Strengthen access control, facilitate compliance and support operational governance across the enterprise

Tivoli® software

IBM Tivoli Security Policy Manager

Highlights

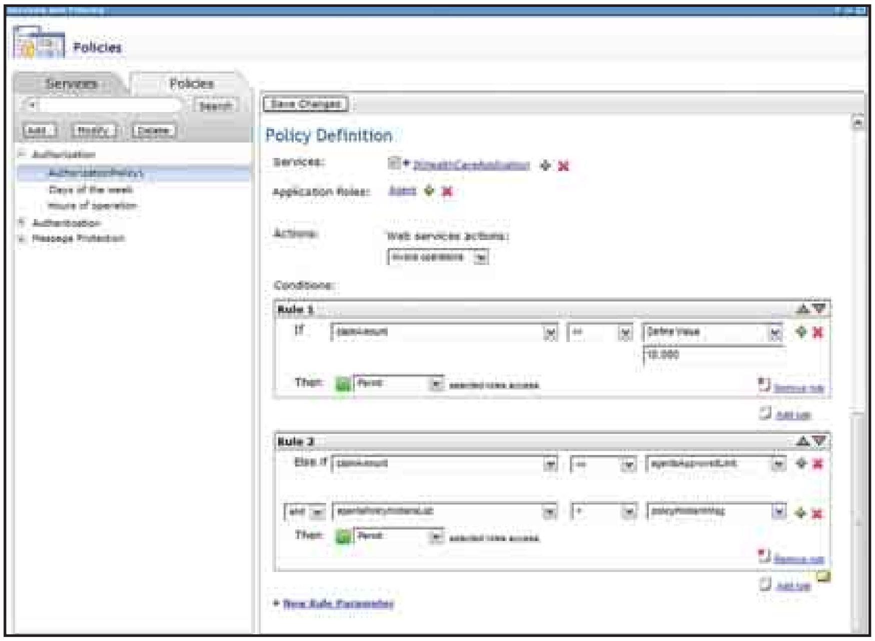
- ***Minimize operational inefficiencies and vulnerability related to application entitlements and SOA security policy management***
- ***Manage SOA security policies throughout the policy lifecycle, from authoring and publishing to enforcing and updating***
- ***Manage application entitlements and enforce policies at run time, strengthening your organization's security posture***
- ***Direct change and control policies centrally, to more quickly, consistently and efficiently address new or more stringent compliance requirements***
- ***Use federated policy management to help bridge the gap between business and IT approaches to security policy***

Enterprises face new and emerging challenges in securing access to their applications and services in today's IT environment. The growing number of industry regulations and compliance requirements drive the need to control access to business transactions and applications using complex, fine-grained authorization policies. Increasing demand to respond to business changes and re-use sensitive data across multiple applications and services is increasing the costs of coding and of maintaining redundant application security development. The increasing risk of intellectual property loss and threats drives the need to ensure data-level entitlements and access control to an increasing number of users. This includes employees in multiple roles, contractors, business partners, and even competitors in some cases.

The adoption of service-oriented architecture (SOA) and Web 2.0 poses unique security policy management challenges—the loose coupling of services and aggregate (mash-up) applications within and across the enterprise creates multiple policy management points, each of which may require its own administration. These security policies and configurations are currently specific to individual products with tool-specific definitions. The IT reality to manage these policies in a heterogeneous environment is manual, error-prone and creates costly islands of security administration. Also, the rapid deployment of Web services increases the risk of deploying inconsistent access control policies and unintended access to business sensitive data. Especially for organizations like banks, hospitals, and insurance agencies, protecting data stored in applications across the business environment becomes a critical factor, and just as critical is the ability to provide a complete audit trail for proof of policy enforcement when required.

Manage SOA security and application entitlements on a single platform

IBM Tivoli® Security Policy Manager offers a comprehensive solution for addressing these security challenges, providing unified SOA security policy management and application entitlements management across registries and applications. Tivoli Security Policy Manager enables full policy lifecycle management—authoring, transforming, distribution, enforcement and monitoring. This adaptable tool provides the ability to import application roles and integrate with existing identity systems, and leverages standards like XACML, WS-Trust, WS-Policy and others to offer centralized control, making it easier to address tightening or new compliance requirements. Tivoli Security Policy Manager offers security as a service, decoupling the native authentication or authorization capabilities of an application to improve security and reduce the complexity of the IT infrastructure. And its OSGi-based plug-in architecture not only works seamlessly with existing security but also allows for extending the product easily in multiple areas.



Application Roles: Agent

Rule 1: If claimAmount ... Define Value 10,000 Then Permit selected roles access

Rule 2: Else if claimAmount ... and ... Then Permit selected roles access

Tivoli Security Policy Manager provides a range of capabilities to help organizations address diverse policy requirements in SOA environments.

