



DATENBLATT

# Password Manager On Demand

SaaS-Bereitstellung für eine optimale Benutzererfahrung,  
niedrigere Supportkosten und höhere Sicherheit

## Vorteile

- Umfassende Kennwortverwaltungsfunktionen mit On-Demand-Bereitstellung
- Geringerer Aufwand für Helpdesk und IT-Personal bei der routinemäßigen Kennwortverwaltung
- Deutliche Reduzierung der Ausfallzeiten
- Sofortige Investitionsrendite
- Höhere Zufriedenheit bei Benutzern und IT-Personal aufgrund der einfachen Handhabung und Bereitstellung
- Höhere Netzwerksicherheit
- Synchronisierung von Kennwörtern zwischen unterschiedlichen Systemen
- Höhere Sicherheit dank Integration mit Multi-Faktor-Authentifizierung über Defender

## Überblick

Bei den meisten Helpdesk-Anfragen geht es um die Zurücksetzung von Kennwörtern. Da Organisationen auch zunehmend darum bemüht sind, strengere Sicherheitsrichtlinien zu implementieren, wird die Kennwortverwaltung immer aufwendiger. Benutzer müssen sich immer komplexere Kennwörter ausdenken und diese Kennwörter immer öfter ändern. Die Wahrscheinlichkeit, dass sie ihre Kennwörter vergessen und Support anfordern müssen, steigt damit drastisch. Organisationen, die mehrere unterschiedliche Systeme und Anwendungen per Kennwort sichern, haben ein noch größeres Problem. Sie müssen nun entscheiden, ob sie lieber die Sicherheit steigern oder die Kosten für den Benutzersupport reduzieren wollen.

Password Manager On Demand ist eine einfache und sichere Selfservice-Lösung, mit der Benutzer selbstständig vergessene Kennwörter zurücksetzen und ihre Konten entsperren können. Mit dieser Lösung können Administratoren strengere Kennwortrichtlinien implementieren und dadurch gleichzeitig den Helpdesk entlasten. Unternehmen müssen dadurch nicht länger Kompromisse bei der Sicherheit machen, um Kosten einzusparen.

## Funktionen und Merkmale

### Verbesserte Sicherheit

Mit Password Manager On Demand können Organisationen sicherere Datenzugriffsrichtlinien implementieren, die über die nativen Steuerungsfunktionen von Microsoft® Active Directory® hinausgehen. Dank dieser Lösung wird die Sicherheit verbessert, da Helpdesk-Fehler vermieden werden, Benutzer keine Kennwörter mehr aufschreiben müssen und das Erraten von Kennwörtern sowie unerlaubte Zugriffe erschwert werden. Die integrierte Datenverschlüsselung erlaubt globalen Zugriff bei gleichbleibend hoher Datensicherheit.

### Sicherstellung des Returns on Investment dank Benutzereinbindung

Mit Password Manager On Demand können Benutzer die einfachsten Kennwortverwaltungsaufgaben selbst übernehmen. Dies schont das IT-Budget und führt zu einem schnellen Return on Investment.

### Eine Investition, die sich lohnt

Password Manager On Demand ist eine langfristige Lösung für ein immer akuter werdendes Problem. Die Investition in diese Lösung ist für alle Unternehmen sinnvoll, die eine höhere betriebliche Effizienz der IT und mehr Sicherheit erreichen möchten.

- Kosteneffektivität dank Nutzung der vorhandenen Active Directory-Infrastruktur: Mit Password Manager On Demand können Sie Ihre bestehende Active Directory-Infrastruktur noch besser nutzen. Sie können die Lösung außerdem schnell

bereitstellen und einen sofortigen Return on Investment erzielen. Darüber hinaus bietet sie eine präzisere gruppenbasierte Kennwortrichtlinie als Windows Server.

- Weniger Aufwand und Kosten für den Helpdesk und höhere Benutzerproduktivität: Mit Password Manager On Demand können Benutzer ihre Kennwörter selbst zurücksetzen und eigene Konten entsperren, ohne sich mit dem Helpdesk oder Administrator in Verbindung setzen zu müssen.
- On-Demand-Benutzerhilfe: Password Manager On Demand bietet Online-Erläuterungen zur Kennwortrichtlinie. Darüber hinaus werden die Benutzer automatisch benachrichtigt, wenn ein Kennwort die vorgegebenen Anforderungen nicht erfüllt, und sie können konforme Kennwörter generieren, ohne den Helpdesk zu bemühen.
- GINA-Erweiterungen für das Windows Anmeldedialogfeld: Um den Benutzern das Zurücksetzen von Kennwörtern zu erleichtern, können Administratoren im Windows Anmeldedialogfeld eine Schaltfläche hinzufügen, mit der Kennwörter vor der Anmeldung zurückgesetzt werden können. Dadurch entfällt die Konfiguration von öffentlichen Kiosks oder kostspieligen telefonbasierten Systemen.

