IBM Security Identity Manager
Version 6.0.0.18
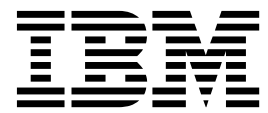
Product Overview Topics

IBM

IBM Security Identity Manager
Version 6.0.0.18

Product Overview Topics

IBM

Table of contents

Table list

Chapter 1. IBM Security Identity Manager overview

IBM® Security 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. By using 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.

IBM Security Identity Manager helps companies automate the process of provisioning employees, contractors, and business partners in one or more organizations with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise. IBM Security Identity Manager provides lifecycle management of user accounts on remote resources, with adapters and policy-based provisioning to enable access to the managed resources that an enterprise requires.

One or more IBM Security Identity Manager organizations contain users, who have membership in groups and have static or dynamic organization roles. Additional policies and workflows enable access to the entitlements to managed resources, and access control items grant rights to selected privileges. A system administrator has full access to all operational areas of IBM Security Identity Manager.

Chapter 2. How to obtain software images

IBM Security Identity Manager installation files and fix packs can be obtained with the IBM Passport Advantage® website, or from a DVD distribution.

The Passport Advantage website provides packages, called eAssemblies, for IBM products.

To obtain eAssemblies for IBM Security Identity Manager, follow the instructions in the IBM Security Identity Manager Download Document.

The *IBM Security Identity Manager Installation Guide* provides full instructions for installing IBM Security Identity Manager and the prerequisite middleware products.

The procedure that is appropriate for your organization depends on the following conditions:

* Operating system used by IBM Security Identity Manager
* Language requirements for using the product
* Type of installation you need to do:

  eAssembly for the product and all prerequisites
  > The IBM Security Identity Manager installation program enables you to install IBM Security Identity Manager, prerequisite products, and required fix packs as described in the *IBM Security Identity Manager Installation Guide*. Use this type of installation if your organization does not currently use one or more of the products required by IBM Security Identity Manager.

  eAssembly for a manual installation
  > You can install IBM Security Identity Manager separately from the prerequisites, and you can install separately any of the prerequisite products that are not installed. In addition, you must verify that each prerequisite product is operating at the required fix or patch level.

Chapter 3. Hardware and software requirements

IBM Security Identity Manager has specific hardware requirements and supports specific versions of operating systems, middleware, and browsers.

The topics in this section list the hardware requirements and the supported versions for each of the software products. The information lists the supported versions when the product release was released.

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Hardware requirements

IBM Security Identity Manager has these hardware requirements:

Table 1. Hardware requirements for IBM Security Identity Manager

System components	Minimum values*	Suggested values**
System memory (RAM)	2 gigabytes	4 gigabytes
Processor speed	Single 2.0 gigahertz Intel or pSeries processor	Dual 3.2 gigahertz Intel or pSeries processors
Disk space for product and prerequisite products	20 gigabytes	25 gigabytes
* Minimum values: These values enable a basic use of IBM Security Identity Manager. ** Suggested values: You might need to use larger values that are appropriate for your production environment.		

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Operating system support

IBM Security Identity Manager supports multiple operating systems.

The IBM Security Identity Manager installation program checks to ensure that specific operating systems and levels are present before it starts the installation process.

Note: The Identity Service Center uses WebSphere 8.5 and is supported on 64-bit operating systems only.

Table 2. Operating system support

Operating system	Platform	Patch or maintenance level
AIX® Version 6.1	System p	None
AIX Version 7.1	System p	Technology Level (TL) 4
AIX Version 7.2	System p	None
Oracle Solaris 10	SPARC	None

Table 2. Operating system support (continued)

Operating system	Platform	Patch or maintenance level
Windows Server 2008 Standard Edition	x86-32 x86-64	None
Windows Server 2008 Enterprise Edition	x86-32 x86-64	None
Windows Server 2008 Release 2 Standard Edition	x86-64	None
Windows Server 2008 Release 2 Enterprise Edition	x86-64	None
Windows Server 2012 Standard Edition	x86-64	None
Windows Server 2012 Release 2 Standard Edition	x86-64	None
Red Hat Enterprise Linux 5.0 Red Hat Enterprise Linux 6.0 Red Hat Enterprise Linux 7.0	x86-32, x86-64, System p, System z x86-32, x86-64, System p, System z	• For 5.0, Update 6. • For 6.0, Update 5. • For both 5.0 and 6.0, Security Enhanced Linux must be disabled. See the topic "Red Hat Linux Server Configuration" in the *IBM Security Identity Manager Installation Guide.* • For 7.0, Update 2
SUSE Linux Enterprise Server 10.0 SUSE Linux Enterprise Server 11.0 SUSE Linux Enterprise Server 12.0	System p, System z, x86-32, x86-64 System p, System z®, x86-32, x86-64	• For 10, SP3 • For 11, SP3 • For 12, SP1

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Virtualization support

IBM Security Identity Manager supports virtualization environments.

See Table 3 for a list of the virtualization products that IBM Security Identity Manager supports at the time of product release.

Table 3. Virtualization support.

Product	Applicable operating systems
IBM AIX Workload Partitioning (WPAR) and Logical Partitioning (LPAR) 6.1 and 7.1 and future fix packs	All supported operating system versions automatically applied

Table 3. Virtualization support (continued).

Product	Applicable operating systems
IBM PowerVM® Hypervisor (LPAR, DPAR, Micro-Partition), any supported version and future fix packs	AIX
IBM PR/SM™, any version, and future fix packs	All supported operating system versions automatically applied
IBM z/VM® Hypervisor 5.4 and any future fix packs	All supported operating system versions automatically applied
IBM z/VM Hypervisor 6.1 and any future fix packs	Linux
KVM in SUSE Linux Enterprise Server (SLES) 11	All supported operating system versions automatically applied
Red Hat KVM as delivered with Red Hat Enterprise Linux (RHEL) 5.4 and future fix packs	Linux, Windows
Red Hat KVM as delivered with Red Hat Enterprise Linux (RHEL) 6.0 and future fix packs	All supported operating system versions automatically applied
Sun Solaris 10 Global/Local Zones (SPARC) 10 and future fix packs	All supported operating system versions automatically applied
Sun/Oracle Logical Domains (LDoms) any version and future fix packs	Solaris
VMware ESXi 4.0 and future fix packs	All supported operating system versions automatically applied
VMware ESXi 5.0 and future fix packs	All supported operating system versions automatically applied
VMware ESXi 5.1 and future fix packs	All supported operating system versions automatically applied
VMware ESXi 5.5 and future fix packs	All supported operating system versions automatically applied

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Java Runtime Environment support

IBM Security Identity Manager requires the Java™ Runtime Environment (JRE).

When a required version of the WebSphere® Application Server is installed, the required version or a later version of the JRE is installed in the *WAS_HOME*/java directory. For information about the required versions of the WebSphere Application Server, see "WebSphere Application Server support" on page 8.

Use of an independently installed development kit for Java, from IBM or other vendors, is *not* supported. The Java Runtime Environment requirements for using a browser to create a client connection to the IBM Security Identity Manager server are different than the JRE requirements for running the WebSphere Application Server.

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

WebSphere Application Server support

IBM Security Identity Manager runs as an enterprise application in a WebSphere Application Server environment.

IBM Security Identity Manager requires one of the following versions of WebSphere Application Server for support of all platforms:

Table 4. Supported versions of WebSphere Application Server

WebSphere Application Server	Fix Pack	Notes
7.0.0.29	Fix Pack 29	Fix Pack 29 is required for support of all platforms.
8.5.5		Network Deployment is required for Identity Service Center user interface
8.5.5.1	Fix Pack 1	Fix Pack 1 is required for support of all platforms. Network Deployment is required for Identity Service Center user interface.
8.5.0.2	Fix Pack 2	Fix Pack 2 is required for support of all platforms. Network Deployment is required for Identity Service Center user interface.
8.5.5.4	Fix Pack 4	Network Deployment is required for Identity Service Center user interface
8.5.5.9	Fix Pack 9	Network Deployment is required for Identity Service Center user interface

WebSphere supports each of the operating systems that IBM Security Identity Manager supports. Review the WebSphere product documentation for the WebSphere requirements for each operating system: https://www.ibm.com/support/knowledgecenter/SSEQTP/mapfiles/product_welcome_was.html

A Java JRE is installed along with WebSphere Application Server. Do not attempt to install an independently installed JRE.

Important: The following configurations are not currently supported:
- WebSphere Application Server version 6.1 with Java 5 JRE
- WebSphere Application Server version 8.5.5 with Java 7.1 JRE. Java 7.0 JRE is supported.
- Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Database server support

IBM Security Identity Manager supports multiple database server products.

Table 5. Database server support

Database server	Fix pack	Notes
IBM DB2® Enterprise Version 9.5 IBM DB2 Workgroup Version 9.5	Fix Pack 3 and future fix packs	IBM DB2 Workgroup Edition is required for Linux 32 bit operating system. **Note:** Contact technical support for the latest security information and fixes.
IBM DB2 Enterprise Version 9.7 IBM DB2 Workgroup Version 9.7	Fix Pack 9 and future fix packs	• IBM DB2 Workgroup Edition is required for Linux 32 bit operating system. • Red Hat Linux 6.0 requires Fix Pack 4. • Windows 2012 requires Fix Pack 7.
IBM DB2 Enterprise Version 10.1 IBM DB2 Workgroup Version 10.1	Fix Pack 3A and future fix packs	• IBM DB2 Enterprise 10.1 is only supported on 64 bit operating systems. • Using IBM DB2 10.1 with IBM Tivoli® Directory Server 6.3 requires Tivoli Directory Server Fix Pack 21.
DB2 Enterprise Version 10.1 IBM DB2 Workgroup Version 10.1	Fix Pack 4 and future fix packs	• IBM DB2 Enterprise 10.1 is only supported on 64 bit operating systems. • Using IBM DB2 10.1 FP4 with IBM Tivoli Directory Server 6.3 requires Tivoli Directory Server Fix Pack 21. • Using IBM DB2 10.1 FP4 with IBM Security Directory Server 6.3.1 requires Security Directory Server Fix Pack 5.
DB2 Enterprise Version 10.5 IBM DB2 Workgroup Version 10.5	Fix Pack 5 and future fix packs	IBM DB2 Enterprise 10.5 is only supported on 64 bit operating systems
Oracle 10g Standard Edition and Enterprise Edition Release 2	none	The Oracle 11.1.0.7 database driver is required for the Oracle 10g Release 2 database.
Oracle 11g Standard and Enterprise Edition Release 2	none	The Oracle 11.1.0.7 database driver is required for the Oracle 11g Release 2 database.
Oracle 12c Standard and Enterprise Edition Release 1	Fix Pack 2 (12.1.0.2)	The Oracle 12.1.0.2 database driver is required for the Oracle 12c Release 1 database.
Microsoft SQL Server Enterprise Edition 2008	none	
Microsoft SQL Server Enterprise Edition 2008 Release 2	none	

Note: Microsoft SQL servers are not supported with WebSphere 8.5 or the Identity Service Center user interface

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Directory server support

IBM Security Identity Manager supports multiple directory servers.

Table 6. Directory server support

Directory server	Fix packs	Notes®
IBM Tivoli Directory Server, Version 6.2	Fix Pack 29 and later fix packs	
IBM Tivoli Directory Server, Version 6.3	Fix Pack 21 and later fix packs	IBM Tivoli Directory Server supports the operating system releases that IBM Security Identity Manager supports. IBM Tivoli Directory Server, Version 6.3 Fix Pack 21 is required for IBM Security Directory Server V6.3 to work with IBM DB2 10.1. A fix pack can have requirements for a specific level of Global Security ToolKit (GSKit). For more information, see documentation that the directory server product provides. For example, access this website: http://www-947.ibm.com/support/entry/portal/documentation_expanded_list/software/security_systems/tivoli_directory_server
IBM Security Directory Server, Version 6.3.1	And later fix packs	IBM Security Directory Server supports the operating system releases that IBM Security Identity Manager supports. You must install fix pack 5 to use IBM Security Directory Server version 6.3.1 with DB2 Universal Database 10.1.0.4.
IBM Security Directory Server Version 6.4	And later fix packs	IBM Security Directory Server supports the operating system releases that IBM Security Identity Manager supports.
IBM Security Directory Suite, Version 8.0	And later fix packs	IBM Security Identity Manager supports IBM Security Directory Suite, Version 8.0.
Sun Java System Directory Server Enterprise Edition 6.3.1 and 7.0	And later fix packs	See Oracle documentation to verify operating system support.
Oracle Directory Server Enterprise Edition 11g (11.1.1)	And later fix packs	

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Directory Integrator support

IBM Security Identity Manager supports IBM Security Directory Integrator and IBM Tivoli Directory Integrator.

You can optionally install IBM Security Directory Integrator or IBM Tivoli Directory Integrator for use with IBM Security Identity Manager.

IBM Security Directory Integrator and IBM Tivoli Directory Integrator are used to enable communication between the installed agentless adapters and IBM Security Identity Manager. See *Installing* in the IBM Security Identity Manager product documentation.

Table 7. Supported versions of IBM Tivoli Directory Integrator

Release	Fix pack
IBM Tivoli Directory Integrator, Version 7.1	Minimum level is Fix Pack 3
IBM Tivoli Directory Integrator, Version 7.1.1	• Minimum level is Fix Pack 4 • 7.1.1-TIV-TDI-LA0022 is required for Java 7 support. **Note:** Interim Fix 21 has limited support on Windows Server 2012. • Fix Pack 5

IBM Security Directory Integrator and IBM Tivoli Directory Integrator support each of the operating system versions that IBM Security Identity Manager supports.

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Prerequisites for IBM Cognos report server

Security Identity Manager 6.0.0.10 supports IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1 as well as IBM Cognos Business Intelligence Server, version 10.2.2.

