ManageEngine
ADSelfService Plus

Proof of Concept (Poc)

Learn how ManageEngine ADSelfService Plus resolve identity security, password management, and application onboarding issues.

www.adselfserviceplus.com

Table of Contents

Document overview

This document sheds light on the identity security and password management-related challenges faced by enterprises. It details how ADSelfService Plus helps IT admins uphold endpoint security, eliminate password reset tickets, maintain password hygiene, and streamline application onboarding.

ADSelfService Plus overview

ADSelfService Plus is an identity security solution with multi-factor authentication (MFA), single sign-on (SSO), and self-service password management capabilities.

Highlights of the product:

- MFA
- Conditional access
- Enterprise SSO
- Self-service password reset and account unlock
- Multi-platform password synchronization
- Password expiration notification
- Password policy enforcer
- Directory self-update
- Employee search and organization chart
- Self-subscription to email group

Challenge 1: Ensuring identity security of offline users

While most users are connected to the enterprise network either directly or indirectly via RDP or a VPN, loss of a connection to the network is possible. Along with this loss of access to gated resources is a lack of connection to services like an MFA provider. If this happens, your system can be left unsecure. To circumvent this, organizations might turn to unsafe practices such as authenticating users with just the password. Another common but flawed solution is to block access to the system completely, leaving the users stranded.

How does ADSelfService Plus ensure identity security with no connection?

An ideal solution is to introduce offline MFA, allowing you to enforce MFA for your users even when they have no access to the MFA server. This way, your users' offline status does not have to limit your organization's cybersecurity.

Providing holistic MFA, ADSelfService Plus supports both offline and online users. While online MFA requires a connection to the ADSelfService Plus server, offline MFA secures access for Windows and macOS machine logins without requiring connectivity. The feature comes into action in two scenarios:

- The user has a network connection, but is not connected to the ADSelfService Plus server.
- The user is connected to neither the internet, nor the ADSelfService Plus server.

IT admins can configure authentication apps for users to confirm access, such as Microsoft Authenticator and Google Authenticator. The authenticator information is securely stored in the user's machine, eliminating the need for a connection to the ADSelfService Plus server.

Advanced settings, such as limiting the number of offline MFA attempts, can require users to adhere to organizational standards by prompting them to connect back to the enterprise network. This eliminates permanent dependence on offline MFA.

Challenge 2: Fortifying all access points to the enterprise network

Securing machine logins is an important part of endpoint security, but not all of it. Today's hybrid work culture has led to an increase in remote endpoints and exploiters are always on the lookout for even the slightest loophole to enter the system. Enterprise applications, VPN, and Microsoft RDP, are the major endpoints that require solid security measures.

Some often overlooked endpoints are system unlocks, user account control prompts, and Microsoft OWA. Although not frequently used, they can provide administrative access to sensitive resources, so they need to be fortified appropriately.

How does ADSelfService Plus ensure endpoint security through MFA?

ADSelfService Plus' Endpoint MFA feature provides two or more layers of authentication in addition to the default username and password-based authentication. This secures machine logins as well other endpoints such as:

- Enterprise logins during SSO
- VPN and other RADIUS-based endpoints
- Microsoft RDP client and server authentication
- Microsoft OWA and Exchange Admin Center logins
- Windows user account control credential prompts
- System unlocks

ADSelfService Plus' machine login feature is available as two versions:

- **User-based MFA:** To protect desktop or laptop logins, including remote desktop logons using MFA for a specific group of users.
- **Machine-based MFA:** To apply MFA specifically to machines, irrespective of the users accessing it, their enrollment status and ADSelfService Plus connectivity.

Challenge 3: Securing endpoints against credential -based cyberattacks

With the number of security breaches increasing every day, relying on usernames and passwords alone to secure users' accounts is no longer safe or sufficient for organizations. Instead of just making passwords stronger, a more viable solution is to add additional layers of security to filter out unauthorized users. MFA—a method in which users are authenticated with something they know and something they have—makes this possible. While Microsoft provides Windows Hello for Business, which enables MFA for Windows, it comes with numerous drawbacks and is costly. Organizations need to ensure that their MFA solution:

a. Mitigates risks associated with poor passwords.

b. Offers an option to control access via OU and group-based policies.

c. Helps comply with security standards.

How does ADSelfService Plus help secure local and remote Windows, macOS, and Linux logons?

ADSelfService Plus' Endpoint MFA feature requires users to authenticate themselves in multiple stages to access their Windows, macOS, and Linux machines. The first level of authentication is through something they know: their usual Windows credentials. The second level of authentication—something they have—can be through one of the 15 authentication methods supported by ADSelfService Plus, including:

a. SMS or email-based verification codes

b. Duo Security

c. RSA SecurID

d. RADIUS Authentication

e. Microsoft Authenticator

f. YubiKey Authenticator

g. ADSelfService Plus mobile app (push notification, QR code, Biometric Authentication, and OTP)

Endpoint MFA ensures that there is no risk to sensitive data, even in cases where passwords are compromised. That is, even if unauthorized users gain access to a user's password, they still need access to the user's phone, email, RADIUS passcode, or YubiKey device to complete the second level of authentication. Moreover, the SMS and email-based verification codes as well as the authentication codes from Duo Security, RSA SecurID and other authentication apps are unique to each user. These codes can only be used once and will expire if they are not used within a certain period of time. When Endpoint MFA is enabled, it adds MFA to all local and remote Windows, macOS, and Linux login attempts.

