HID DigitalPersona® SSO für Microsoft® Office 365

Starke Multi-Faktor-Authentifizierung

STELLEN SIE SICH EINE WELT VOR

In der...

Passwörter fast unmöglich zu knacken sind

Menschen ihre Anmeldedaten nicht weitergeben können

Anwender nicht vorgeben können, jemand anderer zu sein

In der Authentifizierung...

sicherer, umfassender, weniger fehleranfällig, anpassbarer

...ist.

Diese Welt gibt es schon.

Willkommen bei DigitalPersona®

Einführung

Der Schutz der IT-Umgebung vor Datenlecks und anderen unbefugten Zugriffen ist in den meisten Organisationen zur Chefsache geworden. In diesem Solution Brief betrachten wir die Herausforderungen, die mit der Implementierung einer starken Authentifizierung verbunden sind. Das Hauptaugenmerk wird auf der Multi-Faktor-Authentifizierung für Microsoft® Office 365™ und deren Einfluss auf die Organisation liegen. Wir stellen außerdem eine vielversprechende neue Lösung für das Multi-Faktor-Problem vor – DigitalPersona® Single Sign-On für Microsoft® Office 365™.

Die Herausforderung

Aufgrund der anhaltenden Sicherheitsverletzungen durch kompromittierte statische Passwörter, suchen Unternehmen sowie staatliche und akademische Einrichtungen aktiv nach Alternativen zur Authentifizierung. Als Reaktion darauf drängt eine Vielzahl an neuen Ansätzen auf den Markt – darunter 2-Faktor-Authentifizierung (2FA), Multi-Faktor-Authentifizierung (MFA), biometrische, kontext- und verhaltensbasierte Lösungen.

Dennoch haben die meisten Organisationen bisher keinen angemessenen Ersatz gefunden. Sie nutzen trotz der bekannten Unzulänglichkeiten weiterhin Passwörter. Es gibt viele Gründe, warum sich die Authentifizierung in der Praxis nicht schneller weiterentwickelt hat. Zu den häufigsten Hindernissen bei der Einführung einer starken Authentifizierung zählen:

Eingeschränkte Authentifizierungsmethoden

Die meisten Lösungen für 2-Faktor- und Multi-Faktor-Authentifizierung nutzen weiterhin ein Passwort als einen der Faktoren. Bedenkt man die Unsicherheit von Passwörtern, deren unbequeme Nutzung für Endanwender und die Kosten, die durch das Zurücksetzen von Passwörtern generiert werden, wird deutlich, dass Authentifizierungslösungen, die Passwörter einsetzen, nur einen kleinen Fortschritt darstellen. Einen schwachen Faktor mit einem starken zu ergänzen erhöht die Sicherheit nicht wesentlich.

Zusätzlich verhindert die Festlegung auf nur zwei statische Faktoren die Berücksichtigung des individuellen Risikos durch die Security Policies im Authentifizierungsprozess. Nicht jede Authentifizierung ist dem gleichen Risiko ausgesetzt. Deshalb benötigen sie auch jeweils ein individuelles Niveau der Identitätsfeststellung. Damit das Risiko während der Authentifizierung berücksichtigt werden kann, muss es anhand des Kontextes bestimmt werden, beispielsweise unter Betrachtung des Verhaltens, der Uhrzeit, des geographischen Ortes, der Netzwerkadresse und des Geräts.

Leider beziehen nur wenige Authentifizierungslösungen den Kontext oder das Verhalten mit ein, und selbst wenn sie es tun, gibt es nicht genügend Faktoren, um die Sicherheit der Authentifizierung bei risikoreichen Transaktionen zu erhöhen.

Schließlich haben verschiedene Branchen und Organisationen jeweils eigene Security-Anforderungen und unterliegen unterschiedlichen Compliance-Vorschriften. In Behörden kann die Nutzung von Smart Cards und biometrischen Faktoren gefordert sein; andere Organisationen schreiben möglicherweise den Einsatz eines Hardware-Tokens vor.

