Evidian

Authentication Manager – für jede Organisation passend

Multi-Faktor-Authentisierung für die gesamte Organisation

Jederzeit sicheren Zugriff auf Ihre Computer und Server. Unabhängig davon, ob ein Nutzer auf einen oder mehrere Computer zugreift oder mehrere Nutzer gemeinsam einen PC verwenden. Der Evidian Authentication Manager von Atos bietet immer die richtige Authentisierung für jede Situation.

Passwörter sind die Schwachstelle der meisten Authentisierungsstrategien. Einfache wie auch gemeinsam genutzte Windows-Passwörter erhöhen das Risiko, dass Unberechtigte in Ihre Systeme eindringen. Zudem ist es bei gemeinsam genutzten Passwörtern nicht möglich, die tatsächliche Nutzung des Windows-Kontos detailliert zu auditieren, was zusätzliche Sicherheitsrisiken birgt.

Eine starke Authentisierung schafft Abhilfe, indem Passwörter durch spezielle Hardware oder biometrische Verfahren ersetzt werden. Doch auch hier können Probleme entstehen, wenn die Authentisierung beispielsweise unterschiedliche Szenarien nicht berücksichtigen kann und für die Nutzer im Tagesgeschäft zu kompliziert wird.

Auf individuelle Anwendungsfälle zugeschnitten

Mit dem Evidian Authentication Manager (AM) können sich Nutzer einen Computer teilen und dennoch sicher und in Sekundenschnelle auf ihre eigene Umgebung zugreifen, ohne sich in Windows ein- und ausloggen zu müssen.

Ärzte beispielsweise erhalten auf diese Weise sicheren und schnellen Zugriff auf alle notwendigen Unterlagen der verschiedensten Arbeitsplätze im Krankenhaus.

Börsenmakler oder Techniker in Kontrollräumen können Sitzungen öffnen, sperren, entsperren oder schließen, indem sie ihre Multi-Faktor-Authentisierung nutzen.

Ein Mitarbeiter kann flexibel einem anderen Mitarbeiter Zugriff auf seine gesperrte Windows-Sitzung gewähren. Egal ob permanent oder temporär, ob an einem oder an mehreren Computern.

Multi-Faktor-Authentisierung: einfach und schnell ausgerollt

Der AM vereinfacht das Ausrollen und das Management von Multi-Faktor-Authentisierungsmethoden durch:

- zentrales Management der Zugriffsregeln
- gruppenbasierte Authentisierungs-Profile
- integrierte Karten-Administration (ausstellen, inventarisieren, sperren etc.)
- zentralisiertes Auditing sämtlicher Zugriffsversuche auf den Computer

Der AM ist unabhängig von den installierten Technologien einsetzbar. Passend für jeden Anwendungsfall kann die richtige Authentisierungsmethode für jeden Arbeitsplatz gewählt werden. Die dazugehörigen Sicherheitsregeln, einschließlich aller eingesetzten Authentisierungsmethoden, werden zentral verwaltet und überwacht.

Betriebskosten senken

Mit dem AM können die Helpdesk-Mitarbeiter über eine einzige Konsole Zugänge direkt entsperren oder entziehen, unabhängig davon, welche Authentisierungsmethoden eingesetzt werden: RFID, biometrische Verfahren, One-Time-Passwort (OTP), Smart Card usw.

Die Nutzer selbst können Windows-Sitzungen entsperren, indem sie die Funktion Self-Service Password Request (SSPR) nutzen, ohne den Helpdesk beanspruchen zu müssen.

Vorhandene Infrastruktur wiederverwenden

Der AM baut auf Ihrem LDAP-Verzeichnis oder Active Directory Ihres Unternehmens auf. Er nutzt die darin verschlüsselt gespeicherten Nutzer- und Sicherheitsdaten. So müssen Benutzerdaten nicht kopiert werden, zusätzliche Appliances sind nicht erforderlich.

Smart Card-Anmeldung

Der AM unterstützt die vollständige Smart Card-Anmeldung von Microsoft und bietet einfache und effiziente Notfallzugriffsmethoden.

IGEL Thin Client-Integration

Durch das Zusammenspiel des AM und IGEL wird die Anmeldung an Thin Clients einfacher, schneller und sicherer. Nutzer können auf Linux-basierte Thin Clients sowohl über ihren RFID-Ausweis als auch über ihre Smart Card zugreifen.

