ManageEngine
ADSelfService Plus

Vs

Microsoft Entra ID

www.adselfserviceplus.com

Product overview

About ADSelfService Plus

ManageEngine ADSelfService Plus is an identity protection solution that ensures secure and seamless access to enterprise resources and helps establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication (MFA), single sign-on (SSO), self-service password management, a password policy enhancer, remote work enablement, and workforce self-service, ADSelfService Plus provides your employees with secure 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.

About Microsoft Entra ID

Microsoft Entra ID (formerly Azure AD) is a cloud-based identity and access management platform that enables authentication, authorization, and access control for applications and resources. It includes native capabilities such as SSO, MFA, self-service password reset, conditional access, and hybrid identity integration.

What ADSelfService Plus adds to Entra ID environments

Entra ID provides a cloud-native identity control plane with tightly integrated authentication and access management. ADSelfService Plus extends these capabilities with additional authentication flexibility, endpoint security, and hybrid access management. Start using ADSelfService Plus to gain:

- Support for authentication methods not natively available in Entra ID, including Duo Security, RSA SecurID, YubiKey Authenticator, custom TOTP authenticators, and security question-based verification.
- Support for up to three authentication factors within a single MFA workflow, compared to Entra ID's two-step authentication flow.
- Endpoint MFA for Windows logins, UAC prompts, local user accounts, system unlocks, and supported RDP access on Entra ID joined and hybrid joined devices.
- Offline MFA for Windows endpoints, enabling authentication even without internet connectivity.
- Granular MFA and SSPR policy configuration for hybrid environments, with policies scoped based on domains and groups.
- Password synchronization across integrated enterprise applications.
- Advanced password policy enforcement with regex-based rules, dictionary checks, character-sequence restrictions, custom blocklists, and real-time password strength analysis.

ADSelfService Plus is particularly valuable for organizations that require stronger endpoint-level protection, broader authentication flexibility, and enhanced hybrid identity capabilities on top of Entra ID.

Feature comparison

Feature	ADSelfService Plus	Microsoft Entra ID
Multi-factor authentication (MFA)		
MFA	✓	✓
Number of authentication factors in a single MFA workflow	Up to 3	Up to 2 (primary + secondary)
Authenticator diversity	**Supports 17 authentication methods, including:** • Security question and answer • Email verification • SMS verification • Google Authenticator • FIDO2 passkeys • Microsoft Authenticator • Duo Security • RSA SecurID • Push notification authentication • Biometric authentication • QR code-based authentication • TOTP authentication *(via ADSelfService Plus mobile app)* • SAML authentication • YubiKey authenticator • Zoho OneAuth TOTP • Custom TOTP authenticator • Backup codes	**Supports 12 authentication methods, including:** • Windows Hello for Business • FIDO2 *(security keys and device-bound/synced passkeys across Windows, macOS, iOS, and Android)* • Microsoft Authenticator *(passwordless sign-in, push notification MFA, passkeys, and Authenticator Lite in Outlook mobile)* • Certificate-based authentication *(CBA)* • Hardware OATH tokens *(Preview)* • Software OATH tokens • SMS • Voice call • QR code • Email one-time password *(OTP)* • External authentication methods *(third-party MFA via OIDC, requires P1)* • Temporary Access Pass (TAP) *(recovery authentication method)*
Passwordless authentication	✓	✓