Bedenken Sie zudem, dass ein Anwender einen Authentifizierungsfaktor vergessen oder verlegen kann. In diesem Fall sollte die Lösung in der Lage sein, eine alternative Authentifizierungsmethode anzubieten, was mit nur zwei Faktoren nicht möglich ist. Das Fazit ist, dass jede Branche und jede Organisation unterschiedliche Sicherheitsziele, Anwendungsfälle, Architekturen und Compliance-Vorschriften haben, die jeweils von einer breiten Palette an Authentifizierungsfaktoren für jeden Anwendungsfall unterstützt werden müssen.

Komplexität

Die Kosten und die Komplexität bei der Einführung einer Multi-Faktor-Authentifizierung sind wesentliche Hindernisse und die meisten verfügbaren Lösungen bieten keine nahtlose und anwenderfreundliche Benutzererfahrung. Ein Report von Vormetric zeigt:

- In fast allen Regionen war „Komplexität“ das Haupthindernis bei der breiteren Einführung von Datensicherheits-Tools und wurde von 57 Prozent der Befragten angegeben.
- Komplexe Einsatzszenarien erfordern in der Regel auch signifikante Personalressourcen und „Zu wenig Personal für das Management“ war das zweitwichtigste Hindernis, wenn auch mit deutlichem Abstand und 38 Prozent der Befragten.

Der wichtigste Faktor für die Komplexität in der IT war die explosionsartige Zunahme von neuen Endgeräten, Systemen und Anwendungen, die in das IT-Ökosystem geströmt sind. Dies wird durch die Tatsache verschärft, dass Organisationen neue Technologien schneller einführen, als sie ältere ausmustern. Das gilt insbesondere für kleine und mittlere Unternehmen, wo das alte Sprichwort „Was nicht kaputt ist, muss man auch nicht reparieren“ die Maxime des Handelns bestimmt. Im Ergebnis haben diese Unternehmen einen stark fragmentierten oder – noch schlimmer – hoffnungslos veralteten Sicherheitsstatus.

Da dieser Mix aus Endgeräten, Systemen und Anwendungen keine gemeinsamen Schnittstellen bietet, haben sich die Authentifizierungspraktiken in vielen Organisationen in eine Reihe von Insellösungen verwandelt, die über die Zeit organisch gewachsen sind. Jede dieser Lösungen erfüllt die spezifischen Anforderungen zu einem bestimmten Zeitpunkt; es ist jedoch nicht möglich, diese auf die Implementierung neuer Technologien oder die Abwehr neuer Bedrohungen auszurichten. Damit wird die Komplexität der Infrastruktur unangenehmerweise mit einer zusätzlichen Komplexität in Bezug auf die Sicherheit verwoben, was die Herausforderungen für die IT noch größer macht.

Single Sign-On (SSO) hat die Hoffnung auf Erleichterung geweckt, indem Anwender sich nur einmal anmelden müssen und anschließend alle ihre Anwendungen ohne erneuten Authentifizierungsaufwand nutzen können. Leider ist diese einmalige Anmeldung gleichzeitig ein attraktives Ziel geworden, ein „Single Point of Failure“ der Authentifizierung, wenn man so sagen will. Berücksichtigen wir, dass SSO einen Login des Anwenders erfordert – Benutzername und Passwort sind dabei immer noch die häufigste Methode – so stehen wir wieder am Anfang.

Die Implementierung von 2FA oder MFA verspricht, das SSO-Passwort-Risiko zu verringern. Aber keine der auf dem Markt verfügbaren Lösungen ist in der Lage, die Authentifizierungssicherheit auch für Legacy-Assets der IT bereitzustellen. Die Einführung einer neuen Technologie, um alle anderen Protokolle im Security-Management zu ersetzen ist aufwändig und mühsam – und fördert die weitere Fragmentierung der IT-Sicherheit.

