

When millions need access: Identity management in an increasingly connected world

Best practice solutions that scale to meet today's huge numbers of users



Contents

- 2 Introduction
- 3 Effective management based on self service and access control
- 4 Security and compliance across the full user life cycle
- 5 Paths to success in the identity and access management environment
- 5 Use case 1: Portal-based access for large populations of users
- 6 Use case 2: User access to cloud-based services
- 7 Use case 3: Business partner access and application integration
- 8 IBM self-service solutions for internal and external users
- 11 The IBM portfolio of security management solutions
- 11 IBM: Your trusted partner for leading IT security solutions
- 12 For more information
- 12 About Tivoli software from IBM

Introduction

There is one thing that customers, business partners, vendors and all your other constituents want these days. They want in. They want access to your network or your cloud to make purchases, find information or use applications. And there are thousands—in many cases millions—of them.

Their interest and involvement can be good for business. But how do you manage such a number? Manual procedures for identity management—everything from granting access to assets to managing user accounts—are a classic example of processes that simply don't scale. They can work when the number of users is small. But manual procedures can become a significant burden when numbers reach into the thousands—and impossible when the numbers stretch to millions. Just think about resetting passwords. How could you maintain a help desk big enough for a world full of customers?

As organizations transform business by opening their systems to large numbers of internal and external online users, many of whom are mobile, they are increasingly adopting automated solutions that secure sensitive data, support end-user self service and help resolve problems. For today's instrumented, interconnected and intelligent IT operations, best practices for identity management can help ensure the secure, optimized and regulatory-compliant operations necessary to meet the access demands of a smarter planet.

Effective management based on self service and access control

Today's need for effective identity management is the result of an explosive growth in connectivity. An insurance company, for example, that until recently managed access for a few thousand employees now needs to manage millions of customers and partners conducting online transactions through a sales portal. A government agency previously managing access only for its employees now needs to manage access for millions of citizens and a wide range of other agencies accessing information online. Organizations in areas such as healthcare, finance and other customer services industries rely heavily on interaction and data exchange between large numbers of partners and consumers.

The result has been a sudden and unprecedented increase in the scale and requirements of online business operations—and an increased demand on organizations' identity management systems. Organizations now need systems that can give employees, business partners and external end users the self-service capabilities they need to quickly enroll for new services and resolve individual problems—including the ever-present issue of password resets—without having to contact the help desk. At the same time, organizations need systems that give administrators—whether IT operators, line-of-business managers or human resources professionals—control over permissions and other user access functions.

IBM offers industry-leading solutions based on the principles of the IBM Security Solutions “Secure by Design” initiative to meet scalable identity management needs. Developed to help build security into the IT infrastructure from the ground up, the Secure by Design initiative helps organizations incorporate security into the fabric of the services they deliver, making security intrinsic to business processes and daily operations. IBM Tivoli® identity management security offerings support the Secure by Design initiative with solutions for user administration and management, resource protection, and audit and compliance reporting.

IBM Tivoli Federated Identity Manager provides capabilities such as business-to-consumer self-service enrollment and federated single sign-on (SSO) support that organizations can supply to their external constituents. IBM Tivoli Identity Manager is an automated, policy-based solution that manages the life cycle of user access across IT environments within the organization. IBM Tivoli Security Policy Manager allows organizations to centralize fine-grained security policy management to enforce access control across applications, databases, portals and business services.

Security and compliance across the full user life cycle

An effective identity management solution meets a full range of online business needs—from pressures to stay competitive by providing greater access to more information and services, to requirements to demonstrate compliance by controlling and monitoring information access. The solution should include tools for restricting user access to only those resources appropriate to their role and/or job function, centralized user self service, simplified administration and approvals processing, periodic revalidation of user access rights, and documentation of policy controls. Add to all that the need to manage the rising costs of account provisioning and deprovisioning, recertification of access rights, help-desk calls, password resets and other administrative tasks.

