ManageEngine
ADSelfService Plus

Use cases

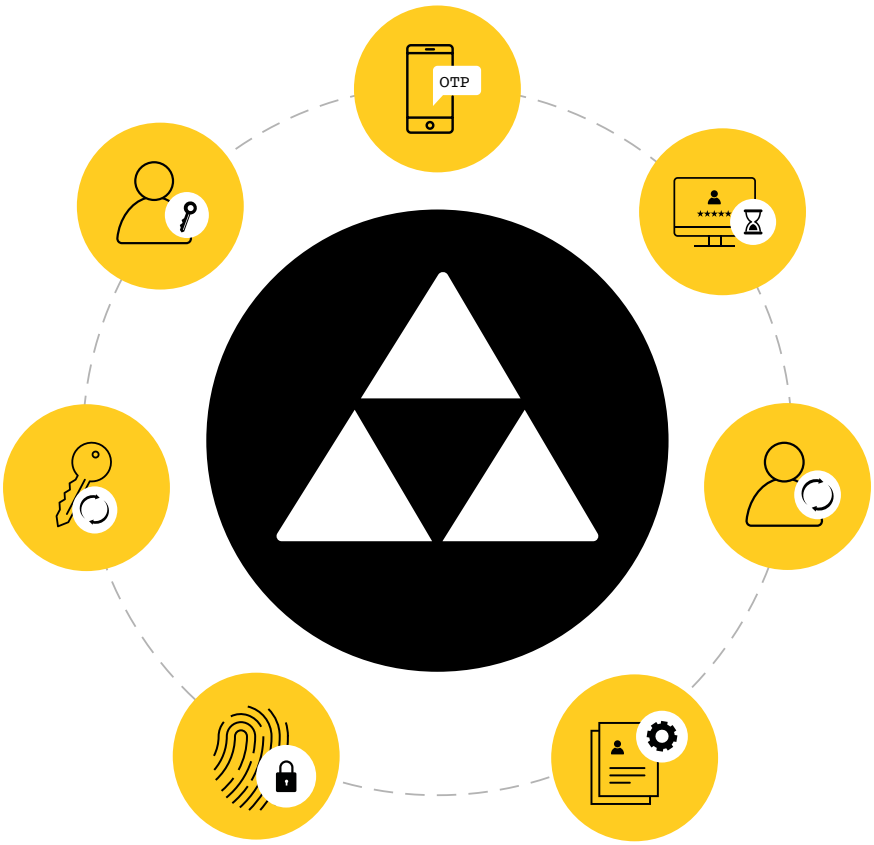


Table of **contents**

Use case 1

Securing access to enterprise user machines when offline

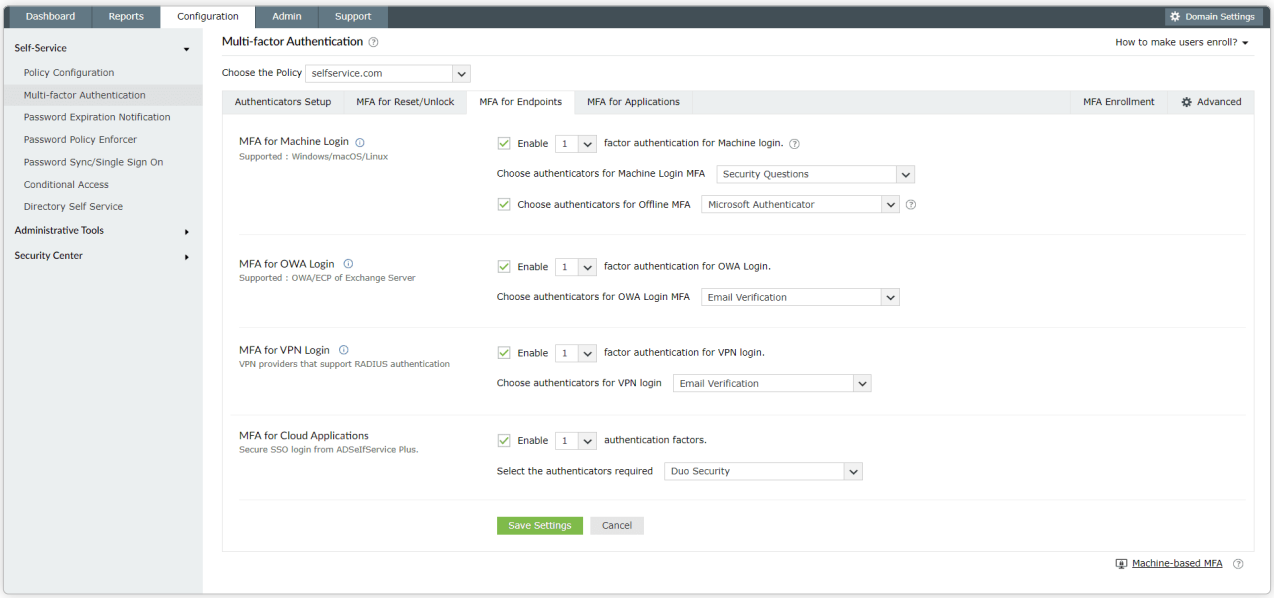
Your users are connected to the enterprise network either locally or remotely through RDP or VPN. Loss of network connection is a possibility, leading them to lose access to gated resources. This also causes the risk of disconnection from the MFA solution, causing a security loophole. Disabling MFA or locking out users when offline are not viable solutions to this issue.

How does ADSelfService Plus help?

ADSelfService Plus offers both offline and online MFA for machine logins. Online MFA necessitates a connection to the server, whereas offline MFA ensures secure access for Windows and macOS machine logins without the need for connectivity.

