



IBM Tivoli Access Manager for e-business

Highlights

- Implement unified authentication and authorization for online business initiatives
- Rely on the confidence and security of a Common Criteria certified product
- Simplify deployment and migration steps
- Deploy policy-based access control, with the confidence that you can scale to tens of millions of users
- Use the new Common Auditing and Reporting Service (CARS) to quickly understand risks and to address compliance challenges
- Deliver single sign-on (SSO) to your users across Web applications and beyond, including IBM WebSphere, Microsoft, BEA, and many other portal and application environments
- Adopt a service oriented architecture (SOA) for Web security that leverages advanced, standards-based authentication and authorization APIs to facilitate rapid application development, across Java 2 Enterprise Edition (J2EE), ASP.NET and C/C++ applications
- Integrate with IBM Tivoli Identity Manager for expanded provisioning, self-service, password synchronization and workflow options
- Integrate with IBM Tivoli Federated Identity Manager to derive increased value — from single-enterprise to federated configurations

Achieve robust security for online business and legacy applications

Business leaders face some critical questions about the security of their applications and transactions:

- “How can I deploy consistently secured applications that are maintained simply, with a unified access control policy?”
- “How can I provide a unified user experience — with features such as SSO — when the number of applications, servers and users I’m responsible for is growing exponentially?”
- “Why is the security of my proprietary applications so inadequate, even though I have committed large amounts of money to it?”
- “How can I address security compliance regulations and audits, when my internal controls for the disclosure of sensitive data seem to be scattered all over the place?”
- “If I invest in an authorization solution for my enterprise today, will I need to rip and replace when I address secure interactions with partners in the future?”
- “Does my business have the resources necessary to effectively implement Web services?”

IBM Tivoli® Access Manager for e-business provides a centralized approach to authenticating and authorizing access to Web and other applications that you host. The single point of authentication also makes it easy to enable advanced logon controls for your applications, including smart cards, certificates, and multi-factor or step-up authentication.

Together, these capabilities can help you manage growth and complexity, control escalating management costs and address the difficulties of implementing security policies across a wide range of Web and application resources.

Tivoli Access Manager for e-business integrates with online business applications out of the box to help you deliver highly secure, unified and personalized online business experiences. The software’s authentication, authorization and administration APIs — and integration with application platforms

such as Microsoft® .NET, J2EE™ and C/C++ — help you secure access to business-critical applications and data spread across the extended enterprise.

Within a single security domain, you can use Tivoli Access Manager for e-business to provide Web-based SSO for your portal and other application environments. Your Tivoli Access Manager for e-business environment can also be the base for cross-site authentication when you incorporate Tivoli Federated Identity Manager, which uses Security Assurance Markup Language (SAML), Liberty Alliance and Web Services Federation Language (WS-Federation) token-passing protocols.

Enjoy significant ease of use in a massively scalable package

To manage users and groups as well as the policy for their access to resources, Tivoli Access Manager for e-business includes a Web-based administration tool. Administrators can leverage the easy-to-use tool to delegate user management and security administration, where appropriate.

The centralized authentication and authorization services of Tivoli Access Manager for e-business can be provided

to Java™ applications (servlets, JavaServer Pages™ and Enterprise JavaBeans™), ASP.NET applications and C/C++ applications to keep the programming model simple. In addition to its J2EE services, The Open Group authorization APIs and .NET support, Tivoli Access Manager for e-business supports many open industry standards and common integration requirements, including:

- Lightweight Directory Access Protocol (LDAP) for storing user and group information, plus supported user registries such as IBM Tivoli Directory Server, Sun Java System Directory Server, Novell eDirectory, Microsoft Active Directory® and IBM Lotus® Domino Server. Added features include Tivoli Directory Server multidomain support, and support for Tivoli Directory Server and Sun Java System Directory Server dynamic groups.
- Metadirectory implementations, including IBM Tivoli Directory Integrator, which is provided in the product license.
- Virtual directory implementations, including those from Radiant Logic and OctetString.
- X.509 V3 client certificates for strong authentication to Web-based resources. Many certificate providers, including VeriSign, Entrust and Baltimore, are supported.
- Mutually authenticated and confidential component interactions through Secure Sockets Layer (SSL).

- Integration with Tivoli Identity Manager lets you import users, synchronize passwords between the two products and enable cost savings through user self-registration and self-service across all your security systems.
- Tivoli Access Manager for e-business audit information uses CARS to generate many useful reports for compliance purposes.
- IBM Tivoli Configuration Manager can use the authentication and authorization capabilities of Tivoli Access Manager for e-business to allow users to selectively manage the configuration of their workstations on their own. This process can help optimize user productivity and administration workload.

Tivoli Access Manager for e-business received a Common Criteria certification, under the auspices of the International Common Criteria process, administered by the National Information Assurance Partnership. This certification verifies that Tivoli Access Manager for e-business has been methodically tested and checked as part of its development cycle.