For example, a security administrator could use a unified security policy tool to manage, delegate and track changes to all security policies for Web services and applications at an insurance company. He or she could use the common authorization framework of Tivoli Security Policy Manager to control access to claims, billing, quotes, records and credit information with message security policies for authentication, confidentiality and integrity. An application developer at the same company could externalize access control decisions and use the authorization service, helping to reduce costs and time spent on internal access control.

Manage security policies in SOA environments

Throughout the cycle of SOA security policy management, Tivoli Security Policy Manager can simplify and consolidate policies and processes. Starting by obtaining service definition and metadata from the WebSphere® Service Registry and Repository (WSRR), it then acts as the centralized policy administration point where one can define not only message security policies but also authorization polices. These policies can be published either back to the service registry or to enforcement points like WebSphere DataPower, where the policies can then be enforced.

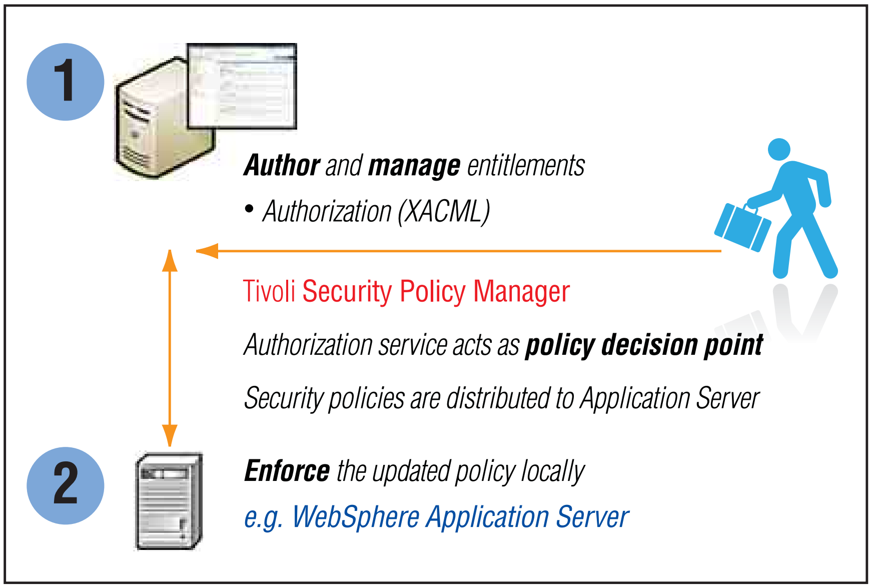
Manage and enforce application entitlements

IT application owners are able to use Tivoli Security Policy Manager to author application entitlements and fine-grained access control policies and transform them to XACML for distributed policy decision. These entitlement policies are based on identity, transaction and service/resource context. IT operations can consistently delegate, distribute and enforce security policies across IT application environments, including WebSphere Application Server–hosted applications and custom applications.

Enhance business agility and improve IT efficiency

Tivoli Security Policy Manager consists of multiple components that can help enhance business agility and improve IT efficiency.

- *The Policy Manager–provides a user interface and data store for complete lifecycle management of services and policies, including service discovery, policy authoring, configuring and distribution*
- *Runtime Security Services (RTSS)–provides the engine for the run time evaluation of authorization policy and decision*


1
Author and manage entitlements
• Authorization (XACML)
Tivoli Security Policy Manager
Authorization service acts as policy decision point
Security policies are distributed to Application Server
2
Enforce the updated policy locally
e.g. WebSphere Application Server

Tivoli Security Policy Manager can make it easier for IT organizations to comply with line of business decisions.

- *WebSphere Policy Enforcement Point–an IBM WebSphere plug-in allowing for container-managed authorization control leveraging RTSS for authorization decisions*

Tivoli Security Policy Manager allows IT organizations to author, administer, transform and distribute security policies from a single platform. For example, a hospital can author a security policy based on roles and groups (user/subject, service/target), then configure the policy to best control dissemination of information. The organization could also discover resources and metadata for creating or classifying policies, and import services from different registries and applications.

Tivoli Security Policy Manager can import application roles and integrate with existing identity systems, making it a flexible tool that can adapt and grow with your organization and can help you address changing compliance requirements. Each application wants to know information about a user's service level or role, and this information is often spread over many applications (e.g., LDAP, HR system, databases, etc.). The software's identity service uses a common interface for communication and helps provide security and privacy.

