



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

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.

The screenshot displays the ADSelfService Plus web interface. At the top left is the logo, and at the top right are links for 'Mobile Access' and 'Help'. The main content area features a 'Reset Your Password' dialog box with the instruction 'Please, provide your user name and domain name.' Below this, there is a text input field for 'Domain User Name' with an example '(Example : Jamith)' and a dropdown menu for 'Domain Name' currently showing 'MSLYNC10'. At the bottom of the dialog are 'Continue' and 'Cancel' buttons.

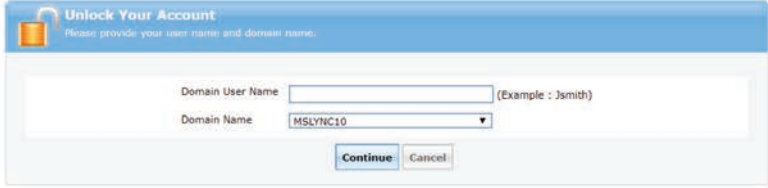
A. Self-service password reset and account unlock

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.



The screenshot shows the ADSelfService Plus interface. At the top left is the logo, and at the top right are 'Mobile Access' and 'Help' buttons. The main content is a dialog box titled 'Unlock Your Account' with the instruction 'Please provide your user name and domain name.' The dialog box contains two input fields: 'Domain User Name' with a text box and '(Example : Jsmith)' to its right, and 'Domain Name' with a dropdown menu showing 'MSLYNC10'. At the bottom are 'Continue' and 'Cancel' buttons.

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.



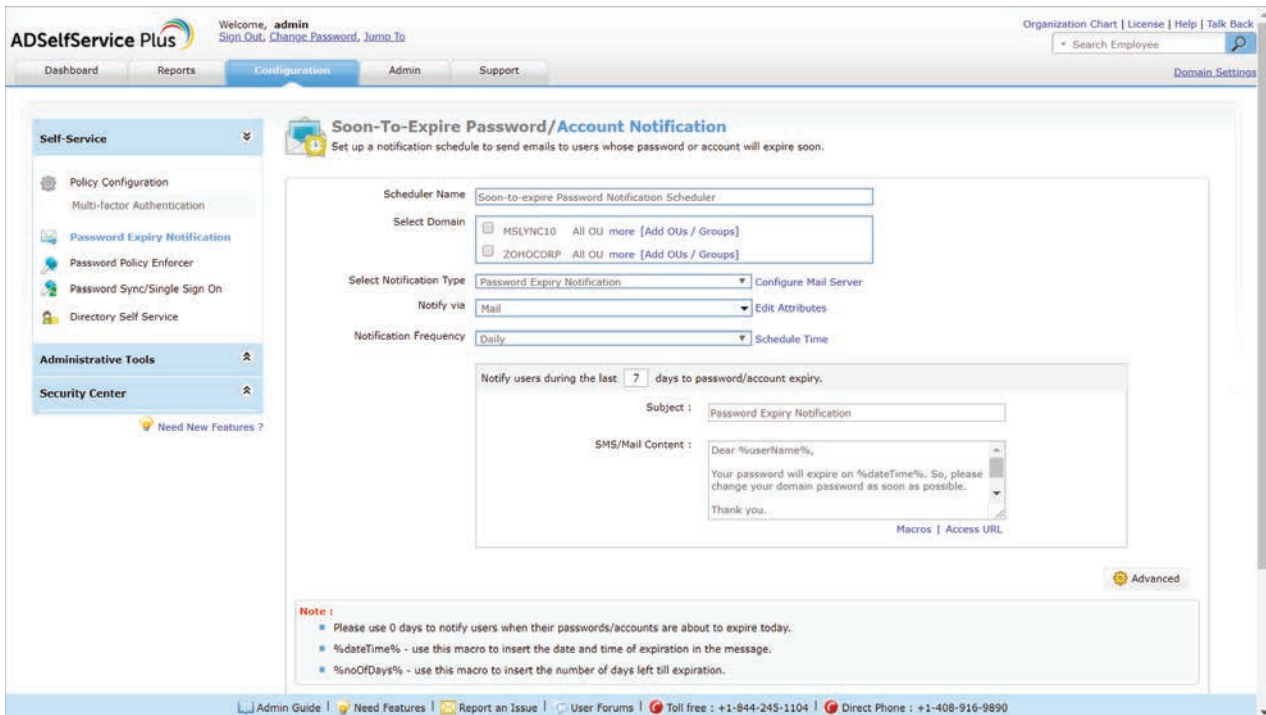
In ADSelfService Plus, the GINA client software can be installed:

- 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.



