ManageEngine
ADSelfService Plus

Enhancing your

security posture with ADSelfService Plus' MFA

1

What is multi-factor authentication?

- Multi-factor authentication (MFA) is the process of using multiple factors of authentication to verify a user's identity before giving them access to a particular resource
- Along with entering a password, users are "asked to enter a code sent to their email, answer a secret question, or scan a fingerprint"
- It plays an integral role in identity and access management, helping organizations get closer to creating a Zero Trust security framework
- It strengthens account security and prevents fraudulent account access by providing more protection than single-factor authentication

2

Why is MFA essential?

- Cybercrime costs are predicted to rise **15%** per year for the next five years, reaching **$10.5 trillion** in 2025
- In today's digital age, passwords are not enough to protect sensitive information from cyberthreats
- MFA blocks **99.9%** of modern automated cyberattacks

Cost savings for organizations

- According to IBM's Cost of a Data Breach Report 2022, the average total cost of a data breach is **$4.35 million**
- Implementing MFA can provide significant cost savings for organizations by decreasing the risk of data breaches and cyberattacks

Comply with IT regulations and avoid penalties

- Regulations such as HIPAA, the PCI DSS, the GDPR, and more prioritize the protection of sensitive data
- Implementing a stronger security posture will reduce the risk of data breaches and subsequent compliance fines. E.g., HIPAA's penalties for violations range from $100 to $50,000 per violation, going up to $1.5 million annually

Save money on insurance premiums

- In the next 5-10 years, cyber insurance will grow from $12 billion in premiums today to $60 billion, according to the chief executive of Lloyd's
- Many insurance agencies require organizations to have MFA to qualify for cyber insurance coverage
- Some insurance companies offer discounts to organizations that implement MFA

3

How does MFA work?

MFA requires users to provide multiple authentication factors other than usernames and passwords

The knowledge factor

- Information that only the authorized user knows
- Passwords, PINs, passphrases, security questions, etc.

The possession factor

- Authentication is performed with something the user possesses
- Smartphones, physical tokens, smart cards, etc.

The inheritance factor

- Verifying identities with the help of inherited characteristics and biometrics
- Fingerprint scans, facial scans, voice recognition, and retinal scans

3. How does MFA work?

- A user signs on with their username and password
- The system prompts the user to provide a second method of identification
- After authentication, the user gains access to the requested resource

4

What is ADSelfService Plus?

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

It ensures seamless access to enterprise resources and establishes a Zero Trust environment

5

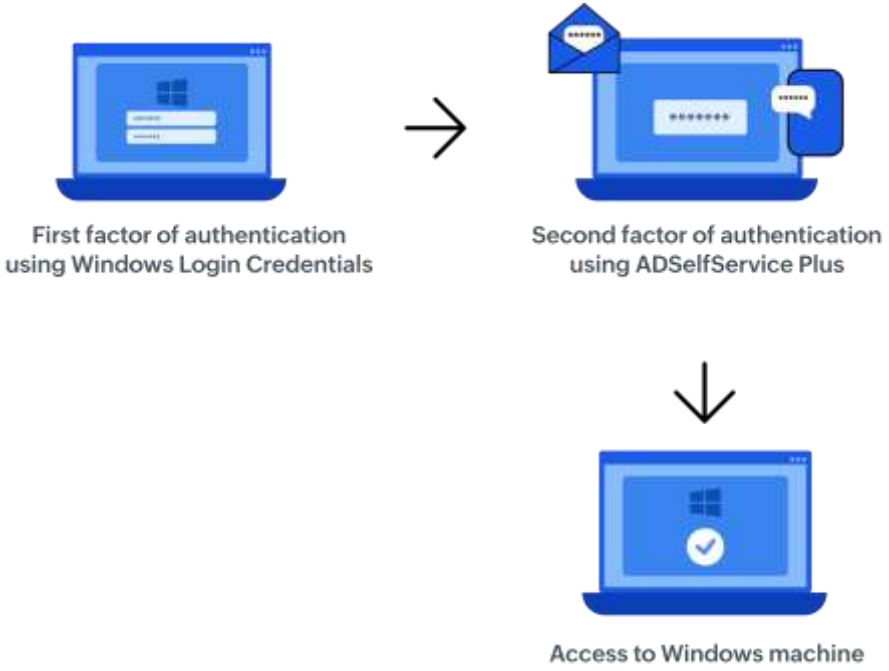
Secure your organization with ADSelfService Plus' MFA