The solution supports Microsoft Authenticator, Google Authenticator, Zoho OneAuth's TOTP feature, and even your in-house TOTP provider as authenticators for offline MFA. The authenticator information is securely stored on the user's systems, available to be accessed during offline authentication.

You can also use offline MFA to secure peripheral Windows actions like UAC prompts, RDP server authentication, and machine unlocks.



Use case 2

Securing peripheral endpoints in your enterprise

Your enterprise network has a myriad of endpoints, local and remote. While machine logins and web applications are often scrutinized and secured, your peripheral endpoints like RDP and OWA may be lacking protection. Intruders on the lookout for loopholes in your system security could exploit such under-protected secondary endpoints and compromise your system.

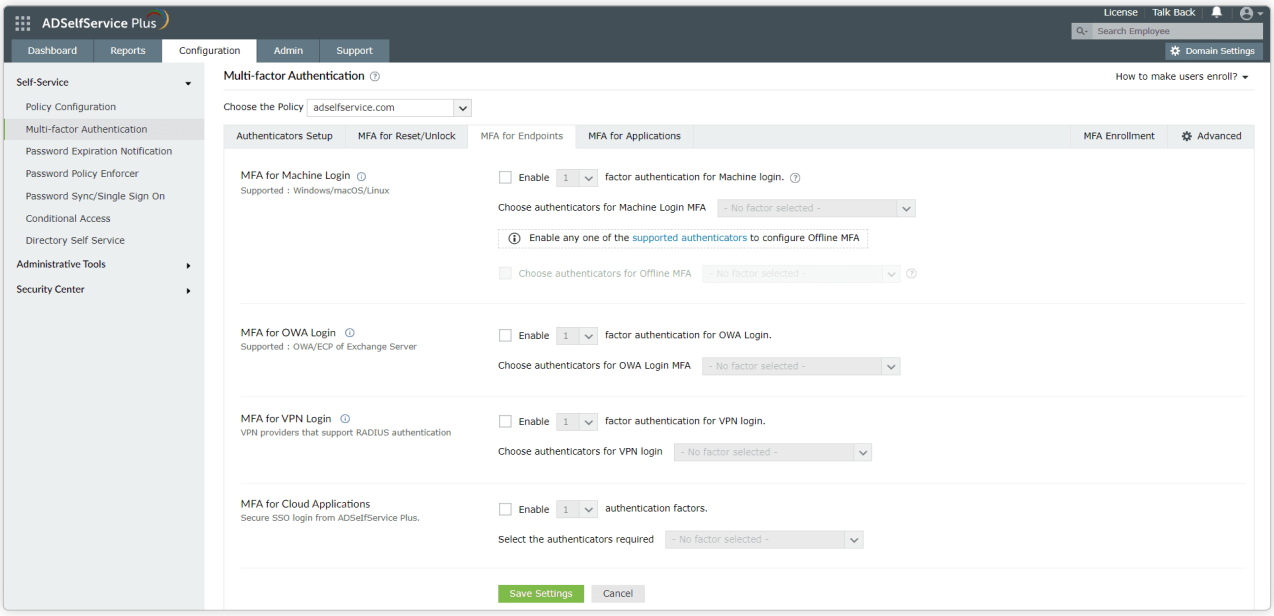
How does ADSelfService Plus help?

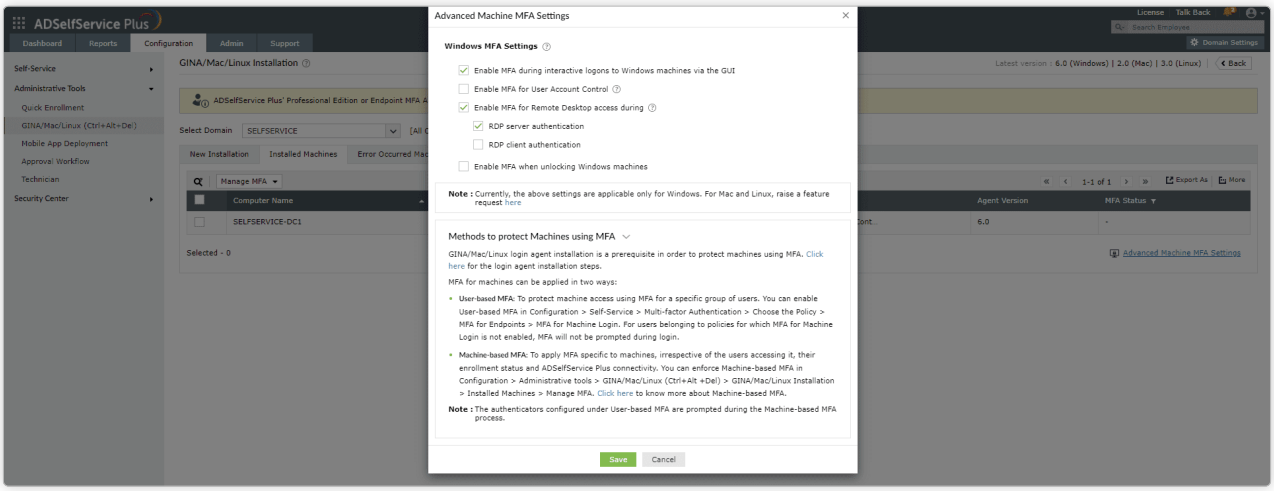
ADSelfService Plus' MFA feature provides one or more layers of authentication in addition to the default username and password-based authentication. The feature protects local and remote machine logins, enterprise application logins as well as:

1. Access through VPN and other RADIUS-based endpoints
2. Microsoft RDP client and server authentication
3. Microsoft OWA and Exchange Admin Center logins
4. Windows user account control credential prompts
5. 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 connection.





