



ManageEngine[®]
ADSelfService Plus

Efficient Password management:

The key to increasing IT productivity

www.adselfserviceplus.com

Table of Contents

1. The current climate of IT management	2
2. Ever-present passwords	2
3. The risk of mishandled passwords	2
4. Password management dependency on the help desk	2
5. Clearing a path through password-related obstacles with ADSelfService Plus	3
A. Self-service password reset and account unlock	3
i. ADSelfService Plus GINA	4
B. Password expiration notification tool	5
C. Detailed reports	6
i. User reports	7
ii. Audit reports	7
iii. Enrollment reports	8
6. Single sign-on and password synchronization	9
7. Unlocking true productivity	11

1

The current climate of IT management

Many organizations rely heavily on their IT departments to manage work and enhance productivity. From the early 2000s, this dependency has only continued to grow. Organizations take great care in hiring IT personnel, as many of these organizations understand the impact that efficient IT management can make. IT administrators are required to stay aligned with market trends and are responsible for keeping their company's IT environment secure, up, and running. Even a single day of down time can translate into huge losses for any company.

2

Ever-present passwords

Despite advances in technology over the last decade, most employees still use usernames and passwords to access their work. Although it was initially released with Windows 2000, Active Directory (AD) and its related services are still predominantly used by organizations to manage their IT. AD hasn't kept with the times and lacks the finesse to let administrators change password complexity rules and set different passwords for specific groups and OUs, or allow users to unlock their accounts or reset their passwords on their own.

But AD isn't the only application employees have to deal with; the number of enterprise applications each employee utilizes is far greater than what it was just a few years ago. Plus, each application comes with its own set of login credentials, meaning employees have to remember an increasing amount of passwords. In fact, a survey by [Data Insider](#) revealed that more than 70 percent of its 999 participants had over 10 passwords to remember.

3

Risk of mishandled passwords

With so many applications to handle and passwords to remember, it's inevitable that employees will confuse passwords with one another or resort to very unsafe methods to store their passwords such as writing them down or sharing them with others. Since it's not possible to keep individual tabs on every employee's passwords, IT administrators should instead focus on reducing the risk of mishandled passwords by eliminating such password hassles altogether.

4

Password dependency on the help desk

Even with all the recent advances in technology, most users still depend on their IT help desk to get their password issues resolved, unless they're using applications that support password reset through security questions. This issue may seem trivial to the user, but for the help desk, the narrative changes; when users can't remember their passwords, it's the help desk that pays for it.

Remembering passwords isn't the only problem users run into. Users can enter the wrong credentials multiple times and lock themselves out of their work applications. In most cases, they have to seek aid from help desk technicians to regain access.

Whether it's a password reset ticket, a forgotten login password, or an account unlock request, it has to be immediately addressed in order to avoid employee downtime and loss of productivity. It's estimated that at least 40 percent of help desk tickets are password related, and on average, each password-related ticket consumes around 20 minutes, which prevents the help desk from focusing on more critical issues.

5

Clearing a path through password-related obstacles with ADSelfService Plus

End users need a self-service password reset solution that allows them to remotely reset their own AD domain passwords from a web browser, without contacting the help desk, and ADSelfService Plus offers exactly that.

ADSelfService Plus is a secure, end-user password self-service solution that helps domain users perform self-service password reset, self-service account unlock, and employee self-update of personal details (telephone number, email, etc.) in AD.

