ManageEngine
ADSelfService Plus

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

ManageEngine
ADSelfService Plus

SelfService capabilities

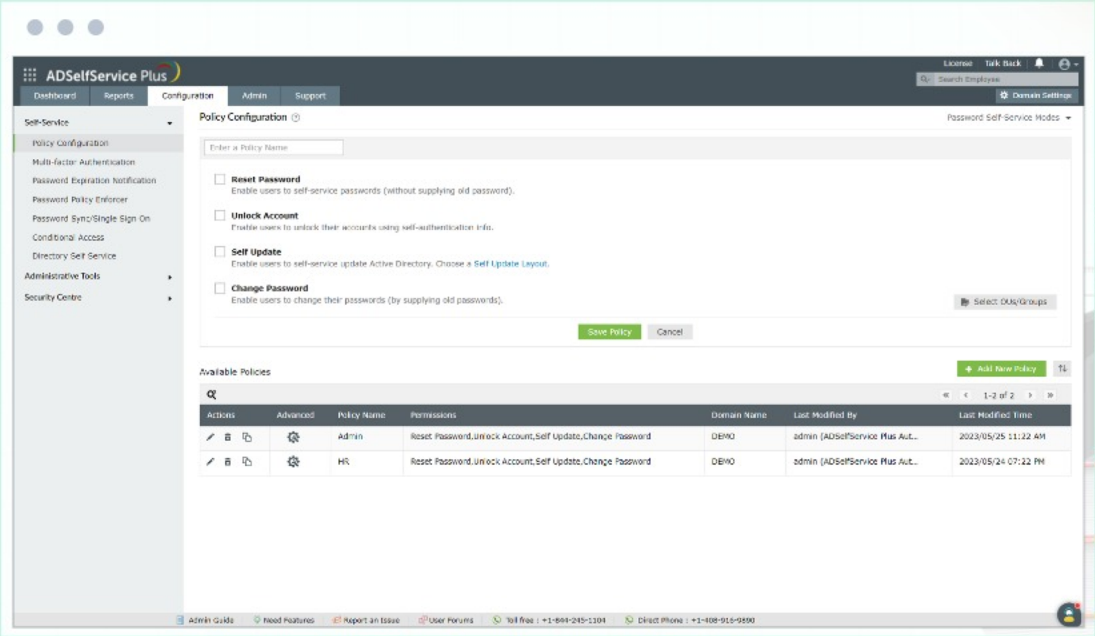
Before ADSelfService Plus

- 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

SelfService 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



Policy Configuration

Enter a Policy Name

□ **Reset Password**
Enable users to self-service passwords (without supplying old password).

□ **Unlock Account**
Enable users to unlock their accounts using self-authentication info.

□ **Self Update**
Enable users to self-service update Active Directory. Choose a Self Update Layout.

□ **Change Password**
Enable users to change their passwords (by supplying old passwords).

Available Policies

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
		Admin	Reset Password,Unlock Account,Self Update,Change Password	DEMO	admin (ADSelfService Plus Aut...	2023/05/25 11:22 AM
		HR	Reset Password,Unlock Account,Self Update,Change Password	DEMO	admin (ADSelfService Plus Aut...	2023/05/24 07:22 PM