ADSelfService Plus supports MFA for the following:

- Domain users logging in to machines (Windows, macOS, Linux, servers)
- Local user and admin accounts login (workgroup and domain-joined Windows machines)
- VPN logins (RADIUS- or IIS-based network endpoints)
- OWA and Exchange admin center (EAC) logins
- Application access (SAML-, OIDC-, and OAuth-enabled applications)
- Self-service password reset and account unlock
- Remote Desktop Protocol (RDP)
- Windows User Account Control (UAC)

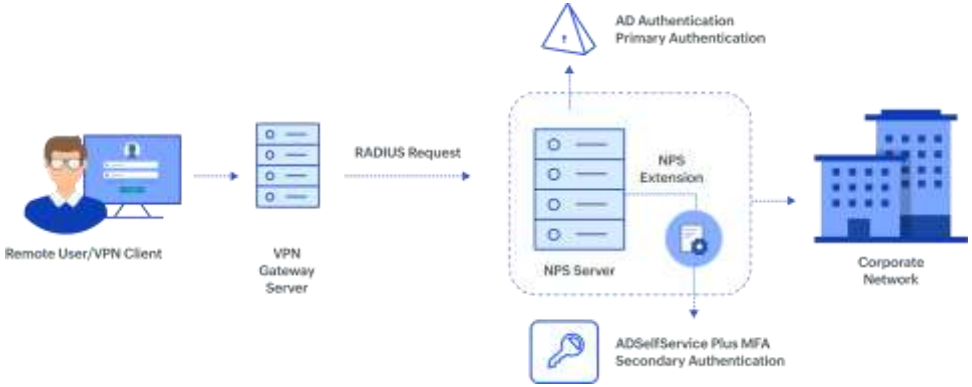
Machine logins

- With ADSelfService Plus' endpoint MFA feature, users can authenticate their identities to access Windows, macOS, and Linux machines
- The first factor is the user's domain credentials, while the second factor varies from biometrics to smart cards



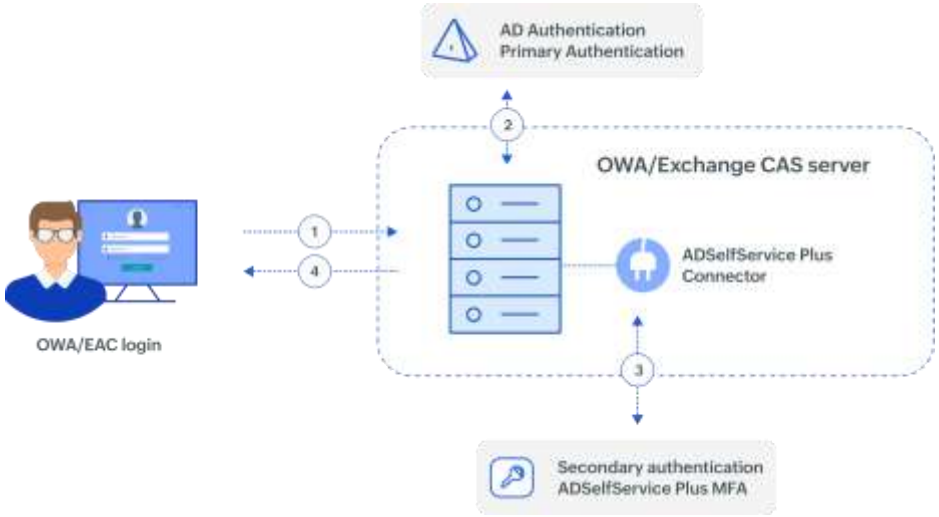
Local user MFA

- Enable MFA for local user accounts on both domain-joined and workgroup Windows machines, even without internet connectivity.
- Supports both policy-based (user-specific) and device-based MFA configurations.



