IBM Security Privileged Identity Manager
Version 2.0

Product Overview Guide

IBM

IBM Security Privileged Identity Manager
Version 2.0

Product Overview Guide

IBM

Note

Before using this information and the product it supports, read the information in Notices.

Edition notice

Note: This edition applies to Version 2.0 of *IBM Security Privileged Identity Manager* **(product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

Figures

Tables

Chapter 1. Virtual appliance overview

The IBM® Security Privileged Identity Manager is an appliance-based solution that provides privileged identity management, Application identity management, and session recording.

IBM Security Privileged Identity Manager Virtual Appliance features:

- A configuration wizard for the first time configuration of the IBM Security Privileged Identity Manager solution in a stand-alone or a cluster mode.
- A dashboard for viewing system status such as system notifications, cluster status, component and application status, deployment statistics, and disk usage.
- Analysis and diagnostics tools such as memory statistics, CPU utilization, and troubleshooting log files..
- Control of system settings such as host name, date, time, and network settings.
- A graphical management interface for configuring the IBM Security Privileged Identity Manager features.

Privileged identity management overview

IBM Security Privileged Identity Manager helps organizations manage, automate, and track the use of shared privileged identities.

The solution provides the following features:

- Centralized administration, secure access, and storage of privileged shared account credentials
- Role-based access control for shared account credentials
- Lifecycle management of shared accounts' password
- Single sign-on through automated check-out and check-in of shared credentials
- Auditing of shared credentials access activities
- Session recording and replay
- Integration with the broader Identity and Access Management Governance portfolio
- Application identity management

Privileged IDs are general user IDs that are distinguished by the assignment of security, administrative, or system privileges. These IDs include pre-built administrative accounts found in operating systems and applications, such as root, administrator, sa, db2admin.

In an enterprise environment, multiple Administrators might share access to a single privileged ID for easier administration. When multiple Administrators share accounts, you can no longer definitively prove that an account was used by one Administrator as opposed to another. You lose personal accountability and audit compliance.

With IBM Security Privileged Identity Manager, organizations can better manage privileged IDs. IBM Security Privileged Identity Manager ensures that a privileged user can acquire privileged credentials only:

- If they need it.

- When they need it.
- On the condition that they need it.
- If they have access to it.

When deployed with its Single Sign-On feature, IBM Security Privileged Identity Manager allow privileged users to log on to a system without any knowledge of the password for the privileged identity.

Architecture overview

The privileged identity management solution consists of IBM Security Privileged Identity Manager, database, managed resources, and endpoints.

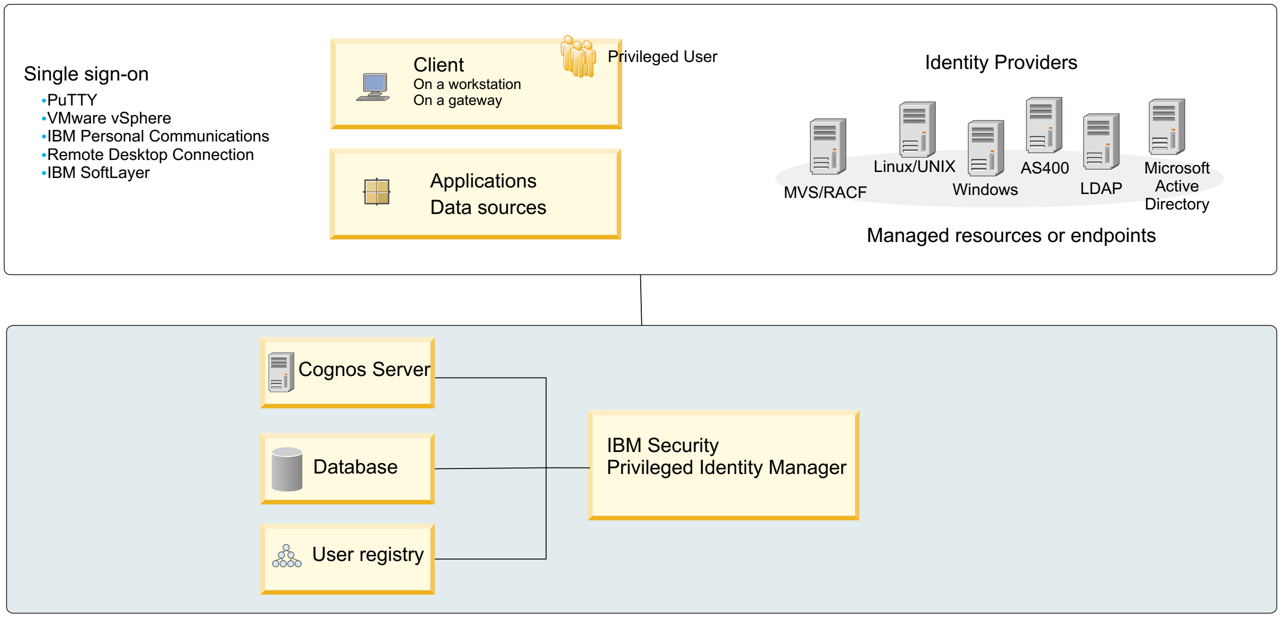

Figure 1. IBM Security Privileged Identity Manager components

IBM Security Privileged Identity Manager consists of the following components:

Privileged Credential Manager
The Privileged Credential Manager provides privileged administrators access to a credential or pool of shared credentials that are stored in a secure credential vault. It enforces access controls to credentials and automate password changes to these credentials. It also features user and role management.

It provides the following consoles.

Table 1.