Key benefits:

Mitigates risks associated with poor passwords

Many users today have multiple accounts—both for personal and business use. To avoid forgetting the numerous passwords they have to remember, users often use the same password across all accounts, or set weak passwords. Admins can mitigate the risks of poor password behavior by enabling MFA.

Granularly enforce MFA

Admins can enforce MFA for all users or only for select individuals—such as those that have elevated privileges and are at higher risk of security attacks—through OU and group-based policies.

Comply with important regulations

Multi-factor authentication helps comply with PCI DSS, NIST SP 800-63B, FFIEC, GDPR, and HIPPA regulations.

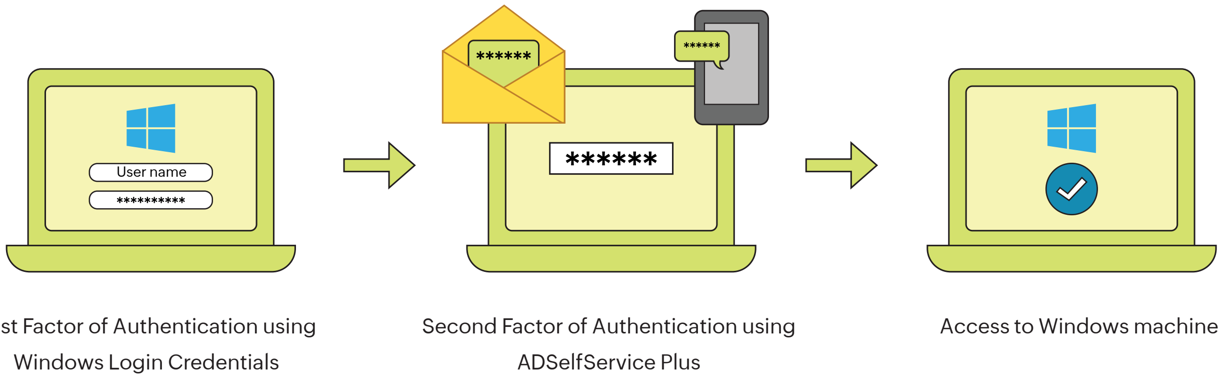

User name
****
******
******
******
First Factor of Authentication using Windows Login Credentials
Second Factor of Authentication using ADSelfService Plus
Access to Windows machine

Fig 6: Windows logon 2FA in ADSelfService Plus.

Challenge 4: Securing access to the IT environment without compromising on the user experience

The remote work model offers a range of benefits and has taken center stage in recent times. Since remote connections to the AD environment are susceptible to cyberattacks, admins implement restrictions and security checks for remote access. However, these measures are unnecessary when the user is within the secure office network.

When users alternate between working from the office premises and remotely, admins have to juggle strengthening the user access policy and relaxing it. This leads to an increased admin workload and an inconvenient user experience. An effective solution is to automate access control decisions based on context using conditional access.

How does ADSelfService Plus help automate access control decisions?

ADSelfService Plus' conditional access feature automatically assigns access policies to determine whether or not to enable capabilities like endpoint MFA, self-service, and SSO based on the users' parameters such as IP address, device, time of access, and geolocation.

This means when a user attempts to log in to their machine, tries to access an application, or attempts to use one of the self-service features in ADSelfService Plus, the users' parameters are analyzed and an access policy is assigned according to it. The policy enables admins to allow complete access to features, limit access to certain features, or restrict other features.

Key benefits:

Automatically implement access policies without admin intervention

With conditional access, admins need not edit or create multiple access policies to secure access to resources based on the context. Conditional access analyzes users' parameter data and automatically assigns appropriate access policies. This saves admins the time and resources spent in creating multiple access policies.

Improve your security posture without affecting the user experience

Applying a stringent organization-wide access policy might benefit some users while having adverse effects on others. With conditional access, access policies are implemented in real time based on user parameters to avoid unnecessarily strict security measures imposed in no-risk scenarios.

Challenge 5: Cloud app explosion

As organizations adopt cloud applications in droves, end users have to deal with more and more passwords throughout the workday. The more passwords users have to remember, the higher the chance users will forget them. This often leads to an increased number of help desk calls from exasperated users demanding password resets. A viable solution is to employ one-click access to all enterprise cloud applications via SSO. Organizations need to make sure that their SSO solution meets the following criteria:

a. Supports all SAML-enabled applications.

b. Offers an AD integration.

c. Supports multi-factor authentication for enhanced security.

d. Provides OU and group-based access control to easily provide or deny application access to users.

e. Gives secure, password-less access to the SSO provider.

How does ADSelfService Plus offer one-click access to all enterprise apps?

ADSelfService Plus provides AD-based SSO that gives users seamless, one-click access to cloud applications with just one corporate credential. Users are simply required to log in to ADSelfService Plus, which acts as the identity provider. They can then view a dashboard that lists every cloud application they have access to. With one click, users can access each application without having to enter their username and password again.