Implement policy-driven security

Tivoli Access Manager for e-business allows you to define a comprehensive policy and administer security based on that policy — giving your employees, partners, suppliers and customers role-based access that's appropriate

to each user's responsibilities. You can group users and assign permissions to groups, thereby simplifying administration of access control across multiple applications and resources.

The software gives you the power and flexibility to incorporate business rules into access control decisions. Because the rules are evaluated at run time, access control decision making is dynamic. Tivoli Access Manager for e-business enables you to manage these business rules outside of application code; consequently, you can change policy parameters that affect access without having to rewrite and recompile applications. This feature can help you deploy and adapt applications very quickly.

Tivoli Access Manager for e-business provides both Web server plug-in and HTTP reverse proxy mechanisms to suit a broad variety of Web infrastructures. The latest iteration of the proxy provides unparalleled levels of transparency to help you achieve rapid deployment and time to value. Compared to the plug-in approach, the highly secure advanced proxy model helps minimize overall hardware requirements and maintenance costs.

Facilitate compliance with audits

Tivoli Access Manager for e-business writes audit records in a standard XML format that allows easy parsing when you need to extract required information. It also exploits CARS, which provides secure, centralized collection and reporting of audit, log, statistics and other information across the extended enterprise. CARS is being added to multiple Tivoli solutions and provides out-of-the-box audit reporting.

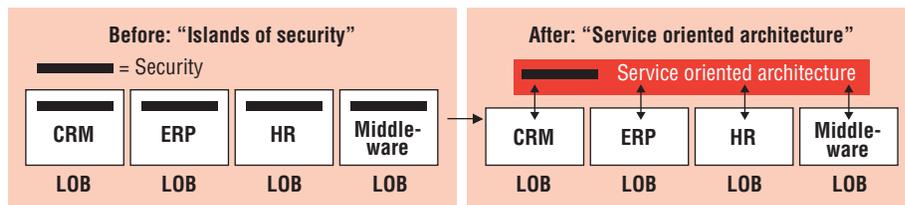
Enable security for an SOA

Application platforms such as Web servers provide security and other services to the application developer. But managing access then becomes isolated in line-of-business silos that are dependent on the skills and tools available in each application environment.

The following figure shows how — in contrast — the IBM approach helps enable businesses to operate under an

SOA. With this on demand paradigm, vital functions are provided to the business as common services that can be executed consistently and reused. Tivoli Access Manager for e-business helps provide security services to heterogeneous environments.

With this architecture in place, access control is based on a single, consistent layer that allows for applications to be deployed rapidly and security to be accurately and consistently managed. Tivoli Access Manager for e-business provides the common platform for authentication and authorization at the HTTP/HTTPS level, as well as through the provisioning of security services to application platforms like J2EE and .NET. Through integration with Tivoli Federated Identity Manager, Tivoli Access Manager for e-business can also provide the base for your Simple Object Access Protocol (SOAP) message security.



Tivoli Access Manager for e-business enables applications to call out to standard security services and thereby helps organizations minimize the size and complexity of applications.

Businesses that deploy an SOA achieve more IT reuse, which means that they deploy highly agile IT systems, can deploy applications rapidly and achieve high levels of automation.

Integrate with other identity management solutions

Tivoli Access Manager for e-business is an integrated component of IBM Tivoli identity management solutions that can help you quickly get users, systems and applications online and productive; minimize costs; and optimize the value you derive from your security and systems investments. Other IBM Tivoli identity management offerings include:

- Tivoli Identity Manager — workflow-based identity life-cycle management, including user self-care, enrollment and provisioning.
- Tivoli Federated Identity Manager — cross-domain authentication, authorization and SSO, plus Web services security management.
- Tivoli Directory Server — a highly scalable and highly available LDAP directory for sharing user and other information.
- Tivoli Directory Integrator — a 100-percent Java implementation that synchronizes user information across numerous registries, directories, databases and other repositories — across your operational environment and without adding yet another repository to the mix.

Together, IBM Tivoli identity management solutions help you effectively manage internal users and an increasing number of customers and partners.

Deliver highly secure, unified user experiences

Tivoli Access Manager for e-business includes support to help large numbers of users participate in convenient, available and personalized transactions. With authentication and access control services for online business and enterprise applications and resources, you can secure customer, supplier, employee and partner connectivity across:

- Web servers.
- J2EE-based application servers, such as IBM WebSphere® Application Server, BEA WebLogic Server and Oracle.
- Microsoft .NET application servers.
- Industry-leading Web applications with a list that grows all the time:
 - Siebel
 - Microsoft Exchange
 - Oracle
 - IBM WebSphere Portal
 - IBM WebSphere Edge Server
 - IBM WebSphere Host On-Demand
 - IBM WebSphere Host Publisher
 - IBM WebSphere Host Access Transformation Server

- IBM DB2® Content Manager
- IBM WebSphere Everyplace® Server Service Provider Offering
- IBM Lotus Domino®
- IBM Lotus iNotes™
- IBM Lotus QuickPlace®
- IBM Lotus Sametime®
- SAP Internet Transaction Server (ITS)
- SAP Enterprise Portal
- Epicentric Foundation Server
- BroadVision One-To-One Enterprise
- Vignette V5
- Plumtree Corporate Portal
- Oracle Portal
- KANA Platform
- i2 TradeMatrix
- iPlanet
- Aelita Directory Manager
- Blockade ESconnect
- Cash-U Pecan
- Citrix MetaFrame/NFuse XP
- Kintana Suite
- OpenConnect WebConnect
- Rocksteady RockNet
- Verity K2 Enterprise
- WinCom Systems Switching Server

Tivoli Access Manager for e-business accommodates a broad range of possible user-authentication mechanisms, including user IDs and passwords, client-side certificates, mobile and wireless identities, and support for RSA SecurID tokens.

