

# Streamlining access and ensuring security for students and staff with ADSelfService Plus



# Cyber security in the education sector

- [Microsoft](#) says nearly 80% of enterprise malware encounters are in education

- ✓ Educational institutions hold a vast amount of sensitive data, ranging from students' personal information to financial records
- ✓ To protect sensitive data, educational institutions should implement robust security measures like enabling MFA, and enforcing strong passwords

- ✓ Students often forget their passwords and get locked out of their accounts, resulting in the help desk getting backlogged and end users being unable to complete their tasks
- ✓ By letting users reset their own passwords, admins can focus on critical tasks

- ✓ In the education sector, students, teaching staff, management staff, parents, and alumni struggle to remember passwords for multiple applications, resulting in time-consuming repetitive logins
- ✓ By implementing SSO, users can access applications with just one click, eliminating the need to enter multiple passwords



# Cyber security in the education sector



- In addition to protecting user data, educational institutions must comply with various regulations such as COPPA, FERPA, HIPAA, the GDPR, the PCI DSS, and more
- This involves educational institutions to implement a comprehensive identity security solution to protect sensitive data, streamline user access, and maintain compliance with regulations





# An all-encompassing identity security solution

- ManageEngine ADSelfService Plus is an identity security solution with MFA, SSO, and self-service password management capabilities
- ADSelfService Plus offers the following solutions
  - ✓ Self-service password management
  - ✓ Adaptive MFA
  - ✓ SSO for applications
  - ✓ Remote work enablement
  - ✓ Enterprise self-service



# How ADSelfService Plus mitigates cybersecurity risks for education institutions



# Self-Service capabilities

## Before ADSelfService Plus

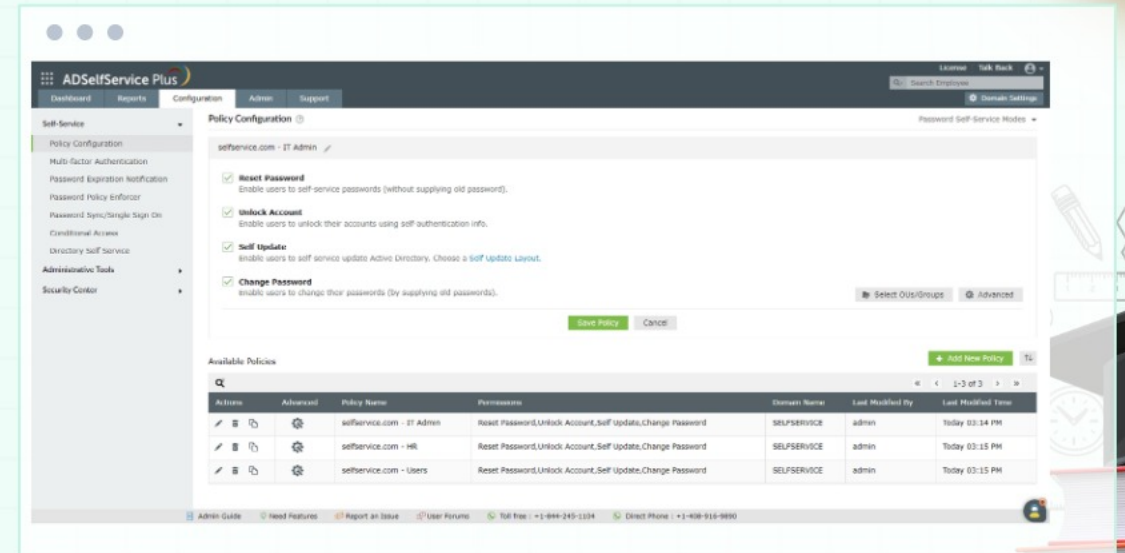
- Students and staff often forget their login passwords. They approach admins to reset passwords or unlock accounts, which can disrupt their regular workflow and lead to high volumes of password reset requests
- Users must send admins email requests about changes to their personal details or password modifications, resulting in delays or omissions in informing admins about these updates
- Furthermore, administrative staff can make mistakes when updating school records due to human error



