EVIDEN

Identity und Access Management

DirX Identity V9.0

Sicheres und flexibles Passwortmanagement

Die Passwortmanagement-Lösung für Organisationen aller Art

Herausforderungen bei der Nutzung von Passwörtern

Durch die starke Zunahme von Anwendungen, die eine Anmeldung mittels Passworts erfordern, müssen sich die Benutzer immer mehr Passwörter merken. Damit nimmt die Wahrscheinlichkeit zu, dass Passwörter immer öfter vergessen werden. Wenn ein Passwort vergessen wird, erfolgt das Zurücksetzen (Reset) des Passworts häufig mit Unterstützung durch den Service-Desk. Das hat hohe Service-Desk-Kosten zur Folge, speziell dann, wenn das Zurücksetzen außerhalb der Geschäftszeiten angefordert wird. Ebenso ist nach Feiertagen oder nach Wochenenden ein erhöhtes Aufkommen von Service-Desk-Anrufen für das Zurücksetzen von Passwörtern festzustellen.

Aus Sicherheits- und Compliance-Gründen tendieren Organisationen dazu, stärkere Passwortrichtlinien einzuführen. Dies führt zu einer größeren Komplexität der Passwörter, mit der Folge, dass sie noch öfter vergessen werden. Damit besteht eine heikle Beziehung zwischen Sicherheit und Compliance auf der einen Seite und der Anzahl von Passwortrücksetzungen und damit verbundenen Service-Desk-Kosten auf der anderen Seite.

Aus diesem Grund gibt es einen großen Bedarf dafür, dass Benutzer ihre Passwörter selbst zurücksetzen können (Self-Service Passwort Reset). Das ermöglicht den Organisationen, auch bei stärkeren Passwortrichtlinien, die Passwort-bezogenen Service-Desk-Kosten zu senken. Auch aus Sicht der Benutzer besteht ein starker Bedarf, ihre Passwörter sofort, zu jeder Zeit und von jedem Ort aus zurücksetzen zu können.

Für den Fall, dass Benutzer keinen direkten Zugang zu den Zielsystemen haben, um ihre Passwörter zurückzusetzen, sollte eine Passwortmanagement-Lösung das Service-Desk-Personal dabei unterstützen, ein Passwort auf Anfrage des Benutzers zurückzusetzen. Dies erfordert auch, dass die Service-Desk-Mitarbeiter dabei unterstützt werden, die Benutzer eindeutig zu authentifizieren.

Mit der Vielzahl von Anwendungen, die eine Anmeldung über Passwort erfordern, müssen sich Benutzer viele verschiedene Passwörter merken – eines für jede Anwendung. Das kann leicht dazu führen, dass sich die Benutzer die Passwörter aufschreiben oder leicht zu erratende Passwörter wählen, was wiederum die Sicherheit der Anwendung gefährdet.

Um die Anzahl der Passwörter, die die Benutzer benötigen, zu reduzieren, bietet sich die Synchronisation von Passwörtern in verschiedene Anwendungen an. Damit müssen sich die Be-nutzer nur noch ein einziges Passwort für alle von ihnen benutzten Anwendungen merken. Dieses Passwort basiert auf einer einzigen, übergreifenden Passwortrichtlinie.

Für die Passwörter privilegierter Accounts gibt es zusätzliche Anforderungen. Diese Accounts sind üblicherweise nicht einem bestimmten Benutzer zugeordnet, sondern werden oftmals von verschiedenen Administratoren verwendet. Die Passwörter dieser Accounts sollten vom System gesetzt, erst bei Bedarf dem Administrator bekannt gemacht werden und anschließend wieder geändert werden.

Eine Passwortmanagementlösung erfordert auch Funktionalitäten zur Verwaltung und Durchsetzung von Passwortrichtlinien, wenn Benutzer neue Passwörter wählen.

Zur Sicherstellung und Dokumentation von Compliance-Anforderungen oder auch um Abrechnungsanforderungen zu erfüllen, wird Audit- und Reportfunktionalität zur Unterstützung der Administratoren und Service-Desk-Mitarbeiter benötigt.

DirX Identity adressiert all diese Herausforderungen; es stellt eine Passwortmanagement-Lösung mit einer reichhaltigen Funktionalität bereit.

