

ADSelfService Plus

is an **integrated Active Directory self-service password management** and **single sign-on solution** fit for any enterprise.



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

Highlights

- Empower end users to perform password reset and account unlock without compromising on security.
- Deliver password and account expiration notifications directly to end users.
- Utilize enterprise single sign-on for one-click access to cloud apps.
- Synchronize password and account changes across multiple on-premises and cloud apps.
- Enforce a multi-platform granular password policy.
- Allow end users to update their personal details in AD and perform comprehensive corporate directory searches.

The Challenge

A day in the life of your organization's IT help desk technician can be extremely taxing, especially when they have to deal with recurring password reset and account unlock tickets that constitute over 40 percent of the help desk ticket pool. The fact that you have to incur about \$30 for every password related ticket is alarming and would eventually take a toll on the organization's productivity and progress. What you need is a reliable tool to help you tide over this potential mess.

Introducing ADSelfService Plus

A secure and robust web based self-service solution, ADSelfService Plus reduces the most critical of help desk tickets by enabling your employees to reset their password and unlock their account. ADSelfService Plus also unifies user identities and serves as a single portal for logging into all enterprise cloud applications thereby enhancing user experience.

“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

Password Management

- **Password self-service:** Empower end users to perform secure password reset and account unlock without help desk intervention.
- **Password expiration notification:** Remind employees (including remote and VPN users) about their impending password expiration via SMS, email, or push notifications.
- **Password policy enforcer:** Customize fine-grained password policies at the organizational unit (OU) and group level for different users across multiple platforms.

Active Directory Self-Service

- **Self directory update:** Maintain accurate and up-to-date directory information by allowing end users to update their personal details in AD.
- **Corporate or employee directory search:** Enable employees to easily search for users, contacts, and groups in your organization.
- **Email group subscription:** Define group subscription policies and allow users to opt-in or opt-out of selected distribution groups when their role changes, all without having to go to the help desk.

One Identity

- **Enterprise single sign-on:** Integrate over 100 cloud apps with your enterprise's Windows AD accounts to give users the convenience of accessing any application by logging in just once with their AD credentials.
- **Real-time password synchronizer:** Synchronize all password and account changes in real time and let users sail smoothly between various cloud services and on-premises systems with a single password.

Features that make our product even more secure

- Establish user identities with multi-factor authentication options, including security questions and answers; SMS and email verification codes; push notifications; Google Authenticator; Duo Security; RSA SecurID; RADIUS; fingerprint authentication; QR code-based authentication; and time-based one-time passcodes (TOTPs).
- Run audit reports to keep track of every self-service action.
- Integrate with help desk software that supports workflow approval.
- Secure both remote and local accesses to Windows using two-factor authentication.
- Utilize secure channels for communication: HTTP over SSL (web browsers and ADSelfService Plus) and LDAP over SSL (Active Directory and ADSelfService Plus).
- Create an anti-hacking system that prevents brute-force, dictionary, and man-in-the-middle attacks.

Specifications:

Processor: P4 - 3.0 GHz | RAM: 2 GB | Disk Space: 2 GB

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

Supported browsers: Internet Explorer 7 and above; Firefox 4 and above; Chrome 10 and above

Supported databases: PostgreSQL (default), MS SQL, MySQL