Use case 3

Balancing security posture and user experience

Your enterprise comprises of networks and endpoints that carry sensitive customer data and intellectual property. To ensure the data contained in your systems remain secure and unexploited, you decide to enable advanced authentication systems with rigid MFA factors.

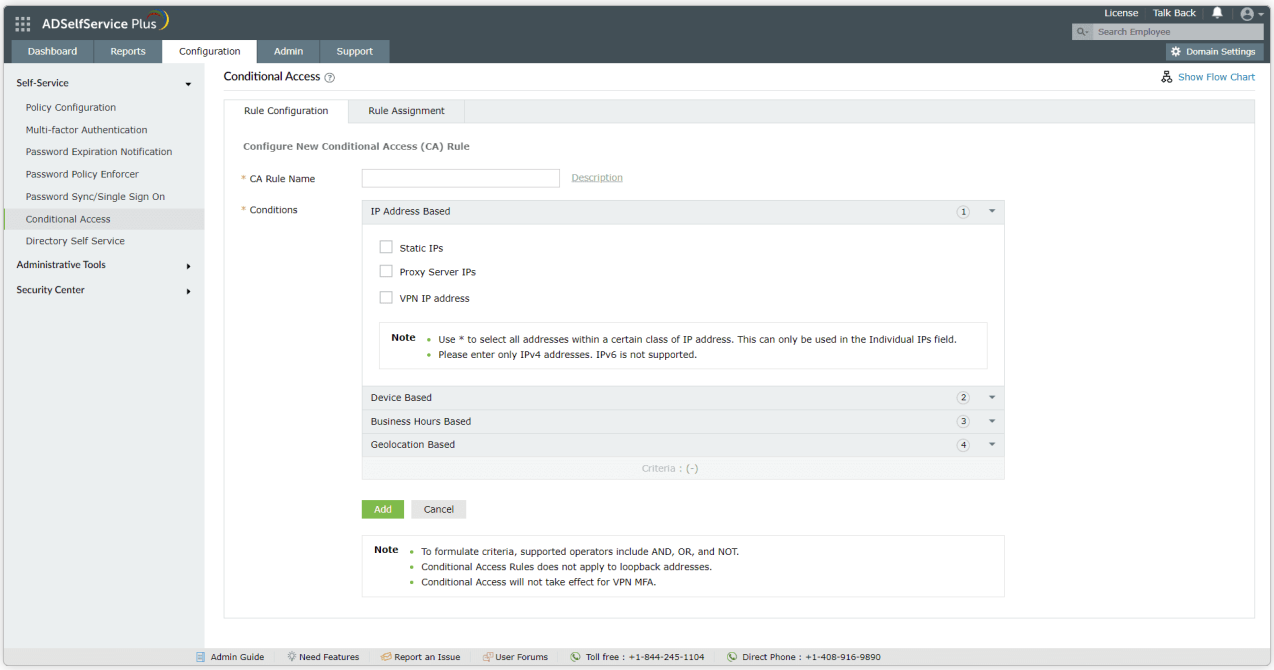
But setting up a highly complex authentication system across your enterprise has its implications. Users with lower privileges, temporary users, and guest users don't require a rigorous identification process. Enabling an unnecessarily stringent access flow for such users can daze them and hamper their productivity.

How does ADSelfService Plus help?

ADSelfService Plus offers a conditional access feature that automates the access control process and adjusts security posture based on context. With this feature, authentication flow and factors are automatically altered after the access data is gathered and risk is quantified. The access data is analyzed using pre-configured rules built on AND and OR operators and depending on the risk level, pre-configured authentication policies with either heightened or lowered security posture are applied.

IP address, geolocation, time of access, and device type are the access information analyzed to determine the appropriate authentication policy. Conditional access can be used to automate access to the following actions:

- Enterprise application access via SSO
- Endpoint logins
- Self-service password resets and account unlocks



Use case 4

Evading phishing attacks through FIDO2 authenticators

Your enterprise, by choice or due to compliance laws, has updated its IT policy to require MFA. You decide to set up MFA to secure your network endpoints. Your enterprise consists of users with varying levels of privilege, with many user accounts storing sensitive and crucial data. You need an MFA solution that not only evades credential-based attacks like brute-force and dictionary attacks, but also thwarts phishing attacks.

How does ADSelfService Plus help?

