IBM United States Software Announcement
212-327, dated October 2, 2012

IBM Security Privileged Identity Manager V1.0 and IBM Security Identity Manager V6.0 help the enterprise strengthen security, enhance its governance posture, and improve user productivity

Table of contents

At a glance

IBM® Security Privileged Identity Manager V1.0 helps thwart insider threats by tracking the use of privileged user credentials.

IBM Security Identity Manager helps you:

- Simplify and reduce cost of administration
  - Password management supports user self-service, which can help vastly reduce help desk costs.
  - Automated user lifecycle management provides entitlements for users much more quickly over manual provisioning, and can reduce costs of updating user entitlements upon job change.
  - Bulk user access recertification allows managers to quickly make access decisions by certifying roles, accounts, and groups all at once.
  - Role lifecycle management can streamline the role structure approval process and can reduce errors when validating access with the business.
- Enhance security and compliance through implementation of strong password policies and establishment of preventative separation of duties policies that manage access conflicts

```
For ordering, contact Your IBM representative or an IBM Business Partner.
For more information contact the Americas Call Centers at
800-IBM-CALL (426-2255).

Reference: YE001
```

Overview

IBM Security Privileged Identity Manager V1.0

This new solution includes IBM Security Identity Manager V6.0 and IBM Security Access Manager for Enterprise Single Sign-On V8.2 capabilities for licensed privileged users. You get privileged user entitlement provisioning, strong password management policies, and support for all IBM Security Identity Manager adapter endpoints. IBM Security Privileged Identity Manager helps thwart insider threat

by tracking the use of user credentials having elevated access privileges. It also provides:

- An encrypted credential vault providing controlled check-out and check-in of shared IDs for entitled users.
- Automated login with available strong authentication that delivers an additional level of assurance while hiding the current password from the end user.
- User activity logging that contains an audit trail on use of privileged credentials.
- Password update capability, after use, upon check-in, to help ensure it is not written down and reused outside the governance structure.

IBM Security Identity Manager V6.0 (formerly known as IBM Tivoli® Identity Manager) is an automated and policy-based solution that manages user access across IT environments, helping to drive effective identity management and governance across the enterprise. Through the use of roles, accounts, and access permissions, it helps automate the creation, modification, and termination of user privileges throughout the entire user lifecycle. IBM Security Identity Manager can help increase user efficiency, reduce IT administration costs, enforce security, and manage compliance.

The new key features of IBM Security Identity Manager V6.0 help improve usability and performance. They include role management enhancements, improved self-monitoring and troubleshooting, performance enhancements, an IBM Cognos® data model for custom reporting (available in the Integrated Service Management Library), and a new mobile application for manager request approvals.

Key prerequisites

For details, refer to the Hardware requirements and the Software requirements sections.

Planned availability date

October 19, 2012: Electronic availability

November 23, 2012: Media availability

Description

IBM Security Privileged Identity Manager V1.0

IBM Security Privileged Identity Manager V1.0 is an identity and access management solution for privileged users. These users include system administrators, database administrators, and sensitive application administrators as well as executives with elevated access privileges to sensitive applications and data.

Administrative users typically share privileged login credentials to target endpoints. For example, multiple IT employees might actually use the same login credential Administrator. This can be problematic when an inadvertent mistake occurs and the actual employee needs to be contacted to correct the issue. It can be even more problematic when such an employee is terminated but still has potentially damaging access to key resources. Furthermore, because there are so many of these identities, employees often write down the login credentials and display the list openly at their desks. This provides nonentitled employees access to these sensitive credentials. As the number of privileged accounts grows, the security risk and associated administrative burden of supporting these accounts grows as well.

Shared and privileged credentials need to be tracked for individual accountability to help ensure only those who are approved for access are able to get it.

IBM Security Privileged Identity Manager addresses these issues by forcing users to check these credentials out of a credential vault and tracking their use. The logged out credentials can be set to expire and a warning note sent to the overdue user to return the credentials. The password for these credentials can be configured to change after every check in. Sharing a set of credentials between privileged users can cut down on the overall number of privileged accounts needed, helping reduce the associated security risk and management burden.

IBM Security Identity Manager

IBM Security Identity Manager is an automated and policy-based solution that manages user access across IT environments. Through the use of roles, accounts, and access permissions, it helps automate the creation, modification, and termination of user privileges throughout the entire user lifecycle.

IBM Security Identity Manager can help increase user efficiency, reduce IT administration costs, enforce security, and manage compliance. It does this with centralized user self-service, delegated administration, automated approvals processing, periodic revalidation of user access rights, documentation of controls, role mining, and role lifecycle management.

The extensive role management functionality in Security Identity Manager helps you bridge the gap between how business users view their IT resources and the actual IT implementation of user access rights. This helps you to simplify and reduce the cost of administering user access rights, offers you a set of additional controls to manage internal security, and enables you to scale existing user provisioning deployments across the enterprise. Separation of duty support helps establish preventative policies that can manage business conflicts by excluding user membership to multiple roles while allowing for policy exceptions.

IBM Security Identity Manager helps provide automated audit readiness with access rights recertification, additional prebuilt reports, a custom report builder, direct auditor access to reports, and mapping of low-level IT entitlements into business-friendly descriptions of what a user can actually do with access.

IBM Security Identity Manager also provides:

- A highly customizable self-service user interface that can be easily modified to match intranet and extranet portal look and feel.
- A mapping of low-level IT entitlements into business-friendly descriptions of what users can actually do with their access.
- Password self-service reset to help improve user productivity and reduce help desk costs.
- Access request management that provides a quick-start option to streamline user provisioning and offers users the opportunity to manage their role membership, access rights, passwords, personal information, and approval tasks.
- A dynamic policy management engine that automates user provisioning and aids in compliance efforts.
- Access rights reconciliation, recertification, and reporting to address audit requirements.
- Broad support for system adapters to accelerate installation of new applications.
- Scalable, fault tolerant, and internalized architecture.
- A powerful workflow and policy engine that can be configured in either simple or advanced mode.
- Recertification of user entitlements to help improve governance and audit readiness.
- A flexible and powerful role modeling and mining platform with the IBM Security Role and Policy Modeler component.
- Role and Policy Modeler supports entitlement data gathering, analysis of entitlement patterns, an IBM Research based Role Mining algorithm, visualization techniques, and scoring metrics that facilitate interaction with business users to produce an effective role and access structure. The proposed role structure

can be managed throughout its lifecycle with a workflow for business process automation.

