ManageEngine
ADSelfService Plus

Extend Microsoft Entra ID with ADSelfService Plus

Fill the gaps in native Entra ID with stronger MFA, smarter SSPR, and endpoint-level protection

The gaps in native Entra ID

Entra ID gives you a solid cloud identity foundation. But organizations running it at scale hit the same limits:

MFA stops at the cloud sign-in

Conditional access MFA applies to applications and cloud resources, but not to the Windows login screen, UAC prompts, local accounts, or system unlock

Authenticator choice is narrow

No native support provided for Duo, RSA SecurID, YubiKey OTP, custom TOTP, or security questions. Third-party MFA via OIDC requires P1 license

Password policy is fixed

Minimum length is locked at 8 characters Complexity is "3 of 4 character types." No regex, no sequence rules, no real-time strength feedback, and no custom dictionaries beyond the 1,000-term banned list

Risk-based controls sit behind P2

User risk, sign-in risk, and Entra ID Protection require the top SKU which isn't always convenient.

Account unlock requires a password reset

For cloud-only users, there's no standalone unlock—the only way out of a lockout is SSPR

4 capabilities, layered on top of your existing Entra ID tenant

Additionally, ADSelfService Plus provides SSO for applications outside Entra ID's catalog, and password synchronization to those applications.

Endpoint MFA

Windows login, UAC, local accounts, system unlock, supported RDP. Works offline

Broader MFA authenticator support

17 methods, including Duo, RSA SecurID, YubiKey, custom TOTP, and security questions

Granular password policy enforcement

Regex rules, sequence restrictions, dictionary blocklists, real-time strength analysis

Self-service password reset and change

Via Microsoft Graph API, with your choice of MFA verification

Endpoint MFA: Where native Entra ID can't reach

Entra ID's conditional access enforces MFA on application and cloud resource sign-ins. It does not enforce MFA on the Windows login screen.

ADSelfService Plus adds MFA to

- **Windows machine login:** Entra ID joined and hybrid joined devices
- **UAC and system unlock prompts**
- **Local Windows user accounts**
- **Supported RDP access:** Server-side support on Entra ID joined devices
- **Offline scenarios:** Endpoint MFA works without internet connectivity

17 MFA authenticators

Choose the factor that fits your users, endpoints, and security posture.

Possession-based (something you have)

- Email OTP
- SMS OTP
- Push notification
- Google Authenticator
- Microsoft Authenticator
- Zoho OneAuth TOTP
- Custom TOTP
- YubiKey
- RSA SecurID
- FIDO2 passkeys
- QR code login
- Backup codes

Inherence-based (something you are)

- Face ID/biometric
- Fingerprint (FIDO2)

Knowledge-based (something you know)

- Security questions and answers

Federation and third-party

- SAML authentication
- Duo Security

ADSelfService Plus

Self-service password reset for Entra ID users

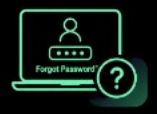
Let Entra ID users reset their own passwords from any device, after verifying themselves through MFA.

Password reset
Forgotten password? Verify with MFA and set a new one without IT involvement.

Change password
Change a known password from the self-service portal at any time.

Force change at next logon
Admins can require users to change their password on next login.

How it works



1

User clicks "Forgot Password
From the Windows login screen, mobile app, or web portal.

2

Identity verified via MFA
Email OTP, TOTP, FIDO2 passkey, push, and more.

3

Password updated in Entra ID
Reset is written through Microsoft Graph API.

ADSelfService Plus

Password policy enforcer

Native Entra ID password policy is fixed: 8-character minimum, "3 of 4" complexity, Microsoft-managed global banned list, and a custom banned list of up to 1,000 terms with P1.

ADSelfService Plus replaces that with a policy you actually control:

- **Configurable length**
  Minimum and maximum length of passwords
- **Granular character rules**
  Specify required and restricted character classes
- **Regex-based rules**
  Match patterns your default policy can't express
- **Sequence and repeat restrictions:**
  Block keyboard walks and repeating patterns
- **Custom dictionary blocklists:**
  No 1,000-term ceiling similar to Entra ID
- **User-attribute restrictions**
  Block passwords containing the user's name or display name
- **Real-time strength analyzer**
  Feedback at the moment of reset or change
- **Breached password protection**
  Via HaveIBeenPwned integration
- **Domain or group-level scoping**
  Different rules for different populations inside the tenant

Adaptive MFA with conditional access

Apply different MFA rules based on context. Three condition types you can combine:

IP-based

Trusted IP ranges. Streamline corporate-network logins; strengthen for public Wi-Fi

Geolocation-based

Allow standard MFA from expected countries; escalate or block from unexpected ones

Time-based

Tighter requirements outside business hours; relaxed during them

SSO for applications outside Entra's coverage

Entra ID is your primary identity provider. ADSelfService Plus operates alongside it:

Application SSO

SSO portal with SAML-based access to integrated enterprise and custom applications

Password synchronization to integrated applications

When users reset or change passwords through ADSelfService Plus, credentials sync to connected enterprise apps. Native Entra ID does not do this

SSO logins with conditional access policies

Apply policy-based controls to application sign-ins (based on IP address, geolocation, and time)

3 deployment scenarios

Scenario A **Cloud-only organization**	Scenario B **Hybrid organization**	Scenario c **Migrating to the cloud**
All users live in Entra ID. ADSelfService Plus delivers self-service password reset, adaptive MFA, and policy enforcement for your entire workforce.	Users exist in both AD and Entra ID. Manage both from one console.	Currently AD-heavy, moving to Entra ID. Onboard Entra ID users at your pace while continuing to serve AD users with the same product.

Already using native Entra ID?
Here's what ADSelfService Plus adds

Capability	Native Entra ID	ADSelfService Plus
MFA at Windows login, UAC, system unlock	✗	✓
MFA for local Windows accounts	✗	✓
Offline endpoint MFA	✗	✓
Authenticator choice	12 methods, including third-party MFA via OIDC requires P1	17 methods natively, including Duo, RSA, YubiKey
Factors in a single MFA workflow	2	Up to 3
Password minimum length	Fixed at 8	Configurable
Password complexity	Fixed: 3 of 4 character types	Regex, sequence rules, custom dictionaries
Real-time password strength feedback	✗	✓
Custom dictionary blocklist	Capped at 1,000 terms (P1)	No fixed cap
Password sync to enterprise applications	✗	✓

Built for IT teams running modern identity

Lower help desk load
Users reset their own passwords. Help desk ticket volume decreases.

Stronger authentication
Adaptive MFA across self-service, applications, and Windows endpoints

Single pane of glass
AD and Entra ID, managed from one console.

Granular password policy
Enforce rules your default policy doesn't cover.

Stronger authentication
Advanced MFA and SSPR without upgrading to Entra ID P1/P2.

Faster user productivity
Self-service reduces time-to-access.

ADSelfService Plus

Ready to extend ADSelfService Plus to Entra ID?

Bring AD and Entra ID under one identity platform

Start a free trial or request a personalized demo to see ADSelfService Plus working with your Entra ID tenant.

Start free trial

Request a demo

ADSelfService Plus