ManageEngine
ADSelfService Plus

Enhancing cyber hygiene in healthcare

Protecting identities with ADSelfService Plus

Cyber security in the healthcare sector

- Between 2009 and 2022, there were 5,150 healthcare data breaches reported to HHS' Office for Civil Rights

- Healthcare organizations store a vast amount of sensitive data—including patient information, hospital records, insurance details, biomedical research findings, and medical test results—which attracts cybercriminals who profit by stealing it and selling it on the dark web
- Security measures like MFA and strong passwords will help healthcare organizations protect sensitive data

- When patients forget their passwords, their accounts get locked out, resulting in a backlog on the help desk and users unable to complete their tasks
- By enabling users to reset their own passwords, users can regain access to their accounts promptly, allowing admins to focus on system-critical tasks

Cyber security in the healthcare sector

- Doctors, clinical staff, IT staff, researchers, and patients struggle to remember passwords for multiple applications, resulting in repetitive time-consuming logins
- By implementing SSO, users can access applications with just one click, eliminating the need to enter multiple passwords

- Additionally, healthcare organizations must comply with various regulations, including HIPAA, HITECH, GDPR, and PCI DSS
- In order to protect sensitive data, streamline user access, and maintain regulatory compliance, healthcare organizations implement comprehensive identity security solutions

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 healthcare organizations

Self-service capabilities

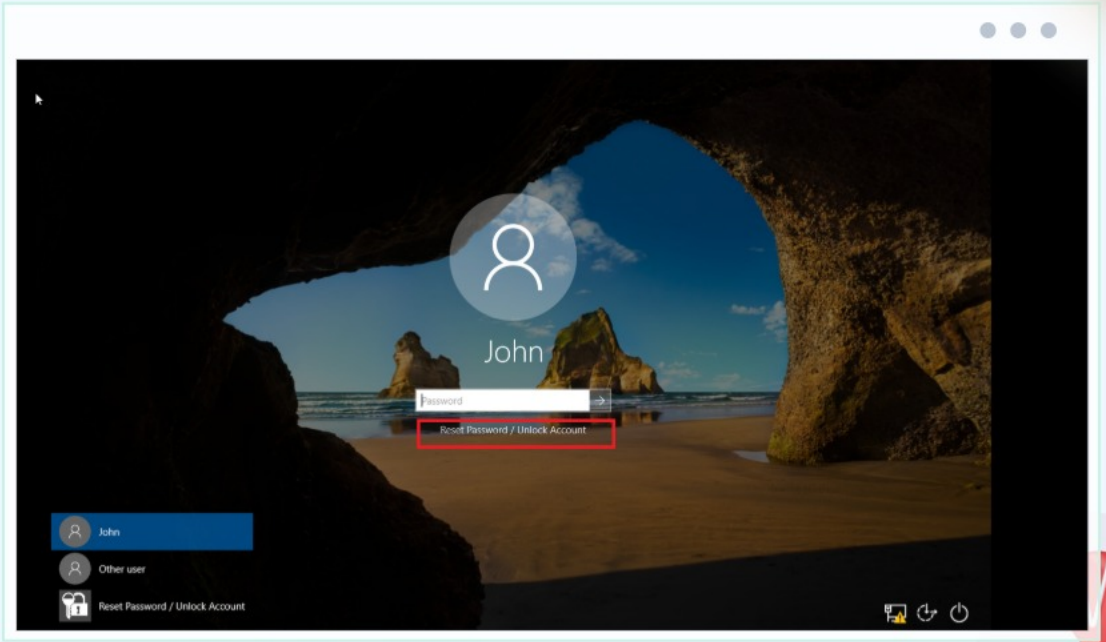
Before ADSelfService Plus

- When patients and healthcare professionals send emails for password resets and account changes, admins forget to resolve the tickets or take longer to respond
- Gartner analysts say 40% of help desk calls are related to password resets. Due to this, critical tasks—such as providing network infrastructure, maintaining servers, or deploying software—are delayed
- When hospital staff and IT admins create and update user records, they can encounter delays or make errors, which leads to longer patient wait times, unsatisfied staff, and low productivity

Self-service capabilities

After ADSelfService Plus

- Users can reset their passwords, change passwords, unlock their accounts, and self-update personal information—all without help from the IT team
- By clicking the Reset Password/Account Unlock option in the GINA/CP client, users can reset their passwords and unlock their accounts themselves
- Admins can restrict what fields users can self-update, and also what fields they can view



