IBM Tivoli Federated Identity Manager

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

Highlights

- Enhance business-to-business and business-to-consumer collaborations with centralized user access management through application integration and secure authentication in federated environments
- Improve user experience and lower costs through business-to-consumer user self-care and federated access control to on- and off-premises applications, Software as a Service (SaaS) and cloud-based services
- Enable single sign-on (SSO) for external users to internal applications and for internal users to cloud-based applications
- Provide web fraud detection and prevention capabilities through risk-based access control

Collaboration across an organization's business ecosystem plays a key role in businesses extending their application access to business partners, customers and consumers. Additionally, internal users need access to externally hosted applications, including cloud-based applications and business partner applications. But with a federated approach, end users can have a seamless sign-on experience to these applications, helping to eliminate the need to provide multiple user IDs and passwords. Using federated SSO and user access management techniques to help integrate this information can provide quick benefits and savings.

IBM® Tivoli® Federated Identity Manager is an access-management solution that provides web and federated SSO to end users across multiple applications. With browser-based integration and open standards, this solution can provide quick gains in user productivity and user experience. And it can reduce administration costs with federated SSO. End users authenticate once and then seamlessly obtain access to applications and services inside and outside their network infrastructure.

Tivoli Federated Identity Manager provides federated SSO capabilities in a way that can minimize the impact on business applications, helping to reduce costs and deployment timeframes for integrating applications into a collaboration infrastructure.

Tivoli Federated Identity Manager provides risk-based access capabilities that can help secure an organization's information assets. With risk-based access, each transaction is assessed using static and contextual attributes to

calculate the risk. This risk assessment determines whether a user's request to access information should be permitted, denied or permitted with some further authentication.

This solution also provides flexible web and identity services using its own security token service (STS) to validate and issue a wide variety of identity formats and to flow auditable identities between applications and services across multiple security domains and the enterprise. This capability ties together applications running on disparate operating system platforms with different sign-on token support, transparently to the end user. End users can use SSO to access desktop- and mainframe-based applications. To aid compliance activities, Tivoli Federated Identity Manager also provides integrated audit data collection and reporting.

Tivoli Federated Identity Manager is offered in two packages:

- **IBM Tivoli Federated Identity Manager Business Gateway** enables external users to access their internal applications using SSO and provides internal users with SSO capabilities for cloud-based applications. This solution can be used to bring together independent business units, enable business-to-consumer collaboration and promote customer collaboration with partners and suppliers. It delivers fast time-to-market for e-business and cloud initiatives, provides a lightweight, easily deployable application for straightforward SSO needs, and provides simplified integration with online business partners. This solution provides pre-configuration for common deployment patterns and is an excellent solution for small and midsize businesses as well as large enterprises.
- **IBM Tivoli Federated Identity Manager** includes Tivoli Federated Identity Manager Business Gateway and IBM Tivoli Access Manager for e-business. This solution provides web access management along with federation support for a more comprehensive access-management solution.

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

- Support broad federation functionality by enabling SSO, rich security customization and web services security
- Provide identity services to validate and centrally manage access across private, public and hybrid cloud deployments
- Manage user authentication and identification information about business partners through support for multiple, open standards-based identity and security tokens
- Support the emerging Open Authorization (OAuth) standard for authorization, which enables users to share private resources stored on one site with another site—for example, photos, files or contact lists—without having to hand out their credentials
- Offer predefined federations that provide configuration assistance to ease definitions and setup
- Support Secure Hash Algorithm (SHA-2), a set of cryptographic hash functions designed by the US National Security Agency
- Support Security Assertion Markup Language (SAML), WS-Federation, Information Card Profile, OpenID and OAuth; Tivoli Federated Identity Manager Business Gateway also offers a security token service, which supports WS-Trust, username, SAML, IBM Resource Access Control Facility (RACF®), X.509 and Kerberos tokens
- Detect and prevent fraud by implementing risk-based access capabilities for context-aware controls that provide superior web security that spans online environments, including cloud and mobile, while helping organizations manage the complexity and costs of web application management

Collaboration through federation

Tivoli Federated Identity Manager can improve the user experience and reduce administration costs through its collaborative capabilities. It provides:

