

ADSelfService Plus

is an identity security solution with **adaptive MFA, SSO, and password management capabilities**



Give end users the right amount of independence and eliminate more than a quarter of your help desk tickets.

Highlights

- Employ MFA to secure endpoint logins, cloud application logins, and self-service password reset and account unlock.
- Give end users one identity to easily access all their enterprise applications through single sign-on and password sync.
- Empower end users to perform password reset and account unlock without compromising on security.
- Deliver fully customizable and automated password and account expiration notifications periodically to end users.
- Enforce a multi-platform, granular password policy with customizable rules, including the dictionary rule and Have I Been Pwned integration.
- Allow end users to update their personal details in AD and perform comprehensive corporate directory searches.

The challenge

Securing and managing user identities can be a real challenge in the modern-day hybrid workplace. Both on-premises and remote users access the enterprise network through various endpoints, and every single access attempt has to be scrutinized. Care must be taken to ensure that users have streamlined access to all enterprise resources at anytime. It would be ideal to have a single solution to address all these requirements.

Introducing ADSelfService Plus

ManageEngine ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and to establish a Zero Trust environment. With capabilities such as adaptive MFA, SSO, password management and security, and workforce self-service, ADSelfService Plus provides your workforce secure, frictionless access to resources. The solution helps block identity-related threats, reduce password-related help desk tickets, fast-track application onboarding, and empower remote workforce with secure access to the resources they need.

“ADSelfService Plus is a tool that we consider indispensable. It is the right tool for the job. Any company that relies on Active Directory authentication with password expiry will benefit from using it.”

Chris Jackson

Systems administrator, TXP Corporation

Core features

Adaptive MFA

- **MFA:** Protect access to machines (Windows, macOS, and Linux), VPNs, OWA, and enterprise applications with MFA by choosing from over 20 methods, including FIDO2 authenticators, biometrics, TOTP, and third-party apps like YubiKey Authenticator and Microsoft Authenticator.
- **Conditional Access:** Automate access control to organizational resources via context-based authentication using details like IP address, time of access, geolocation, and device used.

SSO

- **Enterprise SSO:** Integrate enterprise applications with your organization's AD to give users the convenience of accessing any application by logging in just once with their credentials.
- **Passwordless login:** Thwart credential-based attacks by employing passwordless authentication, backed by MFA for enterprise application logins.

Self-service password management and security

- **Password self-service:** Empower end users to perform secure password reset and account unlock without help desk intervention.
- **Real-time password synchronizer:** Synchronize AD passwords with enterprise applications in real time, and enable users to switch smoothly between various cloud services and on-premises systems with a single password.
- **Password policy enforcer:** Customize fine-grained password policies at the OU and group level for different users across AD and other enterprise platforms.

Remote work enablement

- **Cached credentials update:** Enable automatic update of users' domain password changes in their devices' cached credentials via VPN.
- **Web-based domain password change:** Offer a secure web-based portal for remote employees to change domain and enterprise application passwords.
- **Password and account expiry notification:** Remind on-premises and remote users about their impending password and account expiration via SMS, email, or push notifications.

Workforce self-service

- **Directory self-update:** Maintain accurate and up-to-date directory information by allowing end users to update their own attributes, such as their email address, mobile number, and photograph, in AD.
- **Corporate directory search:** Enable employees to easily search for users, contacts, or groups in your organization.

Email group subscription: Define group subscription policies and allow users to opt in or out of selected distribution groups when their role changes, without help desk intervention.

Supplementary features

- **Predefined reports:** Run audit reports to keep track of users' identity verification attempts, self-service actions, and password and account status.
- **Integrations:** Extend the product's capabilities by integrating with SIEM, ITSM, and IAM solutions.
- **Mobile password management:** Perform self-service actions on the go using the ADSelfService Plus Android or iOS mobile application.



Pricing starts at

\$ **595**

Download **30-day, FREE trial**
with no restrictions!

[Download now](#)

Specifications:

Processor: 2.4 GHz | **RAM:** 8GB | **Disk Space:** 100GB (SSD preferred)

Supported platforms: Windows 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows Server 2000, Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7, and Windows Vista and Windows XP.

Supported browsers: Internet Explorer 9 and above; Firefox 4 and above; Chrome 10 and above; Microsoft Edge.

Supported databases: PostgreSQL (default), and MS SQL.

Contact us at:

Website: www.adselfserviceplus.com

Live demo: demo.adselfserviceplus.com

Sales questions: sales@manageengine.com

Tech support: support@adselfserviceplus.com

Toll-free: +1.844.245.1104