

Centrally Managing and Auditing Privileged User Identities by Using the IBM Integration Services for Privileged Identity Management



Redguides
for Business Leaders

Axel Buecker
Barry Evans
Dirk Rahnenfuehrer

- Understand privileged identities and why they can be a problem for an organization
- Learn about IBM Integration Services for Privileged Identity Management architecture
- Examine scenarios for improving security, compliance, costs, and meeting regulations



Executive overview

Every organization that deploys an IT infrastructure has a requirement for *privileged users*. These privileged users, including *system accounts, administrators, managers, and business executives*, are typically granted administrative or special rights to manage business-critical resources, such as operating systems, databases, ERP systems, and many other applications, systems, and platforms. The privileged IDs are usually shared among a pool of users, can cause accountability and compliance issues, and can increase the risk for sabotage and data theft. The trends towards data center consolidation, cloud computing, and virtualization can create an even greater number of privileged IDs in today's IT infrastructures. Increased outsourcing trends, where resources are used all over the world with historically high turn-over rates of employees, create an even greater need to centrally manage and secure privileged IDs.

High-profile corporate accounting scandals and wide-spread financial turmoil have created an environment of ever tightening government regulations around the world. These regulations articulate technical accountability issues that organizations must comply with or face financial and criminal penalties. Industry standards have also become more specific in regards to data security and the privileged accounts that can access the data. Maintaining compliance with these standards and asserting compliance with government regulations demand appropriate controls and handling of privileged accounts.

The IBM® Integration Services for Privileged Identity Management (also known as IBM Privileged Identity Management solution) includes products and services that can help enable an organization to centrally manage and audit a pool of privileged user IDs, which can be checked in and checked out by authorized people when needed. An integration with IBM identity management and enterprise single sign-on (ESSO) solutions provides a seamless user experience without having to manually enter a password, which can help keep the organization's privileged user IDs more secure. An IBM centralized-compliance auditing and reporting solution can assure that the organization acts according to policy and regulations.

In this IBM Redguide™ publication, we provide information to business leaders, IT architects, and consultants to help in understanding the challenging topic of managing privileged identities in an organization. We discuss the general solution and describe two typical customer deployment architectures.

Privileged IDs and why they are a problem

The term *privileged IDs* refers to the pre-built accounts in nearly every operating system and application. These accounts are distinguished from general user IDs by assignment of security, administrative, or system authorities. They are ubiquitous, we know them by their names, *root*, *Administrator*, *sa*, *sec_master*, *db2admin*, *itim manager*, *wasadmin*, and others. They can be accessed only by specifying a privileged password and are nearly impossible to disable, unlike a personal identity such as *jdoe*. They are extremely powerful, allowing a user to log on, and have complete control of the target system and full access to all of the information about that system. In addition, shared or pooled accounts might cause risks, and audit and compliance issues.

Beyond the obvious risks of a privileged ID being compromised by a hacker, authorized users with privileged accounts within an organization represent a clear and present danger to the data security of an IT infrastructure. In a 2007 E-Crime Watch survey, half of the respondents experienced at least one malicious insider incident. The survey indicated that losses were close to half a million U.S. dollars to each company affected in 2006.¹ IT sabotage and theft for a business advantage are generally committed by technical and privileged users. The United States Computer Emergency Readiness Team (CERT) best practice guidelines recommend to “*Use extra caution with system administrators and technical or privileged users.*”²

The *standard* model of IT administration has long been a process where individual administrators gets their own accounts with access to, or equivalent permissions of, a privileged account. This standard model of IT administration is no longer sufficient for organizations where consolidation, virtualization, and server density continues to increase dramatically. The average organization has to manage tens of thousands of privileged passwords. The risks and costs that are associated with all these accounts continue to rise and productivity suffers as organizations try to manage the ever increasing load of maintaining this model.

Note: Typically, password policies for privileged IDs are very strict. The policies require those passwords to be changed at very short intervals, and sometimes use password strength policies that require people to write down the passwords. Those guidelines can make password management even more costly and risky.

Let us examine why organizations today are facing the proliferation of privileged IDs as IT systems have evolved.

¹ Source: E-Crime Watch survey, US Secret Service/CERT/Microsoft®, September 2007
<http://www.cert.org/archive/pdf/ecrimesummary07.pdf>

² Source: Common sense guide to detection and prevention of insider threats 3rd edition - v3.1, CERT, Jan 2009
<http://www.cert.org/archive/pdf/CSG-V3.pdf>

The growth of risk can be seen in the following stages:

- ▶ In a first stage, a small team manages a local group of servers (Figure 1).

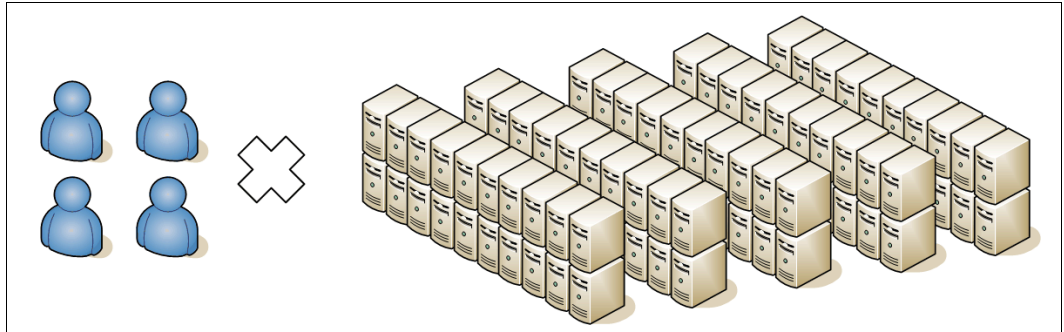


Figure 1 First stage: 4 administrators x 100 servers = 400 administrative accounts

- ▶ In the next stage, data centers emerge (Figure 2).

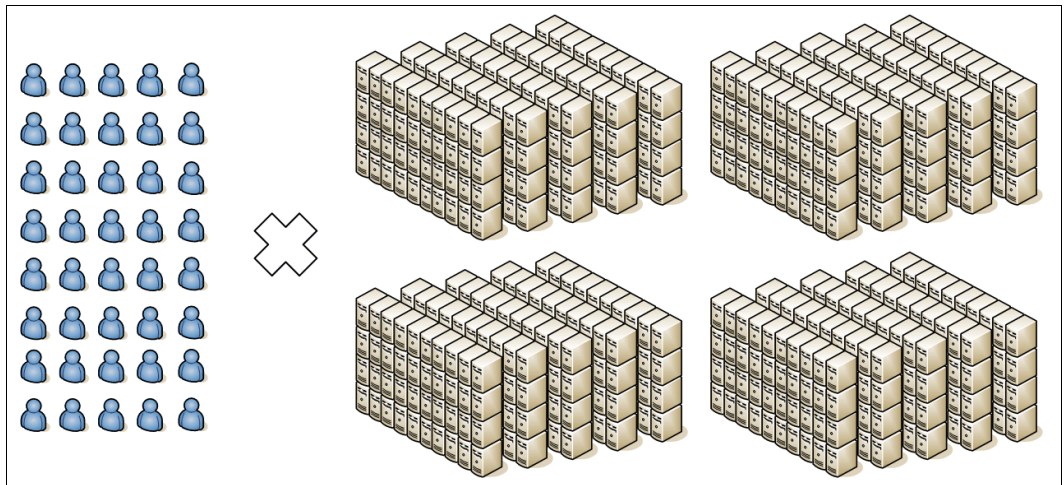


Figure 2 Next stage: 40 administrators x 1000 servers = 40,000 administrative accounts

- ▶ In the final stage, we see the emergence of global delivery centers, blade servers, virtualization, and cloud computing solutions (Figure 3).

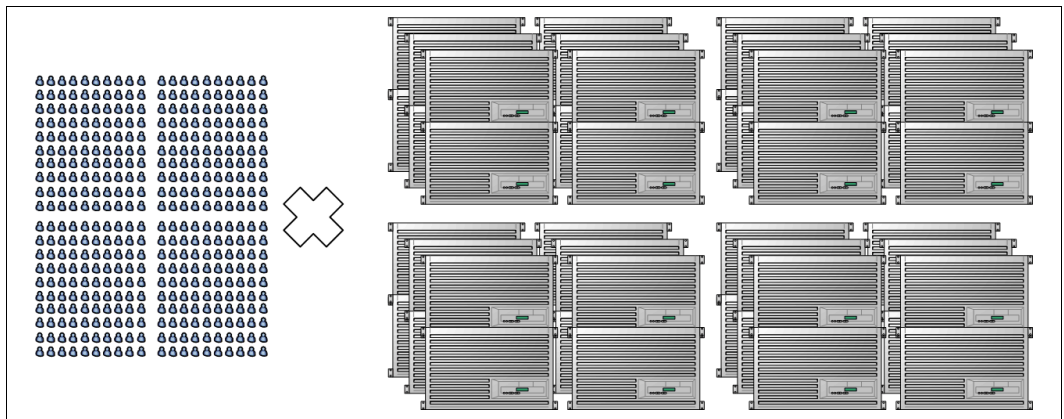


Figure 3 Final stage: 400 administrators x 10,000 servers = 4,000,000 administrative accounts

Ignoring all other aspects, risk has grown 10,000 times, from the small team practice in Figure 1 on page 3 to the large enterprise and cloud computing example in Figure 3 on page 3. The risks can encompass everything from simple mismanagement of privileged IDs, social engineering, brute-force attacks, to compromised passwords. See Figure 4.

