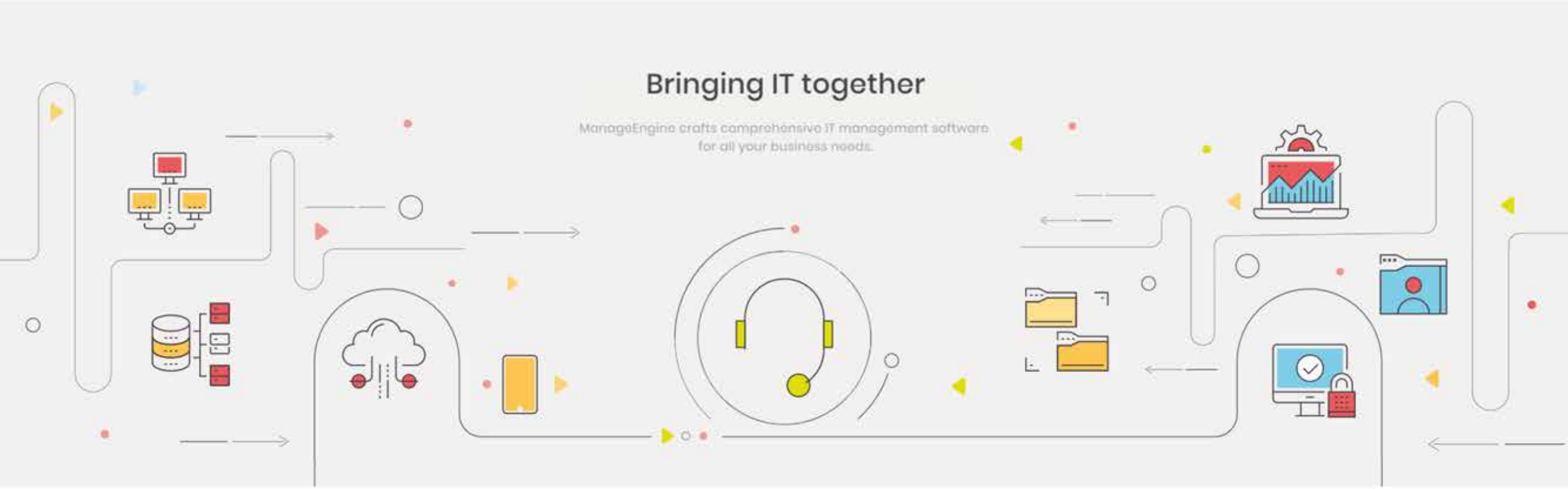


ManageEngine

ADSelfService Plus

Solutions offered by ADSelfService Plus.

Self-Service Password Management

Self-service password reset and account unlock. Password and account expiration notifier

Endpoint Security

Password policy enforcer and endpoint multi-factor authentication (MFA).

One Identity

Enterprise single sign-on (SSO) and real-time password synchronizer.

Download Now

Highlights of **self-service password management**

1. **Password self-service, anywhere, at any time:** Enable users reset passwords and unlock accounts in office, at home, and on the move.

2. **Password/account expiration notifer:** Automate password and account expiration reminders to users via email, push, and SMS alerts.

3. **Force password change:** Force users to change their password at the next logon after a password reset by the help desk admin.

Highlights of **endpoint secuity**

1. **Endpoint MFA:** Secure remote and local machine (Windows, macOS, and Linux), VPN, and OWA logons with advanced MFA techniques like biometrics or QR codes for local and remote access to network resources.

2. **Custom password polices:** Ensure strong user passwords across all their business accounts with advanced password policy settings.

3. **Comply with regulatory mandates:** Helps comply with NIST SP 800-63B, FFIEC, GDPR and HIPPA regulations.

Highlights of **one identity**

1. **Enterprise SSO:** Allow users to access multiple enterprise applications with just one identity.

2. **Real-time password sync:** Synchronize Active Directory (AD) password resets and changes with connected enterprise applications in real time.

