Tivoli® software

IBM Tivoli Identity Manager

Highlights

- ***Reduce overhead costs by automatically managing roles, accounts, and access rights throughout the user life cycle***
- ***Correct and remove noncompliant access rights through periodic recertification workflows or automatically via role-based access control policies***
- ***Manage and prevent business process conflicts through separation of duty policies***
- ***Centralize user access rights control while maintaining local autonomy via self-service features that also reduce help-desk load***
- ***Accelerate onboarding of new applications and users via pre-configured policies and templates***
- ***Be audit-ready and compliant with regulations by quickly producing detailed reports***

Deliver security-rich, automated and policy-based user identity management

To effectively compete in today's challenging environment, organizations are increasing the number of users—customers, employees, citizens, partners and suppliers—allowed to access information across applications, mainframes, service oriented architectures, the Web and other environments. As a result, CIOs continually face three major challenges: meeting internal and regulatory compliance requirements, maintaining an effective security posture, and simultaneously striving for measurable return on investment.

IBM Tivoli® Identity Manager addresses these challenges by providing an easy-to-deploy, user-friendly solution that delivers security-rich, policy-based user

and role management across the IT infrastructure. Tivoli Identity Manager delivers:

- *A role hierarchy that streamlines administration, provides visibility of user access, and helps bridge the gap between how business users view their IT resources and the actual IT implementation of user access rights.*
- *Web self-service for managing business roles, accounts, group membership and passwords.*
- *An embedded workflow engine for automated submission and approval of user requests and periodic certification of user access rights.*
- *A robust provisioning engine that adds and removes user access rights based on membership in business roles or requests for user accounts and fine-grained entitlements like shared folders or Web portlets.*
- *A set of controls that enhance security, including preventative separation of duties and closed-loop reconciliation that detects and corrects changes to native target systems.*
- *Broad, out-of-the-box support for managing user access rights and passwords on applications and systems, plus a rapid integration toolkit for managing custom applications.*
- *Flexible reporting for user access rights leveraging automatic synchronization of user data from different repositories.*

Be audit-ready with automated features

Tivoli Identity Manager delivers automated audit readiness, with certification of fine-grained access rights, separation of duties, closed-loop reconciliation and prebuilt reports that offer direct auditor access and map low-level IT entitlements into business-friendly descriptions of what users can actually do with their access.

Automatically recertify access rights

Tivoli Identity Manager helps keep the simple tasks simple while still allowing for advanced customization. Powerful access rights recertification features provide granular, auditor-friendly details for compliance along with policies that can be easily configured using wizards and templates. Use it to:

- *Quickly define recertification policies based on frequently used scenarios, such as "access to the financial data warehouse must be approved by an employee's manager once a quarter."*
- *Ease administrative impact of manager approval via bulk recertification of a user's roles, accounts and groups.*
- *Model advanced workflows and organization processes with the Web-based graphical workflow designer.*
- *Conduct compliance attestation for a large number of IT resources not configured for automated account provisioning.*

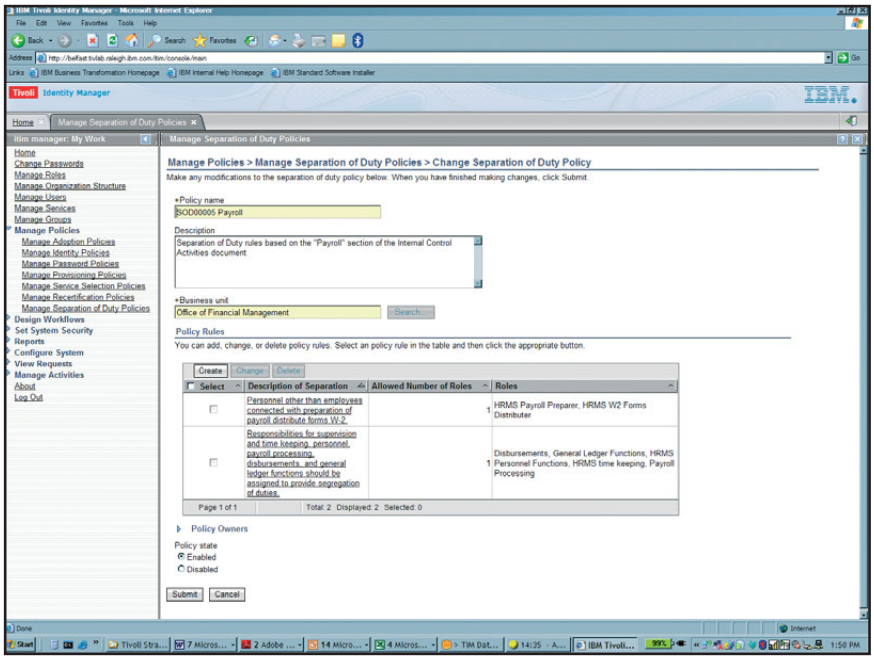
Establish separation of duties to manage business process conflict