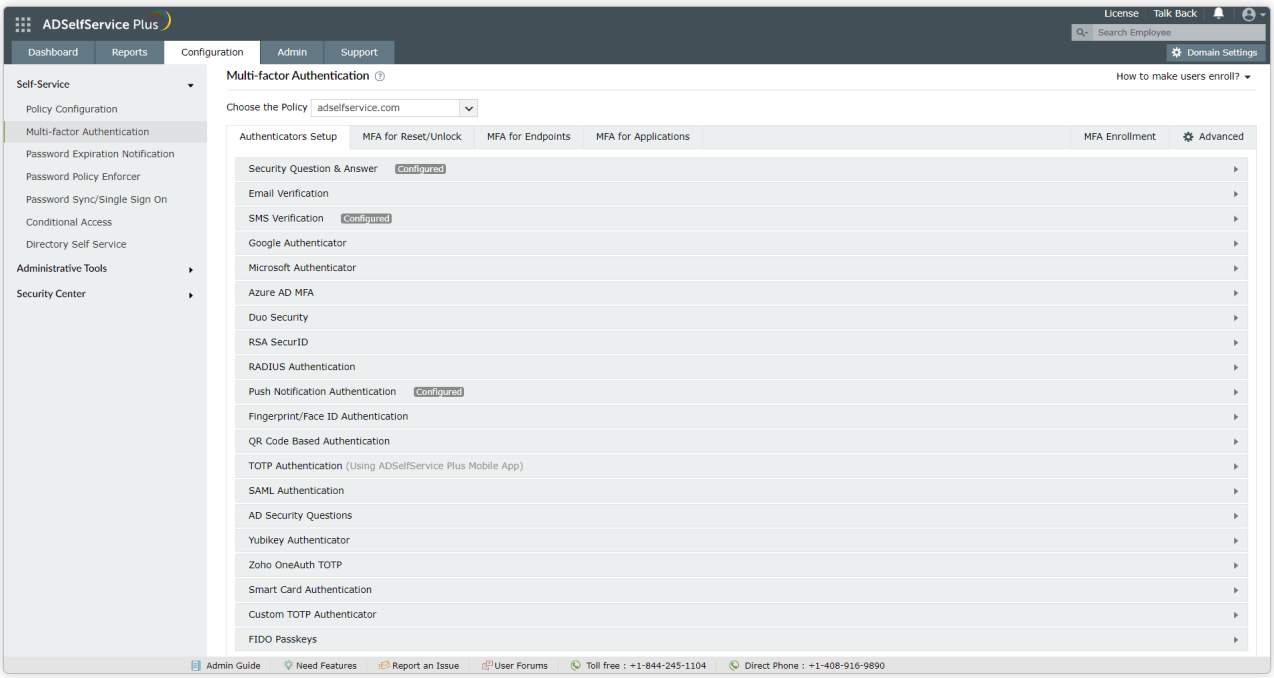
ADSelfService Plus provides 20, diverse authenticators to secure major enterprise endpoints including machines, web applications, VPN, and RDP. These include advanced, phishing-resistant authenticators such as FIDO2 passkeys, smart cards, and biometrics. Since these methods don't rely on any information known to users, bad actors who have phished such information from users cannot complete MFA and takeover their accounts.

You can configure up to three levels of authentication besides username and password for identity verification. So by combining phishing-resistant methods with other types of MFA such as push notifications and TOTPs, you can create an MFA flow that is resistant a myriad of attacks.

ADSelfService Plus also supports granular application of MFA using its AD OU-based and group-based policies. You can configure particular types of authenticators for specific endpoints and end-users. This ensures custom authentication flows appropriate for the end user's privileges.

Here is the full list of authenticators supported by ADSelfService Plus:

- Security Questions and Answers
- Email Verification
- SMS Verification
- Google Authenticator
- Microsoft Authenticator
- Azure AD MFA
- Duo Security
- RSA SecurID
- RADIUS Authentication
- Push Notification Authentication
- Biometric Authentication
- QR Code-Based Authentication
- TOTP Authentication
- SAML Authentication
- AD Security Questions
- YubiKey Authentication
- Zoho OneAuth TOTP Authentication
- Smart Card Authentication
- Custom TOTP Authenticator
- FIDO Passkeys



Use case 5

Configuring seamless and secure enterprise application access

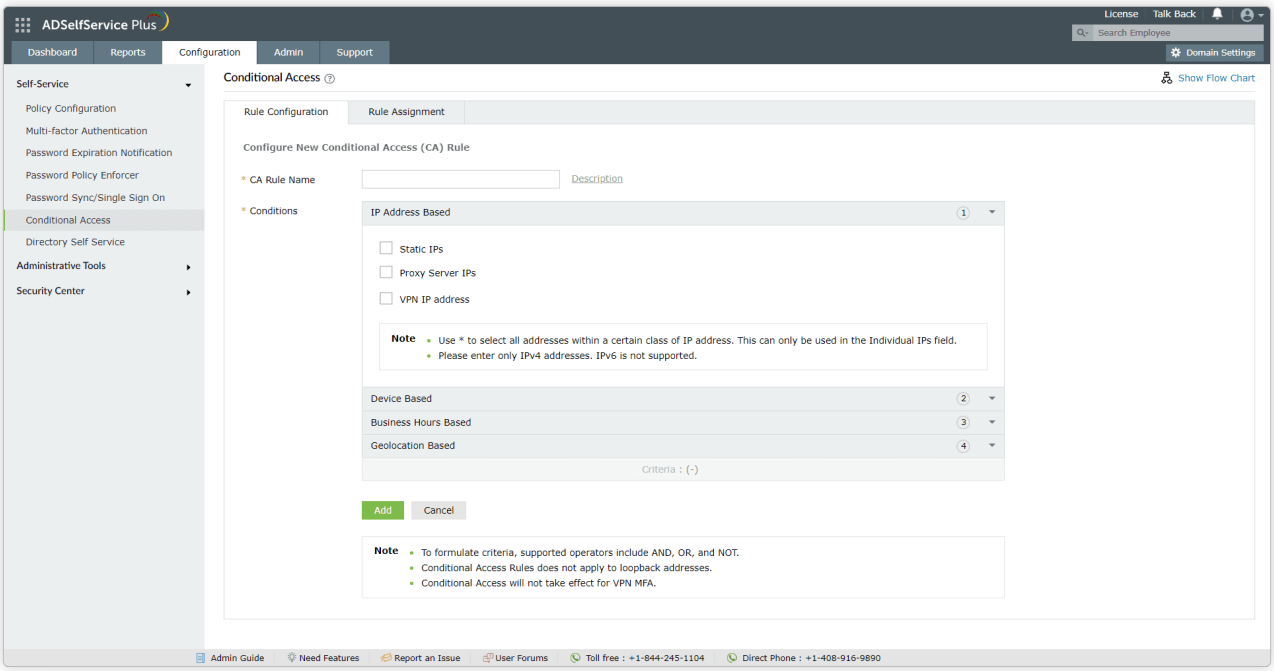
Your users are required to use multiple enterprise applications to perform their day-to-day tasks. This requires them to maintain multiple user accounts, and subsequently, passwords. Using multiple user accounts could also create multiple opportunities for hackers to exploit. User productivity also drops from having to log into each application. They could even forget their passwords. Using multiple user accounts could also create multiple opportunities for hackers to exploit. To circumvent this, you need to reduce the number of user accounts and passwords that users have to go through in a day.