Other highlights.

1. **Directory Self-Update:** Enable users to update their information like their phone number, email address, etc in AD.

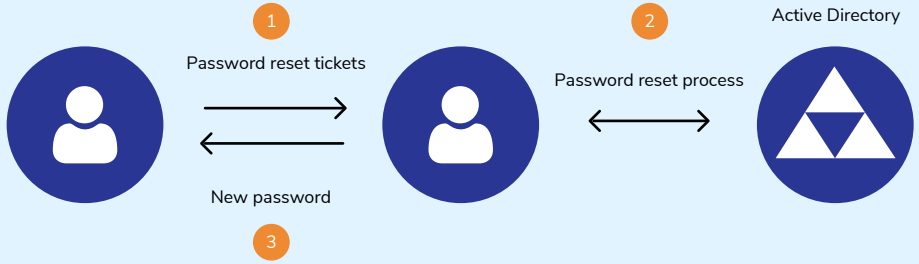
2. **Mail group subscription:** Allow users to opt-in and opt-out of distribution groups.

3. **Employee Search & Organization Chart:** ADSelfService Plus allows admins to view the complete list of their employees and thier position in their organization hierarchy.

How admins can free themselves from redundant password reset tickets?

ManageEngine
ADSelfService Plus

Before ADSelfService Plus



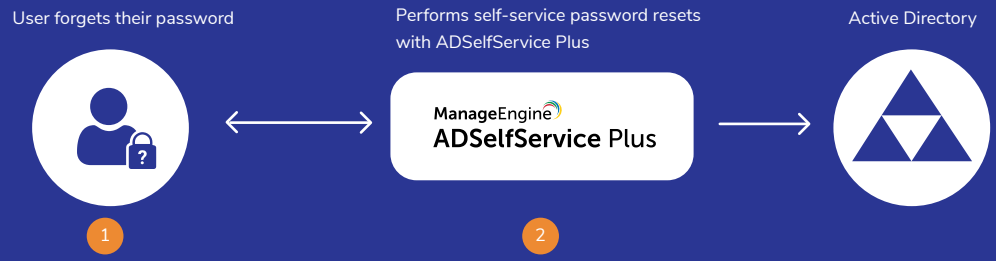
1. A user gets forgets their AD domain password and raises a password reset ticket.

2. The help desk team verifies user identity by asking their employee ID.

3. Employee waits for the IT team to reset password in AD.

4. The user receives the new password.

After ADSelfService Plus

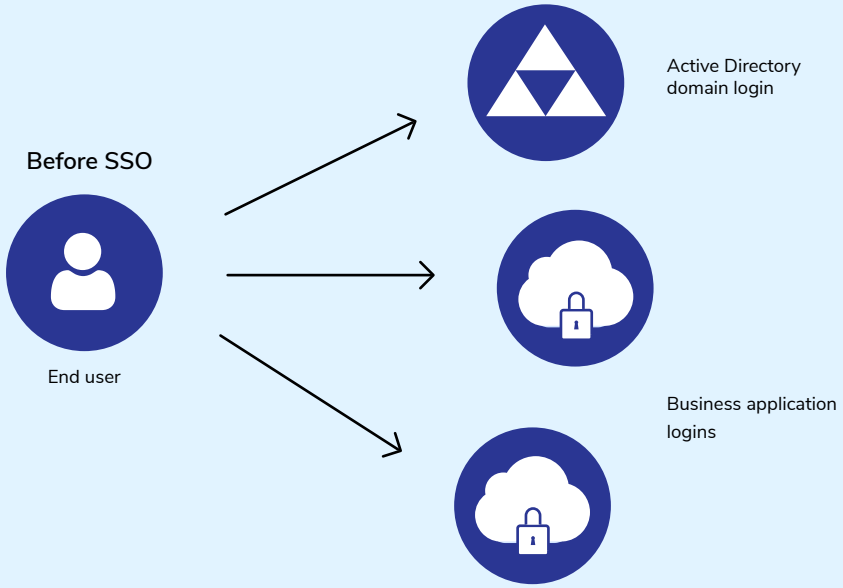


1. A user forgets their AD domain password.

2. The user accesses the ADSelfService Plus portal and resets their password without having to wait for the IT team, via their login screen, web browser, or mobile phones.