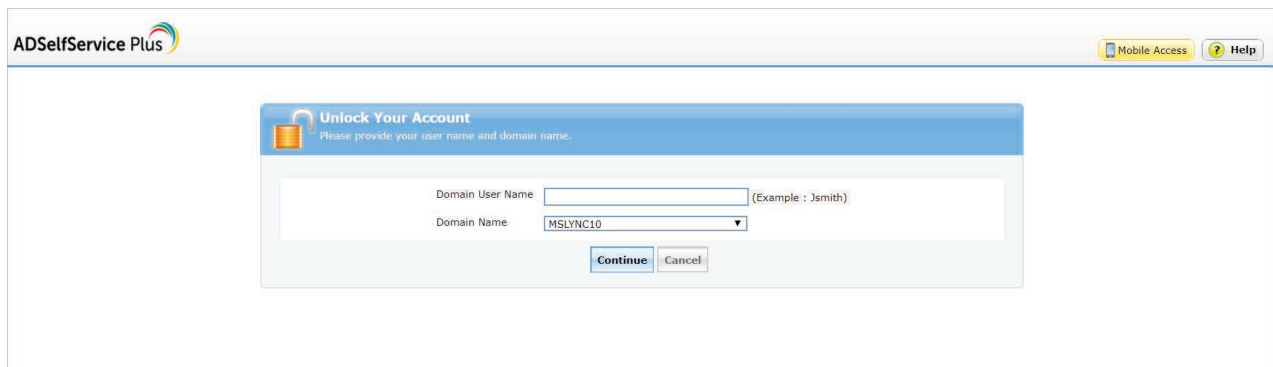
A. Self-service password reset and account unlock

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 aims to tackle this issue by securely enabling users to both reset their forgotten passwords and unlock their accounts, without contacting the help desk. Users' identities are verified and established securely through:

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

Administrators can choose to exercise just one or all of these user identification methods for enhanced security.

To further prevent malicious or accidental password resets, administrators can choose to selectively grant privileges to users by enrolling them into ADSelfService Plus for password resets.



i. ADSelfService Plus GINA

Graphical identification and authentication (GINA) is a Windows component that provides secure authentication and interactive logon services. ADSelfService Plus' GINA is an extension of the standard GINA from Microsoft. It's been designed to add the Reset Password / Unlock Account functionality to the Windows logon screen. It can be installed on machines running Windows XP or higher. ADSelfService Plus' GINA comes bundled with the ADSelfService Plus Professional edition and can be pushed to client machines by the AD administrator through the software itself.

Reset Password

* Select Account(s) : John (test-domain.com), John (thinkt) ▼

* New Password

* Confirm New Password

- John (test-domain.com)
- John (testdomain.onmicrosoft.com)
- John (test-domain1.com)

- The minimum password age is 1
- The maximum password age is 42
- The minimum password length is 7
- No. of Passwords Remembered is 2
- The password complexity property is Disabled

Type the characters you see in the picture below.

24di7k

Letters are not case-sensitive

Cancel Continue

In ADSelfService Plus, the GINA client software can be installed:

- From the ADSelfService Plus console.
- Via Group Policy Object (GPO).
- Via System Center Configuration Manager (SCCM).
- Manually.

The GINA client integrates with ADSelfService Plus' password policies to ensure that password resets from the Windows logon screen still comply with the established password policies.

B. Password expiration notification tool

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 send multiple reminders to the same user until the account or password is reset.

The screenshot shows the 'Password/Account Expiration Notification' configuration page in the ADSelfService Plus web interface. The left sidebar contains navigation links for Self-Service, Policy Configuration, Multi-factor Authentication, Password Expiration Notification (selected), Password Policy Enforcer, Password Sync/Single Sign On, Conditional Access, Directory Self Service, Administrative Tools, and Security Center. The main configuration area includes a 'Select Domain' dropdown, a 'Notification Type' dropdown set to 'Password Expiry Notification', a 'Scheduler Name' input field, and a 'Notify Via' dropdown set to 'SMS'. Below these is a 'Notification Frequency' dropdown set to 'Daily'. The 'Notify users during the last' field is set to '7' days before expiration. The 'Subject' field is 'Password/Account Expiration Notification'. The 'Message' field contains a template: 'Dear %username%, Your password will expire on %datetime%. So, please change your password as soon as possible. Thank you. Regards Administrator'. At the bottom, there are 'Save' and 'Cancel' buttons. A small information box at the bottom left provides details about character limits and macros.