VPN logins

- By using ADSelfService Plus' adaptive MFA, users can secure VPN connections to the organization's networks.
- Admins can secure all RADIUS-based VPN providers, including Fortinet, Cisco AnyConnect, Windows, Juniper Networks, Palo Alto Networks, and SonicWall Global VPN Client.
- MFA Modes for VPN Authentication:
  - VPN Client Verification: MFA prompts appear directly in the VPN client.
  - SecureLink Email Verification: Enables MFA via all ADSelfService Plus authenticators, with users authenticating via an email verification link.
- This prevents unauthorized VPN access using exposed credentials.



OWA logins

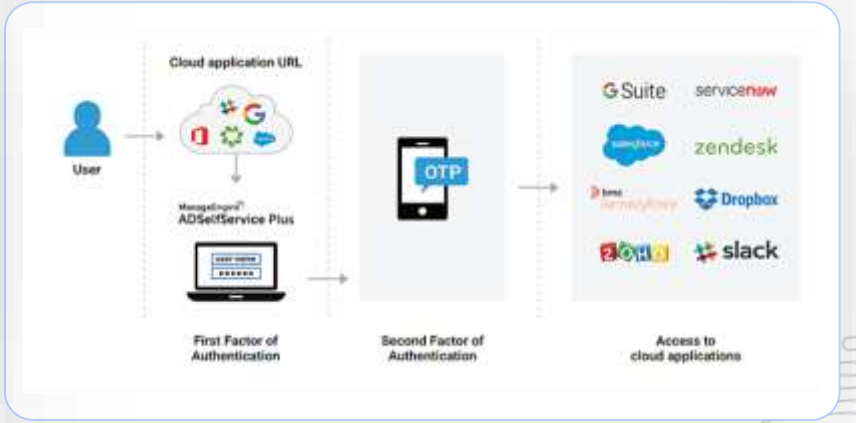
- On the Exchange server, the ADSelfService Plus OWA Connector needs to be installed
- ADSelfService Plus uses the Connector to enable MFA during OWA and EAC authentication

Enterprise applications

- With ADSelfService Plus, users can add MFA for ADSelfService Plus, and SSO- enabled applications logins like Salesforce, Microsoft 365, Slack, and Dropbox
- IdP-initiated SSO requires the user to log into the ADSelfService Plus portal first, whereas a SP-initiated SSO accesses the cloud application first, then the ADSelfService Plus login page
- ADSelfService Plus prompts for an additional authentication factor. After successful authentication, users can access cloud applications