Console	Description
Administrative console	A Privileged Identity Manager administrator and a privileged administrator can use this console to on-board credentials and setup role-based access policies on these credentials.

Table 1. (continued)

Console	**Description**
Privileged Identity Manager Service Center	A Privileged Identity Manager administrator and a privileged administrator can use this console to on-board credentials and setup role-based access policies on these credentials..
Self-service console	A Privileged user can use this console to check out and check in entitled credentials and integrate with IBM Security Access Manager for Enterprise Single Sign-On AccessAgent for automated checkout and checkin.

Client The client can be deployed on a user workstation, or a gateway for shared workstation environments. The client provides single sign-on automation and session recording features when an attempt is made to log on to a managed resource.

Single sign-on

IBM Security Access Manager for Enterprise Single Sign-On provides automated check-out and check-in of shared access credentials from the IBM Security Privileged Identity Manager Server.

AccessAgent is the single sign-on client that is installed on user workstations. This agent automates the checkout and single sign-on with privileged credentials into various systems.AccessAgent consults logon automation profiles or AccessProfiles for specifications on how and when to checkout and single sign-on to different client applications. The Privileged Identity Manager administrator uses the AccessStudio tool to create and maintain AccessProfiles that are uploaded to the IBM Security Privileged Identity Manager Virtual Appliance for distribution to AccessAgent. The Privileged Identity Manager administrator uses the Single Sign-On administration console to configure the single sign-on and Session recording policies when required.

Session recording

Privileged Session Recorder is a virtual surveillance camera that captures user activity during an active session on a workstation. Session recording provides a complete, irrefutable record of what a user did.

The Privileged Session Recorder comprises of a server component in the IBM Security Privileged Identity Manager Virtual Appliance and a client component in the AccessAgent.

When enabled and configured, AccessAgent records user activity and screen outputs of sessions visited with a checked-out privileged ID.

AccessAgent consults the IBM Security Privileged Identity Manager of an application for specifications of when to start and stop recording a session.

The captured recordings are submitted to the Privileged Session Recorder server component where it is stored into the IBM Security

Privileged Identity Manager database. You can later search and replay these recordings through the Privileged Session Recorder console.

Applications and data sources
Privileged credentials that are embedded in applications, scripts, or Java EE data sources can be managed by IBM Security Privileged Identity Manager by registering the applications with the bundled App ID Toolkit.

Cognos server
The Cognos report server provides access to IBM Security Privileged Identity Manager reports.

Database

IBM Security Privileged Identity Manager databases stores credential data, access roles and policies, single sign-on AccessProfiles, audit logs and session recordings.

User registry

User registry stores IBM Security Privileged Identity Manager user accounts and operational data.

Adapters

IBM Security Privileged Identity Manager Virtual Appliance includes an embedded Directory Integrator component with adapters for connecting to external systems. These adapters are used for automating password change of on-boarded credentials. Where needed, one can configure IBM Security Privileged Identity Manager to connect to external adapters hosted outside IBM Security Privileged Identity Manager Virtual Appliance.

Client deployment modes

The IBM Security Privileged Identity Manager uses the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent as its client-side component. You can deploy the client either on user workstations or on a Citrix server acting as a gateway.

Client on user workstations

In this mode, AccessAgent performs automated check-out, check-in, and session recording operations on applications that are running on user workstations. This deployment mode is suitable when users do not have administrative privileges on their workstations.

The workstations where AccessAgent is installed must be configured to run in the default "personal desktop" mode in IBM Security Access Manager for Enterprise Single Sign-On. *Shared desktop* and *private desktop* configurations are not supported.

Client on Citrix gateway

For enhanced security and easier management, AccessAgent can be deployed on a Citrix XenApp server that is acting as a gateway to the managed resources. The client performs automated check-out, check-in, and session recording operations on published applications that are running on the Citrix XenApp server.

Users access applications that are used for connecting to the managed resources, such as Remote Desktop Connection Client and PuTTY, through the Citrix Receiver application.

In this mode, the AccessAgent does not need to be installed on user workstations. If the client is also on the workstation that is used to access the Citrix gateway, then the client on the Citrix gateway can use the Virtual Channel connection or operate in Lightweight mode. For more information, see the section *AccessAgent on Citrix and Terminal Server Guide* in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Client on a Remote Desktop Gateway

Remote Desktop Gateway, a role service that is part of the Remote Desktop Services server role on Windows Server 2012, enables organizations to provide access to standard Windows programs from virtually any location, from the Internet or an intranet.

Similar to the Citrix gateway, the Remote Desktop Gateway acts as a gateway to the managed resources. In this mode, the AccessAgent client can be deployed on a Remote Desktop Gateway server as a RemoteApp. Programs published as RemoteApp programs are accessed remotely by users through Remote Desktop Services or Remote Desktop Web Access and appear as if they are running on the local computer.

Users can perform automated check-out, check-in, and session recording operations with privileged credentials that are managed by IBM Security Privileged Identity Manager, with other RemoteApp programs like PuTTY.

For more information, go to the Microsoft website and search for `Remote Desktop Gateway 2012`.

Related information:

IBM Security Access Manager for Enterprise Single Sign-On product documentation
Learn more about the Virtual Channel Connector configuration and Lightweight mode in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Microsoft website
Go to the Microsoft website to learn more about Remote Desktop Gateway.

Managed resources support

The IBM Security Privileged Identity Manager supports automated check-out and check-in for managed resources.

Managed resources can run on the following architectures or operating systems:

- Linux/UNIX
- Windows
- Mainframes

Chapter 2. Personas and use cases

There are different personas that are involved with the setup and usage of the virtual appliance. Each persona is responsible for a set of tasks or is privileged to do specific workflows.

