

## IBM Tivoli Access Manager for Enterprise Single Sign-On

---

### Highlights

---

- *Trägt zur Vereinfachung der Funktionalität für den Endbenutzer bei, da es nicht mehr notwendig ist, sich Benutzernamen und Kennwörter zu merken und diese zu verwalten, und da Anmeldung und Zugriff automatisiert werden*
- *Verbessert die Sicherheit, da der oft fehlerhafte Umgang mit Kennwörtern durch Endbenutzer vermieden wird*
- *Trägt zur Reduzierung von Help-Desk-Kosten im Zusammenhang mit Kennwörtern bei, da die Anzahl der Anrufe für das Zurücksetzen von Kennwörtern zurückgeht*
- *Ermöglicht umfassendes Sitzungsmanagement für Selbstbedienungsterminals, um die Sicherheit und Benutzerproduktivität zu verbessern*
- *Verbessert die Sicherheit durch eine breite Palette von Verfahren zur starken Authentifizierung*
- *Nutzt zentralisierte Prüfungs- und Berichtsfunktionen, um die Einhaltung von Vorschriften bezüglich Datenschutz und Sicherheit zu vereinfachen*
- *Ergänzt die fein-granulare Autorisierung und Berechtigungskontrolle für Webanwendungen von IBM Tivoli Access Manager for e-business, durch Erweiterung von Single Sign-on auf alle (auch nicht webbasierte) Anwendungen*
- *Ermöglicht umfassendes Identitäts- und Zugriffsmanagement durch den kombinierten Einsatz der zentralisierten Funktionen für das Identitätsmanagement von IBM Tivoli Identity Manager mit Enterprise Single Sign-on und Zugriffsautomation*

### **Mit einer bewährten Single Sign-on-Lösung Probleme mit Kennwörtern vermeiden – für alle Anwendungen, unabhängig von der Art des Zugriffs**

Die Anzahl der Anmeldungen, die Mitarbeiter tagtäglich durchführen müssen, und deren Komplexität steigen fortlaufend an. Dies führt zu Frustration und Produktivitätseinbußen.

In den meisten Unternehmen müssen sich Mitarbeiter zwischen fünf und dreißig Kennwörtern merken und diese alle 30 Tage ändern. Die vergeudete Zeit für das Eingeben, Ändern, Aufschreiben und Zurücksetzen von Kennwörtern, falls man eines vergisst, stellt einen erheblichen Produktivitätsverlust dar und bringt erhebliche Kosten für Anfragen an den IT-Help-Desk mit sich.

Mit IBM Tivoli Access Manager for Enterprise Single Sign-On – einer marktführenden Enterprise Single Sign-on-Lösung – authentifizieren sich Mitarbeiter nur ein einziges Mal und die Software erkennt und automatisiert daraufhin alle kennwortbezogenen Ereignisse für den Mitarbeiter, wie z. B.:

- *Anmeldung*
- *Kennwortauswahl*
- *Kennwortänderung*
- *Kennwortzurücksetzung*
- *Abmeldung*

Mit Tivoli Access Manager for Enterprise Single Sign-On können Sie für alle Microsoft® Windows®, Web-, Java™-, Mainframe- und Teletype-Anwendungen Single Sign-on bereitstellen. Die Lösung ist an allen wichtigen Netzzugriffspunkten, einschließlich Windows-Desktops, Laptops, gemeinsam genutzten Selbstbedienungsterminals, Citrix-Servern, Microsoft-Terminal-Servern und Webportalen, verfügbar. Durch diese umfassende Endpunktnutzung können Endbenutzer sich mit einem einzigen Kennwort von einem beliebigen Standort aus am Unternehmensnetzwerk anmelden und Single Sign-on-Zugriff auf sämtliche Anwendungen erhalten, selbst wenn der Zugriff von einem Internet-Café über einen Browser erfolgt.