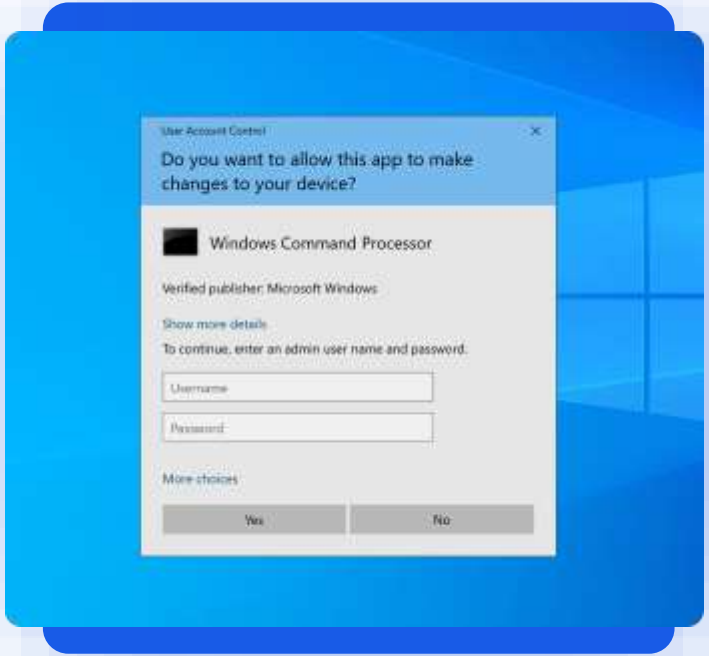
During IdP-initiated logins

During SP-initiated logins



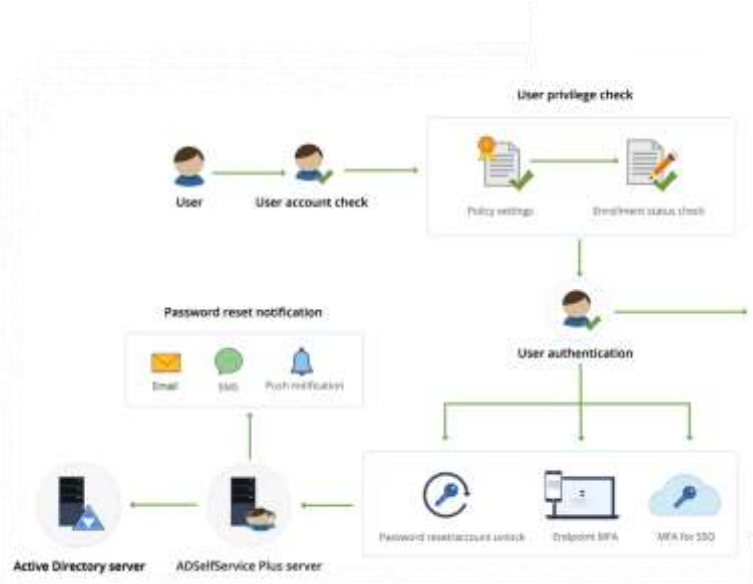
Windows UAC

Compatible with Windows 7+ and Windows Server 2008+



Self-service password reset and account unlock

- Users can reset their passwords and unlock their accounts via self-service only after they prove their identities



6

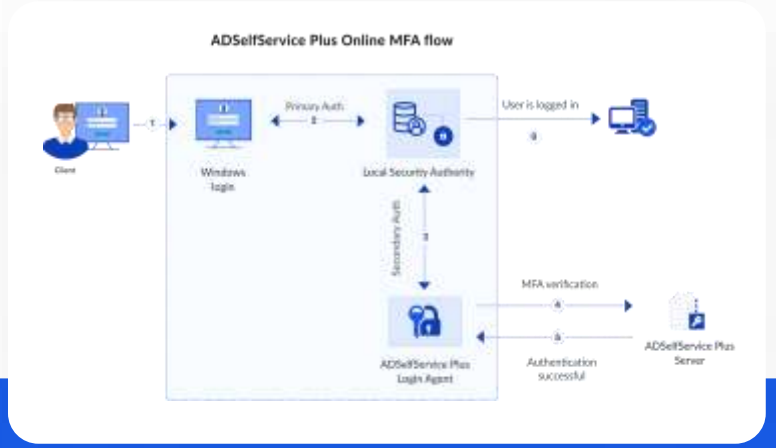
Authenticators supported by ADSelfService Plus

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

7

How does ADSelfService Plus' online MFA work?

Note: ADSelfService Plus supports online MFA for machine logins, VPN logins, OWA logins, UAC, cloud applications, and Microsoft 365



- A user logs in to their machine with their credentials as the primary authentication method
- The initial credentials are verified by the local security authority
- Once the initial credentials have been verified, ADSelfService Plus prompts the user for an additional authentication factor
- ADSelfService Plus sends the relevant MFA factor request to the user's registered device, then the user authenticates themself by providing that factor
- ADSelfService Plus validates the provided MFA factor against the user's registered information
- If the factor is successfully validated, access is granted

8

How does ADSelfService Plus' offline MFA work?