Primary user types

Each privileged identity management user type has a different role and objective to achieve with the solution.

Table 2. Privileged identity management users and tasks

User type	Tasks	Subtasks and references
Virtual appliance administrator	Deploy and configure the IBM Security Privileged Identity Manager Virtual Appliance	1. Installing and configuring the database server 2. Installing and configuring the directory server 3. Setting up the virtual appliance 4. Installing the IBM Security Privileged Identity Manager Virtual Appliance 5. Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance 6. Setting up a stand-alone or primary node for IBM Security Privileged Identity Manager a. Enabling the session recording feature in the virtual appliance b. Managing the Database Server configuration c. Managing the Directory Server configuration d. Managing mail configuration 7. Setting up a member node for the IBM Security Privileged Identity Manager 8. Installing AccessAgent
	Set up and enact disaster recovery for the virtual appliance	1. Setting up a primary virtual appliance 2. Setting up a secondary virtual appliance
	Apply Fix Pack	Use the `fixpack` command in the IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager.
	Upgrade Firmware	Use the `firmware_update` command in the IBM Security Privileged Identity Manager Virtual Appliance command line interface commands for IBM Security Privileged Identity Manager.
	Reconfigure the virtual appliance	• Reconfiguring the data store connection • Reconfiguring the directory server connection
	Use the Appliance Dashboard to manage the virtual appliance	Virtual appliance administrator tasks in Appliance Dashboard

Table 2. Privileged identity management users and tasks (continued)

User type	Tasks	Subtasks and references
Privileged Identity Manager administrator	Uses the Shared access consoles to: • On-board users and roles • Manage the following: – Organization structure – Administrative domains – Privileged administrators and users – System-wide roles – Default credential settings – Access approval workflows – Supported Identity Provider profiles – Resources – Groups – Password policies (password reset scheduler) – Shared credentials and credential pools – System security and views	Privileged Identity Manager administrator tasks in Shared access consoles
	Uses the Single Sign-On administration console to review the session recording policies	Privileged Identity Manager administrator tasks in Single Sign-On administration console
	Uses the IBM Cognos® reporting framework to generate and view the IBM Security Privileged Identity Manager reports.	Report administration
	Install and configure the IBM Security Privileged Identity Manager adapter for the managed resource. **Note:** This step does not apply to agentless adapters.	See the adapter documentation.

Table 2. Privileged identity management users and tasks (continued)

User type	Tasks	Subtasks and references
Privileged administrator	Uses the Privileged Identity Manager Service Center to perform the following tasks: • On-board credentials. • Manage credentials and credential pools. • On-board and manage resources and identity providers. • Approve role access requests • Setup roles and shared access policies	• Privileged administrator tasks in Shared access consoles
Privileged user	Uses the Self-service console to perform the following tasks: • Manually check out and check in shared credentials. • Request access. • Uses the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent to single sign-on to systems and applications with shared credentials.	Privileged user tasks in Shared access consoles

Table 2. Privileged identity management users and tasks (continued)

User type	Tasks	Subtasks and references
Privileged administrator (for applications)	Uses the Shared access consoles to perform the following tasks: • Change passwords that are used by applications, without having to change stored passwords in individual applications. • Change passwords that are used by applications automatically according to the frequency required by the organization. • Revoke access to applications that no longer require access to a resource. • Remove static passwords from scripts, compiled applications or configuration files. • Remove remote, static passwords from shell scripts that run on an automated schedule on remote hosts. • Remove static passwords that are used by various data sources on Java™ EE or WebSphere® Application Server hosts.	• Provide managed credentials to a compiled application workflow • Provide managed credentials to scripts workflow • Providing managed credentials to data source connections for WebSphere Application Server applications • Registering an Application Instance
User manager	Uses the Self-service console to approve user requests.	Privileged User Manager tasks in Shared access consoles
Security administrator or auditor	• Searches and reviews activities of privileged users. • Demonstrates compliance to regulations related to privileged users. • Generate and review reports. • Uses the Privileged Session Recorder console to search and review recordings to verify compliance to audit requirements.	Security administrator and Privileged Session Recorder auditor tasks in Privileged Session Recorder console

Chapter 3. IBM Security Privileged Identity Manager consoles

IBM Security Privileged Identity Manager consists of different consoles that enable users to do the tasks that they need to complete, based on their user role.

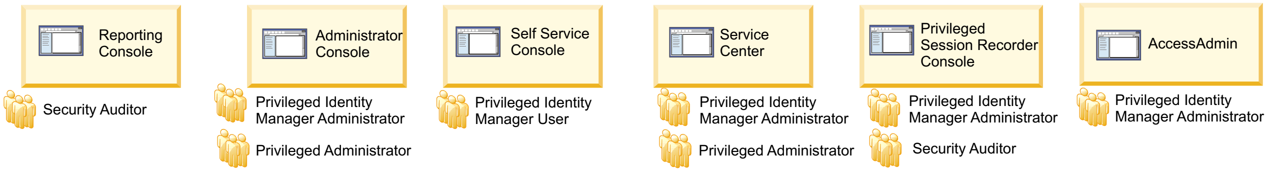
Reporting Console
Security Auditor
Administrator Console
Privileged Identity Manager Administrator
Privileged Administrator
Self Service Console
Privileged Identity Manager User
Service Center
Privileged Identity Manager Administrator
Privileged Administrator
Privileged Session Recorder Console
Privileged Identity Manager Administrator
Security Auditor
AccessAdmin
Privileged Identity Manager Administrator

Figure 2. The various consoles for different users of the IBM Security Privileged Identity Manager solution

Virtual appliance dashboard

The Appliance Dashboard provides important status information, statistics, and quick links to the administrative consoles. The virtual appliance administrator can access the dashboard after completing the virtual appliance configuration.