Key new features in IBM Security Identity Manager V6.0

- Role schema customization, custom form support, and improved support for use of role assignment attributes enhance role management flexibility.
- Web Services API supports integration of IBM Security Identity Manager with service-oriented architecture (SOA) applications. The Adapter Toolkit also provides improved Web Services support.
- IBM WebSphere® Application Server authentication support allows you to use your own WebSphere-supported authentication registries (for example, corporate LDAP) as the IBM Security Identity Manager user repository and not be restricted to using the IBM Security Identity Manager provided registry.
- IBM WebSphere Application Server single sign-on can improve integration between IBM Security Identity Manager and the Role and Policy Modeler, and can also support single sign-on independent from IBM Tivoli Access Manager for e-business use.
- Extra granularity for service setup allows you to create specific per service instance account forms to aid in customizing the solution.
- Enhanced health check on adapters provides more information on the service form test such as the adapter version and status of the resource for enhanced troubleshooting.
- Enhanced performance monitoring aids detection of configuration and connectivity issues using the WebSphere Performance Monitoring Infrastructure (PMI).
- Expanded reporting capabilities under Tivoli Common Reporting - An IBM Cognos reporting data model for custom reporting is available in the Integrated Service Management Library.
- Enhanced self-monitoring via use of IBM Tivoli Monitoring agent available on the IBM Integrated Service Management Library.
- IBM WebSphere Application Server vertical clustering support allows you to tap unused capacity on the same physical box for WebSphere clusters for quicker, less costly capacity expansion.
- Service group tagging for entitlements provides the ability to assign entitlements to groups of services (for companies with large numbers of similar services), which supports more consistent policy enforcement across like endpoints.
- For more timely support, DataSynch performance enhancements provide quicker synchronization between the LDAP user repository and the reporting database.
- Reconciliation performance enhancements support improved usability of the solution.
- Audit log size management enhancements provide reduced footprint of the audit log for more efficient resource utilization.

Capabilities no longer supported in IBM Security Identity Manager V6.0

The Free EcmaScript Interpreter (FESI) programming interface, part of the now withdrawn IBM Tivoli Identity Manager V4.6, was deprecated in the last IBM Tivoli Identity Manager release. It will no longer be supported in IBM Security Identity Manager V6.0. It is replaced with the Bean Scripting Framework (BSF) component of the IBM JavaScript Engine that ships with IBM Security Identity Manager V6.0.

IBM Security Identity Manager V6.0 adapters

To provision and maintain user accounts in systems, IBM Security Identity Manager relies on its adapters. The adapters use APIs to remotely manage user accounts in systems such as operating systems, relational databases, public key infrastructure (PKI) registration authorities, enterprise applications, and other security systems.

Core (infrastructure) adapters are available for IBM Security Identity Manager server, at no additional charge, to help improve your time to value and decrease deployment times. These adapters work with some of the most common IT infrastructure products such as:

- IBM AIX®
- IBM Tivoli Access Manager for e-business
- IBM Tivoli Service Request Manager®
- IBM Security Access Manager for Enterprise Single Sign-On
- IBM DB2 Universal Database™
- IBM Lotus Notes®
- Blackberry Enterprise Server
- Cisco Unified Communication Manager
- Command Line Interface
- HP-UX
- LDAP Directories
- Microsoft™ Windows™ Active Directory
- Microsoft Windows Local Account
- Microsoft SQL Server
- Novell eDirectory (NDS)
- Novell Groupwise
- Oracle Database
- Red Hat Enterprise Linux™
- RSA ACE Server
- RSA Authentication Manager
- Sun Solaris
- SUSE Linux Enterprise Server
- Sybase Adaptive Server Enterprise

Access the following website for the latest supported version and release of the above products

http://www-01.ibm.com/support/docview.wss?uid=swg21599053

These adapters, and their associated documentation, can be downloaded from the Passport Advantage® website at

http://www.ibm.com/software/support/pa.html

IBM Security Identity Manager also has two other groups of adapters that you can purchase to provision and maintain user accounts on additional applications and systems.

The first group, IBM Security Identity Manager Application Edition, contains adapters that interface with common enterprise resource planning applications and other commercial off-the-shelf applications.

The second group, IBM Security Identity Manager Host Edition, provisions and maintains user accounts on systems such as IBM RACF® and IBM System i® . Due to the constantly changing nature of these systems, adapters are updated frequently and are available through download only. For a current list of available adapters access

http://www-01.ibm.com/support/docview.wss?uid=swg21599053

IBM reserves the right to add or remove adapters from a group, move adapters between groups, and add or remove adapter groups at any time without prior notice.

The following adapters are not supported on IBM Security Identity Manager V6.0:

- SAP HR Linking and Perm PW (now offered as sample code)

- UPA (adapter discontinued)
- VIOS (adapter discontinued)

The list of specifically supported endpoint versions is subject to change. IBM Security Identity Manager adapter support for its managed endpoints depends upon the support of that endpoint by its vendor. Generally, support for a specific adapter endpoint version is discontinued on all versions of IBM Security Identity Manager, current and prior, 90 days after the endpoint vendor ends their mainstream support.

For the most current list of endpoint support, refer to the release notes at

http://www-01.ibm.com/support/docview.wss?uid=swg21599053

Accessibility by people with disabilities

A US Section 508 Voluntary Product Accessibility Template (VPAT) containing details on accessibility compliance can be requested at

http://www.ibm.com/able/product_accessibility/index.html

Section 508 of the US Rehabilitation Act

IBM Security Identity Manager V6.0 is capable as of November 23, 2012, when used in accordance with IBM's associated documentation, of satisfying the applicable requirements of Section 508 of the Rehabilitation Act, provided that any assistive technology used with the product properly interoperates with it. A US Section 508 Voluntary Product Accessibility Template (VPAT) can be requested on the following Web site

http://www.ibm.com/able/product_accessibility/index.html

Product positioning

Every organization that deploys an IT infrastructure includes a set of privileged users with elevated access rights. These users are typically granted special rights to manage business critical resources, such as operating systems, databases, ERP systems, and many other business systems and platforms. The privileged identities are usually shared among these users and can cause accountability, compliance issues, and emerging as a potential source for insider breaches. The trends toward data center consolidation, outsourcing, cloud computing, and virtualized infrastructures are increasing the risk of insider threats to an even greater number of privileged users. IBM Security Privileged Identity Manager helps thwart insider threats by securing and tracking the use of privileged user credentials.

IBM Security Identity Manager helps automate the processes of creating provisioning and de-provisioning user's access rights. It can help increase user efficiency, reduce IT administration costs, and address compliance needs. This is accomplished with role management, centralized user account maintenance (including self-service interfaces), delegated administration, automated approvals processing, documentation of controls, standard reports, role mining, and role lifecycle management.

These solutions are part of the IBM Security Identity and Access Management portfolio providing complete user lifecycle management, from planning through user administration to real time access enforcement via web, enterprise, and federated single sign-on, and through to user activity monitoring to feed back into the entire closed loop process.

Program number

Program number	VRM	Program name

```
5725-H30     1.0.0    IBM Security Privileged Identity Manager
5724-C34     6.0.0    IBM Security Identity Manager
```

Education support

IBM training provides education to support many IBM offerings. Descriptions of courses for IT professionals and managers are on the IBM training website

http://www.ibm.com/services/learning/

Call IBM training at 800-IBM-TEACH (426-8322) for catalogs, schedules, and enrollments.

Offering Information

Product information is available via the Offering Information website

http://www.ibm.com/common/ssi

Also, visit the Passport Advantage website

http://www.ibm.com/software/passportadvantage

Publications

IBM Security Privileged Identity Manager V1.0

English publications will be available at general availability. National language publications will be available 30 days after general availability.

The Quick Start Guide publication will be delivered on a separate publications CD-ROM with the basic machine readable material. It can also be downloaded from the IBM Security Privileged Identity Manager Information Center.