Phishing-resistant authentication	✓ (FIDO2 passkeys)	✓ (FIDO2, Windows Hello for Business, CBA)
Conditional access	✓ **Supports 3 condition types:** • IP address • Geolocation • Time-based access policies	✓ **Supports 8 condition categories:** • Network/location *(named IP ranges, countries/regions, GPS coordinates, compliant network)* • User risk • Sign-in risk • Insider risk • Agent risk *(Preview),* • Device platform *(Android, iOS, Windows, macOS, Linux)* • Client app type *(modern and legacy authentication clients)* • Device attribute filters **Note:** User risk, sign-in risk, and agent risk require Entra ID P2 *(ID Protection);* insider risk requires Microsoft Purview adaptive protection.
Machine login MFA	✓ Windows devices (Microsoft Entra ID joined and Microsoft Entra hybrid joined)	✗ Entra ID does not support enforcing a separate MFA prompt at the Windows login screen after device join. Conditional Access MFA policies apply to application and cloud resource sign-ins, not to local Windows login events. Windows Hello for Business secures device login with PIN or biometrics but is a device-bound credential, not a centrally enforced per-login MFA layer.
Offline MFA	✓ (For Windows endpoints)	✗
MFA for local user accounts	✓	✗

MFA for UAC/ system unlock	✓	✗
MFA for RDP	✓ RDP server support for Entra ID joined devices, except web account; RDP client not supported for pure Entra ID joined devices	Limited (Native RDP MFA is supported only for Azure VMs via Conditional Access; not available as a standalone MFA layer for general RDP access to Entra ID-joined Windows machines.)
MFA for enterprise applications	✓	✓
Self-service password reset (SSPR)		
SSPR	✓ Via Microsoft Graph API	✓ Available with Microsoft 365 Business Standard or higher, and all Entra ID P1/P2 SKUs; on-premises writeback requires P1, Business Premium, or P2
Password change	✓	✓
Web-based password reset	✓	✓
Mobile app password reset	✓	✓
Windows login screen reset	✓	✓
Password reset notifications	✓	✓
Account unlock	✓ Not supported for Entra ID users; Entra ID does not expose a standalone account lock/unlock property via Microsoft Graph API	Partial (Cloud-only users can only clear a lockout by resetting their password via SSPR; standalone account unlock without password reset is available only in hybrid environments with on-premises writeback configured; not available for pure cloud Entra ID users.)

Self-service profile update	✓ Not supported in current release for Entra ID users	Limited (Users can update their profile photo and security contact information via the My Account portal; attributes such as display name, job title, and department are admin-managed and not user-editable by default; on-premises synced users must update attributes in on-premises AD.)
Password security and policy enforcement		
Custom password policies	✓	✗
Minimum password length	✓ Configurable	Fixed at 8 characters; not configurable for cloud users
Maximum password length	✓ Configurable	Fixed at 256 characters; not configurable
Character complexity rules	✓ Configurable — enforce or restrict specific character types, sequences, and patterns	Fixed — requires 3 of 4 character types (uppercase, lowercase, numbers, symbols); not configurable
Regex-based password rules	✓	✗
Dictionary-based checks	✓ Custom dictionary blocklists	Limited (Global banned password list (Microsoft-managed, cannot be viewed or modified) + custom banned list of up to 1,000 terms (requires P1).)
Custom banned password list	✓	✓ Supported (Up to 1,000 terms; case-insensitive; accounts for common character substitutions (e.g. “o” and “0”); requires P1.)
Character-sequence restrictions	✓	✗

Unicode character restrictions	✗ Not supported for Entra ID users	✗
Real-time password strength analyzer	✓	✗
Password history enforcement	✓ Granular control (with on-premises AD). **Note:** When used with Entra ID, password history enforcement depends on the tenant's own cloud policy settings.	✓
Breached password protection	✓ Via external integrations (HaveIBeenPwned)	✓ Microsoft global banned list
Password expiration notification	✗ Not supported for Entra ID users in current release	✓
Single sign-on (SSO)		
SSO capability	✓	✓
SSO scope	SSO portal with SAML-based access to integrated enterprise and custom applications	SSO across SaaS, Microsoft 365, and custom applications
Protocol support	SAML 2.0, OAuth 2.0, OpenID Connect	OAuth 2.0, OpenID Connect, SAML, WS Federation, Kerberos
Identity provider (IdP) role	Can act as IdP for SAML applications; operates alongside existing AD/Entra infrastructure	Acts as primary IdP
SSO with conditional access	Policy-based controls (IP address, geolocation, time-based)	Native risk-based conditional access (user risk, sign-in risk, device compliance, client app, and more)

Password synchronization for enterprise applications	✓	✗
Risk-based and device-based access control	✗	✓
Cross-domain / multi-tenant SSO	Supports multiple Entra ID tenants simultaneously via a unified console	Full federation support (Cross-tenant synchronization, B2B collaboration, and direct federation with external identity providers.)

