



---

### Caratteristiche principali

- Implementazione della gestione centralizzata dell'autenticazione e dell'autorizzazione per applicazioni di tipo Web-based
  - Disponibilità di funzioni di Web SSO (single sign-on) verso applicazioni Web eterogenee, inclusi IBM WebSphere, Microsoft®, SAP e molti altri ambienti applicativi
  - Gestione e applicazione del controllo dell'accesso basato su policy e la sicurezza Web alle applicazioni aziendali, con la capacità di scalare di decine di milioni di utenti.
- 

# IBM Tivoli Access Manager for e-business

*Implementazione di una soluzione di autenticazione altamente scalabile. Web di accesso SSO (Single Sign-On) ed autorizzazione*

## Ottenere un livello di sicurezza affidabile per le applicazioni legacy

I business leader affrontano alcune domande critiche sulla sicurezza delle loro applicazioni e transazioni:

- “Come è possibile implementare un accesso sicuro in applicazioni Web eterogenee facilmente gestibili con una policy di controllo degli accessi unificata?”
- “In che modo è possibile garantire un'esperienza utente omogenea con funzionalità quali l'accesso SSO basato su Web, l'autenticazione avanzata e la gestione delle sessioni in una situazione in cui il numero di applicazioni, server e utenti gestiti cresce in modo esponenziale?”
- “Per quale motivo il livello di sicurezza delle applicazioni Web proprietarie sono così inadeguate, benché siano stati investiti ingenti capitali?”
- “Come posso risolvere il problema dei rischi di sicurezza del Web, delle disposizioni in termini di conformità e dei controlli, quando le policy interne richiedono il controllo degli accessi ad applicazioni e servizi sensibili per l'azienda da parte di utenti interni, esterni e amministratori?”
- “Investendo oggi in una soluzione di gestione degli accessi per la propria azienda, in futuro sarà necessario rimuoverla e sostituirla per gestire una collaborazione sicura con partner B2B (Business to Business) e/o utenti privati B2C (Business to Consumer)?”
- “L'azienda avrà la capacità di ampliare in modo efficiente il controllo degli accessi alle applicazioni Internet, alle distribuzioni cloud e ai servizi SaaS (Software as a Service), nonché la capacità di utilizzare i servizi Web e Web 2.0?”

IBM Tivoli Access Manager for e-business offre un approccio personalizzato per l'autenticazione e l'autorizzazione dell'accesso utente ad applicazioni Web, nonché soddisfa le esigenze principali dell'azienda in termini di sicurezza Web e conformità. Inoltre, la disponibilità di un unico punto flessibile di autenticazione e gestione delle sessioni semplifica



## Tivoli

le procedure di attivazione di controlli degli accessi avanzati e basati su policy per le proprie applicazioni, includendo l'integrazione con smart card, certificati digitali, l'autenticazione a più fattori, e meccanismi di step-up authentication.

Insieme, queste funzionalità possono consentire di gestire la crescita e la complessità, di controllare i crescenti costi per la gestione della sicurezza delle applicazioni e di indirizzare le difficoltà nell'implementazione delle policy sulla sicurezza attraverso una vasta gamma di risorse Web e applicative.

Tivoli Access Manager for e-business si integra con le applicazioni Web per fornire un ambiente di business online estremamente personalizzato, unificato e sicuro.

Il reverse proxy estremamente scalabile svolge il ruolo di Point of Contact per le funzioni di identificazione, autenticazione ed autorizzazione semplificando l'integrazione con piattaforme comuni quali Microsoft .NET, Java™ Platform Enterprise Edition e C/C++. Consente una protezione degli accessi alle applicazioni business-critical e la distribuzione dei dati all'interno dell'azienda estesa.

All'interno di un'organizzazione, è possibile utilizzare Tivoli Access Manager for e-business per fornire l'accesso in Web SSO a tutte le applicazioni di tipo Web-based. L'ambiente Tivoli Access Manager for e-business può inoltre essere la base per l'autenticazione cross-domain e per la collaborazione sicura con business partner utilizzando l'integrazione con Tivoli Federated Identity Manager, che utilizza protocolli standard quali SAML (Security Assurance Markup Language), OpenID, Liberty Alliance e Web Services Federation Language (WS-Federation) in modo da supportare le iniziative di integrazione con l'utente finale in scenari B2C.

### **Semplicità di utilizzo in una soluzione altamente scalabile**

Per gestire gli utenti, i gruppi e le politiche per l'accesso alle risorse, Tivoli Access Manager for e-business offre una console amministrativa basata su Web. Gli amministratori possono usare la console Web di facile utilizzo per delegare la gestione delle applicazioni e della sicurezza, secondo necessità.