# Self-Service capabilities

## After ADSelfService Plus

- Empower users to reset passwords, change passwords, and unlock their accounts themselves without IT assistance
- Users can view and update their personal information in the organization's records
- Admins can restrict what fields a user can self-update; they can also configure which fields a user can view





# Password Policy Enforcer

## Before ADSelfService Plus

- Students tend to set weak, easily guessable passwords, increasing unauthorized access
- The default password policy in AD may not enforce password complexity requirements, making it easier for attackers to crack passwords
- Besides that, students reuse passwords across multiple platforms, which significantly amplifies the impact of a compromised password

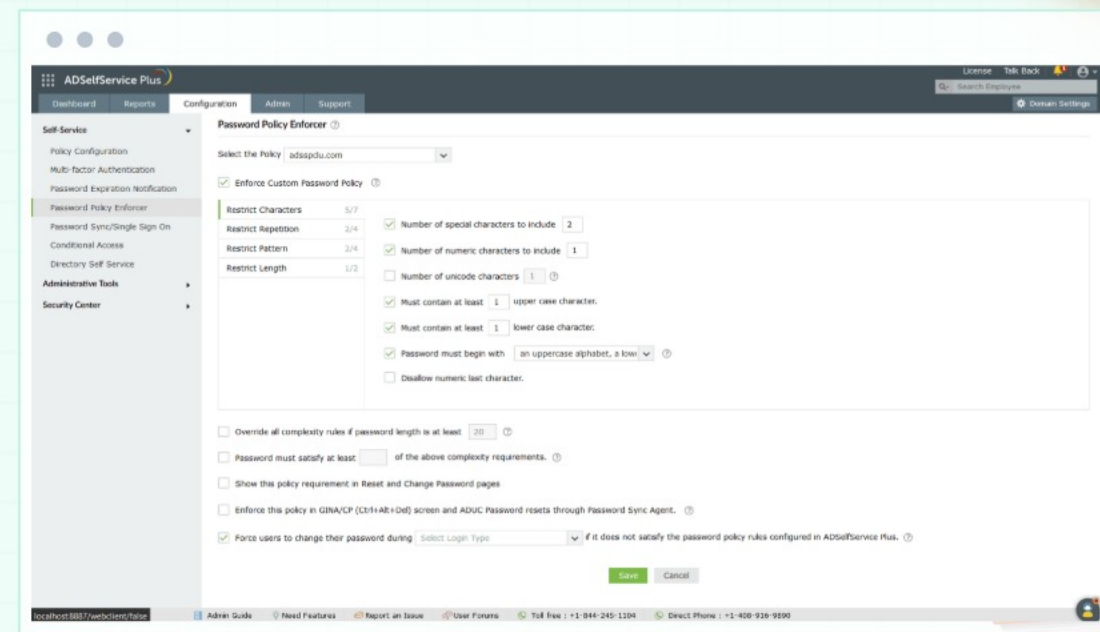




# Password Policy Enforcer

## After ADSelfService Plus

- Admins can implement fine-grained password policies for users based on their OU, group, or domain membership
- Admins can integrate with the Have I been Pwned? service, which can ban the use of passwords involved in previous hacks
- [NIST's SP 800-63B](#) password best practices can be enforced with the Password Policy Enforcer



# Password Policy Enforcer

## After ADSelfService Plus

- Policies can be used to set password controls that are not available in the native policies, like:
  - ✓ Unicode characters are mandatory
  - ✓ Restrictions on the repetition of characters in usernames and old passwords
  - ✓ Restrictions on the usage of weak passwords, dictionary words, and palindromes
  - ✓ Enforce passwords to match the regex pattern



# Multifactor authentication

## Before ADSelfService Plus

- Weak and compromised passwords can, if breached, result in exposed personal information, including birthdates, full names, addresses, and payment information. This leaves students and staff vulnerable to identity theft and financial fraud
- According to a recent [report](#), educational institutions worldwide suffer more cyberattacks than any other sector
- Furthermore, there is a misconception that MFA is too complex for K-12 students