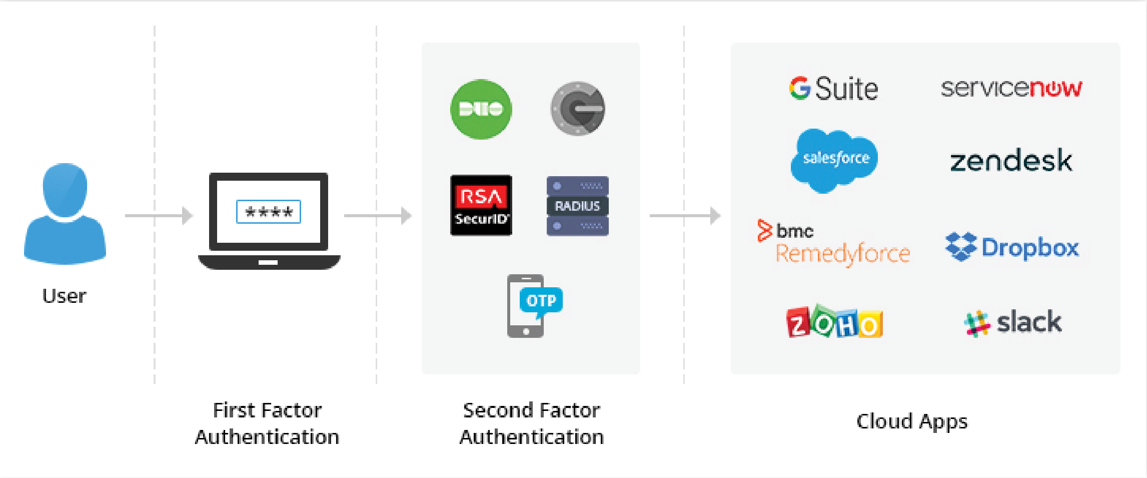


Fig 3: Enterprise SSO in action.

Key benefits:

Support for a vast number of applications

ADSelfService Plus comes with out-of-the-box SSO support for SAML 2.0-enabled cloud applications including Office 365, G Suite, Salesforce, Dropbox, and Slack.

AD integration

Most organizations already use AD to store users' identities and manage their access permissions. ADSelfService Plus uses existing identities for authentication during SSO. This saves time that would have otherwise been spent setting up new identities for users, and removes any dependency on password vaulting tools for storing additional passwords.

Enhanced security via multi-factor authentication (MFA)

ADSelfService Plus protects access to cloud applications with MFA. When SSO is enabled, users must always authenticate themselves in ADSelfService Plus—first using the tried and tested Windows, macOS, and Linux login credentials, and then using the factors chosen by the IT admin. ADSelfService Plus supports native factors such as SMS and email-based verification codes, as well as third-party authentication providers such as Duo Security, RSA SecurID, RADIUS server, Google Authenticator, and YubiKey Authenticator.

Access control using AD OUs and groups

ADSelfService Plus uses the OU and group-based structure of AD to control access to cloud apps. IT admins can create multiple policies for different types of users based on their role and the apps they need access to. For example, they can create a policy to provide only users in the HR OU with access to HR applications such as People HR and BambooHR.

Secure, password-less access to the solution

ADSelfService offers NT (New Technology) LAN Manager (NTLM) authentication to provide password-less access to its web console. The user's identity is verified using the credentials they used to log in to their machine.

Challenge 6: Forgotten passwords and locked-out accounts

Forgotten AD passwords and locked accounts have become a part of the corporate grind for most end users. Although AD was released more than two decades ago, Microsoft still doesn't offer an effective solution to this reoccurring problem. According to statistics, 20 to 50 percent of all calls made to the help desk are related to forgotten passwords, with a typical cost per call of about $70. To avoid this expense, the IT team needs to find a solution that offers password self-service capabilities to end users. The selected password self-service solution should provide:

a. Easy installation.
b. Force enrollment.
c. Flexible access.
d. Password reset for remote users.
e. Improved security.
f. License management and optimization.

How does ADSelfService Plus offer password self-service capabilities?

ADSelfService Plus allows users to reset their forgotten passwords and unlock locked-out accounts, without IT assistance.

With security as a primary concern, ADSelfService Plus puts users through stringent authentication techniques every time they attempt a self-service password reset or account unlock.

ADSelfService Plus secures user accounts by verifying an employee's identity with information provided by them during the enrollment process. Verification options include security questions and answers, verification codes, Google Authenticator, Duo Security, SAML Authentication, RSA SecurID, RADIUS, YubiKey Authenticator, AD security Q&A, and mobile app authenticator (Biometric Authentication; QR code-based; push notifications; and one-time passcodes, or OTPs). Each of these verification methods feature powerful customization options.

Users need to enroll in ADSelfService Plus with any combination of the multi-factor authentication techniques enabled by the IT admin.

After the user verifies their identity, they will be allowed to perform the requested self-service actions.

Key benefits:

Easy installation

Installing ADSelfService Plus only takes a few minutes. Start by downloading the software and double-clicking the downloaded file. Download ADSelfService Plus from here.

Facilitate enrollment

Only enrolled users are allowed to reset their AD passwords and unlock their accounts. However, getting end users to enroll for anything, let alone password self-service, is not an easy task.

