ManageEngine
ADSelfService Plus

The administrator's guide to simplifying password management

www.adselfserviceplus.com

Table of contents

1. Introduction ---- 1

2. Problems caused by password mismanagement ---- 1

2.1 Operational problems ---- 1

2.2 Security problems ---- 1

3. Simplifying password management by implementing password services through ADSelfService Plus ---- 2

3.1 Why ADSelfService Plus ---- 2

3.2 Password self-service and account unlock ---- 2

3.3 Password and account expiration reminders ---- 3

3.4 Password policy enforcer ---- 3

3.5 Single sign-on ---- 4

4. About ADSelfService Plus ---- 5

1. Introduction

Many organizations today rely on Active Directory (AD) to manage their IT environments. Although AD has improved considerably over the last two decades as a directory service, there are still several gaps that need to be filled.

One of those gaps is in the policies that govern passwords. For example, if your regular business operations require the use of multiple applications, signing in once to gain access to all of them would be save your employees a lot of time and effort. With single sign-on (SSO), users can access all their work applications by logging in just once.

AD falls short in a few other aspects, as well; for instance, you can't reset passwords, unlock accounts, prevent password expiration, or set up strong password policies. In a nutshell, AD hasn't evolved to meet today's complex IT requirements, which means enterprises need a third-party solution that can fill the gaps left in AD.

2. Problems caused by password mismanagement

2.1 Operational problems

When users forget their passwords or need to unlock their accounts, they have to contact the help desk. In fact, according to HDI, in over a third of support centers, password reset-related tickets accounted for over 30 percent of all support tickets. These types of tickets not only increase support costs and user downtime, but they also eat up the help desk's time, turning its focus away from other critical operational issues that require attention.

2.2 Security problems

As the number of applications increases, the number of passwords users have to remember also increases. Because of this, users often resort to extremely unsafe practice like:

- Using the same password for all the business applications they use.
- Using weak passwords that are easy to remember.
- Writing down their passwords. and even
- Sharing passwords with colleagues.

According to Verizon's 2018 Data Breach Investigations Report, 81 percent of hacking-related breaches leveraged weak or stolen credentials. Data breaches and other attacks often result in loss of information and negatively affect your organization's reputation. This is why both users and administrators need to take ownership of password security.

3. Simplifying password management by implementing password services through ADSelfService Plus

3.1 Why ADSelfService Plus

ADSelfService Plus is a comprehensive solution that enhances the password management experience. It's a complete password management solution offering features like password self-service, self-account unlock, a password policy enforcer, single sign-on, and much more. Best of all, you can get all these features at a price that won't break your budget.

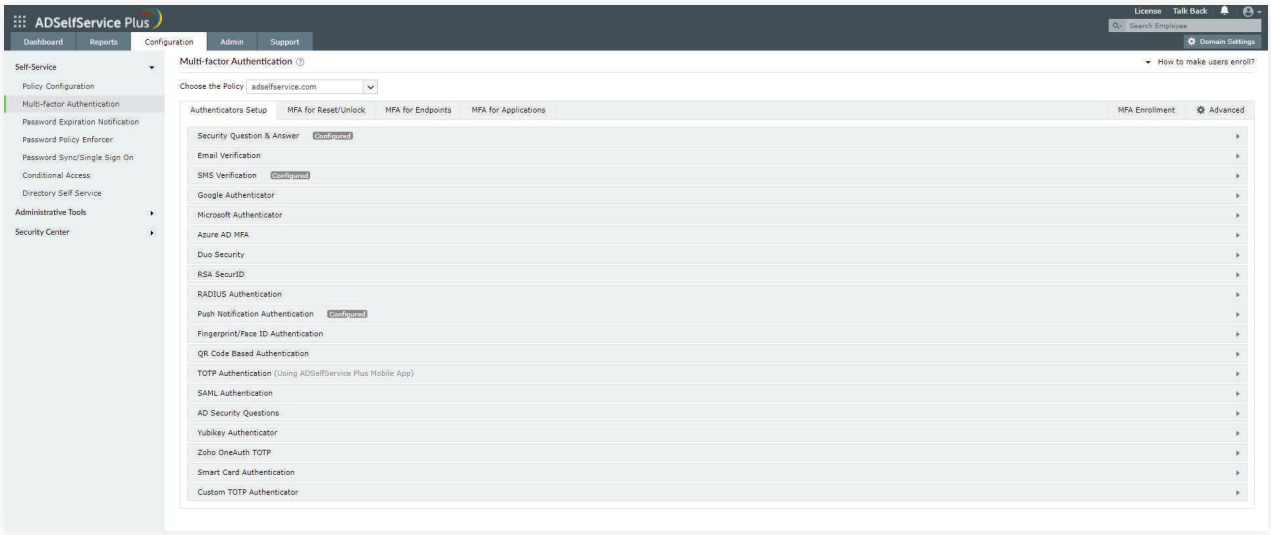
To evaluate the product, you can request a personalized demo, or download a free, 30-day trial of ADSelfService Plus. You can also use our ROI calculator to check how much money you can save by implementing ADSelfService Plus in your organization.