Unvollständige Abdeckung

Die MFA-Anbieter sprechen oft von einfacher Nutzung, einfachem Einsatz und umfassender Abdeckung. Aber sie beschränken ihre Beispiele dabei auf eine Auswahl von IT-Systemen. Durch den starken Anstieg der Cloud-Nutzung liegt das Hauptaugenmerk auf Cloud- und SSO-Anwendungen. Doch was ist mit der Anmeldung am Mainframe, am Client und am Server, mit Anwendungen am Desktop-Client, mit VDI und VPN? Wenn Sie Ihre Cloud mit MFA geschützt haben, was ist mit den übrigen IT-Assets?

Kunden müssen eine Vielzahl von Authentifizierungsprotokollen für jeden Anwendungsfall einführen. Daher nutzen viele Organisationen weiterhin veraltete und unsichere Authentifizierungsmethoden, allen voran Passwörter – und eine Datenschutzverletzung folgt auf die nächste in erschreckender Regelmäßigkeit. Die Haustüre abzuschließen, aber alle Fenster offen zu lassen führt nicht zu einem sinnvollen Sicherheitsstandard. Und ohne eine einheitliche Authentifizierungslösung ist es schwer, wenn nicht unmöglich, einen umfassenden Bericht aller Zugriffsaktivitäten zu erhalten, der wiederum unerlässlich für Compliance-Zwecke ist.

MFA für Microsoft® Office 365

Microsoft bietet die Multi-Faktor-Authentifizierung für Office 365 an. Sie ist als gebrauchsfähig anerkannt und bietet eine verbesserte Zugriffssicherheit für das Office 365 SSO Portal – ein kritischer Aspekt, wenn Sie die sensiblen Daten betrachten, die in der Regel in Office-365-Apps gespeichert sind. Die Herausforderung liegt darin, dass MFA für Office 365 nur wenige weitere gängige Anwendungen und Systeme im Rechenzentrum einschließt. Dazu gehören Desktop-Anwendungen von Microsoft, wie Outlook®, Skype™ for Business, Word®, Excel®, PowerPoint® und OneDrive® for Business.

Das grundlegende Problem ist, dass viele Client-Anwendungen ausschließlich für die traditionelle Authentifizierung mit Benutzername und Passwort konzipiert sind. Sie können nicht durch die Multi-Faktor-Authentifizierung von Microsoft geschützt werden. Um dieses Problem zu beheben, hat Microsoft App-Passwörter eingeführt, die es erlauben, die Multi-Faktor-Authentifizierung zu umgehen und die Anwendung weiter zu nutzen. Der unerwünschte Nebeneffekt ist, dass die Anwender nun mehrere App-Passwörter verwalten müssen, was das Versprechen des Single Sign-On wieder zunichte macht. Um die Auswirkungen dieses Ansatzes für den Endanwender zu veranschaulichen, stellen wir uns ein realistisches Szenario vor, in dem jeder Anwender über 20 App-Passwörter nutzt und diese gemäß der IT-Richtlinien in regelmäßigen Abständen ändern muss. Schlimmer noch, mit App-Passwörtern müssen die Anwender die Passwörter auf jedem einzelnen Gerät ändern. Um dieses Security-Management-Problem zu lösen, hat Microsoft ein System eingeführt, mit dessen Hilfe Anwender ihr Hauptpasswort und alle App-Passwörter ändern können und einen neuen Datumsstempel erhalten, ohne sie tatsächlich zu ändern. Mit diesem Ansatz hat sich zwar die Alltagstauglichkeit der App-Passwörter verbessert, allerdings zu Lasten der IT-Sicherheit – Client-Anwendungen und Peripherie-Geräte haben nun unveränderliche Passwörter.