Transform business policies into enforceable instructions

The software's Runtime Security Services provide the performance, scalability and reliability needed to enforce policies. These services can be used to render decisions of high-level business entitlements into operational-level authorization instructions, then deploy and enforce these instructions using a policy enforcement point (e.g. WebSphere plug-in). The RTSS software can uniquely render authorization decisions in either a remote or local mode (to the application) with support for partial, application-specific policy replication. This enables IT operations to support high-performance production-level deployments.

Collaborate across domains with federated policy management

Because the software offers federated policy management, it makes it easier for IT organizations to bridge the gap between business and IT approaches to security policy, enabling collaboration across domains. Tivoli Security Policy Manager helps administrators organize and manage metadata and enforcement rules, orchestrating who defines them, how they are defined, how they are distributed, how they are enforced, and how their lifecycle is defined.

Enable end-to-end authorization

Tivoli Security Policy Manager for Application Entitlements externalizes security and enables end-to-end application authorization. The key application entitlements management features include policy administration point (PAP), an intuitive user interface that uses wizards and drag-and-drop features, and policy decision point (PDP), an interoperability-tested policy engine built in to the offering. The policy enforcement point (PEP) package supports appropriate plug-ins that natively enforce standards-based policy queries and can support custom applications like Java™ and .NET, as well as mainframe-based applications. Tivoli Security Policy Manager for Application Entitlements is flexible, enabling the use of information from multiple policy information points (PIP) to evaluate and render decisions.

Leverage interoperability and integration through open standards

Tivoli Security Policy Manager integrates with other Tivoli products such as IBM Tivoli Federated Identity Manager, IBM Tivoli Access Manager for e-business, and IBM Tivoli Security Information and Event Manager, helping you extend your capabilities and add value to your existing investments in Tivoli software. Tivoli Security Policy Manager also provides interoperability through collaboration on open standards service registries with Microsoft®, Oracle, SAP, Sun and others. Supported standards include:

- Service interfaces –
- Token exchange and authentication: WS-Trust
- Identity service: IdAS
- Policy expressions –
- Authorization policies: XACML
- Message protection policies such as WS-Security Policy
- Programming model –
- Web Services: WS-Trust, XACML
- Java

Implement a policy-driven approach within your enterprise

Tivoli Security Policy Manager can save time and money by minimizing operational inefficiencies and vulnerability related to entitlements and security policy management. It can give you a level of control and visibility while minimizing development costs, streamlining processes, and helping to manage audit requests.

Tivoli Security Policy Manager is offered in two package options to address the client's IT and application-specific requirements. They include:

- *Tivoli Security Policy Manager for Application Entitlements.*
- *Tivoli Security Policy Manager for SOA.*

Tivoli Security Policy Manager for Application Entitlements provides application owners and administrators the ability to externalize the security from the application logic and simplify the management of complex authorization policies for new and existing applications, including customized applications. It offers organizations the ability to respond quickly to business changes through centralized application roles, entitlements and data-level access control, and helps improve compliance and security management with roles, rules and attributes-based access control. This package includes the policy manager, run-time security services and the WebSphere policy enforcement point.

Tivoli Security Policy Manager for SOA enables enterprise architects and security operations to centrally manage and enforce security policies for Web services resources across multiple policy enforcement points, including WebSphere DataPower SOA appliances. It helps to reduce the manual, inconsistent and costly administration of security policies at each policy enforcement point and enables operational governance with the ability to delegate and audit all changes to policies. This package includes the policy manager with the out-of-box integration with WebSphere Services Registry and Repository and WebSphere DataPower SOA appliances.

IBM Tivoli Security Policy Manager at a glance

Supported platforms:

- IBM AIX® 5.3
- Red Hat Enterprise Linux® (RHEL) 5.0 AS/ES IA64
- Red Hat Enterprise Linux (RHEL) 5.0 AS/ES x86-32
- Red Hat Enterprise Linux (RHEL) 5.0 AS/ES x86-64
- Red Hat Enterprise Linux (RHEL) 5.0 WS x86-32
- Red Hat Enterprise Linux (RHEL) 5.0 WS x86-64
- Solaris 10 SPARC
- Solaris 9 SPARC
- SuSE Linux (SLES) 10.0 Enterprise Server x86-32
- SuSE Linux (SLES) 9.0 Enterprise Server x86-32
- Windows Server® 2003 Enterprise Edition x86-32
- Windows Server 2003 Standard Edition x86-32
- Windows Server 2008 Enterprise Edition x86-32
- Windows Server 2008 Standard Edition x86-32

For more information

To learn more about IBM Tivoli Security Policy Manager, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

About Tivoli software from IBM

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, help minimize risk and protect their brand; and automation to help 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

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

Produced in the United States of America
September 2008
All Rights Reserved

Disclaimer: 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.