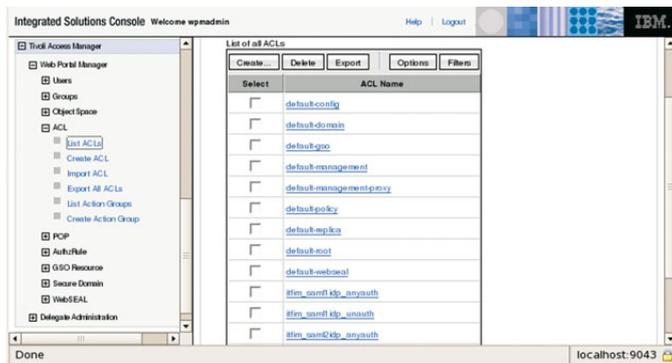
I servizi di autenticazione e l'architettura reverse proxy centralizzati di Tivoli Access Manager for e-business possono essere forniti alle applicazioni Java, alle applicazioni ASP.NET e alle applicazioni C/C++ per mantenere semplice il modello di programmazione per la distribuzione aziendale. Oltre ai servizi Java, alle API di autorizzazione Open Group e al supporto .NET, Tivoli Access Manager for e-business supporta molti open standard di settore e requisiti di distribuzione operativi IT comuni, compresi:

- LDAP (Lightweight Directory Access Protocol) per la memorizzazione delle informazioni dell'utente e dei gruppi. Oltre a directory utente quali IBM Tivoli Directory Server (inclusa nella licenza del prodotto) sono supportati Sun Java System Directory Server, Novell eDirectory, Microsoft Active Directory e IBM Lotus Domino Server. Funzioni aggiuntive includono il supporto esteso per gruppi dinamici e per multi-dominio. Funzioni aggiuntive includono il supporto esteso per gruppi dinamici e per multi-dominio.
- Implementazioni meta-directory, incluso IBM Tivoli Directory Integrator, fornito nella licenza del prodotto. Tivoli Directory Integrator consente di sincronizzare le informazioni dell'utente tra i numerosi registri, directory, database e altri repository senza dover aggiungere un altro repository all'ambiente IT.
- Certificati client X.509 V3 per l'autenticazione forte su risorse di tipo Web. Sono supportati molti provider di certificazione, inclusi VeriSign e Entrust.
- Mutual authentication e confidenzialità nell'interazione tra i componenti tramite il SSL (Secure Sockets Layer).
- Integrazione con sistemi per la gestione identità esistenti, ad esempio Tivoli Identity Manager che consente di importare gli utenti e i ruoli, di sincronizzare le password fra due prodotti e di permettere risparmi in termini di costi attraverso il provisioning degli utenti integrato, con la gestione di accesso ad applicazioni Web per consentire la governance IAM in tutti i sistemi.
- Integrazione con Tivoli Security Information and Event Manager, che consente di fornire una soluzione per il controllo degli accessi, per le verifiche e il reporting di conformità a ciclo chiuso.
- Integrazione con i dispositivi SOA di IBM WebSphere DataPower per garantire un accesso di tipo SSO e una gestione delle sessioni utente più sicure per ambienti Web 2.0 e Web Services.
- L'aggiornamento a Tivoli Federated Identity Manager offre scenari di Federated SSO e casi d'uso per il self care in ambienti B2C per estendere il controllo degli accessi utente alle applicazioni locali e remote, ai servizi SaaS e basati su cloud.

## Implementa una gestione policy-driven gli accessi e alle applicazioni Web

Tivoli Access Manager for e-business consente di definire una politica completa per il controllo degli accessi alle applicazioni Web e di imporre i controlli di sicurezza in base ad elenchi di ACL (Access Control List), offrendo ai propri dipendenti, partner, fornitori ed utenti finali una modalità di accesso basata su ruoli adeguata alle responsabilità di ciascun utente. È possibile riunire gli utenti in gruppi a cui assegnare autorizzazioni, il che semplifica l'amministrazione del controllo degli accessi a più applicazioni e risorse.

Tivoli Access Manager for e-business fornisce sia un architettura basata su plug-in per Web Server sia un architettura basata su reverse proxy di tipo HTTP (HyperText Transfer Protocol) per soddisfare le esigenze di una vasta gamma di infrastrutture di sicurezza Web. L'ultima versione del reverse proxy offre livelli senza precedenti di trasparenza, prestazioni e supporto per diverse tipologie di collegamenti (junction) di effettuare una distribuzione rapida, di semplificare l'integrazione delle applicazioni di backend e di accelerare il time to value. Rispetto all'approccio basato sul plug-in del Web server, questo modello avanzato e altamente sicuro di reverse proxy consente di ridurre al minimo i requisiti hardware complessivi e i costi di sviluppo e manutenzione delle applicazioni.