To ensure a high enrollment rate, ADSelfService Plus supports four features:

a. Force enrollment using a logon script

b. Automatic enrollment by importing data from a CSV file or database

c. Enrollment notifications sent via email or SMS

d. Automatic use of users' AD information for verifying user identity (MFA via SAML and AD security questions)

For more details on the enrollment process and how it helps improve an organization’s ROI, download this informative e-book.

Flexible access

Users can access ADSelfService Plus via the web console, native iOS and Android mobile apps, and the Windows/macOS/Linux logon agent.

- **Web console**

  Users can access the self-service portal through a web browser.

- **Mobile app**

  ADSelfService Plus' native iOS and Android apps help users reset passwords and unlock accounts from their mobile devices, at any time and anywhere.

- **Windows, macOS, and Linux logon agent**

  This feature removes the last bit of dependency in password self-service—the need to borrow someone's computer for password reset. Instead, users can reset passwords and unlock accounts from the login prompt of their machines running on Windows, macOS, or Linux.

Password reset for remote users

Remote users can reset forgotten AD passwords even when they are not connected to the corporate network.

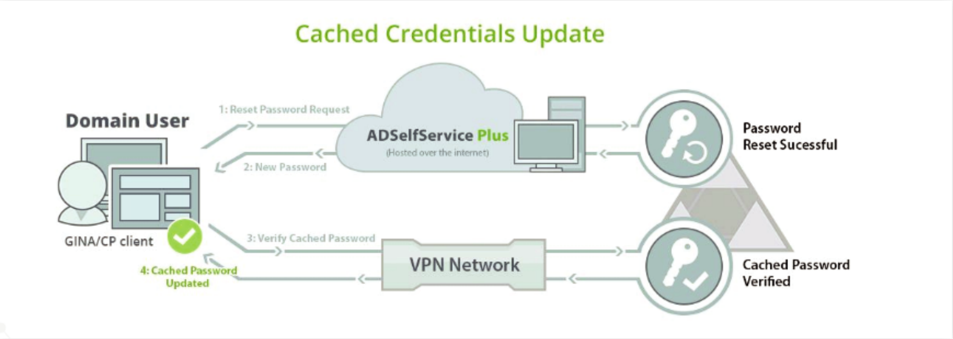


Fig 1: A description of the cached credentials update.

Improved security

ADSelfService Plus offers the options listed below to secure user accounts during password self-service operations.

Features	Security measures
Multi-factor authentication	To authenticate user identity.
Advanced password policy filters which block dictionary words, palindromes, patterns, etc. Also blocks users who failed in verifying their identity.	To prevent brute force attacks, bot-based attacks, low-level research attacks, and man-in-the-middle attacks.
CAPTCHA	To prevent bot-based attacks.
Restrict inactive users	To prevent inactive accounts from being exploited by hackers or disgruntled ex-employees.
Email notification upon password reset and account unlock	To instantly detect and curb any attack attempts.
Session timeout	To minimize the impact of hackers reusing valid session IDs.
Block concurrent login sessions	To prevent misuse of valid user credentials to perform unauthorized actions.

License management and optimization

In an organization, there will always be replacements: old employees will quit, new employees will be recruited. It is a never-ending cycle, so an IT team must expect:

- Inactive (stale) user accounts
- Employee turnover

These factors claim license space that could be given to new arrivals. ADSelfService Plus offers two features, Restrict Inactive Users and Licensed Users Report/Management, that enable IT admins to manage licenses effectively. From time to time, admins can reclaim licenses from inactive users and let new users utilize them. This reduces IT expenses by eliminating the need to purchase unnecessary licenses.

Challenge 7: Expired Active Directory passwords

Regularly changing passwords by setting up policies for password expiration is an important security measure that helps prevent intrusions and stolen passwords. As users with expired passwords will generate increased number of help desk calls, IT admins often resort to sending expiration notifications. However, users often unintentionally let their passwords expire because they have AD accounts only for VPN, Outlook Web Access (OWA), or file shares; these types of users would never actually log on interactively to see standard Windows notifications. For a password expiration notification tool to be effective, it must have the following:

a. Time-phased notifications.

b. Customizable messages.

c. Automated account expiration notification sent via SMS, email, and push notification.

d. OU and group-based access.

How does ADSelfService Plus remind users about their imminent password expiration?