As organizations grant access to different types of users including employees, customers, business partners and suppliers, they need best-practice solutions that can support the full life cycle of user identity, from the efficient onboarding of new users to their final off-boarding and the elimination of unidentified or “orphan” accounts.

Externally, they need a secure, easy-to-use solution that makes minimal demands on the organization’s IT staff to administer.

Internally, they need to create user accounts in ways that allow new hires or employees with new roles to be productive as soon as possible. To avoid potential security exposures, they need to retire accounts and associated access privileges quickly for employees who leave the company.

Cloud environments usually support a large and diverse community of users, so security controls are especially critical. Identity federation and capabilities for rapid onboarding must be available to coordinate authentication and authorization with the enterprise’s back-end or third-party systems. A standards-based, single sign-on capability is required to simplify end-user logins for both internally hosted applications and the cloud, allowing end users to easily and quickly leverage cloud services.

When it comes to compliance, organizations need enterprise-wide capabilities to ensure that both internal and external access are governed by effective authentication, to monitor authorization and network traffic, and to support the system with comprehensive audit and reporting capabilities.

Regardless of the type of user, the solution should enhance security by helping to fill gaps in security measures. It should mitigate the risk of issues such as fraud, theft of intellectual property or loss of customer data. It should help reduce costs by streamlining business and IT processes that grant users access to resources.

Paths to success in the identity and access management environment

Each organization has to determine the details of ensuring effective identity management, because each organization has its own needs, goals and set of users. Leading use cases for identity and access management, however, typically fall into three categories:

- Portal-based access to information for a large population of users
- User access to cloud-based services
- Business partner access and application integration

In each case, organizations are transforming the way they provide access. To achieve this transformation, they typically provide self-service functions as they help ensure secure operations and support regulatory compliance.

For portal-based scenarios—which are rapidly increasing in numbers and complexity as banking, retail and public sector organizations increase the value-added services in their online operations—the organization not only must address issues of security, scalability and usability, it must manage back-end tasks for application integration. Organizations deploying service-oriented architecture (SOA) solutions need an effective policy-based approach that incorporates security management and services that can be integrated with existing SOA components.

Use case 1: Portal-based access for large populations of users

A large state health information exchange portal needs to provide 3 million consumers and several hundred payers and associated providers with access to clinical and administrative data. It also must enable secure collaboration among healthcare organizations, facilities operators and insurance companies. It needs a solution that can centrally manage user authentication to ensure that patient records remain private as it securely expands

access to consumers, payers and providers. By ensuring identity management and enforced access control, the solution must support compliance with Health Insurance Portability and Accountability Act (HIPAA) security regulations and updated healthcare information exchange (HIE) requirements.

How Tivoli Identity Manager helps

Through the use of roles, accounts and access permissions, Tivoli Identity Manager helps automate the creation, modification and termination of user privileges throughout the entire user life cycle. For internal enterprise users and for business partners or trusted suppliers who need access to internal company resources, Tivoli Identity Manager enables the organization to grant permission to access information and applications and then to control access as the user's role and responsibilities change. Users are granted self-service capabilities in areas such as password reset, but the detailed workflow and processes for defining access rights based on role/job requirements and for avoiding access conflicts of interest make Tivoli Identity Manager a solution that is most appropriate for effective internal identity management.

How Tivoli Federated Identity Manager helps

For business-to-business and business-to-consumer scenarios, in which organizations extend access to large numbers of external users, Tivoli Federated Identity Manager provides self-service enrollment capabilities such as the selection of passwords along with secret questions and answers, as well as federated single sign-on and centralized authentication support to enforce access control. This automated user validation reduces the workload for IT administrators.

Tivoli Federated Identity Manager can expand collaboration with business partners who need limited access to internal resources by providing entry-level federation capabilities and by scaling to larger numbers of applications and users when necessary. The result: lower identity management costs, improved compliance and reporting, and simplified integration of services including centralized user access to software as a service.