You must install the software in the following table to work with IBM Security Identity Manager Cognos reports.

Table 8. Software requirements for IBM Cognos report server.

Software	For more information, see
IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1	1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/ knowledgecenter/SSEP7J_10.2.1/ com.ibm.swg.ba.cognos.cbi.doc/ welcome.html. 2. Search for **Business Intelligence Installation and Configuration Guide 10.2.1**. 3. Search for the installation information and follow the procedure. 4. Additionally, install IBM Cognos fix pack 1.
IBM Cognos Business Intelligence Server, version 10.2.2 Fix pack 4	1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/ knowledgecenter/SSEP7J_10.2.2/ com.ibm.swg.ba.cognos.cbi.doc/ welcome.html. 2. Search for **Business Intelligence Installation and Configuration Guide 10.2.2**. 3. Search for the installation information and follow the procedure.
Web server	1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/ knowledgecenter/SSEP7J_10.2.1/ com.ibm.swg.ba.cognos.cbi.doc/ welcome.html. 2. In the right pane of the home page, under **Supported hardware and software** section, click **Supported software environments 10.2.1**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Click the **Web Servers** in the **Supported Software** tab. **Note:** Follow the same procedure for IBM Cognos Business Intelligence, version 10.2.2 by replacing the version number.

Table 8. Software requirements for IBM Cognos report server (continued).

Software	For more information, see
Data sources	1. Access the IBM Cognos Business Intelligence documentation at http://www.ibm.com/support/ knowledgecenter/SSEP7J_10.2.1/ com.ibm.swg.ba.cognos.cbi.doc/ welcome.html. 2. In the right pane of the home page, under **Supported hardware and software** section, click **Supported software environments 10.2.1**. 3. Click **10.2.1** tab. 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence 10.2.1**. 5. Click the **Data Sorces** in the **Supported Software** tab. **Note:** Follow the same procedure for IBM Cognos Business Intelligence, version 10.2.2 by replacing the version number.

Note:

- Security Identity Manager version 6.0.0.10 report package is packaged with IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1 as well as IBM Cognos Business Intelligence Server, version 10.2.2. By default, the Security Identity Manager version 6.0.0.10 uses the IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1.

- Reports in the IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1 can run in the IBM Cognos Business Intelligence Server, version 10.2.2. However, if you work with IBM Cognos Business Intelligence Server, version 10.2.2, the compatibility with an earlier versions of IBM Cognos Business Intelligence Server is not supported. For more information about installation and configuration of IBM Cognos Business Intelligence Server, version 10.2.2, see http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.2/ com.ibm.swg.ba.cognos.cbi.doc/welcome.html?.

- Optionally, you can install IBM Framework Manager, version 10.2.1 if you want to customize the reports or models.

- Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Browser requirements for client connections

IBM Security Identity Manager has browser requirements for client connections.

IBM Security Identity Manager supports the following browser versions:

Table 9. Supported web browsers

Browser	Version	Notes
Microsoft Internet Explorer	11.0	• The Identity Service Center works only in Native mode. • Metro mode is not supported. See Workflow problems.
	10.0	• The Identity Service Center works only in Native mode. • Metro mode is not supported. See Workflow problems.
	9.0	The Identity Service Center works only in Native mode.
Mozilla Firefox	45 Extended Support Release	Is not supported on AIX.
	31 Extended Support Release	Is not supported on AIX.
	24 Extended Support Release	Is not supported on AIX.
	17 Extended Support Release	Is not supported on AIX.
	10 Extended Support Release	• The Identity Service Center is not supported. • Is not supported on AIX.
	3.6 Extended Support Release	• The Identity Service Center is not supported. • Is supported on AIX only for the legacy Console user interface and the Self Service User Interface. • Firefox 3.6 requires the Next-Generation Java™ plug-in, which is included in Java 6 Update 10 and newer version.
Google Chrome	50.0	Supported for the Identity Service Center user interface only.
	42.0	Supported for the Identity Service Center user interface only.

• IBM Security Identity Manager software distribution does not include the supported browsers.
• The IBM Security Identity Manager administrative user interface uses applets that require the Java Web Start.

- You must enable cookies in the browser to establish a session with IBM Security Identity Manager.
- Do not start two or more separate browser sessions from the same client computer. The two sessions are regarded as one session ID, which causes problems with the data.

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the Software Product Compatibility Reports page at http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

Adapter level support

The IBM Security Identity Manager installation program always installs a number of adapter profiles.

The installation program installs these profiles:
- AIX profile (UNIX and Linux adapter)
- Solaris profile (UNIX and Linux adapter)
- HP-UX profile (UNIX and Linux adapter)
- Linux profile (UNIX and Linux adapter)
- LDAP profiles (LDAP adapter)

The IBM Security Identity Manager installation program optionally installs the IBM Security Identity Manager LDAP adapter and IBM Security Identity Manager UNIX and Linux adapter. Newer versions of the adapters might be available as separate downloads. Install the new versions before you use the adapters.

Installation and configuration documentation for adapters can be found in the IBM Security Identity Manager adapter documentation at http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.itim_pim.doc/c_adapters_intro.htm.

Chapter 4. What's new in this release

The documentation updates in this library are added in the context of IBM Security Identity Manager Version 6.0.0, Fix Pack 18.

IBM Security Identity Manager Version 6.0.0, Fix Pack 18

These functions are new or changed for IBM Security Identity Manager Server Version 6.0.0, Fix Pack 18.

IBM Security Identity Manager Server

Manage Accounts enhancements
New accounts-related tasks are now available for administrators and users. Administrators can configure account categories. Users can change account categories on managed accounts, such that, accounts with categories that are configured correctly are excluded from password synchronization. See Account category management.

IBM Security Identity Manager Version 6.0.0, Fix Pack 13

IBM Security Identity Manager Server

Manage Activities enhancements
Enhancement includes displaying more information for activities for operations such as suspend, restore, modify. Earlier, activities for these operations displayed limited information. Now, you can see more and detailed information. Another enhancement about activities include the display of batch activities. To view details in a batch request, go to the activity details page.

Transfer of organizations and roles
You can transfer a business unit to an existing business unit that is under the same organization root. Optionally, you can also create a new business unit and then transfer an existing business unit for people and roles. However, there are few restrictions to transfer a business unit. For detailed information about transferring a business unit, see Transferring a business unit.

You can transfer static and dynamic roles to the business unit that is under the same organization root. However, there are few restrictions to transfer roles. For detailed information about transferring roles, see Transferring roles.

Customization of styles, icons, and labels in the Identity Service Center
Identity Service Center user interface is customizable to change icons, fonts, color, and labels. You can customize Identity Service Center user interface in the following ways:

- Copying and modifying the customizable files that are installed with IBM Security Identity Manager.
- Replacing icons and graphics.
- Applying customized styles.
- Modifying labels.

For more information, see Customization of styles, icons, and labels.

Customized self-approval for requestee and requester
Using JavaScript code, administrator can enable self-approval by requestee or requester for specific workflow even though the global configuration is set to disable the self-approval. See Customized self-approval for requestee and requester.

Running applets outside of a browser
Applets now run in the Java Web Start instead of a browser. Since Java Web Start applications can be launched independently of a browser, users need not to rely on browser plug-in.

IBM Security Identity Manager Version 6.0.0, Fix Pack 10

IBM Security Identity Manager Server

These functions are new or changed for IBM Security Identity Manager Server Version 6.0.0, Fix Pack 10:

Federal Information Processings Standards (FIPS)
By the end of 2015 because of changes in National Institute of Standards and Technology (NIST) rules, the use of IBMSecureRandom results in non-compliance with FIPS140-2 random number rules. IBM Security Identity Manager Server code is updated to use the new random number generation algorithm SHA2DRBG to be compliant with new FIPS 140-2 rule. The new algorithm is available in that default Java virtual machine (JVM) that ships with WebSphere Application Server 8.5.5.7.

Skip delegation
A new property has been added to skip delegation if the delegated approver is also the requestee. See Skip delegation when requestee is the delegated approver.

Oracle eBS responsibility support
Some adapters such as the Oracle eBS adapter support complex group attribute requests. Support for these requests requires the installation of a service profile-specific handler. For more information about handlers, see your specific adapter guide. For accesses that are related to such complex group values, typically the default subattribute values are obtained from the handler plug-in. However, if the provisioning policy for the service has a mandatory enforcement on the group attribute, that value is used instead.

Note: If you are upgrading to IBM Security Identity Manager version 6.0.0.10, you must perform a full reconciliation of the Oracle BS service to support Oracle eBS responsibility access requests.

Visual indication of adapter profile import
The administrative console provides a visual indicator for the adapter profile during the import process.

Administrative console tabbing enhancement
When too many windows were open in the administrative console, some were hidden in the toolbar tabs and could not be selected. You can now access the overflow windows, by clicking the arrow icons that are displayed when the overflow condition occurs.

New Javascript APIs are added to support assigning access by roles
The new UserAccessAccount Javascript APIs are added to get the access

ID, name, description and owner information in workflows. See
UserAccess. The new Role Javascript APIs get the parent and child roles of
a role in a workflow. See Role.

**Integration between IBM Security Identity Manager and IBM Security Identity
Governance**

IBM Security Identity Governance and Administration Data Integrator
version 7.0.3.1 allows synchronization between IBM Security Identity
Governance and IBM Security Identity Manager. The connector must be
installed and configured separately. For instructions and further
documentation, see technote 1968516 at http://www.ibm.com/support/
docview.wss?uid=swg21968516.

High Availability and Disaster Recovery

Setting up High Availability and Disaster Recovery for IBM Security
Identity Manager versions 6 and 7 VA is documented in the Best Practices
section for IBM Security Identity Manager on IBM developerWorks.

Although the deployment topology and configuration are similar to what
is recommended for IBM Tivoli Identity Manager 5.x, there are several new
features in IBM Security Identity Manager and newer versions of
middleware that enhance or simplify configuration.

- IBM Security Identity Manager 6.0 FP 4 allows a cluster node to function
  as a hot-standby node. In a hot-standby server cluster, only the primary
  nodes perform useful work. The standby node is powered on but cannot
  run scheduled jobs, reconciliations, or participate in load-balancing
  work.
- WebSphere Application Server 8.5 includes a messaging engine that is
  enhanced to be able to stop gracefully if a database failure occurs.
  Previously the failure would stop the entire JVM. After it is stopped, it
  can then be automatically re-enabled. The messaging engine uses
  multiple cores to provide quicker messaging engine start-up when large
  numbers of messages and destinations are present.
- DB2 10.1 HADR supports up to three standby databases. You can have
  two auxiliary standby databases in a second data center and keep the
  primary and principle standby database in the primary data center.
- DB2 10.1 log spooling writes the log data that is sent from the primary
  database to the disk on the standby database if the log buffer becomes
  full.

Identity Service Center user interface

These functions are new or changed for the Identity Service Center user interface
in IBM Security Identity Manager Version 6.0.0, Fix Pack 10

View Requests enhancements

- When access is added, modified, or deleted from the administrative
  console, you can view the details in the **View Requests** wizard of the
  Identity Service Center.
- If the requests are initiated from the Identity Service Center, then you
  can view all requests that are raised either by you or someone else on
  behalf of you.

Web services API enhancement

IBM Security Identity Manager web services APIs are updated. The

upgraded web services APIs are available in any fix pack that is later to the IBM Security Identity Manager 6.0.0.6.

The web services are updated for the following two functions:

- To enable the search person functionality with any person category.
- A new web service is added that provides the support to delete an organizational role.

IBM Security Identity Manager Version 6.0.0.6

Identity Service Center user interface

Note: The Identity Service Center supports Google Chrome version 42.0. See "Browser requirements for client connections" on page 14.

These functions are new or changed for the Identity Service Center user interface in IBM Security Identity Manager Version 6.0.0, Fix Pack 6:

View and Edit Profile
Depending upon the configured view, you can view or edit user profiles.

Change Password
Depending upon the configured view, you can change or reset the password, and recover the forgotten password.

Delegate Activities
Depending upon the configured view, you can delegate activities, view, edit, and delete the delegation schedule.

Enhancements to My Activities
You can view the notification on Identity Service Center home page for your pending activities. The count of pending activities is displayed.

IBM Security Identity Manager Server Version 6.0.0, Fix Pack 5

These functions are new or changed for IBM Security Identity Manager Server Version 6.0.0, Fix Pack 5:

Virtualization support for VMWare 5.5
IBM Security Identity Manager now supports VMWare 5.5. See "Virtualization support" on page 6.

Java Runtime Environment (JRE) support
The JRE is installed with WebSphere Application Server. Some JRE versions are not supported. See "WebSphere Application Server support" on page 8.

New password complexity category: "3 of 4"
A new password complexity category specifies that a user's password contain characters from three of four categories. The complexity category enables password complexity requirements in Microsoft Active Directory. Documentation for this capability is in the online help where you set password requirements.

Workflow options

Options are added to nodes to allow finer control over workflow processing.

The following options are added for approval, RFI, and work order nodes:

- **Skip Escalation**

- **No Timeout Action**
- **Complete on Timeout**

See Common attributes for workflow activities.

The following options are added for loop nodes:

- **Asynchronous Processing of the Loop Body**

See Loop node.

A flow diagram that details the influence of the properties is added to Escalation.

A new workflow extension is added that pauses a workflow for a specified time. When the specified time is reached, the extension activity is complete and the workflow continues.

See Wait extension.

A new option is added to enable requesters to self-approve their requests. Previously, if the requester is also the approver or in the approver group, the requester is always skipped by the workflow for approval. With the new property `enrole.workflow.selfapproval`, users can set its value to `true` so the workflow routes the approval request to the requester.

