ManageEngine
ADSelfService Plus

Maximize **Endpoint Security** with **adaptive MFA**

www.manageengine.com/products/self-service-password

Maximize endpoint security with adaptive MFA

Endpoints are an important entity in any organization's security policy. Network data and resource protection starts with securing access to all points of entry. Access policies based only on passwords are now outdated, and modern methods like MFA have become the norm. Industry leaders recommend following stringent security models like Zero Trust that leave no access attempt by any user unverified no matter the user's credibility and the target resource's significance.

ManageEngine ADSelfService Plus is a holistic endpoint authentication solution that prioritizes both security and the user experience. The solution delivers advanced, adaptive MFA to secure enterprise endpoints and alleviate the risk of data compromise and account takeover.

What makes ADSelfService Plus a superior endpoint security solution?

Well-rounded endpoint protection

ADSelfService Plus can secure the following enterprise endpoints using its MFA feature:

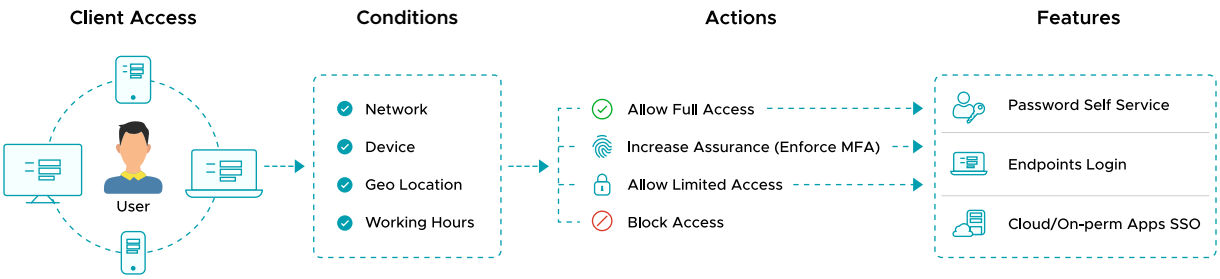
- Workstations and servers (Windows, Linux, and macOS machines)
- VPNs and RADIUS-based access points
- OWA and IIS-based applications
- Windows access points like RDP, machine unlocks, and User Account Control (UAC) prompts
- Enterprise cloud application logins (via SSO)

Balance enterprise security with a good user experience

Enable conditional access policies that leverage access data such as:

- Number of consecutive logon failures
- The device used for access
- The device's IP address
- Time of access
- Geolocation

Conditional access policies use this data to create dynamic authentication flows that scale up or tone down the identity verification process automatically.



*Conditional access is not supported for VPN MFA.

Don't stop with user identities—protect critical machine identities using MFA
<diagram depicting user-based and machine-based MFA>

Description:
User-based MFA: Secure a user's identity through advanced authentication during every login.

Machine-based MFA: Secure an enterprise machine (user workstation, server, domain controller, etc.) through advanced authentication during access attempts by any user.

Enable an elaborate, two-stage advanced authentication system for remote connections.

The user is authenticated using MFA when initiating the remote desktop connection from their local machine.	The user is authenticated using MFA when logging in to the remote desktop.

Endpoints solutions supported by ADSelfService Plus for MFA:

Endpoint type	Solutions supported out of the box	The feature can also be configured for
OS for user-based machine logins	Windows, macOS, and Linux	Chromebook
OS for machine-based logins and other peripheral access attempts	Windows	_
VPN providers	All RADIUS-based VPN providers	Other RADIUS-based endpoints such as Citrix Gateway
OWA	All versions	Other IIS web applications
Enterprise applications	Built-in support for more than 100 SAML, OIDC, and OAuth applications	Custom cloud and on-premises applications