Use case 2: User access to cloud-based services

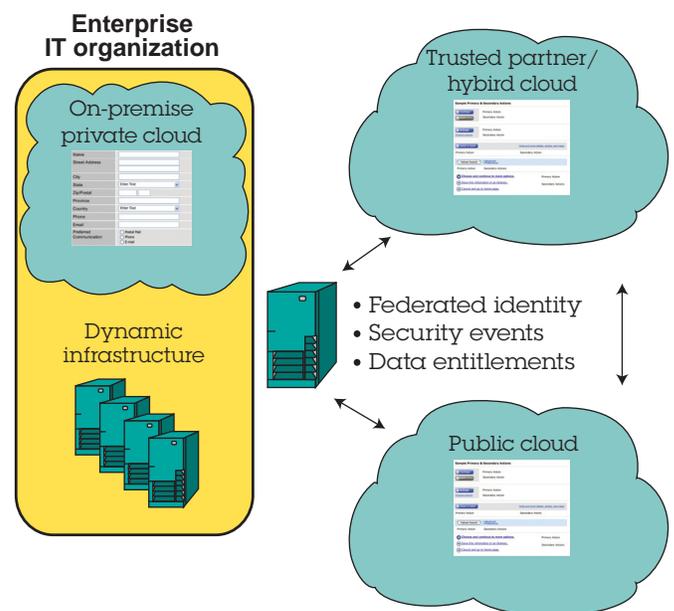
A global financial services company with 120,000 employees, 3 million external users and operations in 50 countries implements a cloud computing architecture to standardize their IT infrastructure and services. In the process, the company consolidates several data centers into a few next-generation data centers. The hybrid cloud solution that results provides the company with an automated, virtualized infrastructure on a single platform with different servers, self-service request-driven provisioning from a Web 2.0 service catalog, and secure access to services based on roles and business needs.

To achieve security management in its new cloud-based data centers, the organization implements IBM Tivoli Federated Identity Manager, securing collaboration with business partners and providing single sign-on for external users into the hybrid cloud environment.

Similarly, an organization with 2,000 software engineers spread across 25 teams implements a developer cloud environment to give teams access to services whenever and wherever they need it. Users log in to request capabilities—including operating systems, memory, disk space, middleware and more—and gain access in minutes.

To achieve secure and dynamic access for users and to eliminate lag times in delivering that access, the organization implements Tivoli Identity Manager. Password resets that used to take hours or days to complete now take only minutes—because users can log into a self-service portal and reset their passwords themselves. As new members join the team, they can gain rapid access to services, and as members depart, IT staff can remove their access rights to all systems with one command, rather than logging into dozens of different systems.

Securing access to cloud-based applications and services



With Tivoli Federated Identity Manager, the organization can centrally control access for large numbers of users to its cloud-based services hosted by external providers such as salesforce.com.

How Tivoli Identity Manager helps

Giving internal users access to a cloud-based application is essentially the same as providing access to other applications. Tivoli Identity Manager provides identity management capabilities that enable the organization to provide internal users, including privileged users, with self service and access rights to cloud-based services.

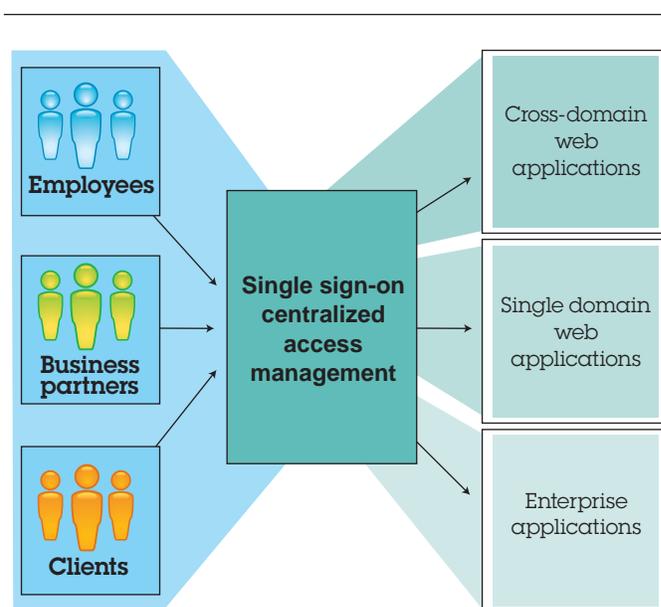
How Tivoli Federated Identity Manager helps