Toll free : +1-844-245-1104 Direct Phone : +1-408-916-9890

ManageEngine
ADSelfService Plus

Password Policy Enforcer

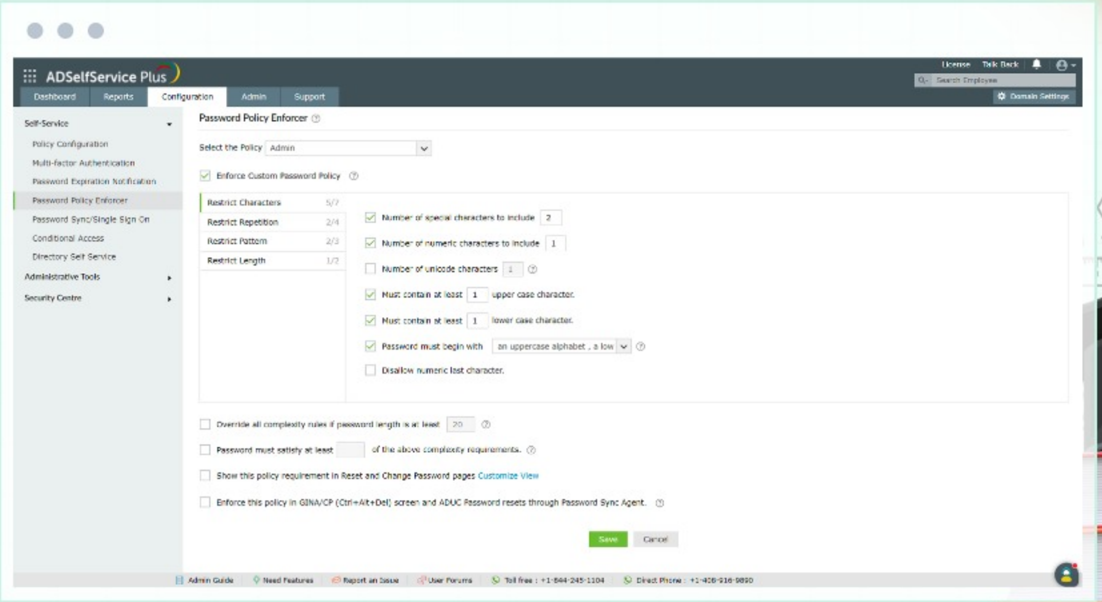
Before ADSelfService Plus

- 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

Select the Policy: Admin

☑ Enforce Custom Password Policy

Restrict Characters	5/7
Restrict Repetition	2/4
Restrict Pattern	2/3
Restrict Length	1/2

☑ Number of special characters to include 2

☑ Number of numeric characters to include 1

□ Number of unicode characters 1

☑ Must contain at least 1 upper case character.

☑ Must contain at least 1 lower case character.

☑ Password must begin with an uppercase alphabet , a low

□ Disallow numeric 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.

Toll free : +1-844-245-1104 | Direct Phone : +1-408-916-9890

ManageEngine
ADSelfService Plus

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

Multifactor authentication

Before ADSelfService Plus

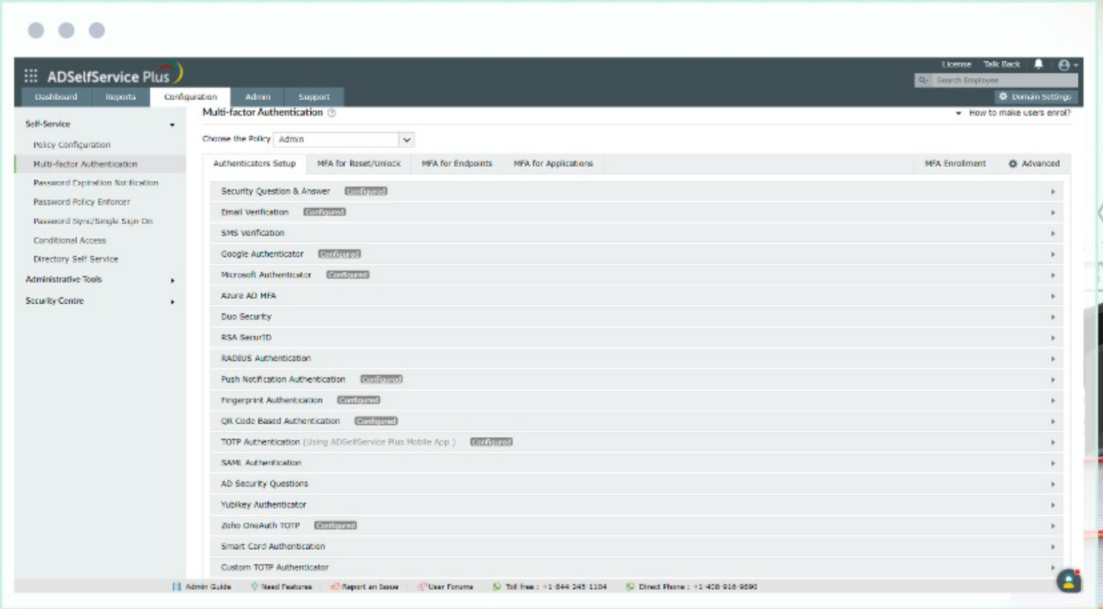
- Weak and compromised passwords can, if breached, result in exposed personal information, including birthdates, full names, addresses, and payment information. This leaves students and staff vulnerable to identity theft and financial fraud
- According to a recent report, educational institutions worldwide 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 19 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