Selbst mit der fragwürdigen Notlösung in Form von App-Passwörtern für einige Rich Clients gibt es immer noch viele Anwendungen und Systeme, für die weder Microsoft MFA noch App-Passwörter einen Zugriffsschutz bieten, beispielsweise Mainframes, Server, VPN, VDI und natürlich die Windows-Anmeldung. Alle diese Assets müssen separat abgesichert werden, was unweigerlich zu gravierenden Sicherheitslücken führt. Um mit dem heterogenen IT-Umfeld klar zu kommen, haben Organisationen eine Reihe von Insellösungen implementiert, die jeweils separat verwaltet werden müssen. Dies führt dazu, dass sich die Anwender einer verwirrenden Vielfalt an unterschiedlichen Schnittstellen und Workflows ausgesetzt sehen. Häufig findet sich die Zugriffssicherheit auf dem kleinsten gemeinsamen Nenner des Passworts wieder. Mit einem solchen Flickwerk haben Organisationen keine Transparenz darüber, wer wann worauf zugreift.

Ein besserer Ansatz für die Zugriffssicherheit ist überfällig

Der historische Ansatz für Zugriffssicherheit ist nicht mehr brauchbar. Organisationen können es sich nicht leisten, weitere Insellösungen für jede neue Anwendung und jedes neue IT-System einzuführen. Das erhöht die Komplexität, gefährdet die Sicherheit, frustriert die Anwender und belastet das ohnehin bereits überlastete IT-Personal weiter. Wir brauchen einen ganzheitlichen Ansatz für die Zugriffssicherheit.

Das bedeutet, dass alle IT-Assets geschützt werden müssen – einschließlich Web, SSO, Mainframe, Client- und Server-Anmeldung, Desktop-Client-Anwendungen, VDI und VPN. Alle Akteure müssen geschützt sein, einschließlich Mitarbeiter, Partner und Lieferanten. Die Lösung muss so integriert sein, dass sie gängige administrative und Benutzerschnittstellen bietet und die gesamte Authentifizierungslandschaft auf einen Blick transparent macht. Ein integrierter Ansatz schützt nicht nur Office 365, sondern bietet Schutz für die gesamte Organisation.

Die DigitalPersona® Lösung Multi-Faktor-Authentifizierung

DigitalPersona® SSO für Office 365 ist Teil der DigitalPersona-Lösungsreihe. Es verändert die Art und Weise, wie IT-Verantwortliche die Integrität der digitalen Organisation schützen. Die Lösung stellt eine umfassende, integrierte Authentifizierung bereit, die einzelne Anwendungen und Systeme schützt. Kunden können endlich alle Ihre IT-Assets mit einem zentrale Identitätsspeicher mit administrativen und Benutzerschnittstellen schützten, einschließlich Microsoft Office 365.

DigitalPersona SSO für Office 365

DigitalPersona SSO für Office 365 ermöglicht Kunden den Ersatz der schwachen „Password only"-Anmeldung durch eine starke Multi-Faktor-Authentifizierung. Die Lösung bietet eine breite Palette an Authentifizierungsfaktoren und flexible Einsatzoptionen. Ob Sie auf Cloud-only Azure setzen oder ein Active Directory On-Premise nutzen, es gibt immer eine geeignete DigitalPersona-Option. Wenn Sie die Authentifizierung über Office 365 hinaus nutzen möchten, können Sie die gleiche Plattform, die gleichen Authentifizierungsfaktoren und die gleiche Authentifizierungsdatenbank dafür nutzen. Eine Lösung schützt Ihre gesamte Organisation.

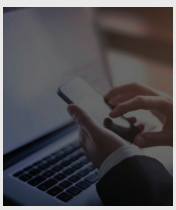
MEHR ALS MFA: ALLE LÜCKEN SCHLIESSEN

DigitalPersona schließt die Lücken in den aktuellen Lösungen zur Nutzerauthentifizierung. Zusätzlich zu den klassischen Authentifizierungsfaktoren – Wissen, Besitz und Biometrie – bietet es Authentifizierung für kontextbasierte Risikofaktoren wie Zeit, Geschwindigkeit, Ort und Verhalten. Diese Faktoren decken ab, was Sie tun, wo Sie sind und wann Sie handeln. So können Sie das richtige Schutzniveau für jede Anwendung, jeden Nutzer und jedes System auswählen.

