ManageEngine
ADSelfService Plus

ADSelfService Plus

ist eine Identitätssicherheitslösung mit Funktionen wie adaptiver MFA, Single-Sign-On (SSO) und Self-Service-Passwort-Management

Schützen Sie die Identitäten Ihrer Anwender in lokalen, Cloud- oder hybriden Umgebungen vor Identitäts-basierten Angriffen.

Highlights

- Sichern Sie Anmeldungen an Endpoints und bei Cloud-Anwendungen sowie Self-Service-Funktionen wie Passwortzurücksetzungen oder Kontoentsperrungen mit Multi-Faktor-Authentifizierung (MFA) ab.
- Stellen Sie Ihren Endanwendern eine einzige Identität zur Verfügung, mit der sie durch Single-Sign-On und Just-in-Time (JIT) Provisioning einfach auf alle Unternehmensanwendungen zugreifen können.
- Erlauben Sie es Ihren Anwendern, ihre Passwörter selbst zurückzusetzen und Konten zu entsperren, ohne die Sicherheit zu gefährden.
- Informieren Sie Anwender regelmäßig mit individuell anpassbaren und automatisierten Benachrichtigungen über das Ablaufdatum von Passwörtern und Konten.
- Erzwingen Sie plattformübergreifende, granulare Passwortrichtlinien mit anpassbaren Mindestanforderungen. Sie können beispielsweise Begriffe aus dem Wörterbuch ausschließen oder die „Have I Been Pwned"-Integration nutzen.
- Ermöglichen Sie es Anwendern, ihre persönlichen Daten im Active Directory (AD) zu aktualisieren oder umfassende Suchen im Unternehmensverzeichnis durchzuführen.

Aktuelle Herausforderungen

Benutzeridentitäten in hybriden Umgebungen abzusichern und zu verwalten, kann für IT-Abteilungen zu einer echten Herausforderung werden. Anwender greifen sowohl lokal als auch remote über verschiedene Endpoints auf das Unternehmensnetzwerk zu, und jeder einzelne Zugriffsversuch muss genau überprüft werden. Gleichzeitig sollte der Zugriff auf alle Unternehmensressourcen jederzeit reibungslos funktionieren. Identitätssicherheitslösungen helfen, diese Herausforderungen zu bewältigen.

ADSelfService Plus – Überblick

ManageEngine ADSelfService Plus ist eine Identitätssicherheitslösung, mit der IT-Administratoren ihren Anwendern einen sicheren und nahtlosen Zugriff auf Unternehmensressourcen ermöglichen können. Funktionen wie adaptive Multi-Faktor-Authentifizierung (MFA), bedingte Zugangskontrollen und passwortlose Authentifizierung helfen, Identitäten besser vor Angriffen zu schützen und das Zero-Trust-Prinzip umzusetzen.

Mit den integrierten Self-Service-Funktionen können Benutzer beispielsweise ihr Passwort selbst zurücksetzen oder das eigene Konto entsperren. Das reduziert passwortbezogene Helpdesk-Tickets, beschleunigt das Application Onboarding und entlastet so die IT-Abteilung. Darüber hinaus ermöglicht ADSelfService Plus den Anwendern dank AD-basiertem Single-Sign-On (SSO) einen sicheren Zugang zu Unternehmensanwendungen wie Microsoft 365, Salesforce und G Suite mit einem Klick.

Zudem bietet die Lösung detaillierte Audit-Reports und Admin-Funktionen, die sichere Passwörter und ein ebenso sicheres Passwort-Reset garantieren.

Highlights-Features

Adaptive Multi-Faktor-Authentifizierung (MFA)

- **MFA:** Schützen Sie den Zugriff auf Endpoints (Windows, macOS und Linux), VPNs, OWA und Unternehmensanwendungen mit MFA. Wählen Sie aus über 20 Methoden, darunter FIDO2-Authentifizierung, biometrische Faktoren, TOTP und Drittanbieter-Apps wie YubiKey Authenticator und Microsoft Authenticator.
- **Bedingter Zugriff (Conditional Access):** Automatisieren Sie die Zugriffskontrolle auf Unternehmensressourcen durch kontextbasierte Authentifizierung anhand von Details wie IP-Adresse, Zugriffszeit, Geolokalisierung und verwendetes Gerät.

Single-Sign-On (SSO)

- **Enterprise SSO:** Integrieren Sie Unternehmensanwendungen in Ihr AD, so dass Benutzer nur einmal ihre Anmeldedaten eingeben müssen, um bequem auf jede Anwendung zuzugreifen.
- **Passwortlose Anmeldung:** Verhindern Sie Angriffe, die auf Anmeldeinformationen basieren, indem Sie eine passwortlose Authentifizierung verwenden. Diese wird durch MFA für die Anmeldung bei Unternehmensanwendungen unterstützt.