Multi-factor Authentication

Choose the Policy: Admin

Security Question & Answer Configured
Email Verification Configured
SMS Verification
Google Authenticator Configured
Microsoft Authenticator Configured
Azure AD MFA
Duo Security
RSA SecurID
RADIUS Authentication
Push Notification Authentication Configured
Fingerprint Authentication Configured
QR Code Based Authentication Configured
TOTP Authentication (Using ADSelfService Plus Mobile App) Configured
SAML Authentication
AD Security Questions
Yubikey Authenticator
Zoho OneAuth TOTP Configured
Smart Card Authentication
Custom TOTP Authenticator

Toll free : +1 844 245 1104 Direct Phone : +1 408 916 9890

ManageEngine
ADSelfService Plus

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

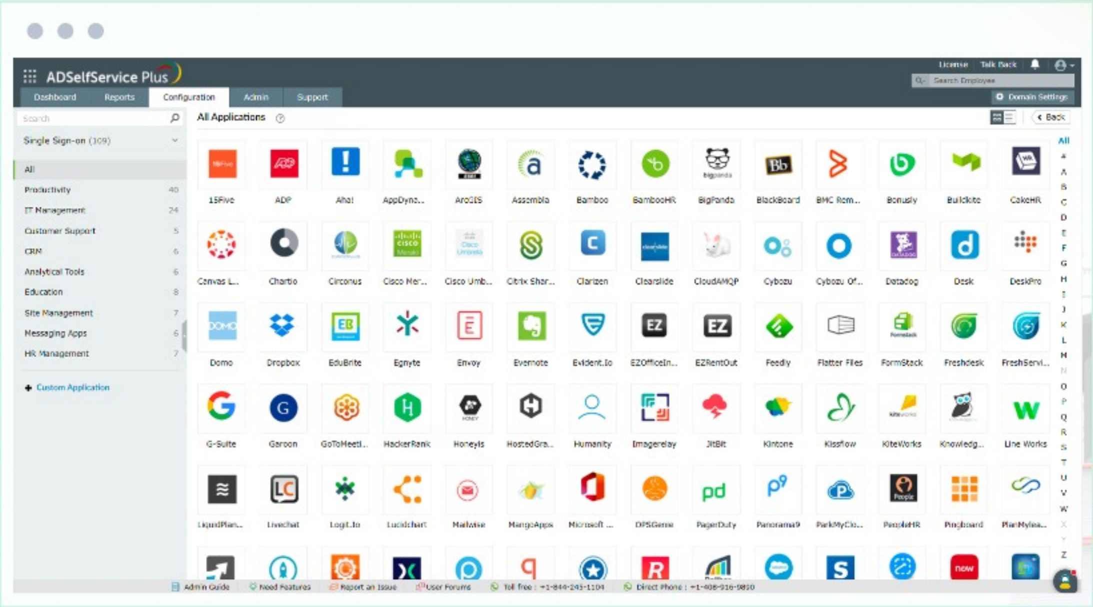
Before ADSelfService Plus

- 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 seamless 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



ManageEngine
ADSelfService Plus

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)

