Bringing IT together

Umfassende IT-Management-Software für
alle Anforderungen der IT-Abteilung

ManageEngine

ADSelfService Plus

ADSelfService Plus bietet Lösungen für:

Self-Service Passwort-Management

Self-Service-Funktionen zum Zurücksetzen von Passwörtern und Freischalten von Konten. Ablaufbenachrichtigung für Passwörter/Konten.

Endpoint-Sicherheit

Passwortrichtlinien durchsetzen und Endpoint-Multifaktor-Authentifizierung (MFA).

One Identity

Enterprise Single Sign-On (SSO) und Passwort-Synchronisierung in Echtzeit.

Jetzt herunterladen

Self-Service Passwort-Management
Highlights

1. **Self-Service Passwort-Management jederzeit und überall**: Ermöglichen Sie es Ihren Anwendern, ihre Passwörter selbst zurückzusetzen, ihre Konten selbst zu entsperren – im Büro, von Zuhause oder von unterwegs.

2. **Passwort-/Kontoablaufbenachrichtigung:** Automatisieren Sie Erinnerungen an Ihre Anwender zu in Kürze ablaufenden Passwörtern oder Accounts und versenden Sie diese per E-Mail, SMS oder Push-Benachrichtigung.

3. **Passwortänderung durchsetzen:** Zwingen Sie Anwender, deren Passwort von einem Helpdesk-Administrator zurückgesetzt wurde, ihr Passwort bei der nächsten Anmeldung zu ändern.

Endpoint-Sicherheit
Highlights

1. **Endpoint-MFA:** Sichern Sie Endpoint-Anmeldungen (Windows, Linux und macOS) mit aktuellen MFA-Verfahren wie biometrischen Faktoren oder QR-Codes ab, bevor Sie lokalen oder Remote-Zugriff auf Netzwerkressourcen gewähren.

2. **Individuell Passwortrichtlinien:** Stellen Sie mit den erweiterten Einstellungen für die Passwortrichtlinien sicher, dass starke Passwörter bei allen geschäftlichen Konten verwendet werden.

3. **Compliance mit gesetzlichen Vorgaben:** ADSelfService Plus unterstützt Sie bei der Einhaltung von Regelwerken und Vorgaben wie NIST SP 800-63B, FFIEC, HIPPA und DSGVO

One Identity
Highlights

1. **Enterprise Single Sign-on (SSO):** Ermöglichen Sie Anwendern Zugriff auf mehrere Unternehmensanwendungen mit einer einzigen Identität.

2. **Passwort-Synchronisation in Echtzeit:** Synchronisieren Sie zurückgesetzte oder geänderte Active-Directory-Passwörter in Echtzeit mit verbundenen Unternehmensanwendungen.

ManageEngine
ADSelfService Plus

Weitere Highlights

1. **Verzeichnis-Aktualisierung als Self-Service:** Ermöglichen Sie es Ihren Anwendern, die eigenen Profilinformationen wie Telefonnummer, E-Mail-Adresse etc. im AD zu aktualisieren.

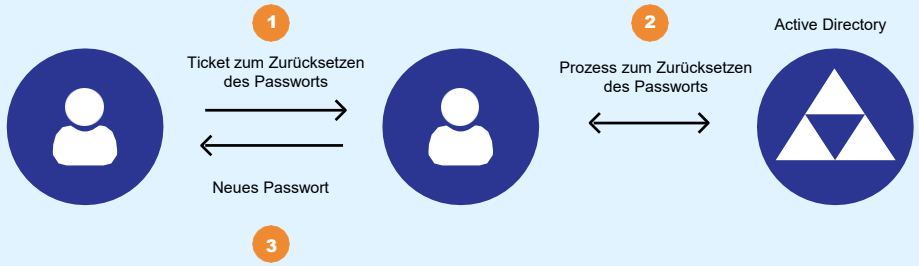
2. **Abonnement von E-Mail-Gruppen:** Ermöglichen Sie es Ihren Anwendern, sich selbst für Verteilergruppen an- und abzumelden.

3. **Suche im Mitarbeiterverzeichnis und Organigramm:** ADSelfService Plus ermöglicht Administratoren, eine vollständige Liste aller Mitarbeiter inklusive deren Position in der Organisationshierarchie abzurufen.

ManageEngine
ADSelfService Plus

Wie können Administratoren die immer wiederkehrenden Tickets zu vergessenen Passwörtern abschaffen?