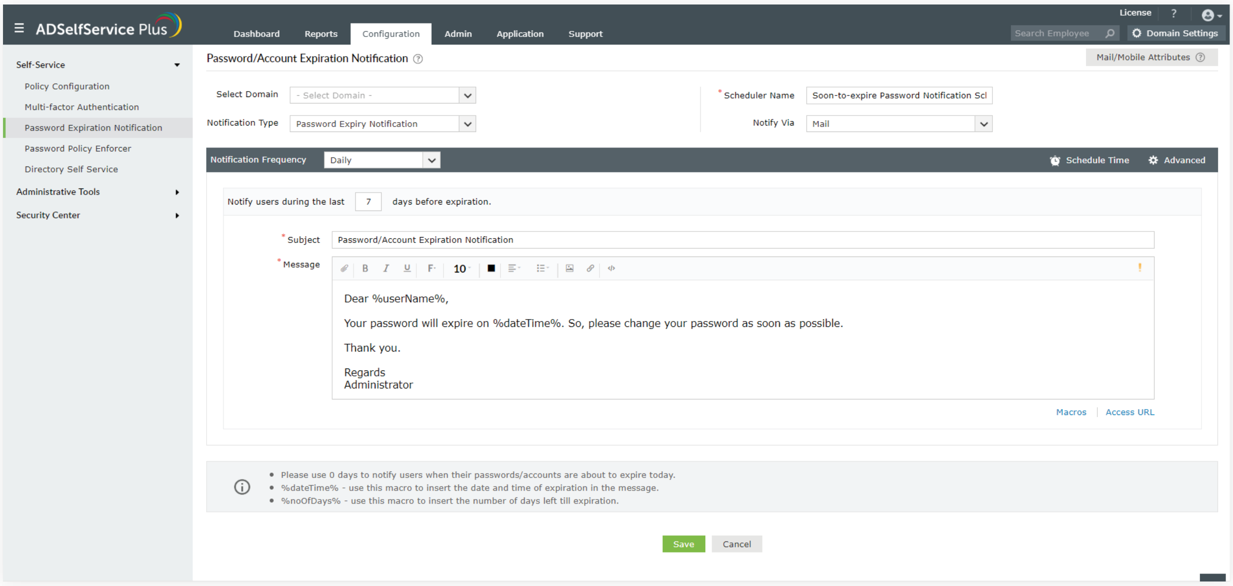
ADSelfService Plus can send reminders about password expiration to users via email, SMS, and push notification. It is highly unlikely that a user will respond to a one-time password change reminder, so ADSelfService Plus enables reminders to be sent at predetermined intervals.

For instance, IT admins can choose to email a password expiration alert when it is 15 days before the password expires; then send a second reminder 10 days before expiration; a third, when it is seven days; a fourth, at three days; and a fifth and final reminder, a day before the password expires. They can even make the content of the email message more imperative every time.

ADSelfService Plus can send reminders about password expiration to users via email, SMS, and push notification. It is highly unlikely that a user will respond to a one-time password change reminder, so ADSelfService Plus enables reminders to be sent at predetermined intervals.

For instance, IT admins can choose to email a password expiration alert when it is 15 days before the password expires; then send a second reminder 10 days before expiration; a third, when it is seven days; a fourth, at three days; and a fifth and final reminder, a day before the password expires. They can even make the content of the email message more imperative every time.

Besides password expiration notifications, ADSelfService Plus can warn users about their AD account expiration too. Managers can also monitor the password or account expiration status of temporary employees. The password expiration notifier can be configured to send reports on the delivery status of all sent notifications to managers and IT admins.



Password/Account Expiration Notification

Select Domain: - Select Domain -

Notification Type: Password Expiry Notification

* Scheduler Name: Soon-to-expire Password Notification Scl

Notify Via: Mail

Notification Frequency: Daily

Notify users during the last 7 days before expiration.

* Subject: Password/Account Expiration Notification

* Message:

Dear %userName%,

Your password will expire on %dateTime%. So, please change your password as soon as possible.

Thank you.

Regards
Administrator

- Please use 0 days to notify users when their passwords/accounts are about to expire today.
- %dateTime% - use this macro to insert the date and time of expiration in the message.
- %noOfDays% - use this macro to insert the number of days left till expiration.

Fig 2: Configuring password and account expiry notifications in ADSelfService Plus.

Sending multiple notification emails achieves a better success rate for getting end users to change their passwords before the expiration date.

Key benefits:

Timely alerts for password expiration

Automate password change reminders sent to users via email, push, and SMS so they can change their passwords before they expire.

Time-phased notifications

Configure multiple notifications to be sent at regular intervals so that reminders result in compliance.

Policy-based access control

Control how and which users should receive notifications by configuring policies based on domain, OU, and group membership.

Automated account expiration notifier

Warn users about their imminent AD account expiration through email and SMS.

Report scheduler

Schedule and export reports directly to the manager's mailbox, including details on which passwords are soon to expire, as well as the delivery status of expiration notifications.

Customizable messages

Customize email and SMS messages by adding specific instructions and images.

Challenge 8: Synchronizing Active Directory passwords across cloud and on-premises apps

Users deal with their password-saturated lives by resorting to unsafe practices like writing down their passwords. The effective solution is to deploy an AD password synchronization tool that applies any changes to AD passwords to the passwords of connected cloud-based and on-premises applications. But implementing password synchronization is a difficult process. Take Microsoft's own platforms, for example. Setting up password sync between on-premises AD and Office 365 is a complex and time-consuming process without the right solution. An effective password sync solution must offer:

> a. Real-time password sync so there is little to no delay in synchronizing passwords with the connected systems and applications.
> b. Support for all major cloud applications and systems.
> c. Freedom to choose when to sync passwords.
> d. The option to enable password sync based on policies.
> e. The option to sync the password only after the password reset or change is successful in AD.
> f. One strong password policy across AD and cloud apps.

How does ADSelfService Plus offer one password for multiple apps?