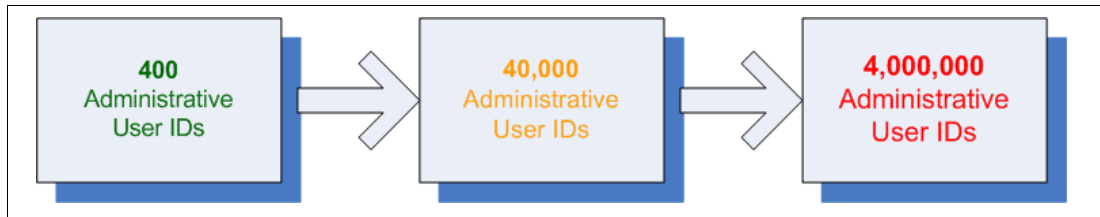


Figure 4 10,000x risk

Beyond risk, all things are not equal in practice. In addition to having 10,000 times the risk exposure, also consider the increased overhead behind user ID management costs. The administrative costs of provisioning, deprovisioning, recertifying continued business need for access, and reconciling accounts all grow exponentially. Turnover and attrition rates further exacerbate the problem for organizations.

Simply sharing a single privileged ID password does not address the problems either. You immediately lose accountability of the individual. Password management across the team and password security quickly become an issue. This practice is out-of-step with current regulatory requirements, too.

Government regulation and industry standards are tightening on the risks that are associated with simple models of IT administration. In the United States, the Sarbanes-Oxley Act of 2002, Section 404, requires (at a minimum) that companies prove exactly who logs in to sensitive systems. Sharing privileged passwords, even among small departments or teams, fails to meet this requirement because individual accountability is lost. Other regulatory and industry standards, which require that an inventory of privileged IDs or levels of access be kept, are also difficult to maintain in this model. Table 1 on page 5 lists several of these relevant regulations.

Table 1 Regulatory compliance initiatives

Compliance initiative	Relevant directive	Relation to privileged account control
Payment Card Industry Data Security Standard (PCI DSS) ^a	Requirements: <ul style="list-style-type: none"> ▶ (#3) Protect stored cardholder data. ▶ (#6) Develop and maintain secure systems and applications. ▶ (#7) Restrict access to cardholder data by business need-to-know. 	Insufficient internal controls of privileged accounts can negatively affect an organization's capability to meet all three of these requirements.
European Union Data Protection Act ^b	Appropriate technical measures must be taken against unlawful processing of personal data and against accidental loss, including controlling access to information.	Insufficient internal controls of privileged accounts can negatively affect an organization's capability to meet these requirements
Sarbanes-Oxley Act of 2002 (SOX) ^c	Section 404: <ul style="list-style-type: none"> ▶ Requires corporate management to take responsibility for establishing and maintaining adequate internal control structures and procedures for financial reporting. ▶ Requires management to assess and report the effectiveness of the internal control structure and procedures for financial reporting. 	Insufficient internal controls of privileged accounts can negatively affect an organization's capability to meet these requirements.
State of California Civil Code Section 1798.82 ^d	Subdivisions (a) and (b): <ul style="list-style-type: none"> ▶ Requires an organization that loses private information of California residents report the loss to affected individuals. 	Unauthorized users of privileged accounts can bypass the access control mechanisms and audit controls of most systems to access private information without the organization knowing about it.

a. PCI DSS at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

b. European Commission - Data Protection at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

c. U.S. Securities Exchange Commission at: <http://www.sec.gov/about/laws.shtml#sox2002>

d. California Civil Code 1798.82 at: http://www.dmv.ca.gov/pubs/vctop/appndxa/civil/civ1798_82.htm

By considering the kinds of problems we describe here, organizations are trying to reduce the proliferation of user IDs to achieve cost, risk, and productivity objectives.

Alternatives that an organization has

Businesses and government agencies have begun to recognize privileged identity management as an issue for several reasons. Economic motivations exist to consolidate data center locations and reduce related staffing requirements. Virtualization and blade computing technologies emerged and have dramatically increased server density while at the same time, increasing the total number of systems in use. Finally, traditional *identity and access management* (IAM) solutions made great gains in managing accounts of individuals but failed to easily or efficiently address accounts that could not be simply owned by, or assigned to, one person or identity.

As a result, today most organizations still operate in one of two obsolete models:

- ▶ Everyone has a user ID on every system, all the time.

When an organization operates with the traditional model of every single administrator having privileged access to many or to all systems, management becomes troublesome and expensive. As shown in Figure 3 on page 3, an organization with 400 IT staff managing 10,000 servers easily results in managing 4,000,000 or more privileged administrative IDs.

- ▶ Everyone shares access to a single user ID for ease of administration.

Other organizations recognize this account management overhead and try to avoid it by simply *sharing* privileged passwords among the teams that require them. Problems quickly arise from this approach because a team will need to immediately change the password when an employee leaves or changes jobs. Methods of securely storing and communicating that password are often very weak in security. This approach typically leaves organizations with their most sensitive privileged accounts as their most poorly secured credentials. Furthermore, personal accountability is completely lost because anyone on a given team might have used a shared *root* credential for a malicious act. This method puts any organization in a very precarious situation, with sensitive credentials being both poorly secured and lacking an ability to trace actions to a single person. This method is also not compliant with regulations.

As described previously, a *privileged ID* is a pre-built account in nearly every operating system and application that has special administrative or security authorities. In comparison, a *shared ID* can be used by more than one individual. Within this document we make no distinction between shared and privileged IDs. Typically a shared ID is also a privileged ID. Otherwise, there would not be a need to share that ID among users or administrators, because the administrators would have their own personalized ID. For example, applications allowing role-based access levels (for example, user, help desk, administration) do not require sharing of any one system ID.

Other organizations with existing identity and access management tools in place try to avoid shared ID management problems by assigning all privileged system accounts to a pseudo-person identity. For example, an organization might create a pseudo-person identity such as *RacfMasterPerson* and assign 3,000 system IDs to this one person/identity record. Depending on the existing identity and access management solution, this approach may allow the organization to maintain a level of individual accountability, but gaps become apparent. Methods of delegating accounts and privileges, or temporarily reassigning accounts are cumbersome. Role-based access and policy definitions become convoluted within the context of pseudo-person identities being used. Software limitations might also be encountered, as an uncommonly high number of accounts, roles, or accesses are assigned to an individual pseudo-person identity.

Successfully integrating privileged identities into an identity and access management solution requires a new concept.

The concept is that a user gets an individual user ID on a system, but only in the following situations:

- ▶ If they need it
- ▶ When they need it
- ▶ For only as long as they need it

Within this new concept of privileged identity management, we also introduce the term *reusable user ID*. A reusable user ID allows a user to log on to a system without knowing or seeing the password.

Important: The password for a reusable user ID must not be known or seen by the user. By creating the technical controls to achieve this concept, a single user ID may be used consecutively by a number of users without requiring a password change in-between each use of the ID. This concept is a necessity where a system, end-point, or application has a policy in place that limits the number of password changes allowed in a given time-frame.

By approaching identity management from this concept of privileged account leasing, sharing, or checking in and checking out, we can achieve individual accountability for the actions taken with privileged accounts. Technical controls monitor and audit each step of the process, allowing someone to be accountable for what they did and when they did it. This concept closes the gaps in traditional IT approaches discussed earlier and is consistent with current regulatory requirements.

The IBM Privileged Identity Management solution

The IBM Privileged Identity Management solution addresses the end-to-end lifecycle management of accounts, single sign-on (SSO), and handling of privileged IDs across both systems and applications.

Overview

The IBM Privileged Identity Management solution was developed as an extension to the existing IBM Tivoli® Identity Manager and IBM Tivoli Access Manager for Enterprise Single Sign-On products. It implements the necessary technical controls to provide the account-sharing concept described previously. This approach enables an organization to effectively control access, manage all accounts, simplify privileged access, and maintain an audit posture that is consistent with regulatory requirements.

An organization defines privileged roles, such as *SystemAdmin_Staff* or *Operations_Database_Admin*, which are tied to appropriate system and account entitlements. The roles can also be tied to pools of accounts (for example, a pool of 15 database administrator accounts) when more than one user is expected to use a given privilege at the same time. When those roles are assigned to an employee, the IBM Privileged Identity Management solution automatically provisions any personal accounts that the user is entitled to, and also allows that employee the option of checking-out any entitled privileged IDs for a specified lease period. The solution uses the Tivoli Identity Manager Self-Service User Interface, allowing an employee to request a new access entitlement. That request is processed in a workflow where approval logic can be implemented if necessary.

The Tivoli Access Manager for Enterprise Single Sign-On client is leveraged to simplify privileged account access and provide automation for the user. When a user accesses a system where a privileged ID is required, the Tivoli Access Manager for Enterprise Single Sign-On client automatically checks-out the required account and inserts the credentials into the users session. This automation works for desktop applications, Web applications, and mainframe applications. After finishing the tasks that required using the privileged account, the user can rely on an automatic check-in process to return the privileged user ID to the stack. This simplified usage does not add any new manual tasks for the privileged users, and it provides increased security because the password for a privileged user ID is never revealed to anyone.