Funktionsüberblick

DirX Identity Passwortmanagement bietet folgende Funktionalitäten:

- Self-Service Passwort Reset: die Benutzer setzen vergessene Passwörter selbst zurück oder entsperren ihre Accounts. Dabei nutzen sie verschiedene Alternativen zur Authentifizierung.
- Unterstütztes Zurücksetzen von Passwörtern: Administratoren oder Service-Desk-Mitarbeiter setzen für die Benutzer Passwörter zurück oder entsperren deren Accounts.
- Abgelaufene Passwörter; Benutzer werden darauf hingewiesen, ihre Passwörter zu ändern, bevor sie ablaufen.
- Erstmalige Registrierung von Benutzern: Die Benutzer wählen Sicherheitsfragen und zugehörige Antworten, die alternativ als Zugangsdaten genutzt werden können, was auch unter dem Begriff Challenge-Response-Verfahren bekannt ist.
- Passwort Listener für Windows: Dieser erkennt die Passwortänderungen, die vom Benutzer am Windows Desktop durchgeführt werden.
- Passwort-Synchronisation: Synchronisiert geänderte Passwörter in Real-Time zu angeschlossenen Zielsystemen.
- Passwortrichtlinien-Management: Verwaltet Regeln zur Komplexität, Ablauf und Historie von Passwörtern und setzt diese Regeln durch.
- Passwortmanagement für privilegierte Accounts: Verwaltet und steuert den Zugriff auf Passwörter für gemeinsam genutzte, privilegierte Accounts.
- Audit und Reports: Führt Aufzeichnungen und erzeugt Reports zu Passwort-bezogenen Aktionen.

Eviden bietet auch “Password Reset as a Service” an, um Benutzern ein einfaches und schnelles Zurücksetzen ihrer Passwörter zu ermöglichen oder ihre Accounts zu entsperren.

Vorteile

DirX Identity Passwortmanagement bietet die folgenden Vorteile und Nutzen für Benutzer und Organisationen:

- Benutzern wird eine schnelle und flexible Möglichkeit gegeben, ihre Passwörter selbstzurückzusetzen oder ihre Accounts zu entsperren.
- Signifikante Reduktion der Service-Desk-Kosten sowohl durch Self-Service als auch durch unterstütztes Passwort Reset und Passwortsynchronisation.
- Verbesserte Sicherheit durch weniger Passwörter, die sich die Benutzer merken müssen, durch die Durchsetzung stärkerer Passwortrichtlinien, durch verschiedene Authentifizierungsoptionen sowie durch die Dokumentation von Passwort-bezogenen Aktionen mittels Audit- und Reportfunktionen.
- Geringere Anzahl von Passwörtern, die von den Benutzern als Folge der Passwortsynchronisation verwaltet werden müssen.
- Verbesserte Produktivität der Benutzer durchweniger Anrufe beim Service-Desk und durch weniger Login-Probleme
- Verbesserte Nutzererfahrung, d.h. weniger Passwörter zu merken, nur ein einziges User-Interface zu bedienen, konsistente Passwort-Policies und frühzeitige Benachrichtigung der Benutzer beim Ablauf eines Passworts.
- Nahtlose Integration mit der Identity und Access Management Landschaft.