- IBM Security Privileged Identity Manager Quick Start Guide (GI13-2307-00) (part number CF3KIML)
- IBM Security Privileged Identity Manager Deployment Overview Guide (SC27-4382-00)

Soft copy publications and release notes are available at

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.ispim.doc_10/i c-homepage.html

IBM Security Identity Manager V6.0

English publications will be available at general availability. National language publications will be available 30 days after general availability.

The Quick Start Guide publication will be delivered on a separate publications CD-ROM with the basic machine readable material. It can also be downloaded from IBM Security Identity Manager Information Center

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/i c-homepage.htm

English publications:

- IBM Security Identity Manager Quick Start Guide ((CF3L2ML)
- IBM Security Identity Manager Product Overview Guide (GC14-7692-00)
- IBM Security Identity Manager Scenarios Guide (SC14-7693-00)

- IBM Security Identity Manager Planning Guide (GC14-7694-00)
- IBM Security Identity Manager Installation Guide (GC14-7695-00)
- IBM Security Identity Manager Configuration Guide (SC14-7696-00)
- IBM Security Identity Manager Security Guide (SC14-7699-00)
- IBM Security Identity Manager Administration Guide (SC14-7701-00)
- IBM Security Identity Manager Troubleshooting Guide (GC14-7702-00)
- IBM Security Identity Manager Error Message Reference (GC14-7393-00)
- IBM Security Identity Manager Reference Guide (SC14-7394-00)
- IBM Security Identity Manager Database and Schema Reference Guide (SC14-7395-00)
- IBM Security Identity Manager Glossary (SC14-7397-00)

For information on IBM Security Identity Manager Adapters publications, refer to the Description section of this announcement.

IBM Security Access Manager for Enterprise Single Sign-On V8.2

The IBM Security Access Manager for Enterprise Single Sign-On V8.2 Information Center includes the following publications.

Publication updated:

- IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide (SC27-4444-00)

There are no changes to the following publications:

- IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide (part number CF38DML)
- IBM Security Access Manager for Enterprise Single Sign-On Installation Guide (GI11-9309-01)
- IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide (C23-9692-01)
- IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide (SC23-9952-03)
- IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide (SC23-9951-03)
- IBM Security Access Manager for Enterprise Single Sign-On User Guide (SC23-9950-03)
- IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide (SC23-9953-03)
- IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide (GC23-9693-01)
- IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide (SC23-9956-03)
- IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide (SC23-9694-01)
- IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide (SC23-9957-03)
- IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide (SC14-7646-00)
- IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide (SC23-9954-03)
- IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide (SC14-7626-00)
- IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide (SC14-7657-00)
- IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide (GC14-7624-00)

Soft copy publications and release notes are available at

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/i c-homepage.html

The IBM Publications Center

http://www.ibm.com/shop/publications/order

The Publications Center is a worldwide central repository for IBM product publications and marketing material with a catalog of 70,000 items. Extensive search facilities are provided. Payment options for orders are via credit card (in the U.S.) or customer number for 20 countries. A large number of publications are available online in various file formats, and they can all be downloaded by all countries, free of charge.

Technical information

Specified operating environment

Hardware requirements

IBM Security Privileged Identity Manager V1.0 hardware requirements are based on the requirements of the underlying IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On products.

IBM Security Identity Manager V6.0 requires a minimum of:

- 4 GB RAM
- 30 GB disk storage

IBM Security Access Manager for Enterprise Single Sign-On V8.2 component minimum requirements

IBM Security Access Manager for Enterprise Single Sign-On V8.2 AccessAgent requirements:

- PC with an x86 or x64 processor, at least 600 MHz processor clock speed
- Minimum 512 MB physical memory for Windows XP
- Minimum 1 GB physical memory for Windows Vista
- Minimum 1 GB physical memory for Windows 7
- Disk space: At least 200 MB free hard disk space

IBM Security Access Manager for Enterprise Single Sign-On V8.2 AccessStudio requirements:

- PC with an x86 or x64 processor, at least 600 MHz processor clock speed
- Minimum 512 MB physical memory for Windows XP
- Minimum 1 GB physical memory for Windows Vista
- Minimum 1 GB physical memory for Windows 7
- Disk space: At least 300 MB free hard disk space

IBM Security Access Manager for Enterprise Single Sign-On V8.2 server requirements:

- PC with an x86 or x64 bit processor, at least 2 GHz processor clock speed
- Minimum 3 GB physical memory (database not co-located)
- At least 8 GB free hard disk space (database not co-located)

Software requirements

IBM Security Privileged Identity Manager V1.0 software requirements are based on the requirements of the underlying IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On products.

IBM Security Identity Manager V6.0 requires one of the following operating systems:

- AIX V6.1, V7.1 on System p®
- Oracle Solaris 10 (SPARC)
- Windows Server 2008 with SP2 (x86-32, x86-64), 2008 R2 Standard Edition and Enterprise Edition (x86-64)
- Red Hat Linux Enterprise 5, 6 for Intel™ (x86-32, x86-64), IBM System p and IBM System z®
- SUSE Linux Enterprise Server 10.0 and 11.0 for Intel (x86-32, x86-64), System p , and System z

Virtualization support:

- VMWare ESX V4.1 and V5
- AIX WPAR and LPAR
- IBM z/VM®
- Solaris Zones and LDOM

IBM Security Identity Manager V6.0 prerequisite releases for optional databases, servers, directory integrators, and browsers:

- Databases:
  - IBM DB2® Enterprise V9.7, Fix Pack 4, or later (for all supported operating systems)
  - IBM DB2 Enterprise V9.5, Fix Pack 3b, or later (for all supported operating systems except 32-bit Linux and Linux on System p)
  - Oracle Database 10g Release 2, or Oracle Database 11g Release 8
  - Microsoft SQL Server 2005 Enterprise Edition
- Directory servers:
  - IBM Tivoli Directory Server V6.2 FP1, and V6.3,
  - Oracle Directory Server Enterprise Edition 6.3.1 and 7.0 (formerly known as Sun Java™ Directory Server)
- Application server:
  - IBM WebSphere Application Server Network Deployment V7.0, fix pack 23 with Interim fixes PM64800 and PM66514

    IBM Security Identity Manager V6.0 and IBM Security Role and Policy Modeler component do not support WebSphere Application Server V8.x.
- Directory integrator:
  - IBM Tivoli Directory Integrator V7.1 and V7.1.1, Fix Pack 1 with Limited Availability Fix 1
- Supported web browsers:
  - Internet Explorer 8.0 and 9.0
  - Firefox 3.6 (AIX only) and 10 (ESR)
- Report Server Support
  - Tivoli Common Reporting V2.1.1, with Interim Fixes 2, 5, and 6 and Tivoli Integrated Portal fix 2.0.0.7

For latest list of software requirements, access

http://www-01.ibm.com/support/docview.wss?uid=swg27020534

IBM Security Role and Policy Modeler component supports a subset of the platforms supported by IBM Security Identity Manager V6.0 server.

