**White paper**
December 2008

Tivoli® software

IBM

# Addressing single sign-on inside, outside, and between organizations

Contents



## Overview

As security threats grow more sophisticated and information security regulations are expanded, organizations are under increasing pressure to control access to sensitive data. The infrastructure at many organizations has expanded and evolved incrementally over time, resulting in a diverse set of hardware and software with equally diverse security standards and sign-on procedures. At the same time, to support new business initiatives IT must now support three types of access:

- *Applications within the organization. These are enterprise single sign-on applications and include access to Microsoft® Windows®, Web, Java™, Citrix, Microsoft Windows Terminal Services, and mainframe applications.*
- *Corporate Web applications, protecting information and resources being accessed via the Web. These are Web applications and include Web servers, Web applications and portals—all within a single domain.*
- *Applications that are federated to seamlessly access resources from another partner, or between different lines of business within the organization, in a secure and trustworthy manner. These are cross-domain applications and include Web servers, Web applications and portals, involving cross-domain exchanges. Federation is a highly effective method to connect partners and suppliers in your business ecosystem and to quickly incorporate new acquisitions, or bridge different divisions within the organization that might have different security implementations.*

*IBM Tivoli Unified Single Sign-On provides comprehensive coverage of single sign-on (SSO) configurations and requirements.*

IBM Tivoli® Unified Single Sign-On addresses all three types of access requirements, and supports heterogeneous environments. IBM Tivoli Unified Single Sign-On provides comprehensive coverage of single sign-on (SSO) configurations and requirements, and can help organizations realize the full promise of end-to-end single sign-on.

IBM Tivoli Unified Single Sign-On's benefits include:

- *Addressing the needs of organizations for enterprise single sign-on, Web single sign-on, and federated single sign-on.*
- *Simplifying the end-user experience by eliminating the need to remember and manage numerous user names and passwords, and by automating sign-on and access.*
- *Improving visibility and compliance with centralized authentication, access and single sign-on to heterogeneous Web applications and services across Java, Microsoft .NET and mainframe environments.*
- *Simplifying application integration using many forms of credentials and facilitating more secure information sharing across trusted business partners and divisions within an enterprise.*
- *Enhancing security by reducing poor end-user password behavior and through a wide choice of strong authentication factors and access control.*
- *Reducing password-related help desk costs by lowering the number of password reset calls.*
- *Enabling comprehensive session management of kiosk machines to improve security and user productivity.*

IBM Tivoli Unified Single Sign-On is comprised of three industry-leading single sign-on products:

- *IBM Tivoli Access Manager for Enterprise Single Sign-On*
- *IBM Tivoli Federated Identity Manager*
- *IBM Tivoli Access Manager for e-business*

This white paper examines the single sign-on capabilities of each of these products and the strengths of these solutions as they work together to provide unified single sign-on.

## IBM Tivoli Unified Single Sign-On: Comprehensively addressing SSO

*Tivoli Unified Single Sign-On combines three industry-leading single sign-on products to comprehensively address the three sources of SSO requests: Internet, extranet, and intranet/kiosk.*

To illustrate how Tivoli Unified Single Sign-On comprehensively addresses sign-on scenarios, let's look at three environment examples that are the source of SSO requests: the Internet, an extranet (airport lounge or Internet café where you are using the Web to access your applications), and intranet/kiosk.

IBM Tivoli Access Manager for Enterprise Single Sign-On addresses enterprise targets, in any scenario where the request is coming from a client that has IBM Tivoli Access Manager for Enterprise Single Sign-On client code installed. IBM Tivoli Access Manager for e-business addresses Web targets, covering all three possible sources of incoming requests: Internet, extranet, and intranet. And for multiple-domain or cross-domain configurations, IBM Tivoli Federated Identity Manager, working with IBM Tivoli Access Manager for e-business, handles access requests across the Internet, extranet and intranet.