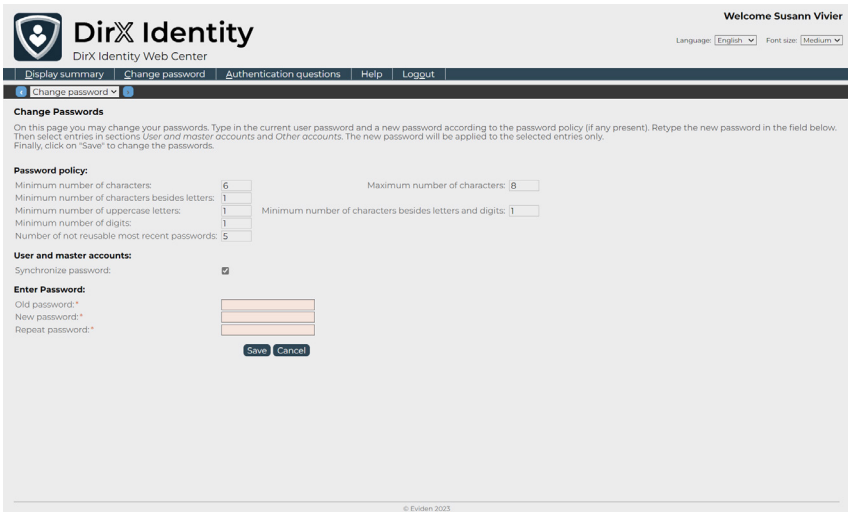

Abbildung 1 - DirX Identity Passwort Reset Benutzer-Dialog mit Web Center

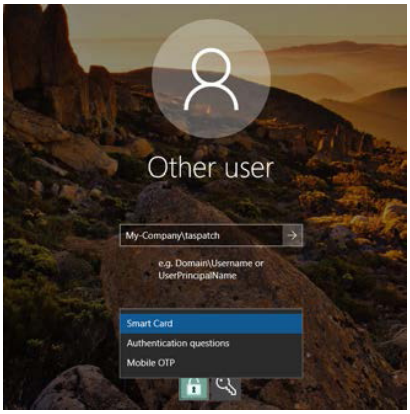

Abbildung 2 - DirX Identity Passwort Reset mit dem DirX Password Reset Client

Self-Service Passwort Reset

DirX Identity Passwortmanagement bietet die Passwort Reset-Funktionalität entweder über eine Webbasierte Benutzerschnittstelle oder vom Windows Client an.

Standardmäßig wird das Passwort Reset für Microsoft Active Directory (AD) zur Verfügung gestellt. Optional können andere Zielsysteme unterstützt werden.

Um ein Passwort zurückzusetzen, muss ein Benutzer mit seinen alternativen Zugangsdaten authentifiziert werden. Nach einer erfolgreichen Authentifizierung kann der Benutzer die Passwörter für Accounts zurücksetzen, für die er berechtigt ist. Das neu eingegebene Passwort wird gegen die für den Benutzer gültige Passwortrichtlinie geprüft.

Authentifizierungsoptionen

DirX Identity Passwort Reset unterstützt die folgenden alternativen Authentifizierungsoptionen:

- Authentifizierung mittels Smartcard
- Authentifizierung mittels Beantwortung von Sicherheitsfragen
- Mobiles OTP (One-Time Passwort)

Wenn Sicherheitsfragen als Alternative zur Authentifizierung genutzt werden, muss ein Benutzer zuerst einen Satz von persönlichen Sicherheitsfragen festlegen, bevor das

Self-Service Passwort Reset genutzt werden kann. Die Anzahl der festzulegenden Fragen und zugehörigen Antworten ist flexibel und hängt von der Sicherheitsrichtlinie der Organisation ab.

Passwort Reset mit Web Center

Auf das Passwort Reset Web Center kann über einen Standard Web Browser zugegriffen werden. Im Fall eines vergessenen Passworts können sich Benutzer möglicherweise nicht mehr am System anmelden, um den Webbrowser zu nutzen. In diesem Fall muss ein sogenanntes Kiosk-System oder der Browser auf dem System eines Kollegen genutzt werden.

Über die Web Center Benutzeroberfläche können Benutzer

- ihre eigenen Passwörter ändern
- nach der Authentifizierung mittels Sicherheitsfragen vergessene Passwörter zurücksetzen
- den persönlichen Satz von Sicherheitsfragen verwalten
- sich bei der erstmaligen Nutzung registrieren und mit ihrem Active Directory Passwort anmelden sowie ihre Sicherheitsfragen und zugehörigen Antworten festlegen
- ihre Passwörter für eine Untermenge ihrer Accounts, die sie in den Zielsystemen haben, ändern oder zurücksetzen
- den Status der Passwortänderungen (anhängig, erfolgreich, nicht erfolgreich) für die gewählten Accounts anzeigen lassen.

Passwort Reset mit DirX Password Reset Client

Der DirX Password Reset Client (DXPRC) ist ein Windows Client, der auf einem Microsoft Windows System des Benutzers eingerichtet werden muss.

Der DXPRC kann genutzt werden, bevor man sich bei Windows anmeldet (nach Strg-Alt-Entf). Dies geschieht über eine zusätzliche Option auf dem Login Screen. Diese Möglichkeit bietet den Vorteil, dass das Zurücksetzen des Passworts direkt von der Workstation des Benutzers aus durchgeführt werden kann.