#### **Kennwörter mit einem hohen Maß an Sicherheit verwalten**

Eine schlechte Auswahl und Handhabung von Kennwörtern durch Mitarbeiter stellt heute eine der größten Schwachstellen der Unternehmenssicherheit dar. Mitarbeiter schreiben ihre Kennwörter häufig an ungesicherten Stellen auf, verwenden leicht zu erratende Kennwörter und halten diese nicht geheim.

Tivoli Access Manager for Enterprise Single Sign-On kann so konfiguriert werden, dass Kennwortänderungen erkannt und für alle Anwendungen automatisch sichere Kennwörter generiert werden. Da die Lösung Single Sign-on mit diesen sicheren Kennwörtern unterstützt, müssen Benutzer sich diese Kennwörter nicht mehr merken und diese nicht mehr selbst verwalten. Dadurch steigt die Sicherheit und Produktivitätseinbußen werden vermieden.

Die Kennwörter und zugehörigen Daten werden mit AES (Advanced Encryption Standard), einen der mächtigsten Verschlüsselungsstandards auf dem Markt, verschlüsselt.

#### **Implementierung und Verwaltung vereinfachen**

Tivoli Access Manager for Enterprise Single Sign-On vereinfacht die Implementierung und die Verwaltung durch eine assistentengesteuerte grafische Webadministrationskonsole, AccessAdmin. Von dieser Konsole aus leiten Point-and-click-Assistenten durch sämtliche Aufgaben in den Bereichen Konfiguration, Implementierung und Administration.

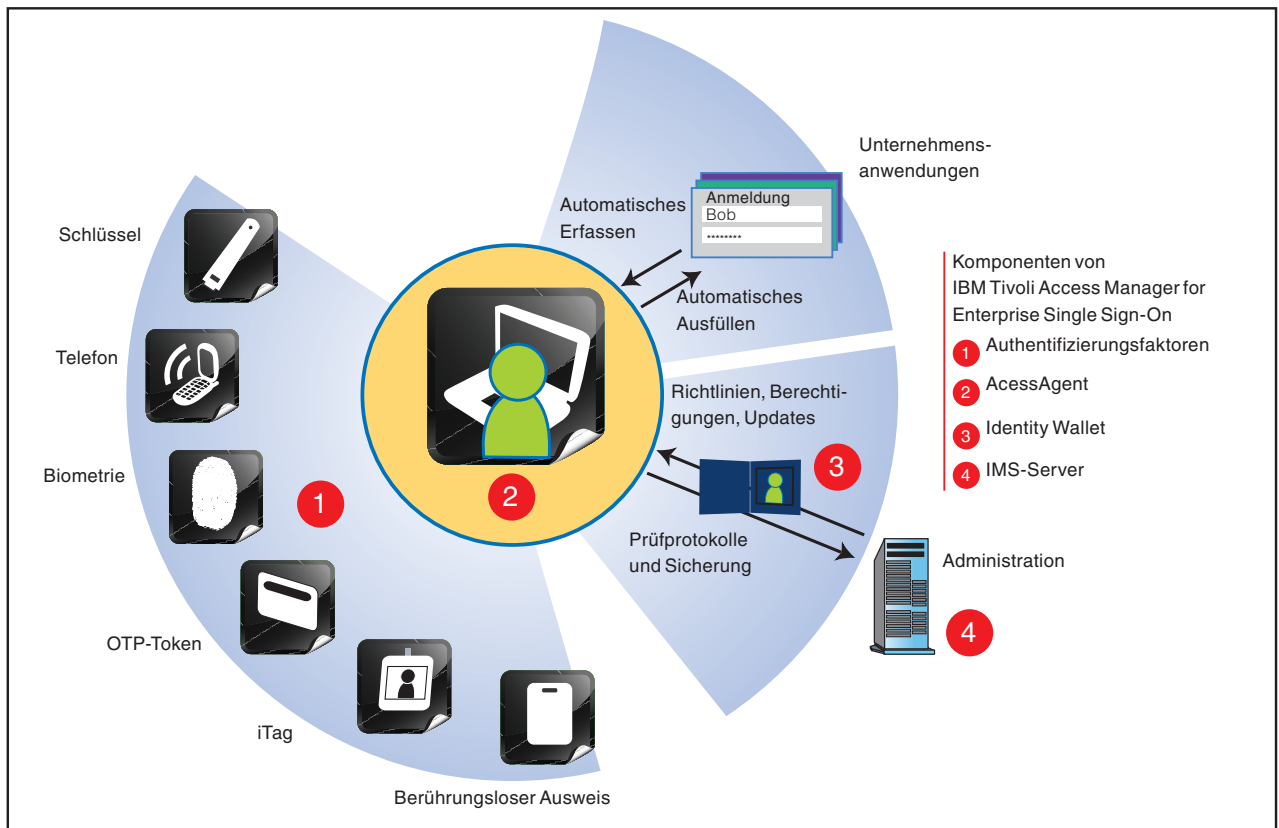
Tivoli Access Manager for Enterprise Single Sign-On wird für viele gängige Anwendungen vorkonfiguriert ausgeliefert. Administratoren können mit AccessStudio automatisch Zugriffsprofile für Anwendungen generieren, ohne dafür mühsam Skripte oder aufwändige Konnektoren erstellen oder Änderungen an den Zielanwendungen oder -systemen vornehmen zu müssen. AccessStudio Advanced bietet darüber hinaus eine visuelle Profilerstellung, eine grafisch orientierte Methode, Automation und Anmeldung für komplexe Anwendungen zu konfigurieren.

