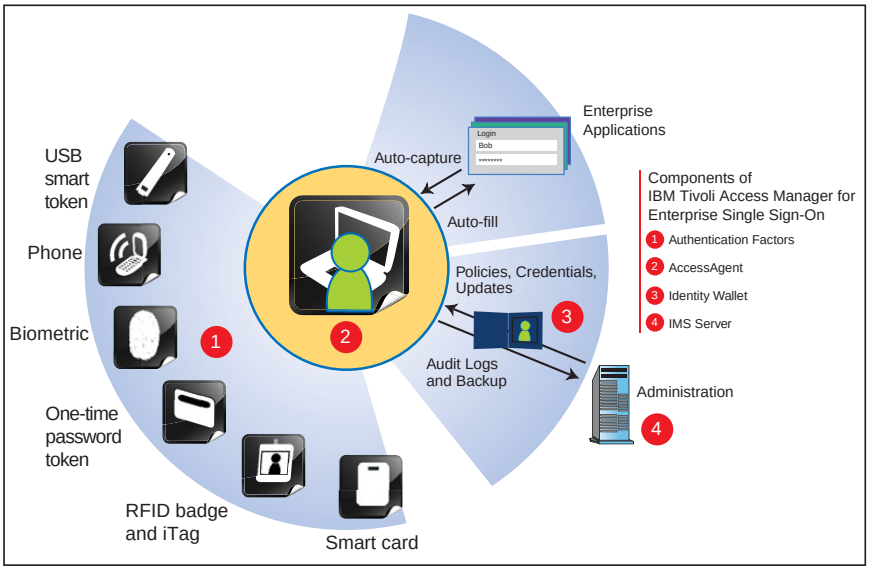
Tivoli® software

IBM Tivoli Access Manager for Enterprise Single Sign-On

Highlights

- ***Reduce password-related help-desk costs by lowering the number of password reset calls***
- ***Strengthen security and meet regulations through stronger passwords and an open authentication device interface with a wide choice of strong authentication factors supported out of the box***
- ***Facilitate compliance with privacy and security regulations by leveraging centralized auditing and reporting capabilities***
- ***Improve productivity and simplify the end-user experience by automating sign-on and using a single password to access all applications***



IBM Tivoli Access Manager for Enterprise Single Sign-On combines single sign-on, strong authentication, session management, automated navigation to any screen in the application, and audit tracking with no change to the existing infrastructure.

Relieve password headaches with a proven single sign-on solution across all types of applications

The complexity and number of logons employees must manage on a daily basis are increasing, resulting in frustration and lost productivity. In most organizations, employees must remember between 5 and 20 passwords and are required to change them every 30 days. The time wasted entering, changing, writing down, forgetting and resetting passwords represents a significant loss in productivity and a significant cost to IT help-desk operations.

With IBM Tivoli® Access Manager for Enterprise Single Sign-On—the market-leading enterprise single sign-on solution—employees authenticate once,

and the software then detects and automates all password-related events for the employee, including:

- *Logon*
- *Password selection*
- *Password change*
- *Password reset*
- *Automated navigation to any screen in the application where productive work can immediately begin*
- *Logoff*

Tivoli Access Manager for Enterprise Single Sign-On helps organizations reduce costs, strengthen security, improve productivity and address compliance requirements. This solution provides single sign-on for all your Microsoft® Windows®, Web, Java™, mainframe and teletype applications, and is available on all major network access points, including Windows desktops, laptops, shared kiosks, Citrix servers, Microsoft Terminal Servers and Web portals. This complete end-point coverage allows users to sign on from anywhere to the enterprise network with one password and get single sign-on access to all applications, even if access is via a browser from an Internet café.

Reduce password management costs

Tivoli Access Manager for Enterprise Single Sign-On can reduce help desk, compliance and administration costs. Up to 80 percent of help-desk calls are for password resets. For large organizations, the cost can run into millions of dollars annually. With Tivoli Access Manager for Enterprise Single Sign-On, when employees forget their password, they can reset it using a simple question-and-answer process. Compliance costs can be decreased by automating the auditing and tracking of user accesses, and also by producing needed compliance reports. Administration costs can be decreased for managing user IDs and passwords while enabling users to leverage self-service capabilities.