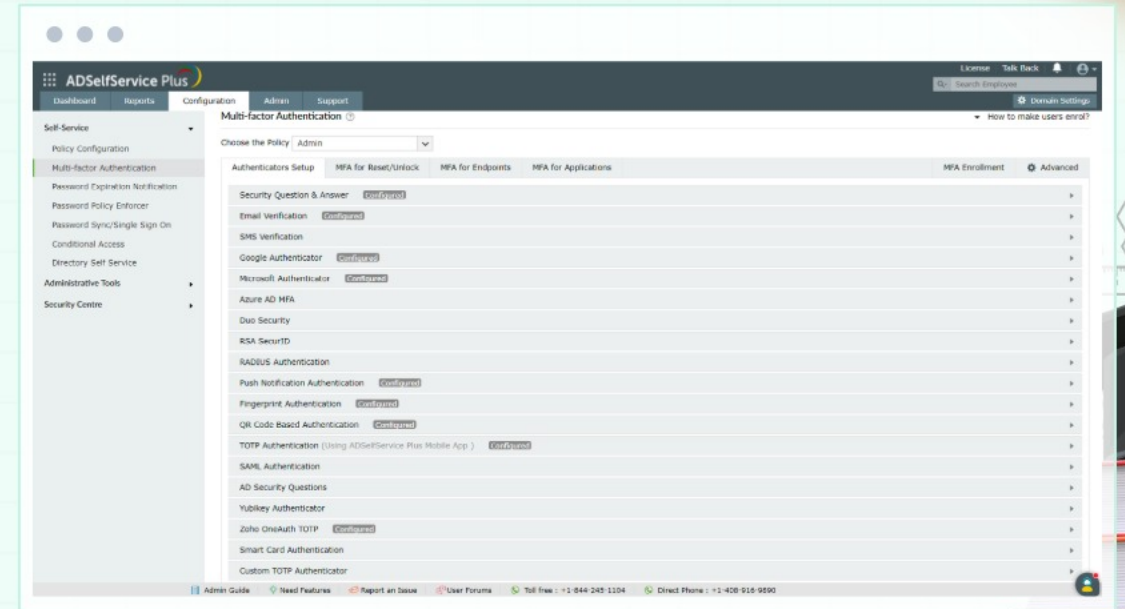




# Multifactor authentication

## After ADSelfService Plus

- Admins can customize MFA by considering each user group's capabilities and responsibilities using 20 authentication methods, including SMS verification, email verification, push notifications, DUO security, Google Authenticator, and Microsoft Authenticator
- Using MFA adheres to [NIST's SP 800-63B](#) and [CISA](#) recommendations to add an extra layer of security



# Multifactor authentication

## After ADSelfService Plus

- Admins can configure MFA for:
  - ✓ Machine logins (Windows, macOS, and Linux, and servers)
  - ✓ VPN logins
  - ✓ OWA and EAC logins
  - ✓ Application access
  - ✓ Self-service password reset and account unlock
  - ✓ Remote Desktop Protocol (RDP)
  - ✓ Windows User Account Control (UAC)



# Single sign-on

## Before ADSelfService Plus

- With the increasing number of online resources available, schools and colleges face the challenge of managing multiple login accounts for a large number of students
- All applications and learning resources have unique login instructions. Some passwords require capital letters, some mandate special characters, and others require numbers. That means it'd be hard for students to remember several usernames and passwords
- Teachers have to spend more time helping users log in to their applications, like EduBrite, Dropbox, and Tableau separately