IBM Security Role and Policy Modeler component requires one of the following operating systems:

- AIX V6.1 and V7.1
- Windows Server 2008 (R1) Standard Edition and Enterprise Edition (32 and 64 bit)
- Windows Server 2008 (R2) Standard Edition and Enterprise Edition (64 bit)
- Red Hat Linux Enterprise 5 and 6 for Intel (64 bit)
- SUSE Linux Enterprise Server 10 and 11 for Intel (64 bit)

IBM Security Role and Policy Modeler prerequisite databases and browsers

- Databases:
  - IBM DB2 Enterprise 9.7 Fix Pack 4 (for all supported operating systems)
  - Oracle Database 11g R2
- Browsers
  - Internet Explorer 8.0 and 9.0
  - Firefox 3.6 (AIX only) and 10 (ESR)

The following products are included with IBM Security Identity Manager V6.0 for use restricted to Security Identity Manager:

- IBM Tivoli Directory Server V6.3
- IBM Tivoli Directory Integrator V7.1.1
- IBM WebSphere Application Server Network Deployment V7.0
- IBM DB2 Enterprise Server Edition 9.7
- IBM WebSphere Business Process Manager Standard Edition V7.5
- IBM Tivoli Common Reporting V2.1.1 (including both BIRT and Cognos reporting capabilities)

The following operating systems are no longer supported by IBM Security Identity Manager V6.0 server and prerequisite middleware:

- Red Hat Enterprise Server 4
- SUSE Linux Enterprise Server 9.0 for Intel , System p , and System z
- IBM AIX V6.1, or earlier
- Window Server 2003

The following directory servers and browsers are no longer supported by IBM Security Identity Manager V6.0:

- Directory servers:
  - Sun ONE Directory Server 5.2
  - IBM Tivoli Directory Server V6.1
- Browsers:
  - Internet Explorer 7.0, or earlier
  - Firefox 3.5, or earlier
- IBM DB2 Enterprise Server Edition V9.1
- IBM Tivoli Directory Integrator V7.0, or earlier

IBM Security Access Manager for Enterprise Single Sign-On

IBM Security Access Manager for Enterprise Single Sign-On AccessAgent and AccessStudio requirements:

- Microsoft Windows XP Service Pack 3 (x86)
- Microsoft Windows XP Service Pack 2 (x64)
- Microsoft Windows Vista Service Pack 2 (x86 and x64)
- Microsoft Windows 7 Service Pack 1 (x86 and x64)
- Microsoft Windows Server 2003 Service Pack 2 (x86)
- Microsoft Windows Server 2008 Service Pack 2 (x86 and x64)
- Microsoft Windows Server 2008 R2 Service Pack 1 (x64)
- Microsoft Internet Explorer 7.0, 8.0, 9.0
- Mozilla Firefox 3.5, 3.6, 9, 10
- Microsoft .NET Framework 2.0

IBM Security Access Manager for Enterprise Single Sign-On server requirements:

- Microsoft Windows Server 2003 Service Pack 2 (x86)
- Microsoft Windows Server 2008 Service Pack 2 (x86 and x64)
- Microsoft Windows Server 2008 R2 Service Pack 1 (x86 and x64)
- WebSphere Application Server V7.0 (x86 and x64) with latest Fix Pack
- AccessAdmin requires Internet Explorer 7.0, 8.0, 9.0 or Mozilla Firefox 3.5, 3.6

The following are supported:

- Directory:
  - Active Directory 2008 R2 Service Pack 1 (x64)
  - Active Directory 2008 Service Pack 2 (x86 and x64)
  - Active Directory 2003 Service Pack 2 (x86)
  - IBM Tivoli Directory Server V6.3.0 (x86 and x64)
  - IBM Tivoli Directory Server V6.2.0 (x86 and x64)
  - LDAP V3 compatible Directory Servers (x86 and x64)
- Database software requirements:
  - IBM DB2 Enterprise Server Edition 9.7 (x86 and x64) with DB2 JDBC driver 4.0 (bundled with product, but must be installed separately)
  - IBM DB2 Workgroup Server Edition 9.7 (x86 and x64) with DB2 JDBC driver 4.0
  - IBM DB2 Enterprise Server Edition 9.7 (x86 and x64) with DB2 JDBC driver 4.0
  - IBM DB2 Workgroup Server Edition 9.5 (x86 and x64) with DB2 JDBC driver 4.0
  - Oracle 11g R2 (x86 and x64)
  - Oracle 11g R1 (x86 and x64)
  - Oracle 10g R2 (x86 and x64)
  - Microsoft SQL Server 2008 R2 Enterprise and Standard Editions (x86 and x64) - with SQL JDBC driver 3.0
  - Microsoft SQL Server 2008 Enterprise and Standard Editions with Service Pack 2 (x86 and x64) - with SQL JDBC driver 3.0
  - Microsoft SQL Server 2005 Enterprise and Standard Editions with Service Pack 4 (x86 and x64) - with SQL JDBC driver 3.0

Included with the program package for use restricted to IBM Security Access Manager for Enterprise Single Sign-On are:

- IBM DB2 Enterprise Server Edition 9.7

- IBM WebSphere Application Server Network Deployment V7.0
- IBM Tivoli Common Reporting V2.1.1 (2.1.1 is only supported in the Privileged Identity Manager deployment)
- IBM WebSphere Application Server Hypervisor Edition V7.0.0.11
- IBM Tivoli Federated Identity Manager V6.2.1

The program's specifications and specified operating environment information may be found in documentation accompanying the program, if available, such as a readme file, or other information published by IBM , such as an announcement letter. Documentation and other program content may be supplied only in the English language.

Planning information

Software Subscription and Support (also referred to as Software Maintenance) is included with licenses purchased through Passport Advantage and Passport Advantage Express® . Product upgrades and technical support are provided by the Software Subscription and Support (Software Maintenance) offering as described in the Agreements. Product upgrades provide the latest versions and releases to entitled software, and technical support provides voice and electronic access to IBM support organizations, worldwide.

IBM includes one year of Software Subscription and Support (also referred to as Software Maintenance) with each program license acquired. The initial period of Software Subscription and Support (Software Maintenance) can be extended by the purchase of a renewal option, if available.

Packaging

IBM Security Privileged Identity Manager V1.0 and IBM Security Identity Manager V6.0 are distributed with:

- International Program License Agreement (Z125-3301)
- License Information document
- CD-ROMs
- Publications (refer to the Publications section)

This program, when downloaded from a website, contains the applicable IBM license agreement and License Information, if appropriate, and will be presented for acceptance at the time of installation of the program. For future reference, the license and License Information will be stored in a directory such as LICENSE.TXT.

Security, auditability, and control

IBM Security Privileged Identity Manager **and** IBM Security Identity Manager use the security and auditability features of the operating system software. The customer is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

Software Services

IBM Software Services has the breadth, depth, and reach to manage your services needs. You can leverage the deep technical skills of our lab-based, software services team and the business consulting, project management, and infrastructure expertise of our IBM Global Services team. Also, we extend our IBM Software Services reach through IBM Business Partners to provide an extensive portfolio of capabilities. Together, we provide the global reach, intellectual capital, industry insight, and technology leadership to support a wide range of critical business needs.

To learn more about IBM Software Services or to contact a Software Services sales specialist, visit

http://www.ibm.com/software/sw-services/

Ordering information

This product is only available via Passport Advantage . It is not available as shrinkwrap.

```
Product group: IBM Security
  Product Identifier Description                    (PID)
  IBM Security Privileged Identity Manager V1.0     5725-H30
  IBM Security Identity Manager V6.0                5724-C34

Product category: Security Identity and Access Management
```

Charge metric

```
Program name                                PID number Charge metric

IBM Security Privileged Identity Manager    5725-H30   User Value Unit
IBM Security Identity Manager               5724-C34   User Value Unit
IBM Security Identity Manager               5724-C34   Processor
                                                         Value Unit
```

Note: Charge metric definitions follow the pricing examples.

