Tivoli software

IBM Tivoli Access Manager for Enterprise Single Sign-On

Highlights

- Help simplify the employee experience by eliminating the need to remember and manage user names and passwords
- Lessen poor end-user password behavior to help enhance security
- Help reduce password-related help-desk costs by lowering the number of password reset calls
- Address a key requirement of complete identity management and compliance initiatives by removing end-user involvement from provisioning and by managing the user credential process through tight integration with IBM Tivoli Identity Manager
- Enhance IBM Tivoli Access Manager for e-business fine-grained authorization and entitlements for Web applications, by fully addressing single sign-on at the client
- Extend base functionality through adapters for kiosks and shared workstations, step-up authentication and multiauthentication environments, automated provisioning and automated desktop password resets
- Leverage audit and reporting capabilities to facilitate compliance with privacy and security regulations

Cut down password headaches with a proven single sign-on solution

The complexity and number of logons employees must manage on a daily basis are increasing sources of frustration and lost productivity. In most organizations, employees must remember between 5 and 30 passwords and are required to change many of them as frequently as every 30 days. The time wasted entering, changing, writing down, forgetting and resetting passwords might be in small increments, but those actions are frequent and add up to a significant consumption of employee time. And when employees are locked out because they've forgotten their passwords, they cannot perform their jobs — or generate revenue for their companies.

Even more importantly, poor password selection and management by employees represents one of the biggest corporate security weaknesses today. Employees often write down their passwords in unsecured locations, use common words like "password" as their password and share their passwords with coworkers.

To help maximize convenience, enhance productivity and strengthen security, today's businesses need a solution that enables them to easily deploy enterprise single sign-on (ESSO). That's why IBM Tivoli® Access Manager for Enterprise Single Sign-On is such a valuable business tool. With Tivoli Access Manager for Enterprise Single Sign-On — the market-leading ESSO solution powered by Passlogix® —

employees authenticate once, and the software then detects and responds to all password-related sign-on events to automate every password management task for the employee, including:

- Logon.
- Password selection.
- Password change.
- Password reset.

Whether you are deploying strong authentication, dealing with compliance issues, implementing an enterprise-wide identity management solution or simply focusing on the sign-on challenges of a specific group of users, the Tivoli Access Manager for Enterprise Single Sign-On suite can support your business and technical requirements. Tivoli Access Manager for Enterprise Single Sign-On can help you deliver single sign-on for all your:

- Microsoft® Windows® applications.
- Client/server applications.
- Web applications.
- Java™ applications.
- Host emulators, including IBM AS/400® (5250), IBM OS/390® (3270) and UNIX® (telnet).
- In-house developed applications.
- Host-based mainframe applications.

Manage passwords in a security-rich fashion

Because it automatically manages passwords, Tivoli Access Manager for Enterprise Single Sign-On minimizes the security vulnerability created when employees select their own passwords, write them down on paper or store them electronically.

You can also use the software to help enforce strict password policies — even for applications that do not enforce strict password policies themselves. You can set policies for minimum and maximum length; allow or restrict alphabetical, numeric and special or repeated characters; establish rules for uppercase and lowercase as well as beginning and end characters; enforce requirements for changing passwords regularly; and more.

In its interactions with the variety of applications, Web sites, mainframe systems and networks across your enterprise, Tivoli Access Manager for Enterprise Single Sign-On can also detect or trigger password changes. The software can eliminate employee involvement in generating, supplying or remembering passwords (with appropriate channels for obtaining the password, if need be).

To protect passwords and related data wherever they are located — in your directory or database, in transit from the directory to the client, in client local disk cache and in client memory — the software uses some of the strongest cryptography available, including the Triple Data Encryption Standard (Triple DES) and Advanced Encryption Standard (AES) algorithms. And the software's ability to comply with Federal Information Processing Standard (FIPS) 140-2 can help financial institutions, government agencies, healthcare and other organizations address the stringent privacy and security regulations that govern their operations.

Enjoy speed and efficiency

In both client/server and terminal services environments, Tivoli Access Manager for Enterprise Single Sign-On delivers high-speed sign-on while consuming few resources. It can log on to any application, including industry-specific applications — in most cases, with subsecond turnaround.

Furthermore, the software has a very small memory footprint — typically less than 2.5MB — and uses resources on an event-specific basis to help minimize the impact on both the client and the network. This is critical for server-side

computing deployments such as those found within Citrix, Sun and Windows Terminal Services environments.

