ManageEngine
ADSelfService Plus

Buyer's guide
Self-service password reset solution

www.adselfserviceplus.com

Liberate your IT team with self-service.

If you're part of your organization's IT team, you've probably heard a few grumbles about password reset calls. Due to the time needed to verify user identities and reset passwords in the target IT system or application, password reset calls can severely reduce help desk productivity.

According to a 2018 Forrester report, several large organizations spend over $1 million on resolving password-related help desk calls. To cut down on this expense, IT decision makers can invest in a self-service password management solution that reduces help desk workload, ensures end user productivity, and improves password security. That said, finding a solution that satisfies your IT team and your end users is no easy task.

This document takes a hard look at the barriers to the success of a self-service password management solution.

The million dollar question:

Is your organization spending a huge amount on resolving password-related tickets?

Did you know?

20% to 50% of all help desk tickets are for password resets.

1% of your employee base raises a password reset ticket every day.

53% of admins feel that they still get too many password reset calls.

Password self-service to the rescue.

Deploying an effective password solution can bring the number of password reset tickets down to zero.

Key barriers to the success of a self-service password management solution.

1. Access points

With the prevalence of bring your own device (BYOD) policies and cloud applications, the days of users solely using Windows PCs are long gone. It's common for end users to use macOS, Linux, and their mobile devices. In many ways, this trend is forcing IT teams to rethink the utility of a password self-service solution.

Organizations need a solution that allows users to reset passwords from multiple access points. These access points can be users' mobile devices, the login screen of their workstation, or even a web portal, which is the default option in most solutions.

Evaluation criteria: Can users reset passwords anywhere, at any time?

Users should be able to reset their passwords regardless of whether they are:

1. **In the office.** Enable password resets via the login screen of users' workstations (Windows, macOS, and Linux).
2. **On the move.** Empower users to perform password resets from mobile devices.
3. **At home.** Allow users to update cached credentials in their workstation.

2. Monitor user activities

With growing cybersecurity threats, a self-service password management solution should go beyond its core features and provide insights into the users' password management activities. It should generate a comprehensive report that details every user's password self-service actions and should be able to send notifications about self-service activities. It should also integrate with help desk solutions to ensure accountability for password management actions and SIEM solutions to keep potential insider threats at bay.

Evaluation criteria: What are the solution's monitoring capabilities?

The solution must offer provisions to:

1. **Audit logs.** Support integration with SIEM and syslog solutions.
2. **Mitigate insider threats.** Get reports on identity verification failures.

3. Adoption rate

To eliminate unauthorized attempts to perform self-service actions, password self-service solutions should initially validate users' identities before performing the self-service actions. User identities can be verified with the information provided during the enrollment process. Typically, users enter their mobile numbers, email addresses, verification codes, or other details to complete the enrollment process. Though verifying user identity via the information provided during the enrollment process is a great way to keep cybercriminals in check, there's a catch.

If the enrollment process proves to be too complex, users might decide not to enroll at all, and they'll keep calling the help desk to reset passwords, leaving you back at square one.

To maximize user adoption and ensure an immediate return on investment, your password self-service solution must offer provisions to automate and force the enrollment process.

Evaluation criteria: Does the solution offer a hassle-free onboarding process?

The solution must allow IT admins to:

1. **Upload enrollment data.** Automate user enrollment by importing data.
2. **Send alerts.** Send multiple enrollment reminders to users via SMS and email.
3. **Force users to enroll.** Enforce enrollment when users log in to their workstation.
4. **Preload user profiles.** Utilize users' existing Active Directory (AD) information for enrollment.

4. Verify user identity

Different sets of users are comfortable with different authentication techniques. Giving a hardware token to users who have only been using one-time passwords (OTPs) to verify their identity will generate a lot of complaints. Also, some users have access to sensitive or critical business data. So it makes sense to use different sets of authentication techniques for different users, as opposed to enforcing, say, three standard authentication techniques across the entire organization.

