White paper
December 2008

Tivoli® software

IBM Tivoli Access Manager for Enterprise Single Sign-On: An overview

Contents

Executive summary

With an increasing number of enterprise applications and access points, organizations face the challenge of providing convenient access while ensuring strong security. Enterprises need software to help ensure that the right users have access to the right information in a timely manner.
IBM Tivoli® Access Manager for Enterprise Single Sign-On is an identity and access management solution that provides:

- *Visibility into user activities.*
- *Control over business processes and risks.*
- *Automation of logins, access and security workflows.*

This white paper describes Tivoli Access Manager for Enterprise Single Sign-On, including its key features and benefits.

The enterprise access challenge

As the number of enterprise applications and access points increase, organizations must manage the trade-off of providing convenient access while at the same time ensuring strong security. Organizations are looking for a balance between easy access to information and strong, compliant security.

A secure system raises identity assurance through strong authentication and provides integrated tracking of user access. It is not sufficient to know that users are who they say they are, but also which applications the users are attempting to access. Enterprises need identity and access management (IAM) software to help ensure that the right users have access to the right information in a timely manner.

Tivoli Access Manager for Enterprise Single Sign-On delivers a simple and flexible identity and access management solution, combining enterprise single sign-on with strong authentication.

Seamless access to applications

Tivoli Access Manager for Enterprise Single Sign-On delivers a simple, flexible and complete identity and access management solution at the enterprise end points. It combines enterprise single sign-on with strong authentication, and audit and compliance services, while integrating seamlessly with provisioning and directory services, with no change to your existing infrastructure. Figure 1 provides an overview of the system architecture.