Tivoli Access Manager for e-business fornisce le policy di controllo degli accessi predefinite per attivare la sicurezza e l'accesso in Web SSO in applicazioni eterogenee e ambienti IT aziendali.

## Miglioramento della sicurezza Web al livello delle applicazioni

Oltre a fornire un livello di sicurezza solida al livello dell'utente, Tivoli Access Manager for e-business risolve problematiche correlate specificamente alla protezione di applicazioni contro minacce e vulnerabilità comuni. Poiché le aziende aprono i propri ambienti per l'accesso degli utenti alle applicazioni aziendali e Internet, l'esigenza di protezione degli accessi e di miglioramento della sicurezza Web diventa fondamentale. La funzionalità di sicurezza Web avanzata può risultare decisiva in quanto le applicazioni Web diventano obiettivi sempre più appetibili per le minacce di sicurezza. Il reverse proxy del Tivoli Access Manager for e-business agisce come un firewall di identità per supportare implementazioni sicure di applicazioni Web e collabora con IBM Rational AppScan per risolvere le vulnerabilità principali delle proprie applicazioni. Rational AppScan valuta le vulnerabilità comuni delle applicazione, come ad esempio XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), processi di autenticazione interrotti e sessioni di gestione, nonché errori nel limitare l'accesso agli URL con cui comandi non autorizzati vengono trasmessi dai siti Web ritenuti attendibili dagli utenti. Tali comuni vulnerabilità Web consentono di aggirare i controlli di accesso degli utenti. Tivoli Access Manager for e-business consente di risolvere tali vulnerabilità una volta rilevate mediante la creazione di un tunnel permanente tra l'utente e l'applicazione e mediante un supporto di gestione delle autenticazioni e delle sessioni più solido per le applicazioni possibili oggetti di attacco.

## Aumento della scalabilità e delle prestazioni

Per consentire distribuzioni altamente scalabili, Tivoli Access Manager for e-business supporta un'implementazione basata su proxy modulare, si integra con i programmi di bilanciamento del carico commerciali effettuando un bilanciamento dei carichi intelligente su server replicati. Questa soluzione è già distribuita in molte implementazioni che superano le decine di milioni di utenti e ha dimostrato doti di scalabilità fino a centinaia di milioni di utenti. Sfrutta inoltre la tecnologia delle schede di accelerazione SSL mediante la protezione degli archivi di chiavi e offre una funzionalità di fail-over che consente il passaggio automatico ai server di backup. Per migliorare

## Tivoli

ulteriormente la scalabilità, i domini amministrativi configurabili consentono il supporto di più istanze dei componenti del reverse proxy (WebSEAL) in una singola directory/LDAP Server. Offre anche funzionalità di replica semplificata nel ciclo di vita di distribuzione e la configurazione del supporto cluster in più istanze di WebSEAL. La versione più recente migliora le prestazioni con le giunzioni combinate dei protocolli TCP (Transmission Control Protocol) ed SSL e mantiene una connessione persistente con le applicazioni di back-end per garantire una maggiore protezione.

Inoltre, il software consente una migliore gestione delle sessioni per tenere traccia delle attività degli utenti, anche tra più sessioni simultanee. Quando gli utenti si disconnettono da una postazione, il software consente di disconnetterli da tutte le restanti postazioni per evitare accessi concorrenti. Il software consente inoltre di far rispettare le politiche relative ai timeout di inattività, alle normative che si rifanno alle threestrikes laws e altre opzioni applicabili nei diversi punti di accesso applicativo.

Tivoli Access Manager for e-business comprende un servizio di gestione delle sessioni centralizzato che consente di migliorare le prestazioni in diversi modi tra cui:

- Il numero di sessioni create dagli utenti è limitato dalla policy, in questo modo le nuove richieste di accesso verranno bloccate una volta raggiunto il numero massimo.
- Una funzione di configurazione dinamica che elimina i riavvii del server di gestione della sessione.
- L'alta disponibilità è nativa consentendo la gestione di più server tramite WebSphere Application Server Network Deployment.