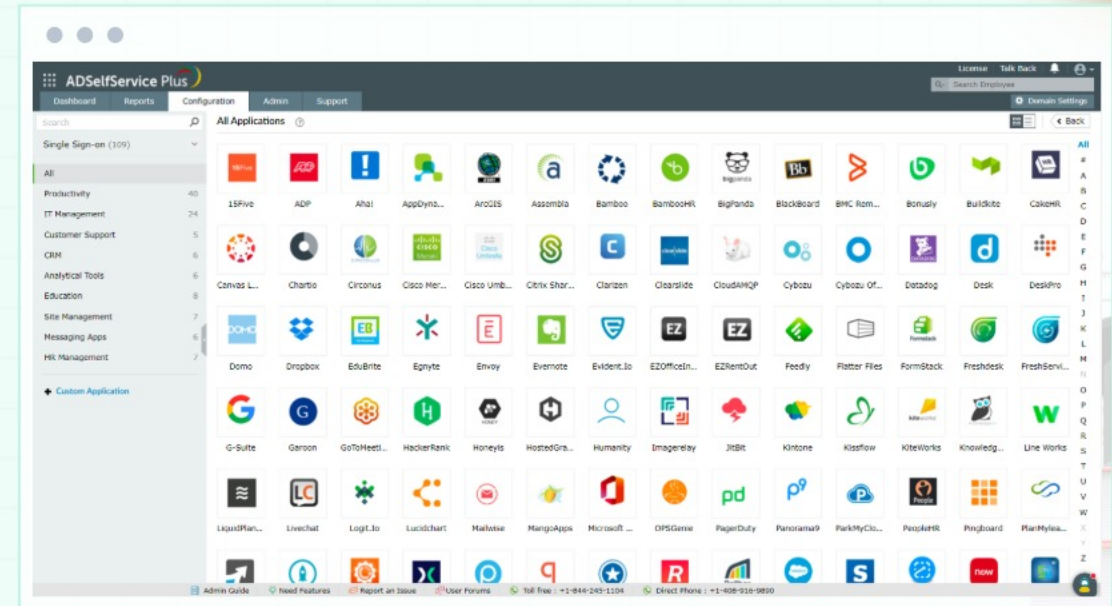




# Single sign-on

## After ADSelfService Plus

- Users can seamlessly access all cloud applications with just one set of credentials
- Our comprehensive SSO solution supports:
  - ✓ SAML-enabled applications like Google Workspace, Microsoft 365, and Salesforce
  - ✓ OAuth- and OIDC-enabled applications
  - ✓ Custom applications



# Single sign-on

## After ADSelfService Plus

- Users can log in to an application or service using SSO in two ways:
  - ✓ Identity provider (IdP) initiated SSO (ADSelfService Plus)
  - ✓ Service provider (SP) initiated SSO (cloud application or service)
  - ✓ Bookmark functionality for seamless access to applications that do not support standard SSO protocols like SAML, OAuth, or OIDC.



# Password expiration notification

## Before ADSelfService Plus

- Faculty and students are often unaware of when their passwords will expire, leading to sudden account lockouts and restricted access to essential resources, which disrupts academic activities
- If passwords are not periodically changed, educational institutions may be unaware of compromised accounts, exposing sensitive information and resources
- Consequently, other critical issues like resolving network issues and system outages get delayed due to an increase in help desk requests from users facing unexpected account lockouts