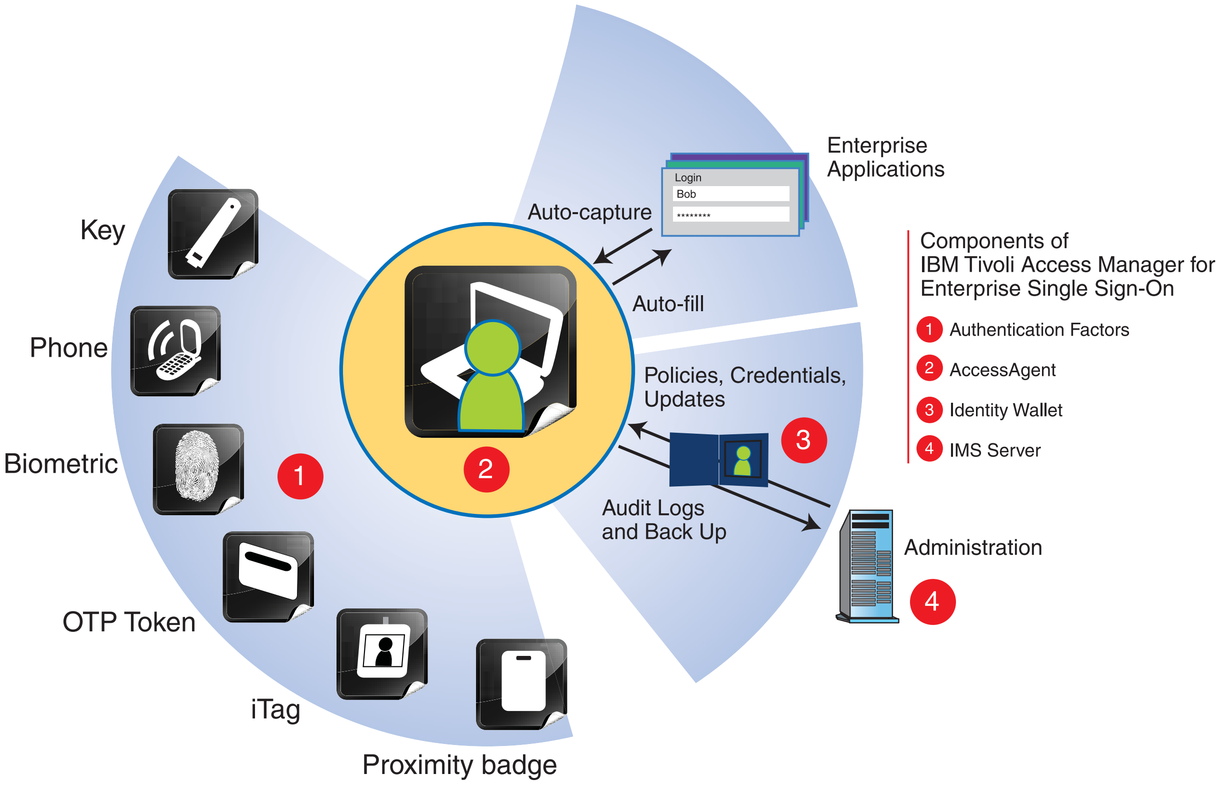

Figure 1: Tivoli Access Manager for Enterprise Single Sign-On combines single sign-on, strong authentication, session management, access workflow automation, and audit tracking, with no change to the existing infrastructure.

The central components of Tivoli Access Manager for Enterprise Single Sign-On are:

- *Identity Wallet*
- *Authentication Factors*
- *AccessAgent and Plug-ins*
- *IMS™ Server*

AccessAgent implements single sign-on and end-point automation with extensible Plug-ins, while the IMS Server provides server-managed controls. Each user has an Identity Wallet, which enables roaming and consolidation of user identities.

Key features

Tivoli Access Manager for Enterprise Single Sign-On provides the convenience of securely signing on once and immediately getting access to the information you need. Tivoli Access Manager for Enterprise Single Sign-On also provides the following key features.

Visibility into user activities

- *Comprehensive coverage of enterprise end points helps ensure a consistent user experience and end-to-end tracking.*
- *User-centric access tracking provides a meta-log for compliance reporting.*

Control over business processes and risks

- *Centralized push deployment with no change to the existing infrastructure provides easy deployment and helps reduce risk.*
- *Web-based administration and integration with provisioning solutions provides centralized identity and access management.*
- *Choice of authentication factors helps reduce the risk of identity fraud.*
- *Customizable end-point identity and access automation enables end-point control without changing the existing IT infrastructure.*

Automation of access and security workflows

- *Leverage a single badge for both physical and logical access.*
- *Enterprise single sign-on and access automation help improve user convenience and productivity.*
- *Complete session management helps ensure that user workflows are supported by the right session capabilities.*
- *Integrated self-help with loss management enables user self-service.*

Comprehensive coverage of enterprise end points

Tivoli Access Manager for Enterprise Single Sign-On provides comprehensive coverage of enterprise end points such as personal and shared workstations, virtualized remote access terminals, Web portals, and extranets.

Tivoli Access Manager for Enterprise Single Sign-On provides comprehensive coverage of enterprise end points such as personal and shared workstations, virtualized remote access terminals (Citrix and Microsoft® Windows® Terminal Services), Web portals, and extranets. Users can access the corporate network across all end points more securely and easily. IT managers can centrally manage and synchronize security policies across end points and track access events for compliance reporting.

In addition to support for applications running on Windows platforms, Tivoli Access Manager for Enterprise Single Sign-On supports access to applications on Citrix MetaFrame servers. AccessAgent provides single sign-on and sign-off for applications through Citrix ICA Client or Citrix Web Interface. It can also enable two-factor authentication to applications on Citrix MetaFrame servers or Windows Terminal Services.

Support for single sign-on to applications on portals and extranets is provided through Web Workplace. Users need just one password and no desktop software to remotely log in to applications. Access to Web Workplace can be secured using one-time password tokens or Mobile ActiveCode. Once access is granted, users can single sign on through their browser to all enterprise applications, including Web applications and legacy applications hosted on Terminal Services or Citrix servers.

User-centric access tracking

Tivoli Access Manager for Enterprise Single Sign-On provides consolidated user-centric logs for more effective audit control.

To facilitate regulatory compliance, enterprises need to know which applications users access, who they log in as, when users access applications, and from where they access them. This information has traditionally been aggregated in application-centric logs. These logs remain unconsolidated silos, and the lack of consolidated identities can make aggregation challenging. With Tivoli Access Manager for Enterprise Single Sign-On, each AccessAgent transparently logs all user login activities and reports them to the IMS Server. The consolidated user-centric logs provide for effective audit control. In addition, information is organized in a relational database, facilitating reporting and real-time monitoring.