Die Software ist für eine zentrale Implementierung ausgelegt. Netzwerkadministratoren können die clientseitige Software von einer zentralen Position aus unter Verwendung von IBM Tivoli Configuration Manager oder anderen Softwareverteilungslösungen implementieren, ohne die Benutzer in den Installationsprozess einbinden zu müssen.

Sobald die Software betriebsbereit ist, können Administratoren über die Administrationskonsole Benutzer einzeln oder in Gruppen verwalten. AccessAdmin bietet zudem eine zentrale Konsole für die Einstellung von Kennwortrichtlinien, Systemregeln, Kenndaten von Benutzerschnittstellen, Parametern für die erneute Authentifizierung und anderen Optionen.

#### **Erstellung von Prüfprotokollen und Berichten über die Einhaltung von Vorschriften vereinfachen**

Damit die Einhaltung gesetzlicher Vorschriften sichergestellt ist, protokolliert Tivoli Access Manager for Enterprise Single Sign-On sämtliche Anmeldevorgänge von Benutzern und meldet diese zentral an den IMS-Server (Integrated Management System). Die resultierenden konsolidierten, benutzerbezogenen Protokolle enthalten die Metainformationen, die Administratoren zu den eigentlichen Anwendungsprotokollen leiten können, in denen sie ggf. detailliertere Analysen vornehmen können. Mit der Software können außerdem individuell angepasste Protokollierung, Echtzeitüberwachung und flexible Berichtsfunktionen realisiert werden.



### Vorhandene IT-Infrastrukturen und Verzeichnisressourcen nutzen

Für die Nutzung von Tivoli Access Manager for Enterprise Single Sign-On sind nur minimale Änderungen an der vorhandenen IT-Infrastruktur eines Unternehmens erforderlich, sie können aber auch ganz entfallen. Die Lösung arbeitet mit den verschiedensten Verzeichnisstrukturen, so ist vor der Implementierung keine kostspielige Verzeichniskonsolidierung erforderlich. Weder eine Erweiterung des Verzeichnisseschemas noch eine Replizierung von Verzeichnisdaten muss durchgeführt werden.

Die Lösung speichert Benutzerberechtigungen, Systemeinstellungen und Richtlinien in einer zentralen Datenbank und bietet Schnittstellen zu Unternehmensverzeichnissen, wie z. B. Active Directory, NT Domain Controller, Sun One LDAP, IBM Tivoli Directory Server und Novell eDirectory für Identitätsdaten.

