

ManageEngine

# ManageEngine ADSelfService Plus

An identity security solution with adaptive MFA, single sign-on, and password management capabilities.



# Outline



**Critical identity security challenges**



**Overview of ADSelfService Plus**



**Solutions offered by ADSelfService Plus**



**Adaptive MFA**



**Single sign-on**



**Self-service password management and security**



**Remote work enablement**



**Workforce self-service**



**Benefits of ADSelfService Plus**



**Our customers**



**Case study**



**Licensing, pricing and feature support**



**Add-ons**



**Contact us**

# Critical identity security challenges in enterprises



## Password reset tickets

Forgotten passwords and account lockouts remain the major source of help desk tickets.

A password reset ticket could take approximately 20 minutes and \$30 to solve. This drastically affects employee productivity; even more so if you have a remote workforce. expiration



## Upholding user productivity using MFA

Credentials remain the top cause of all data breaches. While MFA is a well-known approach today, organizations struggle to implement an effective MFA strategy that fortifies local and remote access security while simultaneously upholding user productivity



## Influx of passwords

As organizations adopt cloud applications in droves, users have to enter more passwords throughout the day just to access these applications and complete their work.



## An all-encompassing identity security solution

**ManageEngine ADSelfService Plus is an identity security solution with multi-factor authentication, single sign-on, and self-service password management capabilities**

# Solutions offered by ADSelfService Plus



## Adaptive MFA

Secure local and remote access to endpoints and applications



## SSO for applications

Establish secure, one-click access to all enterprise applications



## Self-service password management and security

Enable self-service password management and fortify passwords



## Remote work enablement

Streamline and secure remote access to enterprise resources



## Workforce self-service

Provide a self-service portal for group management and AD attributes update

## Adaptive MFA

**Implement adaptive MFA and evade credential misuse—the main culprit for data breaches**



# Why is generic MFA not enough?

IT compliance laws now mandate or recommend the use of context-based MFA

Regulations like NIST mandate additional rules on privileged account protection

With multiple endpoints to protect, using different solutions for different endpoints becomes tiring

Connection to the MFA server can sometimes be severed, taking the user offline. In such cases, bypassing MFA or blocking access are both unwise options

Enabling MFA using the native options in applications and systems can create friction, since different systems support different ways and modes of authentication.

# Adaptive MFA



## Endpoint MFA

Secure access to the enterprise network with advanced MFA for access to machines (Windows, Linux, macOS); VPN and other network endpoints using RADIUS; and OWA and other IIS web applications



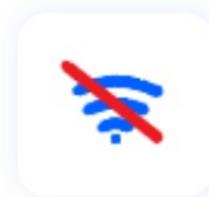
## Conditional access

Automate access control decisions for the enterprise network and its resources based on risk factors like IP address, business hours, device used, and geolocation



## Passwordless MFA for applications

Allow access to enterprise applications via SSO solely using advanced authentication methods such as biometrics, YubiKey, Google Authenticator, and more

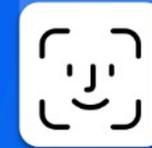


## Offline MFA

Protect user identities and machines by implementing MFA for Windows machines even when there is no internet connectivity or the ADSelfService Plus server is unreachable.

# Supported Authenticators for MFA

- YubiKey Authenticator
- FIDO2 Passkeys
- Microsoft Authenticator
- RADIUS Authentication
- Azure AD MFA
- Google Authenticator
- Zoho OneAuth TOTP
- Duo Security
- AD Security Questions
- Biometric Authentication
- Push Notification Authentication
- RSA SecureID
- Email Verification
- QR Code-based Authentication
- Security Question & Answer
- Smart Card Authentication
- Customer TOTP Authentication



# Endpoint security via MFA

The MFA feature helps secure the following endpoints into the enterprise network.



## Logins into the machine

This feature works in two ways:

### User-based MFA:

Here MFA is applied during logins into any configured machine by a specific user

### Machine-based MFA:

Here MFA is enforced for all logins into a specific machine, irrespective of user



## Microsoft RDP logins

Both RDP client authentication and RDP server authentication is secured by MFA



## Windows machine unlock

MFA will be applied when the user unlocks their Windows machine



## Windows User Account Control (UAC) prompts

MFA will be required for authentication during all elevated UAC prompts or Run As Administrator prompts

# How does MFA work?

## Step 1

The user enters their domain credentials as the first level of authentication into an endpoint or an enterprise application



## Step 2

The user completes further authentication using any of the supported methods such as biometrics, time-based verification codes, or through a third-party authenticator like YubiKey Authenticator