### La distribuzione di un ambiente utente estremamente sicuro ed unificato

IBM collabora con fornitori di applicazioni leader nel mercato attraverso il proprio programma "Ready for Tivoli" e garantisce un'integrazione immediata con le soluzioni software di terze parti. Con i servizi di autenticazione e di controllo degli accessi per le applicazioni e le risorse aziendali online, è possibile proteggere le connessioni dei clienti, dei fornitori e dei partner relative a quanto segue:

- Server Web
- Directory service
- Server di applicazioni J2EE, quali IBM WebSphere Application Server, Oracle WebLogic Server, JBoss e Oracle Application Server

- Gateway e firewall XML
- Un elenco crescente di applicazioni Web leader nel settore:
  - Apache Tomcat
  - IBM Cognos Business Intelligence
  - IBM Content Manager
  - IBM FileNet P8 Platform
  - IBM Lotus Domino
  - CA eTrust Directory
  - EMC Documentum eRoom
  - IBM Lotus Sametime
  - Microsoft .NET
  - Microsoft Exchange
  - Microsoft Internet Information Server
  - Microsoft Office Communications Server
  - Microsoft SharePoint®
  - Oracle Database
  - Oracle eBusiness Suite
  - Oracle Internet Directory
  - Oracle PeopleSoft
  - SAP Netweaver ABAP
  - SAP Netweaver Java
  - SAP Internet Transaction Server (ITS)
  - Siebel.

Tivoli Access Manager for e-business consente la configurazione di una vasta gamma di meccanismi di autenticazione utente, compresi ID utente e password, certificati digitali X509V3 lato client, token universali, lettori biometrici, identità mobili e wireless, token PKI-USB e smart card per l'accesso fisico e alla rete.

Il software consente inoltre di designare i livelli di autenticazione richiesti per l'accesso a risorse protette e far rispettare una policy di tipo "step-up" quando gli utenti devono fornire le credenziali per il livello successivo di autenticazione.

Il meccanismo di autenticazione è completamente configurabile. Può essere inoltre esteso internamente tramite librerie "C" condivise. Inoltre, un'interfaccia EAI (External Authentication Interface) consente di demandare a sistemi esterni la fase di

## Tivoli

autenticazione utilizzando l'interfaccia HTTP per consentire una facile integrazione con server esterni. È possibile utilizzare questa funzionalità per attivare quanto segue:

- Interazione con l'utente durante le richieste di autenticazione a più fattori
- Controllo dell'autenticazione in più repository utente (concatenamento delle directory)
- Separazione dei repository delle policy e dell'utente
- Molti altri tipi di integrazione con sistemi di autenticazione forte e di terze parti, tra cui soluzioni basate sui rischi ed adattive.

Tramite il programma Ready for Tivoli, IBM offre un'integrazione delle funzionalità di autenticazione avanzata con molti fornitori. Per ulteriori dettagli, visitare il sito [ibm.com/tivoli/features/opal](http://ibm.com/tivoli/features/opal)

Tivoli Access Manager for e-business consente di fornire un ambiente utente coerente e sicuro grazie all'utilizzo di una singola identità da parte degli utenti finali per ottenere l'accesso alle risorse, in base a quanto stabilito dalle proprie regole di autorizzazione. Grazie al supporto del protocollo SPNEGO (Simple Protected Negotiation) dell'API GSSAPI (Generic Security Service Application Programming Interface), gli utenti devono autenticarsi una sola volta al desktop per poter accedere a più risorse Web.

Per garantire un accesso SSO semplice tra i desktop Microsoft Windows® e le applicazioni di back-end, questa funzionalità inoltre si estende alle applicazioni .NET, quali Microsoft SharePoint ed Exchange Server. Per semplificare ulteriormente l'accesso degli utenti, Tivoli Access Manager for e-business consente una scalabilità uniforme per ampliare il controllo degli accessi Web alle distribuzioni B2C e consente di accedere in modo protetto alle iniziative aziendali e basate su portali online.

---

### Tivoli Access Manager for e-business in sintesi

---

Tivoli Access Manager for e-business è una soluzione basata su reverse proxy altamente scalabile che offre una gestione della sicurezza delle applicazioni in tutta l'azienda per il Web SSO l'autenticazione e l'autorizzazione utente per il supporto di tutte le applicazioni compatibili con il protocollo HTTP a prescindere dalla piattaforma in cui viene eseguita. Il software per la gestione dell'accesso offre inoltre plug-in per le piattaforme di server Web più comuni.

Il componente reverse proxy (WebSEAL) e l'infrastruttura di Tivoli Access Manager for e-business possono girare nelle seguenti piattaforme:<sup>1</sup>

- IBM AIX 5.2, 5.3 e 6.1
- Sun Solaris 9, 10 su Sun SPARC e Sun Solaris 10 su Opteron
- Microsoft Windows 2003, 2008 e 2008 R2 Standard Server e Enterprise Server
- HP-UX 11i V2 e V3 su PA-RISC e Integrity
- SUSE Linux® Enterprise Server 9, 10 e 11 per x86, IBM System i, IBM System p e IBM System z
- Red Hat Enterprise Linux Advanced Server e Enterprise Server 4.0 e 5.0 per x86, System i, System p e System z

Tivoli Access Manager for e-business utilizza i browser Mozilla Firefox e Microsoft Internet Explorer, così come dispositivi pervasivi che supportano il protocollo Wireless Application Protocol o il protocollo i-mode.