Password expiration notification

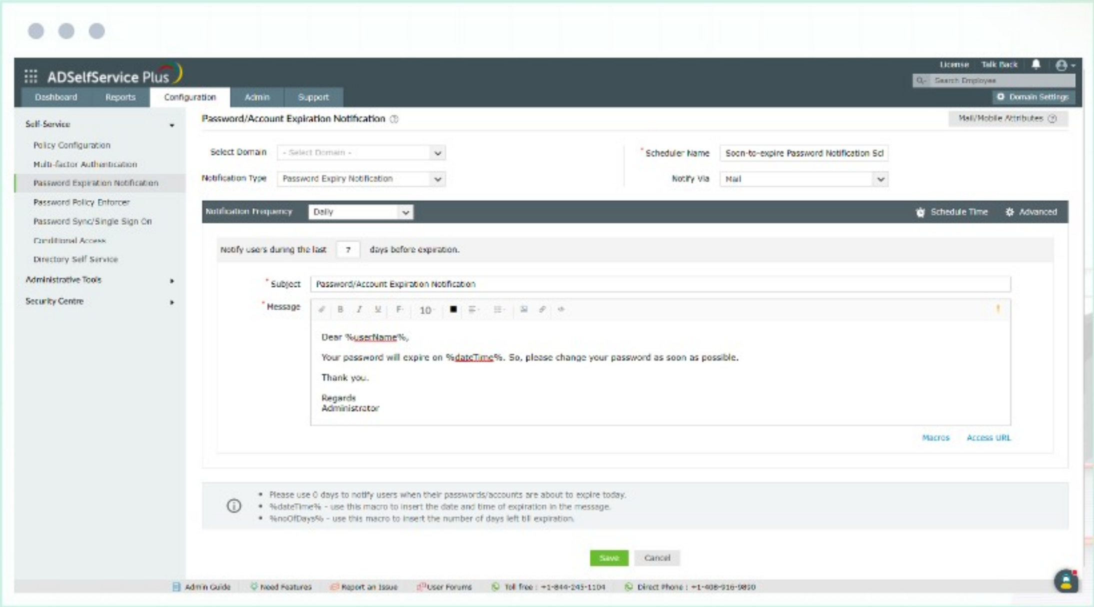
Before ADSelfService Plus

- 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



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.

Toll free : +1-844-245-1104 | Direct Phone : +1-408-916-9850

ManageEngine
ADSelfService Plus

Updated cached credentials over VPN

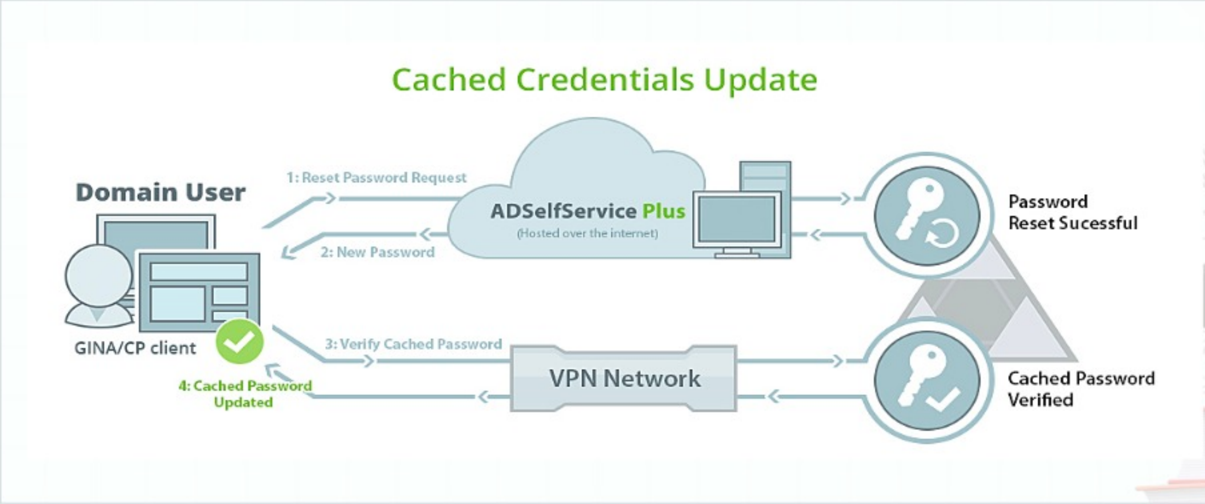
Before ADSelfService Plus

- 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

Updated cached credentials over 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


Cached Credentials Update
Domain User
GINA/CP client
1: Reset Password Request
2: New Password
ADSelfService Plus
(Hosted over the internet)
Password Reset Sucessful
3: Verify Cached Password
4: Cached Password Updated
VPN Network
Cached Password Verified

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

ManageEngine
ADSelfService Plus

Thank you