## Step 3

After successful authentication, the user is allowed access



# Endpoint MFA configuration

The screenshot shows the ADSelfService Plus configuration interface. The top navigation bar includes 'Dashboard', 'Reports', 'Configuration', 'Admin', and 'Support'. The 'Configuration' tab is active. On the left, a sidebar menu lists 'Self-Service' (with sub-items like Policy Configuration, Multi-factor Authentication, Password Expiration Notification, Password Policy Enforcer, Password Sync/Single Sign On, Conditional Access, Directory Self Service), 'Administrative Tools', and 'Security Center'. The main content area is titled 'Multi-factor Authentication' and shows a policy selection dropdown set to 'zoho.local'. Below this are three tabs: 'Authenticators Setup', 'MFA for Reset/Unlock', and 'MFA for Endpoints'. The 'MFA for Endpoints' tab is selected, showing three sections: 'MFA for Machine Login' (enabled, 1 factor, Security Questions), 'MFA for OWA Login' (disabled, 1 factor, No factor selected), and 'MFA for VPN Login' (disabled, 1 factor, No factor selected). At the bottom are 'Save Settings' and 'Cancel' buttons.

ADSelfService Plus

License | Talk Back | Search Employee | Domain Settings

Dashboard | Reports | Configuration | Admin | Support

Self-Service

- Policy Configuration
- Multi-factor Authentication
- Password Expiration Notification
- Password Policy Enforcer
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

### Multi-factor Authentication

Choose the Policy: zoho.local

Authenticators Setup | MFA for Reset/Unlock | MFA for Endpoints | MFA for Applications | MFA Enrollment | Advanced

**MFA for Machine Login**  
Supported : Windows/macOS/Linux

Enable 1 factor authentication for Machine login.

Choose authenticators for Machine Login MFA: Security Questions

Choose authenticators for Offline MFA: Google Authenticator, Microsoft Auth

**MFA for OWA Login**  
Supported : OWA/ECP of Exchange Server

Enable 1 factor authentication for OWA Login.

Choose authenticators for OWA Login MFA: - No factor selected -

**MFA for VPN Login**  
VPN providers that support RADIUS authentication

Enable 1 factor authentication for VPN login.

Choose authenticators for VPN login: - No factor selected -

Save Settings | Cancel

# How do conditional access policies work?



A user attempts to log into their machine or access any other integrated application

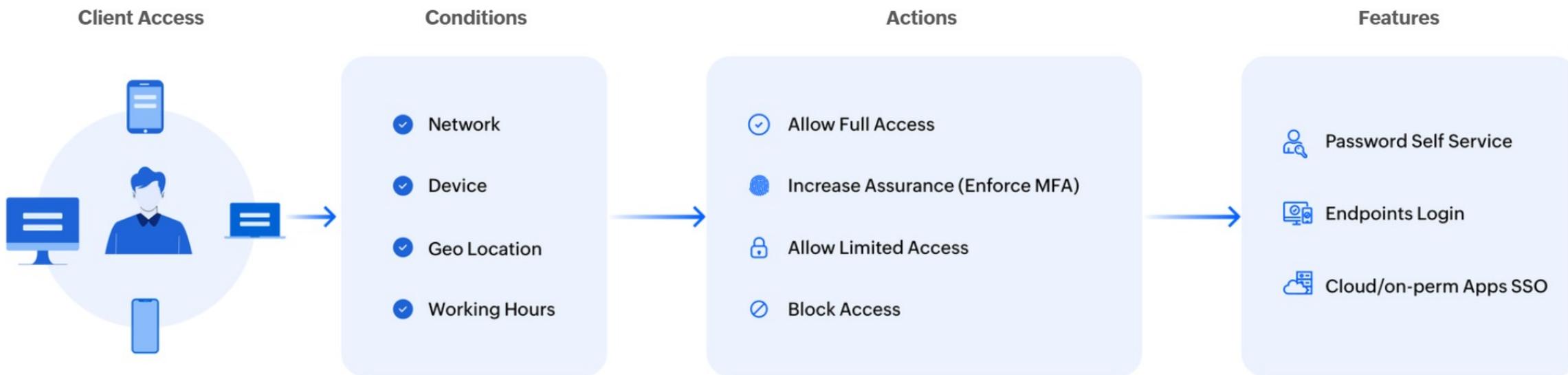


Risk factors such as the user's IP address, time of access, and geolocation are analyzed



Based on pre-configured conditions and the risk factor data, the solution enables one of the following:

- Complete access to the machine or application
- Secure access to the machine or application using MFA
- Limited access to certain ADSelfService Plus features
- Restricted access to ADSelfService Plus features





