ManageEngine ADSelfService Plus

Vs

LogonBox Identity Manager

About ManageEngine ADSelfService Plus

ManageEngine 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 (MFA), single sign-on (SSO), workforce self-service, and password management and security, this solution provides your workforce with secure, yet frictionless access to resources. ADSelfService Plus helps keep identity-related threats out, reduce password-related help desk tickets, fast-track application onboarding, and empower remote workforce with secure access to the resources they need.

About LogonBox Identity Manager

LogonBox Identity Manager (previously Access Manager) is an identity management software offering offers self-service password reset, password vault, browser password manager, user management, SAML SSO, and MFA using various authentication options, including the LogonBox Authenticator 2FA solution.

Disclaimer: This comparison document has been created using information available online on LogonBox Identity Manager. Details may vary in the actual product. In case you find any discrepancies, please write to support@adselfserviceplus.com.

Feature	Description	ManageEngine ADSelfService Plus	LogonBox SSPR
Adaptive MFA			
True MFA	Support for true MFA using more than two levels of authentication.	✓	✓
MFA for machine logins	Configure MFA for Windows, Linux, and macOS desktop logins.	✓	✓ *Only for Windows logins
MFA for UAC prompts and system unlocks	Enable MFA for peripheral Windows access attempts such as UAC prompts and system unlocks.	✓	✗

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.	✓	✗
MFA for remote desktop logins	Secure remote desktop logins using MFA.	✓	✓
MFA for VPN logins	Verify the user's identity during VPN logins using MFA.	✓	✓
MFA for cloud applications	Protect logins to enterprise applications supporting SAML, OAuth, and OpenID Connect protocols using MFA.	✓	✓
MFA for Microsoft Exchange web applications	Secure logins to Microsoft Exchange products like Outlook Web Access and the Exchange Control Panel.	✓	✗
MFA for other RADIUS-based endpoints	Secure endpoints supporting RADIUS authentication, like Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway.	✓	✗
Customized MFA for specific users	Enable specific MFA methods for particular users.	✓ * MFA configuration is achieved through policies that can enforce specific authentication methods for users belonging to particular AD groups and OUs.	✓

Supported authentication methods	The authentication methods supported out of the box for MFA	**Supports 19 authenticators:**	**Supports the following authenticators:**
		• Fingerprint/Face ID authentication • YubiKey Authenticator • RSA SecurID • Duo Security • Azure AD MFA • Google Authenticator • Microsoft Authenticator • SMS-based verification code • Email-based verification code • Time-based One-Time-Passcode • Custom TOTP Authenticator • Zoho OneAuth TOTP Push notifications • QR code-based authentication • SAML authentication • Smartcard authentication • Security questions and answers • AD-based security questions	• Yubico Authentication • PIN Authentication • CAPTCHA Authentication • Duo Authentication • Google 2-Factor Authentication • SMS-based One-Time Password Delivery • Email-based One-Time Password Delivery • LogonBox Authenticator (Available only in the LogonBox Enterprise edition) • LogonBox Cloud Messaging
Passwordless authentication	Support to access SSO-enabled applications using advanced authentication methods such as biometrics, YubiKey, Google Authenticator, and more.	⊘	⊘ *Only using Yubico

Conditional access	Enable, disable, or modify MFA based on risk factors such as IP address, time of access, the device used, and geolocation.	✓ • IP address • Device used • Geolocation • Time of access	✓ • IP address • Device used • Time of access
Password management and security			
Self-service password reset	Allow users to reset their passwords without admin intervention.	✓	✓
Self-service account unlock	Allow users to unlock their accounts without admin intervention.	✓	✓
Web-based domain password change	Offer a secure web browser-based portal for users to change their domain and enterprise application passwords.	✓	✗
Password expiration notification	Notify users about impending password expiration.	✓ *Email, SMS, and Push notifications	✓ *Email notifications only
Account expiration notification	Notify users about impending account expiration.	✓	✗
Real-time password synchronization	Automatically synchronize users' AD passwords with cloud applications and other on-premises systems.	✓ **Supports password sync with 18 applications, including:** • Google Workspace • Microsoft SQL Server • Microsoft 365/Azure • Salesforce • OpenLDAP	✓ **Supports password sync with applications such as:** • Active Directory • LDAP • Linux SSH • Azure Active Directory • Google Directory