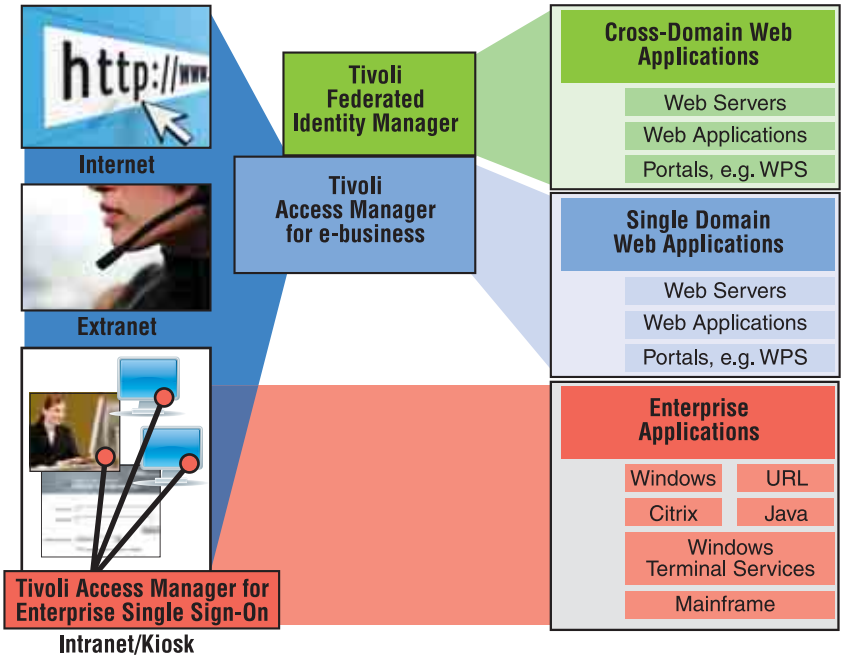


*Figure 1: Tivoli Unified Single Sign-On comprehensively addresses your single sign-on needs*

*Tivoli Access Manager for Enterprise Single Sign-On provides comprehensive single sign-on to applications within the enterprise.*

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

Tivoli Access Manager for Enterprise Single Sign-On empowers enterprises to automate access to corporate information, strengthen security, and enforce compliance at enterprise end points. Tivoli Access Manager for Enterprise Single Sign-On addresses a comprehensive spectrum of single sign-on possibilities, including Microsoft Windows, Web, Java, Citrix, Microsoft Windows Terminal Services, and mainframe applications. In general, IBM Tivoli Access Manager for Enterprise Single Sign-On is a solution that applies to environments where code can be installed on the client (such as corporate desktops, kiosks, Citrix environments or Microsoft Terminal Services environments).

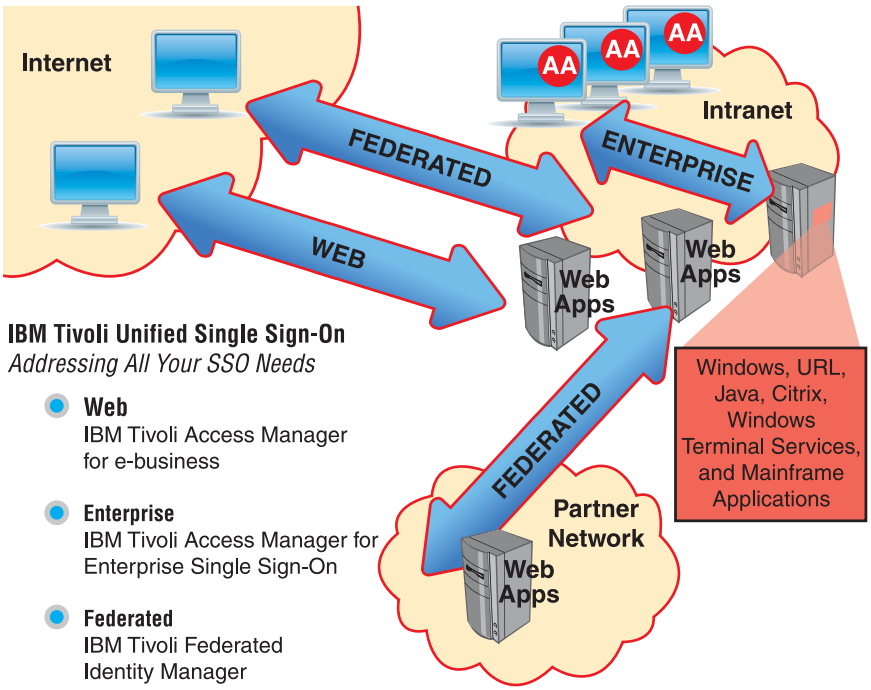


*Figure 2: Tivoli Unified Single Sign-On delivers automated sign-on for all three of the flows your business might be involved with.*

In Figure 2, IBM Tivoli Access Manager for Enterprise Single Sign-On's AccessAgent (symbolized by "AA" in a red circle) is shown offering single sign-on to a variety of enterprise applications, including Tivoli Access Manager for e-business. The AccessAgent code is installed on each client that leverages this SSO capability, and it works with the IBM Tivoli Access Manager for Enterprise Single Sign-On IMS™ Server, which manages credentials, policies, audit logs and backups.

Tivoli Access Manager for Enterprise Single Sign-On delivers the following capabilities—without requiring changes to the existing IT infrastructure:

- *Strong authentication for all user groups*
- *Enterprise single sign-on with workflow automation*
- *Comprehensive session management*
- *User-centric access tracking for audit and compliance reporting*
- *Easy, more secure remote access—any time and from anywhere*
- *Integration with user provisioning technologies*

IBM Tivoli Access Manager for Enterprise Single Sign-On can help enterprises more efficiently manage business risk, address regulatory compliance, decrease IT costs, and increase user efficiency. With IBM Tivoli Access Manager for Enterprise Single Sign-On, enterprises do not have to choose between strong security and convenience.