## Single sign-on

**End login fatigue and simplify application onboarding with SSO**

# Single sign-on



## SSO for established cloud applications

Secure and streamline application access by allowing users to authenticate once and access any of the supported applications without requiring further authentication



## ..... as well as custom enterprise applications

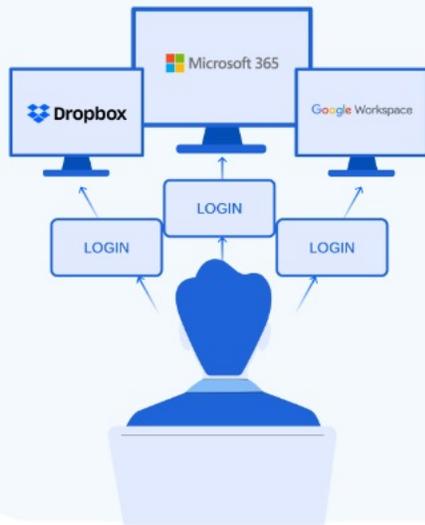
Enable SSO for custom on-premises and cloud applications via SAML, OAuth, and OpenID Connect protocols



# How SSO streamlines access to enterprise applications for users

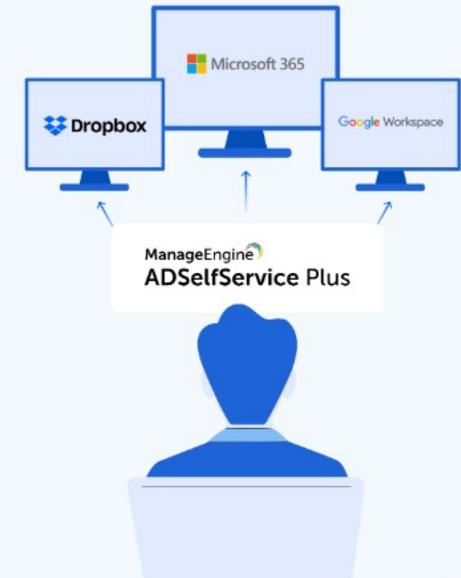
## Before implementing SSO

The user opens and logs in to each enterprise application individually with a separate set of credentials