Der DirX Password Reset Client (DXPRC) bietet eine konfigurierbare Installationsoption zur Auswahl der alternativen Authentifizierungsmethoden an:

- Authentifizierung mittels Smartcard
- Authentifizierung mittels Beantwortung von Sicherheitsfragen
- Mobiles OTP
- Jede Kombination der vorgehend genannten Methoden

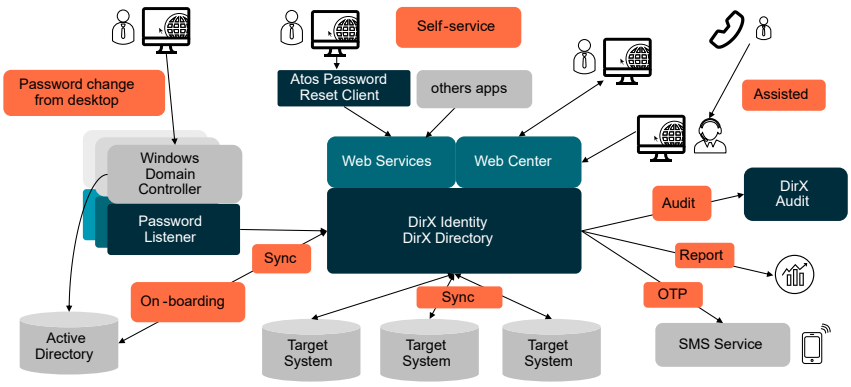

Abbildung 3 - DirX Identity Passwortmanagement Architektur

Unterstütztes Passwort Reset

Für das Service-Desk-Personal stellt DirX Identity erweiterte Funktionen zur Verfügung. Service-Desk-Mitarbeiter können über die Web Center Benutzerschnittstelle

- Passwörter von Benutzern auf Anfrage zurücksetzen. Sie können die Benutzer mittels ihrer Attribute und Sicherheitsfragen authentifizieren.
- Passwortrichtlinien anlegen und verwalten: Diese steuern, wie Passwörter in einem Unternehmen angelegt und administriert werden, zum Beispiel die Passwortlänge und-komplexität, das maximale Alter von Passwörtern oder die erneute Nutzung bereits früher verwendeter Passwörter.
- Reports über Passwortänderungen und Passwortrücksetzungen erzeugen.

Ablauf von Passwörtern

DirX Identity Passwort Management weist optional die Benutzer darauf hin, ihre Passwörter zu ändern, bevor ihr Ablaufdatum erreicht ist. Dies geschieht durch regelmäßige Überprüfung der Passwörter auf ein bevorstehendes Ablaufdatum und durch Benachrichtigung der betroffenen Benutzer mittels E-Mail. Die Anzahl der Benachrichtigungen ist konfigurierbar.

Benutzer-Registrierung

Erstmalige Benutzer registrieren sich beim System mit ihrem Active Directory Account sowie durch die Auswahl von Sicherheitsfragen und deren Beantwortung über die Web Center Benutzerschnittstelle. Die Administratoren können konfigurieren, ob Benutzer ihre eigenen Sicherheitsfragen festlegen oder sie nur aus einer Liste vordefinierter Fragen auswählen können.

Onboarding/Offboarding von Benutzern

Sowohl das Onboarding von Benutzern, d.h. das initiale Laden der Benutzer sowie das Hinzufügen neuer Benutzer in das DirX Identity System als auch das Offboarding, d.h. das Löschen von Benutzern aus dem System, wird mittels der Identity Management Funktionalität von DirX Identity durchgeführt. Synchronisations-Services sorgen für einen korrekten und aktuellen Datenbestand der Identitäten, die die Passwort Reset Funktionalität nutzen dürfen.

Windows Password Listener

Der Windows Password Listener erkennt die Änderungen von Benutzerpasswörtern in einer Windows Domäne, verschlüsselt die Information und erzeugt Passwortänderungs-Events. Diese Events steuern den Event Manager und die zugehörigen Passwortänderungs-Workflows, um die geänderten Passwörter in die angeschlossenen Zielsysteme zu synchronisieren.

Der Windows Password Listener ist geeignet für unterstützte Microsoft Windows Server Systeme.

Passwortsynchronisation

Das DirX Identity Passwortmanagement ermöglicht es den Benutzern, nur ein einziges Passwort pflegen zu müssen, das automatisch mit Microsoft Active Directory und optional

mit anderen relevanten IT-Systemen, in denen der Benutzer Accounts hat, synchronisiert wird.