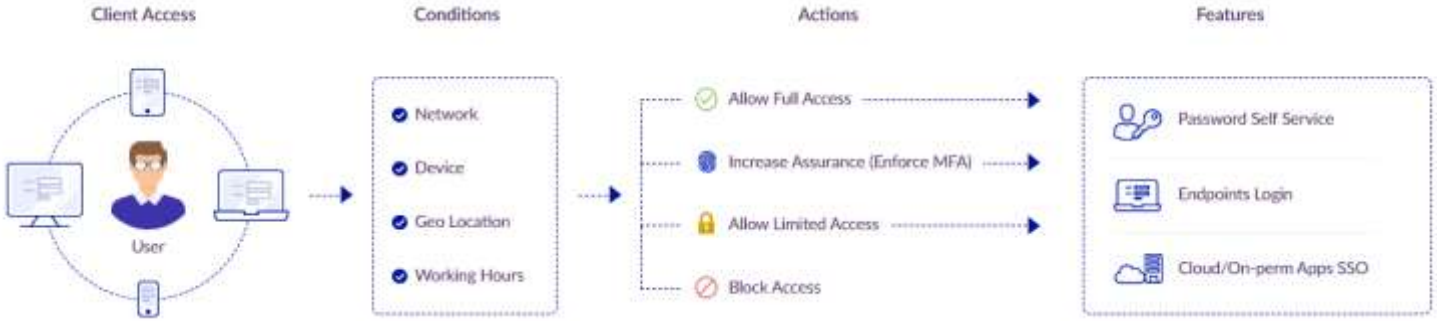
Note: ADSelfService Plus supports offline MFA for Windows, macOS, RDP, and UAC logons.

- A user logs in to their machine with their credentials as the primary authentication method
- Their credentials are verified by the local security authority
- ADSelfService Plus attempts to prompt the user for an additional authentication factor, but fails due to connection issues
- The login agent prompts the user for offline MFA, which supports Google Authenticator, Microsoft Authenticator, custom TOTP authenticators, and Zoho OneAuth TOTPs
- Upon successful validation, access is granted

9

Enforce access control decisions

- With ADSelfService Plus, admins can control which users can access workstations, applications, and various features (such as password changes and directory self-updates) based on factors like their IP address, time of access, device, and location
- After analyzing these risk factors, ADSelfService Plus provides users with complete, unrestricted access; limited access; or no access to the resources
- Admins can set specific rules for specific domains, OUs, and groups



MFA use cases

Fortify endpoint access

- Using Endpoint MFA, users prove their identity during machine logins, VPN logins, OWA logins, UAC, cloud applications, Microsoft 365
- When passwords are compromised due to inadequate password hygiene, Endpoint MFA mitigates the risk of exposing sensitive data

Defend against credential-based attacks

- MFA defends against credential-based cyberattacks, such as brute-force attacks, password spray attacks, and dictionary attacks
- Credential theft and compromise are reduced by requiring users to authenticate using multiple factors, such as a password, biometric scan, or smart card

Risk-based authentication

- Remote users are often more vulnerable to cyberattacks because they access corporate resources through public networks
- With ADSelfService Plus, admins can set access policies based on the user's device type, time of access, IP address, or geolocation to keep IT resources secure
- ADSelfService Plus prompts the user for MFA accordingly, enforcing additional measures for high-risk attempts and streamlining access for low-risk attempts

10

MFA use cases

MFA when not connected to the internet

- When employees travel frequently or work remotely without the internet, they can authenticate using MFA even if they aren't connected to the authentication server

Protect business data while complying with regulations

- Comply with industry regulations that recommend or mandate MFA, such as HIPAA, the PCI DSS, and the GDPR
- E.g., the PCI DSS 8.3 requires MFA whenever a third party or portable computer accesses the network remotely

MFA insurance mandates

- Marsh's Global Insurance Market Index reports that cyber insurance premiums rose 79% in 2022
- Admin access and privileged accounts are required to implement MFA
- Many insurance companies now require MFA before they can provide a quote for coverage

11

Conclusion

- As organizations digitize, cybersecurity becomes increasingly important
- MFA is the #1 way to prevent cybersecurity incidents
- With ADSelfService Plus' MFA, protect your data against unauthorized access

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