ADSelfService Plus is an AD password synchronization solution that provides real-time password sync for several on-premises and cloud applications to help users deal with password fatigue in a secure way. When a user makes changes to their Windows AD password using ADSelfService Plus or any of the native methods in Windows, the changes are automatically reflected in all connected applications as well. The Password Sync Agent synchronizes any password changes made via the native Windows interface (Ctrl+Alt+Del screen) or password resets via Active Directory Users and Computers (ADUC).

Key benefits:

Real-time password synchronization

ADSelfService Plus comes bundled with a Password Sync Agent. The Password Sync Agent functions as a background service and is continuously on the lookout for password changes and password reset operations. The password sync agent captures the new password and encrypts it to ensure security. The encrypted password is then synchronized with the various connected applications and systems.

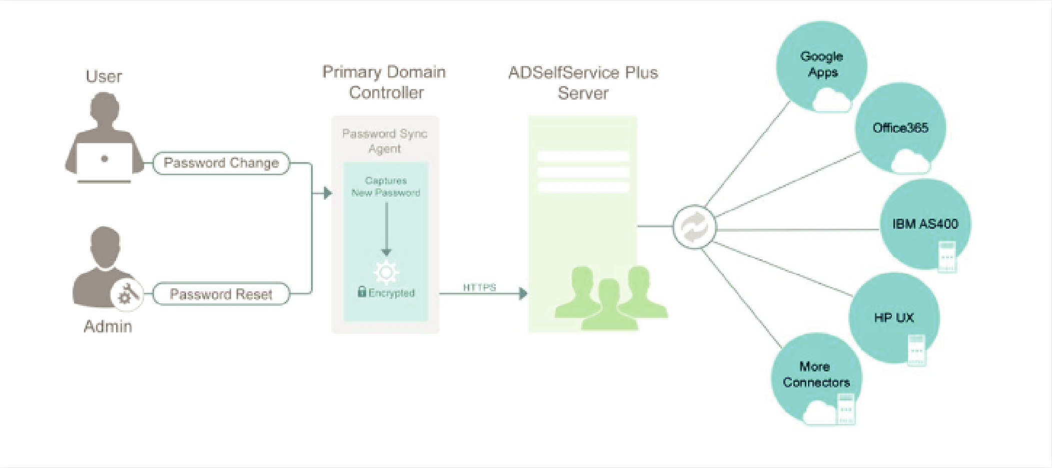


Fig 4: The real-time password sync process.

The entire process, from users changing their passwords in AD to the passwords being synchronized in target systems and applications, takes less than 30 seconds.

Support for major applications and systems

ADSelfService Plus supports Windows AD password synchronization across the following systems and cloud applications:

Cloud-based	On-premises
G Suite	IBM/iAS400
Office 365/Azure	Oracle E-Business Suite
Salesforce	OpenLDAP
Zendesk	HP UX
Microsoft Dynamics CRM	AD LDS
Zoho	SAP NetWeaver
ServiceNow	Oracle Database
	MS SQL Server Database
	PostgreSQL Database

Freedom to choose when to sync passwords

ADSelfService Plus enables IT admins to either force synchronize passwords between AD and other enterprise applications, or let end users decide whether to sync the password or not.

Policy-based password synchronization

IT admins can choose to enable OU and group-based password synchronization, and control which user credentials get synchronized.

Sync password only after successful reset or change in AD

Password synchronization is initiated only after the successful AD password reset or change. This helps maintain the consistency of passwords. Also, there's an option to synchronize account unlocks between cloud-based and on-premises accounts irrespective of the lockout status of the users' AD account.

Enforce custom password policies

ADSelfService Plus enables IT admins to create custom password policies with advanced filters to block dictionary words, patterns, etc. They can also enforce the created password policy across on-premises and cloud applications to improve the network security of their organization.

Challenge 9: Enforcing stronger password policies

Hacking passwords is the easiest way to gain access to a user account in AD. Hackers have been able to compromise the passwords of AD users for years. This is no surprise, considering the password policy and password controls in AD have not been changed since 2000. Therefore, current hacker strategies and technologies still work on a Windows Server 2019 AD, just as they did on a Windows 2000 Mixed Mode AD domain version. To protect users' passwords, the selected self-service solution must also have the following features:

- Ability to apply password rules that safeguard passwords against the latest cyberattacks.

  The option to enforce custom password policies granularly based on OUs and groups.
- Password strength analyzer that helps users select strong passwords by displaying custom messages on password change screens.

How does ADSelfService Plus protect Active Directory from password attacks?

ADSelfService Plus comes with a granular password policy enforcer feature, which enacts strong password policy controls in AD. ADSelfService Plus has a number of password policy rules that are not native in AD. These rules are specifically designed to protect against many of the most common password attack methods used by hackers, including dictionary attacks, rainbow table attacks, and brute force attacks.

Key benefits:

Advanced password policy rules

ADSelfService Plus has many password policy settings that are not native in AD. These include:

a. Dictionary rule: Blocks passwords that contain entries from both language dictionaries and hacker dictionaries.