How ADSelfService Plus helps:

ADSelfService Plus supports passwordless single sign-on (SSO) for SAML-enabled, OAuth-enabled, or OIDC-enabled applications. The solution supports over a hundred established applications including Microsoft 365, Google Workspace, Salesforce, and Slack for SSO. You can also integrate your in-house applications for passwordless SSO.

Users simply have to validate their identity using ADSelfService Plus' MFA feature. Upon successful verification, they are free to access any of the integrated applications without further authentication.

Around 20 authentication methods are supported for MFA, including FIDO2 passkeys, biometrics, and TOTP. This ensures users have access to all their enterprise accounts is thoroughly secured, and don't have to juggle multiple passwords to maintain access.



Use case 6

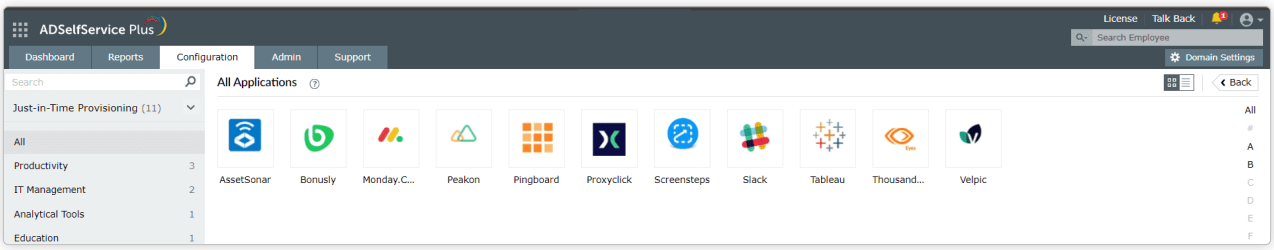
Streamlining enterprise application onboarding for end-users

Your enterprise employs multiple applications across its departments to meet its business and work-force requirements. When new users are onboarded or existing users change teams, they will be required to sign up to new enterprise applications. This can mean creating user accounts for each application, a very time-consuming process. You may also set up bulk user provisioning, but errors may creep in, resulting in loss of access and impeded user productivity.

How does ADSelfService Plus help?

ADSelfService Plus offers just-in-time (JIT) user provisioning using the SCIM protocol. This capability automatically creates user accounts for all the required integrated applications during the first access attempt via ADSelfService Plus' SSO feature. This means users and IT teams don't have to spend time creating users and managing user accounts. They simply have to authenticate to ADSelfService Plus, and they'll automatically gain access to integrated applications.

ADSelfService Plus currently supports JIT provisioning for over 10 applications. Applications supported include Bonusly, Slack, Tableau, and Velpic.



Use case 7

Letting employees reset their own domain account password

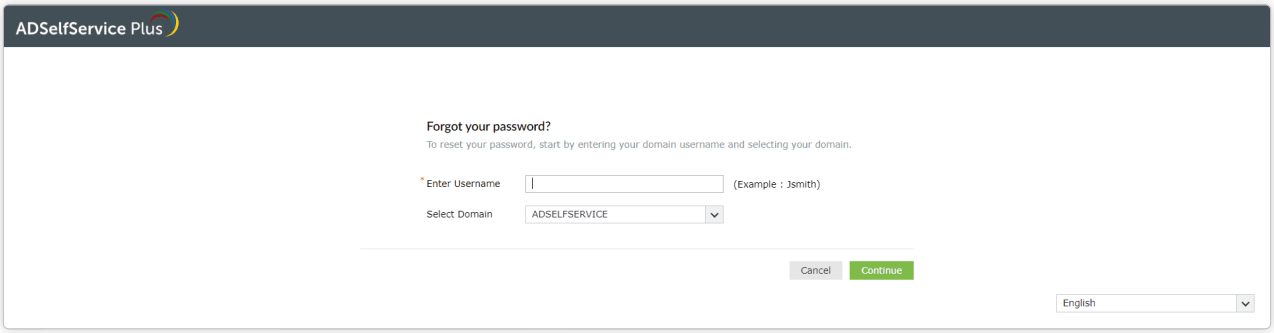
Your end users keep forgetting their AD and enterprise application passwords, and this causes a huge burden on your help desk. You need to give end users the power to reset their own passwords, but there is no provision in Active Directory that allows you to do this. So, how do you allow end users to securely reset their domain account passwords?

How ADSelfService Plus helps:

ADSelfService Plus offers self-service password reset for AD and enterprise applications, empowering end users to securely reset their passwords. The solution offers its self-service password reset from the following portals:

- The user's Windows, macOS, and Linux login screens
- The ADSelfService Plus end user portal
- The ADSelfService Plus Android and iOS mobile app

The self-service password reset feature is also secured through the ADSelfService Plus' MFA feature and the passwords being created are scrutinized using advanced password policies and the Have I Been Pwned? integration. This ensures the users verify their identity and set complex passwords that are resilient to breach.



