IBM Tivoli Federated Identity Manager

Employ user-centric federated access management to enable secure online business collaboration

Highlights

- Enhance B2B and B2C collaborations and user access control across the business ecosystem through simplified application integration and secure information sharing in federated environments
- Improve the user experience and lower the TCO through federated access control to on- and off-premise applications, SaaS and cloud-based services, and B2C user self care
- Simplify integration and Web access management across Java™, .NET and mainframe-based applications and services

Exchanging critical information across company boundaries—among customers, suppliers and partners—is a necessity in today's fast-paced world. End users expect to access all your services via a single interface, user name and password. Yet the proliferation of Web services, cloud and software-as-a-service (SaaS) deployments creates its own set of identity management and compliance challenges. Collaborating and managing user and services identities across a business ecosystem places substantial demand on IT infrastructures. With an ever-increasing amount of vital information contained in different security domains, using federated single sign-on (SSO) and user access management techniques to help integrate this information can provide quick benefits and savings.

IBM Tivoli® Federated Identity Manager helps you establish an identity trust management framework to know which users are connecting to your services and what credentials are being used to connect to them without having to manage each of those individual users. Tivoli Federated Identity Manager will validate and propagate the required credentials end to end, from a point-of-contact server through an enterprise service bus (ESB) to the back-end mainframe. The software provides concurrent support for leading federated SSO protocols, including Security Assertion Markup Language (SAML) 1.0/1.1/2.0, OpenID, Information Card Profile, Liberty Identity Federation Framework (ID-FF) 1.1/1.2 and Web Services (WS)-Federation, enabling users to connect to multiple, heterogeneous business sites, while helping to preserve the confidentiality of user data.

Tivoli Federated Identity Manager delivers two key capabilities:

- ***Federated SSO***—to centrally manage access, enhance user productivity and facilitate trust by delivering SSO across separately managed infrastructure domains, both within an organization and across organizations.
- ***Identity mediation service for cloud, SaaS and Web services implementations***—to reduce administrative costs, establish trust and facilitate compliance by managing, mapping and propagating user identities.

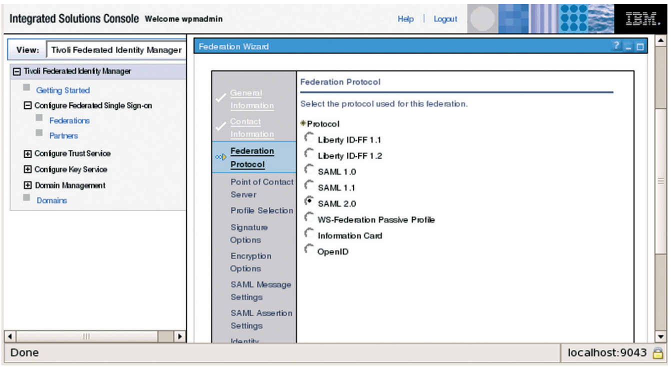
Through these two powerful and modular capabilities, Tivoli Federated Identity Manager enables partner interactions that are trusted, convenient, auditable and address key compliance concerns related to partner access from other domains. Designed to minimize impact on business applications, Tivoli Federated Identity Manager can help you reduce costs and speed deployment timeframes for integrating applications within your collaboration infrastructure. Use it to:

- Support broad federation functionality by enabling SSO, rich security customization and Web services security.
- Provide identity service to validate and centrally manage access to on- and off-premise cloud/SaaS deployments.
- Simplify the integration of identity and security across Java, .NET and mainframe environments.
- Manage user authentication and identification information about business partners through support for multiple, open standards-based identity and security tokens.
- Automate the enrollment of external user accounts and entitlements and provide access to customer portal and online business initiatives.

Enhance B2B and B2C collaborations via simplified identity management

Tivoli Federated Identity Manager helps organizations provide customers, partners and employees with greater flexibility to access multiple business applications (across Java, .NET and mainframe applications and services) while reducing the complexity of managing multiple identities. For instance, you can integrate Tivoli Federated Identity Manager with an organization's Web applications without using proprietary application programming interfaces (APIs). In addition, you can use the B2C user self-care service for enrollment, password setup/change/reset capabilities and securing the B2C collaboration scenarios.