See Self-approval for requester

IBM Security Identity Manager version 6.0.0.5

These functions are new or changed for IBM Security Identity Manager Server Version 6.0.0, Fix Pack 5:

Upgrading: Migration from Microsoft SQL Server database to IBM DB2 database
The Identity Service Center (ISC) user interface is not supported on the Microsoft SQL Server database in IBM Security Identity Manager Version 6.0.0.4 and later.

Important: You must migrate the database before you upgrade to Version 6.0.0.4 or later from Version 5, Version 6.0.0, or Version 6.0.0.1.

Process overview:
1. Upgrade from IBM Security Identity Manager Version 5 to IBM Security Identity Manager Version 6.0.0. Skip this step if you are already running Version 6.0.0 or Version 6.0.0.1.
2. Migrate the database from Microsoft SQL Server to IBM DB2.
3. Upgrade WebSphere Application Server to Version 8.5.
4. Upgrade to IBM Security Identity ManagerVersion 6.0.0.4 or later.

See Migrating from Microsoft SQLServer to DB2 when upgrading from IBM Tivoli Identity Manager Version 5.

Auditing: Excluding long attributes from the audit process
An auditing process fails if it encounters attribute values longer than 4000 bytes. You can now modify entities of type **Person**, **Business Partner Person**, and **Account** to exclude long attributes from the auditing process. This action is typically necessary if an attribute value contains a long description or an image (for example, a picture of a person).

See Attribute auditing for details.

IBM Security Identity Manager Version 6.0.0.4

Identity Service Center user interface

These functions are new or changed for the Identity Service Center user interface in IBM Security Identity Manager Version 6.0.0, Fix Pack 4:

Edit and Delete Access
Depending upon the configured view, you can edit and delete the access for yourself and others. For more information, see the following documentation.

- Editing accesses in Identity Service Center
- Deleting accesses in the Identity Service Center

Subform support for the Identity Service Center
You can use subforms in the Identity Service Center to customize the user interface for complex multivalued attributes.

For more information about the deployment path of the Identity Service Center subforms, see the IBM Security Identity Manager adapters documentation for Oracle eBS and PeopleTools at http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.itim_pim.doc/c_adapters_intro.htm.

Enhancement to Manage Activities and View Access
With the Manage Activities flow, you can view the activities in the summary view and detailed view.

With the View Access flow, you can view the access list with the refined categories.

Launch the IBM Security Identity Governance home page from the Identity Service Center home page
The Security Identity Governance capabilities are achieved through the IBM Security Identity Governance adapter. The capability can be linked into the Identity Service Center through a custom task. You can create a custom task to link to the Security Identity Governance home page from the Identity Service Center. For more information, see Launching the IBM Security Identity Governance home page from the Service Center.

Custom tasks in the Identity Service Center
The following scenarios are shown as custom tasks in the Identity Service Center home page:

- Change Password
- View and Edit Profile
- Delegate Activities

After you select a custom task, the self-care user interface is displayed, in which you can complete the tasks. You cannot start the self-service user interface directly.

IBM Security Identity Manager Server Version 6.0.0, Fix Pack 4

These functions are new or changed for IBM Security Identity Manager Server Version 6.0.0, Fix Pack 4:

Creating a new service: turning off provisioning policies
You can now choose to defer provisioning a new service with a default policy. You might not want to create a default policy when a new service is

created if the amount of time to evaluate the default policy for all users is significant. For more information, see Default settings for provisioning policy when a new service is created.

Concurrency: handle conflict resolution during account provisioning
In certain cases multiple simultaneous operations on the same account during auto-provisioning might result in an undesired result or a failed request to add an account. Options are added to specify what to do when conflicts are encountered. For more information, see Concurrency properties.

Workflows: new scenario supports role removal requests
The `ApproveRolesWithOperation` workflow now handles role removal requests. See the workflows sample file that is provided with the product for information on how to set it up. For more information and other sample workflows, see Sample workflows.

Reconciliation properties: new extension allows you to determine how information about detected account changes is stored
A new extension allows you to determine how to store account change information that is detected during reconciliation. This aspect can help you customize the format of attribute value changes. It can improve reconciliation report readability.

The new property `enrole.reconciliation.accountChangeFormatter` takes a fully qualified class name that you created to handle how account change information is handled. For more information, see Reconciliation properties.

Integration between IBM Security Identity Manager and IBM Security Identity Governance
IBM Security Identity Governance and Administration Data Integrator version 7.0.1 allows access to IBM Security Identity Governance from IBM Security Identity Manager. The connector must be installed and configured separately. For instructions and further documentation, see technote 1688802 at http://www.ibm.com/support/docview.wss?uid=swg21688802.

Pre-upgrade requirements for Java applications
Critical: New and existing applications must use the new WebSphere Application Server authentication APIs. Do not attempt to upgrade until *after* you modified your existing applications. The existence of the old APIs causes the upgrade to fail. For more information, see Pre-upgrade requirements for modifying your Java applications to use new authentication methods.

The following resources can help you with the transition:
- A new technote 1688801 contains more information about the customization areas that are affected and how custom applications are supported. In general, you need to engage services to help you work with your custom applications.
- The `examples` directory in your product installation includes an updated `self_care` example application that uses the WebSphere Application Server authentication API.
- The `docs` directory in your product installation includes an updated `applications` document that includes an example of using the WebSphere Application Server authentication API.
- The JavaDocs included in the product installation provides details on classes and methods.

- The IBM developerWorks® section for IBM Security Identity Manager provides additional support. Follow the **Product support** link at the bottom of the page.

High Availability and Disaster Recovery

Setting up High Availability and Disaster Recovery for IBM Tivoli Identity Manager version 5.x is documented in the Best Practices section for IBM Security Identity Manager on IBM developerWorks.IBM Security Identity Manager allows separate nodes of a cluster to function as hot-standby nodes. Typically the nodes are geographically separate for a disaster recovery application. You also use hot-standby nodes for testing applications on the node without interfering with other nodes.

Implementation of this capability is discussed on the IBM developerWorks site at Setting up HA and DR environments for ITIM 5.x. You can also use the setup instructions with IBM Security Identity Manager Version 6 and Version 7.0 VA.

The `enroleStartup.properties` file is modified for this capability. See the **Reference** > **Supplemental property files** for enroleStartup.properties. Note the following changes for this release:

- The `enroleStartup.properties` file can be modified starting in this release. It was not modifiable in previous releases.
- The following new and changed properties play a role in High Availability and Disaster Recovery applications:

```
enrole.startup.MessageListeners.attributes
enrole.appServer.standby
enrole.appServer.standby.inactiveMessageListeners
enrole.appServer.standby.inactiveStartupInitializer
```

Integration with IBM® Control Desk

The IBM Security Identity Manager integration for IBM® Control Desk section now points to Chapter 19 of the Redbook Tivoli Integration Scenarios for instructions in setting up the integration.

Migration from Microsoft SQL Server database to IBM DB2 database

Consult technote 1695611 for instructions on how to migrate your IBM Security Identity Manager database from Microsoft SQL Server to IBM DB2.

Shared Access

Shared Access functions have moved to the IBM Security Privileged Identity Manager product. For information about integrating Privileged Identity Manager with Security Identity Manager, see:

- Features overview
- Integration with IBM Security Identity Manager
- Scenario: Integration with IBM Security Identity Manager

Shared Access Reports

Support of shared access reports is now available in the IBM Security Privileged Identity Manager reporting package. For more information, see the "Report administration" section of the *IBM Security Privileged Identity Manager Administrator Guide* at http://www.ibm.com/support/knowledgecenter/SSRQBP_1.0.1.1/ com.ibm.ispim.doc_1.0.1.1/admin_guide/concepts/cpt_ic_reports_oview.html.

Reports

The following function is new or changed for the IBM Security Identity Manager Version 6.0.0, Fix Pack 4:

New access audit model and report for Identity Service Center
>   The new access audit model and report are developed for the Identity Service Center. An old access audit model is renamed to Access Audit (Deprecated).
>
>   For more information, see Access Audit namespace.

Documentation

PDF documentation available in English only
>   PDF copies of the documentation are provided as a convenience, and thus linking in the PDF files is not fully functional. When you click a cross-reference link that is in another PDF file, the link does not work. The PDF documentation is available at http://www.ibm.com/support/docview.wss?uid=swg21688805.

Instructions for creating PDF files from the Knowledge Center
>   You can create PDF files from the content collections in the IBM Knowledge Center. For more information, see http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#create.

IBM Security Identity Manager Version 6.0.0.3

Identity Service Center user interface

Note: The Identity Service Center does not support Microsoft SQL Server database. Use DB2 Universal Database™ or Oracle database instead.

Unified access catalog
>   The Identity Service Center user interface contains a unified access catalog that provides sets of tasks, each tailored for the needs of the default user types:
>   - System administrator
>   - Manager
>   - Employee
>   - Auditor

Enhanced user experience
>   The Identity Service Center gives you an enhanced user experience that is tailored to your business goals:
>   - Request access to applications
>   - View your requests
>   - View accesses for yourself and others (new for Fix Pack 3)
>   - Manage your activities (new for Fix Pack 3)
>   - Request access for yourself (new for Fix Pack 3)

Modern, intuitive, and efficient user interface
>   You can model your business goals and user interface with a dedicated flow. The Identity Service Center has:
>   - Type-ahead search
>   - Guided tasks

- Usable layout
- Work flow and tasks that are applicable to your business goals
- Context-sensitive help

Customizable user interface

System administrators can easily customize the Identity Service Center user interface either by copying and modifying the customizable files that are installed with IBM Security Identity Manager. They can also customize the new user interface by replacing the icons and graphics. See the "Identity Service Center user interface customization" section of the *IBM Security Identity Manager Configuration Guide* for details.

These functions are new or changed for the Identity Service Center user interface in IBM Security Identity Manager Version 6.0.0, Fix Pack 3:

View Access (Self and Others)

You can view the list of your current accesses or the accesses that are in the process of being approved. You can view accesses either for yourself or for the employees that you are entitled to view. You can search, sort, and filter the list of accesses as needed. Inactive or noncompliant accesses are identified.

Request Access (Self)

You can request access for yourself.

For more information, see "Requesting access for yourself with the Identity Service Center" in the *IBM Security Identity Manager Scenarios Guide*.

Manage Activities (Self)

You can manage approval activities through the Identity Service Center. You can search, sort, and filter your pending activities. Activities are highlighted if they are locked, escalated, or approaching their due date.

You can also select multiple approval activities to act on at the same time. Nonapproval activities and detail information are also displayed in the Identity Service Center. However, you must act on nonapproval activities individually and are redirected to the self-service user interface.

For more information, see the following documentation:
- "Managing approval activities" in the *IBM Security Identity Manager Scenarios Guide*
- "Managing multiple activities" in the *IBM Security Identity Manager Scenarios Guide*

Launch the administrative console from the Identity Service Center home page

You can launch the IBM Security Identity Manager admin console as a custom task from the Identity Service Center home page.

IBM Security Identity Manager

These functions are new or changed for IBM Security Identity Manager Version 6.0.0, Fix Pack 3:

Improved performance and scalability

Performance and scalability is enhanced to support large numbers of accounts per person.

Provide justification for canceled requests

When you cancel a request, you can now provide the justification for a canceled request and view the justification in all three user interfaces.

For more information, see the following documentation:
- "Configuring the Justification field in the user interface" in the *IBM Security Identity Manager Configuration Guide*
- "Required field properties" in the *IBM Security Identity Manager Reference Guide*
- "ui.properties" in the *IBM Security Identity Manager Reference Guide*

Audit canceled requests

You can view canceled requests in the admin console, the self-service user interface, and the Identity Service Center user interface. You can also configure the email notification template to include canceled requests that contain cancellation information such as who canceled the request, when it was canceled, and the reason it was canceled.

For more information, see the following documentation:
- "Canceling pending requests" in the *IBM Security Identity Manager Administration Guide*
- "Manually applying the email notification template changes for canceling a request" in the *IBM Security Identity Manager Administration Guide*
- "Email notification template for canceling requests is not applied after installing Fix Pack 6.0.0.3" in the *IBM Security Identity Manager Administration Guide*
- "Request for information (RFI) states" in the *IBM Security Identity Manager Administration Guide*
- "ACTIVITY table" in the *IBM Security Identity Manager Database and Directory Server Schema Reference Guide*
- "Workflow default messages" in the *IBM Security Identity Manager Reference Guide*

Manage provisioning policies associated with a role

In the admin console, you can now view and manage provisioning policies that are associated with a role. On the Manage Roles page in the admin console, you can select the new **Manage Provisioning Policies** menu item. On the Work With Provisioning Policies page in the admin console, you can filter the list of policies based on the role search filter.

For more information, see "Managing provisioning policies by role" in the *IBM Security Identity Manager Administration Guide*.

Configuration of the user interface to display the group description

You can use the form designer in the admin console to specify the description attribute for groups. This enables the display of the group description in the search results table for groups on a form. The group description is displayed in the search results table for groups when you request an account using the admin console or the self-service user interface. In the Identity Service Center, the group description is displayed in the search results table for groups when you request an access.

For more information, see the following documentation:
- "Customizing an account request" in the *IBM Security Identity Manager Configuration Guide*
- "Control types used by the form designer" in the *IBM Security Identity Manager Configuration Guide*

Access control item (ACI) enhancement for nonadministrators to perform life cycle operations

Users that do not have IBM Security Identity Manager administrator privileges can now perform life cycle operations.

For more information, see the following documentation:

- "Operations management" in the *IBM Security Identity Manager Configuration Guide*
- "Access control item management" in the *IBM Security Identity Manager Administration Guide*
- "Specifying a custom operation and its access control item" in the *IBM Security Identity Manager Configuration Guide*

New API in JavaScript extension DirectoryObject to remove properties

You can now remove individual attribute values from directory objects in the JavaScript extension DirectoryObject.

For more information, see "DirectoryObject.removeProperty(name,value)" in the *IBM Security Identity Manager Reference Guide*.