Tivoli Identity Manager helps manage business process conflicts with IT user access rights. Preventative, policy-based separation of duties enables you to define a business conflict (e.g. an investment banker cannot also be a stock broker at the same time) and ensure proper administration of user access rights. This associates the appropriate security and compliance requirements that are critical to preventing business conflicts with the roles and provisioning policies governing user access rights. Organizations can still maintain business flexibility by utilizing an exception workflow that gathers the business justification when an exception to the separation of duties policy is required.

Use automated reconciliation to detect and correct noncompliant accounts

"Closed loop" reconciliation features can automatically detect and repair access policy violations that occur due to erroneous changes made on a managed resource's administrative console. You can use access rights reconciliation, recertification and reporting to:

- *Automatically load and reconcile account data.*
- *Identify and eliminate dormant and ghost accounts.*
- *Provide ongoing proof for compliance and auditing.*
- *Maintain records of changes related to access rights.*



Manage and prevent business process conflicts through separation of duty policies

Create audit trails with detailed reports

Tivoli Identity Manager enables you to deliver reports on consolidated workflows as well as access rights changes. Policy compliance monitoring and reporting includes audit trail collection, correlation and reporting to address compliance mandates. Report examples include:

- *Recertification history*
- *Orphan and dormant accounts*
- *Separation of duties summary*

By using the IBM Tivoli Common Reporting Module alongside Tivoli Identity Manager, you can leverage custom report authoring, report distribution, and run and manage reports from multiple Tivoli products.

Help reduce errors by automating user administration

User administration can be automated using roles and self-service requests. Both can simplify and reduce the cost of administering user access to resources and help reduce the potential for administrative errors and inconsistencies inherent in manual processes.

Roles typically represent collections of users and/or permissions. Role management, together with user provisioning, automates the process of administering user access by delivering access rights to target systems based on the roles assigned to each user. Self-service requests can be configured to let you define which attributes are allowed for self-service and which require approval. You can approve, modify or reject requests electronically through a Web browser, and users can be automatically notified of the status of their requests. To make the process easier for users, the self-registration and self-enrollment interfaces collect information automatically, and the approval of user requests can be automated by a workflow engine.

Deliver access via a hierarchical role structure

Tivoli Identity Manager offers a role hierarchy that establishes parent/member role relationships to automatically create user access rights through the notion of inheritance between roles. You can administer a role structure that contains business roles (collections of users) and/or application roles (collections of

permissions). And when roles are associated with provisioning policies, they can automatically grant, modify, or remove user access rights. As a result, it reduces the number of administrative objects used to manage user access and enhances the visibility of access across your organization.

Leverage request-based provisioning and access entitlements

Managers and delegated administrators can take advantage of comprehensive, request-based provisioning to easily request (with approval workflow) user access to roles, accounts or fine-grained access entitlements, such as shared folders and Web portlets.

In addition, end users and line-of-business managers can view current access rights, personal profile information and status of pending requests; request new access to roles, accounts or fine-grained access entitlements (for example, shared folders or Lightweight Directory Access Protocol [LDAP] groups); update profile information; change or reset passwords; and take action on management tasks such as approving new access rights or recertifying existing access rights.