Here are a few highlights of the Password Expiration Notifier:

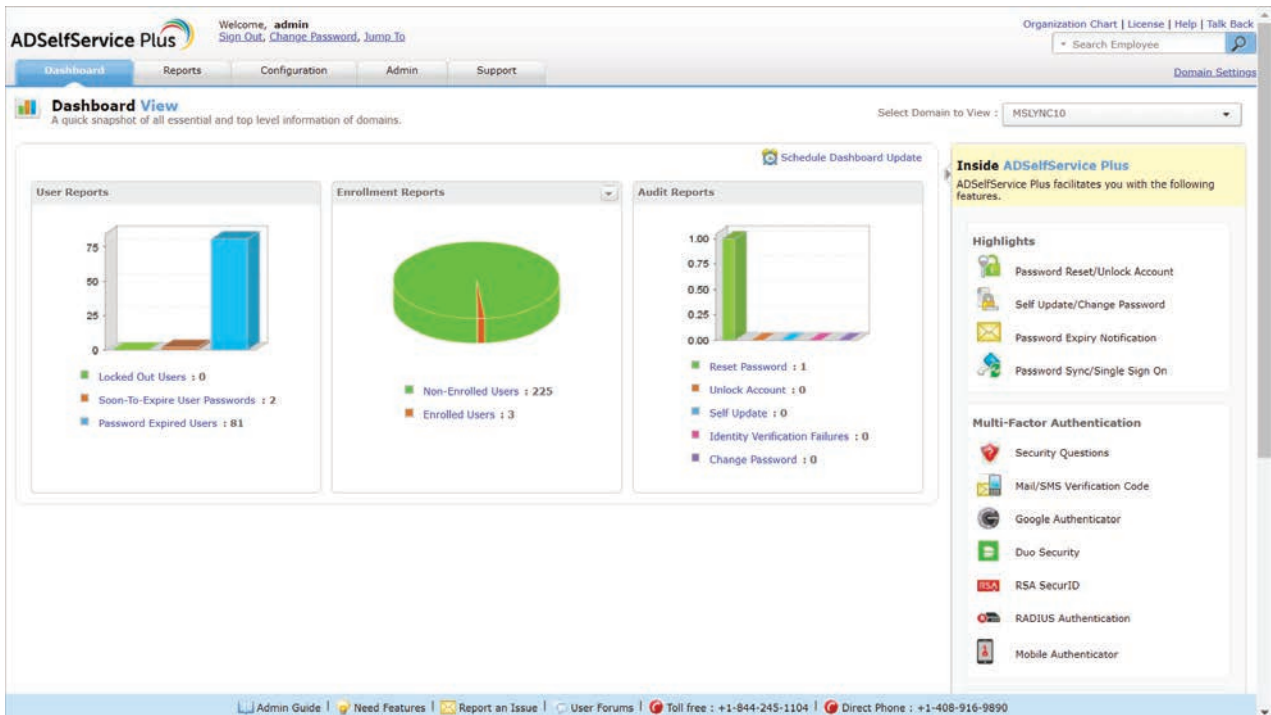
- Administrators can customize the content of the password change reminder email. For example, administrators can choose a more imperative tone when the expiration date draws closer.
- Both end users and managers can be notified about a users' account expiration.
- Users can be notified via SMS or email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