The Tivoli Identity Manager Self-Service User Interface also allows users to manually check-out a user ID by providing them the user ID and password. This feature is useful for

offline maintenance tasks and other scenarios where a user might not be able to use the SSO client. An automated password change is part of this manual check-in process to ensure that individual accountability is still maintained. The workflow features in Tivoli Identity Manager can also automate periodic user recertification if needed.

All steps of an employee's check-out process, use, and subsequent check-in are audited. This audit data remains available to fulfill reporting and compliance purposes for the organization.

The IBM Privileged Identity Management solution is implemented as a complete management process as shown in Figure 5.

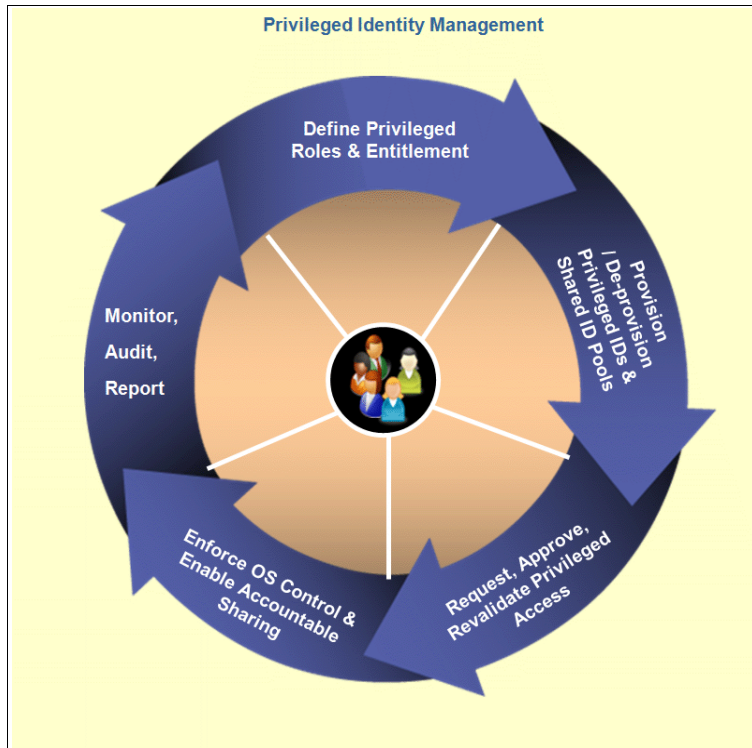


Figure 5 Privileged identity management process

When a new employee joins the organization that employee is added only to the roles within the IBM Privileged Identity Management solution related to the employee's job. Setting up another individual privileged user ID for this person is unnecessary. This model helps to reduce the number of individual administrator user IDs and the number of provisioning activities per hiring, and conversely deprovisioning automatically when an employee leaves. This reduction in primary control activities can also alleviate other time consuming secondary control activities an organization takes with employee hirings and terminations.

Privileged access automation features of the solution that are provided by Tivoli Access Manager for Enterprise Single Sign-On can keep the process simple for users. Let us look at a typical workstation-related workflow:

1. The user works from a notebook or workstation, as the user would in any of the traditional IT models.
2. The user starts the required application or log-on interface for Web or mainframe applications.

3. Tivoli Access Manager for Enterprise Single Sign-On interjects by prompting the user to select a role, determining the privileged ID needed.
4. Tivoli Access Manager for Enterprise Single Sign-On transparently handles checking-out the required account and then automatically inserts the credentials to authenticate the user to the application/host.

IBM uses the best-in-class identity provisioning and enterprise single sign-on tools to create a solution that can manage the entire privileged identity lifecycle. The IBM Privileged Identity Management solution centralizes privileged ID management to improve IT control and reduce risk. It automates the single sign-on and check-in and check-out processes to help simplify usage and reduce costs. The IBM Privileged Identity Management solution also provides comprehensive tracking and reporting to enhance accountability and compliance by capturing both *how* a privileged ID was used and *what* a user did with that privileged ID.

Architecture

The following IBM Privileged Identity Management solution core components are depicted in Figure 6. Communication interconnectivity is denoted by the lines between each component. The figure uses the following acronyms:

- ▶ IBM Tivoli Identity Manager (TIM)
- ▶ IBM Tivoli Directory Integrator (TDI) based adapter for Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO)
- ▶ IBM Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO)

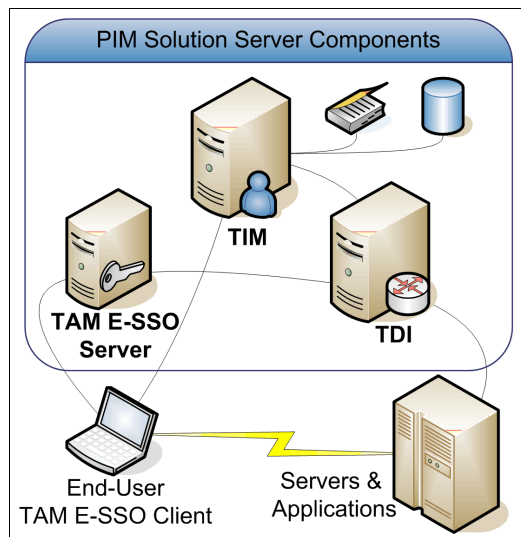


Figure 6 IBM Privileged Identity Management solution components

Although the Tivoli Directory Integrator product is shown in Figure 6, it is used only for the Tivoli Identity Manager adapter. For details about these components, use the references that are listed in “Other resources for more information” on page 26.

To better explain the integration of these IBM products into the IBM Privileged Identity Management solution offering, we focus on the following items:

- ▶ User flow architecture
- ▶ Tivoli Identity Manager integration
- ▶ Tivoli Access Manager for Enterprise Single Sign-On integration
- ▶ High-level process flow

IBM Tivoli Security Information and Event Manager: This optional component can further enhance the compliance capabilities of the IBM Privileged Identity Management solution. Beyond the auditing data that is captured by Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On, Tivoli Security Information and Event Manager provides forensic capabilities to investigate user behavior and also provides the tools to prove log file continuity. It can track malicious user behavior to help understand and alert staff to insider threats using near real-time analytics.

Tivoli Security Information and Event Manager provides a centralized dashboard and advanced reporting capabilities. Compliance reporting is made simple with predefined audit reports in Tivoli Security Information and Event Manager's regulation-specific Compliance Management Modules. Monitoring capabilities are included to track privileged user activities. Tivoli Security Information and Event Manager includes native log collection features to capture logs from all servers and end-points in an organization. Log aggregation and event translation using a patented methodology help to further simplify events into understandable information for security personnel, auditors, and management.

For more information about this product, go to the following Web address:

<http://www.ibm.com/software/tivoli/products/security-info-event-mgr/>

User flow architecture

The user flow architecture, shown in Figure 7, depicts the available functions to the IBM Privileged Identity Management solution's user.

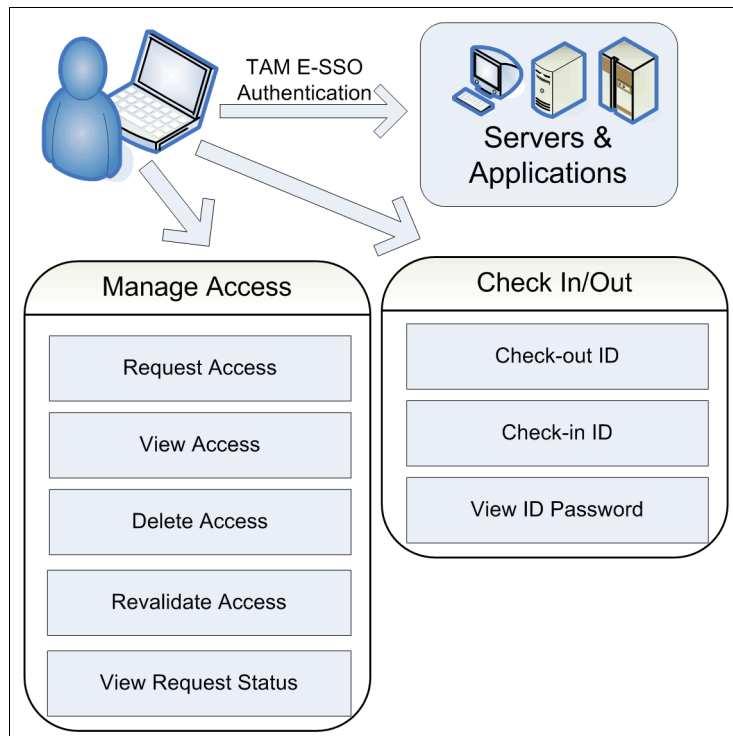


Figure 7 User flow architecture

IBM Privileged Identity Management solution users that have *elevated authorities*, such as Tivoli Identity Manager administrators, system owners, HR representatives or managers, may perform the functions that are shown in Figure 8.

