Nahtloser Zugriff auf Anwendungen mit einer leicht zu implementierenden Lösung

Tivoli software

IBM Tivoli Access Manager for Enterprise Single Sign-On

Highlights

- Arbeitserleichterung durch nicht mehr notwendiges Einprägen und Verwalten von Benutzernamen und Passwörtern
- Mehr Sicherheit durch die Vermeidung von nachlässigem Verhalten beim Umgang mit Passwörtern
- Geringere Help-Desk-Kosten durch das Reduzieren der telefonischen Anfragen zum Zurücksetzen des Passworts
- Wichtiger Beitrag für ein umfassendes Identitätsmanagement und für Compliance-Initiativen durch die Bereitstellung und Verwaltung von Benutzerberechtigungen in enger Kooperation mit IBM Tivoli Identity Manager ohne die Beteiligung des Benutzers
- Weitere Differenzierung der IBM Tivoli Access Manager for e-business-Autorisierungen und -Nutzungsrechte für Webanwendungen durch einmalige Anmeldung (Single Sign-on, SSO) am Client
- Erweiterung der grundlegenden Funktionen durch Adapter für Selbstbedienungsterminals und gemeinsam genutzte Workstations, durch Umgebungen mit erweiterter Authentifizierung und Mehrfachauthentifizierung sowie durch die automatisierte Bereitstellung und Zurücksetzung von Desktop-Passwörtern
- Einsatz von Prüf- und Berichtsfunktionen zur Unterstützung der Einhaltung von Datenschutz- und Sicherheitsvereinbarungen

Keine Passwortprobleme mehr dank einer bewährten SSO-Lösung

Die Komplexität und Anzahl der täglich anfallenden Anmeldungen sind für die Mitarbeiter in zunehmendem Maße eine Quelle der Frustration und führen zu deutlichen Produktivitätsverlusten. In den meisten Unternehmen müssen sich die Mitarbeiter zwischen fünf und 30 verschiedenen Passwörtern einprägen, von denen viele in einem Abstand von 30 Tagen geändert werden müssen. Der Zeitaufwand für Eingabe, Ändern, Notieren, Vergessen und Zurücksetzen eines einzelnen Passworts mag nicht ins Gewicht fallen, aber diese Aktionen werden wiederholt ausgeführt und beanspruchen in ihrer Gesamtheit einen erheblichen Teil der Arbeitszeit Ihrer Mitarbeiter. Hinzu kommt, dass Mitarbeiter, die ihr Passwort vergessen haben und sich folglich nicht anmelden können, in dieser Zeit weder ihren Aufgaben nachkommen, noch Umsätze für das Unternehmen erwirtschaften.

Der nachlässige Umgang der Mitarbeiter mit ihren Passwörtern zählt heute zu den größten Sicherheitslücken in Unternehmen. Als Passwörter werden oft so offensichtliche Wörter wie „Passwort“ gewählt, sie werden an allgemein zugänglichen Orten notiert und von mehreren Kollegen genutzt.

Unternehmen brauchen heute eine Lösung, die Ihnen die einfache Implementierung der Enterprise Single Sign-on-Technologie (ESSO) ermöglicht, damit sie den Benutzerkomfort maximieren, die Produktivität steigern und die Sicherheit optimieren können. Aus diesem Grund ist IBM Tivoli Access Manager for Enterprise Single Sign-On ein so wertvolles Geschäftstool. Bei Tivoli Access Manager for Enterprise Single Sign-On – der führenden ESSO-Lösung von Passlogix – authentifizieren sich die Mitarbeiter nur einmal. Anschließend erkennt und reagiert die Software auf alle passwortbe-

zogenen Abfragen und automatisiert alle anfallenden Passwortmanagementaufgaben der Mitarbeiter. Dazu zählen:

- *Anmeldung*
- *Wahl des Passworts*
- *Änderung des Passworts*
- *Zurücksetzen des Passworts*

Ob Sie eine strikte Authentifizierung implementieren, Konformitätsanforderungen umsetzen, eine unternehmensweite Identitätsmanagementlösung einführen oder einfach nur die Anforderungen einer bestimmten Benutzergruppe in Bezug auf die Anmeldung angehen – die Tivoli Access Manager for Enterprise Single Sign-On-Suite bietet Ihnen Unterstützung bei allen geschäftlichen und technischen Anforderungen. Tivoli Access Manager for Enterprise Sign-On stellt Ihnen Single Sign-On für alle Ihre Anwendungen bereit:

- *Microsoft® Windows®-Anwendungen*
- *Client/Server-Anwendungen*
- *Webanwendungen*
- *Java™-Anwendungen*
- *Host-Emulatoren, z. B. IBM AS/400 (5250), IBM OS/390 (3270) und UNIX® (Telnet)*
- *Unternehmensintern entwickelte Anwendungen*
- *Hostgestützte Mainframeanwendungen*

Sichere Verwaltung von Passwörtern
Mit der automatischen Verwaltung der Passwörter minimiert Tivoli Access Manager for Enterprise Single Sign-On das Sicherheitsrisiko, das entsteht, wenn Mitarbeiter ihre Passwörter selbst wählen und sie entweder auf Papier notieren oder elektronisch speichern.

Die Software unterstützt Sie außerdem bei der Umsetzung strikter Passwortrichtlinien – auch bei Anwendungen, die selbst keine solchen Richtlinien erfordern. Sie können die maximale und minimale Länge der Passwörter festlegen, den Gebrauch von alphabetischen, numerischen sowie wiederholten und Sonderzeichen zulassen oder beschränken, Regeln für die Groß- und Kleinschreibung sowie für Anfangs- und Endzeichen aufstellen, das regelmäßige Ändern von Passwörtern erzwingen usw.

Bei der Interaktion mit den vielen verschiedenen Anwendungen, Websites, Mainframesystemen und Netzwerken innerhalb Ihres Unternehmens kann Tivoli Access Manager for Enterprise Single Sign-On auch Passwortänderungen feststellen oder auslösen. Die Software kann eine aktive Beteiligung der Mitarbeiter am Generieren oder Bereitstellen der Passwörter sowie deren Einprägen überflüssig machen (ggf. mit Hilfe von entsprechenden Kanälen zur Vergabe von Passwörtern).

Zum Schutz der Passwörter und der dazugehörigen Daten unabhängig vom jeweiligen Standort – in Ihrer Verzeichnisstruktur oder Datenbank, bei der Übergabe vom Verzeichnis zum Client, im lokalen Plattencache und im Hauptspeicher des Clients – nutzt die Software einige der striktesten verfügbaren Verschlüsselungen, z. B. Triple Data Encryption Standard-(Triple DES)- und Advanced Encryption Standard-(AES)-Algorithmen. Auf Grund der Konformität der Software mit dem Federal Information Processing Standard (FIPS) 140-2 können Finanzinstitute und Regierungsbehörden sowie Unternehmen aus den Bereichen Gesundheitswesen usw. zudem die strengen Datenschutz- und Sicherheitsbestimmungen für ihre Unternehmensaktivitäten einhalten.

Schnelligkeit und Effizienz
Sowohl in Client/Server- als auch in Terminal-Serviceumgebungen bietet Tivoli Access Manager for Enterprise Single Sign-On einen Hochgeschwindigkeits-Sign-on bei gleichzeitiger geringer Ressourcenbeanspruchung. Das Programm ermöglicht eine Anmeldung an allen, auch branchenpezifischen, Anwendungen – in meist nur Sekundenbruchteilen.

Hinzu kommt, dass die Software einen äußerst geringen Speicherbedarf hat – in der Regel weniger als 2,5 MB – und auf die vorhandenen Ressourcen ereignisbasiert zugreift, um die Belastung von Client und Netzwerk möglichst gering zu halten. Dies ist besonders bei serverseitigen Implementierungen von Datenverarbeitungssoftware wie z. B. in Citrix, Sun und Windows Terminal Services-Umgebungen entscheidend.

Einfache Implementierung und Verwaltung

Tivoli Access Manager for Enterprise Single Sign-On unterstützt Sie beim Implementieren und Verwalten von Software durch die Bereitstellung einer stabilen, intuitiven, über einen Assistenten gesteuerten grafischen Administrationskonsole und einer vielseitigen Verzeichnisintegration.

Ihr Netzadministrator kann die clientseitige Software mit Hilfe von IBM Tivoli Configuration Manager oder anderen Softwareverteilungssystemen von einem zentralen Standort aus implementieren, ohne zusätzliche Hardware oder Software im Netzwerk zu installieren und ohne eine Beteiligung der Mitarbeiter am Installationsprozess.