Der Event-gesteuerte, Real-Time Passwortsynchronisations-Service sorgt dafür, dass Passwortänderungen, die über die Web Center Oberfläche oder im Windows System durchgeführt wurden, sofort mit den zugehörigen Benutzer-Accounts in den entsprechenden Zielsystemen synchronisiert werden. Für die Passwortsynchronisation werden vorkonfigurierte Passwortsynchronisations-Workflows zur Verfügung gestellt.

Passwortrichtlinien-Management

Administratoren oder Service-Desk-Mitarbeiter können Passwortrichtlinien festlegen, die mit den Passwortrichtlinien der Anwendungen im Unternehmen im Einklang stehen. Es können Passwortlängen und komplexität, Gültigkeitsdauer, Historie von Passwörtern, das Verhalten nach fehlgeschlagenen Login-Versuchen oder die erneute Nutzung von Passwörtern nach deren Ablauf festgelegt werden.

Passwortmanagement für privilegierte Accounts

Zusätzlich zu Accounts, die genau einem festgelegten Benutzer zugeordnet sind, wird in Zielsystemen typischerweise eine kleine Anzahl von privilegierten Accounts angelegt, die für die Verwaltung der Zielsysteme berechtigt sind. Solche Accounts, zum Beispiel der Root-Account in Unix-Systemen, können in den Zielsystemen kritische Aktionen mit hohen Sicherheitsrisiken durchführen. Privilegierte Accounts sind nicht einem spezifischen Benutzer zugeordnet. Eine Reihe von Personen kann sie parallel benutzen.

DirX Identity stellt Mittel zur Steuerung und zur Auditierung der von privilegierten Accounts genutzten Passwörter zur Verfügung:

- Benutzer, denen ein privilegierter Account zugewiesen wurde, können das Passwort in Klartext lesen, um ein Login durchführen zu können.
- Ebenso haben sie die Berechtigung, das Passwort privilegierter Accounts zu löschen.
- uWird einem Benutzer ein privilegierter Account entzogen, wird automatisch dessen Passwort geändert.
- Alternativ kann festgelegt werden, dass bei der Zuweisung eines Benutzers zu einem privilegierten Account die Zertifikate des Benutzers zum Account kopiert werden. Dies ermöglicht im Zielsystem die Authentifizierung mittels Zertifikats.
- DirX Identity ändert automatisch die abgelaufenen Passwörter privilegierter Accounts.

Audit und Reports

Um Compliance-Anforderungen zu erfüllen und dies zu dokumentieren oder auch um Abrechnungen zu ermöglichen, führt DirX Identity Aufzeichnungen zu Passwort-bezogenen Aktionen mittels seiner Auditfunktionen durch. Zudem werden Standard-Reports zur Verfügung gestellt, wie zum Beispiel:

- Anzahl der für das Passwortmanagement registrierten Benutzer
- Benutzer mit all ihren Eigenschaften
- Benutzer mit einer zusammengefassten Passwortmanagement-Historie
- Benutzer mit Passwortmanagement
- Benutzer mit ihrer Passwortmanagement-Historie
- Benutzer mit Rollen-Hierarchie
- Benutzer ohne Rollen

Sowohl die Audit-Trails als auch die Reports sind konfigurierbar und kundenspezifisch anpassbar, um Kundenanforderungen bestmöglich erfüllen zu können.

Architektur

DirX Identity Passwortmanagement basiert auf den Kernfunktionen der Produkte DirX Identity und DirX Directory. Dabei dient DirX Directory als Datenhaltung sowohl für die Konfigurations- als auch für die Benutzerdaten. DirX Identity Passwortmanagement nutzt die Agenten und Konnektoren des Connectivity Frameworks von DirX Identity, um Passwort Reset und Synchronisation für die angeschlossenen Systeme zu implementieren. DirX Audit kann für die zentrale, sichere Speicherung, die Analyse und Korrelation sowie zum Review Passwort-bezogener Audit Logs eingesetzt werden.