Login URL
`https://`*`ip-address`*

Default login user name
`admin`

Default login password
`admin`

User Virtual appliance administrator

Table 3. Virtual appliance administrator tasks

Tasks	Subtasks and references
View appliance information	• Viewing notifications • Viewing the cluster status • Viewing and using server controls • Viewing deployment statistics • Viewing the middleware and server monitor widget • Viewing and using quick links • Viewing disk usage • Viewing IP addresses • Viewing partition information • Viewing the About page information • Viewing the licensing
Manage external entities	• Managing the Database Server configuration • Managing the Directory Server configuration • Configuring the Load Balancer settings
Managing firmware and fix packs	• Viewing the update history • Managing the firmware settings • Installing a fix pack

Table 3. Virtual appliance administrator tasks (continued)

Tasks	Subtasks and references
Manage server settings	• Managing mail configuration • Managing the server properties • Managing feed files
Retrieving and configuring logs	Managing log configuration
Feature activation	• Enabling the session recording feature in the virtual appliance • Enabling the application identity management feature in the virtual appliance
Manage system settings	• Viewing the memory utilization • Viewing the CPU utilization • Viewing the storage utilization • Configuring the date and time settings • Configuring the administrator settings • Managing the snapshots • Managing the support files • Restarting or shutting down

Shared access consoles

IBM Security Privileged Identity Manager provides three user interfaces for shared access: the Administrative console, the Self-service console, and the Privileged Identity Manager Service Center. The interfaces are separate and users access them through different web addresses.

Table 4. Shared access consoles.

Consoles	Description	Users	Login URL
Administrative console	Contains the entire set of administrative tasks, such as managing roles, policies, and users. This persona-based console provides sets of tasks, each tailored for the needs of the default administrative user types.	• Privileged Identity Manager administrator • Privileged administrator • Security administrator or auditor	• `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`

Table 4. Shared access consoles (continued).

Consoles	Description	Users	Login URL
Self-service console	Provides a simpler subset of personal tasks that apply only to the user. Users can do the following tasks: • Update their personal information and passwords. • Request and manage access to roles. • Check out and check in shared credentials. • View password of credentials that are checked out.	• Privileged administrator • Privileged user • User manager	• `https://`*`hostname`*`/itim/self` • `https://`*`ip-address`*`/itim/self`
Privileged Identity Manager Service Center	Intended for Privileged administrators to on-board and manage shared credentials, manage resources, identity providers, and application identities.	• Privileged administrator	• `https://`*`hostname`*`/ispim/ui` • `https://`*`ip-address`*`/ispim/ui`

The default login user name is `pim manager` and the default login password is `secret`.

Privileged Identity Manager administrator

The Privileged Identity Manager administrator uses the Shared access consoles to do the following tasks.

Table 5. Privileged Identity Manager administrator tasks

Tasks	Subtasks and reference	Console
Configure system-wide organizational structure, roles, and password policies.	1. Define password policies for the ISPIM user account. For example, set password expiry. See Enabling password expiration. For other policies, see Password administration. 2. Create an administrative domain for the Privileged administrator in an organization tree so that the Privileged administrator can have a domain to manage his shared credentials. See Create a node in an organization tree 3. Create roles. See Creating roles. **Note:** Skip this task if the role exists. 4. Review and configure the default credential settings. See Configuring the credential default settings. 5. Configure approval workflows. See Workflow management. 6. Configure the Self-service console view for privileged users. See View management	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`
On-board Privileged administrators.	1. Create an ISPIM user account. See Creating user profiles. 2. Add user to the predefined privileged administrator group. See Adding members to groups. 3. Add an ISPIM administrative domain and make the Privileged administrator user as the administrator of the domain. See Creating a node in an organization tree.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`
On-board Privileged users.	Create an ISPIM user account. See Creating user profiles.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`
On-board new Service Type to configure IBM Security Privileged Identity Manager with additional adapters for managing credentials through new Identity Provider types.	Create a Service Type by importing a service type profile. **Note:** This process is needed only when you want the password to be reset when the credential for the managed resource is checked in. For each identity provider type, you must configure the profile information in IBM Security Privileged Identity Manager. See Importing service types.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`

Table 5. Privileged Identity Manager administrator tasks (continued)

Tasks	Subtasks and reference	Console
Assign Privileged Session Recorder auditor role to ISPIM user **Note:** • The Security administrator or auditor must already have an ISPIM user account. • Do this task only if Session Recording is enabled.	1. Create a Privileged user. See Creating user profiles 2. Assign the user to a Privileged Session Recorder Auditor role if needed or if the role is already defined. See Adding users to membership of a role.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`
Define and configure approval for user role	1. Create a workflow for an access request. See Adding an entitlement workflow. 2. Assign an owner and attach the access approval workflow to the role. See Modifying roles.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`
Enable and configure password reset life cycle rule.	Enable and configure the system to reset credential's password. See Configuring scheduled password reset.	Administrative console • `https://`*`hostname`*`/itim/console/main` • `https://`*`ip-address`*`/itim/console/main`

Privileged administrator

The Privileged administrator is responsible for the following tasks.

Note: The Privileged Identity Manager administrator can also perform the tasks of a Privileged administrator.