New API in JavaScript extension for traversing the workflow process hierarchy

Prior to Fix Pack 3, the JavaScript API let you navigate from the child workflow process upward by using process.getParent() or process.getRootProcess(). However, you could not traverse the process tree in the other direction. Fix Pack 3 includes process.getSubProcesses() and activity.getSubProcesses() that return the child processes of the given process and activity, respectively.

For more information, see "Process.getSubProcesses()" and "Activity.getSubProcesses()" in the *IBM Security Identity Manager Reference Guide*.

Dutch and Turkish languages are now supported

For more information, see Chapter 8, "Language support," on page 69.

Reports

These functions are new or changed for the IBM Security Identity Manager Version 6.0.0, Fix Pack 3 reports:

Shared Access Reports moved to IBM Security Privileged Identity Manager

Support of shared access reports is now available in the IBM Security Privileged Identity Manager reporting package.

For more information, see the "Report administration" section of the *IBM Security Privileged Identity Manager Administrator Guide* at http://www.ibm.com/support/knowledgecenter/SSRQBP_1.0.1.1/ com.ibm.ispim.doc_1.0.1.1/admin_guide/concepts/ cpt_ic_reports_oview.html.

User Access Report

The User Access Report provides information about the different users in a business unit and all accesses that they are entitled to. The report:

- Lists all accesses and their corresponding users (entitlement details)
- Lists all users and their corresponding accesses (entitlement details)

For more information, see "User Access Report" in the *IBM Security Identity Manager Administration Guide*.

Enhancement to IBM Security Identity Manager Dashboard

The dashboard user experience is improved. A detail tab view shows compliance charts with dynamic filtering capability to render charts that are based on user input.

For more information, see "IBM Security Identity Manager Dashboard" in the *IBM Security Identity Manager Administration Guide*.

IBM Security Identity Manager version 6.0.0.2

Note:

The documentation updates in this library are added in the context of the IBM Security Identity Manager, version 6.0.0, Fix Pack 2.

The Identity Service Center, Cognos Reporting, and selected Shared Access features can only be available in your system after you install the fix pack.

Identity Service Center user interface

IBM Security Identity Manager introduces the Identity Service Center, a new user interface, which provides the capability for managers or individuals to request access for individuals.

IBM Cognos reporting framework

IBM Security Identity Manager provides the Cognos reporting framework to create and analyze reports. You can modify the schema and generate reports in different formats.

IBM Security Identity Manager Version 6.0

Account ownership type

New account ownership types separate personal accounts from custodial accounts.

Shared access module

IBM Security Identity Manager provides a shared access module that extends the identity and access management governance capabilities by supporting privileged identity management.

Role management

Role management now includes management of extended role attributes and role assignment attributes.

Service management and provisioning

Service management and provisioning now supports a new account form, an advanced connection mode, new service status information, and service tagging.

Account and access management

IBM Security Identity Manager extends account and access management to support multiple access levels, and to support account search in the self service console.

Authentication with an external user registry configured with WebSphere Application Server

IBM Security Identity Manager authentication mechanism is integrated with the container-based security capabilities of WebSphere Application Server

Vertical cluster support

You can now install IBM Security Identity Manager in a WebSphere deployment that uses vertical clusters.

Application programming interfaces

IBM Security Identity Manager supports additional application programming interfaces.

Report data synchronization enhancements

Report data synchronization was redesigned to improve performance, and a new utility provides remote data synchronization capability.

Health monitoring

IBM Security Identity Manager server is enhanced to provide deployment health monitoring features. These features include monitoring of performance and availability of various requests in the key components.

Chapter 5. Known limitations, problems, and workarounds

You can view the known software limitations, problems, and workarounds on the IBM Security Identity Manager Support site.

The Support site describes not only the limitations and problems that exist when the product is released, but also any additional items that are found after product release. As limitations and problems are discovered and resolved, the IBM Software Support team updates the online knowledge base. By searching the knowledge base, you can find workarounds or solutions to problems that you experience.

The following link launches a customized query of the live Support knowledge base for items specific to version 6.0:

IBM Security Identity Manager Version 6.0 technotes

From the **Product support content** menu, select the type of information you are looking for, such as **Flashes, alerts and bulletins**, or **Troubleshooting documentation**.

To create your own query, go to the Advanced search page on the IBM Software Support website.

Chapter 6. Features overview

IBM Security Identity Manager delivers simplified identity management capabilities in a solution that is easy to install, deploy, and manage.

IBM Security Identity Manager provides essential password management, user provisioning, and auditing capabilities.

Access management

In a security lifecycle, IBM Security Identity Manager and several other products provide access management. You can determine who can enter your protected systems. You can also determine what can they access, and ensure that users access only what they need for their business tasks.

Access management addresses three questions from the business point of view:
- Who can come into my systems?
- What can they do?
- Can I easily prove what they did with that access?

These products validate the authenticity of all users with access to resources, and ensure that access controls are in place and consistently enforced:
- IBM Security Identity Manager

  Provides a secure, automated, and policy-based user management solution that helps effectively manage user identities throughout their lifecycle across both legacy and e-business environments. IBM Security Identity Manager provides centralized user access to disparate resources in an organization, with policies and features that streamline operations associated with user-resource access. As a result, your organization realizes numerous benefits, including:
  - Web self-service and password reset and synchronization; users can self-administer their passwords with the rules of a password management policy to control access to multiple applications. Password synchronization enables a user to use one password for all accounts that IBM Security Identity Manager manages.
  - Quick response to audits and regulatory mandates
  - Automation of business processes related to changes in user identities by providing lifecycle management
  - Centralized control and local autonomy
  - Enhanced integration with the use of extensive APIs
  - Choices to manage target systems either with an agent or agentless approach
  - Reduced help desk costs
  - Increased access security through the reduction of orphaned accounts
  - Reduced administrative costs through the provisioning of users with software automation
  - Reduced costs and delays associated with approving resource access to new and changed users
- IBM Security Access Manager

  Enables your organization to use centralized security policies for specified user groups to manage access authorization throughout the network, including the

vulnerable, internet-facing web servers. IBM Security Access Manager can be tightly coupled with IBM Security Identity Manager to reconcile user groups and accounts managed by IBM Security Access Manager with the identities managed by IBM Security Identity Manager to provide an integrated solution for resource access control.

IBM Security Access Manager delivers:

– Unified authentication and authorization access to diverse web-based applications within the entire enterprise
– Flexible single sign-on to web, Microsoft, telnet and mainframe application environments
– Rapid and scalable deployment of web applications, with standards-based support for Java Platform, Enterprise Edition (Java EE) applications
– Design flexibility through a highly scalable proxy architecture and easy-to-install web server plug-ins, rule- and role-based access control, support for leading user registries and platforms, and advanced APIs for customized security

• IBM Security Federated Identity Manager

Handles all the configuration information for a federation across organizational boundaries, including the partner relationships, identity mapping, and identity token management.

IBM Security Federated Identity Manager enables your organization to share services with business partner organizations and obtain trusted information about third-party identities such as customers, suppliers, and client employees. You can obtain user information without creating, enrolling, or managing identity accounts with the organizations that provide access to services that are used by your organization. So, users are spared from registering at a partner site, and from remembering additional logins and passwords. The result is improved integration and communication between your organization and your suppliers, business partners, and customers.

For more information about how access management products fit in larger solutions for a security lifecycle, see the IBM Security Management website: http://www.ibm.com/security/

IBM Redbooks® and Redpapers also describe implementing IBM Security Identity Manager within a portfolio of IBM security products.

Support for corporate regulatory compliance

IBM Security Identity Manager provides support for corporate regulatory compliance.

Compliance areas

Security Identity Manager addresses corporate regulatory compliance in the following key areas:

• Provisioning and the approval workflow process
• Audit trail tracking
• *Enhanced* compliance status
• Password policy and password compliance
• Account and access provisioning authorization and enforcement
• Recertification policy and process

- Reports

Provisioning and the approval workflow process

Security Identity Manager provides support for provisioning, for user accounts and for access to various resources. Implemented within a suite of security products, Security Identity Manager plays a key role to ensure that resources are provisioned only to authorized persons. Security Identity Manager safeguards the accuracy and completeness of information processing methods and granting authorized users access to information and associated assets. Security Identity Manager provides an integrated software solution for managing the provisioning of services, applications, and controls to employees, business partners, suppliers, and others associated with your organization across platforms, organizations, and geographies. You can use its provisioning features to control the setup and maintenance of user access to system and account creation on a managed resource.

At its highest level, an identity management solution automates and centralizes the process of provisioning resources. The solution includes operating systems and applications, and people in, or affiliated with, an organization. Organizational structure can be altered to accommodate the provisioning policies and procedures. However, the organization tree used for provisioning resources does not necessarily reflect the managerial structure of an organization. Administrators at all levels can use standardized procedures for managing user credentials. Some levels of administration can be reduced or eliminated, depending on the breadth of the provisioning management solution. Furthermore, you can securely distribute administration capabilities, manually or automatically, among various organizations.

The approval process can be associated with different types of provisioning requests, including account and access provisioning requests. Lifecycle operations can also be customized to incorporate the approval process.

Models for provisioning

Depending on business needs, Security Identity Manager provides alternatives to provision resources to authorized users on *request-based*, *role-based*, or *hybrid* models.

Approval workflows

Account and access request workflows are started during account and access provisioning. You typically use account and access request workflows to define approval workflows for account and access provisioning.

Account request workflows provide a decision-based process to determine whether the entitlement provided by a provisioning policy is granted. The entitlement provided by a provisioning policy specifies the account request workflow that applies to the set of users in the provisioning policy membership. Multiple provisioning policies might apply to the same user for the same service target. There might also be different account request workflows in each provisioning policy. The account request workflow for the user is based on the priority of the provisioning policy. If a provisioning policy has no associated workflow and the policy grants an account entitlement, the operations that are related to the request run immediately. For example, an operation might add an account.

However, if a provisioning policy has an associated workflow, that workflow runs before the policy grants the entitlement. If the workflow returns a result of `Approved`, the policy grants the entitlement. If the workflow has a result of `Rejected`, the entitlement is not granted. For example, a workflow might require a manager's approval. Until the approval is submitted and the workflow completes, the account is not provisioned. When you design a workflow, consider the intent of the provisioning policy and the purpose of the entitlement itself.

Tracking

Security Identity Manager provides audit trail information about how and why a user has access. On a request basis, Security Identity Manager provides a process to grant, modify, and remove access to resources throughout a business. The process provides an effective audit trail with automated reports.

The steps involved in the process, including approval and provisioning of accounts, are logged in the request audit trail. Corresponding audit events are generated in the database for audit reports. User and Account lifecycle management events, including account and access changes, recertification, and compliance violation alerts, are also logged in the audit trail.

Enhanced compliance status

Security Identity Manager provides enhanced compliance status on items such as dormant and orphan accounts, provisioning policy compliance status, recertification status, and various reports.

- **Dormant accounts**. You can view a list of dormant accounts with the Reports feature. Security Identity Manager includes a dormant account attribute to service types that you can use to find and manage unused accounts on services.
- **Orphan accounts**. Accounts on the managed resource whose owner in the Security Identity Manager Server cannot be determined are *orphan accounts*. These accounts are identified during reconciliation when the applicable adoption rule cannot successfully determine the owner of an account.
- **Provisioning policy compliance status.** The compliance status based on the specification of provisioning policy is available for accounts and access. An account can be either compliant, non-compliant with attribute value violations, or disallowed. An access is either compliant or disallowed.
- **Recertification status**. The recertification status is available for user, account, and access target types, which indicates whether the target type is certified, rejected, or never certified. The timestamp of the recertification is also available.

Password policy and password compliance

Use Security Identity Manager to create and manage password policies. *password policy* defines the password strength rules that are used to determine whether a new password is valid. A *password strength rule* is a rule to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be five. The rule might specify that the maximum number of characters must be 10.

The Security Identity Manager administrator can also create new rules to be used in password policies.

If password synchronization is enabled, the administrator must ensure that password policies do not have any conflicting password strength rules. When

password synchronization is enabled, Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

Provisioning policy and policy enforcement

A *provisioning policy* grants access to many types of managed resources, such as Security Identity Manager server, Windows NT servers, and Solaris servers.

Provisioning policy parameters help system administrators define the attribute values that are required and the values that are allowed.

Policy enforcement is the manner in which Security Identity Manager allows or disallows accounts that violate provisioning policies.

You can specify one of the following policy enforcement actions to occur for an account that has a noncompliant attribute.

Mark Sets a mark on an account that has a noncompliant attribute.

Suspend
Suspends an account that has a noncompliant attribute.

Correct
Replaces a noncompliant attribute on an account with the correct attribute.

Alert Issues an alert for an account that has a noncompliant attribute.

Recertification policy and process

A *recertification policy* includes activities to ensure that users provide confirmation that they have a valid, ongoing need for the target type specified (user, account, and access). The policy defines how frequently users must validate an ongoing need. Additionally, the policy defines the operation that occurs if the recipient declines or does not respond to the recertification request. Security Identity Manager supports recertification policies that use a set of notifications to initiate the workflow activities that are involved in the recertification process. Depending on the user response, a recertification policy can mark a user's roles, accounts, groups, or accesses as recertified. The policy can suspend or delete an account, or delete a role, group, or access.

Audits that are specific to recertification are created for use by several reports that are related to recertification:

Accounts, access, or users pending recertification
Provides a list of recertifications that are not completed.

Recertification history
Provides a historical list of recertifications for the target type specified.

Recertification policies
Provides a list of all recertification policies.

User recertification history
Provides history of user recertification.

User recertification policy
Provides a list of all user recertification policies.