Vor ADSelfService Plus



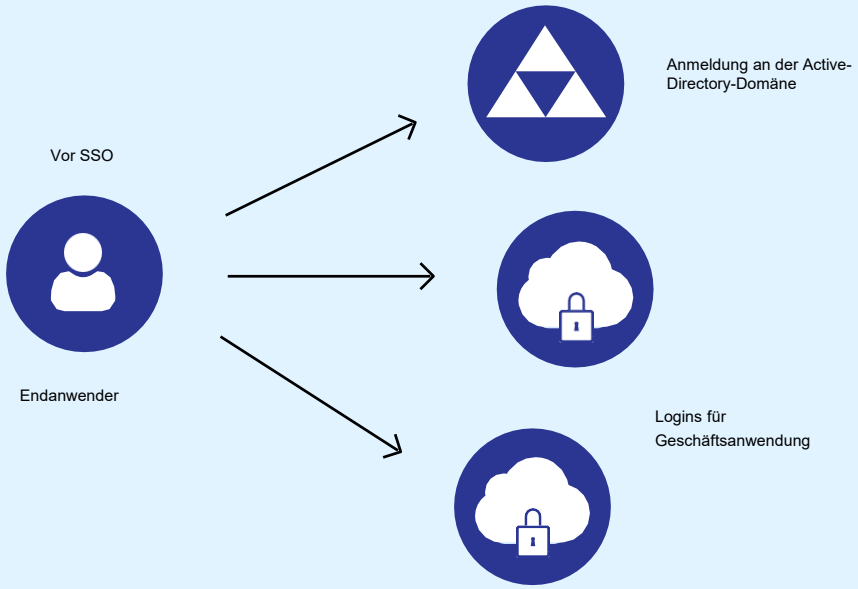
1. Ein Benutzer vergisst sein AD-Domänen-Passwort und erstellt ein Ticket, um das Passwort zurücksetzen zu lassen.
2. Das Helpdesk-Team überprüft die Identität des Benutzers durch Abfrage der Mitarbeiter-ID.
3. Der Mitarbeiter wartet, bis sein AD-Passwort vom IT-Team zurückgesetzt wurde.
4. Der Benutzer erhält das neue Passwort.

Mit ADSelfService Plus

1. Ein Benutzer vergisst sein AD-Domänen-Passwort.
2. Der Benutzer ruft das ADSelfService-Plus-Portal über den Anmelde-Bildschirm seines Rechners, über einen Webbrowser oder über sein Smartphone auf und setzt sein Passwort einfach selbst zurück, ohne auf das IT-Team warten zu müssen.

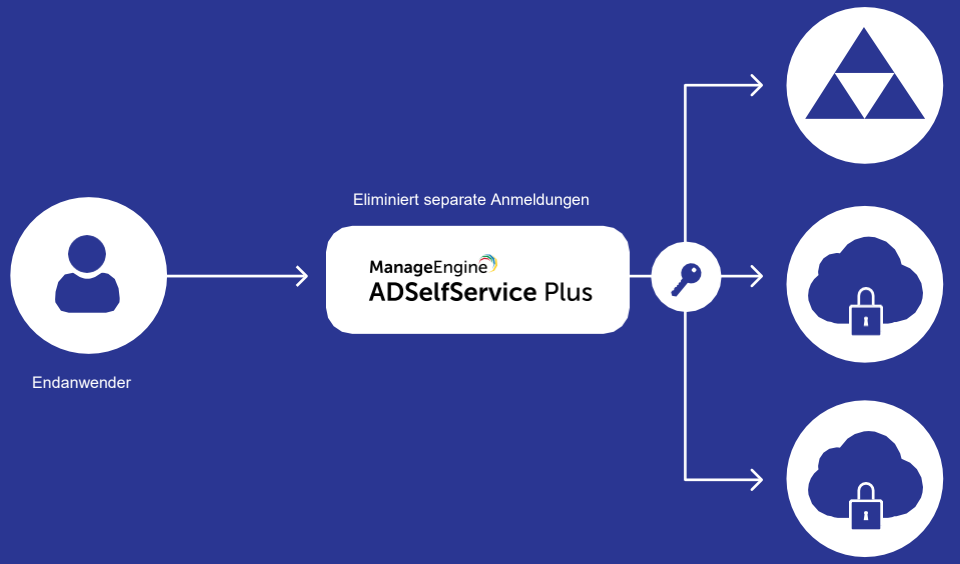
ManageEngine
ADSelfService Plus

Vor Einführung von Single Sign-on (SSO)



Anwender muss sich mehrere Passwörter merken, um auf die verschiedenen Anwendungen zuzugreifen.