Table 6. Privileged administrator tasks

Tasks	Subtasks and reference	Console
On-board Resource	1. Create the service instance for the managed resource. See Creating identity feed services. 2. On-board a Resource. See Adding resources.	Privileged Identity Manager Service Center

Table 6. Privileged administrator tasks (continued)

Tasks	**Subtasks and reference**	**Console**
Configure the Identity Provider that is supported by IBM Security Privileged Identity Manager	1. Install and configure the IBM Security Privileged Identity Manager Adapter for the identity provider. For more information, see the IBM Security Privileged Identity Manager Adapter documentation. **Note:** This step does not apply to agentless adapters. 2. Create the identity provider. See Adding identity providers.	Privileged Identity Manager Service Center
On-board credentials.	1. Add credential to the credential vault. See Adding credentials through Manage Credentials. If you want the password on the credential of the resource to be changed when you check in the credential, you must connect the credential to the identity provider. To create an identity provider, see Creating an identity provider. To connect the credential to the identity provider, see Connecting credential to an identity provider. 2. (Optional) Set up the credential pool for the credentials. See Creating credential pools. 3. Define roles for the group of users who can access the credentials or credentials in the pool. See Creating roles. 4. Assign users to the role. See Adding users to membership of a role. 5. Define a shared access policy to allow role members to check out or check in the credentials or credential pools. See Creating shared access policies. Alternatively, you can add credential to the vault and set up the credential pool by using Batch Upload. See Uploading a CSV file with the administrative console.	Privileged Identity Manager Service Center
Manage credential pools	1. Create a credential pool for added credentials. 2. Create Privileged user role for the credential pool. 3. Define a shared access policy to allow role members to check out or check in the credentials or credential pools. See Creating shared access policies.	Privileged Identity Manager Service Center

Table 6. Privileged administrator tasks (continued)

Tasks	Subtasks and reference	Console
Manage credentials	• Modify credential information in the credential vault. See Modifying credentials. • Delete credentials from the credential vault. See Deleting credentials. • Check in credentials for other users. See Checking in credentials. • Connect credentials to an identity provider. See Connecting a credential to an identity provider. • Disconnect credentials from the identity provider. See Disconnecting a credential from an identity provider. • Reset password of the credential. See Resetting credential password.	Privileged Identity Manager Service Center

Privileged administrator (for applications)

The Privileged administrator (for applications) reviews and manages the list of authorized applications that are using privileged credentials. These users are members of the Privileged administrator group.

Table 7. Privileged administrator tasks (for applications)

Tasks	Subtasks and reference	Console
Change passwords that are used by applications, without having to change stored passwords in individual applications.	See the following topics: • Enabling password synchronization • Changing user passwords	Administrative console
Change passwords that are used by applications automatically according to the frequency required by the organization.	See Enabling password expiration	Administrative console
Revoke access to applications that no longer require access to a resource.	See Managing the list of authorized applications	Privileged Identity Manager Service Center

Privileged user

The Privileged user uses the Self-service console for the following tasks

Table 8. Privileged user tasks

Tasks	Subtasks and reference	Console
Change password	See Changing user passwords.	Self-service console
Reset password	See Resetting user passwords.	Self-service console
Manually check out and check in shared credentials	"Manual checkout and checkin of shared credentials" on page 23	Self-service console
Request role for access to some shared ID	See Requesting access for users.	Self-service console

User manager

The user manager uses the IBM Security Privileged Identity Manager Self-service console for the following task.

Table 9. Privileged User Manager task

Tasks	Subtasks and reference	Console
Approve and review requests	See Approval of user requests.	Self-service console

Privileged Session Recorder console

The Privileged Session Recorder console enables you to search and review recordings to verify compliance to audit requirements.

Login URL

`https://`*`ip-address`*`/recorder/ui`

Default login user name

`pim manager`

Default login password

`secret`

Users

- Security administrator or auditor

Table 10. Security administrator or auditor tasks

Tasks	Subtasks and reference
Search recordings	Searching for recordings
Replay recordings	Playing back recordings

Single Sign-On administration console

The Single Sign-On administration console or AccessAdmin enables you to configure and manage the policies and settings that are related to the single sign-on and Privileged Session Recording functions of the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent.

Login URL

`https://`*`ip-address`*`/admin`

Default login user name

`pim manager`

Default login password

`secret`

User

- Privileged Identity Manager administrator

Table 11. Privileged Identity Manager administrator tasks

Tasks	**Subtasks and reference**
Enable the session recording feature in the virtual appliance and configure the session recording policies	To enable the session recording for AccessAgent, modify the `pid_recorder_enabled` policy in AccessAdmin. See IBM Security Privileged Identity Manager configuration policies
Configure the reauthentication prompt	Configuring the reauthentication prompt
Create a user policy template only for privileged identity management users	Creating a user policy template only for privileged identity management users

Chapter 4. Features overview

IBM Security Privileged Identity Manager provides shared access management, session recorder, application identity management, single sign-on, and report generation features.

Shared access

IBM Security Privileged Identity Manager supports automatic and manual checkout and checkin of shared credentials.

A shared credential enables multiple users to access the same resources. A credential consists of an account ID and password. Depending on how the credential was added to the credential vault, multiple users might access the credentials. If check-out is enabled, only one user can access the credential at a particular time.

Automatic checkout and checkin of shared credentials

Privileged users can automatically check-out and check-in shared access credentials from the IBM Security Privileged Identity Manager Server for convenience.

The IBM Security Access Manager for Enterprise Single Sign-On AccessAgent client automates the check-out and check-in of shared access credentials. AccessAgent automatically checks in shared access credentials when you log out, exit, or close the resource.

AccessProfiles automate the check-out and check-in process.

Manual checkout and checkin of shared credentials

Some IBM Security Privileged Identity Manager deployments do not require automated access to shared credentials. Users who have sufficient privileges, such as membership in the Privileged users group, can manually access shared credentials.