Use case 8

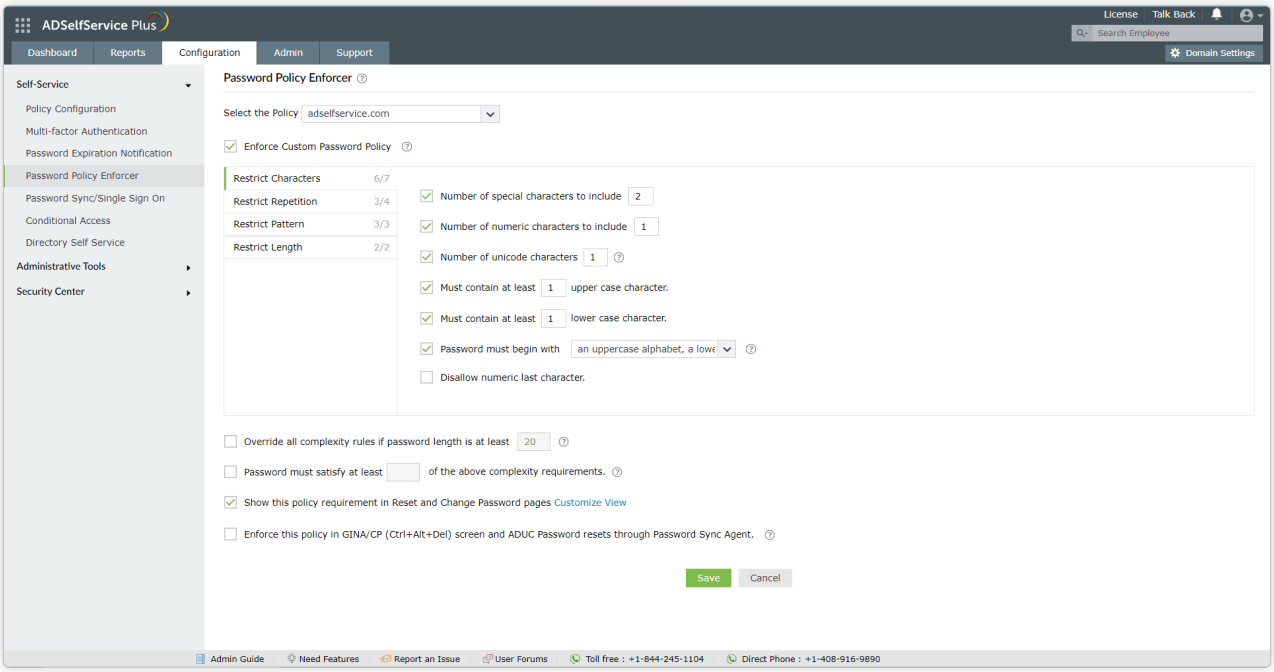
Enabling advanced password policies

While enterprises are aware of the benefits of configuring stringent password policies, AD's password policies are not granular enough. They can only be applied to entire domains or groups and cannot be applied to OUs. They are also composed of surface-level rules that may not contribute to creating complex passwords that evade brute-forcing. This makes them insufficient to abide by regulations like NIST.

How ADSelfService Plus helps:

ADSelfService Plus provides an advanced password policy enforcer that is designed to protect users against the most common attack methods, such as dictionary attacks, brute force attacks, pattern attacks, and rainbow table attacks. The password policy enforcer contains rules that scrutinize character types, length, age, and patterns used. This helps block passwords that contain entries from language dictionaries, hacker dictionaries, common keyboard patterns, and repeating patterns.

You can enforce different password policies with varying degrees of complexity across your domain based on OUs and groups, so those with higher privileges and access to more secure data are required to use stronger passwords than those with fewer privileges. The password policies enabled can be enforced during self-service password resets and web-based password changes using ADSelfService Plus as well as native password changes in the Ctrl+Alt+Del portal and password resets in the Active Directory Users and Computers portal.