Die Administrationskonsole vereinfacht die Verwaltung, da Anwendungen automatisch erkannt und konfiguriert werden. So erfolgt der Sign-on mit minimalem Aufwand des Administrators. Von der Administrationskonsole aus – verfügbar entweder über eine .NET-basierte Konsole oder ein Microsoft Management Console (MMC)-Snap-in – führen Point-and-click-Wizards die Administratoren durch alle Konfigurations-, Implementierungs- und Verwaltungsaufgaben. Tivoli Access Manager for Enterprise Single Sign-On wird für die gängigsten Anwendungen bereits vorkonfiguriert geliefert. Darüber hinaus verfügt die Administrationskonsole über eine integrierte Informationsbeschaffung, so dass die Software bisher unbekannter Anwendungen automatisch konfiguriert werden kann – ohne dass der Administrator zusätzliche Scripts oder kostenintensive Konnektoren entwickeln oder Änderungen an den Zielanwendungen und -systemen vornehmen muss.

Ist die Software einmal betriebsbereit, können die Benutzer mit der Administrationskonsole einzeln, nach Rolle oder nach Gruppe verwaltet werden. Die Konsole führt Sie auch durch den Prozess zur Festlegung von Passwortrichtlinien, Systemregeln, Kenndaten der Benutzerschnittstelle, Parametern für eine erneute Authentifizierung und weiteren Optionen.

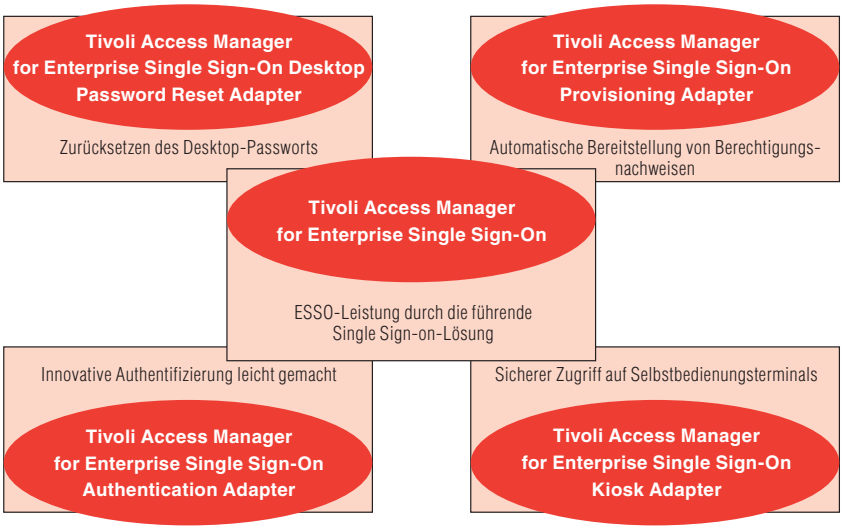
Zur Vereinfachung der Ereignisberichte ermöglicht die Administrationskonsole die Steuerung der Protokollierung von Benutzerereignissen und -aktivitäten wie Anmeldung, Passwortänderung, Authentifizierung, Einführung oder Änderung von Richtlinien usw. Tivoli Access Manager for Enterprise Single Sign-On kann Ereignisse in Form einer XML-Datei, im Windows Event Viewer oder – bei Verwendung der Ereignis-API (Anwendungsprogrammierschnittstelle) – mit Hilfe einer beliebigen anderen Methode protokollieren. Im Anschluss können Sie auf den Ereignissen und der Benutzeraktivität basierende Prüf- und Nutzungsberichte erstellen.

Nutzung vorhandener Verzeichnisressourcen

Tivoli Access Manager for Enterprise Single Sign-On speichert Benutzerberechtigungen sowie eigene Systemeinstellungen und Konfigurationsdaten in einer Auswahl von unterstützten Lightweight Directory Access Protocol-(LDAP)-Verzeichnissen, in einer von mehreren Structured Query Language-(SQL)-Datenbanken, einschließlich IBM DB2 Universal Database, oder in anderen Repositorys und Speichereinheiten. Ein LDAP-Verzeichnis oder ein anderes unternehmensweites Repository ist zwar nicht zwingend erforderlich, aber die meisten Kunden, die mehr als nur einer Handvoll Mitarbeitern Unterstützung bieten müssen, profitieren von der zentralen Steuerung und Berichterstellung, die ein unternehmensweites Repository wie LDAP bereitstellt.