Reports

Security administrators, auditors, managers, and service owners in your organization can use one or more of the following reports to control and support corporate regulatory compliance:

- Accesses Report, which lists all access definitions in the system.
- Approvals and Rejections Report, which shows request activities that were either approved or rejected.
- Dormant Accounts Report, which lists the accounts that were not used recently.
- Entitlements Granted to an Individual Report, which lists all users with the provisioning policies for which they are entitled.
- Noncompliant Accounts Report, which lists all noncompliant accounts.
- Orphan Accounts Report, which lists all accounts not having an owner.
- Pending Recertification Report, which highlights recertification events that can occur if the recertification person does not act on an account or access. This report supports filtering data by a specific service type or a specific service instance.
- Recertification Change History Report, which shows a history of accesses (including accounts) and when they were last recertified. This report serves as evidence of past recertifications.
- Recertification Policies Report, which shows the current recertification configuration for a specific access or service.
- Separation of Duty Policy Definition Report, which lists the separation of duty policy definitions.
- Separation of Duty Policy Violation Report, which contains the person, policy, rules violated, approval, and justification (if any), and who requested the violating change.
- Services Report, which lists services currently defined in the system.
- Summary of Accounts on a Service Report, which lists a summary of accounts on a specified service defined in the system.
- Suspended Accounts Report, which lists the suspended accounts.
- User Recertification History Report, which lists the history of user recertifications done manually (by specific recertifiers), or automatically (due to timeout action).
- User Recertification Policy Definition Report, which lists the user recertification policy definitions.

All reports are available to all users when the appropriate access controls are configured. However, certain reports are designed specifically for certain types of users.

Table 10. Summary of reports

Designed for	Available reports
Security administrators	- Dormant Accounts - Orphan Accounts - Pending Recertification - Recertification History - Recertification Policies - User Recertification History - User Recertification Policies

Table 10. Summary of reports (continued)

Designed for	Available reports
Managers	• Pending Recertification • Recertification History • Recertification Policies • User Recertification History • User Recertification Policies
Service owners	• Dormant Accounts • Orphan Accounts • Pending Recertification • Recertification History • Recertification Policies • User Recertification History • User Recertification Policies
Auditors	• Dormant Accounts • Orphan Accounts • Pending Recertification • Recertification History • Recertification Policies • User Recertification History • User Recertification Policies
End users, help desk, and developers	None

Identity governance

IBM Security Identity Manager extends the identity management governance capabilities with a focus on operational role management. Using roles simplifies the management of access to IT resources.

Identity governance includes these Security Identity Manager features:

Role management
> Manages user access to resources, but unlike user provisioning, role management does not grant or remove user access. Instead, it sets up a role structure to do it more efficiently.

Entitlement management
> Simplifies access control by administering and enforcing fine-grained authorizations.

Access certification
> Provides ongoing review and validation of access to resources at role or entitlement level.

Privileged user management
> Provides enhanced user administration and monitoring of system or administrator accounts that have elevated privileges.

Separation of duties
> Prevents and detects business-specific conflicts at role or entitlement level.

These Security Identity Manager features can be augmented by IBM Security Identity Governance for greater governance capabilities.

User interface options

IBM Security Identity Manager has separate user interfaces that show users only the tasks that they need to complete, based on their user role.

The interfaces are separate, and users access them through different web addresses. IBM Security Identity Manager has these types of user interfaces:

- Administrative console interface
- Self-care interface
- Identity Service Center interface

Administrative console user interface

The administrative console user interface provides an advanced set of administrative tasks, and has new multitasking capabilities.

Persona-based console customization

The administrative console user interface contains the entire set of administrative tasks, such as managing roles, policies, and reports. This persona-based console provides sets of tasks, each tailored for the needs of the default administrative user types:

- System administrator
- Privileged administrator
- Service owner
- Help desk assistant
- Auditor
- Manager

System administrators can easily customize which tasks the different types of users can do. To control user access to accounts and tasks, for example, use a default set of user groups, access control items, and views. You can also customize user access by defining additional user groups, views, and access control items.

Multitasking control

Wizards within the administrative console user interface expedite the administrative tasks of adding users, requesting accounts, and creating new services. The administrator can concurrently manage several tasks.

Advanced search capability

The administrative console user interface also provides a powerful advanced search feature.

Self-care user interface

The self-care user interface provides a simpler subset of personal tasks that apply only to the user. With the IBM Security Identity Manager self-care interface, users can update their personal information and passwords. Users can view requests, complete and delegate activities, and request and manage their own accounts and access.

The self-care user interface provides a central location for users to do various simple, intuitive tasks.

From the self-care home page, the following task panels are available, depending on the authority the system administrator granted.

Action Needed
A list of tasks that require completion.

My Password
A list of tasks to change passwords. If password synchronization is enabled, users can enter one password that is synchronized for all of their accounts. A user can reset a forgotten password by successfully responding to forgotten password questions, if forgotten password information is configured in the system.

My Access
A list of tasks to request and manage access to folders, applications, roles, and other resources.

My Profile
A list of tasks to view or update personal information.

My Requests
A list of tasks to view requests that a user submitted.

My Activities
A list of activities that require user action. Users can also delegate activities.

Privileged users can also check out and check in credentials from the self-care user interface.

Identity Service Center user interface

The Identity Service Center user interface provides a unified catalog that makes manager tasks and user tasks simple and straightforward.

Edit and Delete Access
Depending upon the configured view, you can edit access, edit service access categories, and delete the access for yourself and others. For more information, see the following documentation.
- Editing accesses in Identity Service Center
- Editing service access categories in Identity Service Center
- Deleting accesses in the Identity Service Center

Subform support for the Identity Service Center
You can use subforms in the Identity Service Center to customize the user interface for complex multivalued attributes.

For more information about the deployment path of the Identity Service Center subforms, see the IBM Security Identity Manager adapters documentation for Oracle eBS and PeopleTools at https://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm?cp=SSRMWJ_6.0.0.18.

Configurable and extensible

You can use the Identity Service Center to have a tailored user experience:
- Use the default Identity Service Center features and add to it
- Edit the custom tasks

- Add your own custom tasks

See Identity Service Center user interface customization.

Request Access wizard

The Identity Service Center has a Request Access wizard where users can process new accesses such as role membership, accounts, and access entitlements.

It also supports batch requests by allowing the users to build up a list of items that are requested at the same time. For example, a member moves into a new role from one department to another, and the manager wants to give access to certain systems or applications.

The user can follow the basic steps to use the wizard effectively:

1. Select a person for whom you want to request access.
2. Select one or more accesses to request for that person.
3. Provide the required information, such as justification, account details, account category, or passwords.
4. Submit the request.
5. View a submission confirmation and status page.

View Requests

You can use the Identity Service Center to view the status of the requests that you made.

View Accesses

You can use the Identity Service Center to view the accesses to folders, applications, roles, and other resources that are already granted to a user. Access requests that are pending in the approval process are also listed and information about whether the accesses are inactive or non-compliant. With the View Access flow, you can view the access list with the refined categories.

Manage Activities

You can view and manage the activities that are assigned to you.

With the Manage Activities flow, you can view the activities in the summary view and detailed view.

You can use the Identity Service Center to approve or reject individual approval activities.

You can use the Identity Service Center to approve or reject multiple approval activities at the same time. You can approve or reject several individual approval activities or all the approval activities on the page.

Launch the IBM Security Identity Governance home page from the Identity Service Center home page

The Security Identity Governance capabilities are achieved through the IBM Security Identity Governance adapter. The capability can be linked into the Identity Service Center through a custom task. You can create a custom task to link to the Security Identity Governance home page from the Identity Service Center. For more information, see Launching the IBM Security Identity Governance home page from the Service Center.

Custom tasks in the Identity Service Center

The following scenarios are shown as custom tasks in the Identity Service Center home page:

- Change Password
- Change Access Password
- View and Edit Profile
- Delegate Activities

Recertification

IBM Security Identity Manager Server recertification simplifies and automates the process of periodically revalidating users, accounts, and accesses.

The recertification process automates validating that users, accounts, and accesses are still required for a valid business purpose. The process sends recertification notification and approval events to the participants that you specify.

Reporting

IBM Security Identity Manager reports reduce the time to prepare for audits and provide a consolidated view of access rights and account provisioning activity for all managed people and systems.

A *report* is a summary of Security Identity Manager activities and resources. You can generate reports based on requests, user and accounts, services, or audit and security.

Report data is staged through a data synchronization process. The process gathers data from the Security Identity Manager directory information store and prepares it for the reporting engine. Data synchronization can be run on demand, or it can be scheduled to occur regularly.

Report accessibility
> The Security Identity Manager reports are accessible in the PDF format.

The following categories of reports are available:

Requests
> Reports that provide workflow process data, such as account operations, approvals, and rejections.

User and Accounts
> Reports that provide data about users and accounts. For example: individual access rights, account activity, pending recertifications, and suspended individuals.

Services
> Reports that provide service data, such as reconciliation statistics, list of services, and summary of accounts on a service.

Audit and Security
> Reports that provide audit and security data, such as access control information, audit events, and noncompliant accounts.

Static and dynamic roles

IBM Security Identity Manager provides static and dynamic roles.

In static organizational roles, assigning a person to a static role is a manual process.

In the case of a dynamic role, the scope of access can be to an organizational unit only or to the organizational unit and its subunits. Dynamic organizational roles use valid LDAP filters to set a user's membership in a specific role. For example, a dynamic role might use an LDAP filter to provide access to specific resources to users who are members of an auditing department named audit123. For example, type:

```
(departmentnumber=audit123)
```

Dynamic organizational roles are evaluated at the following times:
- When a new user is created in the Security Identity Manager system
- When a user's information, such as title or department membership, changes
- When a new dynamic organizational role is created

Self-access management

IBM Security Identity Manager allows users and administrators the ability to request and manage access to resources such as shared folders, email groups, or applications.

Access differs from an account. An account exists as an object on a managed service. An access is an entitlement to use a resource, such as a shared folder, on the managed service. The ability to access a resource is based on the attributes of the group to which the user account belongs. The user's access to a resource is therefore dependent on the account and its group mapping. When an account is suspended, their access becomes inactive; similarly, when an account is restored, their access becomes active again. When an account is deleted, access to the resource for that user is deleted. When a group is removed from the service, the user access that maps to that group is also removed.

An administrator typically configures the access to resources on a service based on the need for a particular user group. Users can request or delete access. They can manage access to the resources they use without the need to understand the underlying technology such as account attributes.

Provisioning features

IBM Security Identity Manager provides support for *provisioning*, the process of providing, deploying, and tracking a service or component in your enterprise. In a suite of security products, Security Identity Manager plays a key role to ensure that resources are accessible only to authorized persons. Security Identity Manager safeguards the accuracy and completeness of information processing methods and granting authorized users access to information and associated assets.

Overview

Security Identity Manager provides an integrated software solution for managing the provisioning of services, applications, and controls to employees, business partners, suppliers, and others associated with your organization across platforms,

organizations, and geographies. You can use its provisioning features to control the setup and maintenance of user access to system and account creation on a managed resource. The two main types of information are person data and account data. *Person data* represents the people whose accounts are being managed. *Account data* represents the credentials of the persons and the managed resources to which the persons were granted access.

At its highest level, an identity management solution automates and centralizes the process of provisioning resources. Resources range from operating systems and applications to people in, or affiliated with, an organization. Organizational structure can be altered to accommodate the provisioning policies and procedures. However, the organization tree used for provisioning resources does not necessarily reflect the managerial structure of an organization.

Administrators at all levels can use standardized procedures for managing user credentials. Some levels of administration can be reduced or eliminated, depending on the breadth of the provisioning management solution. Furthermore, you can securely distribute administration capabilities, manually or automatically, among various organizations. For example, a domain administrator can serve only the people and resources in that domain. This user can do administrative and provisioning tasks, but is not authorized to do configuration tasks, such as creating workflows.

Security Identity Manager supports *distributed* administration capabilities, which include the secure distribution of provisioning tasks, whether manual or automatic, among various organizations. Distributing administrative tasks in your organization improves the accuracy and effectiveness of administration and improves the balance of the work load of an organization.

Security Identity Manager addresses provisioning of enterprise services and components in the following areas:
- Account access management
- Workflow and lifecycle automation
- Provisioning policies
- Role-based access control
- Separation of duty capabilities
- Self-regulating user administration
- Customization

Account access management and the provisioning system

With an effective account access management solution, your organization can track precisely who has access to what information across the organization. Access control is a critical function of a centralized, single-point provisioning system. Besides protecting sensitive information, access controls expose existing accounts that have unapproved authorizations or are no longer necessary. *Orphan accounts* are active accounts that cannot be associated with valid users. For orphan accounts on a managed resource, the account owner cannot be automatically determined by the provisioning system. To control orphan accounts, the provisioning system links together account information with authoritative information about the users who own the accounts. Authoritative user identity information is typically maintained in the databases and directories of human resources.

Improperly configured accounts are active accounts that are associated with valid users but were granted improper authorization because the organization allowed local administrators to add or modify users outside of Security Identity Manager. The ability to control improper accounts is much more difficult, and requires a comparison of "what should be" with "what is" at the account authority level. The existence of an account does not necessarily expose its capabilities. Accounts in sophisticated IT systems include hundreds of parameters that define the authorities, and these details can be controlled by your provisioning system.

New users can be readily identified with the data feed that you establish from the human resources directory. The access request approval capability initiates the processes that approve (or reject) resource provisioning for them.

Workflow and lifecycle automation

When a user becomes affiliated or employed with an organization, the lifecycle of the user begins. Your business policies and processes, whether manual or semi-automated, provision the user with access to certain resources based on role and responsibilities. Over time, when the role and functions of a user change, your business policies and processes can provision the resources that are available to the user. Eventually, the user becomes unaffiliated with the organization, associated accounts are suspended and later deleted, and the lifecycle of the user in the organization is finished. You can use *workflows* to customize how accounts are provisioned. You can customize the lifecycle management of users and accounts, such as adding, removing, and modifying users and accounts. A complete provisioning workflow system automatically routes requests to the appropriate approvers and preemptively escalates to other approvers if actions are not taken on the requests.