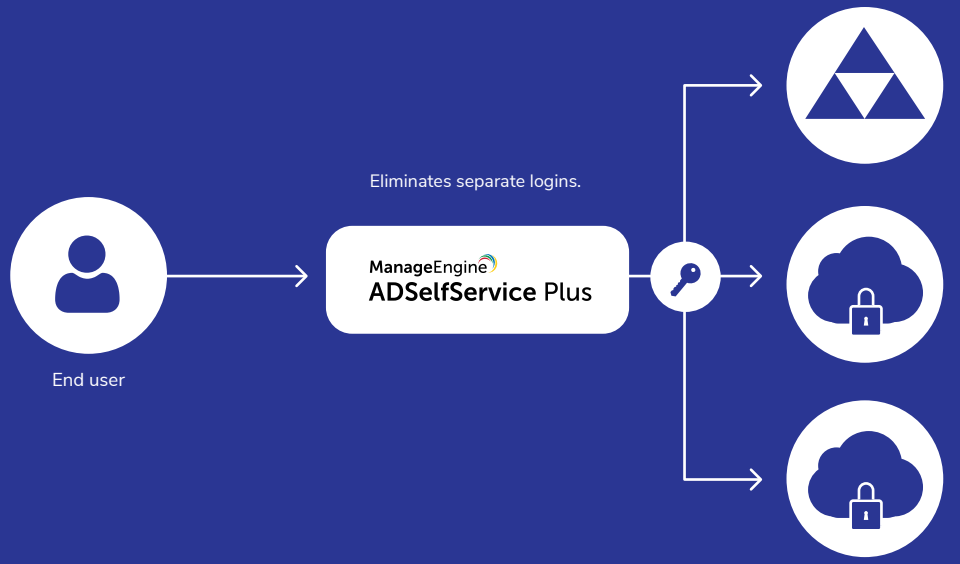
ManageEngine
ADSelfService Plus

Before
implementing single sign on



Users need to remember multiple passwords to access different applications.

After
implementing single sign on



Users can use Active-Directory based single sign-on for all SAML 2.0-enabled applications.

ManageEngine
ADSelfService Plus

Apply a centralized custom password policy to both on-premises and cloud apps.

- **Restrict characters.**

  Restrict the number of special characters, numbers, and Unicode characters that users can use.

- **Restrict patterns.**

  Restrict keyboard sequences, dictionary words, and palindromes.

- **Use passphrases.**

  Option to use passphrases that does not conform to the complexity requirements when the password length exceeds a predefined limit (say, 20 characters)

- **Restrict repetition.**

  Enforce a password history check during password reset, and restrict the repetition of specific character(s) or username as the password.(e.g. “aaaaa” or “user01”).

- **Restrict length.**

  Specify the minimum and maximum password lengths.

- **Password strength checker.**

  Display the password policy requirement on the reset and change password pages

Improve the security stance of your organization with strong user passwords.

Ensure 100% enrollment for password self-service.

1. Notify users to enroll for password self-service via email and push notifications

2. Force users to enroll when they log in to their machines with a persistent desktop pop-up.

3. Automatically enroll users by importing enrollment data from CSV files or an external database

ManageEngine
ADSelfService Plus

Reporting with ADSelfService Plus.

1. Reports on password expiration, locked out users, and more.

2. Audit reports on all user and admin actions.

3. Export, customize, and schedule reports to be delivered via email.

Multi-factor Authentication

ManageEngine
ADSelfService Plus

ADSelfService Plus supports multi-factor authentication for:

Endpoint logins.