Da die Software das bereits bei Ihnen installierte Repository verwendet, gestaltet sich die Konfiguration des zentralen Repositorys oder Verzeichnisses sehr einfach. Die Software unterstützt die folgenden Repositorys (vollständige Unterstützung, falls nicht anders angegeben):

- *LDAP-Verzeichnisse, Version 2/ Version 3, z. B. IBM Tivoli Directory Server, Sun Java System Directory Server, Novell eDirectory, Oracle Internet Directory*
- *Microsoft Active Directory® und Active Directory Application Mode (ADAM)*
- *OpenLDAP (nur Basisunterstützung)*
- *Critical Path (nur Basisunterstützung)*
- *DB2 Universal Database*
- *Microsoft SQL Server*
- *Oracle 9i- und Oracle 10g-Datenbanken*
- *Weitere Repositorys und Speichereinheiten (bei Verwendung der Synchronisations-API)*



Tivoli Access Manager for Enterprise Single Sign-On besteht aus dem Basisprodukt und vier Zusatzadaptern, die Ihnen unterschiedliche inkrementelle Funktionen zur Verfügung stellen, um die spezifischen Anforderungen Ihrer Umgebung zu erfüllen.

Höhere Wertschöpfung mit der Basislösung

Tivoli Access Manager for Enterprise Single Sign-On dient als Basis mehrerer, separat erhältlicher Adapter und bietet Ihnen so die Flexibilität, die Anforderungen unterschiedlicher Benutzergruppen zu erfüllen, ohne die Kosten für die Migration zu einer anderen technologischen Basis tragen zu müssen. Auf Grund der unterschiedlichen Adapter kann Tivoli Access Manager for Enterprise Single Sign-On viele zusätzliche Szenarios unterstützen, vom Zurücksetzen der Desktop-Passwörter bis hin zur Unterstützung von Mehrfach-Authentifizierung und strikter Authentifizierung. Jeder Adapter stellt Point-and-click-Administrationskonsolen zur Vereinfachung der Konfigurations-, Implementierungs- und Verwaltungsaufgaben sowie Prüf- und Berichterstellungsfunktionen zur Reduzierung des Zeit- und Kostenaufwands für die Einhaltung von Vorschriften zur Verfügung.

Beispiele für Tivoli Access Manager for Enterprise Single Sign-On-Adapter:

- *IBM Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter. Ermöglicht Benutzern das Zurücksetzen von Windows-Passwörtern von gesperrten Workstations aus und verringert so die Kosten für die Anrufe beim Help-Desk auf Grund von Passwortproblemen.*
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter. Ermöglicht die strikte Authentifizierung mit Hilfe von Tokens, Smart Cards, berührungslosen Ausweisen und Biometrie und bietet flexible Authentifizierungsoptionen, z. B. das Einsetzen strikter Authentifizierungsmechanismen für den Zugriff auf ausgewählte, kritische Ressourcen.*
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter. Automatisiert den Bereitstellungsprozess der Berechtigungsnachweise für die Benutzer, damit Identitätsmanagementlösungen wie Tivoli Identity Manager die Bereitstellung und Verwaltung der Berechtigungsnachweise ohne Beteiligung der Benutzer abwickeln können.*
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter. Bietet eine sichere und praktische Umgebung mit einer Mehrbenutzerworkstation und einem Selbstbedienungsterminal auf der Basis von Funktionen für das automatische Beenden inaktiver Sitzungen und Anwendungen sowie für ein schnelles Switching zwischen Benutzern.*

Eigenständiges Zurücksetzen von Windows-Passwörtern zur Reduzierung der Help-Desk-Kosten:
Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter
Bei Unternehmen mit Systemen, die durch mehrere Passwörter geschützt sind, wird ein großer Teil der Anrufe am Help-Desk von Mitarbeitern mit Passwortproblemen getätigt. Vor allem bei Großunternehmen können sich die damit verbundenen Kosten auf mehrere Millionen US-Dollar jährlich belaufen. Ganz abgesehen von der verlorenen Arbeitszeit der IT-Mitarbeiter, die statt dessen für Aufgaben mit sehr viel größerem geschäftlichen Nutzen hätte genutzt werden können.