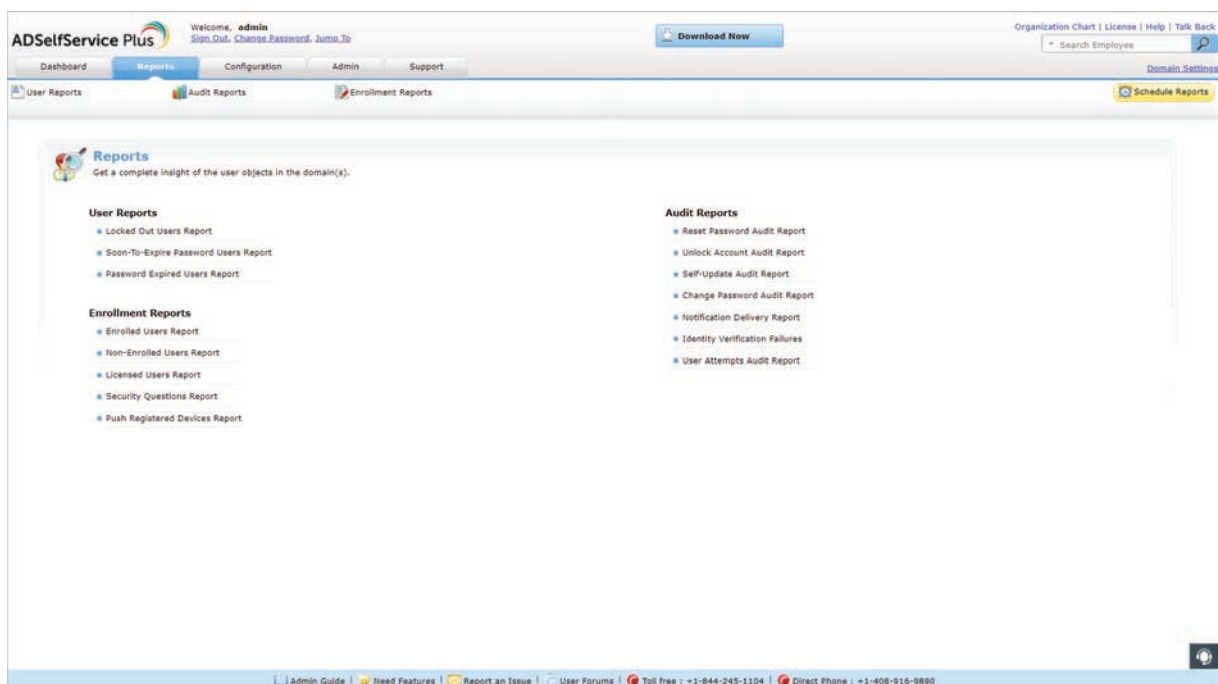
ii. Audit reports

- **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.