Self-service password reset and account unlock

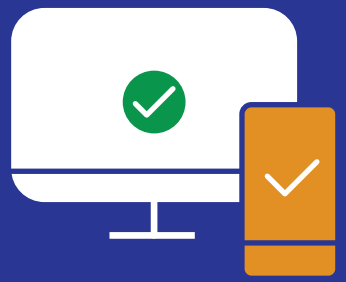
Application access

Supported authenticators:

1. Security questions and answers
2. SMS and email verification codes
3. Google Authenticator
4. Duo Security
5. RSA SecurID
6. RADIUS
7. Push notifications
8. Fingerprint authentication
9. QR code-based authentication
10. Time-based one-time password (TOTP)
11. AD-based security questions
12. Microsoft Authenticator
13. Yubikey Authenticator

ManageEngine
ADSelfService Plus

Endpoint MFA for Windows/macOS/Linux logons.



Step 1 :

Users enter their domain credentials as a first level of authentication to their machine.

Step 2 :

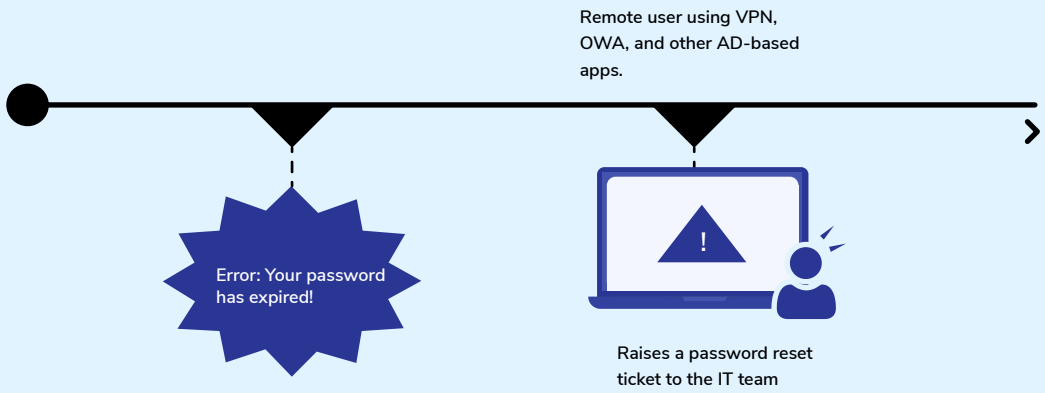
Users must authenticate themselves using any of the supported authentication methods such as the time-sensitive authentication code sent to their SMS or email, or through a third-party authentication provider like Google Authenticator, or RSA SecurID.

Step 3 :

After sucessful authentication, the user is sucessfully logged into their Windows or macOS, or Linux machine.

Help users be proactive by sending password expiration alerts, well in advance.

ManageEngine
ADSelfService Plus



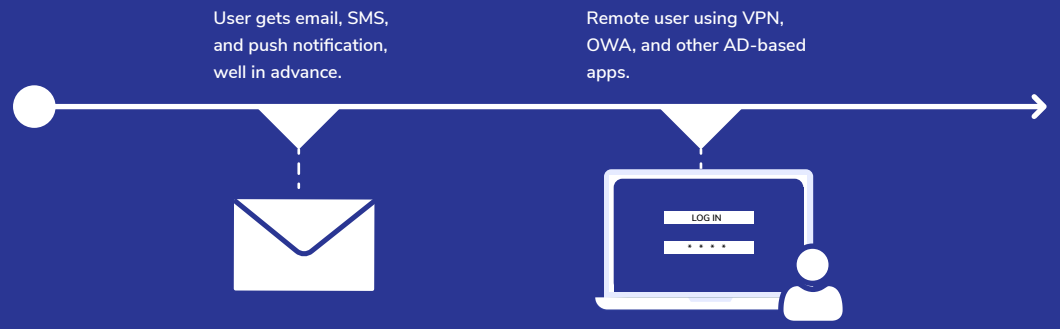
1. Users let their passwords expire because they:

2. Have AD accounts only for VPN or OWA, so they never log on interactively to see Windows notifications.

3. Don't notice the password expiration warning in the taskbar.

4. Use machines that aren't running Windows, don't receive AD password expiration notifications.

5. So they reach out to the IT team to reset passwords.



1. ADSelfService Plus automatically notify users about their expiring password.

2. Admins can send daily, weekly expiry notifications or reminders on specific days before password expiration.

Key benefits of ADSelfService Plus in a glance.