Pricing examples

IBM Security Identity Manager pricing examples

Scenario 1

In Phase I, customer ABC wants to initially secure access for the following users and adapters through one 4-way server for its 12,000 total internal users: Each internal user equals one chargeable user.

- All 12,000 of those internal users will use the LDAP adapter.
- The same 12,000 will use the Lotus Notes adapter.
- The same 12,000 will use the SAP R3 adapter.
- Of those 12,000 internal users, only 2,000 of them will use the RACF adapter.

First, add the users for the class of adapters within a part number. A current list of adapters is available at

http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliIdentityManager.html

Transaction 1

In this example, the LDAP and Lotus Notes adapters are included in the purchase price of the base part number. SAP R3 is in the Application adapter class and RACF is in the Host adapter class. The environment is 12,000 internal users of Security Identity Manager Base, 12,000 internal users of Application, and 2,000 internal users of Host.

Pricing metric	A Internal users	B Internal chargeable uesers at 1:1	C Infrequent internal users (5 times/ year)	D External users	E Infrequent internal and external users at 15:1	F Total chargeable users
Security Identity Manager	12,000	12,000	0	0	0	12,000
Security Identity Manager for Applica-tions	12,000	12,000	0	0	0	12,000
Security Identity Manager for Host	12,000	2,000	0	0	0	2,000

Since the users are all internal users (column A), they equate to 1 chargeable user (column B) on a 1 to 1 basis (where one internal user equals one chargeable user). There are no external users or infrequent internal users to factor in. The total chargeable users are calculated in column F. In the table below, column G applies the volume tiering discount factor (from the scalable usage model table above) to the chargeable users for that tier, with the resulting User Value Units required to purchase for entitlement in column H.

Pricing metric	Chargeable users scale	F Total chargeable	G User Value Units per 1,000 chargeable users	H User Value Units required (F)*(G))/1,000
Security Identity Manager				
Tier 1	1-5,000	5,000	1,000	5,000
Tier 2	>5,000-15,000	7,000	500	3,500
Total chargeable		12,000	Total User Value Units	8,500
Security Identity Manager for Applications				
Tier 1	1-5,000	5,000	1,000	5,000
Tier 2	>5,000-15,000	7,000	500	3,500
Total chargeable		12,000	Total User Value Units	8,500
Security Identity Manager for Host				
Tier 1	1-5,000	2,000	1,000	2,000
Total chargeable		2,000	Total User Value Units	2,000

Total User Value Units to order are in column H.

Note: There is a minimum order quantity of 250 users for both IBM Security Identity Manager and each adapter, the chargeable user quantity is raised to the next incremental 100 quantity. For IBM Security Privileged Identity Manager, the minimum order quantity is 50 and increments of 10 users must be ordered.

Transaction 2

In Phase II, customer ABC wants to secure access for 1,000 additional internal users with LDAP, Lotus Notes , and SAP R3. Customer ABC also wants to entitle 150,000 external users (mostly suppliers, business partners, and consumers) to use the LDAP and Access Manager adapters. Finally, customer ABC has 22,500 factory and construction employees who access their benefit information once or twice a year (if at all), and fall into the infrequent internal user category. This is an increase of 173,500 users of Security Identity Manager. The additional users in the new environment for customer ABC would look as follows:

- 173,500 additional users of Security base who will use the LDAP, Access Manager, and Lotus Notes adapters, or 12,500 chargeable users. Refer to the calculation below.
- 1,000 internal users (1,000 chargeable users at 1:1).
- 150,000 external users (10,000 chargeable users at 1:15).
- 22,500 infrequent internal users (1,500 chargeable users at 1:15).
- 1,000 additional internal users of SAP R3 (1,000 chargeable users of Application Adapters at 1:1).

The LDAP, Access Manager, and Lotus Notes adapters are included in the purchase price of the base Identity Manager and are not priced separately. For the remaining adapters, the incremental Value Units are calculated taking advantage of the scalable user table and customer ABC's previous purchase.

Pricing metric	Phase I chargeable users	Phase II incremental chargeable users	New total chagreable users in ABC's environment
Security Identity Manager	12,000	12,500	24,500 (must be rounded up to 25,000)
Security Identity Manager for Applications	12,000	1,000	13,000
Security Identity Manager for Host	2,000	0	2,000

Pricing metric	Chargeable users scale	F Total chargeable	G User Value Units per 1,000 chargeable users	H User Value Units required (F)*(G))/1,000
Security Identity Manager				
Tier 1	1-5,000	5,000	1,000	5,000
Tier 2	>5,000-15,000	10,000	500	5,000
Tier 3	>15,000-50,000	9,000 (rounded up to 10,000	300	3,000
Total chargeable		25,000	Total User Value Units	13,000
Security Identity Manager for Applications				
Tier 1	1-5,000	5,000	1,000	5,000
Tier 2	>5,000-15,000	8,000	500	4,000
Total chargeable		13,000	Total User Value Units	9,000
Security Identity Manager for Host				
Tier 1	1-5,000	2,000	1,000	2,000
Total chargeable		2,000	Total User Value Units	2,000

The table below shows the User Value Units that were ordered in Phase I in the second column. The new required Value Unit totals required in customer ABC's environment at the end of Phase II is in the third column. The incremental total User Value Units to order are in the last column.

Product	Phase I User Value Unit totals	New required Value Unit totals	Incremental Value Units to order
Security Identity Manager	8,500	13,000	4,500
Security Identity Manager	8,500	9,000	500

```
for Applications

Security          2,000               2,000                  0
Identity Manager
for Host
```

Scenario 2

Assume Customer ABC prefers unlimited user access and unlimited adapters for their environment.

The customer will require Processor Value Units to entitle the following environment.

IBM Security Identity Manager - Unlimited User Option

```
Security Identity     Quantity in customer    Total processors required
Manager Server        environment

4-way single core     2                        8*
4-way dual core       1                        8

                  Total processor cores      16*
                  requiring PVU entitlements
```

* There is a minimum order quantity of three processor cores for the IBM Security Identity Manager Unlimited User Option.

Note: In this example, the Unlimited User Option applies only to the 16 processor cores licensed. If the customer replaced one of the 4-way single core servers with another 4-way dual core server, an additional 4 processor cores would require Processor Value Unit entitlements. This licensing is based on the server in which IBM Security Identity Manager runs. You do not count server on which supporting programs (such as DB2) run.

The Unlimited User Option also includes unlimited adapters, so no adapter part numbers need to be ordered.

For more information about processor core Value Units, go to

http://www-306.ibm.com/software/lotus/passportadvantage/pvu_licensing_for_customers.htm l

IBM Privileged Identity Manager pricing examples

IBM Security Privileged Identity Manager pricing is similar to IBM Security Identity Manager. The same examples apply except with these differences:

- IBM Security Privileged Identity Manager does not offer a PVU based Unlimited User option.
- All IBM Security Identity Manager adapters are included in IBM Security Privileged Identity Manager. There is no need to buy additional adapter licenses for IBM Security Privileged Identity Manager users.
- All IBM Security Privileged Identity Manager users are considered internal and not "infrequent" users for UVU counting.
- The minimum order quantity is 50 for IBM Security Privileged Identity Manager and the UVUs must be ordered in increments of 10.