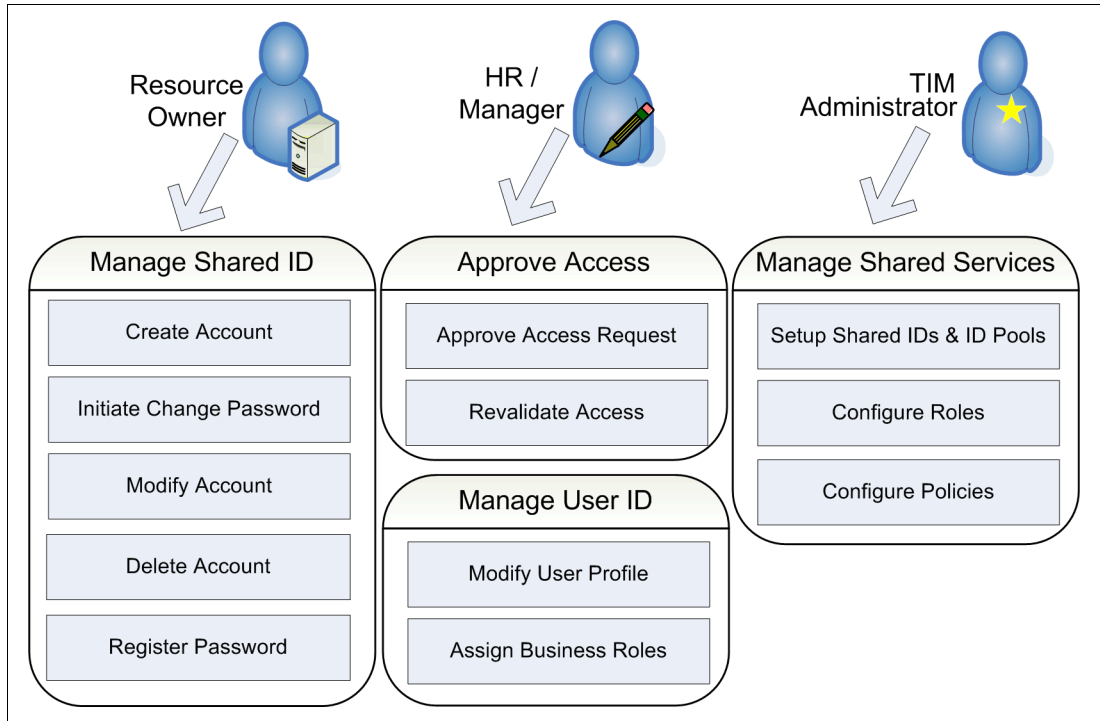


Figure 8 Administrative-user flow architecture

Managing privileged user IDs with your regular user provisioning system brings many advantages; it provides a full lifecycle management solution that is consistent with how user IDs are already being managed, unlike other password vault solutions.

Tivoli Identity Manager integration

The IBM Privileged Identity Management solution builds upon the Tivoli Identity Manager product. The IBM Privileged Identity Management solution adds new functions and integrates other basic features of Tivoli Identity Manager into the IBM Privileged Identity Management solution. The following features are integrated or added to Tivoli Identity Manager:

- ▶ *Vault* securely stores credentials of privileged accounts within Tivoli Identity Manager.
- ▶ *Shared Identity Service* allows users to request access to a privileged account.
- ▶ *Extended Self-Service User Interface* is for users to optionally check-out credentials, view passwords, and check in credentials. See Figure 9 on page 12.

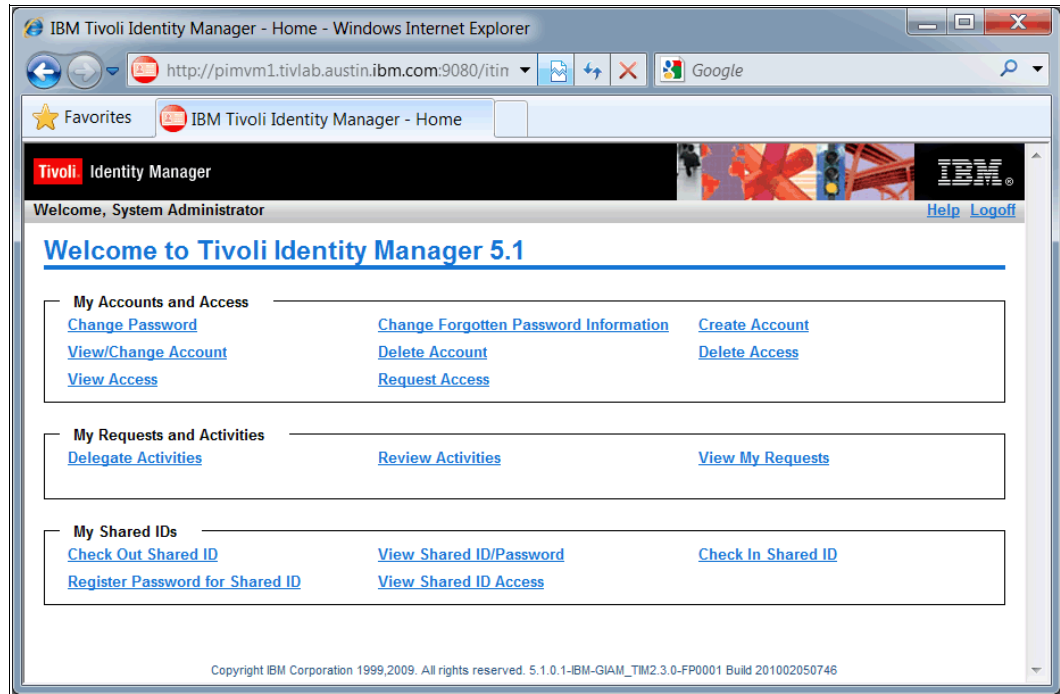


Figure 9 Privileged Identity Management Self-Service User Interface

- ▶ *Timed auto-check-in* of an account is useful if a user fails to check in the account before expiration (lease times are configurable).
- ▶ *Password reset* can be configured to be executed at each check-in.
- ▶ Optionally, the IBM Privileged Identity Management solution can be configured to prevent *manual check-out* and viewing of the password by users. This feature reduces the number of password resets, which can be an issue if end-points have policy restrictions. In this case, only Tivoli Access Manager for Enterprise Single Sign-On is authorized to check out the privileged user IDs, on demand, on behalf of the user.

These features and extensions provide the necessary technical controls within Tivoli Identity Manager to manage privileged accounts in a check-in/check-out (CICO) concept.

Other basic services are provided by the Tivoli Identity Manager component of the IBM Privileged Identity Management solution. Tivoli Identity Manager allows *role based access control* for all accounts and also allows *lifecycle management* for ID access based on roles including requests, approvals, and recertification. Existing Tivoli Identity Manager workflows can be attached to privileged accounts before users are assigned or recertified. Tivoli Identity Manager Self-Service and Administrator User Interfaces use IBM Privileged Identity Management solution services as with other services. Therefore, basic capabilities such as ACIs, password policies, role hierarchy, separation of duties (SoD)³ policies, and provisioning policies can be used as with any other Tivoli Identity Manager service.

The user interface can be customized through Access Control Information (ACI) changes and using Tivoli Identity Manager's Form Designer to provide access to important attributes (for example, administration attributes like `iamIsShared` set to *true* or *false*). As with standard Tivoli Identity Manager features, the Self-Service User Interface can also be customized to reflect your organization's Web look and feel.

³ SoD Policy and Role Hierarchy are unique to Tivoli Identity Manager 5.1 and are not available in earlier versions.

Tivoli Access Manager for Enterprise Single Sign-On integration

The IBM Privileged Identity Management solution integrates Tivoli Access Manager for Enterprise Single Sign-On with Tivoli Identity Manager to provide single sign-on functionality for users. Tivoli Access Manager for Enterprise Single Sign-On can automate application, Web, and mainframe credential storage and authentication for personal accounts. Extensions within Tivoli Access Manager for Enterprise Single Sign-On and the IBM Privileged Identity Management solution provide the necessary integration to check out and check in accounts from and to Tivoli Identity Manager as needed. The check-out is an exclusive check-out of the individual privileged account for the duration of its use by that user. When an application is closed, Tivoli Access Manager for Enterprise Single Sign-On executes a check-in of the credentials back into Tivoli Identity Manager. Audit logging is also part of Tivoli Access Manager for Enterprise Single Sign-On with all steps of authentication and privileged account actions being recorded (additional auditing is captured in Tivoli Identity Manager).

The Tivoli Access Manager for Enterprise Single Sign-On audit trail and reporting (additional auditing is captured in Tivoli Identity Manager) includes the following details:

- ▶ *Who* (username) checked out or checked in the privileged ID?
- ▶ *What* role and privileged ID was requested and used and what did the user do (audit trail) with the privileged ID?
- ▶ *When* (time stamp) was the privileged ID checked out and checked in?
- ▶ *What* (application or system) was the privileged ID used on?
- ▶ *Where* (IP address) was the check-out requested from?

Important product features

The Tivoli Access Manager for Enterprise Single Sign-On integration is built on the following product features that are important to understand. The IBM Privileged Identity Management solution uses these features as part of the overall solution. The Tivoli Access Manager for Enterprise Single Sign-On features are as follows:

- ▶ Provides automated check-out and check-in of a privileged ID within the security context of a Tivoli Access Manager for Enterprise Single Sign-On *AccessProfile*.

Terminology: *AccessProfiles* are short, structured XML files that enable single sign-on/sign-off automation for applications. AccessStudio can be used to generate *AccessProfiles*. *AccessProfiles* are based on a *state engine*, which includes *states*, *triggers*, and *actions*.

AccessStudio is the interface that is used to create the *AccessProfiles* that are required to support end-point automation, including single sign-on, single sign-off, and customizable audit tracking.

A *Trigger* represents an event that causes transitions between two states in a state engine.

An *Application* in AccessStudio refers to the system that provides the user interface for reading or entering the authentication credentials.