UMFASSENDE ABDECKUNG

Endlich ist eine umfassende Abdeckung möglich. DigitalPersona unterstützt ALLE Anwendungen, einschließlich Web, Cloud, Windows, Mobile, VDI und VPN. DigitalPersona geht über diese aktuellen Anwendungen hinaus und unterstützt sogar traditionelle Mainframe-Apps, die eine wichtige Rolle in der Infrastruktur vieler Organisationen spielen. Dank DigitalPersona sind alle Ihre Anwenderkreise abgedeckt – nicht nur Ihre Mitarbeiter, sondern auch Ihre Kunden, Lieferanten und Partner.

HUMAN-PROOFED



Eliminieren Sie die Abhängigkeit von Ihren Nutzern wie auch deren Belastung – so dass Sie sich auf starke Authentifizierung verlassen können, ohne eine Kompromittierung durch Fehlverhalten befürchten zu müssen. Stärken Sie Ihr Compliance-Profil mit einem unwiderlegbaren Anwesenheitsnachweis und senken Sie gleichzeitig die administrativen Kosten mit einer IT-freundlichen Architektur.

SCHNELLE ANPASSUNG

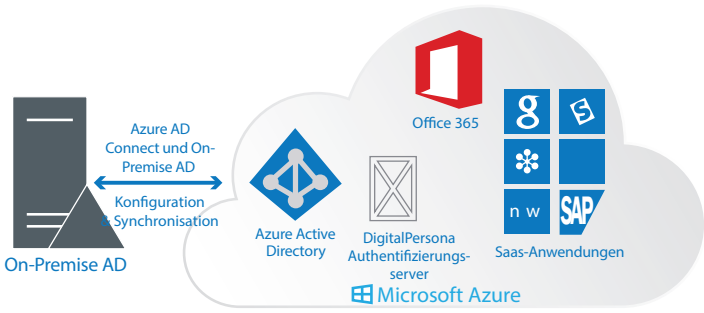
Schnelle Bereitstellung mit minimalen Beeinträchtigungen und ohne, dass Sie IHRE Systeme an UNSER Produkt anpassen müssen. Integrieren Sie die Lösung in Ihre bestehende IT-Infrastruktur mit aktuellen IT-Tools und -Ressourcen. Erhalten Sie mehr Flexibilität beim Personaleinsatz und niedrigere Vorab- und laufende Kosten – und gleichzeitig lässt Sie eine zukunftssichere Architektur ruhig schlafen.

DigitalPersona® passt sich an Ihre bestehende Umgebung an

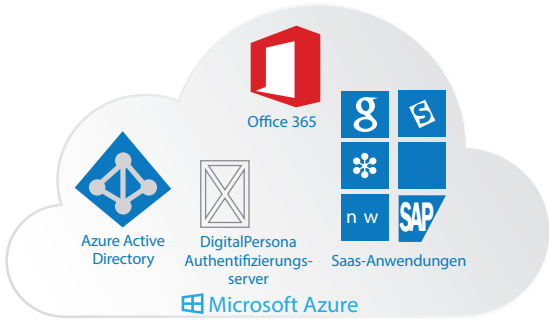
DigitalPersona in der Azure Cloud gehostet

Für Kunden, die sich für ein Cloud-basiertes Modell mit Azure entschieden haben, entweder mit (1) oder ohne (2) ein On-Premise Active Directory, passt DigitalPersona® SSO für Office 365 wie angegossen. Es kann in einer Azure-Instanz gehostet werden, um Multi-Faktor-Authentifizierung für Office-365-Apps sowie das gesamte Spektrum der SaaS-Apps, die von Azure unterstützt werden, bereit zu stellen.