For example, Customer XYZ has 10,000 employees, 200 of which are system administrators to whom they want to give full IBM Security Privileged Identity Manager capabilities. For IBM Security Privileged Identity Manager licenses, the customer would order 200 UVUs of part number D0T0BLL - Sec Privileged Identity Mgr per UVU Lic + SW S& S 12 Mo.

If the customer also wants to manage some or all of the remaining 9,800 employees under IBM Security Identity Manager, follow the ordering information in the preceding section to order the appropriate number of IBM Security Identity Manager entitlements.

If the customer also wants to provide IBM Security Access Manager for Enterprise Single Sign-on for some or all of the remaining employees, refer to Software Announcement 212-004, dated January 10, 2012 .

IBM Security Privileged Identity Manager trade ups

Customers holding IBM Security Identity Manager or IBM Security Access Manager for Enterprise Single Sign-On licenses may exchange (trade up) those licenses for IBM Security Privileged Identity Manager licenses for their privileged users. An example follows.

Licensees of other products, IBM Security Identity Access and Assurance, and IBM Tivoli Identity and Access Management cannot exchange licenses (there is not a 1:1 correspondence that is relevant for the trade up), and must purchase IBM Security Privileged Identity Manager licenses directly for their privileged users.

IBM Security Identity Manager users holding unlimited (PVU) based licenses cannot trade up since there is no PVU based offering for IBM Security Privileged Identity Manager, and privileged users are typically a subset of IBM Security Identity Manager users.

Trade-up example

Customer ABC owns 10,000 UVUs of IBM Security Identity Manager licenses. This currently includes entitlements for 150 system administrators that they want to give full IBM Security Privileged Identity Manager capabilities.

Customer ABC will buy 150 UVUs of IBM Security Privileged Identity Manager trade-up part number (below). They will then have 150 UVUs of IBM Security Privileged Identity Manager and 9,850 UVUs of IBM Security Identity Manager left. The administrative users will still have the capabilities of IBM Security Identity Manager available to them, plus the added capabilities of IBM Security Privileged Identity Manager.

The trade-up license fee includes 12 months of Subscription and Support for IBM Security Privileged Identity Manager.

For example, the customer would order 150 UVUs of part number D0T0ELL - Sec Identity Mgr and Role Mgr UVU to Sec Privileged Identity Mgr UVU Trdup Lic + SW S&S 12 Mo

This example would be the same for exchanging IBM Security Access Manager for Enterprise Single Sign-on licenses, except that a different trade-up part number would be ordered (D0T0FLL Sec Access Mgr for ESSO Suite UVU to Sec Privileged Identity Mgr UVU Trdup Lic + SW S&S 12 Mo).

Also note that licensed IBM Security Privileged Identity Manager customers with existing licensed IBM Security Identity Manager V6.0 or IBM Security Enterprise Single Sign-on V8.2 installations may share those physical deployments with IBM Security Privileged Identity Manager, provided all are separately licensed. A separate physical deployment of IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On is supported, but not required, for IBM Security Privileged Identity Manager.

User Value Unit (UVU)

UVU is a unit of measure by which the program can be licensed. UVU Proofs of Entitlement (PoEs) are based on the number and type of users for the given program. Licensee must obtain sufficient entitlements for the number of UVUs required for licensee's environment as specified in the program specific table. The UVU entitlements are specific to the program and type of user and may not be exchanged, interchanged, or aggregated with UVU entitlements of another program or type of user. Refer to the program specific UVU table.

Additional user counting notes for IBM Security Identity Manager:

- For IBM Security Identity Manager only, under the UVU counting method, nonproduction users need not be counted for licensing. This is a special historical exception only for IBM Security Identity Manager's UVU licensing method.
- Within IBM Security Identity Manager, user subcategories can be exchanged as follows. Infrequent and external users may be exchanged with internal users of IBM Security Identity Manager, as long as the total number of licensed UVUs does not change. So, as an example, the customer could entitle 3,000 external users and 200 internal users, or 4,500 external user and 100 internal users for the 400 UVUs that they purchase. The standard IBM nonexchange restriction language mentioned above refers to IBM standard user types, in this case Authorized User. IBM Security Identity Manager Authorized Users may not be exchanged with other licensed product users or with other IBM defined user types like Concurrent User, but may be within the subcategories of internal, external, and infrequent.

Chargeable users are added up and the volume tiering information below is then utilized to calculate the total User Value Units entitlements required for IBM Security Identity Manager or IBM Security Privileged Identity Manager.

Scalable usage level	1	2	3	4
Chargeable users	1 - 5K	>5K - 15K	>15k - 50K	>50K-150K
Value Units per 1,000 chargeable users	1,000	500	300	200

Scalable usage level	5	6	7	8
Chargeable users	>150-500	>500-1M	>1M - 3M	>3M
Value Units per 1,000 chargeable users	100	50	25	10

Processor Value Unit (PVU)

PVU is a unit of measure by which the program can be licensed. The number of PVU entitlements required is based on the processor technology (defined within the PVU table by processor value, brand, type, and model number at the website below) and the number of processors made available to the program. IBM continues to define a processor, for the purpose of PVU-based licensing, to be each processor core on a chip. A dual-core processor chip, for example, has two processor cores. The PVU table can be found at

http://www.ibm.com/software/lotus/passportadvantage/pvu_licensing_for_customers.html

Licensee can deploy the program using either full capacity licensing or virtualization capacity (sub-capacity) licensing according to the Passport Advantage Sub-Capacity Licensing Terms (refer to the web page below). If using full capacity licensing, licensee must obtain PVU entitlements sufficient to cover all activated processor cores* in the physical hardware environment made available to or managed by the program, except for those servers from which the program has been permanently removed. If using virtualization capacity licensing, licensee must obtain entitlements sufficient to cover all activated processor cores made available to or managed by the program, as defined according to the Virtualization Capacity License Counting Rules at

http://www.ibm.com/software/lotus/passportadvantage/Counting_Software_licenses_using_sp ecific_virtualization_technologies.html

* An activated processor core is a processor core that is available for use in a physical or virtual server, regardless of whether the capacity of the processor core can be or is limited through virtualization technologies, operating system commands, BIOS settings, or similar restrictions.