### Sie stellt Kennwortzurücksetzung per Selbstbedienung bereit, um die Help-Desk-Kosten zu senken

Bei bis zu 80 Prozent aller Anrufe beim Help-Desk geht es um das Zurücksetzen von Kennwörtern. Die Kosten dafür können in Großunternehmen pro Jahr in die Millionen gehen. Wenn Mitarbeiter ihr Single Sign-on-Kennwort vergessen haben, können sie mit Tivoli Access Manager for Enterprise Single Sign-On das Kennwort nach einem einfachen Frage- und Antwortdialog von einer gesperrten Workstation aus direkt zurücksetzen.

### **Problemlos mehrere Arten von Authentifikatoren verwalten**

Da die Sicherheit in der heutigen Zeit immer wichtiger wird, suchen viele Unternehmen nach Authentifizierungsmethoden, die sicherer sind als Kennwörter. Tivoli Access Manager for Enterprise Single Sign-On unterstützt nicht nur eine breite Palette an Authentifikatoren, wie z. B. USB-Smart-Token, aktive und passive berührungslose Ausweise (Proximity Badge), Biometrie und Kennworttoken für einmaliges Anmelden (OTP-Token), sondern auch vorhandene Identifikationsmethoden, wie z. B. Werksausweise, Fotoausweise und Mobiltelefone, für die Authentifizierung. So können die Vertraulichkeit des Benutzers mit der Lösung genutzt und die Gesamtbetriebskosten reduziert werden.

### **Benutzeridentitäten zentral verwalten und gleichzeitig den Zugriff vereinfachen**

Administratoren erstellen normalerweise im Auftrag von Mitarbeitern Konten und Zugangsdaten für die einzelnen Anwendungen, Systeme oder Plattformen, die sie den Mitarbeitern dann per E-Mail oder auf einem Blatt Papier übermitteln. Die manuelle Erstellung und Verteilung von Zugangsdaten führt nicht nur zu Produktivitätseinbußen, sondern auch zu Sicherheitseinbußen, wenn Mitarbeiter Anwendungsberechtigungen selbst verwalten.

Tivoli Access Manager for Enterprise Single Sign-On kann problemlos mit führenden entwickelten Technologien für die Benutzereinrichtung und unternehmenseigenen Lösungen kombiniert werden, um durchgängiges und umfassendes Life-Cycle-Management für Identitäten bereitstellen zu können. Die Lösung nimmt Provisionierungsdaten von Identitätsmanagementsystemen wie Tivoli Identity Manager entgegen und ermöglicht die Vorabspeicherung von zufällig generierten Zugangsdaten in den Speichern für Berechtigungsnachweise von Mitarbeitern

Durch diesen kombinierten Einsatz von Lösungen für die Benutzerverwaltung ist sichergestellt, dass die Änderung eines Zugriffsrechts oder Kennworts durch das System automatisch mit dem Single Sign-on-System synchronisiert wird, so dass immer aktuelle Zugangsdaten zur Verfügung stehen. Wenn umgekehrt ein Benutzer aus den Systemen entfernt wird, stellt diese nahtlose Integration sicher, dass auch das Single Sign-on automatisch inaktiviert wird.

### **Neue Sicherheitsstufen bei Selbstbedienungsterminals und gemeinsam genutzten Workstations einrichten**

Schnellere Benutzerwechsel und Sitzungsmanagement sind in vielen Branchen (z. B. Fertigung, Gesundheitswesen, Lagerhaltung, Einzelhandel und Bildung) von entscheidender Bedeutung. Da Unternehmen immer mehr gemeinsam genutzte Workstations und Selbstbedienungsterminals implementieren, kann eine große Anzahl von Benutzern unabhängig von deren Standort durch Informationen navigieren und darauf zugreifen, ohne an ihren eigenen PC zurückkehren zu müssen. Gemeinsam genutzte Selbstbedienungsterminals stellen jedoch eine schwerwiegende Sicherheitsbedrohung dar, da Benutzer das Terminal häufig verlassen, ohne sich abzumelden, und damit vertrauliche Informationen unbefugtem Zugriff aussetzen. Jeder Versuch, die Sicherheit zu verbessern, eindeutige Benutzeranmeldungen umzusetzen und Vorschriften einzuhalten, kann zur Aussperrung von Benutzern von Workstations und damit zu Produktivitätseinbußen führen.