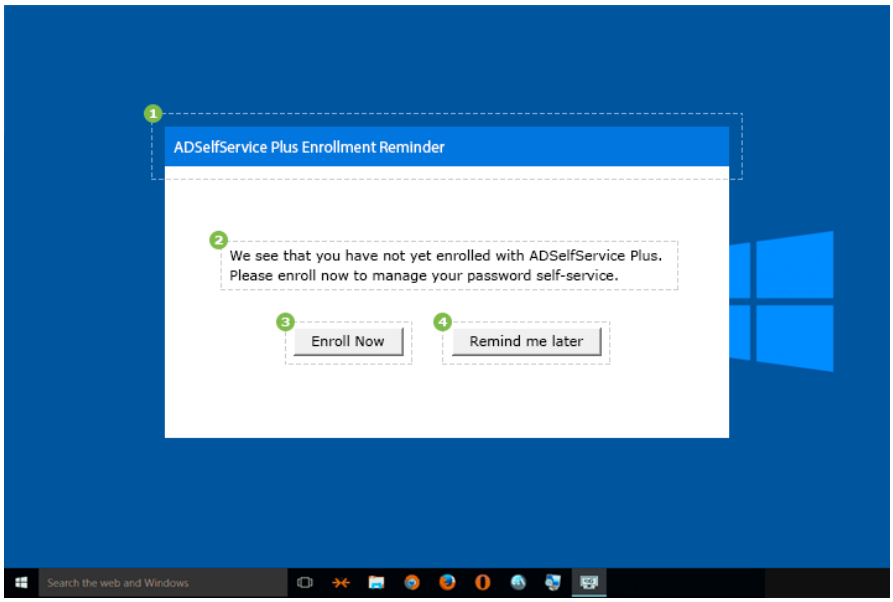
A diverse authentication system

Pick from 19 authenticators to customize an MFA model that fits your enterprise:

1. Fingerprint or Face ID authentication
2. YubiKey Authenticator
3. Google Authenticator
4. Microsoft Authenticator
5. Azure AD MFA
6. Duo Security
7. RSA SecurID
8. RADIUS
9. Zoho OneAuth TOTP
10. TOTP authentication
11. Push notification authentication
12. QR code-based authentication
13. Custom TOTP authenticator
14. SAML authentication
15. Security question and answer
16. Email verification
17. SMS verification
18. AD security questions
19. Smart card authentication

Guaranteed user onboarding

Encourage users to enroll for MFA via notifications, bulk-enroll them without their intervention using CSV files and databases, or force them to enroll using logon scripts.

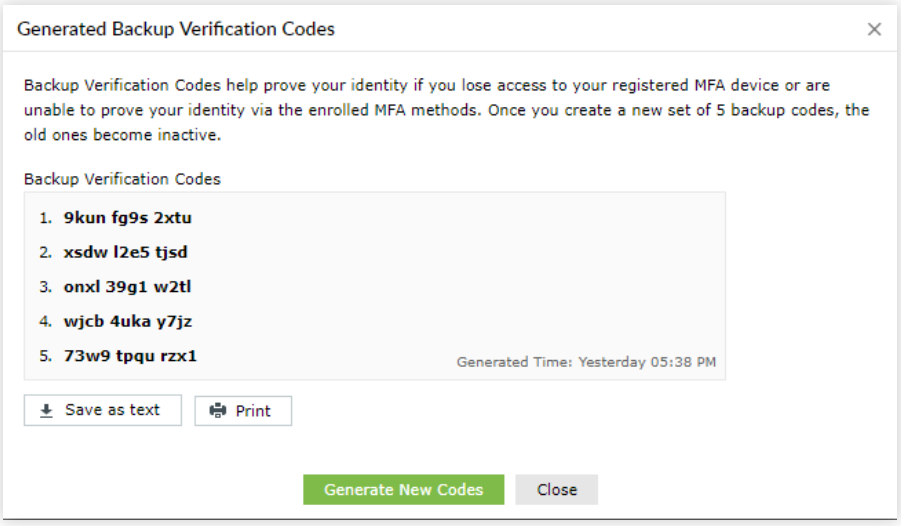


Offline access protection

Ensure secure authentication even when the user is not connected to the internet and the ADSelfService Plus server is unreachable using offline MFA in place of the default Endpoint MFA feature. Offline MFA is supported for Windows authentication events such as Windows machine logins, User Account Control prompts, remote desktop access, and machine unlocks.