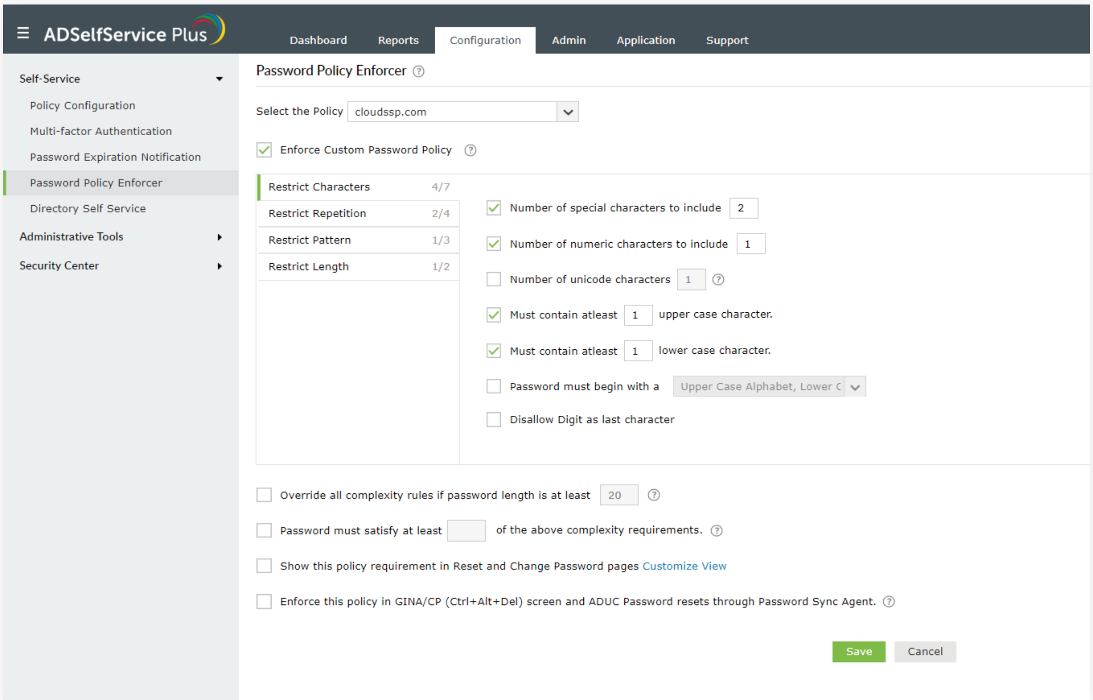
b. Palindrome: Rejects users passwords that are a palindrome.

c. Keyboard patterns: Rejects common keyboard patterns such as QWERTY, 12345, and ASDFGH.

d. Repeating patterns: Bans passwords containing characters that are repeated consecutively, as well as passwords containing consecutive characters from usernames.

e. Multiple complexity enhancements: Enforces both lowercase and uppercase letters, specifies the exact number of special characters and digits required, makes Unicode characters mandatory, makes starting passwords with a letter mandatory, and more.

f. Password history check for password resets: Prevents users from circumventing the minimum password age and using their old passwords during password resets. By default, password history checks are only done when users change their password.



Password Policy Enforcer

Select the Policy: cloudssp.com

☑ Enforce Custom Password Policy

☑ Number of special characters to include 2

☑ Number of numeric characters to include 1

□ Number of unicode characters 1

☑ Must contain atleast 1 upper case character.

☑ Must contain atleast 1 lower case character.

□ Password must begin with a Upper Case Alphabet, Lower C

□ Disallow Digit as last character

□ Override all complexity rules if password length is at least 20

□ Password must satisfy at least of the above complexity requirements.

□ Show this policy requirement in Reset and Change Password pages Customize View

□ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

Fig 5: Password Policy Enforcer tab in ADSelfService Plus

Granular password policies

Admins can create and enforce multiple password policies based on OUs and groups.

Display custom password policy messages

ADSelfService Plus can also replace the obscure password policy rules displayed during change password operations on the Ctrl+Alt+Del screen. By default, Windows doesn't specifically define which rules a user's password fails to comply with. ADSelfService Plus can display the correct password requirements to end users, including the exact number of special characters, numbers, lowercase letters, etc. This helps users easily choose a strong password on the first try.

Challenge 10: Monitoring and managing outdated user profiles

Keeping AD up-to-date with end users' profile information, such as their mobile number, photo, and address, is difficult. Nonetheless, it is a crucial task because this information is often used in an organization's employee directory listing.

An effective directory self-update solution must have the following features:

a. Modification rules which auto-populate values for attributes based on the set organizational policy.
b. Mandatory fields and force update.
c. Custom attribute support.
d. Easily customizable interface.

How does ADSelfService Plus help organizations keep their Active Directory up-to-date?

ADSelfService Plus offers a secure portal through which end users can self-update their AD profile information. Drop-down lists and data validation ensure data is more accurate. The user can only update the information that the administrator allows, and IT admins can force users to update their information when they log in to the self-service portal.

Key benefits:

Modification rules

ADSelfService Plus enables IT admins to set modification rules for individual layouts that auto-populate values for attributes based on the organizational policy. Changes made by the users are checked with the configured modification rules' conditions. If the changes satisfy the provided conditions, the values assigned by the IT admin to specific attributes are also changed.