Mit Tivoli Access Manager for Enterprise Single Sign-On erfolgt die Authentifizierung der Mitarbeiter ausschließlich über das Windows-Passwort; jeder Mitarbeiter muss sich also nur noch ein Windows-Passwort merken, um auf alle Anwendungen zugreifen zu können. Und was passiert, wenn Mitarbeiter ihr Windows-Desktop-Passwort vergessen? Um die in solchen Fällen üblichen Anrufe am Help-Desk zu vermeiden, ermöglicht der Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter den Mitarbeitern, ihr Windows-Passwort mit Hilfe eines einfachen Frage- und Antwortdialogs direkt von der gesperrten Workstation aus zurückzusetzen.

Administratoren geben über die intuitive webbasierte Konsole Fragetexte, Scoring-Werte und ein vertraulichkeitsbasiertes Scoring auf der Basis der unternehmensinternen Sicherheitsrichtlinien ein. Dabei können nach Bedarf Fragen hinzugefügt oder geändert werden, um die erforderlichen Sicherheitsstufen zu gewährleisten. Bei der Registrierung beantwortet der Benutzer die Fragen, die dann im Falle eines Zurücksetzens des Passworts in beliebiger Reihenfolge gestellt werden. Die Fragen und die verschlüsselten Registrierungsantworten können in einem Back-End-Repository gespeichert werden, um die Sicherheit der Antworten zu gewährleisten.

Einfache Verwaltung mehrerer Authentifikatoren:
Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter
Auf Grund der zunehmenden Bedeutung der Sicherheit suchen Unternehmen neben den herkömmlichen Passwörtern nach strikteren Methoden der Authentifizierung, z. B. Smart Cards, Biometrie, Näherungsschalter und Tokens. So kann ein Unternehmen beispielsweise Tokens für ferne Benutzer, Smart Cards für Benutzer im Unternehmen und Passwörter für Auftragnehmer einsetzen, die alle auf dieselben Anwendungen zugreifen.

Allerdings können diese Geräte vor allem solche Unternehmen vor große Herausforderungen bei der Integration und Administration stellen, die sich nicht auf einen bestimmten Anbieter oder eine bestimmte Technologie festlegen wollen. Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter lässt sich in verschiedene Authentifizierungsmethoden integrieren und bietet Unterstützung sowohl bei der Erstanmeldung als auch bei der Anforderung einer erneuten Authentifizierung.

In seiner Rolle als Vermittlungsschicht zwischen Authentifikatoren und Tivoli Access Manager for Enterprise Single Sign-On gibt der Authentifizierungs-Adapter Administratoren die Kontrolle darüber, auf welche Anwendungen Mitarbeiter mit welchen Authentifikatoren zugreifen können. Dieses hohe Maß an Kontrolle stellt sicher, dass der Zugriff der Benutzer auf Anwendungen in Einklang mit aktuellen Sicherheitsrichtlinien erfolgt. Unternehmen erzielen so ein bislang unerreichtes Maß an Datenschutz, das ihren Ansprüchen vollauf gerecht wird.

Schnelles Einrichten von Benutzern ohne Beeinträchtigung der Sicherheit:
Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter
Typischerweise erstellen Administratoren im Auftrag der Benutzer für jede Anwendung, jedes System und jede Plattform Accounts und Berechtigungsnachweise, die sie den Mitarbeitern dann in einer E-Mail oder sogar auf einem Stück Papier mitteilen. Neben einem Produktivitätsverlust führt das Verwalten der Berechtigungsnachweise für Anwendungen durch die Mitarbeiter nicht selten zu einer Beeinträchtigung der Sicherheit.

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter lässt Bereitstellungsinstruktionen von Identitätsmanagementsystemen wie IBM Tivoli Identity Manager zu und gibt Ihnen die Möglichkeit, vorab zufällig erzeugte Berechtigungsnachweise für Anwendungen für Ihre Mitarbeiter zu speichern. Dank der automatischen und direkten Bereitstellung von Berechtigungsnachweisen kommen Mitarbeiter nie mit ihren eigenen Benutzernamen und Passwörtern in Kontakt und müssen diese nicht einmal mehr kennen – selbst die Administratoren müssen nicht mehr zwangsläufig das Passwort für die Erstanmeldung an einer Anwendung kennen.