Einmal authentisierte Nutzer können schnell und sicher von jedem Thin Client auf ihre Sitzung (Citrix XenApp oder Microsoft RDS) zugreifen. Sie müssen dafür nur ihren RFID-Ausweis vor den Leser halten oder ihre Smart Card einstecken. Die Eingabe einer PIN oder eines Passwortes ist an diesem Tag nicht mehr nötig.

Einfach und schnell ausgerollt

Starten Sie mit dem AM in einem Bereich Ihres Unternehmens und weiten Sie diese Lösung sukzessiv auf tausende Nutzer aus. Der AM läuft auf Microsoft Windows, Citrix XenApp und Windows Terminal Server Umgebungen.

Eine große Auswahl an Authentisierungsmethoden

Der Evidian Authentication Manager (AM) unterstützt viele Authentisierungsmethoden:

- Smart Cards und Sicherheits-Token, mit und ohne Zertifikate
- Fingerabdrücke oder Venen als biometrische Codes
- RFID-Ausweise
- One-Time-Passwörter (OTP)
- Frage-/Antwort-Methoden
- Benutzername / Passwort

Ihren Authentisierungs-Lifecycle im Griff

Der AM umfasst die Verwaltung von Smart Cards und erlaubt es Ihnen, den kompletten Lifecycle Ihrer Geräte von einem zentralen Punkt aus zu steuern. So können Sie zum Beispiel eine neue Smart Card, inklusive zusätzlicher Daten und Zertifikate, für einen Mitarbeiter ausstellen oder eine vorhandene Smart Card leihweise an einen Mitarbeiter ausgeben. Auch können Sie eine Smart Card sperren oder auf eine Black List setzen.

Vom Nutzer initiierte Delegation

Wenn ein Mitarbeiter eine Abwesenheit plant, kann er mit Hilfe des AM den Zugriff auf seinen Computer entsprechend der zentral hinterlegten Sicherheitsregeln an einen Kollegen delegieren.

Sichere Verwaltung von geteilten Konten

Nutzer können generische Windows-Konten sicher verwenden. Sie müssen dabei noch nicht einmal das Passwort kennen. Über die Audit-Informationen lässt sich trotzdem transparent nachvollziehen, wer die Konten genutzt hat.

ActiveSync Integration

Der AM ermöglicht den mobilen Zugriff auf Mail-Systeme. Durch die Verwendung des ActiveSync Protokolls muss das Windows-Passwort nicht mehr auf dem mobilen Endgerät hinterlegt werden. In diesem Szenario benutzt der Evidian Web Access Manager das Windows-Passwort, das dem AM bekannt ist, um sich am Mail-System zu authentisieren. Durch das Zusammenspiel von Authentication Manager und Web Access Manager erhalten Nutzer Zugriff auf ihr Mail-System, ohne das Windows-Passwort preiszugeben

Starke Authentisierung mittels QR Code

Mit Hilfe von Evidian QREntry von Atos können sich Nutzer an Windows anmelden, indem sie einfach einen QR Code mit ihrem Smartphone scannen. Dabei spielt es keine Rolle, ob sie mit dem Unternehmensnetzwerk verbunden sind oder nicht.

Notfall-Zugriff über den Windows Anmelde-Dialog

Die Evidian Self Service Password Request (SSPR)-Funktion reduziert die Kosten, in dem sie die Nutzer in die Lage versetzt, ihr Passwort selbst zurückzusetzen. Wenn diese Funktion aktiviert ist, geben Nutzer persönliche Antworten auf voreingestellte Fragen. Sollte ein Nutzer seine Zugangsdaten einmal vergessen haben, kann er mit Hilfe seiner persönlichen Antworten entweder das Passwort zurücksetzen oder Zugriff auf seine Windows-Session bekommen.

Wenn Nutzer ihr Passwort über die Evidian SSPR-Funktion zurücksetzen, dann kann das Passwort:

- ein temporäres Passwort sein, das nur für eine bestimmte Zeit gültig ist;
- ein Passwort sein, dass nur an dem Computer gültig ist, an dem die Passwort-Zurücksetzung durchgeführt wurde;
- das eigentliche Passwort des Nutzers sein.

Sogar im Offline-Betrieb möglich

Mobile Nutzer können das Passwort für ihr Endgerät auch zurücksetzen, wenn sie nicht mit dem Unternehmensnetzwerk verbunden sind.

Alternativ zur Frage-/Antwort-Methode können Nutzer auch QREntry verwenden, um einen Notfall-Zugriff zu erlangen.

