Tivoli software

IBM Tivoli Access Manager for Enterprise Single Sign-On

Highlights

- ***Help simplify the end-user experience by eliminating the need to remember and manage user names and passwords, and by automating sign-on and access***
- ***Enhance security by reducing poor end-user password behavior***
- ***Help reduce password-related help-desk costs by lowering the number of password reset calls***
- ***Enable comprehensive session management of kiosk machines to improve security and user productivity***
- ***Enhance security through a wide choice of strong authentication factors***
- ***Leverage centralized audit and reporting capabilities to facilitate compliance with privacy and security regulations***
- ***Extend IBM Tivoli® Access Manager for e-business's fine-grained authorization and entitlements for Web applications, by fully addressing single sign-on across all network access points***
- ***Enable end-to-end identity and access management by integrating the centralized identity management functions of IBM Tivoli Identity Manager with enterprise single sign-on and access automation***

Relieve password headaches with a proven single sign-on solution across all network access points

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 30 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 of 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.
- Logoff.

Tivoli Access Manager for Enterprise Single Sign-On can help you deliver 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 end 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.

Manage passwords with security-rich capabilities

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 easy-to-guess passwords and share their passwords with co-workers.

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.

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, AccessAdmin. From this console, point-and-click wizards walk administrators through all the tasks of configuration, deployment and administration.

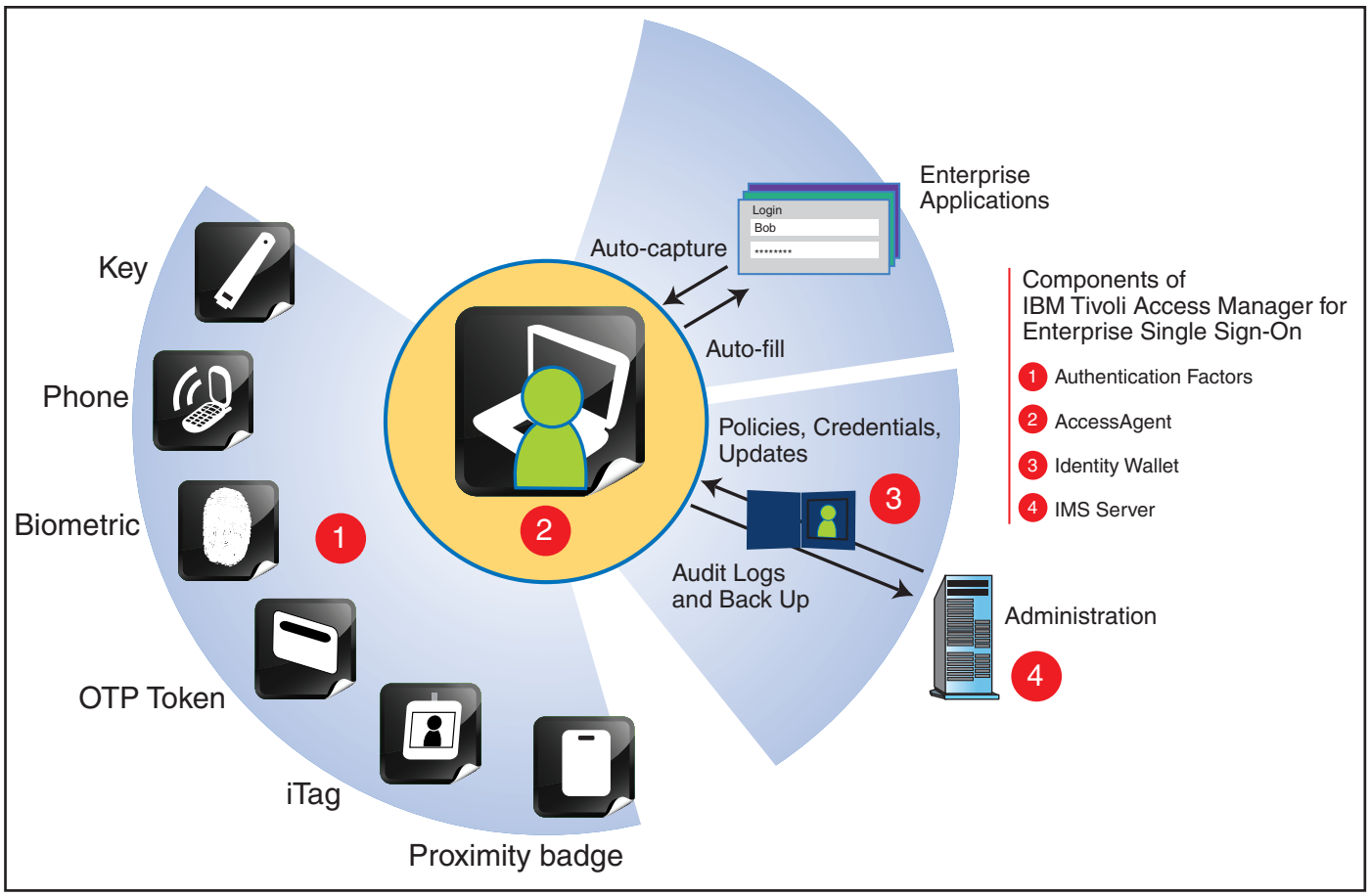
Tivoli Access Manager for Enterprise Single Sign-On ships preconfigured for many popular applications. Administrators can use AccessStudio to auto-generate access profiles for applications it has never seen before—without requiring the administrator to develop cumbersome scripts or costly connectors, or to make changes to the target applications or systems. AccessStudio Advanced also offers visual profiling, a graphical way to configure automation and sign on to complex applications.

