Enterprise SSO
Auf das eigene Business fokussiert bleiben

Single Sign-On für einen sicheren Zugriff von überall aus

Befreien Sie Ihre Nutzer davon, sich unzählige Passwörter merken und immer wieder eingeben zu müssen: Evidian Enterprise Single Sign-on (SSO) eröffnet allen Nutzern, Unternehmen und Organisationen stets abgesicherte Zugriffe.

Das automatisierte Passwort-Management im Hintergrund erleichtert Nutzern alle berechtigten Zugriffe – und dies stets im Einklang mit der Sicherheitsstrategie des Unternehmens und den dafür hinterlegten Sicherheitsregeln.

Einfach und sicher zugleich

Evidian Enterprise SSO weist Nutzern automatisch ihre Zugriffsrechte zu und passt sie bei geänderter Sicherheitsstrategie automatisch über die hinterlegten Sicherheitsregeln an. Damit ist beides, Sicherheitsstrategie und Zugriffskontrolle, immer auf dem aktuellen Stand.

Rollenbasierend können persönliche Zugriffsrechte einfach und schnell per Mausklick der jeweiligen Tätigkeitsrolle im Unternehmen zugeordnet werden. Das automatisierte Passwort-Management im Hintergrund macht es möglich, für zusätzliche Zugriffssicherheit für jede einzelne Zielapplikation komplexe Passwörter zu hinterlegen.

Durch den Einsatz von Re-Authentisierung oder spezifische Authentisierungsmethoden wie Smart Card, One-Time-Passwort, biometrische Daten oder RFID-Ausweis können alle Autorisierungsprozesse, je nach Sensibilität der Anwendungen, nochmals zusätzlich abgesichert werden.

Auf Kostenoptimierung ausgelegt

Mit Enterprise SSO entfallen bis zu 30% der Anrufe und Unterstützungsleistungen des Helpdesk, weil die Nutzer ihre Passwörter nicht mehr verlegen oder vergessen können und daher auch keine neuen anfordern müssen. Damit kommt es zwischenzeitlich auch nicht länger zu Zugriffssperren, bis den Nutzern das neue Passwort sicher zugewiesen worden ist.

Da die Lösung automatisch alle aktiven Nutzerkonten einschließlich der berechtigten Applikationen auflistet, behält das Unternehmen zudem die laufenden Software-Lizenzkosten im Blick.

Gemeinsame genutzte Konten und Delegierung von Zugriffsrechten

Mit Enterprise SSO können Nutzer einzelne Konten gemeinsam nutzen – und das sicher. Ebenso sicher können Nutzer für die Zeit ihrer Abwesenheit ihre Zugriffsrechte an einen anderen Nutzer delegieren. Ihre Passwörter müssen die ursprünglichen Nutzer dafür nicht preisgeben. Dennoch werden auch weiterhin alle persönlichen Zugriffe und Zugriffsversuche auditiert.

Selbst wenn ein Nutzer nicht im Büro anwesend ist, kann er remote via Web- Portal alle oder ausgewählte Zugriffsrechte seines Kontos sicher an Dritte delegieren. Die Zugriffskontrolle erfolgt weiterhin im Kontext mit der Sicherheitsstrategie und den hinterlegten Sicherheitsregeln.

YOU CARD
YouCard Kartensysteme GmbH
Friedenstraße 18
35578 Wetzlar
Tel +49 6441 4459 80
Fax +49 6441 4459 810
www.youcard.de
team@youcard.de

Immer konform mit Gesetzen und Regularien

Ob Sarbanes-Oxley, Regularien des medizinischen Bereichs, PCI DSS und/ oder gesetzliche Bestimmungen im finanziellen Bereich: Enterprise SSO versetzt Ihr Unternehmen in die Lage, jederzeit alle gesetzlichen Bestimmungen und Regulierungen Ihrer Branche zu erfüllen – und dies nachweislich.

Alle Zugriffe und Zugriffsversuche auf Anwendungen und Server werden überwacht. Dazu werden sie namentlich auditiert, unabhängig davon, ob es sich dabei um Zugriffe über Windows-Konten oder auf andere Applikationen handelt. So können Sie jederzeit belegen, dass alle Zugriffe in Übereinstimmung mit der Sicherheitsstrategie und den dafür hinterlegten Sicherheitsregeln erfolgen.