You can define two types of workflows in Security Identity Manager: entitlement workflows that apply to provisioning activities, and operational workflows that apply to entity types. An *entitlement workflow* defines the business logic that is tied specifically to the provisioning actions of provisioning policies. A provisioning policy entitlement ties the provisioning actions to entitlement workflows. For example, an entitlement workflow is used to define approvals for managing accounts. An *operational workflow* defines the business logic for the lifecycle processes for entity types and entities. You can use workflow programming tools to automate key aspects of the provisioning lifecycle, specifically the approval processes that your organization uses. A workflow object in the organization tree can contain one or more participants and escalation participants. A *participant* is a signature authority that approves or rejects a provisioning request.

Provisioning policies and auditing

An organizational role entity is assigned to one or more identities when you implement role-based access control for the resources that are managed by Security Identity Manager. An organizational role is controlled by a *provisioning policy*. The policy represents a set of organizational rules and the logic that the Security Identity Manager Server uses to manage resources such as applications or operating systems.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

A provisioning policy maps the people in organizational roles to services that represent corresponding resources in Security Identity Manager. The policy sets the

entitlements that people have when accessing the services. The provisioning policies you implement must reflect your organizational identity management policies in your security plan. To implement effective provisioning policies, you must analyze and document existing business approval processes in your organization. You must determine what adjustments to make those processes to implement an automated identity management solution. A provisioning policy provides a key part of the framework for the automation of identity lifecycle management.

Security Identity Manager provides APIs that interface to information about provisioning policies defined in Security Identity Manager, and interface to the access granted to an individual task. These APIs can be used effectively to generate audit data. When a provisioning policy is defined, the reconciliation function enables the enforcement of the policy rules. The reconciliation function keeps the participating systems (both the Security Identity Manager Server and the repositories of the managed resources) from potentially becoming a single point of failure.

When two or more provisioning policies are applied, a *join directive* defines how to handle attributes. Two or more policies might have overlapping scope, and the join directive specifies what actions to take when this overlap occurs.

Provisioning policies can be mapped to a distinct portion or level of the organizational hierarchy. For example, policies can be defined at a specific organization unit that affects organization roles for that unit only. Service selection policies extend the function of a provisioning policy by enabling the provisioning of accounts based on person attributes. A service selection policy is enforced when it is defined as a target of a provisioning policy. Using a JavaScript script to determine which service to use, the service selection policy defines provisioning based on the instructions in the script. The logic in the JavaScript typically uses person object attributes to determine which service to use. The attribute is often the location of the person in the organization tree.

Role-based access control

Role-based access control (RBAC) uses roles and provisioning policies to evaluate, test, and enforce your business processes and rules for granting access to users. Key administrators create provisioning policies and assign users to roles and that define sets of entitlements to resources for these roles. RBAC tasks establish role-based access control to resource. RBAC extends the identity management solution to use software-based processes and reduce user manual interaction in the provisioning process.

Role-based access control evaluates changes to user information to determine whether the changes alter the role membership for the user. If a change is needed, policies are reviewed and changes to entitlements are put in place immediately. Similarly, a change in the definition of the set of resources in a policy can also trigger a change to associated entitlements. Role-based access control includes the following features:
- Mandatory and optional entitlements, where optional entitlements are not automatically provisioned but can be requested by a user in a group
- Prerequisite services, where specific services must be granted before certain access rights are set

- Entitlement defaults and constraints, where each characteristic of an entitlement can be set to a default value. The entitlement range can be constrained, depending on the capabilities of the entitlement to be granted
- A single account with multiple authorities governed by different policies
- Private, filtered views of information about users and available resources
- User authentication approaches that are consistent with internal security policies
- Distribution of provisioning system components securely over WAN and Internet environments, including the crossing of firewalls
- User IDs that use consistent, user-defined algorithms

Self-regulating user administration

When your organization starts to provision resources across all internal organizations, you implement the self-regulating user administration capability. You can realize the advantages and benefits of provisioning users across organizational boundaries. In this environment, a change in a user's status is automatically reflected in access rights across organization boundaries and geographies. You can reduce provisioning costs and streamline the access and approval processes. The implementation realizes the full potential of implementing role-based access control for end-to-end access management in your organization. You can reduce administrative costs through automated procedures for governing user provisioning. You can improve security by automating security policy enforcement, and streamline and centralize user lifecycle management and resource provisioning for large user populations.

Incremental provisioning and other customization options

Your team can use business plans and requirements to decide how much to customize Security Identity Manager. For example, a large enterprise might require a phased roll-out plan for workflows and custom adapters that is based on a time line for incrementally provisioning applications that are widely used across geographies. Another customization plan might provide for two or more applications to be provisioned across an entire organization, after successful testing. User-application interaction can be customized, and procedures for provisioning resources might be changed to accommodate automated provisioning.

You can *deprovision* to remove a service or component. For example, deprovisioning an account means that the account is deleted from a resource.

Resource provisioning

Depending on business needs, IBM Security Identity Manager provides alternatives you can use to provision resources to authorized users. Alternatives are based on requests, roles, or a combination of requests and roles.

Request-based access to resources

On a request basis, IBM Security Identity Manager provides a process to grant, modify, and remove access to resources throughout a business. The process establishes an effective audit trail with automated reports.

In request-based provisioning, users and their managers search for and request access to specific applications, privilege levels, or resources with a system. The requests are validated by workflow-driven approvals and audited for reporting and compliance purposes.

For example, users, or their managers, can request access to new accounts. Additionally, managers or other administrators are alerted to unused accounts and given the option to delete the accounts through a recertification process. These periodic reviews of user access rights ensure that access with previous approval is removed, if it is no longer needed.

Roles and access control

An organizational role supports different access control and access provisioning models in a customer deployment.

An organizational role can map to IBM Security Identity Manager access entitlements in a provisioning policy. Specific Security Identity Manager groups can be authorized or automatically provisioned for users that are members of the role.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of the provisioning policy.

Security Identity Manager groups can be used to define views and access control for different types of entities that are managed in Security Identity Manager.

Hybrid provisioning model

The hybrid model of provisioning resources combines request and role-based approaches, which are both supported by IBM Security Identity Manager.

For a subset of employees or managed systems, a business might want to automate access with role-based assignment. A business might also handle all other access requests or exceptions through a request-based model. Some businesses might start with manual assignment, and evolve toward a hybrid model, with an intention of a fully role-based deployment at a future time.

Other companies might find it impractical for business reasons to achieve complete role-based provisioning, and target a hybrid approach as a wanted goal. Still other companies might be satisfied with only request-based provisioning, and not want to invest additional effort to define and manage role-based, automated provisioning policies.

Chapter 7. Technical overview

You can use IBM Security Identity Manager to manage the identity records that represent people in a business organization. This section introduces the product architecture and main components.

Security Identity Manager is an identity management solution that centralizes the process of provisioning resources, such as provisioning accounts on operating systems and applications to users.

Security Identity Manager gives you the ability to add business processes and security policies to basic user management. The ability includes adding approvals for user requests to access resources. In addition, Security Identity Manager provides a uniform way to manage user accounts and to delegate administration, including self-service activities and a help desk user interface.

Users, authorization, and resources

An administrator uses the entities that IBM Security Identity Manager provides for users, authorization, and resources to provide both initial and ongoing access in a changing organization.
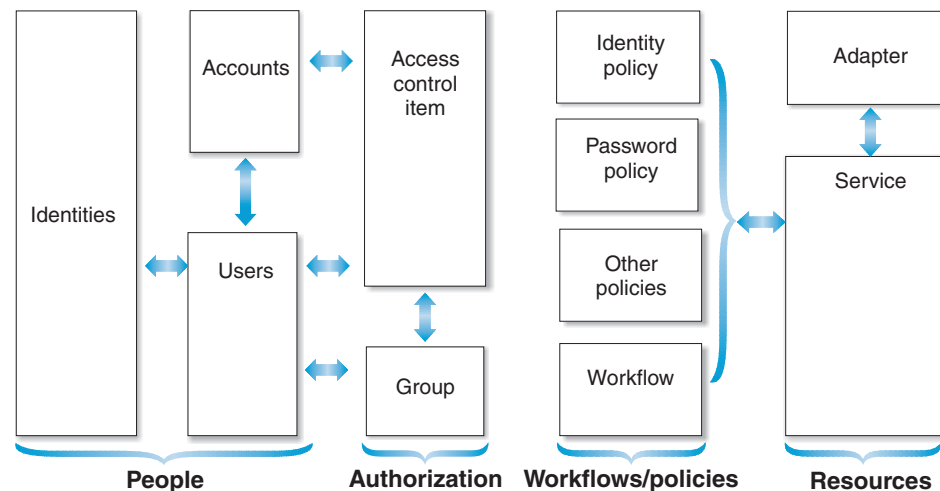
Figure 1. Users, authorization, and resources

Identities
> An identity is the subset of profile data that uniquely represents a person in one or more repositories, and includes additional information related to the person.

Accounts
> An account is the set of parameters for a managed resource that defines your identity, user profile, and credentials.

Users A user is an individual who uses IBM Security Identity Manager to manage their accounts.

Access control items
> An access control item is data that identifies the permissions that users

51

have for a specific type of resource. You create an access control item to specify a set of operations and permissions. You then identify which groups use the access control item.

Groups
A group is used to control user access to functions and data in IBM Security Identity Manager. Membership in a IBM Security Identity Manager group provides a set of default permissions and operations, as well as views, that group members need.

Policies
A policy is a set of considerations that influence the behavior of a managed resource (called a service in IBM Security Identity Manager) or a user. A policy represents a set of organizational rules and the logic that IBM Security Identity Manager uses to manage other entities, such as user IDs, and applies to a specific managed resource as a service-specific policy.

Adapters
An adapter is a software component that provides an interface between a managed resource and the IBM Security Identity Manager Server.

Services
A service represents a managed resource, such as an operating system, a database application, or another application that IBM Security Identity Manager manages. For example, a managed resource might be a Lotus Notes® application. Users access these services by using an account on the service.

Main components

Main components in the IBM Security Identity Manager solution include the IBM Security Identity Manager Server and required and optional middleware components, including adapters that provide an interface to managed resources.
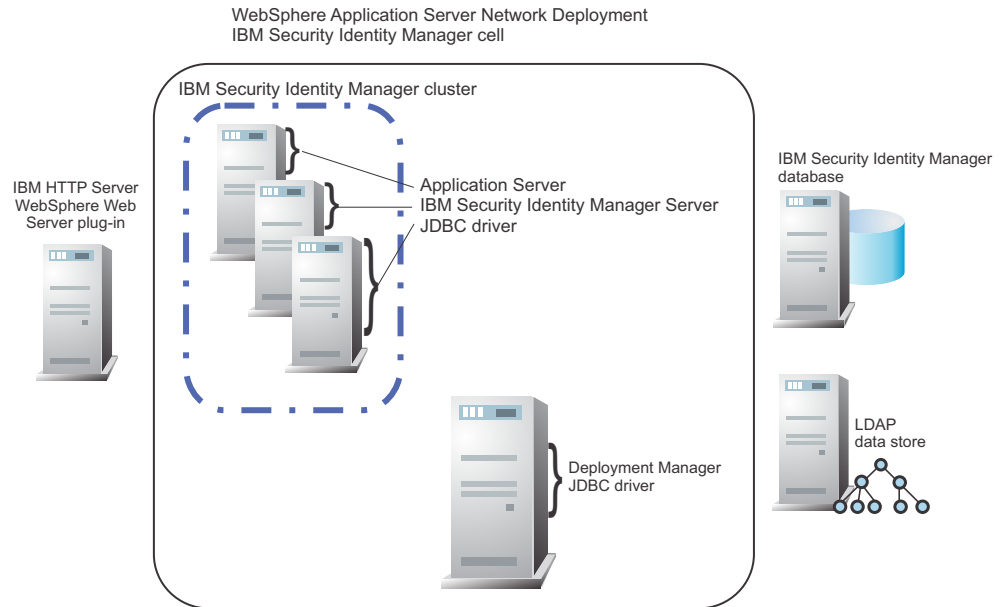
In a cluster configuration, main components include:

Figure 2. Main components

For more information about configuration alternatives, see the *IBM Security Identity Manager Installation Guide*.

Components include:

Database server products

IBM Security Identity Manager stores transactional and historical data in a database server, a relational database that maintains the current and historical states of data.

Computers that communicate with the database require a Java Database Connectivity driver (JDBC driver). For example, a JDBC driver enables a IBM Security Identity Manager Server to communicate with the data source. IBM Security Identity Manager supports a JDBC type 4 driver to connect a Java-based application to a database.

The supported database products are IBM DB2 Database, Oracle DB, and MS SQL database. The information about type 4 JDBC drivers for each database product are as follows:

IBM DB2 Database

DB2 supports a Type 4 JDBC driver. The DB2 type 4 JDBC driver is bundled with the IBM Security Identity Manager installation program.

Oracle database

The Oracle database supports a Type 4 JDBC driver. The IBM Security Identity Manager installation program prompts for the location and name of this JDBC driver.

Before you install the IBM Security Identity Manager Server, obtain this JDBC driver from your Oracle Database Server installation in the `ORACLE_HOME`\jdbc\lib\ directory. Alternatively, you can download the driver from this website: http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html

For WebSphere Application Server version 7.0, the JDBC driver is ojdbc6.jar.

MicrosoftSQL Server database

> **Note:** The Identity Service Center does not support Microsoft SQL Server database. Use DB2 database or Oracle database instead. The SQL Server database supports a Type 4 JDBC driver. The IBM Security Identity Manager installation program prompts for the location and name of this JDBC driver. You can download the driver from this website http://msdn.microsoft.com/en-us/data/aa937724.aspx.