Notfall-Zugriff über das Web Portal

Nutzer können auch auf das Web Portal des AM zugreifen. Es erlaubt ihnen, ihr Passwort zurückzusetzen, indem sie

- ihre persönlichen Antworten eingeben,
- einen Bestätigungs-Code nutzen, der per Mail oder SMS verschickt wird,
- QREntry verwenden.

Die Sicherheit dieser Notfall-Zugriffsmöglichkeit kann durch die Verwendung eines zusätzlichen Captchas verstärkt werden.

Einhaltung gesetzlicher Bestimmungen und Regularien

Prüfprotokolle zu Zugriffen und administrativen Tätigkeiten werden signiert in einer zentralen Datenbank abgespeichert.

Der AM hilft Ihnen, den gesetzlichen und behördlichen Anforderungen nachzukommen, zum Beispiel Sarbanes-Oxley, Verordnungen zur Vertraulichkeit von medizinischen Daten, PCI DSS oder Gesetze zur Finanzintegrität.

Sie können die Zugriffsversuche Ihrer Mitarbeiter auf Computer nachverfolgen. Die Prüfereignisse beinhalten Identitätsinformationen zu den Nutzern, so dass Sie damit nachweisen können, dass Ihre Zugriffsregeln überwacht und deren Ziele erfüllt werden.

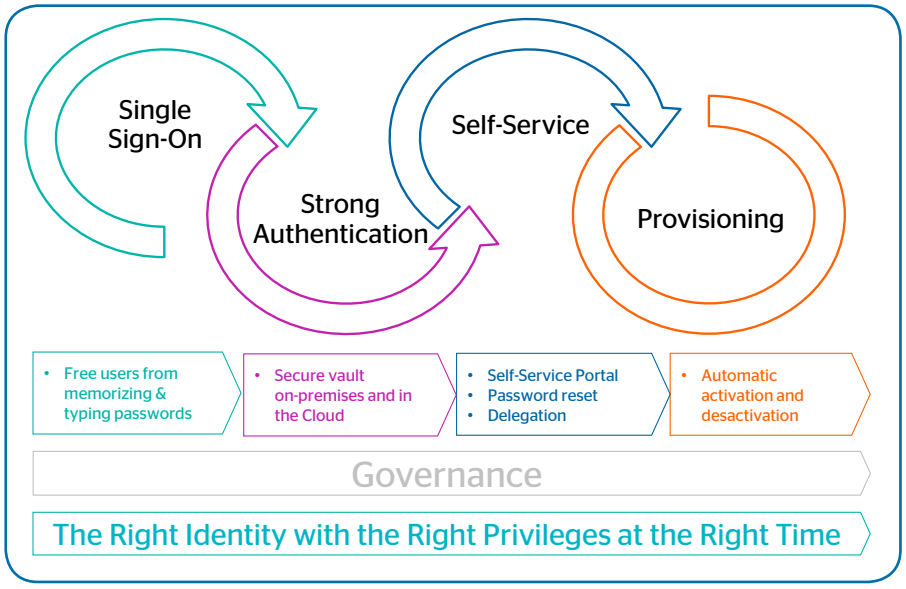
Moderne Reporting-Werkzeuge

Der AM umfasst ein Reporting-Modul, das die Erstellung von Dashboards erlaubt. So haben Sie jederzeit Einblick in die wichtigsten Kennzahlen, z.B. Aktivitäten, Snapshots, Risiken und KPIs. Nur autorisierte Nutzer können diese Berichte herunterladen.

Integration in die umfassende Evidian IAM-Lösung von Atos

Der Evidian Authentication Manager ist Teil der Evidian Identity & Access Management Lösung von Atos. Durch die nahtlose Integration werden der Authentication- und Identity Lifecycle miteinander verschmolzen.

- Mit Evidian Enterprise SSO werden Sie ohne zusätzliche Passwörter in Applikationen angemeldet
- Mit dem Evidian Web Access Manager greifen Nutzer sicher von jedem Browser auf ihre Unternehmens-Webanwendungen zu, ohne sich ständig neu authentisieren zu müssen
- Evidian Identity & Governance Administration ermöglicht die komplette Steuerung von Berechtigungen und die Verwaltung des gesamten Identity Lifecycle – angefangen bei den Identitätsdaten über die Zugriffssteuerung auf die verschiedensten Dienste bis hin zu automatischen und manuellen Genehmigungsworkflows.



Finden Sie mehr heraus unter
evidian.com

CT-200929-JR-EVIDIAN-FACTSHEET-AUTHENTICATION MANAGER-GERMAN