Here are a few highlights of the Password Expiration Notifier:

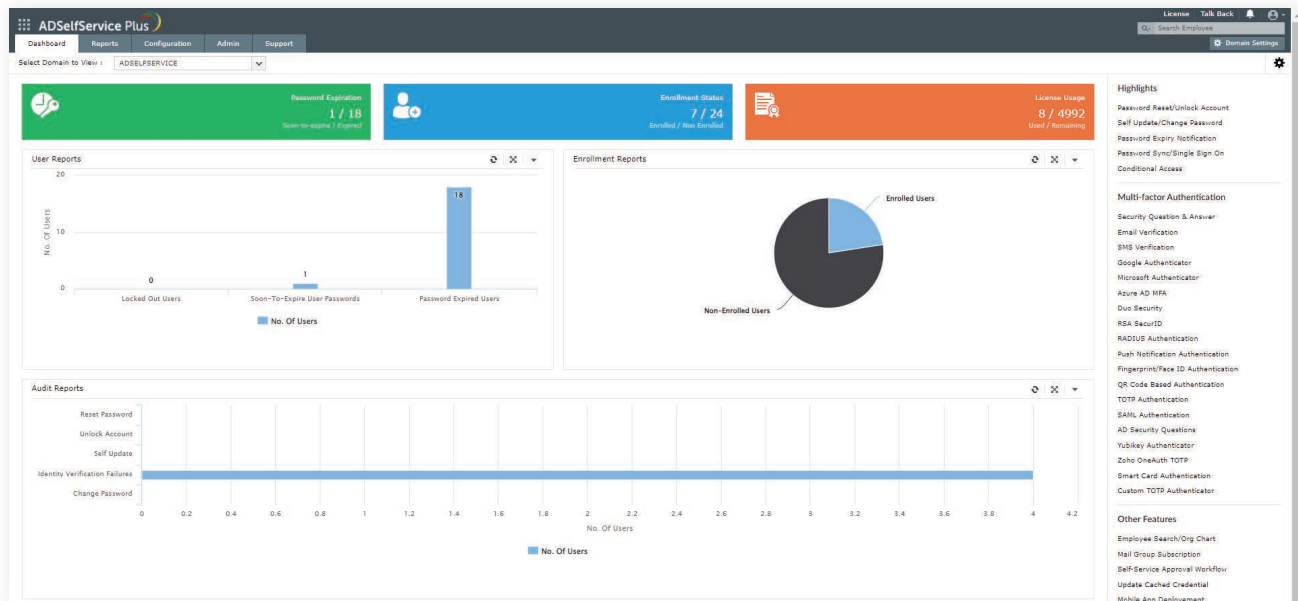
- Administrators can customize the content of the password change reminder email. For example, administrators can choose a more imperative tone when the expiration date draws closer.
- Both end users and managers can be notified about a users' account expiration.
- Users can be notified via SMS or email about their impending password expiration.

What's more? [ADSelfService Plus' Password Expiration Notifier](#) is now absolutely free for unlimited users.

C. Detailed reports

Even if users are granted self-service to their passwords, admins should still keep a sharp eye on user actions. With a large number of users and application passwords, however, this is easier said than done. This is where efficient report generation comes in handy. With granular control over user reports, audit reports, and enrollment reports, administrators can keep a close eye on user actions like the number of user lockouts or password reset attempts.

Administrators can generate reports for specific OUs or the entire domain. A quick snapshot of all essential and top-level information on the domain users' password statuses is available on ADSelfService Plus' Dashboard.



Administrators can:

- Schedule reports to be generated at fixed intervals.
- Configure generated reports to be sent to the administrators' mailboxes instantly.
- Export reports in multiple formats such as CSV, PDF, XLS, HTML, and CSVDE.

Reports in ADSelfService Plus fall into three categories:

i. User reports

- **Locked Out Users Report:** Displays a list of users who are locked out of their accounts.
- **Soon-to-Expire Password Users Report:** Scans all of AD to list which user accounts have passwords that will expire within a defined time.
- **Password Expired Users Report:** Displays a list of user accounts with expired passwords.