Mit Tivoli Access Manager for Enterprise Single Sign-On können Unternehmen durch eine große Auswahl an Funktionen für Sitzungsmanagement und schnellen Benutzerwechsel die Benutzerfreundlichkeit und die Informationssicherheit verbessern, um den Zugriffsanforderungen verschiedener Benutzergruppen gerecht zu werden. Mehrere Benutzer können einen Computer gleichzeitig nutzen und zwischen den Benutzern wechseln, ohne sich abmelden zu müssen oder ein Aussperren zu riskieren. Benutzer, die „mobile“ Desktops benötigen, können die Unterstützung für Roaming der Software nutzen. Sie können darüber hinaus ihre persönlichen Desktops beibehalten, während sie Workstations gemeinsam mit Kollegen nutzen.

Wenn ein Benutzer eine Sitzung verlässt, ohne sich abzumelden, kann Tivoli Access Manager for Enterprise Single Sign-On so konfiguriert werden, dass Richtlinien für Inaktivitätszeitlimits, wie z. B. konfigurierbare Bildschirmsperren, Richtlinien für die Abmeldung von Anwendungen, die ordnungsgemäße Abmeldung von allen Anwendungen etc., umgesetzt werden.

## Vorhandene Implementierungen von Tivoli Access Manager for e-business und IBM Tivoli Federated Identity Manager erweitern

Heute profitieren viele Kunden von den Vorteilen im Bereich Webzugriffsmanagement von Tivoli Access Manager for e-business. Diese Software kann Teil einer Lösung für ein Unternehmen oder Teil einer system- und unternehmensübergreifenden Lösung sein, in deren Rahmen Tivoli Access Manager for e-business und Tivoli Federated Identity Manager nahtlos integriert sind.

Tivoli Access Manager for Enterprise Single Sign-On kann problemlos in diese Umgebungen integriert werden, um die ganze Palette kundenorientierter Funktionen kombiniert mit Tivoli Access Manager for e-business und Tivoli Federated Identity Manager zu nutzen. Diese integrierte Lösungssuite ermöglicht den Einsatz von Single Sign-on innerhalb, außerhalb und zwischen Unternehmen, indem sie eine umfassende und durchgängige Single Sign-on-Lösung bietet, die andere Angebote nicht aufweisen.

### Dezentrale Single Sign-on-Architektur

Tivoli Access Manager for Enterprise Single Sign-On umfasst die folgenden Schlüsselkomponenten:

#### AccessAgent und Plug-ins:

Client Software, die für den Benutzer Single Sign-on und Sign-off, Authentifizierungsmanagement und Sitzungsmanagement übernimmt. Mit JavaScript- und VBScript-Plug-ins kann das Verhalten von AccessAgent angepasst werden.

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

### Clientagent – Voraussetzungen:

- Windows 2000 SP3, XP SP1, 2003 Server
- 600 MHz Intel® Pentium®-basierter Prozessor und 128 MB RAM
- Plattenspeicher: mindestens 100 MB freier Festplattenspeicherplatz
- Microsoft Internet Explorer 5.0 oder höher mit 128-Bit-Verschlüsselung
- Installation über Microsoft Installer (MSI) setzt Microsoft Windows Installer voraus

### Administrationskonsole und Server – Voraussetzungen:

- IMS-Server setzt Windows 2003 Server voraus
- AccessAdmin setzt Microsoft Internet Explorer 5.0 oder höher mit 128-Bit-Verschlüsselung voraus
- 1,2 GHz Pentium-kompatibler Prozessor und 256 MB RAM
- Plattenspeicher: mindestens 300 MB freier Festplattenspeicherplatz
- Verzeichnis: Active Directory, NT Domain Controller, Sun One LDAP, Tivoli Directory Server, Novell eDirectory oder sonstige LDAP
- Datenbank: DB2, Microsoft SQL Server und Oracle

**Identity Wallet:** Verschlüsselter Datenspeicher, in dem alle Logindaten eines Benutzers (also alle Benutzerkennungen, Kennwörter, Zertifikate, Schlüssel) sicher abgelegt sind. Das Identity Wallet navigiert zum Zugriffspunkt und speichert die persönlichen Identitätsprofile des Benutzers, einschließlich Anmeldeberechtigungen, Zertifikaten, Verschlüsselungsschlüsseln und Benutzerrichtlinien.