- ▶ Integrates strong user authentication at the client or workstation through a user ID and password, and through a wide choice of authentication factors and devices such as smart card, RFID, active RFID, and biometrics (for example, fingerprint, iris scan, and so on). The second-factor authentication can be defined granularly by group policies based on host names, IP ranges, and Active Directory groups.

- ▶ Provides application integration capabilities through AccessProfiles can be used for enabling applications to use privileged IDs.
- ▶ Incorporates enterprise single sign-on functionalities with privileged ID automation, workflow automation, and custom audit tracking inside an application by using standard AccessProfile trigger and action capabilities.
- ▶ Provides audit trail and reporting mechanisms for tracking privileged ID activity. This data can be utilized for reporting purposes or it can send alerts to perform further investigation or take preventive actions based on the individual activities of a privileged ID in a given system or application.

Automation around privileged accounts

Tivoli Access Manager for Enterprise Single Sign-On checks out a privileged ID when required by a user. Standard AccessProfile-based triggers identify the screens of interest to manage an automated logon with privileged IDs. Tivoli Access Manager for Enterprise Single Sign-On checks in the credentials when an application is closed. Depending on the individual application architecture, a check-in can occur in various ways and is based on various application-specific triggers. Check-in occurs when the user performs the following tasks:

- ▶ Disconnects from an application *without* shutting down the application by navigating through menus such as **File** → **Exit**.
- ▶ Logs off from an application and shuts down the application by navigating through menus such as **File** → **Exit**.
- ▶ Disconnects from a remote application.
- ▶ Logs off from a remote application.

The AccessProfile for an application also performs any role lookup, check-out and check-in actions through a Web services interface between Tivoli Access Manager for Enterprise Single Sign-On and the IBM Privileged Identity Management solution. These actions are only executed when an AccessProfile trigger match is found and the AccessProfile workflow calls these actions.

High-level process flow

Tivoli Access Manager for Enterprise Single Sign-On is based on AccessProfiles that are defined for a particular executable, mainframe application, or Web application. Figure 10 shows the general flow within the context of an IBM Privileged Identity Management solution.

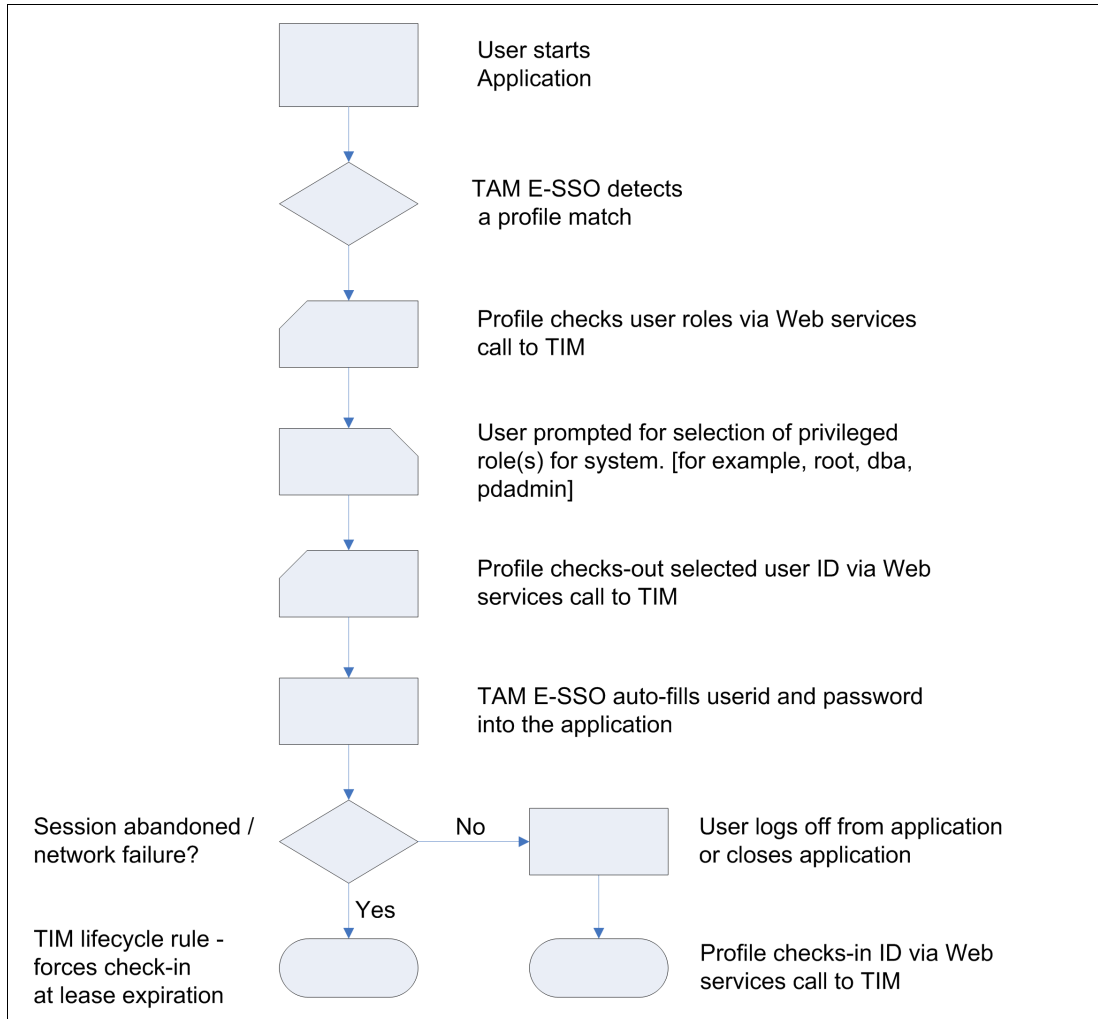


Figure 10 Authentication automation flow

To demonstrate the logic seen in the flow diagram in Figure 10, the example in Figure 11 on page 16 shows the use of Tivoli Access Manager for Enterprise Single Sign-On from a user's perspective when logging on to a managed system as *root*.

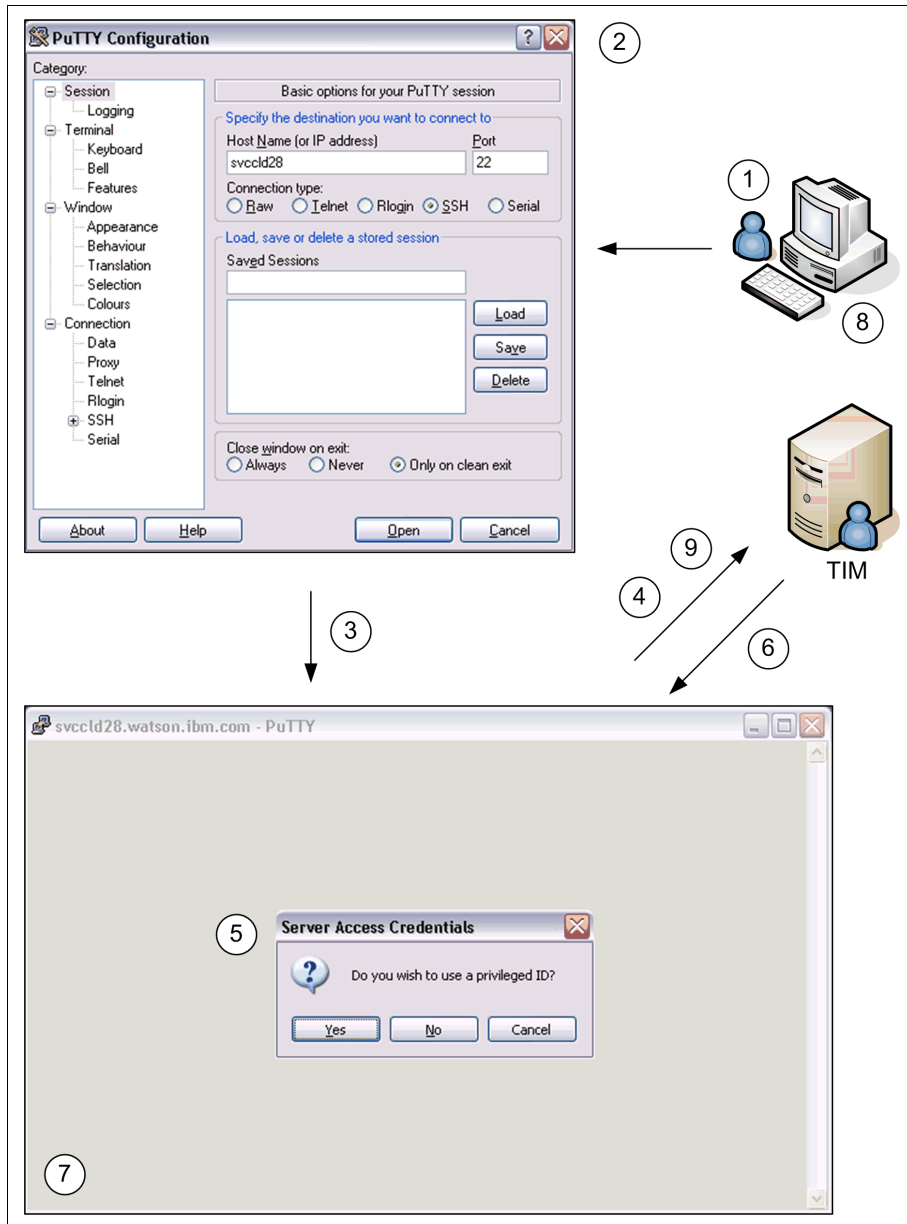


Figure 11 User flow of performing login with a privileged ID

Figure 11 demonstrates the following steps:

1. The user launches PuTTY on the workstation. PuTTY is a common Secure Shell (SSH) terminal application.
2. Tivoli Access Manager for Enterprise Single Sign-On detects matching AccessProfile for PuTTY application.
3. The user initiates an SSH session to a selected host.
4. PuTTY AccessProfile checks user roles through a Web services call to Tivoli Identity Manager.
5. The user is prompted for selection of a privileged role (for example, *root*, or *dba*).
6. PuTTY AccessProfile checks out selected user ID *root* through a Web services call to Tivoli Identity Manager.