For more information about supported database server products, see "Database server support" on page 9.

Directory server products
IBM Security Identity Manager stores the current state of the managed identities in an LDAP directory, including user account and organizational data.

IBM Security Identity Manager supports the following products: .
- IBM Security Directory Server
- Sun Enterprise Directory Server

See "Directory server support" on page 10.

IBM Security Directory Integrator
IBM Security Directory Integrator synchronizes identity data in different directories, databases, and applications. IBM Security Directory Integrator synchronizes and manages information exchanges between applications or directory sources.

WebSphere Application Server
WebSphere Application Server is the primary component of the WebSphere environment. WebSphere Application Server runs a Java virtual machine, providing the runtime environment for the application code. The application server provides communication security, logging, messaging, and Web services.

The Security Identity Manager application can run on a single-server configuration with the WebSphere Application Server base server. Security Identity Manager can also run in a larger cluster configuration. The configuration can have one or more WebSphere Application Servers and a deployment manager that manages the cluster.

HTTP server and WebSphere Web Server plug-in
An HTTP server provides administration of IBM Security Identity Manager through a client interface in a web browser. IBM Security Identity Manager requires the installation of a WebSphere Web Server plug-in with the HTTP server. The WebSphere Application Server installation program can separately install both the IBM HTTP Server and WebSphere Web Server plug-in.

IBM Security Identity Manager adapters
An adapter is a program that provides an interface between a managed resource and the Security Identity Manager Server. Adapters function as trusted virtual administrators on the target platform for account management. For example, adapters do such tasks as creating accounts, suspending accounts, and modifying account attributes.

A Security Identity Manager adapter can be either agent-based or agentless:

Agent-based adapter
> You install adapter code directly onto the managed resource with which it is designed to communicate.

Agentless adapter
> Deploys its adapter code onto the Security Identity Manager Server and the system that hosts Security Directory Integrator. The adapter code is separate from the managed resource with which it is designed to communicate.

Note: For agentless adapters, the SSH process or daemon must be active on the managed resource.

People overview

People, such as employees and contractors, need to use the resources that an organization provides. A person who has a IBM Security Identity Manager account is a IBM Security Identity Manager user.

Users need different degrees of access to resources for their work. Some users need to use a specific application. Other users need to administer the system that links users to the resources that their work requires.

IBM Security Identity Manager manages users' identities (user IDs), accounts, access entitlements on those accounts, and user credentials such as passwords.

Users

A person who is managed by IBM Security Identity Manager is a user. A user who has a IBM Security Identity Manager account is called a IBM Security Identity Manager user. This user can use IBM Security Identity Manager to manage accounts or do other administrative tasks.

Users need different degrees of access to resources for their work. Some users need to use a specific application. Other users need to administer the system that links users to the resources that their work requires. A IBM Security Identity Manager user is assigned to a specific group that provides access to specific views and allows the user to do specific tasks in IBM Security Identity Manager .

As an administrator, you create users either by importing identity records or by using IBM Security Identity Manager .

Identities

An identity is the subset of profile data that uniquely represents a person or entity. The data is stored in one or more repositories.

For example, an identity might be represented by the unique combination of a person's first, last (family) name, and full (given) name, and employee number. An identity profile might also contain additional information such as phone numbers, manager, and email address.

Accounts

An account is the set of parameters for a managed resource that defines an identity, user profile, and credentials.

An account defines login information (your user ID and password, for example) and access to the specific resource with which it is associated.

In IBM Security Identity Manager, accounts are created on services, which represent the managed resources. Such resources might be operating systems (UNIX), applications (Lotus Notes), or other resources.

Accounts, when owned, are either individual or sponsored. Individual accounts are for use by a single owner and have an ownership type of Individual. Sponsored accounts are assigned to owners who are responsible for the accounts, but might not actually use them to access resources. Sponsored accounts can have various types of non-Individual ownership types. IBM Security Identity Manager supplies three ownership types for sponsored accounts Device, System, and Vendor. You can use the Configure System utility to create additional ownership types for sponsored accounts.

Accounts are either active or inactive. Accounts must be active to log in to the system. An account becomes inactive when it is suspended. Suspension can occur if a request to recertify your account usage is declined and the recertification action is *suspend*. Suspended accounts still exist, but they cannot be used to access the system. System administrators can restore and reactivate a suspended account if the account is not deleted.

Access

Access is your ability to use a specific resource, such as a shared folder or an application.

In IBM Security Identity Manager, access can be created to represent access to access types. Such access types might be shared folders, applications (such as Lotus Notes), email groups, or other managed resources.

An access differs from an account in that an account is a form of access; an account is access to the resource itself.

Access is the permission to use the resource. The *access entitlement* defines the condition that grants access to a user with a set of attribute values of a user account on the managed resource. In IBM Security Identity Manager, an access is defined on an existing group on the managed service. In this case, the access is granted to a user by creating an account on the service and assigning the user to the group. Access entitlement can also be defined as a set of parameters on a service account that uses a provisioning policy.

When a user requests new access, by default an account is created on that service. If an account exists, the account is modified to fulfill the access entitlement. For example, the account is assigned to the group that grants access to an access type. If one account exists, the account is associated with the access. If multiple accounts exist, you must select the user ID of the account to which you want to associate your access.

An access is often described in terms that can be easily understood by business users.

Passwords

A *password* is a string of characters that is used to authenticate a user's access to a system. A user ID and password are the two elements that grant access to a system.

As an administrator, you can manage user passwords and the passwords that are set for the users that are used by IBM Security Identity Manager .

Forgotten password administration

You can administer and define forgotten password information so users can reset forgotten IBM Security Identity Manager passwords. The information is in the format of questions and answers.

Password synchronization

Password synchronization is the process of assigning and maintaining one password for all individual accounts that a user owns. Password synchronization reduces the number of passwords that a user must remember.

You can configure the system to automatically synchronize passwords for all individual accounts owned by a user. Then, the user must remember only one password. For example, a user has two individual accounts: a IBM Security Identity Manager account and a Lotus Notes account. If the user changes or resets the password for the IBM Security Identity Manager account, the Lotus Notes password is automatically changed to the same password as the IBM Security Identity Manager password. Passwords might also be synchronized when you provision an account or restore a suspended account.

If password synchronization is enabled, a user cannot specify different passwords for other individual accounts owned by the user.

Note: When you provision an account or restore an account that was suspended, you must specify a password for the account. If password synchronization is enabled, you are not prompted for a password. Instead the individual account is automatically given the same password as the existing individual accounts of the user.

Password strength rules

A password strength rule is a rule or requirement to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be five. The rules might specify that the maximum number of characters must be 10.

You can define password strength rules in a password policy.

Resources overview

Resources are the applications, components, processes, and other functions that users need to complete their work assignments.

IBM Security Identity Manager uses a service to manage user accounts and access to resources by using adapters to provide trusted communication of data between the resources and IBM Security Identity Manager.

Services

A *service* represents a managed resource, such as an operating system, a database application, or another application that IBM Security Identity Manager manages. For example, a managed resource might be a Lotus Notes application.

Users access these services by using an account on the service.

Services are created from service types, which represent a set of managed resources that share similar attributes. For example, there is a default service type that represents Linux machines. These service types are installed by default when IBM Security Identity Manager is installed. Alternatively, they are installed when you import the service definition files for the adapters for those managed resources.

Accounts on services identify the users of the service. Accounts contain the login and access information of the user and allow the use of specific resources.

Most services use IBM Security Identity Manager to provision accounts, which usually involves some workflow processes that must be completed successfully. However, manual services generate a work order activity that defines the manual intervention that is required to complete the request or to provision the account for the user.

A *service owner* owns and maintains a particular service in IBM Security Identity Manager. A service owner is either a person or a static organizational role. For a static organizational role, all the members of the organizational role are considered service owners. If that static organizational role contains other roles, then all members of those roles are also considered service owners.

Service types

A *service type* is a category of related services that share schemas. It defines the schema attributes that are common across a set of similar managed resources.

Service types are used to create services for specific instances of managed resources. For example, you might have several Lotus® Domino® servers that users need access to. You might create one service for each Lotus Domino server with the Lotus Domino service type.

Service prerequisite

A service might have another service defined as a service prerequisite. A user can receive a new account only if they have an existing account on the service prerequisite.

For example, Service B has a service prerequisite, Service A. If a user requests an account on Service B, in order to receive an account, the user must first have an account on Service A.

Service definition file

A *service definition file*, which is also known as an *adapter profile*, defines the type of managed resource that IBM Security Identity Manager can manage. The service definition file creates the service types on the IBM Security Identity Manager Server.

The service definition file is a JAR file that contains the following information:
• Service information, including definitions of the user provisioning operations that can be done for the service, such as add, delete, suspend, or restore.

- Service provider information, which defines the underlying implementation of how the IBM Security Identity Manager Server communicates with the managed resource. Valid service providers are Security Directory Integrator and DSMLv2.
- Schema information, including the LDAP classes and attributes.
- Account forms and service forms. A properties file for accounts and supporting data such as service groups defines the labels for the attributes on these forms. The labels are displayed in the user interface for creating services and requesting accounts on those services.

Manual services

A *manual service* is a type of service that requires manual intervention to complete the request. For example, a manual service might be defined for setting up voice mail for a user.

Manual services generate a work order activity that defines the manual intervention that is required.

You might create a manual service when IBM Security Identity Manager does not provide an adapter for a managed resource for which you want to provision accounts.

When you create a manual service, you add new schema classes and attributes for the manual service to your LDAP directory.

See the following topics:
- "Manual services and service type" in the *IBM Security Identity Manager Configuration Guide*
- "Enabling connection mode" in the *IBM Security Identity Manager Administration Guide*

Adapters

An *adapter* is a software component that provides an interface between a managed resource and IBM Security Identity Manager.

An adapter functions as a trusted virtual administrator for the managed resource. An adapter does such tasks as creating accounts, suspending accounts, and other functions that administrators typically do.

An adapter consists of the service definition file and the executable code for managing accounts.

Several agentless adapters are automatically installed when you install IBM Security Identity Manager. You can install more adapters. See the IBM Security Identity Manager adapter documentation at http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.itim_pim.doc/c_adapters_intro.htm for complete description of each adapter and the installation procedure.

System security overview

An organization has critical needs to control user access, and to protect sensitive information.

First, an organization agrees on security requirements for business needs. Then, a system administrator configures the groups, views, access control items, and forms that IBM Security Identity Manager provides for security of its data.

Security model characteristics

An organization defines a security model to meet its business needs. The model serves as a basis to define the requirements and actual implementation of a security system.

Some characteristic objectives of a security model include:
- Verifying the identity of users, provided by authentication systems that include password strength and other factors.
- Enabling authorized users to access resources, provided by authorization systems that define request or role-based processes, and related provisioning. Resources, for example, include accounts, services, user information, and IBM Security Identity Manager functions.

  A security model also requires additional provisioning processes to select the resources that users are permitted to access.
- Administering which operations and permissions are granted for accounts and users.
- Delegating a user's list of activities to other users, on a request or assignment basis.
- Protecting sensitive information, such as user lists or account attributes.
- Ensuring the integrity of communications and data.

Business requirements

A business needs agreement on its security requirements before implementing the processes that IBM Security Identity Manager provides.

For example, requirement definitions might answer these questions:
- What groups of IBM Security Identity Manager users are there?
- What information does each user group need to see?
- What tasks do the users in each group need to do?
- What roles do users perform in the organization?
- Which access rights need definition?
- What working relationships exist that require some users to have different authority levels?
- How can prevention and auditing provide remedies for activity that does not comply with established policies?

To meet common business needs, a business might frequently have several groups, such as a manager, a help desk assistant, an auditor group. The business might have customized groups that do a more expanded or limited set of tasks.

Resource access from a user's perspective

To provide security of data for a user who works within a range of tasks on specific business resources, IBM Security Identity Manager might provide one or more roles, and membership in one or more groups.

For example, a user in a business unit often has a title, or role that has a responsibility, such as buyer. The user might also be a member of a group that

provides a view of tasks that the user can do, such as regional purchasing. The relationships are illustrated in Figure 3:
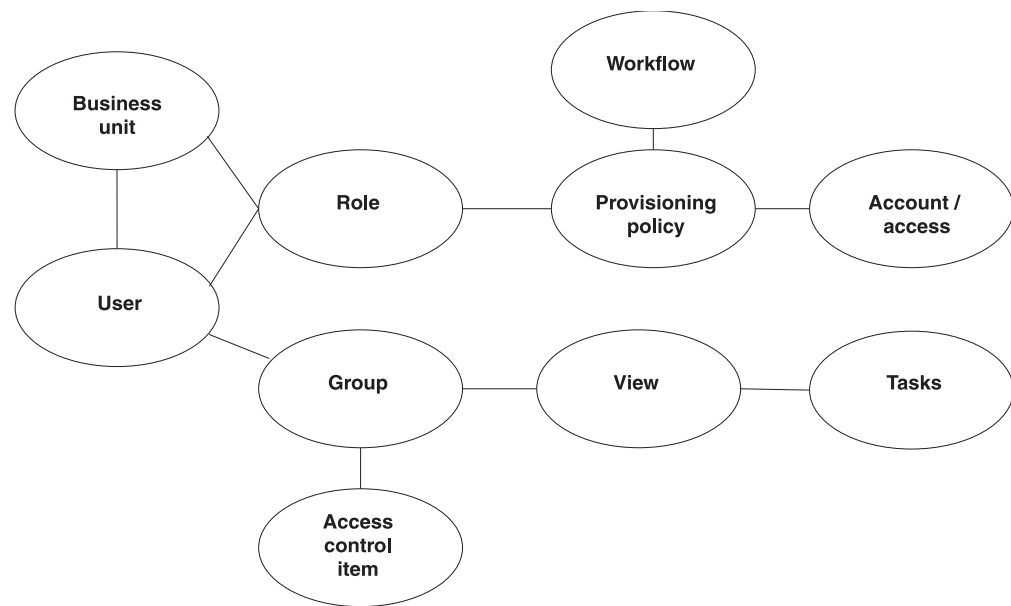

Figure 3. Securing data for user access to resources

Each role has a related provisioning policy and workflow to grant the user to access one or more resources, such as accounts.