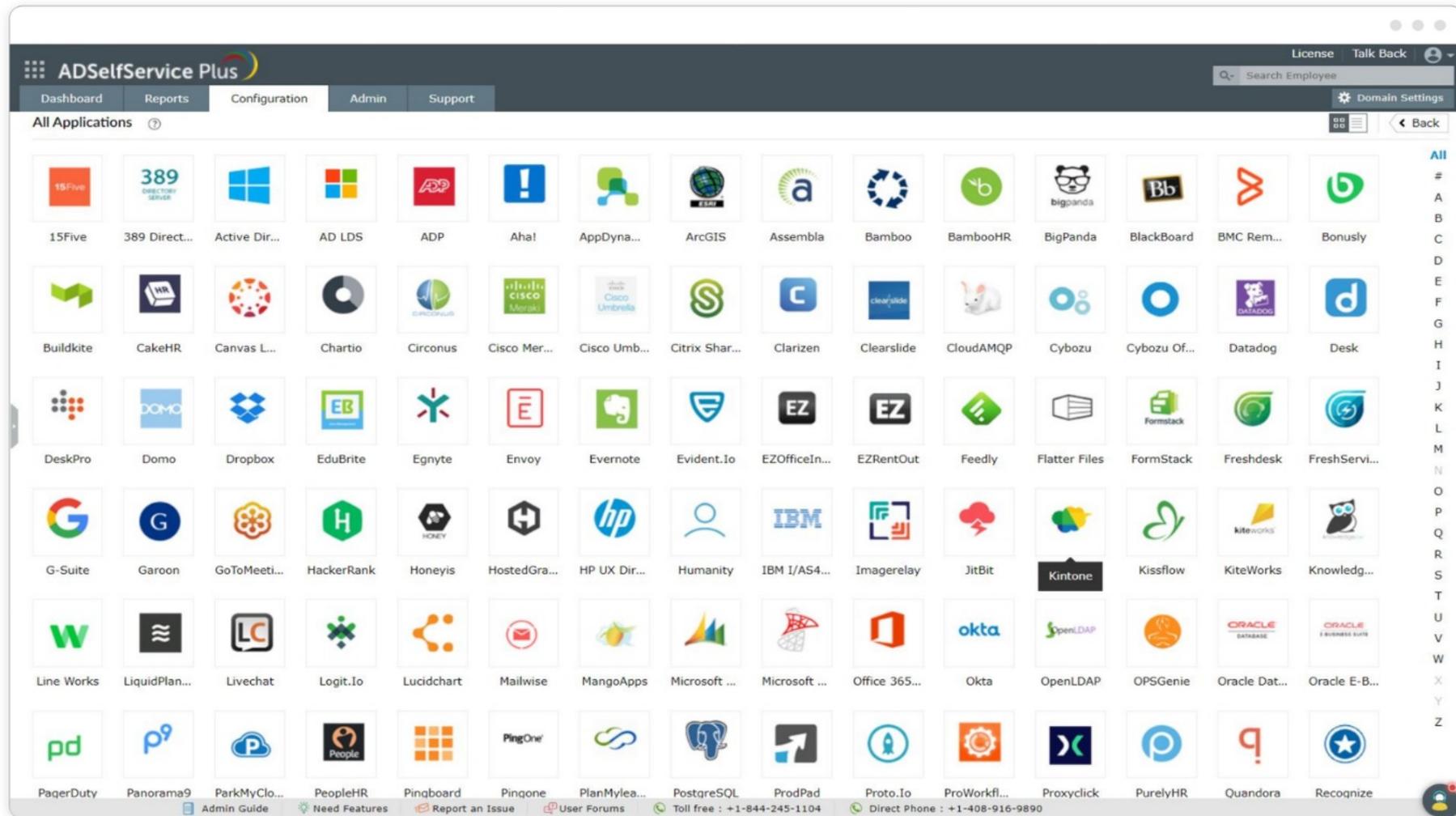


## After implementing SSO

- The user opens the ADSelfService Plus portal (for IdP-initiated SSO) or the enterprise application (for SP-initiated SSO)
- The user completes authentication using ADSelfService Plus (in case of SP-initiated SSO, users will be redirected to the ADSelfService Plus portal)
- The user obtains access to multiple applications



# Applications supported out-of-the-box for SSO





## Self-service password management and security

**Eliminate password reset tickets and uphold password security**

# Self-service password management and security



## Self-service password reset and account unlock

Enable users to reset passwords and unlock accounts in office, at home, or on the move, all without help desk aid



## Password synchronization

Sync AD password resets and changes with the connected enterprise applications, in real time



## Password and account expiration alerts

Automate password and account expiration reminders to users via email, push, and SMS alerts



## Password policy enforcer

Mandate creation of complex passwords by implementing advanced password requirements during password changes and resets

# How admins free themselves from redundant password reset tickets

## Before ADSelfService Plus

- A user who has forgotten their AD domain password, contacts the IT help desk.
- The IT help-desk verifies their identity and resets their password.
- User authenticates using MFA and resets their password