7. Tivoli Access Manager for Enterprise Single Sign-On fills in the *root* ID and password into the PuTTY application window.
8. The user logs out of the server SSH session and closes the application.
9. Tivoli Access Manager for Enterprise Single Sign-On checks in the user ID *root* through a Web services call to Tivoli Identity Manager.

Tivoli Access Manager for Enterprise Single Sign-On provides the technical controls necessary to both simplify the user experience and make the concept of *reusable credentials* possible, because the user does not see the password. This capability applies to any application that an administrator uses and is not limited to SSH, as shown in this example.

Customer deployment scenarios

This section outlines two identity lifecycle management scenarios and how the IBM Privileged Identity Management solution can be used to reduce costs, improve security, and help ensure compliance with common industry and government regulations.

Retail chain that expedites lifecycle management tasks and reduces risks

This retail scenario provides an example of using the IBM Privileged Identity Management solution to rapidly provision, recertify, and deprovision employees, and to reduce costs and risks that are associated with shared administrative accounts.

Scenario description

In this scenario, a retail firm has 1,200 store locations throughout the United States. At each store the chain has deployed two AIX® servers and two to six Windows®-based point-of-sale (POS) systems. The corporate headquarters in Florida has an IT staff of 600 people spanning all disciplines of network, systems, and applications administration, software development, reporting, and help desk roles. Today, each IT staff member has an account on each of the 2,400 or more servers, creating approximately 1,400,000 administrative accounts in the organization. Each retail associate in the organization is provisioned an e-mail account and a local store account.

The retail firm has expanded through the years and used their own developed and maintained Perl scripts to create IT staff accounts. Store employee accounts were created manually by the IT staff; work requests were sent to the e-mail administration team and systems team. Throughout the retailer's growth, IT costs rose sharply. A third-party IT audit, which was ordered by the Chief Information Officer (CIO), found a large number of employee accounts that were still active for employees who had been terminated several months earlier. The audit also identified incidents in which store employees extended fraudulent discounts to customers by using POS stations where a store manager had forgotten to logout.

The IT Director was assigned to perform the following tasks:

- ▶ Resolve the audit failures and ensure they do not reoccur.
- ▶ Expedite the onboarding process of hiring seasonal employees.
- ▶ Secure and simplify in-store authentication to the POS systems.
- ▶ Contain the escalating budget for help desk and systems team staffing.
- ▶ Assert compliance with the PCI DSS standard.

Solution

To fulfill these tasks, an IBM Privileged Identity Management solution provides complete automated end-to-end identity lifecycle management, with auditing and controls that are appropriate to comply with PCI DSS regulations.

Policies within the IBM Privileged Identity Management solution define what accounts and levels of access are appropriate for each employee's role. Store associates have policies that entitle them to an e-mail account and system account for only their store. IT staff are assigned one or more roles that grant them access permissions for privileged accounts on systems and applications that are related to their job requirements.

An HR system-feed to Tivoli Identity Manager automatically triggers the provisioning of personal accounts that are appropriate for the type of employee being added. When the HR system-feed identifies that an individual has been terminated, a customized deprovisioning workflow is also automatically triggered to transfer and suspend accounts of the employees. This automation addresses the IT Director's task of expediting provisioning of new store employee, because the system automatically provisions the required e-mail and store accounts without IT staff involvement. Tasks that previously took a couple of days when performed manually, or even longer during peak seasons, are now completed within minutes. The automation also frees IT staff to concentrate on matters other than addressing tedious error-prone manual-account creation and deletion requests.

When store employees forget their passwords, the IBM Privileged Identity Management solution provides a self-service Web interface that allows employees to answer personal challenge-response questions to immediately reset their password. This self-service feature reduces a large percentage of the organization's help-desk calls that are fielded by their IT staff, and helps the store associate get back to working much faster than calling support staff to open a help-desk ticket.

The retailer's IT architecture is presented in Figure 12 on page 19. IBM Privileged Identity Management solution server components, HR systems, and other corporate applications and servers are located within the headquarter's data center. The HR system feeds employee data to Tivoli Identity Manager. All 1,200 stores are connected through a wide area network (WAN). Each store runs two AIX servers and several Windows-based POS terminals, with the installed Tivoli Access Manager for Enterprise Single Sign-On client and an integrated smart card reader.

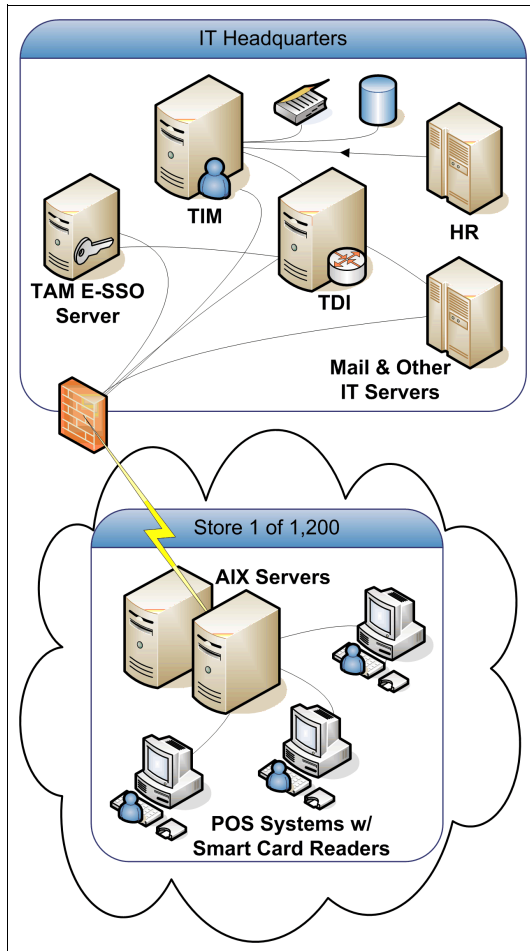


Figure 12 Retail architecture overview

To reduce the vast number of accounts in the organization, the IBM Privileged Identity Management solution eliminates the retailer's practice of provisioning an account with *sudo* or *administrative privileges* on every single server in the organization for each of retailer's 600 IT staffers. By assigning appropriate accesses to IT staff members, the staff members can check out an administrative account for any system or application that they need to work on for a specified amount of time. The check-out process can be performed manually through the Web Self-Service User Interface or automatically through the Tivoli Access Manager for Enterprise Single Sign-On client. After the IT staff members complete their work, the account is checked back in, or if this step is omitted, the account lease expires and the account is automatically checked in and the password is changed. Each account check-out, and subsequent check-in, generates an audit log record for accountability. This model of account leasing eliminates the 600+ individual accounts that were created on each of the retailer's 2,400+ servers. Having approximately *1.4 million fewer privileged accounts* in the organization's infrastructure greatly reduces the risks of an account being compromised. It also reduces the retailer's overhead that is associated with recertifying access requirements and reconciling all those accounts to current active employees.

Recertifying a user's continued business need for an account or access permission is also automated by using the Tivoli Identity Manager recertification feature. Further, the account leasing approach simplifies recertification by authorizing meaningful accesses rather than all 2,400 accounts that an individual IT staffer would have owned under the retailer's traditional process.

Table 2 shows that the IBM Privileged Identity Management solution approach to privileged account management dramatically reduces the total number of accounts in the organization.

Table 2 Comparison of total privileged accounts based on solution approach

Solution approach	IT staff	Servers	Total privileged accounts
Prior state	600	2,400	1,440,000
IBM PIM solution	600	2,400	2,400

To ensure compliance across all systems, the IBM Privileged Identity Management solution reconciles all accounts and privileges weekly for most systems. The retailer also chooses to more frequently reconcile servers and applications of special concern. This check ensures that the organizational policies, which are defined in Tivoli Identity Manager, are applied consistently across all systems and applications. If an administrator or other entity creates an account or extends permissions beyond the defined policies, an alert is generated. These alerts allow the responsible system or application owner to correct the problem, to maintain their compliance posture.

PCI DSS⁴ security standards are a set of comprehensive requirements for enhancing payment account data security within an organization. It is a multifaceted security standard covering security management, policies, procedures, network architecture, software design and other critical protective measures. Although the IBM Privileged Identity Management solution does not address the standard entirely itself, it does provide the retailer a major step towards asserting policy, and ensures that access procedures are followed and enforced effectively. Insufficient internal controls over privileged accounts negatively affect an organization’s capability to meet all of these requirements. The retailer may use the IBM Privileged Identity Management solution to very narrowly limit access to sensitive payment and financial-related systems, databases, and applications to only those employee’s with such a need.