Using cloud-based computing to open applications and data over the Internet to a large group of users—everyone from employees in other parts of the organization to customers and business partners—requires particular attention to security. The larger the group, the more difficult it is to manage user identity. With Tivoli Federated Identity Manager, however, the organization can centrally manage and enforce access policies to on- and off-premise applications and services (including integrating with software-as-a-service and cloud-based solutions) and reduce IT administration costs while helping enterprises strengthen and automate user access rights.

In a typical scenario, authentication of the user takes place outside the cloud and involves IBM Tivoli Access Manager for e-business (for strong authentication). The user's identity is then federated into the cloud using Tivoli Federated Identity Manager (for user-facing sign-on). The entire process is transparent to the user. Tivoli Federated Identity Manager's single sign-on capabilities enable the user to go directly to cloud-based applications and information without having to manage identities within the cloud. The Tivoli Federated Identity Manager package includes Tivoli Access Manager for e-business to support this scenario. In addition, IBM offers Tivoli Federated Identity Manager Business Gateway, which provides standalone capabilities to support federated single sign-on and integration into cloud and software-as-a-service offerings.

Use case 3: Business partner access and application integration

An insurance company is migrating its legacy, host-based application to a new portal-based solution and needs to provide outsourced services providers, mobile agents and clients with



Single sign-on can simplify user access to multiple applications and sources of data.

information on their policies and contracts. The organization also requires fine-grained authorized access to insurance policies and contracts based on roles and additional attributes. Concern for compliance and data security issues lead the company to deploy Tivoli Federated Identity Manager and Tivoli Security Policy Manager to enable easy and secure single sign-on capabilities for both internal and external users, ensure an auditable record across the enterprise, and enforce data-level access control on a need-to-know basis.

How Tivoli Federated Identity Manager helps

Tivoli Federated Identity Manager simplifies application integration for identity management via an identity mediation service. Instead of requiring tiers of access for reaching the application, the solution validates, transforms and authenticates users one time to provide application access, whether it is to legacy mainframe, Java™ or Microsoft® .NET based applications. For enterprise users and business partners who require special access to secure information, this use of identity management provides a record as identities are mapped to access for audit and compliance use.

How Tivoli Security Policy Manager helps

Tivoli Security Policy Manager provides organizations the ability to manage and enforce fine-grained entitlement and data-level access control on a need-to-know basis. In the case of the insurance company, Tivoli Security Policy Manager allows mobile employees access to client contracts based on roles and on additional business attributes and context critical to ensuring privacy and data security.

IBM self-service solutions for internal and external users

IBM's identity management solutions—Tivoli Identity Manager and Tivoli Federated Identity Manager—provide self-service functions for streamlined management of internal or external access to business information and applications. The results can be dramatic—up to 80 percent reduction in provisioning time for new employee accounts, up to 40 percent reduction in identity management administrative costs, and up to 35 percent reduction in password-related calls to the help desk.¹

Tivoli Identity Manager provides complete identity life cycle management capabilities that support enrollment, permission and access control for the complete period in which a person is employed at a company—with management functions that also work for business partners, suppliers and other external constituents who may need trusted access to internal resources. The solution combines role management and user provisioning to deliver access rights to users. In addition, a hierarchical role structure streamlines administration and provides visibility into user access to infrastructure resources. Web self-service for managing roles, accounts and passwords further simplifies administration and reduces administrative costs by enabling users to perform tasks themselves. Self-service requests can be configured to define which attributes are allowed for self-service and which require approval. This is ideal for a high-volume, large-scale web environment where the exact identity of users is not known.