*Tivoli Access Manager for e-business provides single sign-on for corporate Web applications, protecting information and resources being accessed via the Web.*

#### IBM Tivoli Access Manager for e-business

Tivoli Access Manager for e-business is an authentication and authorization solution for corporate Web applications, allowing you to deliver Web single sign-on and control user access to protected information and resources being accessed via the Web. By providing a centralized, flexible, and scalable Web SSO and access control solution, IBM Tivoli Access Manager for e-business allows you to build security-rich and easy-to-manage Web-based applications and e-business infrastructure. You can use Tivoli Access Manager for e-business in conjunction with standard Internet-based applications to build highly secure and well-managed access to applications and data located in your intranet. Access can be from within the intranet, from the Internet or from an extranet.

As shown in Figure 2, IBM Tivoli Access Manager for e-business expects incoming Web-based requests from a client, and its main tasks are to authenticate the user, to provide access to resources they have permissions for, to manage the user's session, and to provide Web single sign-on for that user for the duration of their session. This is best for Internet, intranet or extranet applications where no software installation is required, and only a browser is available.

Tivoli Access Manager for e-business can be integrated into existing and emerging infrastructures to provide centralized policy management capability. Tivoli Access Manager for e-business integrates with IBM WebSphere® Application Server, IBM WebSphere Portal, IBM Tivoli Identity Manager, IBM Tivoli Access Manager for Enterprise Single Sign-On and IBM Tivoli Federated Identity Manager to form a complete Enterprise Identity Management solution.

Many businesses use IBM Tivoli Access Manager for e-business not only to address Web requests coming from the Internet, but they also deploy Tivoli Access Manager for e-business in their intranet environments, or private networks, to manage employee and contractor access to Web resources. IBM Tivoli Access Manager for Enterprise Single Sign-On integrates with IBM Tivoli Access Manager for e-business to automatically provide the identities and passwords required to log into IBM Tivoli Access Manager for e-business. In this configuration, IBM Tivoli Access Manager for Enterprise Single Sign-On handles all application logins, including login to Tivoli Access Manager for e-business, while Tivoli Access Manager for e-business seamlessly logs into Web resources under its management.

*Tivoli Federated Identity Manager provides maximum flexibility for federated single sign-on by supporting all three major federation standards.*

### IBM Tivoli Federated Identity Manager

A federation is a group of two or more trusted business partners with business and technical agreements that allow a user from one federation partner (participating company) to seamlessly access resources from another partner in a secure and trustworthy manner. In a federated business model (in which services are being federated, or shared, with business partners), the entities involved agree on an arrangement whereby a user from one company will have their identity transformed for legitimate access on a second company's Web site, without the second company needing to know the user's original identity. Tivoli Federated Identity Manager's ability to transform identities in this way enables a partner-organization to make access and authorization decisions about a user from another company (for example, customer, supplier, or client employee) without the partner organization necessarily needing to create and manage identity data for the third-party user.

With Tivoli Federated Identity Manager, a user has to know and use only one user ID and password combination in order to access not only the Web sites in their domain, but also Web sites in other companies' domains. This approach expands single sign-on to include sessions that involve visits to multiple domains, and it simplifies integration, communication and information exchange among suppliers, business partners and customers.

And with Tivoli Federated Identity Manager, organizations have maximum flexibility in configuring their cross-domain relationships with their partners, because it supports all three major federation standards: Liberty, WS-Federation, and Security Assertions Markup Language (SAML), as well as the emerging user-centric SSO initiatives such as OpenID and CardSpace. And since Tivoli Federated Identity Manager is loosely coupled with the applications it interacts with, those applications can be deployed much more quickly and maintained much more inexpensively than the alternative of handling identity transformation using proprietary APIs within each application.

In the scenario depicted in Figure 2, Tivoli Federated Identity Manager federates access to other partner systems. In essence, this extends the single-domain scenario that Tivoli Access Manager for e-business manages, and with Tivoli Access Manager for e-business and Tivoli Federated Identity Manager working together, multiple domain (federated) Web transactions can take place in a secure, authenticated and auditable fashion.

## Conclusion

*Tivoli Unified Single Sign-On comprehensively addresses all single sign-on requirements inside, outside and between organizations.*

Tivoli Unified Single Sign-On comprehensively addresses all single sign-on requirements inside, outside and between organizations. Tivoli Unified Single Sign-On is also integrated with other identity and access management solutions from IBM to provide a complete end-to-end identity, access and security compliance solution. Integration with Tivoli Identity Manager helps ensure that users can be centrally managed while single sign-on is comprehensively enabled across all use scenarios.

IBM provides a unified strategy for enterprise security that allows you to start anywhere in the security stack, then grow to cover the entire security spectrum, with the peace of mind that IBM has the breadth of solutions and the depth of integration to meet your growing needs. Tivoli Unified Single Sign-On is a good example of this unified strategy. Enterprises should consider their unified single sign-on needs and invest in a solution that can address their end-to-end single sign-on requirements from the outset, or that can grow with them as required. Point solutions from multiple vendors cannot provide the same breadth and integration.

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

For more information about IBM Tivoli Unified Single Sign-On, 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




TIW14018-USEN-00