- Federated SSO for information sharing across private, public and hybrid cloud deployments; it enables central access management and enhanced user productivity, and it facilitates trust by delivering SSO across separately managed infrastructure domains—both within an organization and across organizations
- Support for cloud-based applications such as IBM LotusLive™, Salesforce.com and Google Apps through the use of open standards such as SAML, Liberty, WS-Federation, WS-Security, WS-Trust, OpenID and OAuth
- An identity mediation service for cloud, SaaS and web services implementations that helps reduce administrative costs, establish trust and facilitate compliance by managing, mapping and propagating user identities
- A command-line infrastructure and an enhanced trust-chain editor for quick deployment of the security token server
- Key management via a console that can change key-store passwords and manage certificate operations
- The ability to develop additional Tivoli Federated Identity Manager plug-ins using Eclipse extensions
- Support for organization- and application-specific deployments
- Predefined federations, which offer configuration assistance to ease definitions and setup

In addition, Tivoli Federated Identity Manager Business Gateway provides web SSO capabilities. While Tivoli Federated Identity Manager uses open standards to provide a smooth migration pathway to an enterprise-level application in a single, easy-to-deploy application, Tivoli Federated Identity Manager Business Gateway is built especially for small to midsize organizations to bring together customers, business partners and suppliers. It can deliver fast time to market for e-business initiatives, provide a lightweight, easily deployable application for straightforward SSO needs, and provide simplified integration with online business partners. It generates audit logs, tracking and incident reports to help meet compliance policies. This solution adds expanded token support to the existing SAML support. Tivoli Federated Identity Manager Business Gateway also offers a smooth migration to the enterprise-level Tivoli Federated Identity Manager solution, with little or no business application changes. Moreover, both solutions use the same management user interface to minimize administration training and transition costs.

Federated access management for cloud and SaaS deployments

Many 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, which allows users to sign on once, 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 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.

Security token service

The STS built into Tivoli Federated Identity Manager provides identity mediation services for a service-oriented architecture (SOA) implementation by managing, mapping and propagating identities. The functionality provided by the STS can also be accessed from leading XML firewall gateways, including IBM WebSphere® DataPower® SOA Appliances, to provide identity mediation services to these boundary devices for XML-based interactions with external organizations.

Many organizations are moving away from using multiple application-level user IDs and passwords for a given individual. The Tivoli Federated Identity Manager STS can be used to map distributed user IDs to RACF user IDs and associated RACF pass tickets (one-time passwords for authentication to RACF). The RACF ID and pass ticket can then be used to connect to IBM z/OS® hosted resources using individual user identities.

Tivoli Federated Identity Manager STS, in this use case, can be hosted on z/OS or a supported distributed platform. It can also be leveraged as a critical component within an IBM federated enterprise service bus (ESB). An ESB is a flexible connectivity infrastructure for integrating disparate applications and services, but many ESBs have identity and compliance challenges and cannot efficiently connect and track identities across separately managed domains. This can lead to significant administrative costs and auditing difficulties. The federated ESB simplifies administration and ensures compliance by making an organization's ESB identity aware.