When users must access resources beyond their own organization, Tivoli Federated Identity Manager provides a highly scalable business-to-consumer self-service solution for enrollment along with authentication in which:

- External users initiate enrollment and select their password
- The organization customizes challenge/response, strong authentication and access to applications.
- The user deletes the account when it is no longer needed.

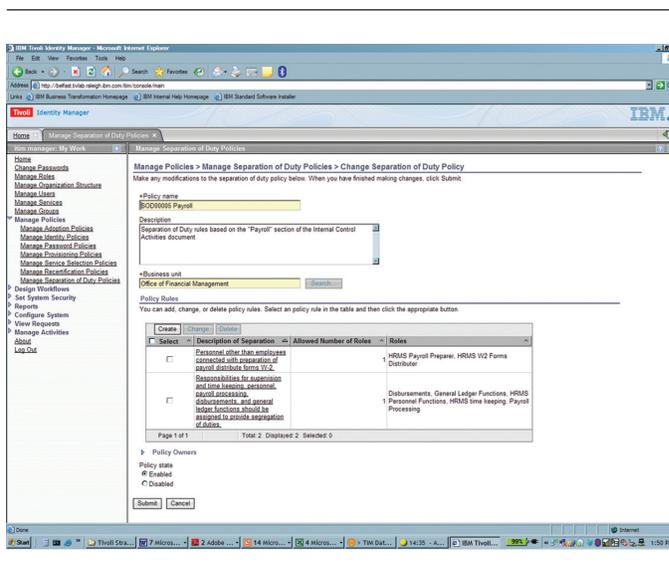
Tivoli Federated Identity Manager provides the federated single sign-on and user access management techniques that are necessary for integration across organizational boundaries.

The solution provides an identity trust management framework that enables an organization to know who is connecting to resources and what credentials they are using—without having to manage users individually. This is ideal for protecting assets where users are connected to critical resources from access points over the Internet or other less secure environments.

The two solutions can be deployed independently or together. When Tivoli Federated Identity Manager is deployed with Tivoli Identity Manager, the combination can provide access to an expanded set of applications and services. Organizations also can employ a phased implementation to gradually increase the number of users supported. This enables the organization to prove the solution's business value with a smaller initial set of users, and then expand the number of supported users over time.

Tivoli Identity Manager

This automated, centralized, policy-based solution utilizes roles, accounts and access permissions to manage user access throughout the entire user life cycle. Using user self-service, delegated administration, automated approvals processing, periodic revalidation of access rights, and documentation of controls, it can help increase user efficiency, reduce IT administration costs, enforce security and manage compliance. Tivoli Identity Manager is designed to reduce cost and risk by easing the on-boarding and off-boarding of users, and by reporting on user activity and ongoing access certification.



Tivoli Identity Manager is a centralized source for identity management throughout the user life cycle.

Tivoli Identity Manager helps organizations meet major challenges of identity management: meeting internal and regulatory compliance requirements, maintaining an effective security posture, and achieving a measurable return on investment.

Using Tivoli Identity Manager, the organization can:

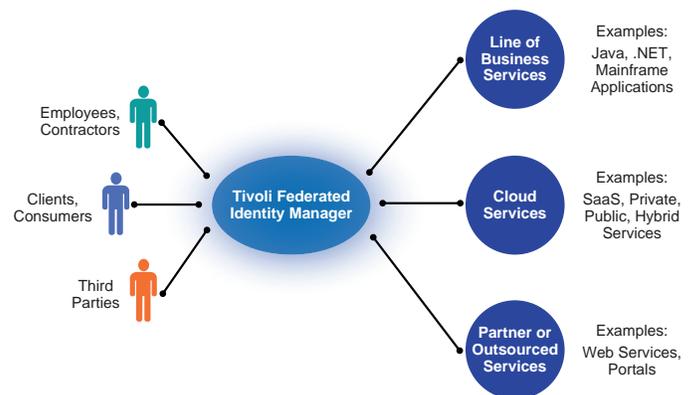
- Simplify and reduce the cost of administration with streamlined group management and bulk user recertification.
- Reduce setup time and training with simplified policy, workflow and configuration.
- Support enhanced security and reduce help-desk costs with centralized password management.
- Correct and/or remove non-compliant access rights automatically or through periodic access recertification workflows.
- Enhance security and compliance with separation of duties.
- Define processes for workflow and provisioning using predefined templates.