Privileged users can manually check out shared credentials for workflows and applications that are not supported by the bundled Privileged Identity Management AccessProfiles.

For supported client applications, AccessAgent can be configured to prompt privileged users to use shared credential. AccessAgent checks out and injects credentials automatically to the logon prompt.

Note: Privileged Session Recording is not effective when manual checkout is allowed.

Privileged users can use the Self-service console for the manual checkout and checkin. For initial access to theSelf-service console, see Initial login and password information.

Session recording

You can record privileged identity sessions for auditing, security forensics, and compliance.

Recordings are stored in a centralized database. To find recorded sessions or play back recordings, you can use the web-based Privileged Session Recorder console.

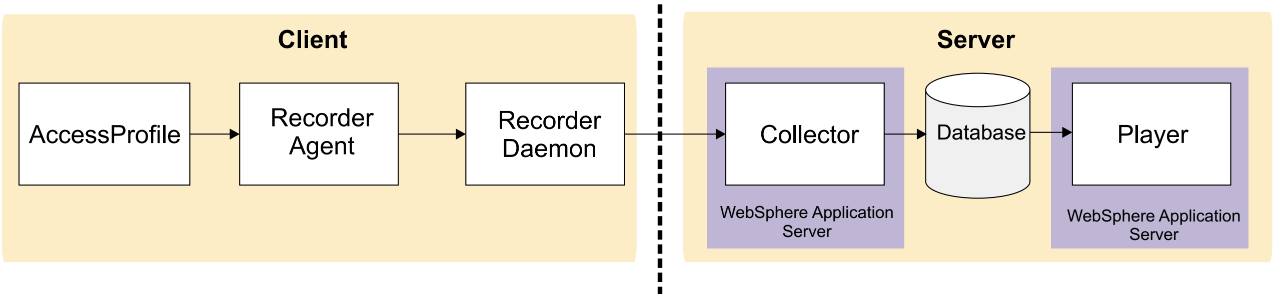

Figure 3. Session recording components.

When supported Windows applications are started, the IBM Privileged Session Recorder is started so that user activity is captured.

Recordings are either snapshots of the screen or a text-based representation of the console. Recordings include metadata that can be searched.

The software includes some AccessProfiles that have session recording enabled. The following applications are supported:

- PuTTY or IBM Personal Communications for terminal sessions

  Captured and played back as text-based recordings.
- Microsoft Remote Desktop connection for remote desktop sessions.

  Captured as snapshots.
- VMware vSphere for sessions on virtualized infrastructure.

  Captured as snapshots.

To add session recording support for other applications, you can design your own custom AccessProfiles.

Screen-based recordings

Recordings are captured as a sequence of snapshots of the screen. Screen-based recordings typically apply to desktop-based or graphics-driven applications such as VMware vSphere and Microsoft Remote Desktop.

For a list of the attributes, see Searching for recordings.

Text-based recordings

Text-based recordings apply to terminal based applications such as PuTTY or IBM Personal Communications. Text that displays in the terminal window are captured. For text-based recordings with PuTTY to a UNIX endpoint, commands that are entered are also captured for search and retrieval.

Differences exist between text-based recordings with PuTTY and IBM Personal Communications:

- For recordings triggered by PuTTY to UNIX endpoints, commands that you enter during the session are captured. When the recording is played back, the identified commands are displayed in a command list sidebar. Captured commands are searchable through global and advanced search.
- For recordings triggered by IBM Personal Communications to mainframe applications, commands are not captured.

Application identity management

Application administrators can use IBM Security Privileged Identity Manager for Applications (App ID) to remove hardcoded and unsafely stored credentials from applications and scripts. App ID can also be used to manage the credential entitlements for each application, track the use of each credential, and automate periodic password change.

App ID is a feature that needs to be activated separately. The App ID toolkit allows the management of credentials that are used in the following applications:

Java Enterprise Edition Applications accessing databases
Credentials that are used for establishing a JDBC connection in supported Java EE application servers can be managed by installing the App ID Java EE data source. No code change is required for the applications that are running on the application server.

Java Applications
Credentials that are used by a Java application can be managed by modifying the applications to get the credentials by using the App ID Java SDK.

Scripts
Credentials that are stored in a script can be managed by modifying the script to get the credentials by running the Java-based App ID Command-Line tool.

Single sign-on

IBM Security Privileged Identity Manager integrates with IBM Security Access Manager for Enterprise Single Sign-On to automate check-out and check-in of shared access credentials.

IBM Security Access Manager for Enterprise Single Sign-On is composed of the following components.

AccessAgent
A client software that is configured to connect to the IMS Server on the IBM Security Privileged Identity Manager Virtual Appliance. AccessAgent is deployed on the Windows desktop (Client AccessAgent). You can also deploy it on the Citrix or Terminal Server (Server AccessAgent).

IMS Server
Stores and manages user credentials, AccessProfiles, identity Wallets, and policies.

AccessStudio
An application that is used by Administrators for creating and maintaining AccessProfiles. AccessProfiles automates sign-on or sign-off and custom workflows.

AccessAdmin
AccessAdmin is the Web-based management console that Administrators use for:

- Searching and administering users
- Managing user, machine, system, and application policies
- Searching and viewing logs

Cognos Reports

The IBM Security Privileged Identity Manager solution supports the IBM Cognos reporting framework for report generation.

The reporting package includes the following reports:

Shared Access Entitlements by Owner Report
This report shows the credentials and credential pools that are owned by the selected owner.

Shared Access Entitlements by Role Report
This report shows the information about the credentials and credential pools that are entitled by the selected role.

