ManageEngine
ADSelfService Plus

An insider's tips on essential **password management enhancements to boost productivity**

www.adselfserviceplus.com

Table of contents

1. Introduction

When it comes to guarding the digital identities of users, passwords have stood firm against the test of time for over two decades. Although a few organizations like Microsoft have claimed that they're going to eliminate passwords, they've never been able to completely replace passwords for authentication, and the replacement doesn't seem to be coming anytime soon. Moreover, with the advent of the Internet of Things (IoT), or the extension of the internet into physical devices, the number of passwords is going to increase exponentially.

2. What the increase in passwords means for IT admins

Password management is a large part of an IT admin's workday. They have to keep tabs on everything from basic password change operations to setting the right password policies—and that's just the tip of the iceberg. Admins also have to account for frills like multi-factor authentication, remote logons, single sign-on, and password synchronization. With the rise in the number of passwords, the workload of IT admins is also increasing multifold; this means organizations require more support staff to handle password requests, such as password resets and account unlocks, leading to inflated support costs, loss of valuable time for IT staff, and a drop in productivity. On the other hand, being understaffed can cause users to get stuck and be unable to reset their password or regain access to their locked account, decreasing productivity. For large organizations, this problem can spiral out of hand very quickly.

3. The reality of password management

According to Gartner, over 40 percent of help desk calls are for password resets, and Forrester Research estimates that the average cost of a single password reset performed by a help desk is about $70.

Smart IT admins optimize their routine by automating these mundane password management tasks with the help of a third-party tool. However, with an overload of solutions available in the market, choosing the right password management solution can be a tough decision. The ideal password management solution should reduce manual efforts for all password operations, without taking a chunk out of already stretched IT budgets.

4. Essential features for a password management solution

A password management solution should at least possess a few features to help admins with all of their day-to-day password management activities. The features below address all the critical password touchpoints, from an employee logging in to a system to accessing different applications from a single console.

1. **Self-service password reset and account unlock**
2. **Two-factor authentication for Windows logons**
3. **Single sign-on**
4. **Multi-factor authentication during single sign-on**

5. ADSelfService Plus—a solution with all the essential features

ADSelfService Plus is a secure, web-based password management portal that comes with all the above mentioned features and more, right out of the box. This solution is very competitively priced, and will put an end to mundane password management tasks that steal the valuable time of IT admins.

5.1 Self-service password reset and account unlock

ADSelfService Plus allows end users to reset their domain passwords in Windows Active Directory (AD) remotely from a web browser. This not only reduces the number of password tickets coming into the help desk, but also enhances the productivity of the end user by averting downtime caused by waiting to get access to their account due to a forgotten password.

Your domain users can reset their passwords in four simple steps.

Step 1: Access the self-service portal from the logon prompt.

Step 2: Enter the domain username.

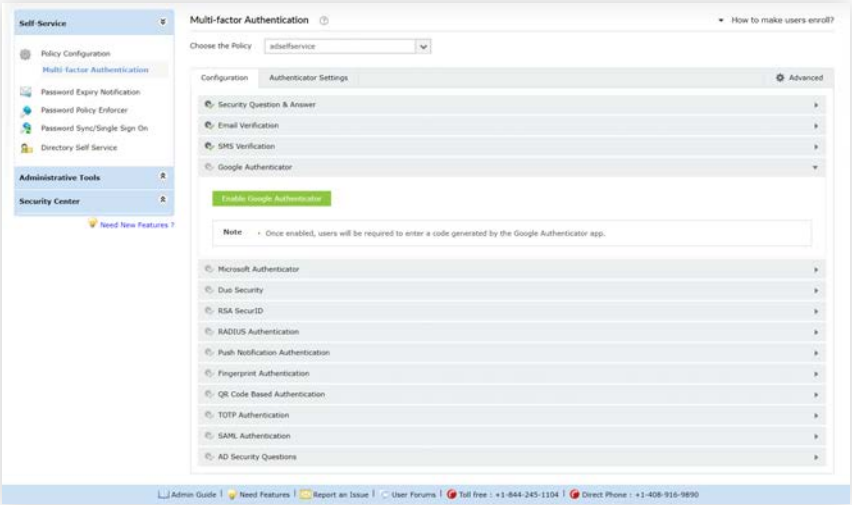
Step 3: Answer the security questions.

Step 4: Reset the domain password.

Self-service password reset steps in ADSelfService Plus.

ADSelfService Plus also saves users from frustrating and unproductive waits for the help desk to unlock their locked out accounts. This self-service account unlock tool allows end users to manage accounts on their own and securely unlock their account from a web console by answering a set of validation questions, all without revealing their identity.

Since users are authenticated by one or more methods for every password reset and account unlock, the process is very secure. Additionally, a timer is in place to thwart attacks like brute force, requiring the users to perform the change, reset, or unlock before the timer runs out.



Multi-factor authentication in ADSelfService Plus for self-service password resets and account unlocks.