Centralized push deployment with no change to the existing infrastructure

Tivoli Access Manager for Enterprise Single Sign-On can work with minimal or no change to an enterprise's existing IT infrastructure.

Tivoli Access Manager for Enterprise Single Sign-On will work with Microsoft Windows Active Directory® group policy objects and all major software distribution solutions for remote installations. It may also be configured to support auto-registration so that users with Active Directory accounts are auto-registered.

Tivoli Access Manager for Enterprise Single Sign-On can work with minimal or no change to an enterprise's existing IT infrastructure. It will work with any directory structure and does not require directory consolidation or schema changes prior to deployment.

Web-based administration and integration with provisioning solutions

Tivoli Access Manager for Enterprise Single Sign-On is integrated with IBM Tivoli Identity Manager, and provides easy integration with other provisioning and password management solutions.

Administrators and help desk personnel use AccessAdmin, a Web console for the IMS Server, to manage users. Through AccessAdmin, an administrator can revoke a user's access. Administrators can easily define policy templates that may be applied to select user groups.

To provide complete identity and access management, Tivoli Access Manager for Enterprise Single Sign-On is integrated with IBM Tivoli Identity Manager, and provides a complete provisioning API over SOAP/HTTPS for easy integration with other provisioning and password management solutions.

Integration with user provisioning enables IT to use their provisioning solutions for identity lifecycle management, while ensuring that any new user created will automatically be created in the single sign-on system, and any de-provisioning or updating of application rights will automatically be reflected in the single sign-on system.

Choice of authentication factors

A wide choice of authentication factors help meet the needs of different user groups with a single, integrated solution.

Tivoli Access Manager for Enterprise Single Sign-On can help reduce password management costs by consolidating authentication credentials in the Identity Wallet. Enterprises have a choice of second factors, including strong passwords, building access badges, active radio frequency identification (RFID) badges, iTag, one-time password-based authentication via cell phones or other tokens, biometrics, and USB smart cards.

A wide choice of authentication factors help meet the needs of different user groups with a single integrated solution as shown in Table 1.

Table 1: Authentication factors and user scenarios

Authentication Factor	**User Scenario and Target User Group**
Building access badge	The user taps their badge on the reader and enters a password to log in. Best for users working within corporate premises with managed desktops.
Active RFID	The user is identified as they approach the workstation. They enter a password to log in. Best for users who need fast login/logout.
Mobile device	The user receives a Mobile ActiveCode on SMS-enabled or e-mail-enabled mobile device. They use this code with their user name and password to log in to their extranet remotely via their browser. Best for the mobile workforce who may need access from Internet cafés and business centers.
iTag	The user leverages any personal device or photo ID badge with smart labels to enable two-factor authentication. User adoption is high, and training costs are minimal. Best for users working within corporate premises with managed desktops.
Biometrics	The user logs in using fingerprints. This is an alternative to building access badges or Active RFID badges for corporate users and removes the need for a password. However, building access badges and Active RFID are more robust. Best for users working within corporate premises with managed desktops.
USB smart tokens	The user inserts a USB smart token and enters a password to log in. Best for users with high security requirements.
Strong password	The user enters a user name and a strong password to log in. Best for users who do not need stronger authentication.

Through Web Workplace, Tivoli Access Manager for Enterprise Single Sign-On also enables secure remote access by combining two-factor authentication with leading SSL-VPN platforms. Users can access Web, desktop and legacy applications through the SSL-VPN and enable two-factor authentication via one-time password tokens or passwords delivered to smart phones or other mobile devices.

Tivoli Access Manager for Enterprise Single Sign-On provides a customizable and scalable framework that may be used to implement custom identity and access management functions such as in-depth application auditing.

Customizable end-point IAM framework

With Tivoli Access Manager for Enterprise Single Sign-On, AccessAgent software is installed at each enterprise end point. Each AccessAgent implements the three-tier end-point automation framework outlined in Figure 2.