Shared Access Entitlement Definition Report
This report shows the configuration information of Privileged IDs and the Shared Access Policies that are associated with these Privileged IDs.

Shared Access History Report
This report shows the history of actions that are performed on the shared credentials.

Single Sign-On Privileged ID Audit Report
This report provides a log history of check-out and check-in actions that are performed for each Privileged ID on the managed resource. This report also includes a subreport that is called User Activity Audit Report. With this subreport, you can play back the user session recording or view the terminal commands that the user executed on the managed resource.

Privileged Session Recorder Report
This report shows the history of activities that occurred in the Privileged Session Recorder console sorted by User Name. You can use this report to track and monitor the actions of the selected user in the Privileged Session Recorder console.

Integration with IBM Security Identity Manager

IBM Security Privileged Identity Manager Version 2.0 is a separate product offering from IBM Security Identity Manager but these products can still be integrated when necessary. IBM Security Privileged Identity Manager account and role entitlements are managed and reported on at IBM Security Identity Manager. Shared credential entitlements are managed and reported at IBM Security Privileged Identity Manager.

New with integration

Existing IBM Security Identity Manager customers can deploy IBM Security Privileged Identity Manager without disrupting or changing their IBM Security Identity Manager deployment.

There is no need to upgrade IBM Security Identity Manager to support current IBM Security Privileged Identity Manager features. As such, the cost of migrating configuration, data, processes, and extensions; and the risk of destabilizing user provisioning services are avoided.

The following functions are decoupled from IBM Security Privileged Identity Manager and are available only in IBM Security Identity Manager:

- User Account Provisioning and Lifecycle Management

  IBM Security Privileged Identity Manager does not provision privileged credentials on target systems. The privileged accounts must already exist on the target system before the credentials are onboarded into the IBM Security Privileged Identity Manager credential vault.
- Service Reconciliation
- Access Request and Re-certification workflows

  IBM Security Privileged Identity Manager Role Memberships are reconciled to IBM Security Identity Manager and can be re-certified with IBM Security Identity Manager processes.

IBM Security Privileged Identity Manager contains a simplified user interface for setting up single or multiple-stage approval workflows (by Role Owner, User Manager, ISPIM Admin) for role requests.

Note: Privileged accounts can be provisioned by IBM Security Identity Manager but the privileged accounts must be onboarded separately onto IBM Security Privileged Identity Manager.

IBM Security Privileged Identity Manager shared access entitlements are managed only in IBM Security Privileged Identity Manager by respective privileged admins, and is not visible to IBM Security Identity Manager.

Existing customers:

- Use IBM Security Identity Manager for identity management and governance of all users in the organization, including privileged users. For users who must use IBM Security Privileged Identity Manager, IBM Security Identity Manager is used to provision ISPIM accounts for these users and to manage the role and group memberships of these accounts.
- Use IBM Security Privileged Identity Manager for managing and tracking the use of shared access credentials, automated password reset, and for recording sessions visited with such credentials.
- IBM Security Privileged Identity Manager shared access entitlements are managed only in IBM Security Privileged Identity Manager by respective privileged admins, and is not visible to IBM Security Identity Manager. There is no assumption or requirement that all the shared credentials managed by IBM Security Privileged Identity Manager is visible to IBM Security Identity Manager.

For a scenario, see Integration with IBM Security Identity Manager.

The IBM Security Privileged Identity Manager Adapter must be deployed on IBM Security Identity Manager.

Deploy the adapter so that IBM Security Identity Manager can be used to manage IBM Security Privileged Identity Manager users, roles, groups, and administrative domains.

The IBM Security Privileged Identity Manager Adapter is supported on IBM Security Identity Manager 5.1, 6.0, and 7.0.

IBM Security Privileged Identity Manager Adapter

The IBM Security Privileged Identity Manager Adapter enables communication between the IBM Security Identity Manager and the IBM Security Privileged Identity Manager. The IBM Security Privileged Identity Manager Adapter automates the management of user accounts and different service groups such as ISPIM roles, ISPIM system groups, and ISPIM administrative domains.

The IBM Security Privileged Identity Manager Adapter automates the following tasks:

User account management on the IBM Security Privileged Identity Manager server

- Adding user accounts
- Changing user account passwords
- Modifying user account attributes
- Suspending and restoring user accounts
- Retrieving user accounts for the first time
- Deleting user accounts
- Reconciliation of modified user accounts

Service group management on the IBM Security Privileged Identity Manager server

- Adding groups
- Modifying group attributes, including adding and removing members
- Deleting groups
- Adding roles
- Modifying role attributes, including adding and removing members
- Deleting roles
- Adding and deleting administrative domains
- Modifying administrative domain attributes, including adding and removing administrators
- Reconciliation of other support data from the IBM Security Privileged Identity Manager server to IBM Security Identity Manager

For more information, see the IBM Security Privileged Identity Manager Adapter documentation in the IBM Security Identity Manager documentation site.