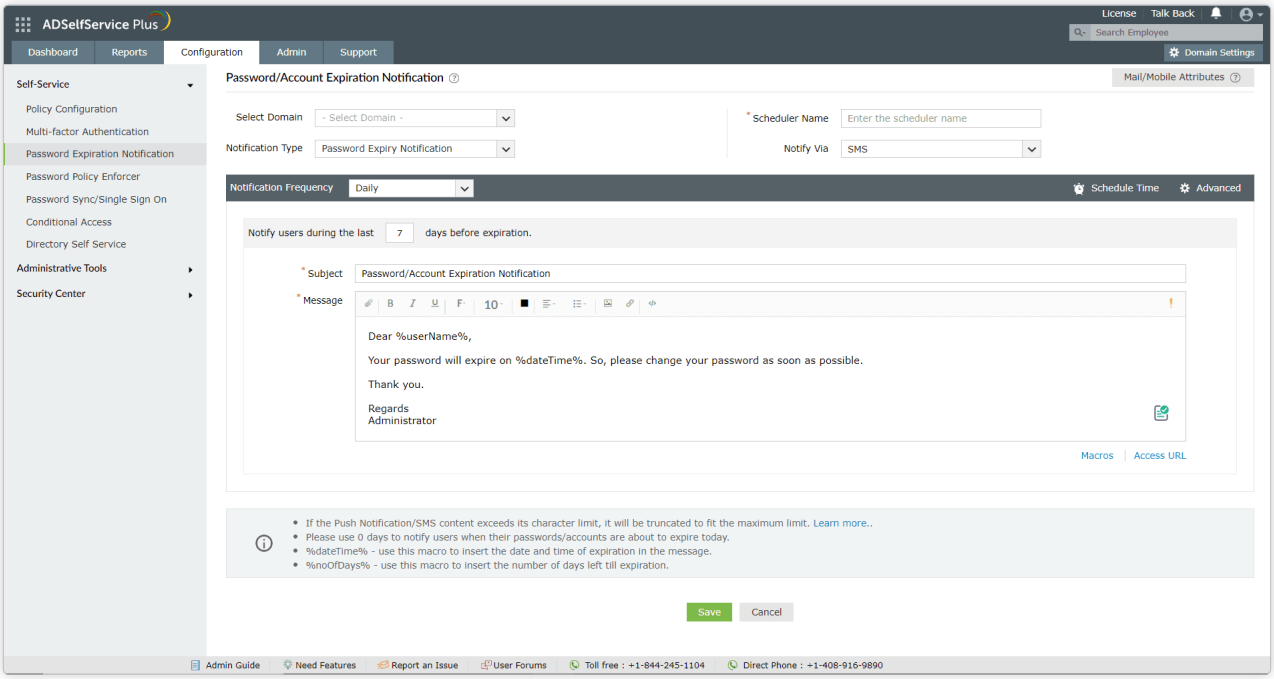
Use case 9

Reminding employees about their password expiration

If users don't change their domain passwords before they expire, they will lose access to business-critical applications that depend on domain authentication, including Outlook Web Access (OWA) and your organization's VPN. The default tray notification in Windows for soon-to-expire passwords is too obscure, and employees don't notice it and take necessary action. Is there a better way to notify users before their passwords expire? And how do you make sure users are reading notifications?

How ADSelfService Plus helps:

ADSelfService Plus supports password expiration notification, which can be used to remind users about their soon-to-expire passwords at regular intervals. The product searches Active Directory for user accounts whose passwords are about to expire and notifies the account owners via SMS, email, or push notifications recommending a password change.You can choose whether to notify users weekly, daily, or on certain days before the password is set to expire.



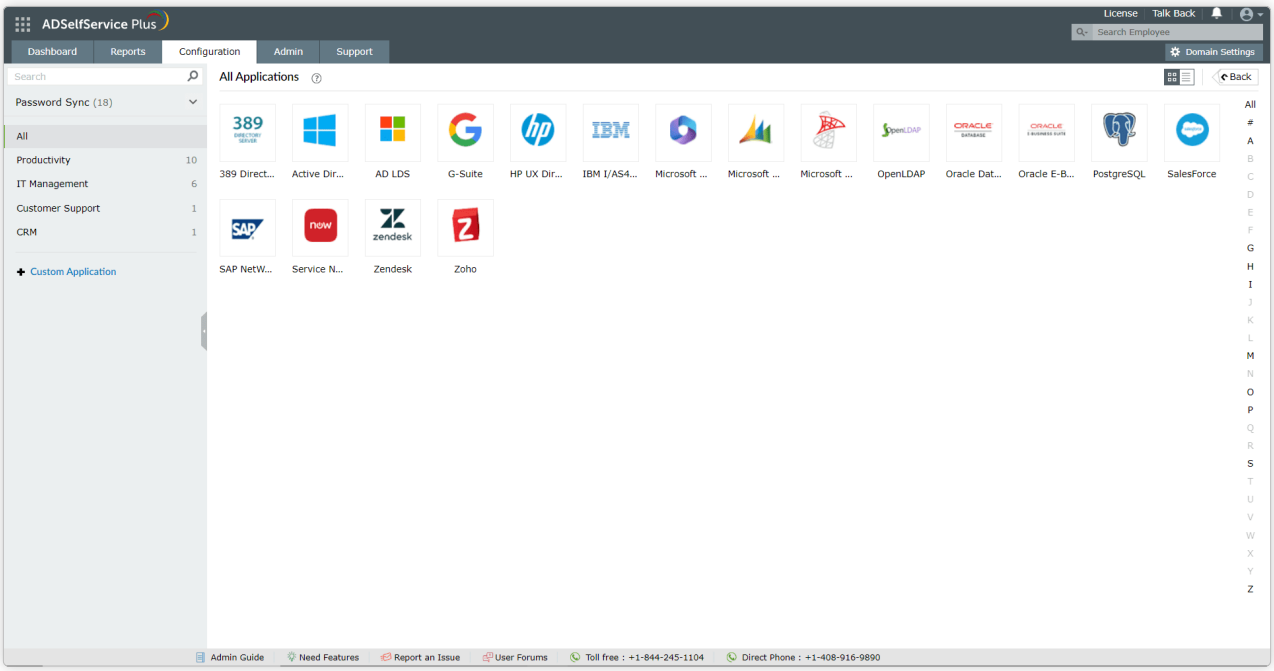
Use case 10

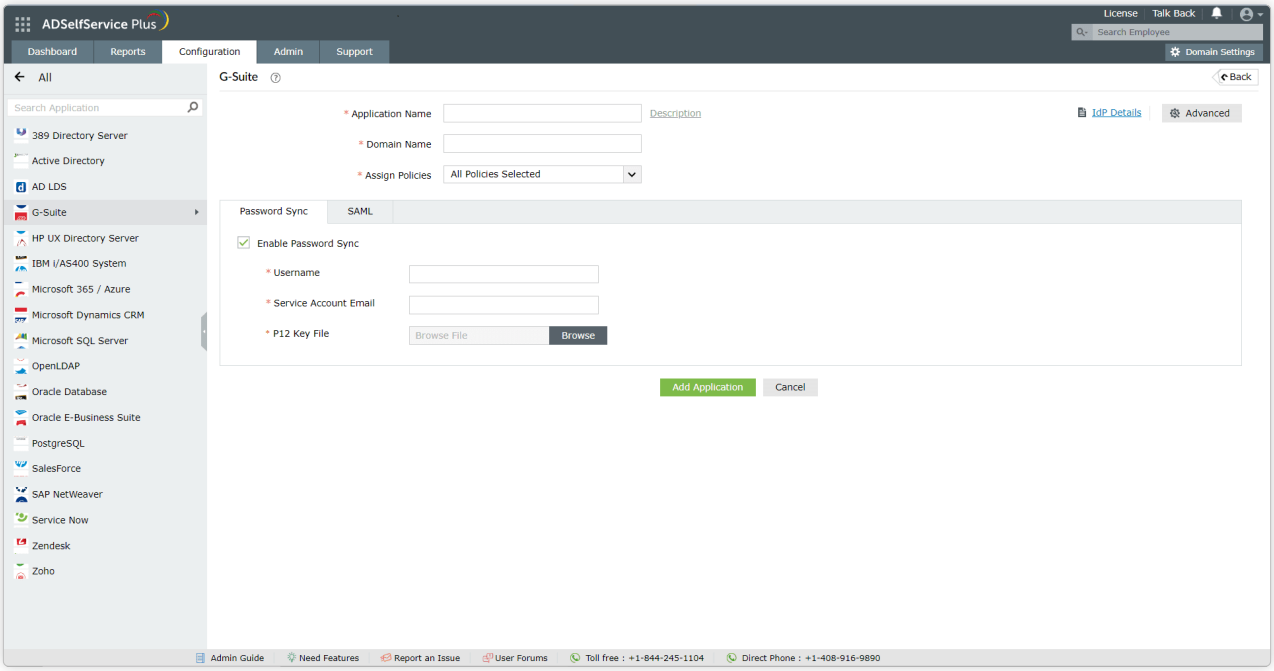
Synchronizing password changes across major enterprise applications