Tivoli Access Manager for e-business is included with Tivoli Federated Identity Manager and helps you secure access to corporate Web applications via an HTTP/HTTPS connection, and provides centralized authentication and session management, and single sign on to a wide variety of application servers including Java and .NET. This proxy-based solution provides loose coupling between the federated SSO middleware and the application security layer, so a wide variety of Web applications can be connected into a federated environment with little or no application changes. In addition, Web applications and their associated middleware and servers can be upgraded without changes to the integration with the federated SSO services, and you can easily add new federation relationships and protocols to collaborate with business partners. This federation deployment capability can dramatically reduce time to value and maintenance costs, compared to the more intrusive API- or plug-in-based approaches.



Federation Protocol

Select the protocol used for this federation.

*Protocol

○ Liberty ID-FF 1.1
○ Liberty ID-FF 1.2
○ SAML 1.0
○ SAML 1.1
● SAML 2.0
○ WS-Federation Passive Profile
○ Information Card
○ OpenID

Tivoli Federated Identity Manager enables user-centric identity management and SSO using open standards.

User-centric identity management through open standards support

Trust between parties in a business transaction is paramount, yet today this trust is increasingly threatened with the continued rise in identity thefts and other fraudulent activities. Identity managers must move from enterprise-centric identity management to a user-centric approach that puts customers, partners and suppliers in control of asserting trust, determining where sign-on is occurring and which specific user attributes they want to share between an identity provider and a relying party or service provider.

Tivoli Federated Identity Manager goes beyond traditional identity management offerings by supporting user-centric identity management through integration with open standards frameworks, such as OpenID and Information Card Profile, using identity selectors from Microsoft® Windows® CardSpace and the Higgins Trust Framework that do not require sharing of metadata between identity and service providers. These open identity frameworks encourage collaboration between organizations and business partners, and help provide a greater level of service to end users.

A federated, user-centric identity management can help you:

- Drive down identity management and maintenance costs (for consumers, employees and contractors).
- Increase authentication strength.
- Enhance compliance reporting and auditability.

Advanced operational management features ease identity management tasks

Your identity management team can leverage a wide range of operational capabilities and ease-of-use features built into Tivoli Federated Identity Manager, including:

- Ability to support multiple point-of-contact servers, including IBM Tivoli Access Manager for e-business, third-party access management offerings, IBM WebSphere®, Microsoft .NET, and third-party Web servers via a customized Web server and custom point-of-contact server plug-ins.
- Cross-domain identity assurance through expanded support for SSO token types.
- An advanced command line infrastructure and trust chain editor for quick deployments of identity service in SOA and Web 2.0 environments.
- Advanced key management through a console, to easily change key store passwords and manage certificates during operation.
- The ability to make run-time services reload configuration changes without requiring server restarts.
- Enhanced integration with IBM Tivoli Identity Manager, IBM WebSphere DataPower®, IBM WebSphere Enterprise Service Bus, IBM WebSphere Message Broker and deploy consistent Web and federated single sign-on to WebSphere Portal deployments.
- Simplified application integration across Java, .NET and mainframe applications and services.

Federated access management for cloud and SaaS deployments

Organizations are looking at cloud and SaaS deployments as a way to reduce costs. Applications such as sales management, human resource management, and customer relations management are increasingly implemented using a cloud or SaaS approach.

SaaS and cloud adopters can benefit further with the deployment of federated SSO. It allows users to sign on once, and then securely access multiple SaaS-based applications without additional logins. Support for SAML 2.0 facilitates a complete trust model across the sender and the receiver regardless of the underlying architecture, enabling identity federation in a cloud environment. The Security Token Service (STS) can help transform, validate and exchange the identity credentials across cloud/SaaS-based applications, enabling rapid deployments and faster adoption. Tivoli Federated Identity Manager also strengthens application security and minimizes administrative tasks such as password resets and user account management for a cloud-based infrastructure.

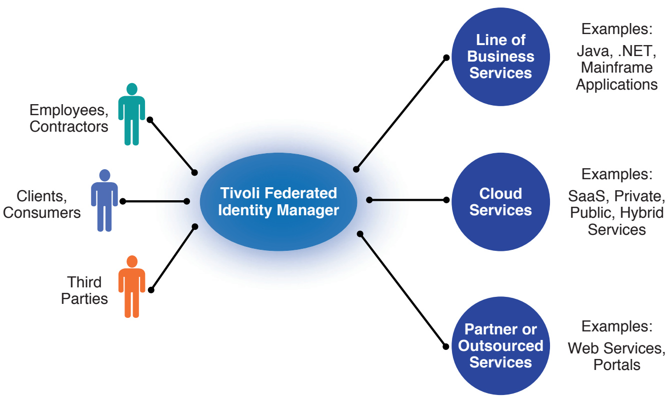
Establish identity awareness for Web services and SOA environments

Many benefits of an SOA come from the reuse of existing application assets by dividing them into discrete business services and then combining these services in various combinations to implement business processes. Many existing applications are developed independently and have different representations of user identity and different ways in which identities can be exchanged. Successfully managing different user identities and improving visibility of true identity exchange are critical to the success of your SOA.