Simplify deployment and management

Tivoli Access Manager for Enterprise Single Sign-On helps ease the challenges of implementing and managing the software by offering a robust, intuitive, wizard-driven graphical administrative console and versatile directory integration.

Your network administrator can deploy the client-side software from a central location using IBM Tivoli Configuration Manager or other software distribution systems, without having to add any hardware or software to the network and without having to involve employees in the installation process.

The administrative console simplifies administration by automatically recognizing and configuring applications for sign-on with minimal effort by the administrator. From the administrative console — available either from a .NET-based console or a Microsoft Management Console (MMC) snap-in — point-and-click wizards walk administrators through all the tasks of configuration, deployment and administration. Tivoli Access Manager for Enterprise Single Sign-On ships preconfigured for most popular applications. And the administrative console has built-in intelligence to automatically configure the software for applications it has never seen before — without requiring the administrator to develop cumbersome scripts or costly connectors, or make changes to the target applications or systems.

Once the software is up and running, you can use the administrative console to manage users individually, by role and by group. The console also walks you through the process of setting password policies, system rules, user interface characteristics, reauthentication parameters and other options.

To facilitate event reports, the administrative console allows you to control logging of user events and activities such as logon, password change, authentication, establishment or alteration of policy and more. Tivoli Access Manager for Enterprise Single Sign-On can log events to an XML file, the Windows Event viewer or — using the event application programming interface (API) — another method you choose. You can then generate audit and usage reports based on the events and user activity.

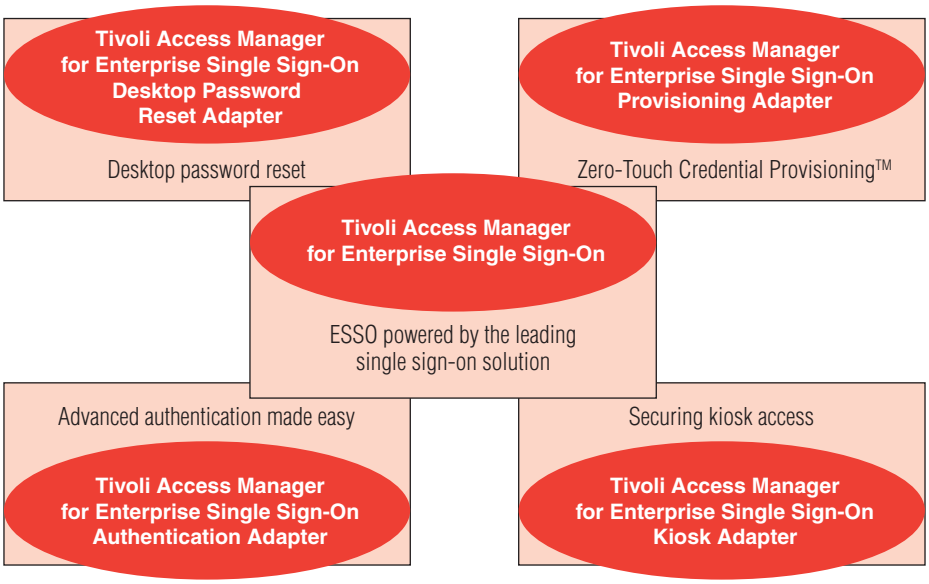
Leverage existing directory resources

Tivoli Access Manager for Enterprise Single Sign-On can store user credentials and its own system settings and configuration information in a range of supported Lightweight Directory Access Protocol (LDAP) directories, one of several structured query language (SQL) databases, including IBM DB2 Universal Database™, or other repositories or storage devices. While an LDAP directory or other enterprise-level repository is not a requirement, most customers who need to support more than a handful of employees will benefit from the centralized control and reporting that an enterprise repository like LDAP can provide.

Because the software utilizes the repository you already have installed, configuring the central repository or directory is simple. The software

supports the following repositories (full support except as noted):

- LDAP, Version 2/Version 3 directories such as IBM Tivoli Directory Server, Sun Java System Directory Server, Novell eDirectory, Oracle Internet Directory
- Microsoft Active Directory® and Active Directory Application Mode (ADAM)
- OpenLDAP (basic support only)
- Critical Path (basic support only)
- DB2® Universal Database
- Microsoft SQL Server
- Oracle 9*i* and 10*g* databases
- Other repositories or storage devices (using the synchronizer API)



Tivoli Access Manager for Enterprise Single Sign-On consists of the base product plus four optional adapters which provide distinct incremental value to meet the specific demands of your environment.