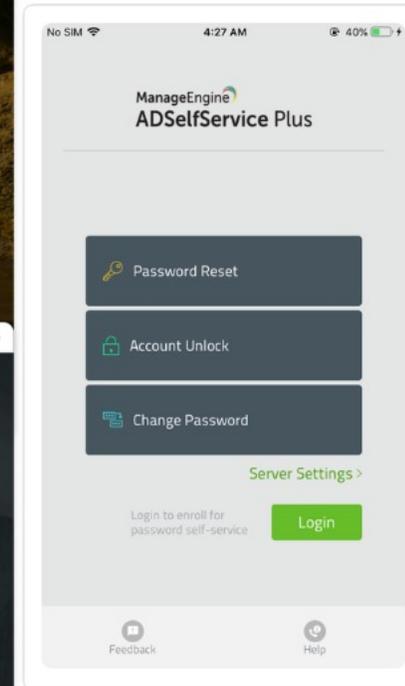
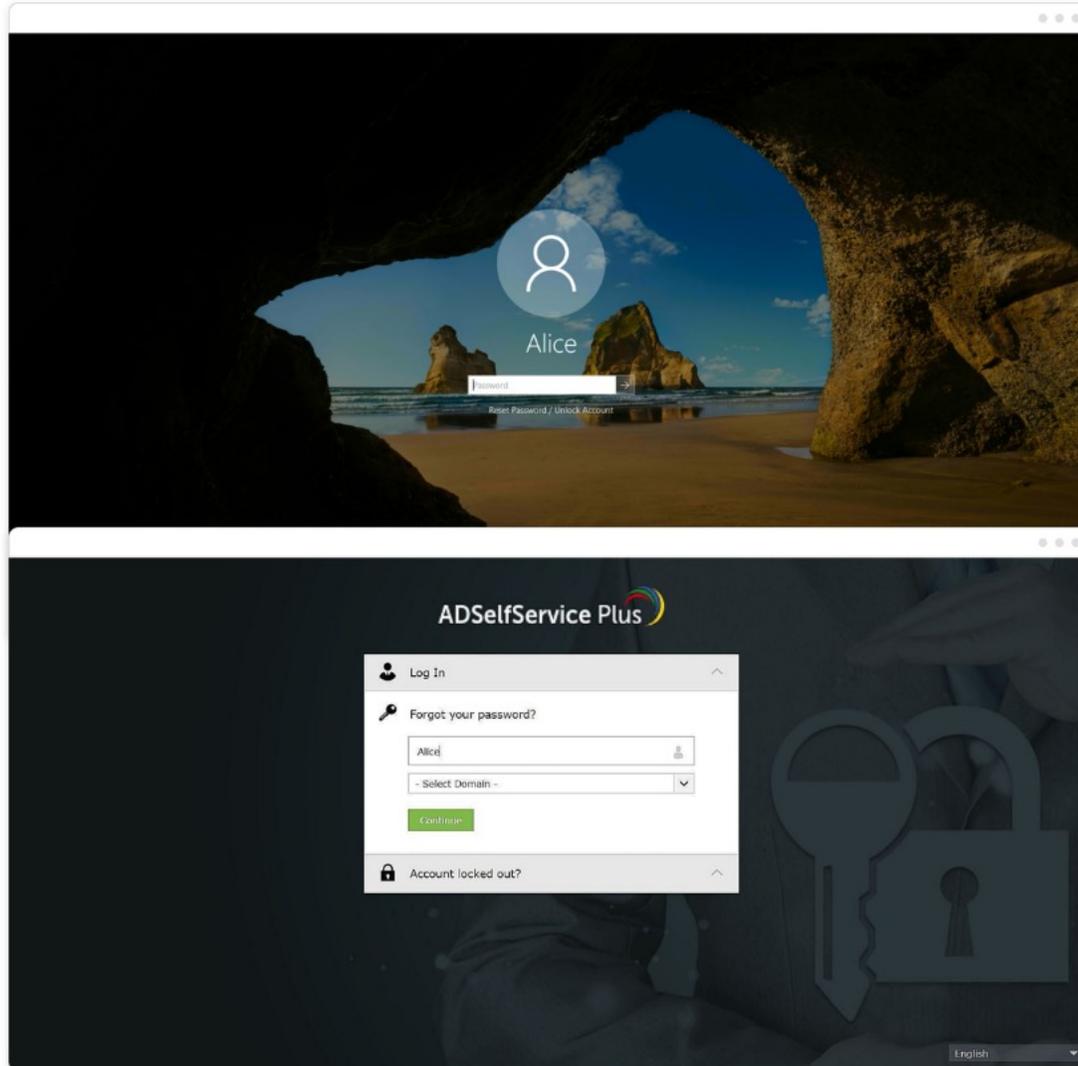


## After ADSelfService Plus

- A user who has forgotten their AD domain password opens the ADSelfService Plus password reset portal via a web-browser, their login screen, or mobile device
- User authenticates using MFA and resets their password



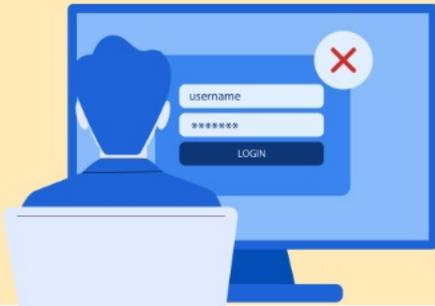
# Self-service password management and security



# How remote users stay on top of AD password and account expiration

## Before ADSelfService Plus

Remote users, especially VPN and OWA users, have no way of being notified about their expiring passwords and accounts. Users often lose access to their accounts and the help desk are rendered unable to assist the users remotely



## After ADSelfService Plus

- Users with passwords or accounts that are nearing expiration receive regular reminders via SMS, email, and push notifications
- Users can change their passwords before expiration and contact the help desk to deal with their AD account expiration



# Rescue users from password fatigue

## Before ADSelfService Plus

A user has to create and maintain a separate set of credentials for each of their enterprise application accounts. This may lead to forgotten passwords or poor password hygiene



## After ADSelfService Plus

- The user's AD password is synchronized across integrated applications
- Any password change or reset is replicated across the applications. They can also choose to change or reset the password of particular applications, if required



# Advanced custom password policies

Create multiple password policies and enable them for users belonging to specific domains, OUs, and groups. Impose the password policy during password changes via the Ctrl+Alt+Del portal and password resets from the Active Directory Users and Computers console.