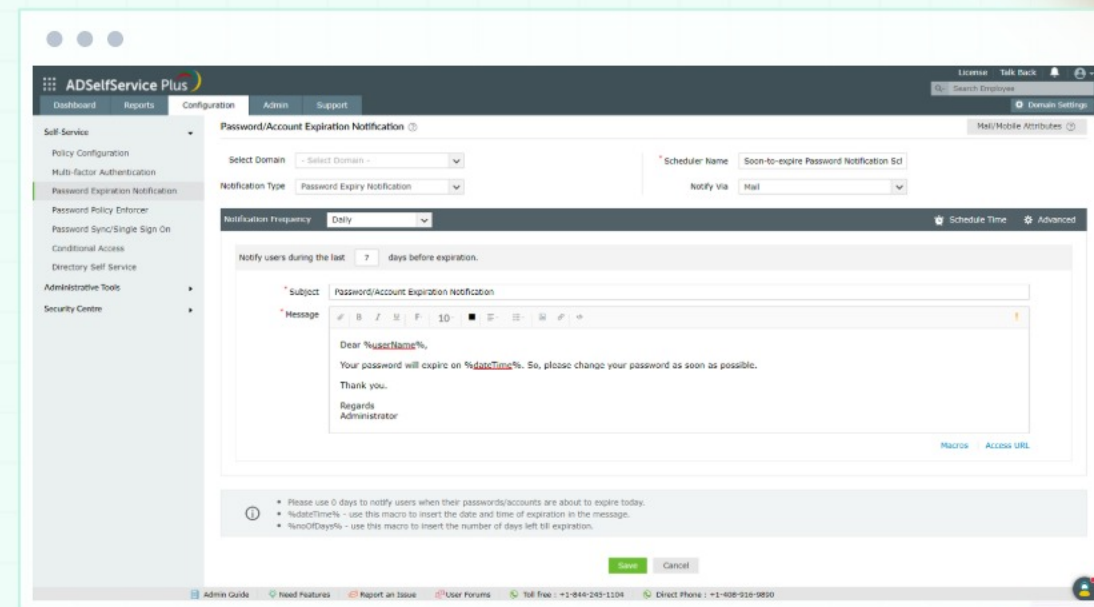




# Password expiration notification

## After ADSelfService Plus

- Notifications can be set to notify users about soon-to-expire passwords and accounts via SMS, email, or push notifications
- Admins can set the notification frequency and customize notification content with images and instructions
- In addition, admins can create a schedule to automatically reset expired passwords and unlock locked-out accounts



The screenshot displays the 'Password/Account Expiration Notification' configuration page in the ADSelfService Plus web interface. The left sidebar shows a navigation menu with options like Self-Service, Policy Configuration, Multi-factor Authentication, Password Expiration Notification (which is currently selected), Password Policy Enforcer, Password Sync/Single Sign On, Conditional Access, Directory Self Service, Administrative Tools, and Security Centre. The main configuration area includes fields for 'Select Domain' (set to 'Select Domain'), 'Scheduler Name' (set to 'Soon-to-expire Password Notification Sd'), and 'Notification Type' (set to 'Password Expiry Notification'). The 'Notify Via' dropdown is set to 'Mail'. The 'Notification Frequency' is set to 'Only'. Below these, there is a section for 'Notify users during the last 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 instructions for using macros like %dateTime% and %userName%. The interface also includes a 'Schedule Time' button, an 'Advanced' link, and a footer with 'Admin Guide', 'Need Features', 'Report an Issue', 'User Forums', and contact information.

# Update cached credentials

## Before ADSelfService Plus

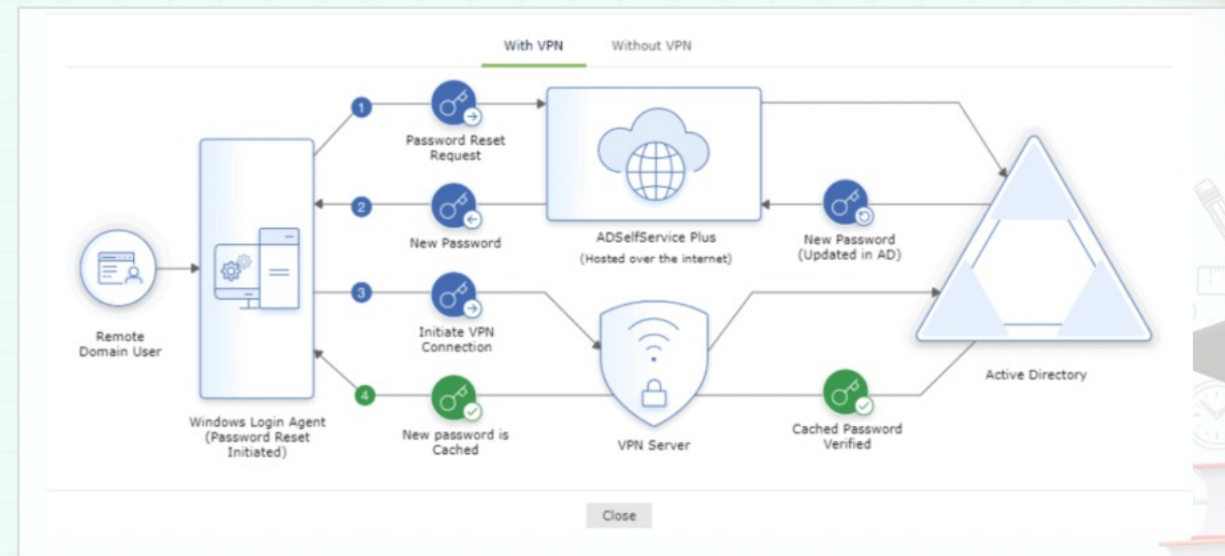
- When a user changes their password, the cached credentials on their device may not update automatically if the network connection is unstable. This can result in login failures or account lockouts when accessing resources with outdated credentials
- Additionally, forgotten passwords or expired credentials often cause account lockouts, requiring assistance from the IT help desk
- The frequent need to reenter credentials can disrupt the workflow of students and faculty, consuming valuable time