Enterprise SSO umfasst ein Berichtsmodul der neuen Dashboard-Generation. Es erlaubt, KPIs auf bestimmte Aktivitäten, Snapshots, Risikoparameter und andere Überwachungsfunktionen zu setzen. Anschließend dürfen und können ausschließlich autorisierte Nutzer die Berichte herunterladen.

Keine Anpassungen notwendig

Für den Einsatz von Enterprise SSO sind keine Anpassungen an bestehenden Applikationen erforderlich. Single Sign-on greift bei allen Applikationen, unabhängig davon, ob es sich um Windows-Applikationen, Web-Terminal-Emulationen oder andere Applikationen handelt.

Universell gelöst

Enterprise SSO läuft auf Windows- und Mac OS-Workstations ebenso wie auf Tablet-PCs, beliebigen Servern und in virtuellen Umgebungen (Citrix, Microsoft...) zudem auf virtualisierten Desktops wie Zero- und Thin-Clients.

Auch Tablets und Smartphones unter IOS und Android werden unterstützt. Unabhängig davon, von welchen Endgeräten Nutzer auf Applikationen und Ressourcen per Single Sign-on zugreifen. Alle damit verbundenen Berechtigungen und persönlichen Eintragungen sind immer abgesichert und jederzeit verfügbar.

Mobile Zugriffe ohne Eingabe von Passwörtern

Über Enterprise SSO für mobile Endgeräte erhalten alle Endgeräte unter iOS und Android per Single Sign-on Zugriff auf Applikationen und Ressourcen. Die Passwörter dafür werden automatisch im Hintergrund zugeordnet. Dies erspart mobilen Nutzern die Eingabe von Passwörtern. Sämtliche persönlichen Eintragungen und Passwörter sind in einer Private Cloud durch Verschlüsselung hermetisch abgeschirmt und vor Angriffen sicher.

Mobile Zugriffe zusätzlich abgesichert durch starke Authentisierung

Im Zusammenspiel mit QR Code wird den mobilen Single Sign-on-Zugriffen eine starke Authentisierung vorangestellt, was die mobilen Zugriffe auf Applikationen und Ressourcen zusätzlich absichert.

Schnell ausgerollt und einsatzbereit

Enterprise SSO sammelt im Hintergrund alle Passwörter und hält sie für die Zugriffe vor. Dies erspart allen Nutzern auch die Neuvergabe und den Wechsel von Passwörtern.

Geführt über ein bestehendes Provisionierungssystem kann das Unternehmen mit der Einführung des Systems in einem Teilbereich der Organisation beginnen und den Einsatz sukzessiv auf Tausende Endgeräte und Nutzer ausdehnen. Da die Lösung auf LDAP, Active Directory oder Active Directory LDS (Lightweight Directory Services) als Verzeichnisstruktur aufbaut, ist für den Ausrollprozess keine zusätzliche Hardware erforderlich.

Auch Remote-User kommen ohne Passworteingaben aus

Nutzer greifen oftmals aus der Ferne auf Applikationen zu, die innerhalb einer virtualisierten Umgebung angesiedelt sind. Auch sie brauchen sich ihre Passwörter nicht mehr merken bzw. immer wieder für die virtualisierten Applikationen einzugeben. Enterprise SSO ist zertifiziert für Citrix Ready for Citrix, XenApp, XenDesktop, Receiver und viele weitere Lösungen. Nähere Informationen finden Sie auf der Website von Evidian.

Remote Access für BYOD und Endgeräte ohne Management-Anbindung

Kommt zusätzlich der Evidian Web Access Manager von Atos zum Einsatz, kann SSO auch auf Endgeräte ohne Management-Anbindung ausgedehnt werden. Das erspart dem Unternehmen nicht nur die Installation von Agenten auf diesen Endgeräten, sondern auch Passwörter für Applikationen außerhalb des Unternehmensnetzes zu verteilen. Dadurch können auch Nutzer an PCs, Tablets, Smartphones sicher auf Applikationen in Clouds zugreifen.