Nach Einführung von Single Sign-on (SSO)



Anwender kann Active-Directory-basiertes Single Sign-on (SSO) für alle SAML-2.0-fähige Anwendungen nutzen.

ManageEngine
ADSelfService Plus

Verwenden Sie zentralisierte, maßgeschneiderte Passwortrichtlinien für lokale und Cloud-Anwendungen.

- **Zeichen einschränken**

  Beschränken Sie den Einsatz von Sonderzeichen, Ziffern und Unicode-Zeichen, die Benutzer verwenden können.

- **Muster verhindern**

  Verhindern Sie die Nutzung von Tastaturzeichenfolgen (wie „asdf“), in Wörterbüchern vorkommende Wörter und Palindrome.

- **Passphrasen verwenden**

  Option zum Einsatz von Passphrasen, die nicht den Komplexitätsvorgaben entsprechen, wenn die Passwortlänge ein vorgegebenes Limit (z. B. 20 Zeichen) überschreitet.

- **Wiederholungen unterbinden**

  Erzwingen Sie eine Überprüfung des Passwortverlaufs beim Zurücksetzen des Passworts und beschränken Sie die Wiederholung bestimmter Zeichen oder des Benutzernamens als Passwort (z. B. „aaaaa“ oder „benutzer01“).

- **Länge beschränken**

  Legen Sie die minimale und maximale Passwortlänge fest.

- **Passwortstärke prüfen**

  Zeigen Sie die Anforderungen für Passwörter auf den Seiten zum Zurücksetzen und Ändern des Passworts an.

Verbessern Sie die Sicherheitslage Ihres Unternehmens mit sicheren Benutzerpasswörtern.

Stellen Sie sicher, dass sich alle Anwender für den Passwort-Self-Service registrieren.

1. Fordern Sie die Anwender per E-Mail und Push-Benachrichtigungen auf, sich für den Passwort-Self-Service zu registrieren.

2. Zwingen Sie die Benutzer, sich zu registrieren, wenn sie sich an ihrem Computer mit einem dauerhaften Desktop-Pop-up anmelden.

3. Melden Sie Benutzer automatisch an, indem Sie Anmeldedaten aus CSV-Dateien oder externen Datenbanken importieren.

ManageEngine
ADSelfService Plus

Berichterstellung mit ADSelfService Plus

1. Berichte zum Ablauf von Passwörtern, zu gesperrten Benutzern und mehr

2. Audit-Berichte über alle Benutzer- und Administratoraktionen.

3. Exportieren, Anpassen und Planen Sie Berichte, die per E-Mail zugesendet werden.

Multi-Faktor-Authentifizierung

ManageEngine
ADSelfService Plus

ADSelfService Plus unterstützt mehrstufige Authentifizierungsverfahren für:

Endpoint-Anmeldungen

Funktionen zum Zurücksetzen des Passworts und Entsperren des eigenen Accounts

Anwendungszugriff

Unterstützte Authentifikationsmethoden:

1. Sicherheitsfragen und Antworten
2. Bestätigungs-Codes per SMS oder E-Mail
3. Google Authenticator
4. Duo Security
5. RSA SecurID
6. RADIUS
7. Push-Benachrichtigungen
8. Authentifizierung per Fingerabdruck
9. QR-Code-basierte Authentifizierung
10. Zeitbasierte Einmalpasswörter (TOTP)
11. AD-basierte Sicherheitsfragen
12. Microsoft Authenticator
13. YubiKey Authenticator

ManageEngine
ADSelfService Plus

Endpoint-MFA für Windows-/Linux-/macOS-Anmeldungen

Schritt 1:

Benutzer geben ihre Domänen-Anmeldedaten als erste Authentifizierungsebene für ihren Computer ein.