## Durchsetzung von Unternehmensstandards

Password Manager On Demand unterstützt mehr organisatorische Richtlinien und Datensicherheitsstandards als jede andere Lösung.

- Strenge Richtlinienerzwingung: Password Manager On Demand setzt vom Administrator definierte Standards durch, protokolliert misslungene Authentifizierungsversuche und sperrt die entsprechenden Konten bei Bedarf.
- Zwingende Registrierung: Password Manager On Demand bietet eine Reihe von Mechanismen, um sicherzustellen, dass sich Benutzer registrieren und die Software auch verwenden, was deren Effektivität sicherstellt.
- Zuverlässige Authentifizierung: Die persönlichen Profile für Benutzer enthalten Fragen mit eindeutigen Antworten, die sich Benutzer gut merken, Unbefugte aber nicht leicht erraten können. Darüber hinaus kann Password Manager On Demand in Defender integriert werden, um eine sicherere Authentifizierung per Einmalkennwort zu implementieren – wahlweise in Kombination mit dem Frage-Antwort-Profil oder als Ersatz desselben.

- Sicherheit und Einfachheit: Password Manager On Demand kann nahtlos in Windows integriert und von Benutzern aus mehreren Domänen mit oder ohne Vertrauensstellungen genutzt werden. Eine starke Datenverschlüsselung und sichere Datenübertragung werden durch Unterstützung für führende Sicherheitstechnologien wie Microsoft CryptoAPI und SHA-256 sichergestellt.

## Überwachung der Systemaktivität

Password Manager On Demand stellt robuste Protokollierungs- und Berichterstellungsfunktionen für Administratoren bereit und erleichtert diesen die Überwachung der Systemaktivität und die Korrektur von Anomalien.

## Unterstützung von Initiativen zur Identitätsverwaltung

Password Manager On Demand verfügt über eine reaktionsschnelle Weboberfläche und bietet Kennwortverwaltung für alle mit Microsoft Identity Integration Server (MIIS) verbundenen Systeme. Die Lösung kann außerdem für nicht von Microsoft stammende Betriebssysteme wie Unix und Linux eingesetzt werden, und zwar durch Authentication Services; die Ergänzung von Zwei-Faktor-Authentifizierung über Defender.

## One Identity-Hybrid-Abonnement

Erweitern Sie die Möglichkeiten von Password Manager On Demand mit dem One Identity-Hybrid-Abonnement, das Ihnen zusätzliche, über die Cloud bereitgestellte Funktionen und Dienste bietet. Erhalten Sie Zugriff auf unbegrenzte Starling Two-Factor Authentication, um den Zugriff von Administratoren und Endbenutzern mit Password Manager On Demand zu schützen, der das Add-on zur telefonischen Verifizierung ersetzt. Ein einziges Abonnement ermöglicht die Bereitstellung aller One Identity-Lösungen.

## Nach ISO 27001 zertifiziert

One Identity ist ein Unternehmen von Quest und ein führender globaler Anbieter von identitätsbasierten Sicherheitslösungen. Seine Cloud-Infrastruktur und -Prozesse sind gemäß der internationalen Norm ISO/IEC 27001 zertifiziert, die Best Practices für Systeme zum Informationssicherheitsmanagement vorgibt.

## Infos über One Identity

Das Quest Software-Unternehmen One Identity ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breiten und integrierten Portfolios mit Angeboten zur Identitätsverwaltung einschließlich Kontoverwaltung, Identitätsgovernance und -verwaltung sowie Verwaltung privilegierten Zugriffs haben Unternehmen mehr Macht, ihr volles Potential zu erreichen, wo Sicherheit dadurch erreicht wird, dass Identitäten im Kern des Programms platziert werden, so dass für alle Benutzertypen, Systeme und Daten der richtige Zugriff gewährt wird. Weitere Informationen erhalten Sie unter [OneIdentity.com](https://www.oneidentity.com).