Mandatory fields and force update

IT admins can set any fields as mandatory. Users must enter the value of the mandatory fields to be able to save the other details they have entered. Also, IT admins can force users to self-update their information when they log in to the self-service portal.

Custom attributes support

Apart from the default attributes in AD, ADSelfService Plus also enables IT admins to configure custom attributes to obtain organization-specific information from end users.

Easily customizable interface with drag-and-drop support

The form used to obtain the information from end users must be easy to build and customize. ADSelfService Plus provides a drag-and-drop layout so IT admins can quickly build custom forms. It also allows them to separate similar attributes into groups.

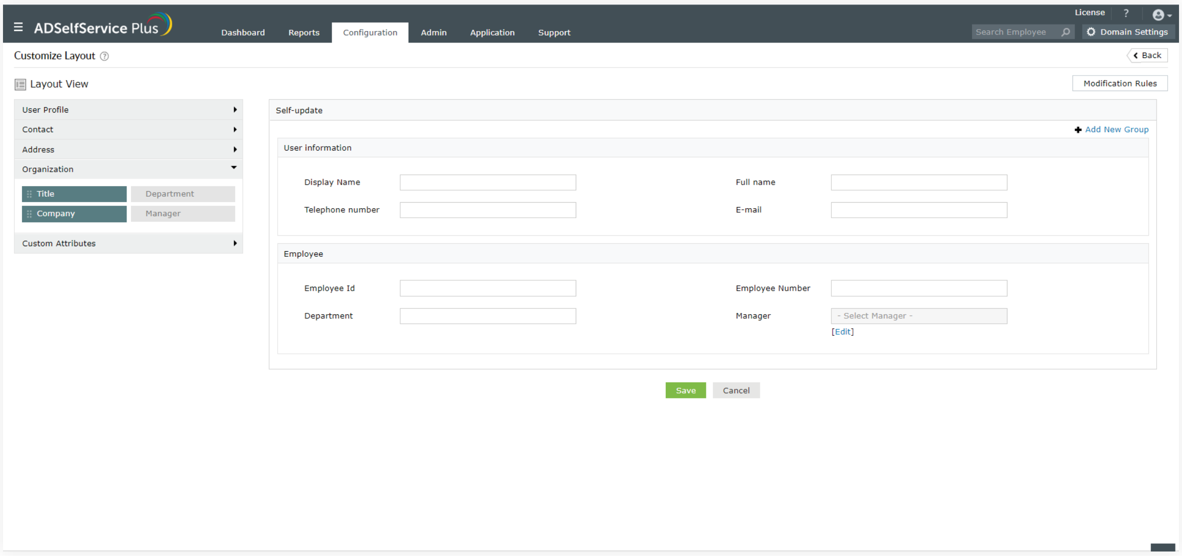


Fig 7: The drag-and-drop self-update layout in ADSelfService Plus.

Challenge 11: Managing Active Directory group membership

Group management is an important task in making sure that IT resources are accessed only by authorized personnel. Cycles of adding and removing users from groups can consume a lot of an IT admin's time. The number of groups and the frequency of role changes make this a challenging task, and can lead to major problems like:

a. An increase in help desk calls from users requesting resource allocation.

b. Loss in employee productivity while users wait to obtain the required access rights.

c. Unsolicited emails being sent to users who have changed roles but still receive messages from their previous distribution group.

How does ADSelfService Plus automate group management through self-service?

ADSelfService Plus enables group owners to delegate the burden of adding members to a group to end users. The group owner can authorize self-service management for their group and designate select users to oversee membership tasks.

IT admins can define group subscription policies that determine which users can subscribe to which groups from ADSelfService Plus. Essentially, these policies act as a security barrier that prevents unauthorized subscriptions to groups.The IT admins can also enable users to view the names of other members of the group.

Key benefits:

Quite often users email or call the help desk to request access to a particular email group. IT admins can easily identify the email groups that a user should join based on their departmental role. The full list of email groups an end user in a specific role should join can be provided through a group subscription policy.

ADSelfService Plus enables IT admins to define which groups are available for self-subscription, as well as which users are authorized to self-subscribe. For each group in AD, IT admins can also define a list of users who can opt-in or opt-out of that group.

Conclusion

Every IT admin must be prepared to address all the challenges listed above to ensure a productive and secure environment for end users. It is nearly impossible to find a single solution that meets all these business needs, so many organizations resort to tackling each challenge with a separate solution. This strategy might offer a short-term fix but, in the long run, it only makes the situation more complicated for the IT team and end users.

ADSelfService Plus' arsenal of self-service password management and SSO capabilities are tailored to meet any organization's requirements, reduce the burden on IT help desks, and bring down costs.

Further reading

Download ADSelfService Plus

Receive a 30-day free trial of ADSelfService Plus here.

Evaluator's guide

Download the evaluator's guide to learn how different features in ADSelfService Plus will benefit every organization.

Scalability guide

Can ADSelfService Plus scale to any enterprise environment and meet the demands of the ever-changing IT landscape? Click here to discover how.

Contact support

If you need assistance or have questions, contact our technical support team.

Direct dialing number: +1-408-916-9890

Support email: support@adselfserviceplus.com

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

ManageEngine
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, visit
www.manageengine.com/products/self-service-password.

$ Get Quote   ⤓ Download