Tivoli Federated Identity Manager offers a robust, standalone identity service tool, providing identity awareness—in SOA and Web services environments to IBM WebSphere DataPower SOA Appliances, your ESB or IBM Customer Information Control System (CICS®)—to any organization.

Numerous features help enrich your SOA environment and improve visibility across multiple security domains and the IT infrastructure:

- A security token service (STS) offers common identity mediation services for your SOA and Web services deployments by validating, mapping and propagating auditable identities. The Tivoli Federated Identity Manager identity service can be accessed from leading XML firewall gateways, ESBs and/or a mainframe CICS environment to provide identity mediation services for interactions across multiple security domains and with external organizations and services.
- Support for multiple security tokens—including SAML assertions, IBM RACF® PassTicket, x.509 certificate and Kerberos tickets, as well as customizable token types—to communicate authentication information about a business partner or service all the way to the back-end, mainframe or legacy applications.
- Administrators can link Web services transaction access to an actual user identity using RACF PassTicket to improve transparency of IBM z/OS® or other legacy applications in an SOA.


Employees, Contractors
Clients, Consumers
Third Parties
Tivoli Federated Identity Manager
Line of Business Services
Examples: Java, .NET, Mainframe Applications
Cloud Services
Examples: SaaS, Private, Public, Hybrid Services
Partner or Outsourced Services
Examples: Web Services, Portals

Tivoli Federated Identity Manager expands B2B and B2C collaboration by simplifying application integration, self-care user enrollment and federated single sign-on across the business ecosystem.

Maintain auditable access into the mainframe environment

The Tivoli Federated Identity Manager enables you to conduct "identity validations and translations" by checking identity from the point of login, to data access, to transaction completion. Credentials are verified in the beginning and then passed along during each step. So while you are able to quickly deploy new services or repurpose existing services to support business goals, the unique ability of Tivoli Federated Identity Manager to simultaneously flow auditable identities from the distributed environment to the back-end mainframe environment enables you to maintain accountability and meet growing compliance requirements by helping you maintain a central, consistent source of user identities.

Choose the federation solution that's right for your organization

In addition to using Tivoli Federated Identity Manager on distributed systems, you can use Tivoli Federated Identity Manager on z/OS for a high-availability identity management solution that also supports SSO and identity service natively on your IBM System z® mainframe environment.

Also, organizations that want to establish federated identity management with a small-to-midsize business partner can leverage IBM Tivoli Federated Identity Manager Business Gateway, an entry-level solution that offers access management for cloud and SaaS environments with SAML-only protocol support, and can be seamlessly upgraded to Tivoli Federated Identity Manager for an enterprise-level deployment.

Tivoli Federated Identity Manager at a glance

Supported platforms:

- IBM AIX® 5.2, 5.3, 6.1
- Sun Solaris 9, 10 (SPARC)
- Microsoft Windows 2003, 2008, and 2008 R2 Standard Server and Enterprise Server
- Red Hat Linux® Advanced Server 3.0 and 4.0 for IBM System x®
- Red Hat Linux Advanced Server and Enterprise Server 5.0 for System x
- Red Hat Linux Advanced Server 4.0 and 5.0 for IBM System p® and IBM System z
- SUSE Linux Enterprise Server 9 , 10, and 11 for System p, System x and System z
- HP-UX 11i V2 and V3 on Integrity

Web Server plug-in component supports the following:

- Apache Web Server 2.0 and 2.2
- IBM HTTP Server 6.1
- Microsoft Windows Internet Information Server 6.0

For more information

To learn more about how Tivoli Federated Identity Manager can help your organization employ new user-centric, trusted identity management and Web services identity awareness, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/security

About IBM Tivoli service management software

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

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.

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

Produced in the United States of America
March 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

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

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

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

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

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.

Please Recycle

Tivoli software