Aside from their Windows domain account, there's a good chance that your end users have multiple user accounts for applications like Salesforce, Microsoft 365, and Google Workspace. Password fatigue is an unfortunate effect of having to juggle multiple passwords. It could lead users to unsafe password management practices such as reusing passwords across multiple user accounts and manually noting down passwords. This could leave their digital identities vulnerable to breach.

How ADSelfService Plus helps:

ADSelfService Plus' password synchronization feature syncs password changes and resets, both native and via ADSelfService Plus, across integrated applications. The solution comes bundled with a password sync agent that synchronizes native password changes to users' Active Directory passwords in real-time with other linked cloud applications and on-premises systems. The password changes can be synchronized granularly for select users belonging to specific OUs and groups and for particular applications. This helps users maintain as many passwords as they prefer across their applications.





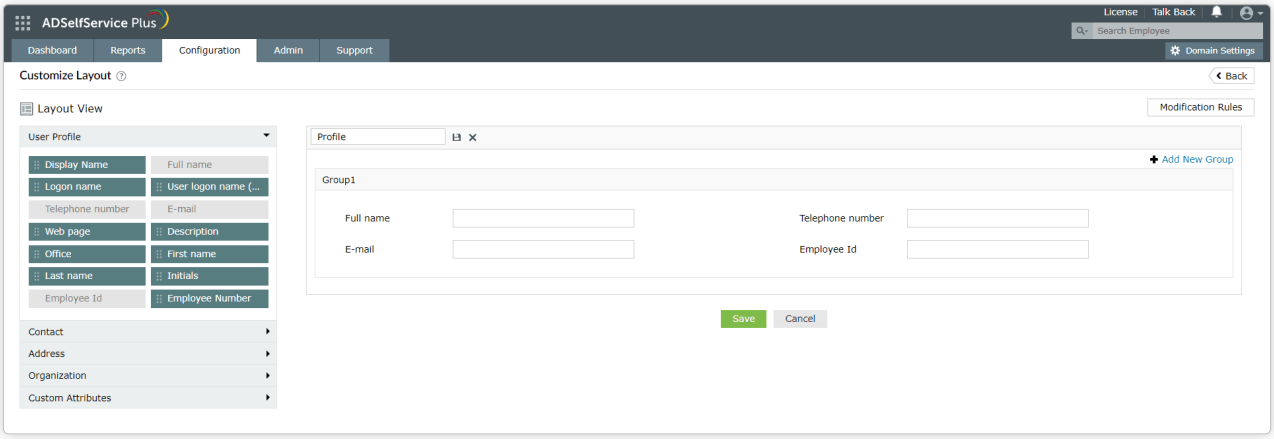
Use case 11

Forcing users to update their photo and contact information in Active Directory

If you're using the profile information of users stored in Active Directory to update your organization's human resource management system (HRMS) or company white pages, you need to make sure that information remains up to date. Manually updating the attribute values for each employee simply takes too much time and keeps the help desk from focusing on other critical tasks. Instead, you can force users to update their profile information such as photos, mobile numbers, and addresses.

How ADSelfService Plus helps:

ADSelfService Plus allows end users to update their profile details on their own through its self-service portal. You can control which attributes the user can view and update, as well as force users to update their information when they log in to the self-service portal. ADSelfService Plus supports validation rules to ensure users enter accurate data. There's also an employee search option that allows users to search for their colleagues' information.



Use case 12

Enforcing MFA for local user accounts across domain and workgroup machines

Organizations often maintain a mix of domain-joined and workgroup Windows machines—especially in remote branches, isolated environments, or specialized setups like labs, training centers, or frontline operations. These machines are typically accessed using local user accounts, which are not managed by Active Directory and often lack consistent security controls.

This creates a major vulnerability, as local accounts are frequently overlooked in traditional MFA deployments. If an attacker gains access to a local account on any such system, it could lead to system compromise, data theft, or lateral movement across the network.

How ADSelfService Plus helps:

ADSelfService Plus addresses this gap by enabling Local User MFA, which enforces multi-factor authentication for local user accounts across:

- Domain-joined Windows machines (in addition to domain users)
- Workgroup machines (outside AD control)

Key capabilities include:

- Support for a wide range of online MFA methods like SMS, Email, Duo Security, RSA SecurID, and more.
- Policy-based MFA for interactive logins, UAC prompts, RDP sessions, and system unlocks.
- Device-based MFA to secure machines regardless of the user account.
- Built-in reports to track enrollment, activity, failures, agent deployment, and authenticator usage.
- Centralized CSV-based enrollment for all local users (admin-controlled).

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 https://www.manageengine.com/products/self-service-password.

$ Get Quote Download