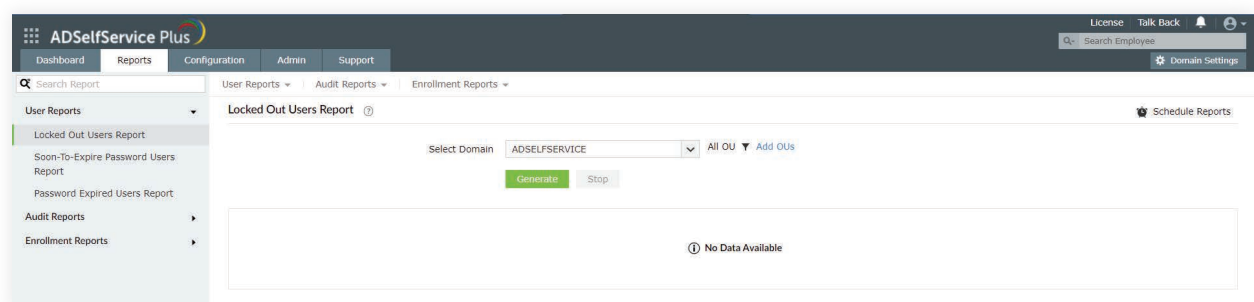
ii. Audit reports

- **Reset Password Audit Report:** Displays information about password reset attempts, including whether they were automated or manual.
- **Unlock Account Audit Report:** Displays information about which locked-out user accounts have been unlocked and when.
- **Self-Update Audit Report:** Displays information about updates to personal data in AD made by end users through ADSelfService Plus.

- **Change Password Audit Report:** Displays information about attempted password changes by end users.
- **Notification Delivery Report:** Displays information on the delivery status of various notifications sent like enrollment notifications, password expiration notifications, and notifications sent upon execution of self-service operations.
- **Identity Verification Failures Report:** Displays information about secondary level security identity verification failures by end users. For example, if a user enters the wrong answer to a security question, it gets reported here.
- **User Attempts Audit Report:** Displays information about user actions, including logins, resets, and unlocks.

iii. Enrollment reports

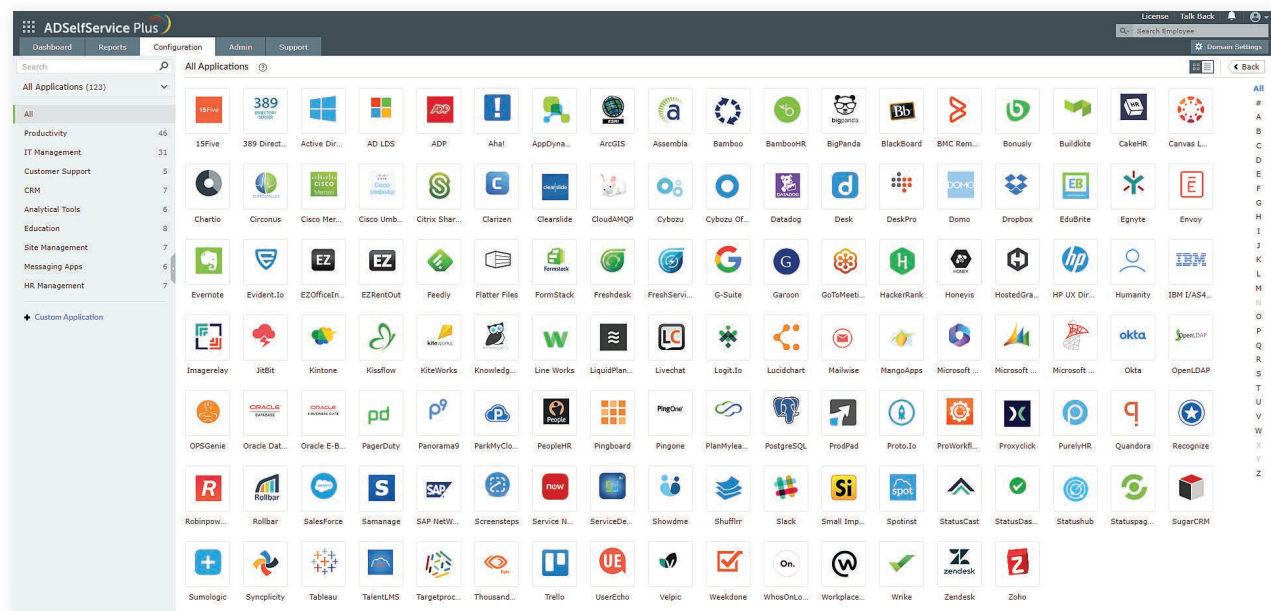
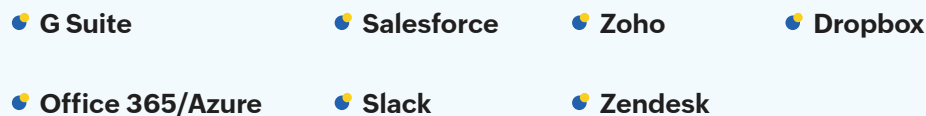
- **Enrolled Users Report:** Lists which users have been enrolled into ADSelfService Plus.
- **Non-Enrolled Users Report:** Lists which users have not enrolled into ADSelfService Plus.
- **Licensed Users Report:** Displays information about user accounts that are currently using ADSelfService Plus licenses.
- **Security Questions Report:** Displays information about security questions for particular user accounts along with their answers. These answers will be hidden if the answer storage format is set as irreversible.
- **Push Registered Devices Report:** Displays information about which devices have been configured to receive ADSelfService Plus push notifications.