## Restrict characters

Restrict the number of special characters, numbers, and Unicode characters that users can use



## Restrict patterns

Restrict keyboard sequences, dictionary words, and palindromes



## Use passphrases

Option to use passphrases that does not conform to the complexity requirements when the password length exceeds a predefined limit (say, 20 characters)



## Restrict repetition

Enforce a password history check during password reset, and restrict the repetition of specific character(s) or username as the password.(e.g. "aaaaa" or "user01")



## Restrict length

Specify the minimum and maximum password lengths



## Password strength checker

Display the password policy requirement on the reset and change password pages

# Remote work enablement

Secure and streamline remote work



# Remote work enablement



## MFA for remote endpoints

Implement MFA for remote endpoints such as RDP and VPN logins to secure remote access



## Cached credentials update

Automatically update users' remote password resets in the local cache of their machines via VPN for smooth authentication



## Web-based domain password change

Offer a secure web-based portal for remote employees to change their domain and enterprise application passwords



## Mobile-based password management

Empower users on the go with self-service password reset and account unlock, password change, and enrollment capabilities right from their mobile devices

# How cached credentials update works

The ADSelfService Plus login agent places a Reset Password/Account Unlock link on the login screen of the machine to enable self-service password reset.



To perform password reset, the user first completes identity verification through MFA. Then they submit the new AD password



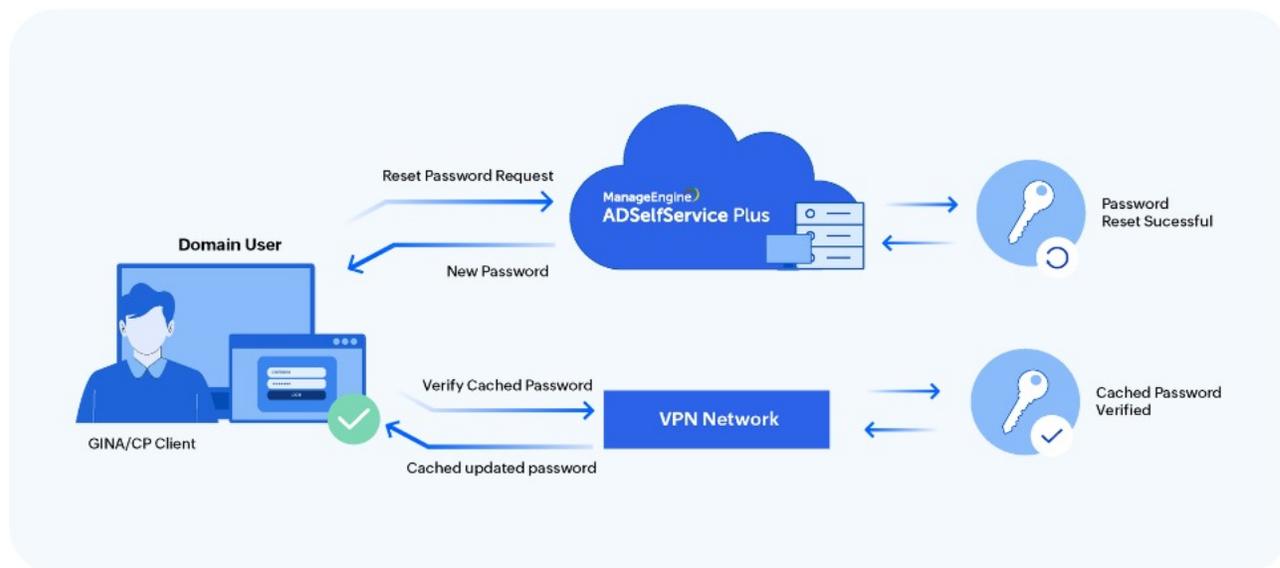
The login agent then establishes a secure VPN connection with AD and requests an update of the local cached credentials



The ADSelfService Plus server resets the AD password and informs the login agent



The new password is now updated as the cached credentials in the machine



## Workforce self-service

**Maintain an up-to-date user profile directory without overburdening the help desk**



# Workforce self-service



## Directory self-update

Allow users to self-update their AD profile information using a secure portal



## Self-service group management

Let users subscribe and unsubscribe from AD groups appropriate to them



## Organization chart

Display the position of users in the organizational hierarchy and allow them to look up employee relations and IDs



## Employee search

Allow users to search for information on their colleagues via a filter-based corporate directory search tool



## Approval-based workflow for self-service

Give help desk technicians the ability to review and approve users' self-service actions

# How does self-update of employee profile information work?

## Before ADSelfService Plus

User has to contact the help desk each time any of their AD profile information needs updating



## After ADSelfService Plus

- User securely logs in to the ADSelfService Plus web portal
- User updates their AD profile information using the console provided
- The information provided is updated in AD in real time



# Directory self-update portal

The screenshot displays a web interface for a directory self-update portal. The top navigation bar includes tabs for "Profile", "Change Password", and "Enrollment", along with a "Search Employee" search bar. The main content area is titled "Edit Profile" and is divided into several sections: "General", "Contact", "Address", and "Organization".