Schritt 2:

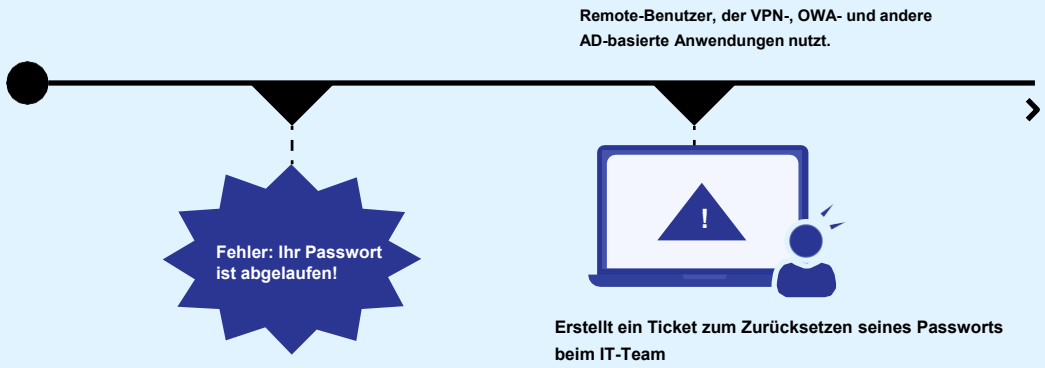
Benutzer müssen ihre Identität zusätzlich mit einer der unterstützten Authentifizierungsmethoden bestätigen, z. B. mit einem zeitbasierten Authentifizierungs-Code, der ihnen per SMS oder E-Mail zugesendet wird, oder über einen Authentifizierungs-Drittanbieter wie Google Authenticator oder RSA SecurID.

Schritt 3:

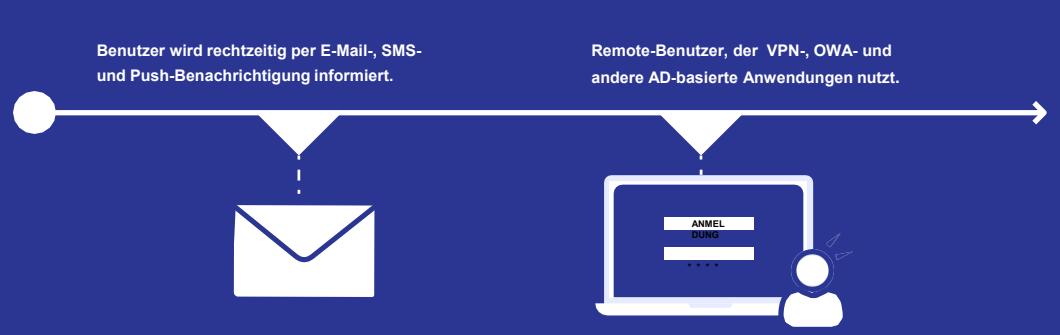
Nach erfolgreicher Authentifizierung wird der Benutzer an seinem Windows-, Linux- oder macOS-Rechner angemeldet.

Unterstützen Sie Ihre Anwender durch rechtzeitig zugesendete Benachrichtigungen zu in Kürze ablaufenden Passwörtern.

ManageEngine
ADSelfService Plus



1. Folgende Gründe führen dazu, dass Benutzer ihre Passwörter ablaufen lassen:
2. Sie benutzen AD-Konten nur für VPN oder OWA und melden sich daher nie aktiv an, wodurch sie die Windows-Benachrichtigungen verpassen.
3. Sie übersehen die Warnung zum Passwortablauf in der Task-Leiste.
4. Sie arbeiten auf Rechnern ohne Windows und erhalten daher keine Warnung, dass ihr AD-Passwort abläuft.
5. Also wenden sie sich an das IT-Team, um ihr Passwort zurücksetzen zu lassen.



1. ADSelfService Plus informiert Benutzer automatisch über in Kürze ablaufende Passwörter.
2. Administratoren können vor Ablauf des Passworts, täglich, wöchentlich oder zu benutzerdefinierten Zeitpunkten Erinnerungen an die Anwender versenden.

Die wichtigsten Vorteile von ADSelfService Plus auf einen Blick

Geringere Kosten

1. Eliminiert den häufigsten Grund für Anrufe beim Helpdesk.
2. Ermöglicht es IT-Administratoren und Helpdesk-Technikern, sich auf andere wichtige Aufgaben zu konzentrieren.

Mehr IT-Sicherheit

1. Setzen Sie starke Passwortrichtlinien durch.
2. Ermöglichen Sie eine Multi-Faktor-Authentifizierung für Cloud-Anwendungen.
3. Gewähren Sie rollenbasierten Zugriff auf Anwendungen und Self-Service-Funktionen.

Besseres Anwendererlebnis

1. Keine Wartezeiten!
2. Zugriff von überall aus möglich!
3. Anmeldung ohne Frustration!
4. Schluss mit Passwort-Müdigkeit!