3.2 Password self-service and account unlock

Using too many applications combined with strong password policies only sets users up to forget their passwords and get locked out of their accounts. ADSelfService Plus tackles this issue by securely enabling users to reset their forgotten passwords as well as unlock their accounts without contacting the help desk.

User identities can be securely verified through:

- Security questions and answers
- SMS or email-based ID verification
- Google Authenticator
- RSA SecurID
- RADIUS Authentication
- Mobile Authenticator



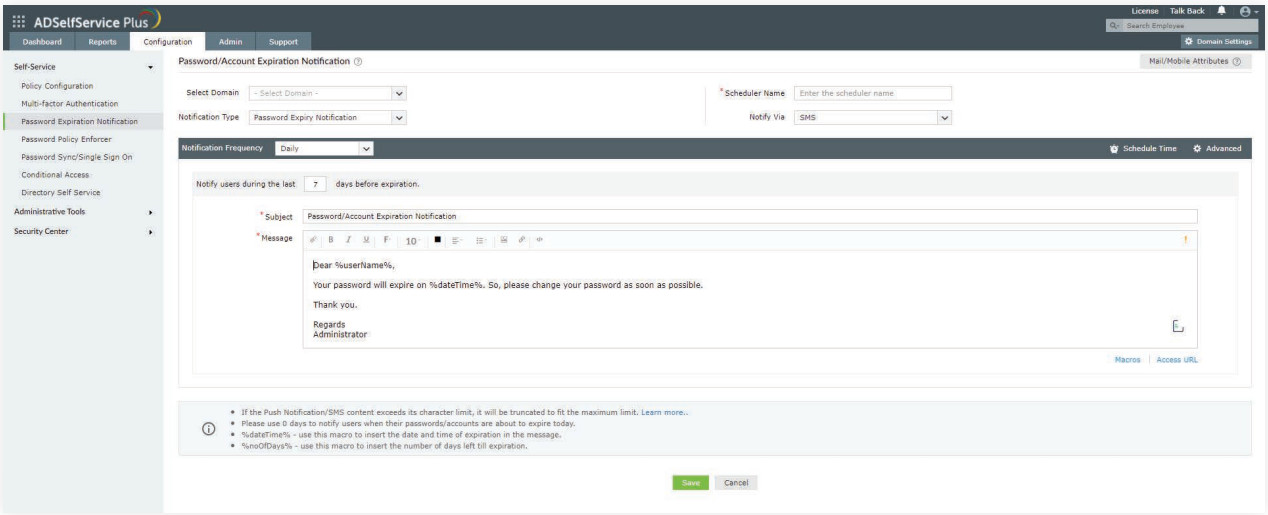
Administrators have the option to exercise one or all of these user identification methods for enhanced security.

3.3 Password and account expiration reminders

One way to mitigate the issue of users being locked out of their accounts when their passwords expire is by sending them reminders well in advance. Of course, there are always those employees who procrastinate or forget. For these users, ADSelfService Plus' Password Expiration Notifier will keep sending reminders until the account or password is reset.

Some highlights of the Password Expiration Notifier:

- Administrators can customize reminder emails. For example, choose a more imperative tone when the expiration date draws closer.
- Both end users and managers can receive notification about user account expiration.
- Notifications can also be sent via SMS.



What's more? ADSelfService Plus' Password Expiration Notifier is now free for an unlimited number of users.

3.4 Password policy enforcer

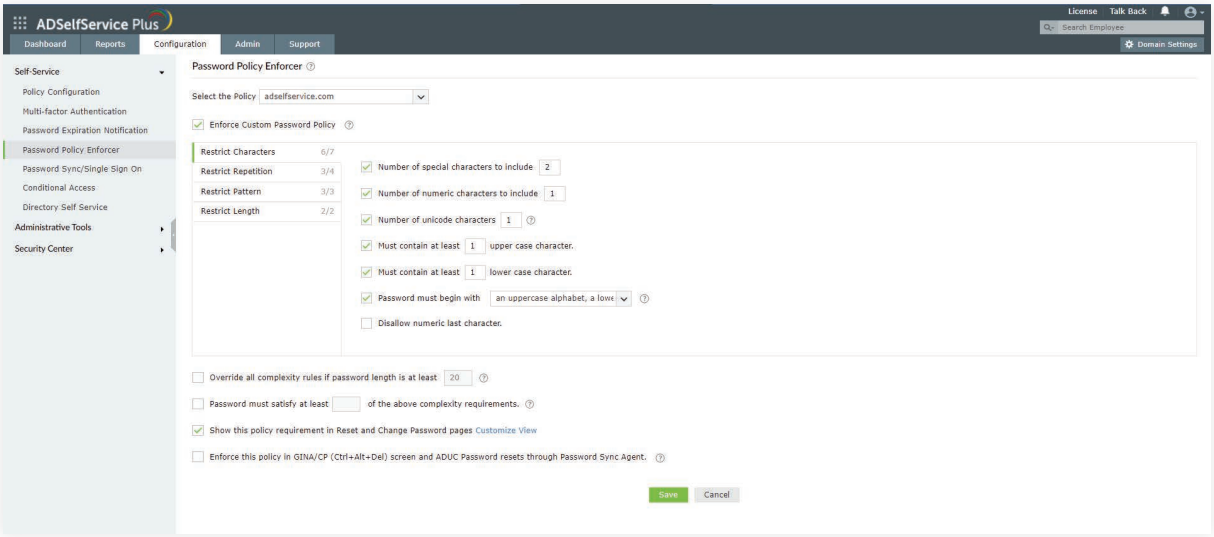
AD's password policies haven't undergone any major change in the last two decades and fall short in the following ways:

- Password policies (including fine-grained password policies), fail to work with the organizational unit (OU) structure that organizations have built and rely on every day.
- They fail to prevent cliched passwords like incorrect, password, letmein, etc. from being set as passwords.
- They fail to prevent incremental passwords like password1, password2, password3, and so on.

Today's typical everyday operations require more stringent password policies. The password policies should be enabled so that common password attacks like dictionary and brute force attacks can be prevented. For such requirements ADSelfService Plus' password policy enforcer hits the mark.

The password policy enforcer allows administrators to:

- Use strict password policies and restrict commonly used patterns like 1234, qwerty, asdfgh, and even palindromes to make it harder for cyber criminals to guess passwords.
- Restrict users from leaving their passwords unchanged for extended periods of time (passwords should be changed every 45 to 60 days).
- Show the password complexity requirements on the password change GINA screen to help users comply when setting passwords.



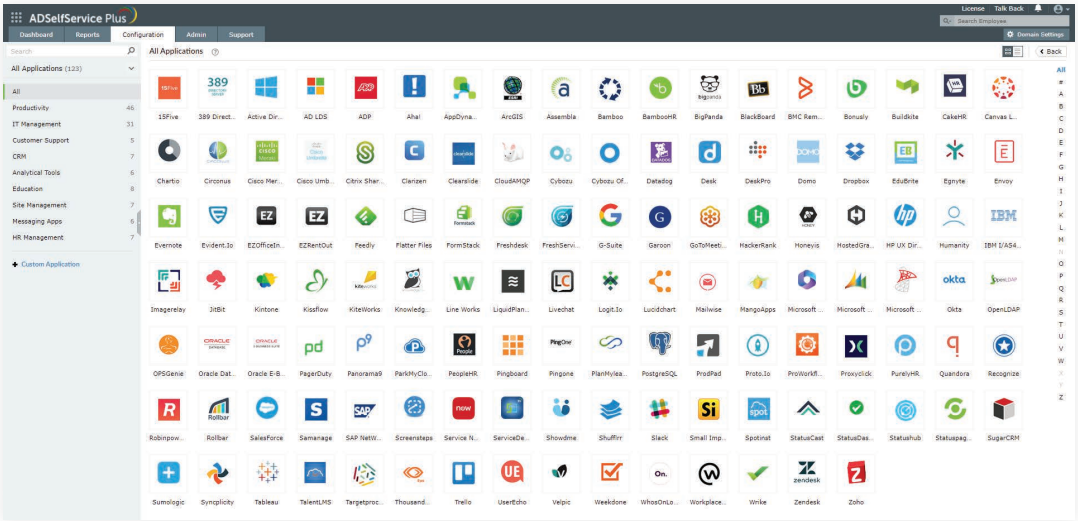
3.5 Single sign-on

Businesses today use a variety of critical applications that are either deployed on-premise or in the cloud. Having to log in to each application separately with a different set of credentials negatively effects the employee experience. The higher the number of applications in use, the more likely users are to mix up passwords and get locked out of their accounts, resulting in more help desk calls and lower productivity.

ADSelfService Plus' single sign-on (SSO) feature is a great way to address these concerns. With SSO, users can seamlessly access over 100 applications with a single click.

ADSelfService Plus' SSO feature offers:

- Restricted access based on OU/group memberships and specific user attributes.
  The flexibility to choose the attribute for account linking between AD and cloud applications.
- SSO support for both service provider (SP) and identity provider (IDP) initiated flows.
- SSO support for any SAML 2.0 application, whether it's internally developed, custom built, or from a third-party service provider. You also gain built-in support for over 100 enterprise applications like G Suite, Office 365, Salesforce, and more by default.
- Multi-factor authentication using a variety of mechanisms like Duo Security, RSA SecurID, and more for both SP and IDP-initiated logins.
- Multiple configurations within ADSelfService Plus for each SSO-supported application.



Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus, www.manageengine.com/products/self-service-password.

$ Get Quote Download