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 systems 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. AccessAdmin also provides a central console for setting password policies, system rules, user interface characteristics, re-authentication parameters and other options.

Simplify audit tracking and compliance reporting

To help address regulatory compliance, Tivoli Access Manager for Enterprise Single Sign-On transparently logs all user logon activities and centrally reports them to the Integrated Management System (IMS) Server. 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. The software also enables customized tracking, real-time monitoring, and flexible reporting capabilities.



Tivoli Access Manager for Enterprise Single Sign-On combines single sign-on, strong authentication, session management, access workflow automation and audit tracking, with no change to the existing infrastructure.

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 enterprise's existing IT infrastructure. The solution works with any directory structure and does not require an expensive directory consolidation project prior to deployment. It also 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.

Provide self-service password resets to help reduce help-desk 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 single sign-on password, they can reset the password directly from a locked workstation after a simple question-and-answer process.

Manage multiple types of authenticators with ease

As security takes ever greater precedence today, many organizations are looking beyond passwords to stronger authentication methods. Tivoli Access Manager for Enterprise Single Sign-On not only supports a wide choice of authenticators such as USB smart tokens, active proximity cards, passive proximity badges, biometrics and one-time password tokens, but also enables existing identification devices, such as building badges, photo badges and cell phones, to be used for authentication, leveraging user familiarity and reducing the total cost of ownership.

Centrally manage user 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 on a piece of paper. Not only does manual creation and dissemination of credentials lower productivity, 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 lifecycle management. It accepts provisioning instructions from identity management systems such as Tivoli Identity Manager and enables you to pre-populate employees' credential stores 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, the user wallet will be synchronized so that up-to-date application credentials are available. Similarly, when a user is de-provisioned, this tight integration ensures that single sign-on will automatically be denied.

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 information 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 across 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.

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

Today, many customers are realizing the Web 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 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. 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.

A distributed single sign-on architecture

Tivoli Access Manager for Enterprise Single Sign-On includes the following key components:

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.

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

Client agent requirements:

- Windows 2000 SP3, XP SP1, 2003 Server
- 600MHz Intel® Pentium®-based processor and 128MB RAM
- Disk space: At least 100MB free hard disk space
- Microsoft Internet Explorer 5.0 or higher with 128-bit encryption
- Installation via Microsoft Installer (MSI) package requires Microsoft Windows Installer

Administrative console and server requirements:

- IMS Server requires Windows 2003 Server
- AccessAdmin requires Microsoft Internet Explorer 5.0 or higher with 128-bit encryption
- 1.2GHz Pentium-compatible processor and 256MB RAM
- Disk space: At least 300MB free hard disk space
- Directory: Active Directory, NT Domain Controllers, Sun One LDAP, Tivoli Directory Server, Novell eDirectory, or other LDAP
- Database: DB2, Microsoft SQL Server and Oracle

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.

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 back-up of credentials, loss management, audits and compliance reporting.

Authentication factors: Supports a choice of strong authentication factors such as USB keys, one-time password tokens, biometrics, building access badges and iTag.

For more information

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

About Tivoli software from IBM

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation — visibility to see and understand the workings of their business; control to effectively manage their business, minimize risk, and protect their brand; and automation to optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

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

Produced in the United States of America
June 2008

TAKE BACK CONTROL WITH Tivoli.

TID10298-USEN-01