DirX Identity

DirX Identity stellt eine umfassende, prozessgesteuerte, kundenspezifisch anpassbare, Cloud-fähige, skalierbare und hochverfügbare Identity Management Lösung für Unternehmen und Organisationen zur Verfügung. Es stellt Risiko-basierte Identity und Access Governance Funktionalität bereit, die nahtlos mit automatisiertem Provisioning integriert ist. Die Funktionalität umfasst Life-Cycle-Management für Benutzer und Rollen, plattformübergreifendes und regelbasiertes Provisioning in Echtzeit, Web-basierte Self-Service-Funktionen für Benutzer, delegierte Administration, Antrags-Workflows, Berechtigungsprüfung, Passwortmanagement, Metadirectory sowie Audit- und Report-Funktionalität.

DirX Directory

DirX Directory stellt einen standardkonformen, leistungsstarken, hochverfügbaren, sehr zuverlässigen und sicheren LDAP und X.500 Directory Server mit sehr hoher linearer Skalierbarkeit zur Verfügung. DirX Directory kann als Identity-Datenhaltung für Informationen über Mitarbeiter, Kunden, Geschäftspartner, Abonnenten von Diensten sowie über andere Teilnehmer von eBusiness-Verfahren dienen.

DirX Audit

DirX Audit bietet Auditoren, Sicherheitsbeauftragten und Administratoren analytischen Einblick und Transparenz in Identity und Access Management Prozesse. Mit historischen Identitätsdaten und aufgezeichneten Aktivitäten aus den Identity und Access Management Prozessen ermöglicht DirX Audit die Beantwortung der „Was, Wann, Wo, Wer und Warum“-Fragen bei Benutzerzugriffen und -berechtigungen. DirX Audit bietet historische Ansichten und Reports auf Identitätsdaten, ein grafisches Dashboard, einen Monitor für Identitäts-bezogene Aktivitäten und die Verwaltung von Jobs für die Reporterstellung. Mit seinen Analyse-Funktionen unterstützt DirX Audit Unternehmen und Organisationen bei der nachhaltigen Einhaltung von Compliance-Anforderungen und stellt Business Intelligence für die Identity und Access Management Prozesse bereit.

Sicherheit

Die Authentifizierungs- und Autorisierungsmechanismen des zugrundeliegenden LDAP Directories ermöglichen den Schutz von Attributen und Passwörtern. DirX Identity bietet zusätzliche Sicherheitseigenschaften:

- Alle Komponenten können optional im SSL/TLS-Modus arbeiten, wenn sie LDAP-Verbindungen

benutzen

- Der Datenaustausch über den Messaging Service kann verschlüsselt werden, um hohe Sicherheit bei dem Datentransfer über das Netzwerk zu ermöglichen.
- Passwörter, Sicherheitsfragen und die dazugehörigen Antworten können stark verschlüsselt im Identity Store gespeichert werden. DirX Identity sorgt dafür, dass das Log-ging und der Datentransfer bis an die Schnittstelle des angeschlossenen Zielsystems gesichert sind.

Passwort Reset as a Service

Zusätzlich zur Passwortmanagementfunktiona-lität, die mit dem Produkt DirX Identity zur Verfügung gestellt wird, bietet Eviden Passwort Reset as a Service an, um Endbenutzern eine einfache und schnelle Möglichkeit zur Verfü-gung zu stellen, ihre Passwörter zurückzusetzen oder ihre Accounts zu entsperren.

Passwort Reset as a Service kann angeboten werden als

- Shared Service
- Kundenspezifischer Service vom Eviden-Standort aus
- Kundenspezifischer Service am Kundenstandort

Die Eviden Passwort Reset Services werden sowohl für Microsoft Active Directory als auch optional für andere Umgebungen bereitgestellt.

Passwort Reset as a Service bietet eine Reihe zusätzlicher Vorteil für die Kunden:

- Hohe Agilität – schnelle Einsatzbereitschaft
- All-Inclusive Ansatz – vermeidet hohe Vorabinvestitionen in Hardware und Software – kein CAPEX
- Technologie-unabhängig – der Kunde kann sich auf die Funktionalität konzentrieren anstatt auf die Technologie
- Externer und interner Zugriff
- Mehrere Zielsysteme werden unterstützt
- Passwort Reset und Entsperren
- 24*7*365 verfügbar, zu jeder Zeit, an jedem Ort

Technische Voraussetzungen

Hardware

- Intel server platform für Microsoft Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

Speicherbedarf:

Hauptspeicher: mindestens 8 GB

Plattenspeicher: mindestens 4 GB plus Speicher für Daten

Software

- DirX Identity V9.0
- DirX Directory V8.9 oder neuer
- DirX Audit V7.1 oder neuer