YOU CARD
YouCard Kartensysteme GmbH
Friedenstraße 18
35578 Wetzlar
Tel +49 6441 4459 80
Fax +49 6441 4459 810
www.youcard.de
team@youcard.de

Die vermittelnde Instanz ist in diesem Fall Identity Federation über standardisierte Protokolle wie OAUTH, OpenID Connect oder SAML.

Starke Authentisierung inbegriffen

Evidian Authentication Manager von Atos eröffnet unter Windows eine starke Authentisierung u.a. mittels Smartcard, USB Token, One-Time-Passwort, biometrischer Daten, RFID-Ausweis oder über die Kombination von Smartphone mit QRentry.

Für den Fall, dass Nutzer ihr Windows-Passwort oder ihre Karte vergessen haben, können sie sich ersatzweise über die Funktion Self-Service Password Request (SSPR) in die Sitzung einwählen – sogar ohne Verbindung zum Unternehmensnetzwerk und ohne Helpdesk-Unterstützung.

Notfallzugriff auf Windows-Sitzungen

Über SSPR können Nutzer zudem ihre Windows-Sitzung mittels einer Notfallprozedur freischalten, sowohl online als auch offline (via Web-Portal). Dies erspart ihnen in Notfällen viele Anrufe beim Helpdesk. Die Freischaltung der Windows-Sitzung oder die Zurücksetzung des Windows-Passworts erfolgt in diesem Fall über eine Frage-/Antwort-Sequenz.

Die Sicherheit der Notfallprozedur kann durch die Funktion Captcha erhöht werden. Dabei werden zufällig angeordnete Ziffern und Buchstaben angezeigt, die der Nutzer eingeben muss. Diese Sequenz kann über den Helpdesk, am Smartphone mit QRentry oder am mobilen Endgerät mittels SMS, E-Mail oder Push-Mechanismus ausgelöst werden.

Hautnah am Geschäft agieren

Über den Evidian Authentication Manager können beispielsweise Verkaufsteams oder Mitarbeiter einzelner Niederlassungen einen PC gemeinsam nutzen. Sie haben auf diesem Kiosk-PC ihre eigene sichere Umgebung, ohne dass sie zwischenzeitlich ihre Windows-Sitzung schließen und später wieder öffnen müssen.

Nutznießer solcher sicheren Kiosk-PCs sind zum Beispiel auch Ärzte und Pflegepersonal auf ihrem Weg durch die Station oder durch Fachabteilungen. Alles, was sie tun müssen, ist ihren RFID-Ausweis zu zücken oder ihre Smartcard einzuführen.

Börsenhändler, die oftmals über PC-Cluster arbeiten, haben mittels starker Authentisierung jeweils sicheren Zugriff auf ihre Umgebung. Ebenso sicher können sie ihre Zugriffe an andere Trader delegieren – für ihre komplette Arbeitsumgebung oder nur Teile davon, für den kompletten Arbeitstag oder nur für bestimmte Zeitabschnitte.

Integration in IAM-Lösungen von Evidian

Enterprise SSO ist Teil der Evidian Identity & Access Management-Lösung von Atos. Darüber können Sie mühelos Identity-Management-Funktionen Ihrer Installation hinzufügen:

- Über Provisionierung müssen Passwörter nicht länger an die Nutzer verteilt werden. Sobald Anwendungskonten definiert, gelöscht oder aktualisiert sind, werden alle Passwörter automatisch mit Enterprise SSO synchronisiert.

- In Bezug auf das Policy-Management weiß Ihr Unternehmen jederzeit, welche Anwendungskonten tatsächlich genutzt werden. Alle anderen, nicht mehr genutzten oder unnötigen Anwendungskonten können dadurch gezielt eliminiert werden. Durch Kenntnis der tatsächlich gebrauchten und verwendeten Anwendungskonten und deren Nutzer kann Ihr Unternehmen nach Maß seine Sicherheitsstrategie auf diese Konten ausrichten.

- Der Evidian Identity & Access Manager von Atos versetzt Ihr Unternehmen in die Lage, jederzeit alle Governance-Auflagen zu erfüllen und alle Identitäts- und Zugriffsservices entlang des Lebenszyklus zu managen. Dies stets orientiert an der Sicherheitsstrategie Ihres Unternehmens und gestützt durch automatisierte Genehmigungs-Workflows.