---

<sup>1</sup> La documentazione del prodotto e le note sulla versione sono disponibili nel Product Information Centre IBM all'indirizzo <http://publib.boulder.ibm.com/infocentre/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml>  
I clienti IBM possono visualizzare la matrice di supporto della piattaforma più aggiornata all'indirizzo [ibm.com/software/sysmgmt/products/support/Tivoli\\_Supported\\_Platforms.html](http://ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html)

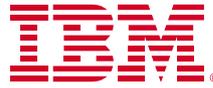
## Ulteriori informazioni

Per maggiori informazioni su IBM Tivoli Access Manager for e-business, contattate il vostro responsabile commerciale o un Business Partner IBM o visitare il seguente sito Web:

[ibm.com/software/it/tivoli/security](http://ibm.com/software/it/tivoli/security)

## Informazioni sul software IBM Tivoli

Il software Tivoli fornito da IBM facilita una gestione efficiente ed efficace delle risorse, delle attività e dei processi IT, consentendo di soddisfare esigenze di business costantemente mutevoli, garantendo una gestione flessibile e dinamica dei servizi IT e contribuendo a ridurre i costi. Il portafoglio Tivoli comprende software per la gestione della sicurezza, della conformità, dello storage, delle prestazioni, della disponibilità, delle configurazioni, delle operazioni e del ciclo di vita dell'infrastruttura IT e si basa sulle capacità di IBM di fornire servizi, supporto e ricerca all'avanguardia.



### IBM Italia S.p.A.

Circonvallazione Idroscalo  
20090 Segrate (Milano)  
Italia

La home page di IBM Italia si trova all'indirizzo **ibm.com**

IBM, il logo IBM, [ibm.com](http://ibm.com), AIX, Cognos, DataPower, Domino, FileNet, Lotus, Rational, Sametime, System i, System p, System z, Tivoli e WebSphere sono marchi o marchi registrati di International Business Machines Corporation negli Stati Uniti e/o in altri paesi. Se questi e altri termini commerciali di IBM sono contrassegnati da un simbolo del marchio (® o ™) alla loro prima ricorrenza nel presente documento informativo, tali simboli indicano marchi registrati o non registrati di proprietà di IBM negli Stati Uniti al momento della pubblicazione del presente documento informativo. Tali marchi possono anche essere marchi registrati o comunemente riconosciuti in altri paesi.

Un elenco aggiornato dei marchi IBM è disponibile sul Web nella pagina "Informazioni su copyright e marchi" all'indirizzo: [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Java e tutti i marchi e logo con Java sono marchi o marchi registrati di Oracle e/o sue affiliate.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft, Windows e SharePoint sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Altri nomi di società, prodotti e servizi possono essere marchi o marchi di servizio di altre società.

I riferimenti contenuti in questa pubblicazione a prodotti, programmi o servizi di IBM non implicano la volontà, da parte di IBM, di rendere tali prodotti, programmi o servizi disponibili in tutti i paesi in cui IBM opera.

Qualsiasi riferimento a prodotti, programmi o servizi di IBM non implica che possano essere usati solo prodotti, programmi o servizi IBM. In alternativa, è possibile utilizzare qualsiasi prodotto, programma o servizio funzionalmente equivalente.

I prodotti hardware IBM vengono costruiti utilizzando parti nuove, oppure parti nuove ed usate. In alcuni casi, il prodotto hardware potrà non essere nuovo e risultare già installato in precedenza. Independentemente da ciò, sono validi i termini della garanzia IBM.

Questa pubblicazione è fornita a titolo esclusivamente informativo. Le informazioni sono soggette a modifiche senza preavviso. Per informazioni più aggiornate sui prodotti e sui servizi IBM, contattate l'ufficio vendite o il rivenditore IBM più vicino.

IBM non fornisce assistenza legale, contabile o di controllo e non dichiara né garantisce che i propri prodotti o servizi siano conformi alla legislazione vigente. I clienti sono responsabili dell'osservanza di ogni legge ed obbligo normativo applicabile, comprese le leggi e le norme nazionali.

Le fotografie possono mostrare dei prototipi.

© Copyright IBM Corporation 2011  
Tutti i diritti riservati.



Si prega di riciclare