Establish simple or advanced workflows and policies

The powerful workflow and policy engine within Tivoli Identity Manager can easily be configured in either "simple" or "advanced" mode. "Simple mode" uses predefined best-practice templates to implement basic provisioning, recertification and compliance alert workflows. Configuration and setup is easy using only drop-down lists, check boxes and radio buttons—no scripting or programming knowledge is required.

"Advanced mode" provides a graphical, drag-and-drop workflow designer to quickly organize and easily develop workflow processes to support the organization's provisioning policies. For example, the workflow engine supports parallel and serial approval processes, and also provides checkpoints in a workflow process to allow input of additional provisioning information.

Establish group management

Tivoli Identity Manager helps automate and centralize the definition of groups used to manage user access on native applications and systems. You can add, modify or delete groups directly from Tivoli Identity Manager and streamline the process for defining access and assigning user membership to groups.

Use self-service features to reduce help-desk calls

Intuitive, customizable Web self-care interfaces in Tivoli Identity Manager enable users to perform tasks such as password changes and request new access rights, helping to reduce costly help-desk calls. For example, a self-service challenge/response system is included to enable users to correct the common problem of forgotten passwords without calling the help desk. A sophisticated self-service interface and embedded workflow engine helps users securely and easily manage portions of their own information. Web-based, self-service, role- and rule-based administration features enable you to group users according to business needs and delegate functionality—such as who can add, delete, modify and view users, and reset user passwords—to other organizations and business units as needed.

> *IBM Tivoli is positioned in the Leaders Quadrant of Gartner, Inc.'s Magic Quadrant for User Provisioning.*
>
> – Gartner Magic Quadrant for User Provisioning, Research Note G00159740, 15 August 2008[1]

Customizable interface delivers an optimized user experience

Tivoli Identity Manager is not built with a one-size-fits-all approach to identity management. Rather, a simple, highly customizable user interface includes out-of-the-box configurations for those who participate in each stage of the life cycle, including auditors, end users, managers, help-desk personnel, application owners and administrators—so users see the information that is most important to them.

You can easily customize and integrate the interface into an existing intranet or extranet site. Customization options include style sheets and on/off configuration options, such as whether or not to show navigation "bread crumbs" or a header banner. And, there is no need to reimplement customizations during software upgrades.

Quickly configure systems and onboard new services

Tivoli Identity Manager can help you significantly reduce turn-on time for new accounts and onboarding of new managed services. Preinstalled adapters, wizard-driven templates and built-in account defaults help accelerate deployments and reduce the learning curve for new users.

Support existing, new and customized environments with little or no coding

Tivoli Identity Manager provides out-of-the-box support for more than 50 end point managed systems that can be managed remotely or with a local adapter, simplifying deployment. It also provides tools to help assimilate these new business resources as they are added.

Through its dynamic schema discovery process and flexible architecture, embedded IBM Tivoli Directory Integrator technology can provide Tivoli Identity Manager with administrative control over organizations' homegrown applications—without requiring you to write or maintain code.

For more information

To learn more about how IBM Tivoli Identity Manager and integrated solutions from IBM can help you increase IT efficiency, reduce administration costs and address policy compliance needs, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security

About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards–based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers 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 is the overall worldwide identity and access management security software revenue leader.*
>
> – IDC Worldwide Identity and Access Management 2008-2012 Forecast and 2007 Vendor Shares, August 2008

Tivoli Identity Manager at a glance

Supported platforms:

- HP-UX
- IBM AIX®
- Red Hat Enterprise Linux®
- Sun Solaris
- SUSE Linux Enterprise Server
- Microsoft® Windows® Server
- z/OS®

Supported managed systems:

Integrates with dozens of popular applications and platforms:

- Operating systems
- Databases, directories, content management systems
- Access control systems
- E-mail and messaging systems
- Service desks
- Business applications and ERP systems

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.

[1] The Gartner Magic Quadrant is copyrighted 2008 by Gartner, Inc., and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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

Produced in the United States of America
June 2009

TID10294-USEN-02