Just-in-Time (JIT) Provisioning

- **SCIM-basierte Bereitstellung:** Automatisieren Sie die Bereitstellung neuer Benutzerkonten in den integrierten Anwendungen unmittelbar nach der Benutzeranmeldung. Dies rationalisiert und vereinfacht den Onboarding-Prozess.

Self-Service-Passwort-Management und Sicherheit

- **Passwort-Self-Service:** Ihre Anwender können Passwörter sicher selbst zurücksetzen und ihr Konto entsperren, ohne dass der Helpdesk eingreifen muss.
- **Passwort-Synchronisierung in Echtzeit:** Synchronisieren Sie AD-Passwörter in Echtzeit mit Unternehmensanwendungen und ermöglichen Sie es Ihren Anwendern, mit einem einzigen Passwort nahtlos zwischen verschiedenen Cloud-Diensten und lokalen Systemen zu wechseln.
- **Durchsetzung von Passwortrichtlinien:** Setzen Sie granulare Passwortrichtlinien auf OU- und Gruppenebene für verschiedene Benutzer in AD und anderen Unternehmensplattformen durch.

Remote-Arbeit ermöglichen

- **Aktualisierung der zwischengespeicherten Anmeldeinformationen (Cached Credentials):** Lassen Sie die im Geräte-Cache Ihrer Benutzer gespeicherten Anmeldeinformationen automatisch über VPN aktualisieren, sobald diese ihr Domänenpasswort ändern.
- **Webbasierte Änderung des Domänenpassworts:** Bieten Sie Remote-Mitarbeitern ein sicheres webbasiertes Portal, um Domänen- und Unternehmensanwendungs-Passwörter zu ändern.
- **Passwort- und Account-Ablaufbenachrichtigungen:** Erinnern Sie lokale und Remote-Benutzer per SMS, E-Mail oder Push-Benachrichtigung an das bevorstehende Ablaufdatum von Passwörtern und Accounts.

Workforce-Self-Service

- **Aktualisierung eigener AD-Attribute:** Halten Sie die Informationen im AD aktuell, indem Sie Ihren Anwendern die Möglichkeit geben, ihre eigenen Attribute im AD zu aktualisieren, z. B. E-Mail-Adresse, Handynummer und Foto.
- **Suche im Firmenverzeichnis:** Ermöglichen Sie Anwendern eine einfache Suche nach Benutzern, Kontakten oder Gruppen in Ihrem Unternehmen.
- **E-Mail-Gruppenverwaltung:** Definieren Sie Richtlinien für E-Mail-Gruppen. Auf diese Weise können sich Ihre Anwender bei Rollenänderungen selbstständig in ausgewählte Verteilergruppen ein- oder auszutragen, ohne dass der Helpdesk eingreifen muss.

Weitere Features

- **Vordefinierte Berichte:** Führen Sie Audit-Berichte aus, um Authentifizierungsversuche der Benutzer, Self-Service-Aktionen sowie den Passwort- und Kontostatus zu überprüfen.
- **Integrationen:** Erweitern Sie die Funktionen von ADSelfService Plus durch Integration mit SIEM-, ITSM- und IAM-Lösungen.
- **Mobiles Passwort-Management:** Nutzen Sie die ADSelfService-Plus-App für Android oder iOS, um von unterwegs aus Self-Service-Aktionen durchzuführen.

Testen Sie alle Funktionen von ADSelfService Plus
30 Tage lang KOSTENLOS!

Testversion herunterladen

Spezifikationen:

Prozessor: 2,4 GHz | RAM: 8 GB | Speicherplatz: 100 GB (SSD bevorzugt)
Unterstützte Plattformen: Windows Server 2000 und höher (inkl. Windows 2022), Windows 7 und höher, Windows Vista, Windows XP. Eine detaillierte Auflistung finden Sie in den Systemvoraussetzungen.
Unterstützte Browser: Internet Explorer 9 und höher; Firefox 4 und höher; Chrome 10 und höher; Microsoft Edge
Unterstützte Datenbanken: PostgreSQL (Standard) und MS SQL.

Ihr ManageEngine-Partner:

MicroNova AG
Unterfeldring 6, D-85256 Vierkirchen
Tel.: +49 8139 9300-456
E-Mail: sales-ManageEngine@micronova.de
Support: www.manageengine.de/support
www.manageengine.de/adselfserviceplus