Passport Advantage

IBM Security Privileged Identity Manager V1.0

Program name/Description	Part number
Sec Privileged Identity Mgr per UVU Lic + SW S&S 12 Mo	D0T0BLL
Sec Privileged Identity Mgr per UVU Annual SW S&S Rnwl	E0EETLL
Sec Privileged Identity Mgr per UVU SW S&S Reinstate 12 Mo	D0T0DLL
Sec Identity Mgr and Role Mgr UVU to Sec Privileged Identity Mgr UVU Trdup Lic + SW S&S 12 Mo	D0T0ELL
Sec Access Mgr for ESSO Suite UVU to Sec Privileged Identity Mgr UVU Trdup Lic + SW S&S 12 Mo	D0T0FLL
Sec Privileged Identity Mgr per UVU for Linux on System z Lic + SW S&S 12 Mo	D0T08LL
Sec Privileged Identity Mgr per UVU Linux on System z Annual SW S&S Rnwl	E0EERLL
Sec Privileged Identity Mgr per UVU Linux on System z SW S&S Reinstate 12 Mo	D0T09LL

IBM Security Identity Manager V6.0

Program name/Description	Part number
Security Identity Manager and Role Management User VU for zEnterprise® BladeCenter® Extension and Linux on System z SW Maint Reinstate 12 Mos	D61VWLL
Security Identity Manager and Role Management User VU for zEnterprise BladeCenter Extension and Linux on System z SW Maint Annual Renew	E047QLL
Security Identity Manager and Role Management User VU for zEnterprise BladeCenter Extension and Linux on System z Lic & SW Maint 12 Mos	D61VVLL
Security Identity Manager and Role Management User Value Unit SW Maint Reinstate 12 Mos	D61VYLL
Security Identity Manager and Role Management User Value Unit License & SW Maint 12 Mos	D61VXLL
Security Identity Manager and Role Management User Value Unit SW Maint Annual Renewal	E047RLL
Security Identity Manager App Edition User VU from Tiv Dir Integ VU Tradeup Lic & SW Maint 12 Mos	D61VULL
Security Identity Manager Application Edition User VU SW Maint Annual Renew	E047PLL
Security Identity Manager Application Edition User VU Lic & SW Maint 12 Mos	D61VSLL
Security Identity Manager Application Edition User VU SW Maint Reinst 12 Mos	D61VTLL
Security Identity Manager Host Ed User VU from Identity Dir Integ Tradeup Lic & SW Maint 12 Mos	D61VILL
Security Identity Manager Host Edition	E047JLL

User VU SW Maint Annual Renew	
Security Identity Manager Host Edition User VU License & SW Maint 12 Mos	D61VGLL
Security Identity Manager Host Edition VU SW Maint Reinstate 12 Mos	D61VHLL
Security Identity Manager and Role Management Unlimited User Option Processor Value Unit (PVU) SW Subscription & Support Reinstatement 12 Months	D61VKLL
Security Identity Manager and Role Management Unlimited User Option Processor Value Unit (PVU) Annual SW Subsctription & Support Renewal 12 Months	E047KLL
Security Identity Manager and Role Management Unlimited User Option for zEnterprise BladeCenter Extension and Linux on System z Processor Value Unit (PVU) SW Subscription & Support Renewal	E047ILL
Security Identity Manager and Role Management Unlimited User Option for zEnterprise BladeCenter Extension and Linux on System z Processor Value Unit (PVU) License + SW Subscription & Support 12 Months	D61VELL
Security Identity Manager and Role Management Unlimited User Option Processor Value Unit (PVU) License + SW Subsctription & Support Renewal 12 Months	D61VJLL
Security Identity Manager and Role Management Unlimited User Option for zEnterprise BladeCenter Extension and Linux on System z Processor Value Unit (PVU) SW Subscription & Support Reinstatement 12 Months	D61VFLL
ISIM Host Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit Lic + SW S&S 12 Mo	D0LJPLL
ISIM Host Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit Annual SW S&S Rnwl	E0CXHLL
ISIM Host Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit Annual SW &S1 Reinstate 12 Mo	D0LJQLL
ISIM App Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit Lic + SW S&S 12 Mo	D0LJMLL
ISIM App Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit Annual SW S&S Rnwl	E0CXGLL
ISIM App Edition for zEnterprise BladeCenter Extension and Linux on System z User Value Unit SW S&S Reinstate 12 Mo	D0LJNLL

Passport Advantage trade up

You must have previously acquired a license for the above precursor products to be eligible to acquire an equivalent license of the trade-up product.

Consult your IBM representative if you have any questions.

Refer to the Basic license section.

Passport Advantage customer: Media pack entitlement details

Customers with active maintenance or subscription for the products listed are entitled to receive the corresponding media pack.

Entitled maintenance offerings

description	Part number
IBM Security Identity Manager 6.0 DVD Media Pack, MultiPlatform, ML	BJ11NML
IBM Security Privileged Identity Manager V1.0 DVD Media Pack, MultiPlatform, ML	BJ11MML

Withdrawal of previous Passport Advantage part numbers

The following IPLA software media pack part numbers are being replaced or are obsolete as a result of this announcement. The effective withdrawal date is November 23, 2012.

Orders for these part numbers will not be accepted after the stated effective date of withdrawal, nor will normal marketing activities or educational support be available unless previous agreement exists between the customer and IBM .

Withdrawn from marketing information

Program name/Description	Part number
IBM Tivoli Identity Manager 4.6 Media Pack Multilingual	BJ0F9ML
IBM Tivoli Identity Manager for Multiplatforms Version 5.0 Multilingual	BJ0B5ML

New release information

Program name/Description	Part number
IBM Security Identity Manager 6.0 Multiplatform, Multilingual	BJ11NML

Terms and conditions

The information provided in this announcement letter is for reference and convenience purposes only. The terms and conditions that govern any transaction with IBM are contained in the applicable contract documents such as the IBM International Program License Agreement, IBM International Passport Advantage Agreement, and the IBM Agreement for Acquisition of Software Maintenance.

This product is only available via Passport Advantage . It is not available as shrinkwrap.

Licensing

IBM International Program License Agreement including the License Information document and Proof of Entitlement (PoE) govern your use of the program. PoEs are required for all authorized use. Part number products only, offered outside of Passport Advantage , where applicable, are license only and do not include Software Maintenance.

This software license includes Software Subscription and Support (also referred to as Software Maintenance).

These programs are licensed under the IBM Program License Agreement (IPLA) and the associated Agreement for Acquisition of Software Maintenance, which provide for support with ongoing access to releases and versions of the program. IBM includes one year of Software Subscription and Support (also referred to as Software Maintenance) with the initial license acquisition of each program acquired. The initial period of Software Subscription and Support (also referred to as Software Maintenance) can be extended by the purchase of a renewal option, if available. These programs have a one-time license charge for use of the program and an annual renewable charge for the enhanced support that includes telephone

assistance (voice support for defects during normal business hours), as well as access to updates, releases, and versions of the program as long as support is in effect.

License Information form number

- L-SLEE-8TG7GM - IBM Security Privileged Identity Manager V1.0 (5725-H30)
- L-YSOI-8SYHEL - IBM Security Identity Manager V6.0) (5724-C34)

The program's License Information will be available for review on the IBM Software License Agreement website

http://www.ibm.com/software/sla/sladb.nsf

Limited warranty applies

Yes

Limited warranty

IBM warrants that when the program is used in the specified operating environment, it will conform to its specifications. The warranty applies only to the unmodified portion of the program. IBM does not warrant uninterrupted or error-free operation of the program or that IBM will correct all program defects. You are responsible for the results obtained from the use of the program.

IBM provides you with access to IBM databases containing information on known program defects, defect corrections, restrictions, and bypasses at no additional charge. For further information, consult the IBM Software Support Handbook found at

http://www.ibm.com/support/handbook

IBM will maintain this information for at least one year after the original licensee acquires the program (warranty period).