Password policy enforcer

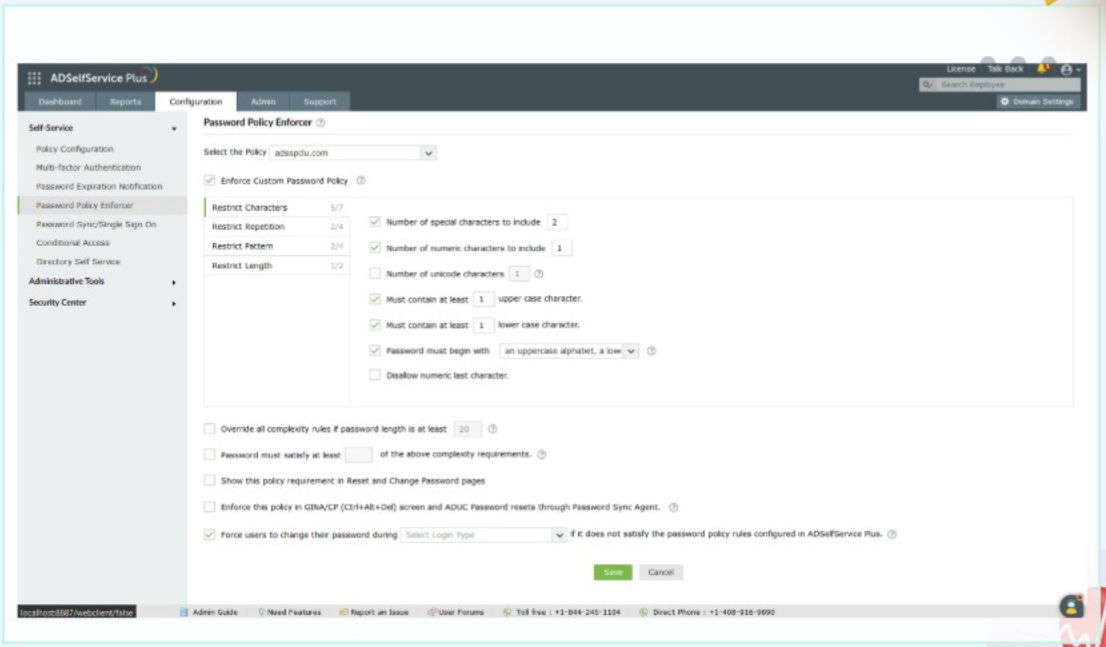
Before ADSelfService Plus

- While creating passwords, clinical staff and patients often choose easy-to-type passwords that include simple patterns, hospital names, or common dictionary words
- Moreover, the default password policy in AD may not support password complexity requirements like unicode characters. Attackers can exploit this weakness by targeting passwords, making them easier to crack

Password policy enforcer

After ADSelfService Plus

- By implementing fine-grained password policies, admins can protect users based on their membership in an OU, group, or domain
- It is possible to set password controls not available in native policies, including:
  - Mandatory use of Unicode characters
  - Restrictions against character repetition in usernames and reusing old passwords
  - Limitations on weak passwords, dictionary words, and palindromes
  - Enforce passwords to match the regex pattern



Password policy enforcer

After ADSelfService Plus

- By integrating with the "Have I been Pwned?" service, users are prevented from using passwords involved in previous hacking incidents
- Moreover, the password policy enforcer aligns with the password best practices outlined in NIST SP 800-63B