For example, you must have the flexibility to enforce three levels of authentication for remote users (e.g., push notification, Google Authenticator, and security Q&A), two levels for users inside the LAN (e.g., OTPs and tokens), and one level of authentication for C-level executives (e.g., biometrics).

The solution you choose must strike a balance between usability and security. It should be able to support the latest and most sophisticated authentication techniques, with the provisions to enforce different authentication techniques for different sets of users.

Evaluation criteria: How stringent are the solution's supported authentication techniques?

The solution must allow IT admins to:

1. **Enforce multiple authentication techniques.** Enforce specific multiple authentication techniques depending on the users' privileges for self-service password resets and account unlocks.

2. **OU and group-based enforcement:** Enforce specific authentication techniques for users based on OUs and groups.

5. Enforce strong passwords

Microsoft's native password policy controls are nearly two decades old, and they're filled with a lot of security loopholes. For example, AD does not enforce password history during password resets. This security loophole lets users configure weak, easy-to-remember passwords for their business accounts, which can put the entire organization at risk by exposing network resources to the outside world.

The ideal solution must be able to patch potential security loopholes in the native password policies; enable admins to configure custom password policies with comprehensive controls; and ensure users set strong passwords as well.

Evaluation criteria: How strong is the enforced password policy?

The solution must allow IT admins to:

1. **Ban common passwords.** Enforce a custom password policy with advanced password policy controls to ban common passwords, patterns like @123, and more.

2. **Maintain the security stance of your organization.** Apply a centralized password policy to both on-premises and cloud apps in your organization.

3. **OU and group-based enforcement.** Implement different levels of password controls to different sets of users.

4. **Help users set strong passwords.** Display the enforced password rules on the password reset and change screens.

Did you know?

18% of admins employ a lenient password policy fearing password reset calls.

Other considerations

The solution must also allow IT admins to:

- Synchronize passwords in real time.
  Instantly synchronize password changes and resets from Windows AD with on-premises and cloud applications.
- Enable self-service password resets for cloud applications.
  Allow users to reset passwords of their cloud accounts, including Office 365, G Suite, Salesforce, and Zendesk, in addition to their AD account.
- Secure network resources with MFA.
  Protect your organization's network by securing all remote and local accesses to machines (Windows, macOS, and Linux), VPNs, and OWA with MFA.
- Implement conditional access.
  Automate access control decisions for self-service features, MFA, and SSO based on risk factors such as IP address, device, business hours, and geolocation.
- Manage group memberships.
  Manage outdated user profiles and group memberships.
- Manage user licenses.
  Reclaim licenses from inactive users and utilize them.

Why choose ADSelfService Plus?

- Self-service password reset and account unlock:
  Allow users to securely reset passwords and unlock accounts for Windows AD, Office 365, and other applications in a matter of seconds.
- Granular password policy enforcer:
  Enforce password policies across Windows and enterprise cloud apps with advanced filters to blacklist dictionary words, patterns, etc.
- Password expiration notifier:
  Warn users about their imminent password expiration via SMS, email, and push notifications.
- Real-time password synchronizer:
  Enable users to use just one password for multiple enterprise applications.
- Enterprise SSO:
  Offer seamless access to any SAML-based enterprise application via AD-based SSO.
- Multi-factor authentication (MFA):
  Secure every self-service action; Windows, macOS and Linux login; and enterprise application login with additional layers of authentication.
- Real-time alerts: Send notifications to users via email, SMS, or push notification for password resets and account unlocks.

ADSelfService Plus: The intelligent choice.

ADSelfService Plus is an integrated self-service password management and single sign-on (SSO) solution for AD and other enterprise applications.

A shift in power.

Empowering users to manage their passwords on their own paves the way to a new era in IT management. Go ahead and try ADSelfService Plus free for 30 days, and see how all these features can bring a positive change to your organization.

Scalability guide.

Can ADSelfService Plus scale to any enterprise environment and meet the demands of the ever-changing IT landscape? Click here to find out.