The software can also designate the authorization level required for access to protected resources and enforce a “step-up” policy when users must provide the next level of authentication.

The authentication mechanism is completely configurable. It can be extended internally through “C” shared libraries. Plus, a new external authentication interface allows authentication to be offloaded to an external server through an easy-to-use HTTP interface, thereby accommodating Web applications written in any language. You can use this feature to enable:

- Interaction with the user during authentication.
- Authentication checking against multiple user repositories — directory chaining.
- Separation of policy and user repositories.
- Many other types of authentication integration — Tivoli Access Manager for e-business includes a license for Tivoli Directory Integrator, which can act as a metadirectory and authentication service.

Furthermore, the software helps you deliver enhanced session management to keep track of what a user is doing — even across multiple concurrent sessions. When users log out once,

the software can log them out everywhere to avoid concurrent logons. The software can also enforce your policies about inactivity timeouts, three-strikes rules and other options across multiple enforcement points.

Through the work that IBM does with security vendors, Tivoli Access Manager for e-business does away with the need to enable your applications for such capabilities as:

- Fingerprint readers, such as DaonConnect for Tivoli Access Manager software.
- Virtual private network (VPN) appliances, such as Ingrian DataSecure Appliance and Neoteris IVE.
- SSL accelerator cards, such as IBM 4960 PCI, nCipher nFast, Rainbow Technologies CryptoSwift PCI and Eracom ProtectServer Orange.
- Combo cards that combine SSL accelerators and hardware key storage, such as IBM 4758 PCI and nCipher nForce.
- Directories, such as Siemens DirX 6.0 and SecurIT CDAS for Vasco DigiPass.
- Tokens, such as Aladdin Knowledge Systems eToken.
- Mobile digital certificates, such as Entrust TruePass.
- Load balancers, such as F5 Networks BIG-IP.
- SSO tokens, such as Sena Systems PortalPass.

Tivoli Access Manager for e-business helps you deliver a consistent and secure user experience by having end users use a single identity to gain access to resources — according to your authorization rules. With support for Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO), users only need to log on once to the enterprise portal or Microsoft desktop (using Active Directory). Subsequently, they can access Web resources without the need for another logon — Tivoli Access Manager for e-business performs the authentication against Active Directory seamlessly.

To help you achieve highly scalable deployments, Tivoli Access Manager for e-business performs intelligent load balancing over replicated servers. This solution is already deployed in many implementations that exceed one million users and has been shown to scale to tens or hundreds of millions of users. It also takes advantage of SSL accelerator card technology and secure hardware key-stores, and provides a failover capability that allows automatic switchover to backup Web servers.



Hardware and software requirements

The Tivoli Access Manager for e-business HTTP proxy mechanism for SSO and authorization enables the support of any HTTP-compliant application regardless of the platform on which it runs. The software also provides plug-ins for the most popular Web server platforms.

The Tivoli Access Manager for e-business proxy and infrastructure can run on the following platforms:*

- IBM AIX® on IBM RISC System/6000®
- Sun Solaris on Sun SPARC
- Microsoft Windows® 2000 Advanced Server
- Microsoft Windows 2003 Standard Server and Enterprise Server
- HP-UX
- United Linux® including SUSE Linux Enterprise Server for Intel®, IBM S/390® and IBM zSeries®
- Red Hat Enterprise Linux for Intel®, S/390 and zSeries
- IBM WebSphere Application Server for z/OS®

Tivoli Access Manager for e-business works with Netscape Navigator, Mozilla and Microsoft Internet Explorer browsers, as well as pervasive devices that support the Wireless Application Protocol or i-mode protocol.

For more information

To learn more about Tivoli Access Manager for e-business and integrated solutions from IBM, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli/solutions/security

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 reducing 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.

© Copyright IBM Corporation 2005

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

Produced in the United States of America
11-05
All Rights Reserved

AIX, DB2, Domino, Everyplace, IBM, the IBM logo, iNotes, Lotus, QuickPlace, RISC System/6000, S/390, Sametime, Tivoli, WebSphere, z/OS and zSeries are trademarks of International Business Machines Corporation in the United States, other countries or both.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

Active Directory, Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

*The product release notes — with more detailed platform support status — can be found in the IBM Tivoli Product Information Center: publib.boulder.ibm.com/infocenter/tivihelp/v1r1/index.jsp

IBM customers can view the latest platform support matrix at ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html