5.2 Two-factor authentication for Windows logons

With ADSelfService Plus' Windows logon two-factor authentication (2FA) feature enabled, users have to authenticate themselves in two successive stages to access their Windows machine. The first level of authentication is through something they know: their usual Windows credentials. The second level of authentication—something they have—can be through one of the following:

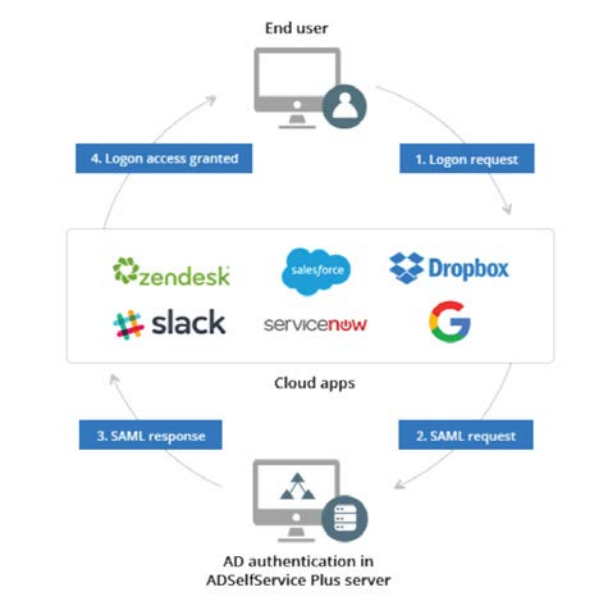
1. SMS or email-based verification codes.
2. DUO Security.
3. RSA SecurID.
4. Remote Authentication Dial-In User Service (RADIUS).

This feature ensures that there is no risk to sensitive data, even in cases where passwords are compromised. For example, if an unauthorized user gains access to a user's password, they still need access to that user's phone or email to get the verification codes. Moreover, the SMS and email-based verification codes, as well as the authentication codes from Duo Security and RSA SecurID, are unique to each user. These codes can also only be used once, and will expire if they aren't used within a certain period of time.

Windows logon 2FA in ADSelfService Plus.

5.3 Single sign-on

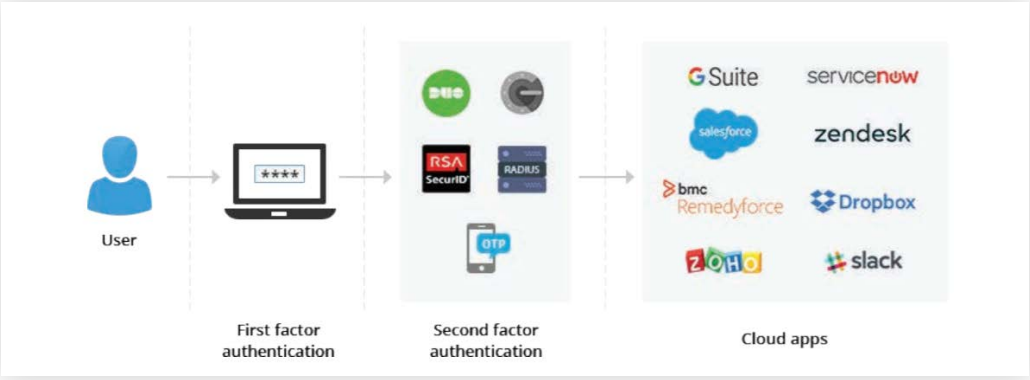
ADSelfService Plus provides users with seamless, one-click access to over 100 enterprise applications. Users simply need to log in to ADSelfService Plus, which acts as the identity provider for single sign-on (SSO). Once logged in, users are presented with a dashboard that lists every cloud application they have access to, and can access each application without having to enter their username and password again.



SSO flow in ADSelfService Plus.

5.4 Multi-factor authentication during SSO

ADSelfService Plus protects access to cloud applications with multi-factor authentication (MFA). When SSO is enabled, users must always authenticate themselves in ADSelfService Plus—first using the tried and tested Windows AD domain credentials, and then using another factor chosen by the admin. For the second factor, ADSelfService Plus supports native factors such as SMS or email-based verification codes, as well as third-party authentication providers such as Duo Security, RSA SecurID, RADIUS, and Google Authenticator.