Improve password behavior to strengthen security

When users have multiple user IDs and passwords, they typically write them down in unsecured locations, use easy-to-guess passwords and share their passwords with co-workers. With Tivoli Access Manager for Enterprise Single Sign-On users only need to remember a single password.

Tivoli Access Manager for Enterprise Single Sign-On can be configured to detect password changes and auto-generate strong passwords for each application. Because it remembers and enables single sign-on with these strong passwords, users never have to remember or manage these passwords themselves, providing security while maintaining user productivity. To protect passwords and related data wherever they are located, the software uses Advanced Encryption Standard (AES) algorithms, some of the strongest cryptography available.

Use strong authentication to protect information

Many organizations are looking beyond passwords to stronger authentication methods to protect access to sensitive information and help meet compliance requirements. Tivoli Access Manager for Enterprise Single Sign-On not only supports a wide choice of strong authenticators, such as USB smart tokens, smart cards, active proximity cards, passive proximity badges, one-time password tokens and fingerprint biometric devices, but also enables existing identification devices, such as building badges, photo badges and cell

phones to be used for authentication. Leveraging devices users already have and know can accelerate implementation and reduce the total cost of ownership.

For added flexibility, Tivoli Access Manager for Enterprise Single Sign-On provides an open authentication device interface to easily integrate any smart card that is PKCS#11 or MS-CAPI compliant, and any serial ID device, such as your building access badge or photo badge.

Add new levels of security to kiosks and shared workstations

Fast user switching and session management are vital requirements in many industries such as manufacturing, healthcare, warehousing, retail and education. As organizations deploy an increasing number of shared workstations and kiosks, a large number of users can roam and access information from anywhere without having to return to their personal PCs. But shared kiosks pose severe security threats as users often walk away without logging off, potentially exposing confidential information to unauthorized access.

Any attempt to tighten security, enforce unique user logons and comply with regulations can lead to users being locked out of workstations, resulting in a loss of productivity.

With Tivoli Access Manager for Enterprise Single Sign-On, organizations can increase user convenience and improve security via a comprehensive choice of session management and fast user switching capabilities to meet the access needs of various user groups. Multiple users can share a computer simultaneously and switch between users without the need to log out or face any risk of getting locked out. Users who want their desktops to "follow them" can use the software's roaming desktop support. Users can also maintain their private desktops while sharing workstations with co-workers.

If a user walks away from a session without logging out, Tivoli Access Manager for Enterprise Single Sign-On can be configured to enforce inactivity timeout policies such as configurable screen locks, application logout policies, graceful logoff of all applications, and more.

Simplify audit tracking and compliance reporting

To help address compliance requirements, Tivoli Access Manager for Enterprise Single Sign-On transparently logs all user logon activities and centrally records them to the Integrated Management System (IMS™) Server. The software also enables customized tracking, allowing you to track and monitor activities not otherwise possible through your applications. The resulting consolidated user-centric logs provide the meta-information that can guide administrators to the right application logs for more detailed analysis when required. Integration with Tivoli Common Reporting provides flexible reporting to meet your compliance reporting needs.

Simplify deployment and management

Tivoli Access Manager for Enterprise Single Sign-On simplifies deployment and management by offering a wizard-driven graphical administrative Web console. From this console, 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 many popular applications, and an even larger number of applications can be supported through an easy no-fee download of their access profiles. In addition, administrators can auto-generate access profiles for new applications through a simple wizard interface —without requiring the administrator to develop cumbersome scripts or costly connectors, or to make changes to the target applications or systems. More complex applications can be supported with visual profiling, a simple drag-and-drop graphical approach to configure automation and sign on.

The software is designed to be centrally deployed. Network administrators can deploy the client-side software from a central location using IBM Tivoli Configuration Manager or other software distribution solutions without having to involve employees in the installation process.

Once the software is up and running, administrators can use the administrative console to manage users individually, or by group. From the central console administrators can set password policies, system rules, user interface characteristics, reauthentication parameters and other options.

Leverage existing IT infrastructure and directory resources

Tivoli Access Manager for Enterprise Single Sign-On is designed to work with minimal or no change to an organization's existing IT infrastructure. The solution works with any directory structure and does not require an expensive directory consolidation project prior to deployment. Unlike some competing single sign-on offerings, it does not require a directory schema extension or replication of directory data.