**Profile Information:**

- Name: Alex Samuel
- Employee Id: 12742

**General Information:**

- First name: Alex
- Last name: Samuel
- E-mail: alexsamuel@adselfservice
- Telephone Number: 12 - 35726 - 383
- Web Page: (empty)
- Description: (empty)
- Office: Head office

**Contact Information:**

- Home Phone: (empty)
- Pager: (empty)
- \*Mobile: 521 - 634 - 7851
- Fax: (empty)
- IP Phone: (empty)
- Country/region: ---Select Country---

**Address Information:**

- Street: 57, Cougar Avenue
- PO Box: 2357
- City: Canton
- State: Ohio
- Zip: 2500

**Organization Information:**

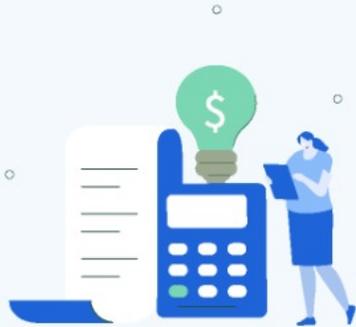
- Title: Technical Support Engineer
- Department: Sales
- Employee Number: A12742
- Company: ADSelfService
- Manager: Bob Riley [Edit]

At the bottom of the form, there are "Update" and "Cancel" buttons.

# Benefits of ADSelfService Plus

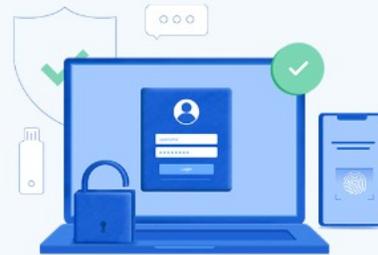
## Cost savings

- Eliminates password resets—a major source of help desk calls
- Allows IT admins to focus on critical tasks
- Protects enterprises from data breach recovery costs



## Improves IT security

- Secures critical enterprise endpoints with MFA
- Provides risk-based access control for enterprise resources and self-service actions
- Enforces strong password policies



## Improves user experience

- Reduces dependency on help desk
- Provides access to self-service features from anywhere
- Enables seamless login for enterprise applications
- Puts an end to password fatigue



# Trusted By



# How ADSelfService can help organizations across sectors

## Government sector

- Comply with the requirements of regulations like FISMA and the NIST Cybersecurity Framework
- Prevent credential-based attacks on the domain network using adaptive MFA and advanced password policies

## IT sector

- Comply with the requirements and guidelines of the GDPR and NIS Directive
- Implement SSO for enterprise applications secured by passwordless authentication based on robust authenticators like biometrics
- Enable users to reset their domain passwords and unlock their domain accounts without depending on their IT help desk

## Education sector

- Comply with the requirements and guidelines of regulations like the Family Educational Rights and Privacy Act (FERPA), and the NIST Cybersecurity Framework
- Empower students and staff to reset their passwords and unlock their accounts from anywhere and access multiple applications from a single console

# How ADSelfService can help organizations across sectors

## Finance sector

- Comply with the requirements and guidelines of SOX, GLBA, PCI DSS, and the NIST Cybersecurity Framework
- Provide seamless access to sensitive data using MFA, conditional access, and SSO
- Enable employees to perform password resets while upholding stringent password policies

## Healthcare sector

- Comply with the requirements and guidelines of HIPAA and the NIST Cybersecurity Framework
- Secure and streamline access to ePHI using SSO, MFA, and conditional access
- Allow healthcare professionals to perform password self-service and ensure up-to-date employee profiles

# TriMark deploys ADSelfService Plus to tackle password problems

**Industry:** Food industry **Location:** USA

“When our employees needed a password reset while they were outside the organization, ADSelfService Plus helped us by allowing them to reset their passwords remotely. It was beneficial for us,”

**Roger DeVivo,**  
senior system administrator at TriMark



## Business needs

- Allow users to self-update their AD profile information using a secure portal
- No trust was established between AD domains leading to password fatigue. They needed a solution that could sync passwords across all of users' account

# How ADSelfService Plus helps Trimark?



ADSelfService Plus helps remote employees reset their passwords, and then it locally updates the credentials in users' machines



ADSelfService Plus' Password Sync feature allowed TriMark to automatically sync all password changes between multiple Active Directory domains



ADSelfService Plus helped admins to schedule password expiration alerts via SMS, email, and push notifications so users change their soon-to-expire passwords, well in advance

"The support team helped me pretty quickly every time I called in, and I'd say I'm happy with the support!"