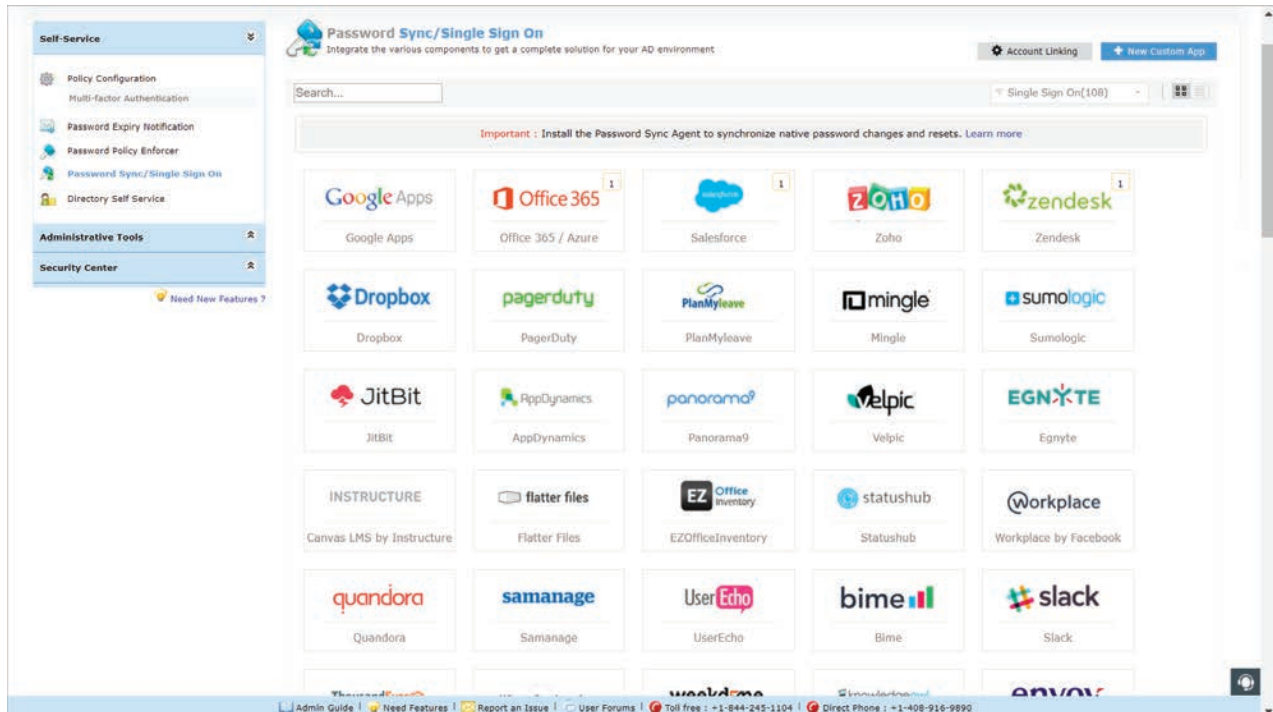


Single sign-on and password synchronization

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.

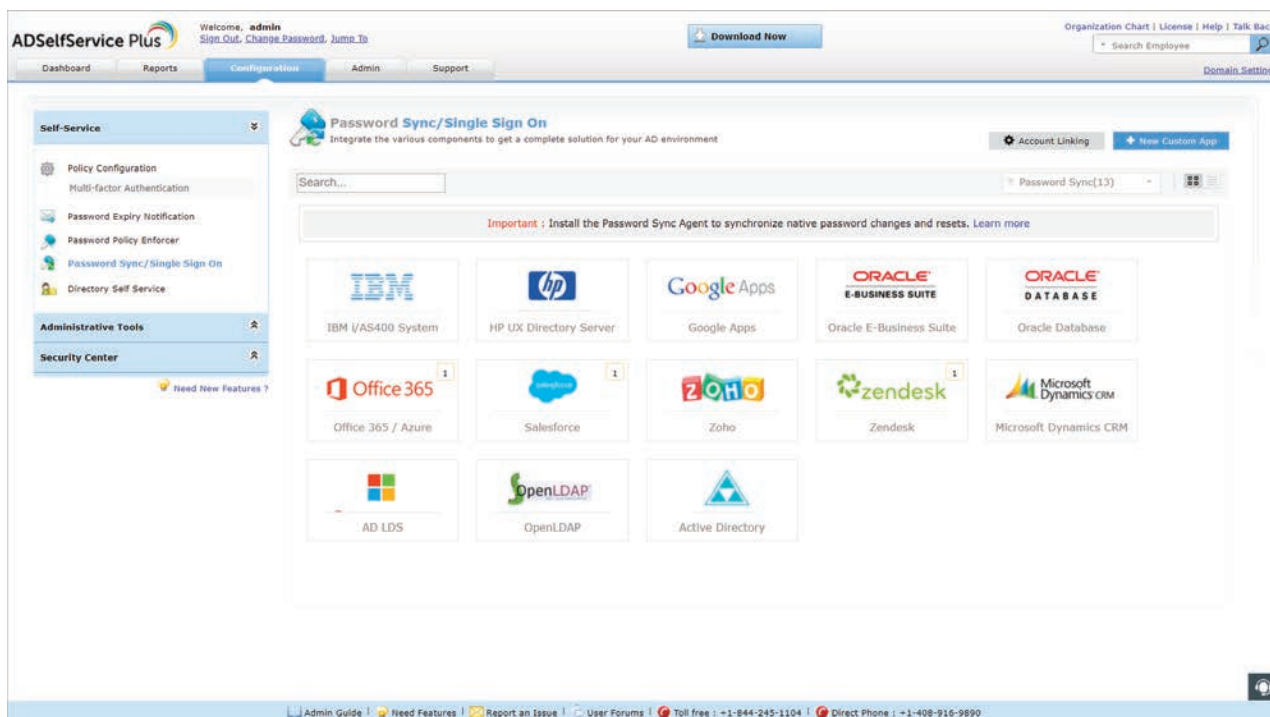
ADSelfService Plus supports SSO for over 100 applications including:

- G Suite
- Salesforce
- Zoho
- Dropbox
- Office 365/Azure
- Slack
- Zendesk



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

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



7 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.



ManageEngine ADSelfService Plus

ADSelfService Plus is an integrated Active Directory self-service password management and SSO solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications. ADSelfService Plus supports IT help desks by reducing password reset tickets and spares end users the frustration caused by downtime.

For more information, please visit www.manageengine.com/products/self-service-password.

\$ Get Quote

↓ Download