Multi-factor authentication

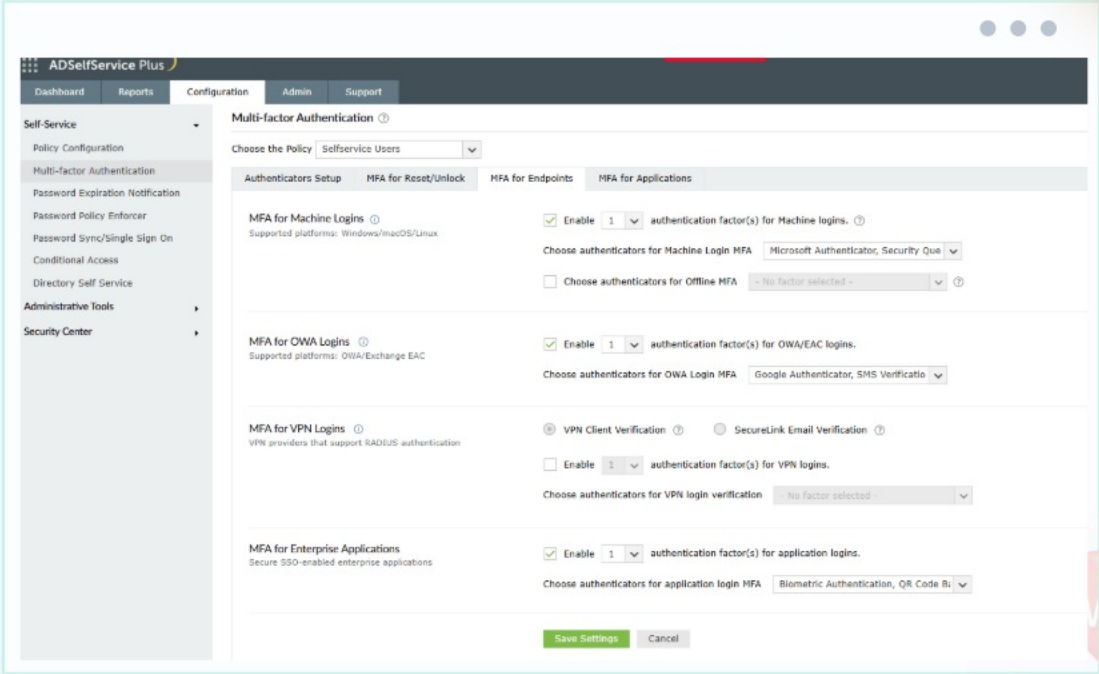
Before ADSelfService Plus

- Shared devices in healthcare settings, like those found in emergency rooms and laboratories, create additional security vulnerabilities, especially when password sharing is involved
- This behavior allows a malicious employee to exploit shared passwords, potentially gaining unauthorized access to sensitive information
- Moreover, if there is limited network access, traditional authentication methods that rely on internet connectivity may result in delayed verification

Multi-factor authentication

After ADSelfService Plus

- Enables customized MFA by considering each user group's capabilities and responsibilities using 20 authentication methods
- Also, offline MFA is supported for Windows, macOS,RDP, and UAC logons
- Adding MFA complies with NIST's SP 800-63B and CISA's recommendations to add an extra layer of security



Multi-factor authentication

After ADSelfService Plus

- Admins can configure MFA for:
  - Machine logins (Windows, macOS, Linux, 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