Single sign-on and password synchronization

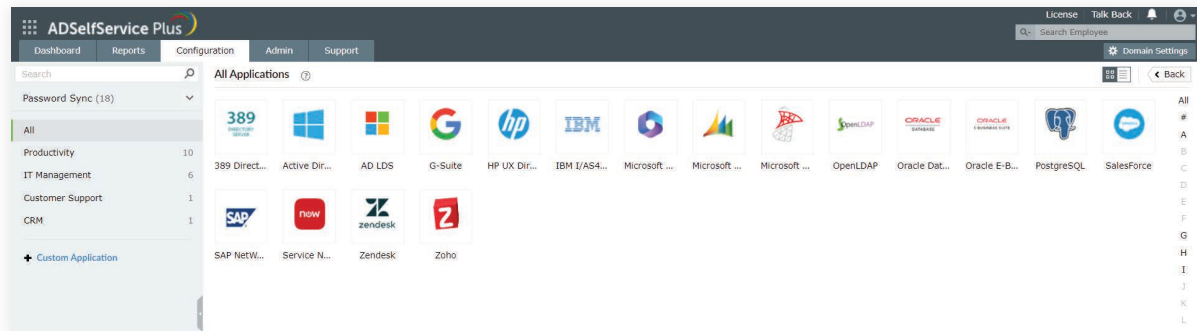
ADSelfService Plus is a password self-service tool that not only reminds users about account or password expiration and provides a wide number of live reports, but it also offers identity and access management features like AD single sign-on (SSO) as well as AD-based real-time password synchronization. Using these features, administrators can give users the power to access all their applications with just one password. This feature really comes in handy when employees use a large number of applications, but don't want to keep entering their credentials each time they access a new application. With real-time, AD-based password synchronization, password changes made in AD are automatically pushed to every configured cloud application.

ADSelfService Plus supports SSO for over 100 applications including:



ADSelfService Plus supports password synchronization for more than a dozen popular applications including:

 **G Suite**  **Oracle E-Business Suite**  **Salesforce**  **Office 365**



Unlocking true productivity

Performing efficient password management puts you on the path to improve overall productivity, and ADSelfService Plus is the key to unlocking that path. With features like password self-service, password/account expiration reminders, granular user action reports, SSO, and password synchronization, help desk personnel can concentrate on the more critical tasks that require their attention.

It's not just the help desk that will see improvements; end users will benefit too. They'll be able to get to work without the hassle of depending on the help desk each time they run into issues accessing their accounts.



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](#)