily business operations require more stringent password policies to prevent common password attacks like dictionary and brute-force attacks. ADSelfService Plus' Password Policy Enforcer helps achieve this goal.

The Password Policy Enforcer allows administrators to:

a. Implement strict password policies and restrict commonly used patterns, like “1234,” “qwerty,” and “asdfgh,” and even palindromes; this makes it harder for cybercriminals to guess passwords.

b. Restrict users from leaving their passwords unchanged for extended periods of time (passwords should be changed every 45 to 60 days).

c. Show the password complexity requirements on the password change screen to help users comply when setting passwords.

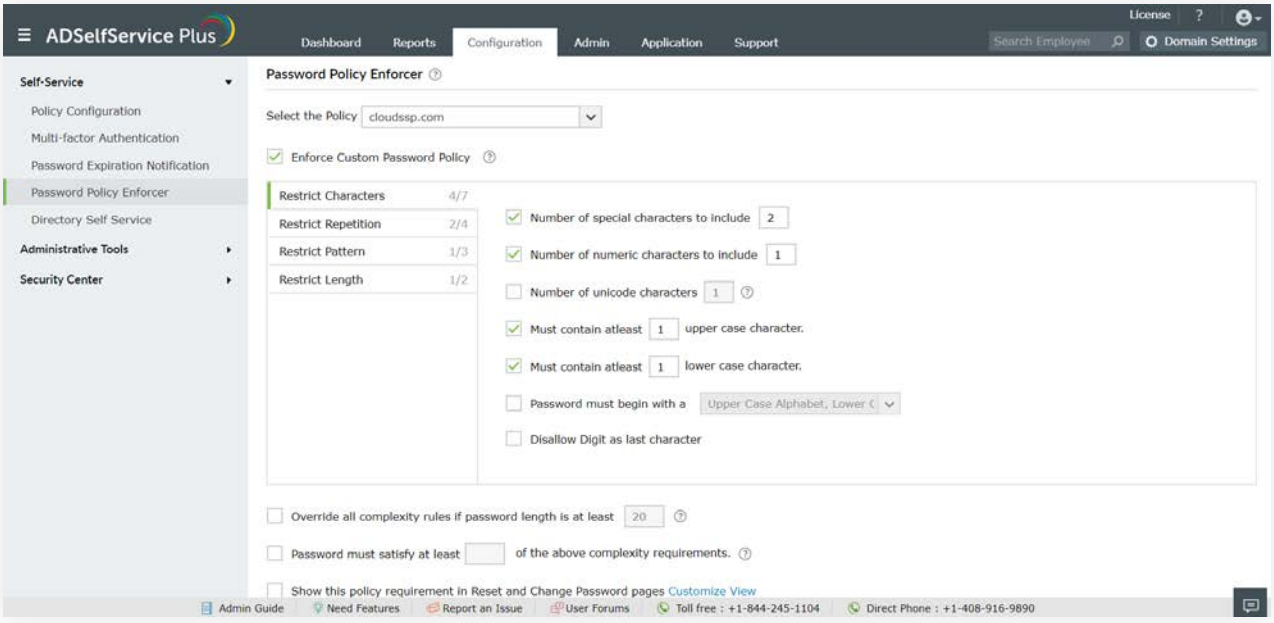

Fig 3: The Password Policy Enforcer tab in ADSelfService Plus

c. Implement two-factor authentication

With two-factor authentication (2FA) in place, even if a hacker steals a user's password, they still need access to the user’s mobile phone or email to successfully hack into the account. ADSelfService Plus supports 2FA for logons to Windows, macOS, and Linux systems.

ADSelfService Plus enables admins to protect user accounts with two levels of authentication during login. Apart from the traditional method of authentication using a username and password, it authenticates users through:

- SMS and email-based verification codes.
- Duo Security authentication.
- RSA SecurID.

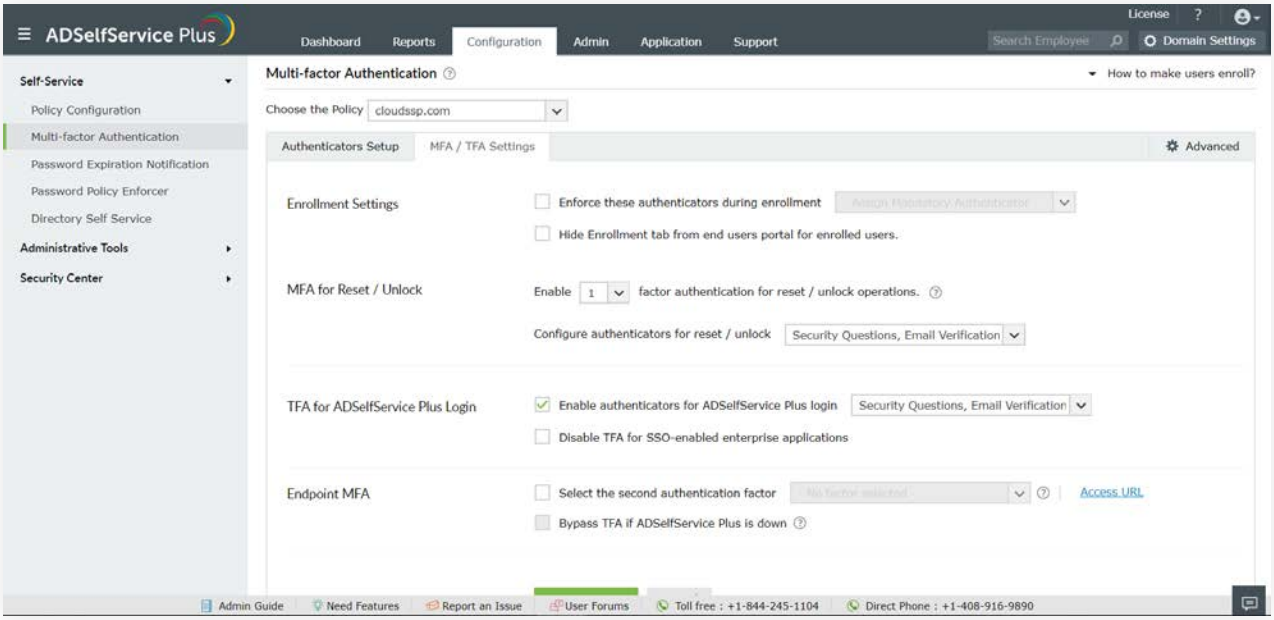

Fig 4: The Multi-factor Authentication tab for two-factor authentication in ADSelfService Plus