Separation-of-duties capabilities can strengthen security and compliance by creating, modifying or deleting policies that exclude users from membership in multiple roles that may present a business conflict. For example, a user in an accounts receivable role cannot also have an accounts payable role. This preventive approach can guard against violations occurring in the first place.

Tivoli Identity Manager supports role-based provisioning, which grants access rights according to corporate policies and individual duties, as well as request-based user provisioning, which automatically routes a user's requests for access to the appropriate manager for approval. The resulting flexibility helps organizations administer quick, secure user access. It enables the provisioning of new users in minutes rather than days so they can be productive as soon as possible.

Tivoli Federated Identity Manager

Tivoli Federated Identity Manager provides a central, standards-based web access management system to manage and enforce user authentication, single sign-on and self service for business-to-business, business-to-employee and business-to-consumer deployments across the enterprise. For scenarios in which the number of consumers connecting and interacting with a company often number in the millions, this user-centric solution relieves the complexity and expense of provisioning and managing user accounts.



Tivoli Federated Identity Manager provides users external to the organization with easy-to-use, self-service access to services.

Tivoli Federated Identity Manager helps organizations establish a framework for knowing which users are connected to services and what credentials are being used to connect without having to manage individual users.

Using Tivoli Federated Identity Manager, the organization can:

- Support user self-care for business-to-consumer and mobile user scenarios with initial password selection, password change/reset, and the ability to customize challenge/response for customer-specific needs.
- Manage user authentication and identification information about business partners through multiple open standards-based identity and security tokens.
- Reduce administrative costs, establish trust and facilitate compliance by managing, mapping and propagating user identities.
- Simplify integration between the organization's and its business partners' websites to reduce security exposure.
- Manage and enforce access to multiple services with a single sign-on to improve the user experience with Tivoli Access Manager for e-business.
- Provide federated single sign-on for cloud and software-as-a-service scenarios using Tivoli Federated Identity Manager Business Gateway.

Tivoli Federated Identity Manager provides automation for creating accounts, creating or modifying user profiles, and creating and changing passwords or secret questions. Policy-based integrated security management supports SOA services, and security administration is simplified for cross-company business processes.

The IBM portfolio of security management solutions

Tivoli Identity Manager and Tivoli Federated Identity Manager are included within IBM Tivoli Identity and Access Assurance, a broader solution that also enforces and monitors access in a closed-loop process that supports compliance.

Tivoli Identity and Access Assurance provides automated and policy-based management for user accounts, centralizes authorization for applications and provides federated single sign-on capabilities. It provides policy-based access control for business-critical applications, files and operating platforms. It automates monitoring, investigating and reporting on user activity.

IBM: Your trusted partner for leading IT security solutions

Tivoli Identity Manager and Tivoli Federated Identity Manager are part of the comprehensive IBM Security Framework, a portfolio of software, hardware and services that helps organizations address security challenges for users and identities, data and information, applications and processes, networks, servers and endpoints, and physical infrastructures. Facilitating the instrumented, interconnected and intelligent IT operations of a smarter planet, IBM Security Solutions deliver real-time visibility, centralized control and enhanced security for the entire IT infrastructure, helping clients address cost, complexity and compliance issues.

For more information

To learn more about Tivoli Identity Manager, Tivoli Federated Identity Manager and Tivoli Security Policy Manager, or IBM Security Solutions, contact your IBM sales representative or IBM Business Partner, or visit: ibm.com/security

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life cycle management, and is backed by world-class IBM services, support and research.

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 Results and savings based on IBM customer experience from installed systems.



© Copyright IBM Corporation 2011

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

Produced in the United States of America
January 2011
All Rights Reserved

IBM, the IBM logo, ibm.com and Tivoli 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

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. 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.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

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 noninfringement. 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