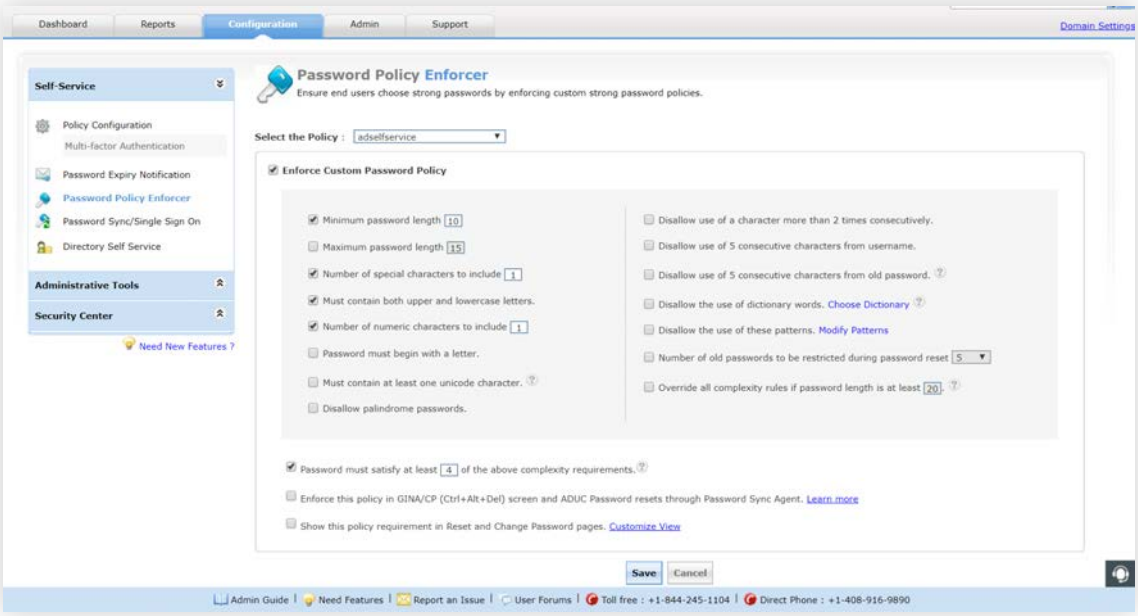


SSO protected with MFA in ADSelfService Plus.

6. Other noteworthy features of ADSelfService Plus

6.1 Password policy enhancer

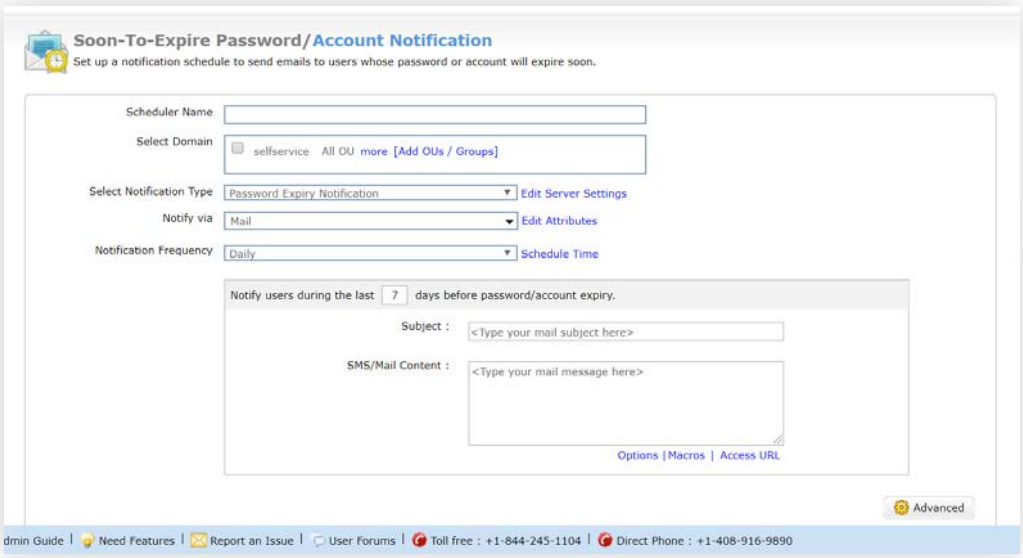
Native AD password policies haven't changed in over two decades. These policies are not stringent enough to prevent even common mishaps like the allowance of dictionary words, incremental passwords, or specific patterns. ADSelfService Plus' password policy enhancer helps overcome the shortcomings of native AD password policies by allowing admins to set stringent password policies to enhance security.



The password policy enhancer in ADSelfService Plus.

6.2 Password expiration notifier

The native Microsoft pop-up that reminds users of their soon-to-expire passwords or accounts seldom gets the job done. Users simply ignore the pop-up, or worse, just close it without paying attention to the message itself. These users will eventually find themselves shut out of their accounts once their password or account expires. To prevent this, ADSelfService Plus allows admins to send out scheduled, customized emails or SMS alerts that remind users about their soon-to-expire passwords or accounts.



The password expiration notifier in ADSelfService Plus.

7. Why ADSelfService Plus is worth it

ADSelfService Plus is a comprehensive password management tool that helps admins with their everyday password management tasks. It's packed with thoughtful features that provide 360-degree support through all critical password touchpoints, including logons, SSO, and password change/reset operations. Furthermore, ADSelfService Plus' extremely competitive pricing makes it a no-brainer for IT admins.

Don't believe us? Check out the ROI on installing the solution.