To secure and simplify store POS systems Tivoli Access Manager for Enterprise Single Sign-On is used to provide smart-card-based single sign-on with session locking after the smart card is removed. Store employees already use a smart-card-based ID badge to clock-in, clock-out, and gain access to secured employee-only areas of the retail store. Typically, two or three employees share the same POS system at some time during a workday shift. Smart card support is integrated into Tivoli Access Manager for Enterprise Single Sign-On and the IBM Privileged Identity Management solution integrates the retailer’s existing smart card to both harden the security and simplify the employee’s use of the retailer’s POS systems with the following features:

- ▶ Grace period given to maintain rapid on-boarding of new employees

The IT department recognized that smart card badges took several days to be printed and be delivered, therefore, the department extended a grace period for which a new employee could log on with only a Windows password (single-factor authentication). The employee then has to register a smart card (second-factor authentication) before the grace period expires. After the expiration, the employee can register and log on only with the help of an administrator.
- ▶ Two-factor authentication for initial POS logon

Employees log on with both their smart card inserted and also enter their Windows password when they access a POS system for the first time that day.

⁴ For more information about PCI DSS, see: <https://www.pcisecuritystandards.org>

- ▶ Simplified authentication and locking during the day

During the day, the employee only has to remove the smart card to lock the POS system when that employee steps away. When the employee returns to the POS system during the day, logon is simplified by requiring the employee only to insert the smart card into the POS system again. Because the smart card is part of the employee's store ID badge, which is integrated with the store's physical access controls to employee-only areas, and also tied to the time-recorder, the employee is unlikely to leave or forget the badge/smart card in a POS system.

- ▶ Fast user switching between employees

Tivoli Access Manager for Enterprise Single Sign-On provides *fast user switching*. This switching allows employees to rotate POS duties through breaks or other tasks while still using the simplified re-authentication explained previously. This approach is a significant time-saver when manager overrides are required to complete a transaction (the transaction requires manager authority to approve). The fast user switching also allows employees to respond more quickly to peaks in customer volume, therefore keeping check-out lines short.

System administrators are granted permission to manually check out a password by using the Tivoli Identity Manager Self-Service User Interface for disaster recovery, hardware maintenance, and other needs. Using a secure Tivoli Identity Manager Self-Service User Interface session, the user manually checks out an entitled credential. The IBM Privileged Identity Management solution can be configured to prompt for additional authentication information before displaying the requested credentials. This feature is necessary for situations where the Tivoli Access Manager for Enterprise Single Sign-On client might not be used, or there is a lack of network connectivity. After the administrator's work is completed, the administrator may manually check in the ID or allow the lease period to expire, and then Tivoli Identity Manager automatically checks in the ID, changing the password as part of the check-in process.

By moving from a traditional siloed/department IT approach to the complete end-to-end lifecycle management solution of the IBM Privileged Identity Management solution, the retailer makes productivity gains, greatly improves its security and audit posture, and reduces costs.

Alternative: In our scenario, we used a smart card in this retail environment. An alternative way is for the organization to use, for example, biometric fingerprints or the employee's photo badge.

Financial services organization with compliance issues

The financial services scenario describes an organization facing security and compliance regulations in addition to the costs and risks described in the retail scenario. The use of privileged identities must be controllable and distinctly referable to the specific person who is requesting privileged access to a system, database, or application.

Scenario description

In this scenario, a global financial services organization, headquartered in Germany, must regain control of its security posture to pass audits and remain in compliance with several national regulations and the tightening of industry standards. The organization operates branches in several countries where IT management has been done on a mostly local basis. The organization owns several thousand servers and applications and does not have

complete report or inventory of user access permissions, which affects the organization's ability to meet audit requirements.

The Chief Security Officer (CSO) has mandated that the following improvements be made throughout the global organization:

- ▶ Maintain a centralized inventory of all privileged IDs.
- ▶ Maintain an inventory of the level of accesses of all privileged IDs.
- ▶ Enforce controls for individual accountability.
- ▶ Provide SSO to privileged and personal accounts.
- ▶ Ensure SSO login works consistently across domains.
- ▶ Integrate corporate smart cards, and also Swiss employee's RFID badges, with the SSO authentication process.
- ▶ Monitor activity performed with privileged IDs on systems.
- ▶ Issue alerts and take action when a user attempts to access a system for which they are not authorized.
- ▶ Assert compliance with the EU Data Protection Act and industry security standards.

Solution

To better centralize the management of the financial organization's IT infrastructure, the IBM Privileged Identity Management solution is deployed to address control and inventory of both IDs and access levels. Tivoli Access Manager for Enterprise Single Sign-On features fulfill the SSO mandates that are laid out by the CSO, and aspects of the monitoring mandate.

As described in the retail scenario, the IBM Privileged Identity Management solution provides automated provisioning, recertification, deprovisioning, and reporting per defined policies throughout all managed systems and applications. This centralized control allows the IBM Privileged Identity Management solution to serve as an authoritative source to report on privileged IDs in the organization. Detailed reporting on the level of access for all privileged IDs is available. This data and reporting functions provide the documentation necessary for compliance with industry standards and government regulations.

Figure 13 shows the financial organization's IT infrastructure. The infrastructure uses various second-factor authentication methods.

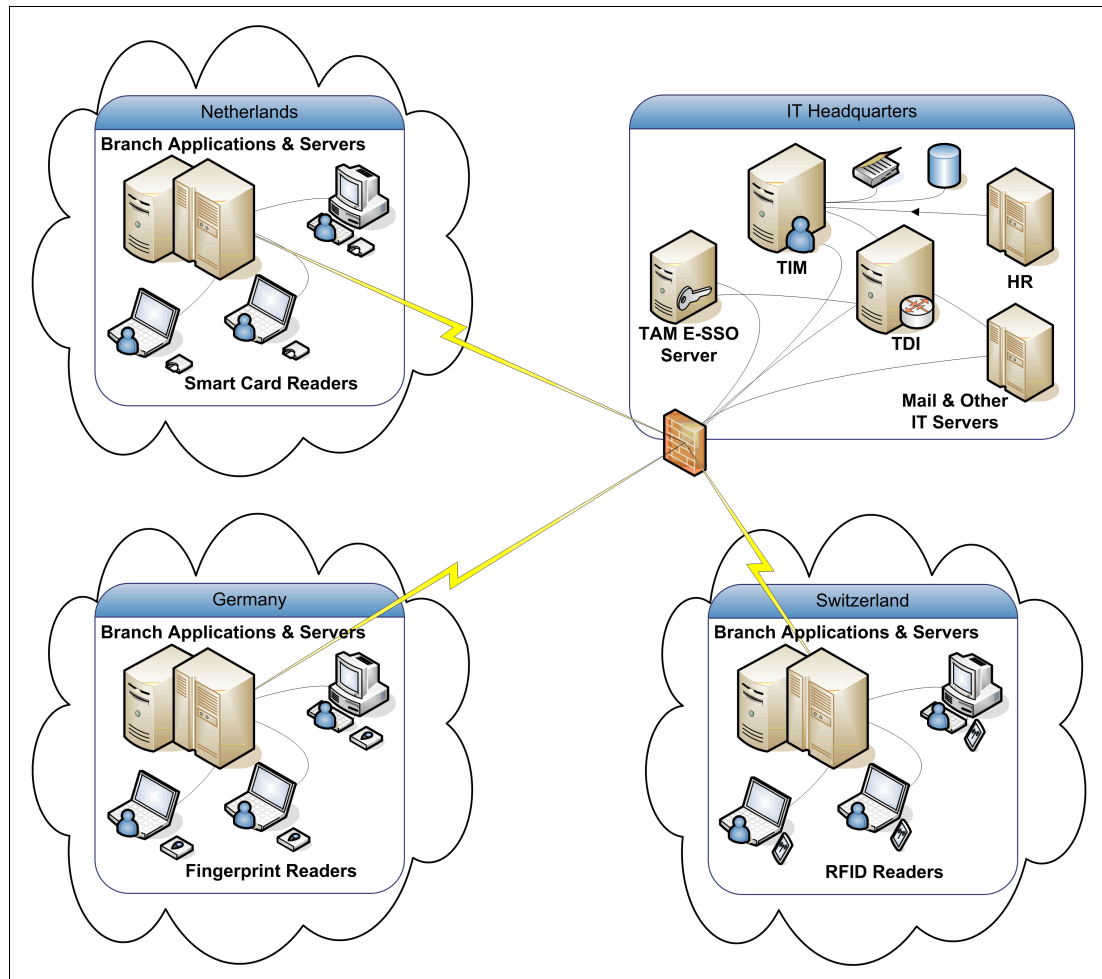


Figure 13 Financial organization infrastructure

The Tivoli Access Manager for Enterprise Single Sign-On component of the IBM Privileged Identity Management solution provides robust SSO capabilities. The Tivoli Access Manager for Enterprise Single Sign-On client allows an ATM technician from the main office in the Netherlands to address an outage at a branch office. The technician logs in once to the notebook, a process also requiring the technician's physical smart card, and then starts the SSH client to connect to the local branch server. Because personal accounts are not allowed on branch servers, Tivoli Access Manager for Enterprise Single Sign-On prompts the technician for which privileged ID to use. The technician selects the DBA role because the technician has to restore data to the ATM's underlying DB2® tables. Based on that selection, Tivoli Access Manager for Enterprise Single Sign-On contacts the Tivoli Identity Manager server to check out the db2admin user ID and password. The credentials are seamlessly inserted into the technician's SSH client, directly authenticating the technician's connection to the server. This check-out grants the technician exclusive use of the branch servers' db2admin account for up to four hours. The db2admin account check-out is logged for audit purposes both by Tivoli Access Manager for Enterprise Single Sign-On and the Tivoli Identity Manager server.