Program technical support

Technical support of a program product version or release will be available for a minimum of five years from the general availability date, as long as your Software Subscription and Support (also referred to as Software Maintenance) is in effect. This technical support allows you to obtain assistance (via telephone or electronic means) from IBM for product-specific, task-oriented questions regarding the installation and operation of the program product. Software Subscription and Support (Software Maintenance) also provides you with access to updates (modifications or fixes), releases, and versions of the program. You will be notified, via announcement letter, of discontinuance of support with 12 months' notice. If you require additional technical support from IBM , including an extension of support beyond the discontinuance date, contact your IBM representative or IBM Business Partner. This extension may be available for a fee.

Money-back guarantee

If for any reason you are dissatisfied with the program and you are the original licensee, you may obtain a refund of the amount you paid for it, if within 30 days of your invoice date you return the program and its PoE to the party from whom you obtained it. If you downloaded the program, you may contact the party from whom you acquired it for instructions on how to obtain the refund.

For clarification, note that (1) for programs acquired under the IBM International Passport Advantage offering, this term applies only to your first acquisition of the program and (2) for programs acquired under any of IBM's On/Off Capacity on Demand (On/Off CoD) software offerings, this term does not apply since these offerings apply to programs already acquired and in use by you.

Other terms

Volume orders (IVO)

No

IBM International Passport Advantage Agreement

Passport Advantage applies

Yes, and through the Passport Advantage website at

http://www.ibm.com/software/passportadvantage

Usage restriction

Yes. Usage is limited to the quantity of Value Units licensed.

For additional information, refer to the License Information document that is available on the IBM Software License Agreement website

http://www.ibm.com/software/sla/sladb.nsf

Software Subscription and Support applies

Yes. Software Subscription and Support (also referred to as Software Maintenance) is included with licenses purchased through Passport Advantage and Passport Advantage Express . Product upgrades and Technical Support are provided by the Software Subscription and Support offering as described in the Agreements. Product upgrades provide the latest versions and releases to entitled software and Technical Support provides voice and electronic access to IBM support organizations, worldwide.

IBM includes one year of Software Subscription and Support with each program license acquired. The initial period of Software Subscription and Support can be extended by the purchase of a renewal option, if available.

While your Software Subscription and Support is in effect, IBM provides you assistance for your routine, short duration installation and usage (how-to) questions, and code-related questions. IBM provides assistance via telephone and, if available, electronic access, only to your information systems (IS) technical support personnel during the normal business hours (published prime shift hours) of your IBM support center. (This assistance is not available to your end users.) IBM provides Severity 1 assistance 24 hours a day, 7 days a week. For additional details, consult your IBM Software Support Handbook at

http://www.ibm.com/support/handbook

Software Subscription and Support does not include assistance for the design and development of applications, your use of programs in other than their specified operating environment, or failures caused by products for which IBM is not responsible under the applicable agreements.

For additional information about the International Passport Advantage Agreement and the IBM International Passport Advantage Express Agreement, visit the Passport Advantage website at

http://www.ibm.com/software/passportadvantage

System i Software Maintenance applies

No

Variable charges apply

No

Educational allowance available

Not applicable.

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in misuse of your systems to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

IBM Electronic Services

IBM has transformed its delivery of hardware and software support services to help you achieve higher system availability. Electronic Services is a web-enabled solution that offers an exclusive, no-additional-charge enhancement to the service and support available for IBM servers. These services are designed to provide the opportunity for greater system availability with faster problem resolution and preemptive monitoring. Electronic Services comprises two separate, but complementary, elements: Electronic Services news page and Electronic Services Agent.

The Electronic Services news page is a single Internet entry point that replaces the multiple entry points traditionally used to access IBM Internet services and support. The news page enables you to gain easier access to IBM resources for assistance in resolving technical problems.

The Electronic Service Agent™ is no-additional-charge software that resides on your server. It monitors events and transmits system inventory information to IBM on a periodic, client-defined timetable. The Electronic Service Agent automatically reports hardware problems to IBM . Early knowledge about potential problems enables IBM to deliver proactive service that may result in higher system availability and performance. In addition, information collected through the Service Agent is made available to IBM service support representatives when they help answer your questions or diagnose problems. Installation and use of IBM Electronic Service Agent for problem reporting enables IBM to provide better support and service for your IBM server.

To learn how Electronic Services can work for you, visit

http://www.ibm.com/support/electronic

Prices

Business Partner information

If you are an IBM Business Partner -- Distributor for Workstation Software acquiring products from IBM , you may link to Passport Advantage Online for resellers where you can obtain Business Partner pricing information. An IBM ID and password are required.

https://www.ibm.com/software/howtobuy/passportadvantage/paoreseller

For Passport Advantage information visit

http://www-01.ibm.com/software/howtobuy/passportadvantage/

IBM Global Financing

IBM Global Financing offers competitive financing to credit-qualified customers to assist them in acquiring IT solutions. Offerings include financing for IT acquisition, including hardware, software, and services, from both IBM and other manufacturers or vendors. Offerings (for all customer segments: small, medium, and large enterprise), rates, terms, and availability can vary by country. Contact your local IBM Global Financing organization or visit

http://www.ibm.com/financing

IBM Global Financing offerings are provided through IBM Credit LLC in the United States, and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Rates are based on a customer's credit rating, financing terms, offering type, equipment type, and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension, or withdrawal without notice.

Financing from IBM Global Financing helps you preserve cash and credit lines, enables more technology acquisition within current budget limits, permits accelerated implementation of economically attractive new technologies, offers payment and term flexibility, and can help match project costs to projected benefits. Financing is available worldwide for credit-qualified customers.

For more financing information, visit

http://www.ibm.com/financing

Order now

To order, contact your local IBM representative or your IBM Business Partner.

To identify your local IBM Business Partner or IBM representative, call 800-IBM-4YOU (426-4968). For more information, contact the Americas Call Centers.

```
Phone:     800-IBM-CALL (426-2255)
Fax:       800-2IBM-FAX (242-6329)
 For IBM representative: callserv@ca.ibm.com

 For IBM Business Partner: pwswna@us.ibm.com

Mail:      IBM Teleweb Customer Support
           ibm.com® Sales Execution Center, Americas North
           3500 Steeles Ave. East, Tower 3/4
           Markham, Ontario
           Canada  L3R 2Z1

Reference: YE001
```

The Americas Call Centers, our national direct marketing organization, can add your name to the mailing list for catalogs of IBM products.

Note: Shipments will begin after the planned availability date.

Trademarks

DB2 Universal Database and Electronic Service Agent are trademarks of IBM Corporation in the United States, other countries, or both.

IBM, Tivoli, Cognos, WebSphere, AIX, Service Request Manager, Lotus Notes, Passport Advantage, RACF, System i, System p, System z, z/VM, DB2, Express, zEnterprise, BladeCenter and ibm.com are registered trademarks of IBM Corporation in the United States, other countries, or both.

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

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

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

Terms of use

IBM products and services which are announced and available in your country can be ordered under the applicable standard agreements, terms, conditions, and prices in effect at the time. IBM reserves the right to modify or withdraw this announcement at any time without notice. This announcement is provided for your information only. Additional terms of use are located at

http://www.ibm.com/legal/us/en/

For the most current information regarding IBM products, consult your IBM representative or reseller, or visit the IBM worldwide contacts page

http://www.ibm.com/planetwide/us/

Corrections

(Corrected on December 4, 2012)
Updated web address in the Description section.