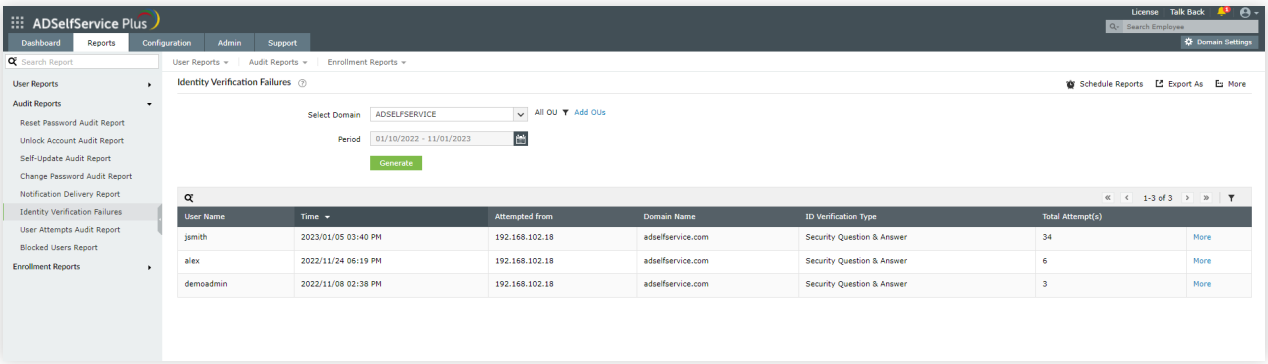
Backup verification support

Allow users to prove their identities in case their MFA device is not reachable or if they are unable to use their enrolled MFA methods of authentication. Once the setting is enabled, the backup codes can be generated. End users can save them and use them to authenticate themselves during endpoint logins.



Up-to-date reports on authentication attempts

Gain insight into users' MFA attempts and authentication status through audits detailing information such as time of authentication attempt, type of authentication method used, status of authentication attempts, and user enrollment status.



Why choose ADSelfService Plus for endpoint security

Identity-first security approach

- Move on from the age-old network perimeter security model to the latest identity-first security approach by verifying access attempts by users into any enterprise endpoint and resource.
- Use advanced authentication techniques to secure access to all major local and remote enterprise endpoints.
- Ensure enterprise resources are well-fortified without subjecting genuine users to a lengthy authentication process.

Thwart credential attacks

- Curb credential exploitation at the earliest stages using contextual MFA, i.e., modern techniques such as biometrics and hardware tokens.
- Set a true MFA model with up to three levels of identity verification to render stolen credentials useless.

Context-aware authentication

- Enable dynamic authentication flows that leverage access data such as the device used for access, the device's IP address, time of access, and the user's geolocation to scale up or tone down the identity verification process automatically.
- Rely on offline MFA and backup codes for secure data and resource protection even during unforeseen network disruptions.
- Ensure enterprise resources are well-fortified without subjecting genuine users to a lengthy authentication process.

Hybrid work security

- Guard VPN and remote desktop connections to the enterprise network using advanced authentication techniques.
- Set automatic access controls that heighten the authentication process upon remote access detection.
- Verify remote access attempts in detail by setting advanced verification techniques at both the source and the target machine.

Other features offered by the solution

- Enterprise single sign-on
- Self-service password management
- Password synchronization
- Advanced password policy
- Password expiration notifications
- Cached credentials update
- Directory self-update
- Employee search and organizational chart

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets, and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

$ Get Quote Download