# Update cached credentials through VPN

## After ADSelfService Plus

- Users can reset their domain passwords by installing the GINA/CP client, which places the Reset Password/Account Unlock link
- With the logon agent, users can automatically update their credentials by connecting to AD through a VPN client
- This way, users can access their accounts seamlessly without interruptions or login failures

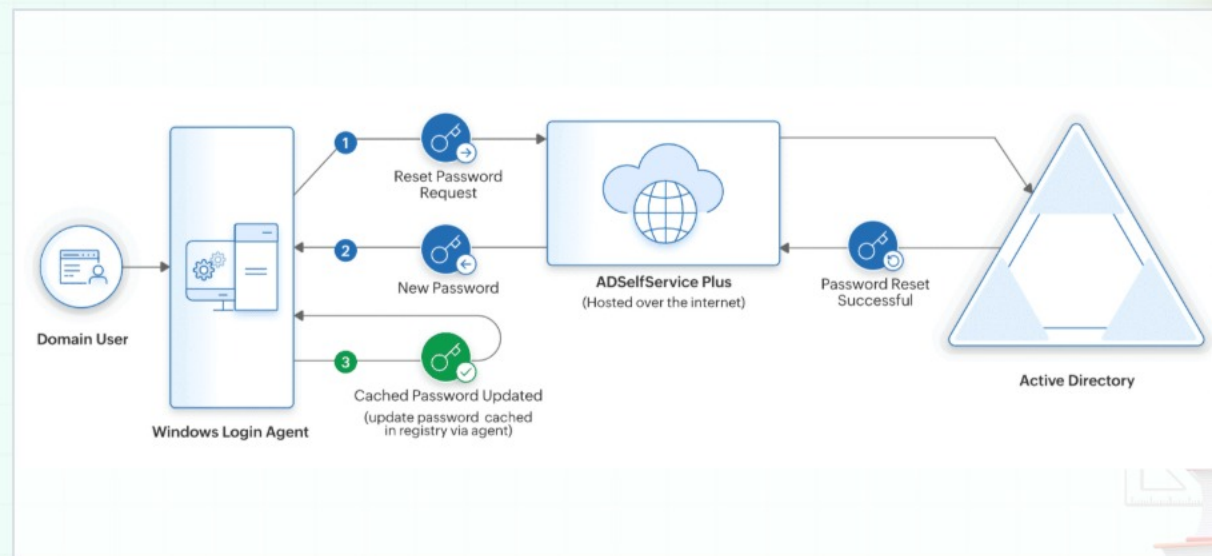




# Update cached credentials without VPN

## After ADSelfService Plus

- Users' identities are verified through MFA before the reset request is sent to ADSelfService Plus, which updates the new password in Active Directory.
- Once updated in AD, the new password is automatically synced with the local cache on users' machines.
- This ensures users can log in without facing credential mismatches or login issues.



# Conclusion

- Schools, colleges, and universities are a significant target for malicious cyber activity
- The standards for the educational sector are constantly changing, and hackers and malicious insiders may find new ways to compromise and steal data from these organizations
- Using ADSelfService Plus, educational institutions can strengthen insider threat protection, secure users' data, and comply with regulations



# Thank you