Password policy enforcer	Configure custom password policies for OUs and groups.	✓	✓
Automatic password reset and account unlock	Automatically reset expired passwords and unlock locked accounts.	✓	✗
Password strength analyzer	Analyze and display the strength of the password being created.	✓	✗
Password history enforcement	Enforce AD password history settings during password reset.	✓	✓
Cached credentials update	Update cached credentials when users reset their passwords even if they are not connected to the corporate network.	✓	✓
Help-desk-assisted password reset and account unlock	Integrate password self-service with your review- and approval-based help desk software.	✓	✓
Account unlock, password reset, and change notifications	Notify users when their password is reset or changed or their account is unlocked successfully.	✓	✓
Single sign-on			
Single-sign on for enterprise apps	Offer out-of-box SSO support for hundreds of enterprise applications.	✓	✓
Supported SSO protocols	The protocols supported by the product for SSO	• SAML • OpenID Connect • OAuth	• SAML

SSO for custom applications	Supports SSO configuration for custom applications.	✓	✓
Single sign-on for product login	Automatically login users with their domain login credentials using NTLMv2 authentication.	✓	✗
Workforce self-service			
Directory self-update	Allow users to update their AD information without admin intervention.	✓	✗
Self-service group management	Let users subscribe to or unsubscribe from mail groups of their choice.	✓	✗
Employee search	Provide admins and end users with an option to search and view information about themselves and other domain users.	✓	✗
Organization chart	Let users check their position in the organization hierarchy.	✓	✗
Enrollment for identity verification			
Force enrollment	Force users to enroll for MFA when they log in to their machine.	✓	✓
Enrollment notification	Remind users of enrollment through email or push notification.	✓	✓
Import enrollment data	Enroll users without their intervention by importing enrollment data through CSV files or external databases.	✓	✗

Enroll users using AD	Use AD attribute values to enroll users automatically for SMS and email OTP.	✅	✅
Accessibility			
Web interface	Access the admin portal and user portal from a web browser.	✅	✅
Mobile interface	Access the admin portal and user portal from a mobile web browser.	✅	❌
Self-service password reset and account unlock from login screens	Enable self-service password reset capability from Windows and macOS login screens		
Dedicated mobile app	Allow users to perform self-service actions from dedicated Android and iOS apps.	✅	✅
Rebranding	Customize the product with the desired browser title, logo, theme color, etc.	✅	✅
Reporting			
Native reporting feature	Access built-in reports on user actions and status.	✅	✅
Dashboard	View a graphical representation of password status, user actions, and enrollment data.	✅	❌

User reports	Get reports on locked-out users and users with expired or soon-to-expire passwords.	✓	✓
Audit reports	Get reports on reset passwords, unlocked accounts, identity verification, and user login attempts.	✓	✓
Enrollment reports	Get reports on enrolled users, non-enrolled users, and licensed users.	✓	✓
Export and schedule reports	Export reports in the desired formats, and configure a scheduler to generate and email the selected reports.	✓	✓
Pricing			
Pricing information		ADSelfService Plus offers two editions: Standard and Professional. Pricing starts at USD 595 for the Standard edition, and USD 1,195 for the Professional edition for 500 domain users.	LogonBox SSPR self-install and LogonBox SSPR cloud are available in two editions, Professional and LogonBox Enterprise. Pricing for 50 users is as follows: • Self-install SSPR's Professional and LogonBox Enterprise editions are priced at USD 422 and USD 528 respectively. • Cloud SSPR's Professional and LogonBox Enterprise editions are priced at USD 845 and USD 1,705 respectively.

What makes ADSelfService Plus a cut above LogonBox Identity Manager?

- **Automatic password reset:** ADSelfService Plus's automatic password reset feature improves user productivity by instantly resetting expired user passwords without prompting based on custom, advanced password policies.

- **MFA support for Linux and macOS machines:** ADSelfService Plus offers MFA for Linux and macOS machines. It also extends the self-service password reset feature to Linux login screens.

- **SSO for OAuth and OpenID Connect applications:** In addition to offering SSO for enterprise applications based on SAML, ADSelfService Plus also supports OAuth -based and OpenID Connect-based applications both established and custom.

- **In-house authenticators:** In addition to supporting major third-party authenticators for MFA, all editions of ADSelfService Plus also offers a suite of in-house authenticators including biometrics, QR code-based authentication, push notification and, TOTP. LogonBox offers the LogonBox Authenticator that supports only biometric authentication as part of the Enterprise edition.

- **Workforce self-service:** ADSelfService Plus offers features that empowers users to manage their AD profile without help desk assistance. It offers directory self-update, self-service group subscription, and employee search to not just offload the help desks ticket but also boost end-user productivity.

Try our free, 30-day trial for first-hand experience of ADSelfService Plus. For more information on the product, visit our website.

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