DATENBLATT

Privileged Password Manager

Mit unserem Safe für privilegierte Kennwörter können Sie gemeinsam genutzte und privilegierte Anmeldedaten effektiv sichern.

Vorteile

- Kennwortverwaltung für gemeinsam genutzte, privilegierte und geschäftskritische Konten in Einklang mit allen Compliance-Vorgaben
- Individuelle Zurechenbarkeit von Zugriffen auf gemeinsam genutzte Konten
- Einfache Bereitstellung als sichere, skalierbare und maßgeschneiderte Appliance
- Automatische Erkennung für eine schnelle Integration von neuen Benutzern, Konten und Systemen in den Verwaltungsprozess
- Einfache Erweiterung um Funktionen für Sitzungsüberwachung und -aufzeichnung sowie Befehlskontrolle

Systemanforderungen

Eine vollständige Liste der Systemanforderungen finden Sie unter oneidentity.com/privileged-password-manager.

Die Verwaltung von Anmeldedaten für Konten mit erweiterten Zugriffsrechten oder gemeinsam genutzte Konten ist eine der größten Herausforderungen, denen sich komplexe heterogene Unternehmen heute stellen müssen. Einerseits müssen Administratoren beim Zugriff auf die von ihnen verwalteten Systeme alle die Berechtigungen besitzen, die sie für ihre Arbeit benötigen. Andererseits jedoch müssen Organisationen auch sicherstellen, dass dadurch keine Sicherheitsrisiken entstehen oder gesetzliche Vorschriften missachtet werden.

Mit Privileged Password Manager können Sie den gesamten Prozess der Erteilung von Administratoranmeldedaten automatisieren, steuern und absichern. Das Tool ist eine Schlüsselkomponente der One Identity Lösungen für die Verwaltung privilegierter Konten und wird auf einer sicheren, gehärteten Appliance bereitgestellt.

Privileged Password Manager gewährleistet, dass die Zugriffsrechte für Administratoren nur auf Grundlage der vom Unternehmen festgelegten Richtlinien und nur mit entsprechender Genehmigung gewährt werden. Die Lösung stellt außerdem sicher, dass alle Aktionen vollständig überwacht und nachverfolgt werden und Kennwörter sofort nach ihrer Rückgabe geändert werden.

ONE IDENTITY™

Keine Sicherheitslücke mehr bei Anwendungskennwörtern

Geht es um die Sicherheit, wird eine der kritischsten Schwachstellen häufig übersehen: die integrierten Kennwörter, die für die Kommunikation zwischen verschiedenen Anwendungen und zwischen Anwendungen und Datenbanken benötigt werden. Diese Kennwörter sind oft mittels einfacher CLI-Aufrufe (Command Line Interface, Befehlsschnittstelle) oder API-Aufrufe (Application Programming Interface, Anwendungsprogrammierschnittstelle) in Skripten, Prozessen und Programmen hartcodiert. Privileged Password Manager ersetzt hartcodierte Kennwörter durch programmgesteuerte Aufrufe, die Kontoanmeldedaten dynamisch abrufen.

Funktionen

Freigabesteuerung: Mit Privileged Password Manager können Sie Kennwortanforderungen von autorisierten Benutzern, Programmen und Skripten für Konten, für die sie eine Zugriffsberechtigung haben, effizient verwalten. Hierfür steht Ihnen eine sichere Webbrowserverbindung zur Verfügung, die auch mobile Geräte unterstützt. Die Kennwortanforderungen können entweder automatisch oder manuell genehmigt werden. Für die manuelle Genehmigung können Sie beliebige Genehmigungsstufen definieren.

Änderungskontrolle: Die Lösung ermöglicht außerdem eine konfigurierbare, granulare Änderungskontrolle für gemeinsam genutzte Anmeldedaten. Dabei erlaubt sie unter anderem die Aufschlüsselung nach Zeitpunkt und letzter Verwendung und kann zwischen manuellen und erzwungenen Änderungen unterscheiden.

Automatische Erkennung von:

- **Konten und Systemen:** Neue Konten und Systeme werden sofort erkannt und in den Verwaltungsprozess integriert. Auf Wunsch kann Sie Privileged Password Manager darüber benachrichtigen.
- **Benutzern:** Unsere Lösung kann Ihre LDAP (Lightweight Directory Access Protocol) oder Ihre Microsoft® Active Directory® Umgebung

Unterstützung für Anwendungskennwörter: Kennwörter, die in Skripten, Prozessen und Programmen hartcodiert sind, werden ersetzt:

- **Programmgesteuerter Zugriff:** Privileged Password Manager bringt sowohl eine Befehlsschnittstelle als auch eine API mit, die beide C++, Java, .NET und Perl unterstützen. Die Verbindung erfolgt über SSH mit einem Austausch von DSS-Schlüsseln.
- **Rollenbasierter Zugriff:** Sowohl die CLI als auch die API unterstützen rollenbasierten Zugriff. CLI oder API fungieren dabei als "programmgesteuerter" Benutzer, dem Sie entweder grundlegende Zugriffsrechte oder Administratorzugriffsrechte gewähren. Mit grundlegenden Zugriffsrechten können die CLI oder die API Kontokennwörter anfordern und auf autorisierte Ziele oder Konten zugreifen. Zugriffsrechte auf dieser Ebene sind zum Beispiel für einen Anforderer (auch Requestor genannt) angemessen. Mit Administratorzugriffsrechten können CLI und API administrative Aufgaben durchführen.
- **Optimale Leistung:** Privileged Password Manager kann nativ circa 100 Aufrufanforderungen pro Minute ausführen. Für Ihre anspruchsvollsten Anwendungen, die höhere Leistung benötigen, ermöglicht ein optionaler Cache mehr als 1.000 Kennwortanforderungen pro Sekunde.
- **Umfassender Befehlssatz:** Unser Tool bietet einen umfassenden Satz an Befehlen, die über die CLI oder die API ausgeführt werden können. Neben simplen Befehlen für die Kennwortanforderung stehen Ihnen auch Befehle auf Administratorebene zur Verfügung, die für eine enge Integration mit bereits im Unternehmen vorhandenen Tools und Workflows sorgen.

Sofortige Integration in die Unternehmensinfrastruktur: Privileged Password Manager lässt sich problemlos mit bestehenden Verzeichnissen, Ticketsystemen und Benutzerauthentifizierungsquellen integrieren, darunter Active Directory und LDAP. Zudem bietet die Lösung vollständige Unterstützung für Zwei-Faktor-Authentifizierung über Defender™ von One Identity oder andere Drittanbieterprodukte. Dank stabiler CLI und API ist die Integration mit vorhandenen Tools und in bestehende Arbeitsabläufe unkompliziert – auch in Eskalierungs-Workflows und Prozesse zur Benachrichtigung von Genehmigern.

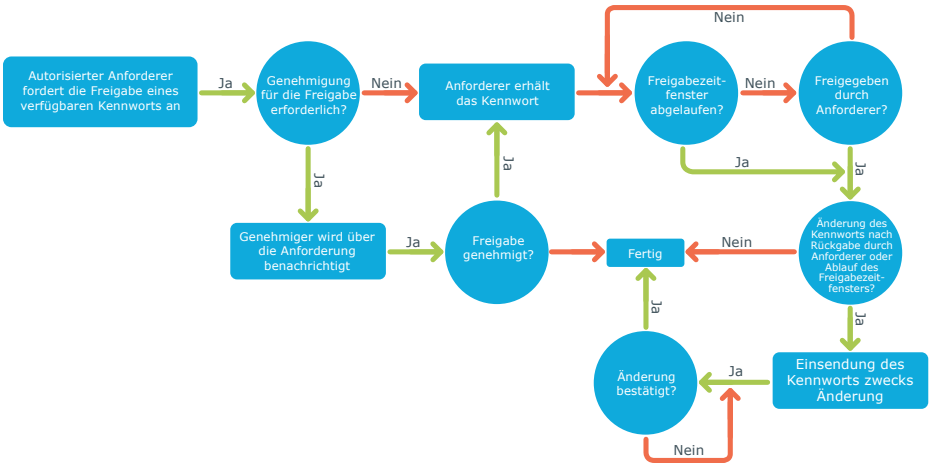
Sichere Appliance: Die Appliance hat weder einen Konsolen-Port noch eine Konsolenoberfläche. Der Zugriff ist nur über eine sichere, rollenbasierte Webschnittstelle möglich. Damit ist sie vor Host-Admin-Angriffen sowie vor Änderungen auf Betriebssystem-, Datenbank- oder Systemebene geschützt. Zusätzlich verfügt sie über eine interne Firewall, die externe netzwerkbasierte Angriffe abwehrt und zusätzliche Überwachungsfunktionen bereitstellt.

Skalierbare Appliance: Die Appliance ist sofort bei Lieferung einsatzbereit. So können Sie den Zugriff auf gemeinsam genutzte Anmeldedaten ebenso wie deren Verwaltung effektiv sichern, und das für mehr als 250.000 Konten gleichzeitig.

Sichere Kennwortspeicherung: Alle in Privileged Password Manager gespeicherten Kennwörter werden per AES-256-Bit-Verschlüsselung verschlüsselt. Darüber hinaus bietet die Appliance dank BitLocker™ Laufwerkverschlüsselung vollständige Festplattenverschlüsselung.

Stabile Unterstützung für verschiedenste Ziele: Privileged Password Manager ermöglicht die Verwaltung von gemeinsam genutzten Anmeldedaten auf unzähligen Typen von Zielservern, Netzwerkgeräten und Anwendungen.

Unterstützung für Handheld-Geräte: Kennwörter können auch über Handheld-Geräte angefordert, genehmigt und abgerufen werden. Sie können selbst festlegen, welche Benutzer dies dürfen und welche nicht.



Mit Privileged Password Manager können Sie die Genehmigung von Kennwortanforderungen vollständig automatisieren oder eine oder mehrere Genehmigungsstufen definieren.

Weitere Informationen

Weitere Informationen über Privileged Password Manager finden Sie unter oneidentity.com/privileged-password-manager.

Datasheet-PrivPassManager-US-DE-WL-JM

ONE IDENTITY™