Reporting is centralized for the organization, using Tivoli Identity Manager's audit log database as seen in Figure 14. These reports can be run and customized to meet regulatory requirements and the need to assert compliance or account inventories.

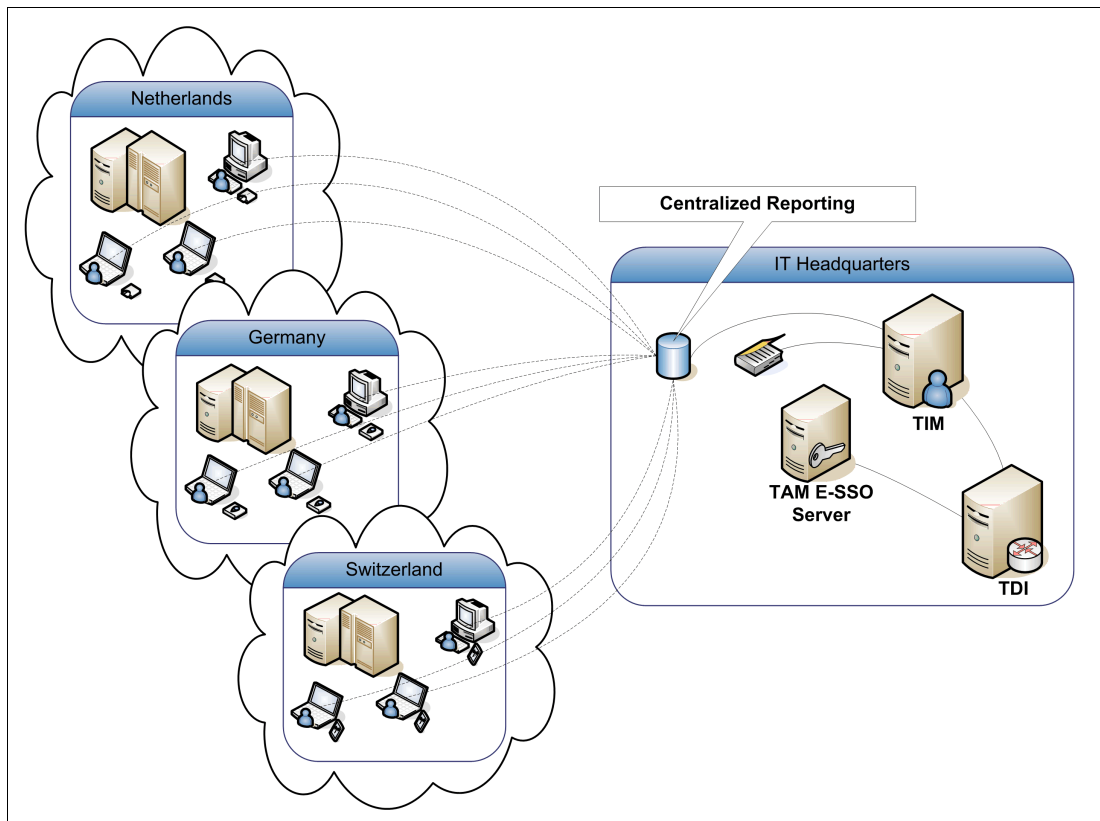


Figure 14 IT reporting data is available in Tivoli Identity Manager

After completing the work required, the ATM technician logs off the SSH connection. Tivoli Access Manager for Enterprise Single Sign-On detects the logoff and automatically checks in the db2admin account. This step also generates log entries for auditing purposes.

A sample of the Tivoli Access Manager for Enterprise Single Sign-On auditing data that is captured is listed in Table 3.

Table 3 Audit log example entry

Audit field	Audit value
Time	Jun 30, 2010 2:23:07 PM
Event	Privileged/Shared ID Checked for pComm from 10.103.44.83 Privileged User Id=jdoe, Privileged Role=ServiceDesk_Admin
Enterprise User Name	jdoe@us.ibm.com
Target System Name	app_pcomm
IP Address	10.103.44.83
Result	OK

Because the financial organization's employees have access to very sensitive customer information, Tivoli Access Manager for Enterprise Single Sign-On features are utilized to provide strong second-factor authentication controls. The financial firm recently acquired another bank in the Netherlands where branch employees use smart cards, other branches in Germany use fingerprint readers, and the Switzerland branch offices use RFID cards. Tivoli Access Manager for Enterprise Single Sign-On features allow all three second-factor technologies to be supported in policies. Many employees also store sensitive customer data on their notebooks, which is of particular concern because they travel frequently and notebook loss and theft can occur. To augment existing disk encryption security, the Chief Security Officer directed that Tivoli Access Manager for Enterprise Single Sign-On be implemented to always require strong two-factor authentication, which can help prevent compromising any customer data. This requirement forces the employees of any branch, world-wide, to provide both their second-factor credential (fingerprint, smart card, RFID card) and the password each time they log on or unlock the system. Tivoli Access Manager for Enterprise Single Sign-On features allow this second-factor authentication requirement to be defined as very granular group policies, based on host name, IP ranges, or Active Directory groups.

A mortgage broker in one of the German offices authenticates to the notebook, swiping a fingerprint, and then entering a password. The broker then uses the corporate mortgage application to submit a new loan application for a client. In an attempt to force the loan through, the broker then attempts to log in to the organization's loan approval application. Tivoli Access Manager for Enterprise Single Sign-On detects that this broker does not have any credentials to access this application and informs the broker, audits the attempt, and triggers a custom notification event to alert the organization's fraud department.

The IBM Privileged Identity Management solution can provide SSO to both privileged and personal accounts within the organization. Administrators benefit from the automation of checking out, authenticating, and then checking in a privileged ID. The process is consistent across all the systems they have to administer in the organization, including Windows, Linux®, AIX, and mainframe applications. Both administrators and staff employees without any extra privileges can log on to their personal systems and applications using credentials, which are saved on their local Tivoli Access Manager for Enterprise Single Sign-On client.

Summary

More stringent industry standards and ever tightening government regulations now demand that organizations adopt privileged account management practices to help maintain their compliance posture. Traditional identity management approaches in use today can leave gaps around proper privileged user management and are often inconsistent with current regulatory requirements. The IBM Privileged Identity Management solution helps to close those gaps and can provide a complete end-to-end solution based on our existing industry-leading identity and access-management products.

The IBM Privileged Identity Management solution allows an organization to centrally manage and audit privileged users across systems, applications, and platforms to maintain compliance throughout the entire privileged identity lifecycle. Enterprise single sign-on features provide a consistent, seamless, user experience across applications, hosts, and servers, and help keep the solution even more secure. By significantly reducing the number of privileged accounts in an organization, the IBM Privileged Identity Management solution helps reduce the risks. It can also dramatically reduce the overhead that is associated with provisioning, deprovisioning, recertifying, and reconciling accounts that have become an increasing problem as server density increases exponentially with virtualization, cloud computing, and other technology trends.

Other resources for more information

For additional information about the following products, see the resources listed:

- ▶ IBM Tivoli Identity Manager:
 - Tivoli Identity Manager Version 5.1 information center
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm>
 - *Identity Management Design Guide with IBM Tivoli Identity Manager*, SG24-6996
<http://www.redbooks.ibm.com/abstracts/sg246996.html>
- ▶ IBM Tivoli Access Manager for Enterprise Single Sign-On
 - Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 information center
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itamesso.doc/toc.xml>
 - *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350
<http://www.redbooks.ibm.com/abstracts/sg247350.html>

The team who wrote this guide

This guide was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).



Axel Buecker is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.



Barry Evans is an Advisory Software Engineer with IBM Tivoli Security Software division, working at Research Triangle Park, North Carolina. He is a Technical Lead with the IBM Tivoli Identity Manager L3 service team and has worked in the Identity and Access Management area for eight years. Before joining IBM, he worked for Cisco Systems for two years as an IT Analyst, developing Web-based support tools. Barry holds a degree in Computer Science from North Carolina State University.



Dirk Rahnenfuehrer is a Senior Accredited IT Specialist in Switzerland. He has 11 years of experience in the IT industry and holds a degree in Physics from RWTH Aachen University. He has worked at IBM as a Systems Management Specialist for nine years. His areas of expertise include Systems Management and Security products, focusing on identity management since 2003 and single sign-on since 2005.

Thanks to the following people for their contributions to this project:

Milton Hernandez, Eng Kiat Koh, John Sullivan, Sharad Ganesh, Ryan Fanzone, Prema Vivekanandan, Leanne L. Chen
IBM

Diane Sherman, Editor
IBM ITSO

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:
<http://www.facebook.com/pages/IBM-Redbooks/178023492563?ref=ts>
- ▶ Follow us on twitter:
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4660-00, was created or updated on May 6, 2010.




Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US 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 <http://www.ibm.com/legal/copytrade.shtml>



The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
DB2®
IBM®

Redbooks®
Redguide™
Redbooks (logo) ®

Tivoli®

The following terms are trademarks of other companies:

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

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

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