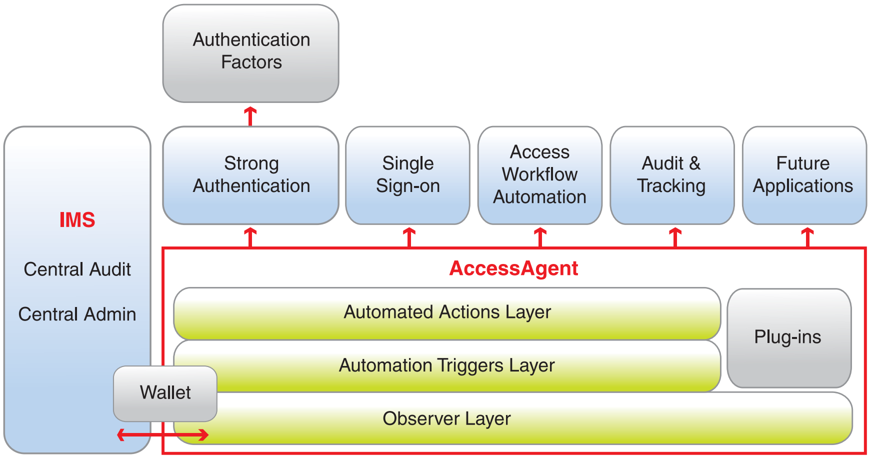

Figure 2: Tivoli Access Manager for Enterprise Single Sign-On—An end-point IAM architecture

The end-point IAM framework is composed of three core layers to provide definition, flexibility and scalability:

- *The Observer Layer provides the ability to observe presentation layer events at the end point.*
- *The Automation Triggers Layer defines automation triggers at each end point. Triggers "fire" when certain events are observed in the Observer Layer.*
- *The Automated Actions Layer defines automated actions to execute when a trigger is fired.*

This three-tier approach ensures clean separation of "what," "when" and "how" the end point should interact. This clean separation provides ease of definition, flexibility and scalability.

This customizable and scalable framework may be used to implement custom identity and access management functions such as in-depth application auditing beyond the native application logging capabilities, and can be used to automate complex access workflows.

AccessProfiles and Plug-ins may be uploaded centrally and distributed automatically to all enterprise end points.

Combined physical-logical access

By supporting the use of existing building access cards as second factors for logical access, Tivoli Access Manager for Enterprise Single Sign-On delivers a combined physical-logical access solution. As building access cards are already provisioned, no additional provisioning or re-badging is required.

Tivoli Access Manager for Enterprise Single Sign-On supports the use of building access cards as second factors for logical access.

Alternatively, Tivoli Access Manager for Enterprise Single Sign-On may turn any photo ID badge or magnetic stripe-based card into a logical access card through iTag. iTag is a patent-pending smart label technology that contains RFID tags, which can be affixed to personal objects, such as photo badges, cell phones or PDAs.

Enterprise single sign-on and access automation

Tivoli Access Manager for Enterprise Single Sign-On provides single sign-on and single sign-off.

Tivoli Access Manager for Enterprise Single Sign-On provides single sign-on to all applications, including Web, mainframe, teletype and desktop applications. AccessStudio Wizard auto-generates XML-based AccessProfiles for single sign-on, while AccessStudio Advanced provides visual profiling for advanced AccessProfile configuration and Plug-in definition.

Tivoli Access Manager for Enterprise Single Sign-On can be configured to gracefully sign off applications by locking the screen or logging off a session. It can also be configured to automatically navigate users to any screen or to specific points of information access within applications.

Complete session management

Session management provides fast user switching and is a key requirement in many industries, including manufacturing, health care and warehousing. Three different types of session management options are available:

Tivoli Access Manager for Enterprise Single Sign-On provides three different types of session management.

- *Shared desktops–Support desktop sharing through a generic Microsoft Windows account, helping to ensure that users can quickly sign on and sign off at a shared kiosk.*
- *Private desktops–Manage multiple private desktops on the same workstation so that users can share a kiosk while maintaining their own private sessions.*
- *Roaming desktops–Provide personal desktops that "follow" the user as he or she roams from workstation to workstation.*

Tivoli Access Manager for Enterprise Single Sign-On provides integrated self-help and loss management capabilities.