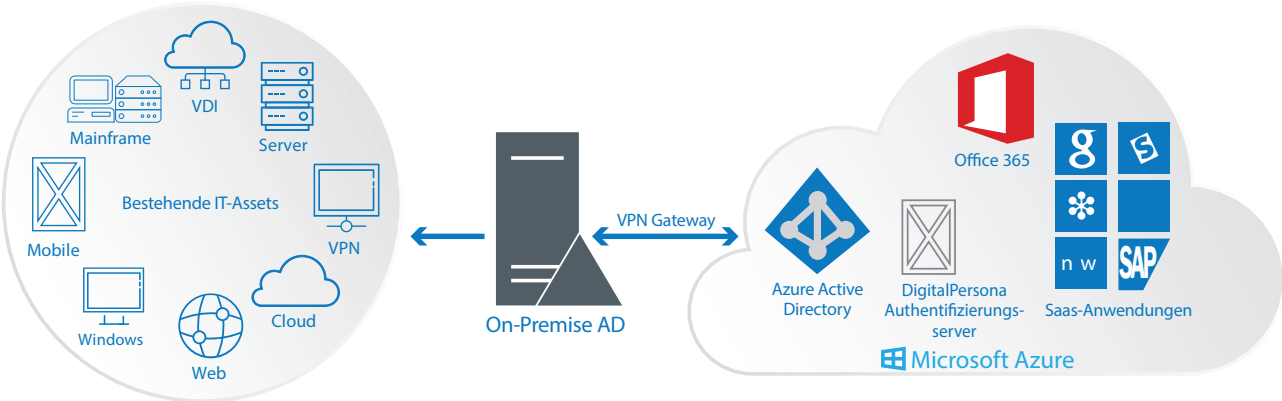
1) DigitalPersona Server in Azure gehostet, mit On-Premise AD



2) DigitalPersona Server in Azure gehostet, ohne On-Premise AD



3) DigitalPersona Server in Azure gehostet, mit vollständiger Abdeckung von Anwendungen

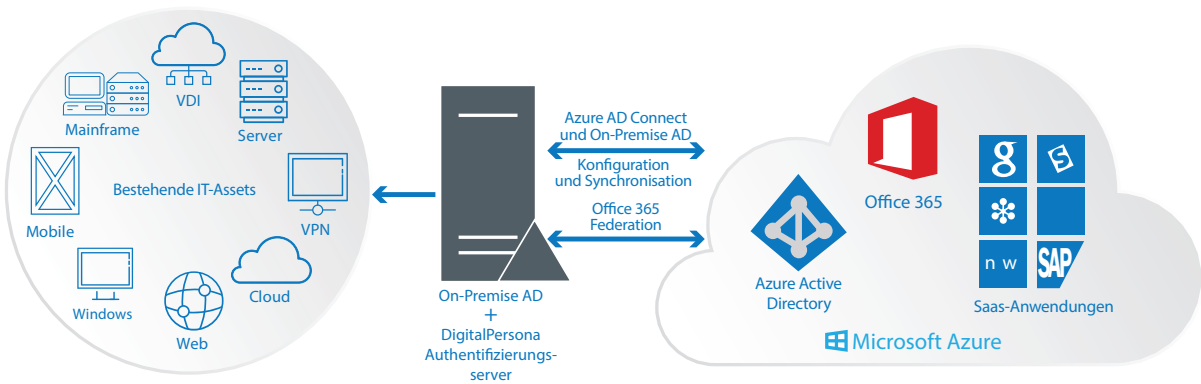


DigitalPersona® SSO für Office 365 befreit Organisationen von der Tyrannei der Security-Insel-lösungen. Mit einer einheitlichen Plattform schützt DigitalPersona nicht nur Ihre Office-365-SaaS-Umgebung, sondern kann auch einfach für den jederzeitigen Schutz aller Anwendungen, Nutzer und Systeme erweitert werden. Kontaktieren Sie uns, um mehr zu erfahren oder für eine kostenlose Testversion.