Extend the value of your base solution

Tivoli Access Manager for Enterprise Single Sign-On serves as the foundation for several separately available adapters — giving you the flexibility to respond to the requirements of specific user groups without the cost of migrating to a different technology base. Through these adapter options, Tivoli Access Manager for Enterprise Single Sign-On can support a wide range of additional scenarios, from desktop password resets to support for multi-authentication requests and strong authentication. Each adapter offers point-and-click administrative consoles to help simplify the tasks of configuration, deployment and administration — as well as auditing and reporting capabilities to help reduce the time and costs associated with compliance efforts.

Tivoli Access Manager for Enterprise Single Sign-On adapters include:

- *IBM Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter.* Enables end users to reset their Windows password from locked workstations, helping to eliminate costs associated with help-desk calls related to Windows password resets.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter.* Allows strong authentication using tokens, smart cards, proximity cards and biometrics — plus flexible authentication options such as stepping up from passwords to stronger authentication mechanisms for accessing select, critical resources.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.* Automates the end-user credential distribution process so that identity management solutions such as Tivoli Identity Manager can provision and remove end-user involvement in the credential provisioning and management process.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter.* Provides a security-rich and highly convenient multiuser workstation and kiosk environment by providing automated termination of inactive sessions, application shutdown and fast user switching.

Provide self-service Windows password resets to help reduce help-desk costs:
Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter
Companies with multiple password-secured systems often attribute a substantial portion of their help-desk calls to employee difficulties with passwords. Especially for large organizations, the cost can run into millions of dollars annually. Not to mention the lost opportunity of IT staff time that could be spent on activities with much greater business value.

With Tivoli Access Manager for Enterprise Single Sign-On, however, the Windows password is the only form of authentication for employees; the end result is that each employee only needs to know a single Windows password to access all their applications. But what if employees forget their Windows desktop passwords? To eliminate the help-desk calls that would occur under those circumstances, Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter enables employees to reset their Windows password directly from the locked workstation after a simple question-and-answer process.

Administrators input question text, scoring values and confidence-based scoring that complies with the organization's security policies through the intuitive Web-based console — adding or modifying questions as needed to maintain appropriate security levels. During a one-time enrollment, the user answers the questions that will randomly appear during the reset quiz. A configurable back-end repository enables you to store questions and encrypted enrollment answers to help ensure answers are not at risk.

Manage multiple types of authenticators with ease:
Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter
As security takes ever greater precedence today, many organizations are looking beyond passwords to stronger authentication methods, such as smart cards, biometrics, proximity devices and tokens. For example, an organization might want to deploy tokens to remote users, smart cards to corporate users and passwords to contractors — all to access some of the same applications.

But these devices can pose an integration and administration challenge, especially for organizations that don't want to be locked into a particular vendor or technology. Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter integrates with multiple types of authentication methods and provides support for both primary login and reauthentication requests.

By acting as a mediating layer between authenticators and Tivoli Access Manager for Enterprise Single Sign-On, the authentication adapter lets administrators control which applications employees can access with which authenticators. This high level of control ensures that users have access to applications in line with security policy. Organizations obtain an unsurpassed level of data protection that is best suited to their requirements.

Get users up and running quickly without compromising security:
Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter
Administrators typically create accounts and credentials for each application, system or platform on behalf of employees, which they then send to employees by e-mail or even a piece of paper. In addition to lowering productivity, employees' handling of application credentials can compromise security.

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter accepts provisioning instructions from identity management systems such as IBM Tivoli Identity Manager and enables you to prepopulate employees' credential stores with randomly generated application credentials. With the ability to automatically and directly distribute credentials, employees never have to touch, or even know, their user names and passwords — even administrators may not know an application's first-time-use password.

Add new levels of security to kiosks and shared workstations:

Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter

Organizations with large numbers of shared-workstation users, such as those in the healthcare industry, are increasingly turning to kiosks and shared workstations for high-volume data access. Kiosks enable employees to share computers while roaming during their workday without having to run back to PCs to access various applications and computing resources. But too often users walk away without logging off, potentially exposing sensitive data to a serious security risk. And enterprise-wide auditing is often a major challenge because the kiosks depend on application-level security.

Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter maintains credentials by prompting users to log in to an LDAP directory or other authoritative source, rather than rebooting the system.

After determining the LDAP identity, the kiosk adapter uses the user's credentials, application definitions and settings for all subsequent single sign-on activity.

To prevent sensitive data from getting into the wrong hands, the Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter provides automated termination of inactive sessions and application shutdown for kiosk or shared workstation users. Administrators can determine how long a session should remain inactive before it becomes suspended or terminated.

Finally, because it does not depend on the Windows login, the Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter enables users to switch between accounts quickly and in a highly secure manner.

The adapters provide additional value when used in conjunction with one another. For example, the kiosk adapter and the authentication adapter are used in a number of kiosk environments to enhance the kiosk support with the convenience of proximity cards.

Enhance existing Tivoli Access Manager for e-business and Tivoli Federated Identity Manager implementations

Today, many customers are realizing the Web single sign-on and access management benefits of Tivoli Access Manager for e-business. This software can be part of a single enterprise solution or part of a federated, cross-enterprise solution in which Tivoli Access Manager for e-business and IBM Tivoli Federated Identity Manager are tightly integrated.

Tivoli Access Manager for Enterprise Single Sign-On can easily integrate into these environments to deliver its full set of client-focused capabilities in concert with Tivoli Access Manager for e-business and Tivoli Federated Identity Manager.

Flexibly support your security initiatives and your environment

The entire range of Tivoli Access Manager for Enterprise Single Sign-On software helps you reduce the clutter and confusion caused by nonstop requests to enter or change employee IDs and passwords. The base software broadens the IBM identity and password management capabilities and adds single password access for IBM Lotus Notes®, SAP and Windows-based applications, among many others. Optional adapters extend the base functionality to provide additional support for simplified desktop password resets, stronger and more flexible step-up authentication and multiauthentication, automated credential provisioning, and kiosk and shared workstation environments. Easy to configure, deploy and administer, the Tivoli Access Manager for Enterprise Single Sign-On architecture helps you generate substantial value from your security management investment.

Tivoli Access Manager for Enterprise Single Sign-On at a glance

Client agent requirements:

- Windows 2000, XP, 2003 Server
- 100MHz Intel® Pentium® processor and 64MB RAM
- Disk space: approximately 2.5MB for the installed program and data; a complete installation requires approximately 7MB; approximately 25MB available on hard disk for installer
- Microsoft Internet Explorer 5.5 SP2 or higher with 128-bit encryption

Administrative console and server requirements:

- Windows 2000, XP, 2003 Server
- 100MHz Pentium-compatible processor and 64MB RAM
- Microsoft .NET Framework 1.0
- Windows Installer 2.0 or higher
- Disk space: approximately 4MB for MSI installer; approximately 31MB for EXE installer; overall approximately 15MB for the installed program and data
- Directory: IBM Tivoli Directory Server, Microsoft Active Directory, Sun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP, Version 2/Version 3–compliant directory
- Database: DB2 Universal Database, Microsoft SQL Server, Oracle and more

Additional Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter requirements:

- Microsoft Internet Information Server 5.0 or 6.0
- Microsoft .NET 1.1
- Microsoft Active Directory and ADAM
- Microsoft SQL

Additional Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter requirements:

- 120MHz Pentium processor
- Disk space: approximately 1MB
- Internet Explorer 6.0 or higher with 128-bit encryption
- Note: Strong authenticators likely have their own system requirements, which may differ from these requirements.
- Administrative console and server requirements:
  - 400MHz Pentium II processor and 96MB RAM
  - Disk space: approximately 1MB

Additional Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter requirements:

- Disk space for client agent: approximately 1MB
- Server requirements:
  - Microsoft Internet Information Server 5.x or 6.x (6.x recommended)
  - Directory: Microsoft Active Directory and ADAM, SunOne Directory or IBM Tivoli Directory Server
  - Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine
  - Internet Explorer 6.0 or higher with 128-bit encryption
  - Disk space: approximately 3MB
  - 900MHz Pentium III processor and 512MB RAM

Additional Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter requirements:

- Microsoft .NET 1.1
- 733MHz Pentium III processor and 128MB RAM
- Disk space: approximately 3MB
- Internet Explorer 6.0 with 128-bit encryption

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (IT) resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

For more information

To learn more about how Tivoli Access Manager for Enterprise Single Sign-On helps you simplify password management for your IT administrators and end users, call your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
4-06

GC28-8426-00