Neue Sicherheitsstufen für Selbstbedienungsterminals und Workstations:
Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter
Unternehmen, in denen viele Mitarbeiter Workstations gemeinsam benutzen, z. B. im Gesundheitswesen, interessieren sich zunehmend für Selbstbedienungsterminals und gemeinsam genutzte Workstations, die einen großvolumigen Datenzugriff bieten. Mit Hilfe von Selbstbedienungsterminals können Mitarbeiter während eines Arbeitstags mehrere Computer standortunabhängig nutzen, ohne jedes Mal zu einem bestimmten PC zurückkehren zu müssen, wenn sie auf verschiedene Anwendungen und IT-Ressourcen zugreifen müssen. Leider geschieht es viel zu oft, dass Benutzer den Arbeitsplatz verlassen, ohne sich abzumelden, und so sensible Daten einem potenziellen Sicherheitsrisiko aussetzen. Und eine unternehmensweite Überwachung stellt in vielen Fällen eine große Herausforderung dar, da die Selbstbedienungsterminals von der Sicherheit auf Anwendungsebene abhängig sind.

Der Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter verwaltet Berechtigungsnachweise, indem er die Benutzer auffordert, sich an einem LDAP-Verzeichnis oder einer anderen autoritativen Quelle anzumelden statt das System neu zu starten.

Nachdem die LDAP-Identität zweifelsfrei festgestellt wurde, greift das Selbstbedienungsterminal bei allen folgenden Single Sign-on-Aktivitäten auf die benutzerspezifischen Berechtigungsnachweise, Anwendungsdefinitionen und Einstellungen zurück.

Um zu verhindern, dass sensible Daten in falsche Hände gelangen, stellt der Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter den Benutzern von Selbstbedienungsterminals und gemeinsam genutzten Workstations Funktionen für das automatische Beenden inaktiver Sitzungen und Anwendungen zur Verfügung. Die Administratoren können festlegen, wie lange eine Sitzung inaktiv sein muss, bis sie ausgesetzt oder beendet wird.

Schließlich ermöglicht es der Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter auf Grund seiner Unabhängigkeit von der Windows-Anmeldung den Benutzern, schnell und sehr sicher zwischen verschiedenen Accounts zu wechseln.

Von zusätzlichem Nutzen sind die Adapter vor allem dann, wenn sie in Kombination eingesetzt werden. So werden z. B. die Adapter für Selbstbedienungsterminals und Authentifizierung in einer Reihe von Selbstbedienungsterminal-Umgebungen eingesetzt, um die Unterstützung von Selbstbedienungsterminals mit Hilfe berührungsloser Ausweise zu verbessern.

Funktionale Erweiterungen für vorhandene Tivoli Access Manager for e-business- und Tivoli Federated Identity Manager-Implementierungen
Viele Kunden haben die Vorteile der Tivoli Access Manager for e-business-Funktionen für Web-Single Sign-on und Zugriffsmanagement erkannt. Diese Software kann Bestandteil einer eigenständigen Unternehmenslösung oder auch einer unternehmensübergreifenden Lösung sein, in die Tivoli Access Manager for e-business und IBM Tivoli Federated Identity Manager nahtlos integriert sind.

Tivoli Access Manager for Enterprise Single Sign-On lässt sich ohne großen Aufwand in diese Umgebungen integrieren und stellt dann gemeinsam mit Tivoli Access Manager for e-business und Tivoli Federated Identity Manager eine ganze Reihe von kundenorientierten Funktionen bereit.

Flexible Unterstützung für Ihre Sicherheitsinitiativen und Ihre Umgebung

Das gesamte Portfolio an Tivoli Access Manager for Enterprise Single Sign-On-Software hilft Ihnen dabei, das Chaos zu beseitigen, das durch die ständigen Anfragen zur Eingabe oder Änderung von Mitarbeiter-IDs und -passwörtern entsteht. Die Basissoftware weitet die IBM Funktionen für das Identitäts- und Passwortmanagement aus und ergänzt sie um die Möglichkeit, auf IBM Lotus Notes-, SAP- und Windows-basierte Anwendungen mit nur einem Passwort zuzugreifen. Zusatzadapter erweitern die grundlegenden Leistungsmerkmale und bieten zusätzliche Unterstützung für das einfache Zurücksetzen der Desktop-Passwörter, für eine striktere und gleichzeitig flexiblere erweiterte Authentifizierung und Mehrfach-Authentifizierung, für die automatisierte Bereitstellung von Berechtigungsnachweisen sowie für Selbstbedienungsterminal-Umgebungen und Umgebungen mit gemeinsam genutzten Workstations. Die Tivoli Access Manager for Enterprise Single Sign-On-Architektur lässt sich problemlos konfigurieren, implementieren und verwalten. Zudem können Sie mit diesem Produkt Ihre Sicherheitsmanagementinvestitionen ausgesprochen nutzen- und gewinnbringend einsetzen.