Licensing comparison

Capability	Entra ID Free Plus	Entra ID P1	Entra ID P2	ADSelfService Plus
Self-service password management	Limited	Advanced SSPR	Advanced SSPR	Advanced SSPR
MFA and adaptive access controls	Basic MFA	MFA with Conditional Access	Risk-based access with Identity Protection	MFA with Conditional Access
SSO	Basic SSO	Enterprise SSO	Enterprise SSO	Enterprise SSO
Password policy enforcement	Basic	Advanced	Advanced + risk insights	Advanced granular password policy enforcement

Closing the gaps: Why Entra ID users choose ADSelfService Plus

While Microsoft Entra ID provides robust cloud-native identity capabilities, organizations often require greater flexibility and control to address real-world identity security challenges. ADSelfService Plus extends Entra ID in these areas, helping organizations strengthen security and improve user experience without disrupting their existing identity infrastructure.

Greater flexibility and customization in MFA

ADSelfService Plus offers a broad authenticator ecosystem, including FIDO2 passkeys, Duo Security, RSA SecurID, YubiKey, custom TOTP authenticators, biometrics, and email/SMS OTP. In addition to authenticator support, ADSelfService Plus provides extensive MFA customization capabilities, including configurable authentication workflows with up to three authentication factors, factor sequencing, authenticator-specific settings, browser trust options, MFA timeout controls, and customizable email/SMS OTP settings such as verification code length and templates. This enables organizations to tailor MFA experiences to their security, compliance, and usability requirements while integrating with existing identity infrastructure.

Extend identity security beyond the login layer

Entra ID primarily focuses on identity and access management for applications, cloud services, and user sign-ins. ADSelfService Plus extends MFA enforcement to the endpoint login surface for Windows devices and supported RDP access, helping organizations secure how identities are actually used.

Enhanced self-service experience

ADSelfService Plus enhances password self-service with customizable MFA policies and support for web-based, mobile, and supported Windows login screen password reset scenarios, helping organizations strengthen security while providing flexible self-service options for users.

Advanced password policy control

ADSelfService Plus enables granular password policy enforcement with real-time strength analysis, dictionary checks, and pattern restrictions, allowing organizations to strengthen password security beyond native Entra ID capabilities.

Extended password synchronization capabilities

ADSelfService Plus enables password synchronization for integrated enterprise applications when users reset or change passwords through the product, helping maintain consistent credentials across connected systems.

Cost effective security expansion

Organizations that require advanced self-service password management and MFA capabilities may need to upgrade from Entra ID P1 to P2 licensing to access the full range of advanced controls and capabilities. ADSelfService Plus delivers these capabilities at up to 6x–8x lower cost than Entra ID P2 while enabling organizations to continue leveraging their existing Entra ID infrastructure.

Conclusion

Microsoft Entra ID provides a cloud-native identity foundation, but organizations that require broader MFA options, endpoint-level protection, advanced password policy enforcement, and greater control in hybrid environments often need capabilities beyond native Entra ID offerings. ADSelfService Plus fills these gaps by extending identity security beyond login with endpoint MFA, flexible authentication policies, advanced self-service password management, and password synchronization. For organizations looking to strengthen identity security without replacing their existing Entra ID infrastructure, ADSelfService Plus provides a flexible and cost-effective extension to native Entra ID capabilities.

Disclaimer: This comparison document has been created using information available online about Microsoft Entra ID. Details may vary in the actual product. In case you find any discrepancies, please write to **support@adselfserviceplus.com**.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus
M365 Manager Plus

ManageEngine
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