**IMS-Server:** Bietet zentrales Management von Benutzern und Richtlinien. Alle Richtlinien werden über den Access Agent zentral definiert und umgesetzt. Der IMS-Server bietet zudem eine umfassende Sicherung von Berechtigungen, Verlustmanagement, Prüfungen und Berichte über die Einhaltung von Vorschriften.

### Authentifizierungsfaktoren:

Unterstützt mehrere Faktoren für eine sichere Authentifizierung, wie z. B. USB Schlüssel, Kennworttoken für einmaliges Anmelden, Biometrie, Werksausweise und iTag.

### Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Access Manager for Enterprise Single Sign-On Ihr Unternehmen bei der Vereinfachung des Kennwortmanagements für Ihre IT-Administratoren und Endbenutzer unterstützt, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

[ibm.com/tivoli](http://ibm.com/tivoli)



## Tivoli-Software von IBM

Tivoli-Software bietet eine Service-Management-Plattform für Unternehmen, die dank ihrer Transparenz, Steuerung und Automation die Bereitstellung qualitativ hochwertiger Services ermöglicht. Transparenz bedeutet, dass Sie die Abläufe in Ihrem Unternehmen erkennen und nachvollziehen können. Steuerung steht für das effektive Management Ihrer Geschäftsabläufe, die Minimierung von Risiken und den Schutz Ihrer Unternehmensmarke. Automation erlaubt die Optimierung Ihres Unternehmens, die Senkung der Betriebskosten und die schnellere Bereitstellung neuer Services. Anders als das IT-orientierte Service-Management stellt Tivoli-Software eine gemeinsame Grundlage für das Management, die Integration und die Abstimmung von Business- und IT-Anforderungen bereit. Tivoli-Software ist dafür konzipiert, die dringendsten Service-Management-Anforderungen eines Unternehmens rasch zu erfüllen und das Unternehmen dabei zu unterstützen, proaktiv auf sich ändernde geschäftliche Anforderungen zu reagieren. Das Tivoli-Portfolio wird durch erstklassige IBM Services und Supportangebote sowie ein Netz aus aktiven IBM Business Partnern unterstützt. Tivoli-Kunden und -Business Partner können sich zudem an unabhängig geführten IBM Tivoli-Benutzergruppen weltweit beteiligen und dabei bewährte Verfahren austauschen. Weitere Informationen hierzu finden Sie unter:

[www.tivoli-ug.org](http://www.tivoli-ug.org)

IBM Deutschland GmbH  
Pascalstrasse 100  
70569 Stuttgart  
**ibm.com/de**

IBM Österreich  
Obere Donaustrasse 95  
1020 Wien  
**ibm.com/at**

IBM Schweiz  
Vulkanstrasse 106  
8010 Zürich  
**ibm.com/ch**

Die IBM Homepage finden Sie unter:

**ibm.com**

IBM, das IBM Logo, ibm.com und Tivoli sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter:

**ibm.com/legal/copytrade.shtml**

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder deren Tochtergesellschaften in den USA oder anderen Ländern.

Java und alle auf Java basierenden Marken sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicennamen können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Diese Veröffentlichung darf ohne schriftliche Genehmigung der IBM Corporation weder vervielfältigt noch übertragen werden.

Die Produktdaten wurden zum Datum ihrer ersten Veröffentlichung auf ihre Korrektheit überprüft. Die Produktdaten können von IBM jederzeit ohne vorherige Mitteilung geändert werden. Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

© Copyright IBM Corporation 2008  
Alle Rechte vorbehalten.

**TAKE BACK CONTROL WITH Tivoli.**

TID10298-DEDE-01