Tivoli Access Manager for Enterprise Single Sign-On auf einen Blick

Clientagent-Anforderungen:
- Windows 2000, XP, 2003 Server
- 100MHz Intel® Pentium®-Prozessor und 64MB RAM

- Plattenspeicherplatz: ca. 2,5 MB für das installierte Programm mit Daten; die vollständige Installation erfordert ca. 7 MB; ca. 25 MB verfügbar auf der Festplatte für das Installationsprogramm

- Microsoft Internet Explorer 5.5 SP2 oder höher mit 128-Bit-Verschlüsselung

Administrationskonsole und Servervoraussetzungen:
- Windows 2000, XP, 2003 Server
- 100 MHz Pentium-kompatibler Prozessor und 64 MB RAM
- Microsoft .NET Framework 1.0
- Windows Installer 2.0 oder höher
- Plattenspeicherplatz: ca. 4 MB für das MSI-Installationsprogramm; ca. 31 MB für das EXE-Installationsprogramm; insgesamt ca. 15 MB für das installierte Programm mit Daten
- Verzeichnis: IBM Tivoli Directory Server, Microsoft Active Directory, Sun Java System Directory 5.1 oder höher, Novell eDirectory 8.5 oder ein höheres, mit LDAP, Version 2/Version 3 kompatibles Verzeichnis
- Datenbank: DB2 Universal Database, Microsoft SQL Server, Oracle usw.

Zusätzliche Anforderungen für Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter:
- Microsoft Internet Information Server 5.0 oder 6.0
- Microsoft .NET 1.1
- Microsoft Active Directory und ADAM
- Microsoft SQL

Zusätzliche Anforderungen für Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter:
- 120 MHz Pentium-Prozessor
- Plattenspeicherplatz: ca. 1 MB
- Internet Explorer 6.0 oder höher mit 128-Bit-Verschlüsselung
- Hinweis: Für strikte Authentifikatoren können eigene Systemvoraussetzungen gelten, die von den hier genannten abweichen können.
- Administrationskonsole und Servervoraussetzungen:
  - 400 MHz Pentium II-Prozessor und 96 MB RAM
  - Plattenspeicherplatz: ca. 1 MB

Zusätzliche Anforderungen für Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter:
- Plattenspeicherplatz für den Clientagent: ca. 1 MB
- Servervoraussetzungen:
  - Microsoft Internet Information Server 5.x oder 6.x (6.x empfohlen)
  - Verzeichnis: Microsoft Active Directory und ADAM, SunOne Directory oder IBM Tivoli Directory Server
  - Microsoft SQL Server 2000 oder Microsoft SQL Server 2000 Desktop Engine
  - Internet Explorer 6.0 oder höher mit 128-Bit-Verschlüsselung
  - Plattenspeicherplatz: ca. 3 MB
  - 900 MHz Pentium III-Prozessor und 512 MB RAM

Zusätzliche Anforderungen für Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter:
- Microsoft .NET 1.1
- 733 MHz Pentium III-Prozessor und 128 MB RAM
- Plattenspeicherplatz: ca. 3 MB
- Internet Explorer 6.0 mit 128-Bit-Verschlüsselung

Tivoli Software von IBM

Tivoli Software unterstützt Unternehmen bei der effizienten Verwaltung von IT-Ressourcen, -Aufgaben und -Prozessen, damit diese den sich ständig ändernden geschäftlichen Anforderungen gewachsen sind. Darüber hinaus ermöglicht die Software die flexible und reaktionsschnelle Verwaltung von IT-Services und senkt gleichzeitig die Kosten. Das IBM Tivoli Portfolio umfasst Softwarelösungen für die Bereiche Sicherheit, Compliance, Speicher, Leistung, Verfügbarkeit, Konfiguration, Prozesse und IT-Lebenszyklusverwaltung. Ergänzt wird das Portfolio durch die weltweit erstklassigen IBM Leistungen in den Bereichen Service, Support und Forschung.

Weitere Informationen

Wenn Sie mehr über Tivoli Access Manager for Enterprise Single Sign-On erfahren möchten und darüber, wie Sie mit diesem Produkt Ihr Passwortmanagement für IT-Administratoren und Benutzer einfacher gestalten können, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner – oder besuchen Sie uns unter:
ibm.com/tivoli

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Sxhweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Hergestellt in den USA
04-06

GC28-8426-00-GE