Feature comparison

Table 12. Comparing features between a standalone IBM Security Privileged Identity Manager and one that is integrated with IBM Security Identity Manager

Feature	Standalone	With IBM Security Identity Manager
Shared credential management with secure storage in a vault with access control with role-based policies	Supported.	With ability to use IBM Security Identity Manager to provision and manage ISPIM accounts and role and group memberships
Self-service check-in and check-out from web console	Supported.	Same as standalone.
Automated check-in and check-out with single sign-on with AccessAgent	Supported.	Same as standalone.
Session recording with AccessAgent	Supported.	Same as standalone.
Application identity management	New. Supported.	Same as standalone.
Cognos reports	Supported.	Same as standalone.
Account provisioning and lifecycle management of accounts on managed systems	Not supported. Lifecycle of shared credentials are not tied to individual employees.	Same as standalone. **Note:** You can configure IBM Security Identity Manager to provision shared credentials into target systems if required but the privileged credentials must be separately on-boarded into IBM Security Privileged Identity Manager
Service reconciliation	Full service reconciliation is not supported.	Same as standalone.
Access recertification	Not supported.	With ability to use IBM Security Identity Manager for managing and certifying users ISPIM account and ISPIM role memberships.
Adapter support	The virtual appliance includes the SoftLayer adapter. Supports adapters that include the self-change password mode.	Same as standalone.
2-factor authentication	Log on with smartcards or fingerprint biometrics into the single sign-on AccessAgent is not supported. Deployments of the IBM Security Privileged Identity Manager with IBM Security Access Manager for Web WebSEAL as a front-end is not supported. Step up-authentication by using OTP before automatic check-out is supported with the customization of single sign-on AccessProfiles.	Same as standalone.

Task comparison

Table 13. User experience differences

Tasks	Standalone	With IBM Security Identity Manager
On-boarding privileged administrators	You can use the IBM Security Privileged Identity Manager administrative console, HR feed, or APIs	You can use IBM Security Identity Manager to on-board users into IBM Security Privileged Identity Manager
On-boarding and managing unconnected credentials	You can use the IBM Security Privileged Identity Manager Service Center	Same as standalone.
On-boarding and managing connected credentials	You can use the IBM Security Privileged Identity Manager Service Center	Same as standalone.
Managing groups, roles, and memberships for groups and roles	You can use the IBM Security Privileged Identity Manager administrative console	Users, groups, and roles in IBM Security Privileged Identity Manager can be reconciled and managed on IBM Security Identity Manager
Role request and approval workflows	Simplified user interface for single or multiple-stage approval workflows (by Role Owner, User Manager, ISPIM Admin) for role requests.	Groups and roles in IBM Security Privileged Identity Manager are reconciled and can be managed in IBM Security Identity Manager You can set up request approval workflows on these roles and groups with IBM Security Identity Manager, where requests are accomplished through the IBM Security Identity Manager Service Center.
Managing shared access policies	You can use the IBM Security Privileged Identity Manager administrative console	Same as standalone.
Managing credential settings. For example: reset password on check-in	You can use the IBM Security Privileged Identity Manager Service Center.	Same as standalone.
Scheduled password reset	IBM Security Privileged Identity Manager administrator console	Same as standalone.

Integration with SoftLayer

SoftLayer AccessProfile

The SoftLayer AccessProfile provides single sign-on functionality to log on to SoftLayer.

The SoftLayer AccessProfile supports the following functions:

- Check out the credentials from IBM Security Privileged Identity Manager.
- Inject the credentials after the web browser is closed.
- Check in the credentials to IBM Security Privileged Identity Manager.

You must consider the following issues and limitations before using the SoftLayer AccessProfile:

- It can only be used in IBM Security Access Manager for Enterprise Single Sign-On supported web browsers. For example: Microsoft Internet Explorer 9, Microsoft Internet Explorer 10, or Mozilla Firefox 31.
- The profile is not checked in if a tab is closed. Close the web browser to check in the profile.
- The user is not prompted to check out the credential after restarting the web browser due to the cache that is maintained by the web browser. The user is logged on to SoftLayer automatically.

SoftLayer Adapter

The SoftLayer Adapter enables connectivity between the IBM Security Privileged Identity Manager and SoftLayer.

This adapter automates several administrative tasks on the SoftLayer server. You can use the adapter to automate the following tasks:

- Create, modify, suspend, restore, change password, and delete a user.
- Reconcile user and user attributes.

The SoftLayer Adapter is bundled with the IBM Security Privileged Identity Manager Virtual Appliance. As such, you only need to:

1. Create an identity provider for the SoftLayer profile (**SoftLayerProfile**) . See Adding identity providers.
   a. Specify a name that defines the adapter service on the server. For example, SoftLayer.

      Note: Do not use forward (/) or backward slashes (\) in the service name.
   b. Specify the URL which the adapter can use to communicate with SoftLayer. For the current SoftLayer release, use **https://api.softlayer.com**.
2. Create a credential and connect it to the SoftLayer identity provider that you created. See Adding credentials through Manage Credentials and Connecting a credential to an identity provider.

   Note: In the **Resource** field, specify `control.softlayer.com`.
3. Create a shared access policy and add the credential that you created to the entitlement. See Creating shared access policies.
4. (Optional) If the credential check-in fails because the default SoftLayer password policy is not strong enough, modify the password strength rule in **Manage Password Policies**.

Chapter 5. Language support overview

The IBM Security Privileged Identity Manager Virtual Appliance is translated in several languages.

See the following table for the supported languages:

Table 14. Supported languages

Language	Supported
Arabic	No
Chinese (Simplified)	Yes
Chinese (Traditional)	Yes
Czech	No
Danish	No
Dutch	No
English (United States)	Yes
Finnish	No
French (Standard)	Yes
German	Yes
Greek	No
Hebrew	No
Hungarian	No
Italian	Yes
Japanese	Yes
Korean	Yes
Polish	No
Portuguese (Brazilian)	Yes
Russian	Yes
Spanish	Yes

Note: To change the language for IBM Security Privileged Identity Manager virtual appliance console, select the required language from the **Language** drop-down menu at the top right corner of the console. For languages with right-to-left text orientation, for example, Hebrew or Arabic, the **Language** drop-down menu is on the upper left corner of the console.

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.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 might 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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. 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 IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a Service".

Printed in USA