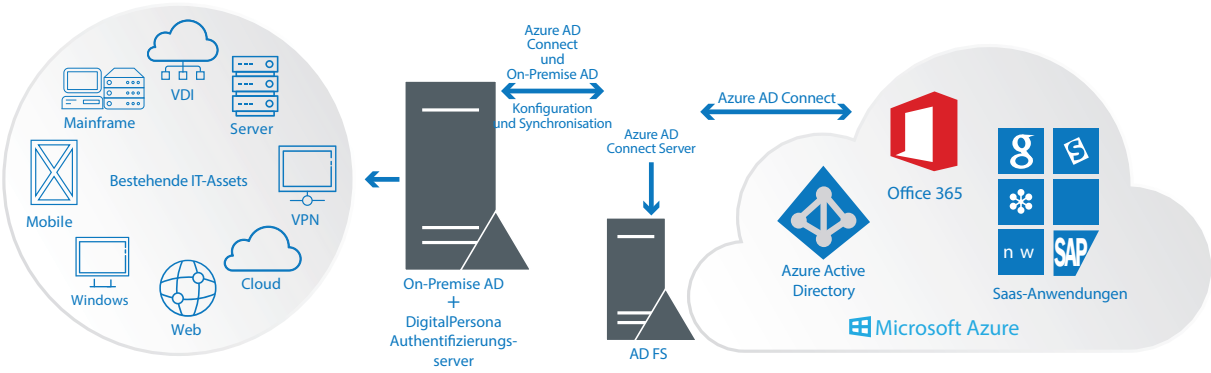
DigitalPersona® Server On-Premise-Einsatzoptionen

Kunden haben die Möglichkeit, den DigitalPersona® Server On-Premise zu installieren, um einen kombinierten Authentifizierungsschutz für Azure-SaaS-Anwendungen zu erhalten. DigitalPersona unterstützt Kundenkonfigurationen mit (4) Office 365 Federation oder (5) Microsoft Active Directory Federation Services (AD FS). In beiden Fällen kann DigitalPersona erweitert werden, um unter Zuhilfenahme eines Endpoint-Clients umfassenden Anwendungsschutz bereit zu stellen.

4) On-Premise Server-Einsatz, Office 365 Federation



5) On-Premise Server-Einsatz, Microsoft AD FS



Umfassende Lösungen von HID Global

HID bietet Kunden eine vollständige Palette von Authentifizierungs-Hardware, um das Software-Angebot von DigitalPersona zu ergänzen. Die folgenden Produkte von HID sind verfügbar:

- Kartenleser: z.B. OMNIKEY® 3021 (kostenoptimierter Kartenleser mit horizontaler Einführung), 3121 (Kartenleser mit vertikaler Einführung)
- Kontaktlose Hochfrequenz-Kartenleser (13,56MHz): z.B. OMNIKEY 5022, 5023
- Duale Kartenleser (mit Kontakt und kontaktlos): z.B. OMNIKEY 5422 (HF und Kontakt), 5427 (LF und HF, einschließlich HID SEOS und HID Mobile Credentials)
- Fingerprint-Leser
  - DigitalPersona 4500, optischer Leser – schneller Leser für den Einsatz im Büro
  - EikonTouch® TC510, kapazitiver Leser – robuster Leser mit AES256-Verschlüsselung
  - EikonTouch® TC710, kapazitiver Leser – FBI-PIV-zertifizierter Leser mit AES256-Verschlüsselung
  - Lumidigm M211, multispektraler Leser – robuster, ISO-PAD-zertifizierter Leser
  - Lumidigm V311, multispektraler Leser – beste Leistung, robuster, ISO-PAD-zertifizierter Leser

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 9171 1108

2020-11-06-iams-digitalpersona-sso-office-365-br-de PLT-05786

Part of ASSA ABLOY

hidglobal.com