The solution stores user credentials, system settings and policies centrally in your corporate database, while interfacing with corporate directories such as Active Directory, NT Domain Controllers, Sun One LDAP, IBM Tivoli Directory Server and Novell eDirectory for identity data.

In addition, the solution accommodates both Microsoft Internet Explorer and Mozilla Firefox browsers, offering the convenience and savings of single sign-on for users who use one browser or the other, or a combination of the two.

Centrally manage end-user and privileged identities while simplifying access

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 via paper. Not only does this manual creation and dissemination of credentials lower productivity, but employee handling of application credentials can compromise security.

Tivoli Access Manager for Enterprise Single Sign-On integrates with best-of-breed user provisioning technologies and homegrown solutions to provide end-to-end, comprehensive identity life-cycle management. It accepts provisioning instructions from identity management solutions such as Tivoli Identity Manager and enables you to pre-populate the employee's identity wallet with randomly generated application credentials.

This tight integration with provisioning solutions helps ensure that whenever an access right or password is changed through the provisioning

system, Tivoli Access Manager for Enterprise Single Sign-On user information is synchronized so that up-to-date application credentials are available. Similarly, when a user is deprovisioned, this tight integration ensures that access via Tivoli Access Manager for Enterprise Single Sign-On will automatically be denied.

Integrating Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On enables account sharing among a predefined group of users and provides single sign-on for each user in the group to a designated shared account, even as the account password is updated. These products can be configured to enforce strict check-in and checkout of a pool of shared accounts to ensure accountability for privileged identity management.

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

Today, many customers are realizing the Web and federated access management benefits of Tivoli Access Manager for e-business and Tivoli Federated Identity Manager. Tivoli Access Manager for Enterprise Single Sign-On easily integrates into these environments to deliver its full set of client-focused capabilities. This integrated solution suite enables single sign-on inside, outside and between organizations, providing a complete end-to-end single sign-on solution that is not available in other offerings.

Key components of Tivoli Access Manager for Enterprise Single Sign-On

Authentication factors: Supports an open authentication device interface and a wide choice of strong authentication factors, including iTag—smart labels containing RFIDs that can be affixed to badges and other personal objects for flexible, cost-effective, two-factor authentication.

AccessAgent and Plug-ins: Client software that acts on the user's behalf for single sign-on and sign-off, authentication management and session management. JScript and VBScript plug-ins allow AccessAgent behavior to be customized.

Identity Wallet: A personal, encrypted repository of user credentials. The identity wallet roams to the point of access and stores the user's personal identity profiles including log-in credentials, certificates, encryption keys and user policies.

Integrated Management System (IMS) Server: Provides centralized management of users and policies. All policies are defined centrally and enforced through the AccessAgent. The IMS Server also provides comprehensive backup of credentials, loss management, audit information and compliance reporting.

For more information

To learn more about how Tivoli Access Manager for Enterprise Single Sign-On can help simplify password management for your users and IT administrators, please contact your IBM marketing representative or IBM Business Partner, or visit **ibm.com**/tivoli/security

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes 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 life-cycle management, and is backed by world-class IBM services, support and research.

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

Client agent requirements:

- Windows XP SP2, Vista, 2003 Server, 2008 Server
- 600MHz Intel® Pentium®-based processor and 256 MB RAM
- Disk space: At least 200 MB free hard disk space
- Microsoft Internet Explorer 5.0 or higher with 128-bit encryption, Firefox 3.x
- Installation via Microsoft Installer (MSI) package requires Microsoft Windows Installer

Administrative console and server requirements:

- IMS Server requires Windows 2003 or 2008 Server
- AccessAdmin requires Microsoft Internet Explorer 6.0 or higher with 128-bit encryption
- 1.2GHz Pentium-compatible processor and 1 GB RAM
- Disk space: At least 3 GB free hard disk space
- Directory: Active Directory, NT Domain Controllers, Sun One LDAP, Tivoli Directory Server, Novell eDirectory, or other LDAP
- Database: DB2® 9.5 or 9.7, Microsoft SQL 2000 or 2005 Server, Oracle 9i or 10g

Certification:

- FIPS 140-2
- In evaluation for Common Criteria EAL 4+, which is given only to a select few products that can demonstrate that that they were methodically designed, tested and reviewed

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

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

Produced in the United States of America
November 2009

Recyclable, please recycle.

TID10298-USEN-02