Wie unterstützt ADSelfService Plus im **Bildungs-, Finanz- und Gesundheitsbereich?**

ManageEngine ADSelfService Plus

Bildungsbereich

Studierenden und Mitarbeitern können:

1. Passwörter über ihren Anmelde-Bildschirm zurücksetzen – auch von zuhause.
2. persönliche Daten selbst aktualisieren.
3. mehrere Anwendungen über eine einzige Konsole aufrufen.

Finanzbereich

1. Mitarbeiter können die Passwort-Self-Service-Funktionen nutzen, Zugriff auf erforderliche Ressourcen erhalten, mit starken Passwörtern arbeiten – und mehr.
2. Compliance mit Vorgaben wie SOX[1], GLBA[2] und PCI DSS[3].

Gesundheitsbereich

1. Ärzte und Krankenhauspersonal können die Passwort-Self-Service-Funktionen, mit Single Sign-on sicher auf EHR[4] zugreifen, aktuelle Profile sicherstellen, ePHI[5]-Daten mit spezifischen Passwortrichtlinien absichern – und mehr.
2. Unterstützt bei der Einhaltung von HIPAA[6]-Vorgaben.

1. SOX: Sarbanes-Oxley Act
2. GLBA: Gramm-Leach-Bliley Act
3. PCI DSS: Payment Card Industry Data Security (Datensicherheit bei Kreditkartentransaktionen)
4. EHR: Electronic Health Records (elektronische Krankenakten)
5. ePHI: Electronic Protected Health Information (elektronisch geschützte Gesundheitsdaten)
6. HIPAA: Health Insurance Portability and Accountability Act (Sicherheit und Datenschutz im Zusammenhang mit geschützten Patientendaten)

ManageEngine
ADSelfService Plus

Kundenreferenzen

ManageEngine
ADSelfService Plus

TriMark setzt auf ADSelfService Plus, um Passwort-Probleme zu lösen.

Branche: Lebensmittelbranche. Standort: USA

Zitat:

„When our employees needed a password reset while they were outside the organization, ADSelfService Plus helped us by allowing them to reset their passwords remotely. It was beneficial for us“ – Roger DeVivo, Senior System Administrator bei TriMark.

Anforderungen des Unternehmens:

- Benutzern ermöglichen, ihre Passwörter ohne Unterstützung der IT-Abteilung zurückzusetzen, auch wenn sie nicht mit dem Firmennetzwerk verbunden sind.

- Da zwischen den AD-Domänen keine vertrauenswürdigen Verbindungen eingerichtet waren, kam es zu Passwort-Müdigkeit. Die neue Lösung sollte daher in der Lage sein, Passwörter über alle Benutzerkonten hinweg zu synchronisieren.

Wie unterstützt ADSelfService Plus?

ADSelfService Plus hilft Remote-Mitarbeitern, ihre Passwörter zurückzusetzen, und aktualisiert die Zugangsdaten anschließend auf den Rechnern der jeweiligen Benutzer.

Durch die Passwort-Synchronisierungs-Funktion von ADSelfService Plus konnte TriMark alle Passwortänderungen zwischen mehreren Active-Directory-Domänen automatisch synchronisieren.

ADSelfService Plus unterstützte die Administratoren bei der Planung von Passwort-Ablaufwarnungen per SMS, E-Mail und Push-Benachrichtigungen, so dass Benutzer ihre in Kürze ablaufenden Passwörter rechtzeitig ändern können.

Zitat:

„The support team helped me pretty quickly every time I called in, and I'd say I'm happy with the support!"

ManageEngine
ADSelfService Plus

Lizenzen und Preise

Details	Testversion	Kostenlose Version	Standard- und Profi-Editionen
Gültigkeitsdauer	30 Tage	Kein Ablaufdatum	Gemäß Lizenzbedingungen
Anzahl Domänen	Unbegrenzt viele Domänen	Unbegrenzt viele Domänen	Gemäß Lizenzbedingungen
Anzahl Domänen-benutzer	Unbegrenzt viele Benutzer	50 Benutzer	Gemäß Lizenzbedingungen
Features	Uneingeschränkte Funktionen	Uneingeschränkte Funktionen	Gemäß Lizenzbedingungen
24/5 Kundensupport	✓	✓	✓

Jetzt herunterladen

Unternehmen, die auf uns vertrauen:

Kontakt

Telefon

+49 8139 9300-456

LiveChat

für sofortige Antworten

E-Mail

Sales-ManageEngine@micronova.de

Besuchen Sie unsere Website

www.manageengine.de/adauditplus

Jetzt herunterladen