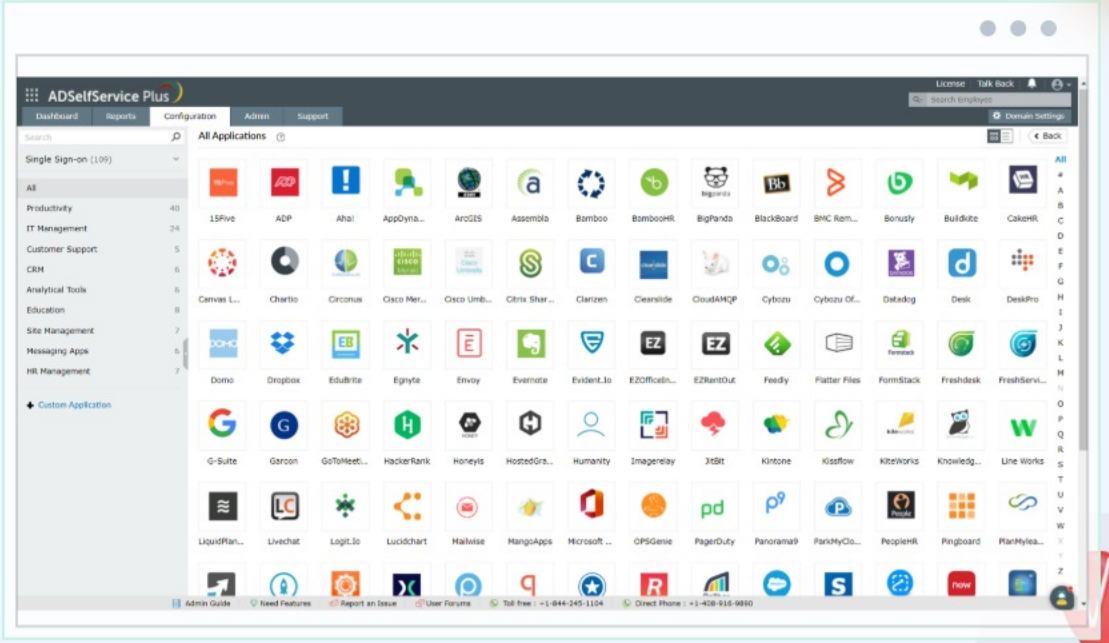
Before ADSelfService Plus

- Healthcare companies require employees and patients to use long and complicated passwords, and they need to remember multiple passwords
- Staff members use multiple applications such as EHR systems, patient management software, and others across various devices
- However, repetitive logins and complex passwords reduce productivity and consume valuable time

Single sign-on

After ADSelfService Plus

- Users can 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

- SSO allows users to log in using two methods:
  - 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.

Conditional access policy

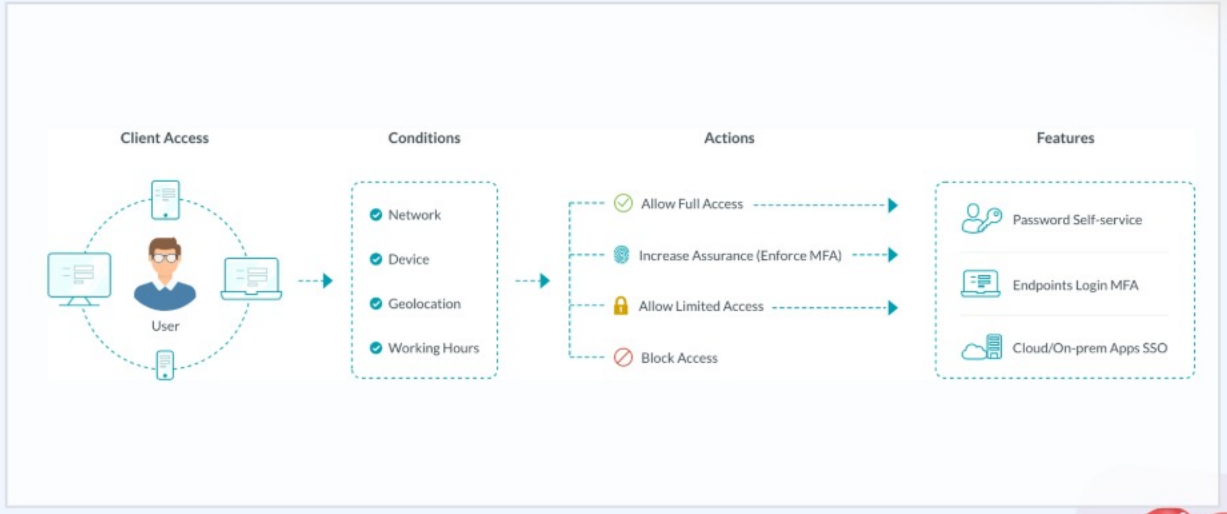
Before ADSelfService Plus

- Physicians accessing the hospital's electronic medical records system via personal smartphones outside the premises face an increased risk of device hacking when connected to public networks
- These networks lack security measures, leaving them vulnerable to hackers. Personal smartphones may also lack hospital-owned security, risking sensitive patient information exposure

Conditional access policy

After ADSelfService Plus

- Enabling conditional access automatically assigns access policies to determine whether to enable MFA based on users' parameters such as IP address, device, time of access, and geolocation
- This allows admins to effectively manage access by granting complete access, limited access, or denying access to resources
- Based on the risk level, users are prompted to provide additional authentication factors. This enhances security by protecting endpoints against unauthorized access attempts



Conclusion

- The healthcare sector faces challenges in managing identities due to its ongoing digital transformation and expansive attack surface
- Prioritizing cyber hygiene has become crucial as healthcare organizations are lucrative targets for cybercriminals seeking financial gains
- With ADSelfService Plus, healthcare organizations can enhance their cybersecurity posture and mitigate identity management risks

Contact us

Contact Number

+1-408-916-9890

Support Email

support@adselfserviceplus.com

Live chat

For instant responses.

Visit our website

www.adselfserviceplus.com/

DOWNLOAD NOW