Cost savings

1. Eliminates the No.1 source of help desk calls.
2. Allows IT admins and the help desk to focus on other critical tasks.

Improves IT security

1. Enforce strong password policies.
2. Provide multi-factor authentication for cloud apps.
3. Provide role-based access control to apps and self-service features.

Improves user experience

1. No wait time.
2. Access from anywhere
3. Seamless login experience.
4. No more password fatigue.

ManageEngine
ADSelfService Plus

How ADSelfService can help in **education, finance, and the healthcare sector?**

Education sector

Students and staff can:

1. Reset passwords from their login screen even from home.
2. Self-update their personal information.
3. Access multiple application from a single console.

Finance sector

1. Employees can perform password self-service, get access to the required resources, ensure strong user passwords, and more.
2. Be compliant with SOX[1], GLBA[2], and PCI DSS[3].

Healthcare sector

1. Clinicians and doctors can perform password self-service, have secure access to EHR[4] with SSO, ensure up-to-date profiles, secure ePHI[5] data with custom password policies, and more.
2. Helps comply with HIPAA[6].

1. SOX: Sarbanes-Oxley Act
2. GLBA: Gramm–Leach–Bliley Act
3. PCI DSS: Payment Card Industry Data Security
4. EHR: Electronic health records
5. ePHI: Electronic protected health information
6. HIPAA: Health Insurance Portability and Accountability Act

ManageEngine
ADSelfService Plus

Case study

ManageEngine
ADSelfService Plus

TriMark deploys ADSelfService Plus to tackle password problems.

Industry: Food industry Location: USA

Quote:

"*When our employees needed a password reset while they were outside the organization, ADSelfService Plus helped us by allowing them to reset their passwords remotely. It was beneficial for us,*" - *Roger DeVivo, senior system administrator at TriMark.*

Business needs:

- Allow users to reset passwords when not connected to their corporate network, without IT assistance.

- No trust was established between AD domains leading to password fatigue. They needed a solution that could sync passwords across all of users' account.

How ADSelfService Plus helps?

ADSelfService Plus helps remote employees reset their passwords, and then it locally updates the credentials in users' machines.

ADSelfService Plus' Password Sync feature allowed TriMark to automatically sync all password changes between multiple Active Directory domains.

ADSelfService Plus helped admins to schedule password expiration alerts via SMS, email, and push notifications so users change their soon-to-expire passwords, well in advance.

Quote:

"The support team helped me pretty quickly every time I called in, and I'd say I'm happy with the support!"

Licensing and pricing.

Details	Evaluation edition	Free edition	Standard and Professional editions
Expiration	30 days	No expiration	As per license terms
Number of domains	Unlimited domains	Unlimited domains	As per license terms
Number of domain users	Unlimited users	50 users	As per license terms
Features	Unrestricted features	Unrestricted features	As per license terms
24x5 support	✓	✓	✓

Get quote

Trusted By


DTI


hp


IBM


Symantec


ebay


asics


unicef


CISCO


SAMSUNG


SONY MUSIC


IDG
INTERNATIONAL DATA GROUP


TOSHIBA
Leading Innovation


American
Apparel


VOLVO


World Health
Organization

Contact us

Contact Number

+1-408-916-9890

Live chat

For instant responses.

Support Email

support@adselfserviceplus.com

Visit our website

www.adselfserviceplus.com/

Download now