# Licensing, pricing, and feature support

Detail	Evaluation edition	Free edition	Standard edition	Professional edition
Expiration	Expires in 30 days	No expiration	As per license terms	As per license terms
Number of domains	Unlimited domains	Unlimited domains	As per license terms	As per license terms
Number of domain users	Unlimited domains	50 users	As per license terms	As per license terms
24-5 support	Available	Available	Available	Available
Pricing	<b>Free</b>	<b>Free</b>	<ul style="list-style-type: none"> <li>Starts at <b>\$595</b> for <b>500 users</b></li> <li>Endpoint MFA starts at <b>\$195</b> for <b>100 users</b> (Free for up to 10 users with the ADSelfService Plus Standard and Professional editions)</li> </ul>	<ul style="list-style-type: none"> <li>Starts at <b>\$1195</b> for <b>500 users</b></li> <li>Endpoint MFA starts at <b>\$295</b> for <b>100 users</b></li> </ul>
Features	Fully-functional Professional Edition, along with Endpoint MFA. Converts to Free Edition after evaluation period.	All features offered in Professional edition.	<ul style="list-style-type: none"> <li>Web-based self-service password reset and account unlock</li> <li>MFA for self-service password resets/account unlocks and cloud application logins</li> <li>Password expiry notifier</li> <li>Password policy enforcer</li> <li>Real-time password synchronizer</li> <li>Password reset using ADSelfService Plus' iOS or Android app, or via mobile browser</li> <li>Self-service directory update, employee search, organization chart, and self-service group management</li> <li>Passwordless authentication for cloud applications</li> </ul>	All features supported Standard edition and: <ul style="list-style-type: none"> <li>Password reset from Windows, macOS, and Linux logon screens</li> <li>Conditional access</li> <li>Cached credentials update for remote password reset</li> <li>Password policy enforcement in Windows Change Password page and ADUC</li> </ul>

# Licensing, pricing, and feature support

Detail	Evaluation edition	Free edition	Standard edition	Professional edition
<p><b>Endpoint MFA Features</b></p>	<p>Fully-functional Professional Edition, along with Endpoint MFA. Converts to Free Edition after evaluation period.</p>	<p>Supports all features of the Standard Edition for 50 users. (Includes the Standard Edition of Endpoint MFA for 10 users)</p>	<p>Endpoint MFA's Standard edition offers:</p> <ul style="list-style-type: none"> <li>• SSO for applications</li> <li>• JIT provisioning</li> <li>• MFA for Applications</li> <li>• MFA for Windows, macOS, and Linux machines</li> <li>• Security Question &amp; Answer, SMS and email verification, Google Authenticator, Microsoft Authenticator, AD Security Questions, Zoho OneAuth, and custom software token-based TOTP provider</li> </ul>	<p>Endpoint MFA's Professional edition offers all features supported by the Standard edition and:</p> <ul style="list-style-type: none"> <li>• MFA for Windows server machines</li> <li>• MFA for RDP</li> <li>• Device-based MFA for Windows</li> <li>• MFA for UAC sessions</li> <li>• MFA for VPN &amp; other RADIUS servers</li> <li>• MFA for OWA &amp; other IIS servers</li> <li>• Passwordless logins for applications</li> <li>• Adaptive SSO</li> <li>• Adaptive MFA</li> <li>• Offline MFA for Windows and macOS</li> <li>• Custom hardware token-based TOTP provider for authentication, FIDO Passkeys, Smart card Authentication, SAML Authentication, YubiKey Authenticator, Duo Security, Radius Authentication, Push Notification, QR Code Based Authentication, biometric authentication, ADSelfService Plus mobile app TOTP, Azure AD MFA, and RSA SecurID</li> </ul>



# Add-ons

Add-on name	Description	Pricing
<b>Failover and Secure Gateway Services add-on</b>	Includes high availability, load balancing) and reverse proxy	<b>\$395</b>
<b>SMS add-on</b>	Includes Clickatell, a third-party SMS gateway, to send notifications and MFA verification codes via SMS.	Starts at <b>\$395</b> for <b>2000</b> SMS credits

# 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**