Integrated self-help with loss management

Complete self-help and loss management facilities cover most loss scenarios. To help ensure rapid recovery, Identity Wallets are encrypted and automatically synchronized with the IMS Server. The following loss scenarios are supported:

- **Forgotten application password**–*The user may view application passwords from AccessAssistant, a Web self-help system. This should happen only when single sign-on is not available from where the user is logging in.*
- **Forgotten password for Tivoli Access Manager for Enterprise Single Sign-On**–*During installation, the user is required to answer a select number of personal questions. They may reset passwords by correctly answering these personal questions or by requesting an authorization code from the help desk (if the user fails to correctly answer personal questions). Passwords can also be reset offline.*
- **Forgotten authentication token**–*The user may request an authorization code from the help desk, which may be used as a temporary second factor until they regain possession of the token. Or the user may bypass the second factor by successfully answering his or her personal questions.*
- **Lost authentication token**–*The user may request a replacement by obtaining an authorization code from the help desk. This code authorizes the user to reset authentication factors required for login.*

Tivoli Access Manager for Enterprise Single Sign-On supports the workflow of all user groups in a single, integrated solution.

Single sign-on across a variety of user groups

Tivoli Access Manager for Enterprise Single Sign-On caters to all user groups, as shown in Table 2.

Table 2: User groups and recommended authentication factors

User Group	Recommended AccessAgent Platform	Recommended Authentication Factor
IT users	• AccessAgent for Microsoft Windows configured as personal workstations • AccessAgent for Terminal Services on servers to enable remote administration	• Strong passwords, or • Building access badge, or • iTag
Desktop business users	AccessAgent for Microsoft Windows configured as personal workstations	• Strong passwords, or • Building access badge, or • iTag
Laptop business users	AccessAgent for Microsoft Windows configured as personal workstation	• Strong passwords, or • USB smart card, or • iTag
Remote users	AccessAgent for Citrix, Microsoft Terminal Services or Web Workplace	• Strong passwords, or • One-time password tokens, or • Mobile devices using Mobile ActiveCode
Kiosk users	AccessAgent for Microsoft Windows configured as shared, private or roaming desktops	• Strong passwords, or • Building access badge, or • iTag

Tivoli Access Manager for Enterprise Single Sign-On helps enterprises improve user productivity, facilitate regulatory compliance, decrease help desk costs, and enhance security.

A unified strategy from IBM

Tivoli Access Manager for Enterprise Single Sign-On provides visibility into user activities, control over business processes and risks, and automation of access and security workflows. It helps enterprises improve user productivity, facilitate regulatory compliance, decrease help desk costs, and enhance security.

IBM provides a unified strategy for enterprise security that includes powerful, cost-effective and easy-to-use identity management and access management solutions. With IBM, you can develop a solution that covers the identity and access management lifecycle while addressing security needs in a compliant, cost-effective manner.

IBM not only offers best-in-class IAM solutions, but also unsurpassed breadth and integration across its security suite. IBM Unified Single Sign-On is one such integrated solution. It extends the capabilities of Tivoli Access Manager for Enterprise Single Sign-On to address end-to-end enterprise requirements for single sign-on inside, outside and between organizations.

IBM enables you to focus on driving business innovation by reducing the complexity of securing the enterprise through a flexible and adaptable approach across the entire realm of IT security risk. IBM can address the big picture, including identity and access management, threat protection, managed services, mainframe security, application security, information and data security, and service management. IBM is ready to support your long-term security goals, and has the breadth and depth to address your broader security management needs.

For more information

To learn more about how IBM Tivoli Access Manager for Enterprise Single Sign-On can help you better address end-point identity access management in your environment, contact your IBM sales 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, help minimize risk and protect their brand; and automation to help 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

Additionally, IBM Global Financing can tailor financing solutions to your specific IT needs. For more information on great rates, flexible payment plans and loans, and asset buyback and disposal, visit: **ibm.com**/financing

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

Produced in the United States of America
December 2008

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED “AS IS” WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

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.

Recyclable, please recycle