Für DirX Identity Web Center/ Web Admin/Server Admin

- Mozilla Firefox 78 oder neuer
- Google Chrome 96 oder neuer
- Microsoft Edge 96 oder neuer

Für DirX Password Reset Client (DXPRC)

- Microsoft Windows 10 64-bit
- Microsoft Windows 11 64-bitUser interface

Benutzeroberfläche

- Englisch
- Web Center: Englisch / Deutsch / kundenspezifisch anpassbar
- DXPRC: Englisch / Deutsch / kundenspezifisch anpassbar

Dokumentation

- DirX Identity Dokumentation
- DirX Directory Dokumentation

DirX Produkt-Suite

Die DirX Produkt-Suite bietet die Basis für ein vollständig integriertes Identity- und Access-Management; zur DirX-Produktfamilie gehören folgende Produkte, die separat bestellt werden können.

DirX Identity

DirX Identity stellt eine umfassende, prozessgesteuerte, kundenspezifisch anpassbare, Cloud-fähige, skalierbare und hochverfügbare Identity Management Lösung für Unternehmen und Organisationen zur Verfügung. Es stellt übergreifende, Risiko-basierte Identity und Access Governance Funktionalität bereit, die nahtlos mit automatisiertem Provisioning integriert ist. Die Funktionalität umfasst Life-Cycle-Management für Benutzer und Rollen, plattformübergreifendes und regelbasiertes Provisioning in Echtzeit, Web-basierte Self-Service-Funktionen für Benutzer, delegierte Administration, Antrags-Workflows, Zugriffszertifizierungen, Passwortmanagement, Metadirectory sowie Audit- und Report-Funktionalität.

DirX Directory

DirX Directory bietet einen standardkonformen, hochperformanten, hochverfügbaren, hochzuverlässigen, hochskalierbaren und sicheren LDAP- und X.500-Directory-Server und LDAP-Proxy mit sehr hoher linearer Skalierbarkeit. DirX Directory kann als Identitätsspeicher für Mitarbeiter, Kunden, Partner, Abonnenten und andere IoT-Einheiten dienen. Es kann auch als Bereitstellungs-, Zugriffsverwaltungs- und Metaverzeichnis-Repository dienen, um einen einzigen Zugriffspunkt auf die Informationen in unterschiedlichen und heterogenen Verzeichnissen bereitzustellen, die in einem Unternehmensnetzwerk oder einer Cloud-Umgebung für die Benutzerverwaltung und -bereitstellung verfügbar sind.

DirX Access

DirX Access ist eine umfassende, Cloud-fähige, skalierbare und hochverfügbare Zugriffsverwaltungslösung, die richtlinien- und risikobasierte Authentifizierung, Autorisierung basierend auf XACML und Föderation für Webanwendungen und -dienste bietet. DirX Access bietet Single Sign-On, vielseitige Authentifizierung einschließlich FIDO, Identitätsföderation basierend auf SAML, OAuth und OpenID Connect, Just-in-Time-Bereitstellung, Berechtigungsverwaltung und Richtliniendurchsetzung für Anwendungen und Dienste in der Cloud oder vor Ort.

DirX Audit

DirX Audit bietet Auditoren, Security-Compliance-Beauftragten und Audit-Administratoren analytische Einblicke und Transparenz für Identität und Zugriff. Basierend auf historischen Identitätsdaten und aufgezeichneten Ereignissen aus den Identitäts- und Zugriffsverwaltungsprozessen ermöglicht DirX Audit die Beantwortung der „Was, Wann, Wo, Wer und Warum"-Fragen zu Benutzerzugriff und Berechtigungen. DirX Audit bietet historische Ansichten und Berichte zu Identitätsdaten, ein grafisches Dashboard mit Drilldown zu einzelnen Ereignissen, einen Monitor zum Filtern, Analysieren, Korrelieren und Überprüfen von identitätsbezogenen Ereignissen und eine Auftragsverwaltung für die Berichterstellung. Mit seinen analytischen Funktionen unterstützt DirX Audit Unternehmen und Organisationen dabei, eine nachhaltige Compliance sicherzustellen und Business Intelligence für die risikobasierten Identity- und Access-Management-Prozesse bereitzustellen.

Connect with us

eviden.com