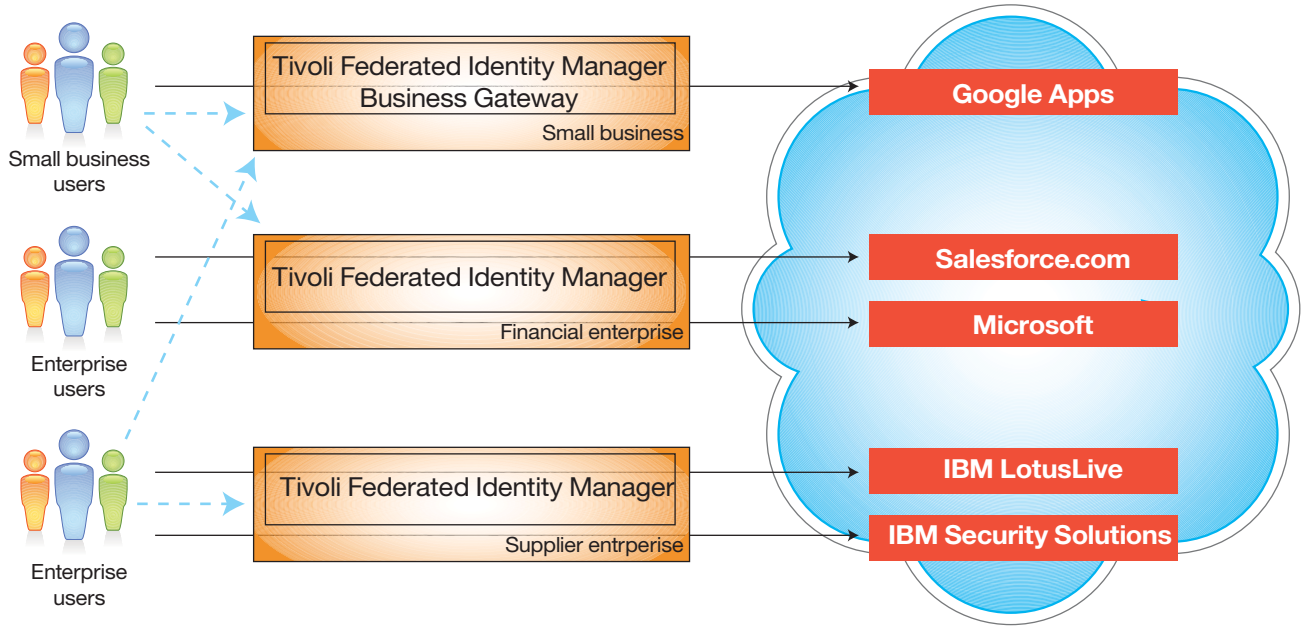
Risk-based access for fraud detection and prevention

Risk-based access is a pluggable and configurable component for Tivoli Federated Identity Manager that:

- Improves security during authentication and authorization of business transactions
- Assesses risk based on static, contextual and analytically calculated attributes
- Calculates a risk score based on multiple weighted attributes
- Provides policy rules that determine whether an access request must be permitted, denied or challenged

Risk-based access provides several capabilities to identify potential risk and limit the ability for an attacker to use stolen credentials, including:

- Silent device registration where the system does not require any user interaction
- Ready-to-use policy attributes that are specific to risk-based access
- A risk-scoring engine that calculates a risk score for the current transaction based on configurable weights assigned to context attributes and behavior attributes; with a high risk score, further challenges are presented to the user or access is denied; with a low risk score, the user is permitted access
- An interface for configuring and managing the risk-based access policies and policy attributes with commands available through the IBM WebSphere Application Server AdminTask framework, which supports Jacl scripting, Jython scripting and programmatic Java API



Tivoli Federated Identity Manager expands business-to-business and business-to-consumer collaboration by simplifying application integration, self-care user enrollment and federated SSO across the business ecosystem.

IBM Tivoli Federated Identity Manager at a glance

Supported platforms:

- IBM AIX® v5.3 TL4, AIX v6.1, AIX v7.1 on IBM Power Systems™
- Red Hat Enterprise Linux (RHEL) 3 Update 5 AS/ES x86-32
- RHEL 4 Update 2 AS/ES x86-32
- RHEL 5 Advanced Platform x86-32 and x86-64
- RHEL Server 6 x86-32 and x86-64
- RHEL 4 Update 2 AS/ES Power System
- RHEL 5 Advanced Platform Power System
- RHEL Server 6 Power System
- RHEL 4 Update 4 AS/ES IBM System z®
- RHEL 5 Advanced Platform System z
- RHEL Server 6 System z
- SUSE Linux Enterprise Server (SLES) 9 SP2, 10, 11 x86-32 and x86-64
- SLES 9 SP2, 10, 11 Power System
- SLES 9 SP2, 10, 11 System z
- Sun Solaris 9 and 10 Sun SPARC
- Solaris 10 x86-64
- Microsoft Windows Server 2003 SP1 Standard Edition and Enterprise Edition x86-32
- Windows Server 2008 Standard Edition and Enterprise Edition x86-32
- Windows Server 2008 Standard Edition and Enterprise Edition x86-64
- Windows Server 2008 R2 Standard Edition, Enterprise Edition, Datacenter Edition x86-64

Why IBM?

IBM has delivered federated identity management and identity awareness for organizations worldwide. As a leader in the delivery of federated identity management, we have helped many organizations maximize their capabilities so they can offer higher value-based services to their clients and partners.

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 Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2013

Please Recycle

TID14021-USEN-03