Each group has a view of specific tasks, and one or more access control items that grant specific operations and permissions to do the tasks. By using a form designer applet, you can also modify the user interface that a user sees. You might remove unnecessary fields for account, service, or user attributes.

Groups

A *group* is used to control user access to functions and data in IBM Security Identity Manager.

Group members have an account on the IBM Security Identity Manager service. Membership in an IBM Security Identity Manager group provides a set of default permissions and operations, as well as views, that group members need. Your site might also create customized groups.

Additionally, some users might be members of a service group that grants specific access to a certain application or other functions. For example, a service group might have members that work directly with data in an accounting application.

Predefined groups, views, and access control items

IBM Security Identity Manager provides predefined groups. The groups are associated with views and access control items.

The following user interfaces, or consoles, are available:
- Self-service console for all users, for self-care activities such as changing personal profile information, such as a telephone number.
- Identity Service Center for all users, for self-care activities such as changing personal profile information, requesting access.

- Administrative console, for selected users who belong to one or more groups that enable a range of administrative tasks.

A IBM Security Identity Manager user with no other group membership has a basic privilege to use IBM Security Identity Manager.

This set of users needs only a self-service console or the Identity Service Center for self-care capabilities. The users are not in a labeled "group" such as a Help Desk Assistant group.

The predefined groups are associated with predefined views and access control items, to control what members can see and do, as illustrated in Figure 4
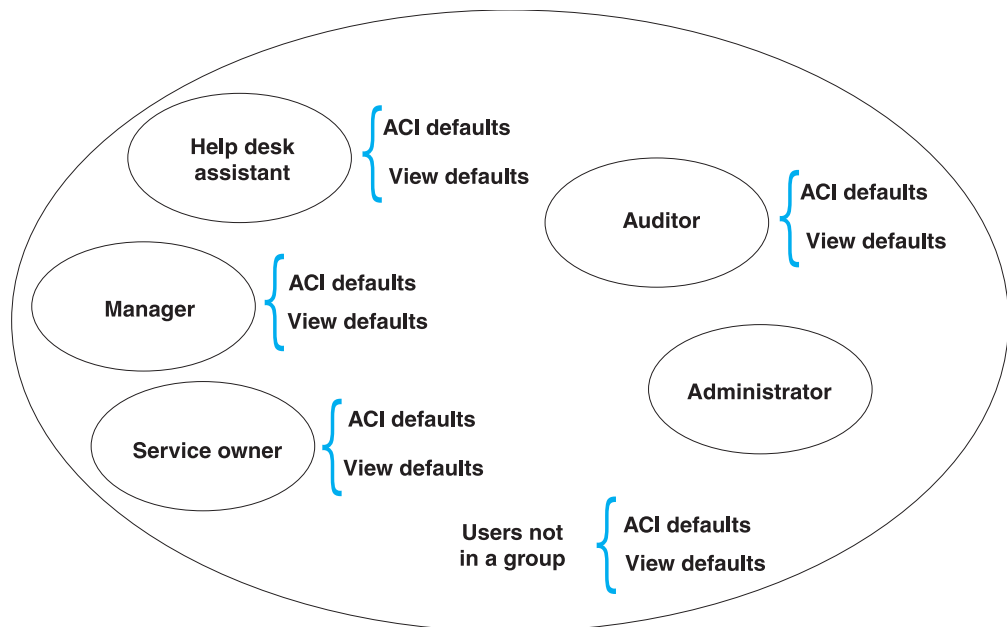
Figure 4. Predefined groups, views, and access control items

The predefined groups are:

Administrator
> The administrator group has no limits set by default views or access control items and can access all views and do all operations in IBM Security Identity Manager. The first system administrator user is named "itim manager".

Auditor
> Members of the auditor group can request reports for audit purposes.

Help Desk Assistant
> Members of the Help Desk Assistant group can request, change, suspend, restore, and delete accounts. Members can request, change, and delete access, and also can reset passwords, profiles, and accounts of others. Additionally, members can delegate activities for a user.

Manager
> Members of the Manager group are users who manage the accounts, profiles, and passwords of their direct subordinates.

Service Owner

> Members of the Service Owner group manage a service, including the user accounts and requests for that service.

Views

A *view* is a set of tasks that a particular type of user can see, but not necessarily do, on the graphical user interface. For example, it is a task portfolio of the everyday activities that a user needs to use IBM Security Identity Manager.

On both the self-service console and the administrative console, you can specify the view that a user sees.

Access control items

An *access control item* (ACI) is data that identifies the permissions that users have for a specific type of resource. You create an access control item to specify a set of operations and permissions. You also identify which groups use the access control item.

An access control item defines these items:
* The entity types to which the access control item applies
* Operations that users might do on entity types
* Attributes of the entity types that users might read or write
* The set of users that is governed by the access control item

IBM Security Identity Manager provides default access control items.

You can also create a customized access control item. For example, a customized access control item might limit the ability of a specific Help Desk Assistant group to change information for other users. Access control items can also specify relationships such as Manager or Service Owner.

When you create customized reports, you must also manually create report access control items and entity access control items for the new report. These ACIs permit users who are not administrators, such as auditors, to run the custom report and view data in the custom report.

After you create an access control item or change an existing access control item, run a data synchronization to ensure that other Security Identity Manager processes, such as the reporting engine, use the new or changed access control item.

Forms

A *form* is a user interface window that is used to collect and display values for account, service, or user attributes.

IBM Security Identity Manager includes a form designer, which runs as a Java applet, that you use to modify existing user, service and account forms. For example, you might add the fax number attribute and an associated entry field to capture that number for a particular account. You might remove an account attribute that your organization does not want a user to see. If you remove an attribute from a form, it is completely removed; that is, even system administrators cannot see the attribute.

You can see only those attributes that are on the form and that you have read or write access to (as granted by access control items). Using the form designer, you can also customize forms for other elements in the organization tree, such as location or organization unit.

Organization tree overview

Business organizations have various configurations that contain their subordinate units, including services and employees.

For a specific set of business needs, you can configure IBM Security Identity Manager to provide a hierarchy of services. You can configure organizations, users, and other elements in a tree that corresponds to the needs of a user population.

Note: This release provides enhanced menus to search for a specific user, but not a graphic organization tree for that purpose.

In this release, you cannot browse and create entities by navigating the organization tree. The association to a business unit within the organization tree is specified during the creation of the entity.

Nodes in an organization tree

An organization tree has nodes that include organizations and subordinate business units, as well as other elements.

An organization tree can have these nodes:

Organization
Identifies the top of an organizational hierarchy, which might contain subsidiary entities such as organization units, business partner organization units, and locations. The organization is the parent node at the top of the node tree.

Organization Unit
Identifies a subsidiary part of an organization, such as a division or department. An organization unit can be subordinate to any other container, such as organization, organization unit, location, and business partner organization.

Business Partner Organization Unit
Identifies a business partner organization, which is typically a company outside your organization that has an affiliation, such as a supplier, customer, or contractor.

Location
Identifies a container that is different geographically, but contained within an organization entity.

Admin Domain
Identifies a subsidiary part of an organization as a separate entity with its own policies, services, and access control items, including an administrator whose actions and views are restricted to that domain.

Entity types associated with a business unit

Different types of entities can be associated with a business unit in an organization tree.

The association to a business unit is specified when the entity is created. Normally, an entity cannot change the business unit association after it is created. The only exception is the User entity. IBM Security Identity Manager supports the transfer of users between different business units.

The following entity types can be associated to a business unit in the organization tree:

- User
- ITIM group
- Service
- Role
- Identity policy
- Password policy
- Provisioning policy
- Service selection policy
- Recertification policy
- Account and access request workflow
- Access control item

Entity searches of the organization tree

This release provides menus to search for a specific user, but not a graphic organization tree to navigate to locate a specific user.

To locate a specific user with search menus, use the advanced search filter to search by user type such as Person or Business Partner Person. In the search, you can also select a business unit and its subunits, and the status of the user, such as Active. Additionally, you can add other fields to qualify the search, including an LDAP filter statement.

Policies overview

A *policy* is a set of considerations that influence the behavior of a managed resource (called a *service* in IBM Security Identity Manager) or a user.

A policy represents a set of organizational rules and the logic that Security Identity Manager uses to manage other entities, such as user IDs, and applies to a specific managed resource as a service-specific policy.

Security Identity Manager enables your organization to use centralized security policies for specified user groups. You can use Security Identity Manager policies to centralize user access for disparate resources in an organization. You can implement additional policies and features that streamline operations associated with access to resources for users.

Security Identity Manager supports the following types of policies:

- Adoption policies
- Identity policies
- Password policies
- Provisioning policies
- Recertification policies
- Separation of duty policies

- Service selection policies

A policy can apply to one or multiple service targets, which can be identified either by a service type or by listing the services explicitly. These policies do not apply to services that represent identity feeds.

- Adoption policies apply to services. A global adoption policy applies to all services of a service type.
- Identity policies, password policies, and provisioning policies can apply to all service types, all services of a service type, or specific services.
- Recertification policies cannot act on all service types, but you can add all the different services for a specific recertification policy.
- Separation of duty policies does not apply directly to service types, and apply only to role membership for users.
- Service selection policies apply to only one service type.

Policy types and navigation

Table 11. Policy types and navigation

Type of policy	Navigation
Adoption	**Manage Policies > Manage Adoption Policies**
Identity	**Manage Policies > Manage Identity Policies**
Password	**Manage Policies > Manage Password Policies**
Provisioning	**Manage Policies > Manage Provisioning Policies**
Recertification	**Manage Policies > Manage Recertification Policies**
Separation of duty	**Manage Policies > Manage Separation of Duty Policies**
Service selection	**Manage Policies > Manage Service Selection Policies**

Account defaults

Account defaults define default values for an account during new account creation. The default can be defined at the service type level that applies to all services of that type. Alternatively, the default can be defined at the service level, which applies only to the service.

Policy enforcement

Global policy enforcement is the manner in which Security Identity Manager globally allows or disallows accounts that violate provisioning policies.

When a policy enforcement action is global, the policy enforcement for any service is defined by the default configuration setting. You can specify one of the following policy enforcement actions to occur for an account that has a noncompliant attribute.

Note: If a service has a specific policy enforcement setting, that setting is applied to the noncompliant accounts. The global enforcement setting does not apply. Policy enforcement can also be set for a specific service.

Mark   The existing user account on the old service is marked as disallowed, and a new account is not created on the new service.

Suspend
    The existing user account on the old service instance is suspended, and a new account is not created on the new service.

Alert   An alert is sent to the recipient administrator to confirm removal of the old account on old services. A new account is created on new service if the user does not have account on new service, and entitlement is automatic.

Correct
    Existing accounts are removed on the old service. A new account is created on new service if the user does not have account on new service and entitlement is automatic.

To work with global policy enforcement, go to the navigation tree and select **Configure System > Configure Global Policy Enforcement**.

Note: To set service policy enforcement, go to the navigation tree and select **Manage Services**.

Workflow overview

A *workflow* defines a sequence of activities that represent a business process. You can use workflows to customize account provisioning and access provisioning, and lifecycle management.

A workflow is a set of steps or activities that define a business process. You can use the IBM Security Identity Manager workflows to customize account provisioning and lifecycle management. For example, you can add approvals and information requests to account or access provisioning processes. You can integrate lifecycle management processes (such as adding, removing, and modifying people and accounts in Security Identity Manager) with external systems.

Security Identity Manager provides these major types of workflows:

Operation workflows
    Use operation workflows to customize the lifecycle management of accounts and people, or a specific service type, such as all Linux systems.

    Operation workflows add, delete, modify, restore, and suspend system entities, such as accounts and people. You can also add new operations that your business process requires, such as approval for new accounts. For example, you might specify an operation workflow that defines activities to approve the account, including notifications and manager approvals.

Account request and access request workflows
    Use account request and access request workflows to ensure that resources such as accounts or services are provisioned to users according to the business policies of your organization.

    Note: The term *entitlement workflow* was previously used for this workflow type in Security Identity Manager Version 4.6.

- An *account request workflow* can be bound to an entitlement for an access or an account.

  In provisioning policies, an entitlement workflow for accounts adds decision points to account requests, such as adding or modifying an account. If the request is approved, the processing continues; if the request is rejected, the request is canceled.

  The account request workflow is started during account provisioning requests, including adding and modifying an account, made by a Security Identity Manager user or made during account auto provisioning. An account request workflow can be also started during an access request if there is no access request workflow defined.

- An *access request workflow* is bound to an access by the access definition, rather than by a provisioning policy. This workflow can specify the steps and approvals that authorize access to resources in a request.

  The access request workflow is started only for access requests that are made by a Security Identity Manager user. The workflow is not started if the access is provisioned for the user as a result of an external or internal account request. An external account request is an account request made by a Security Identity Manager user. An internal account request is an account request made by the Security Identity Manager system. For example, an auto account provisioning gives the user a default or mandatory group that maps to an access.

Chapter 8. Language support

IBM Security Identity Manager supports various languages through the browser.

You can change your browser language configuration to access the IBM Security Identity Manager web interface in any of the supported languages. IBM Security Identity Manager is translated for these languages:

- Arabic
- Brazilian Portuguese
- Czech
- Dutch
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Russian
- Simplified Chinese
- Spanish
- Traditional Chinese
- Turkish

Attention: A known issue exists with the Turkish language and forgotten password support. See Forgotten password problems in Turkish. Also, Turkish reports in PDF format must use a font that supports Turkish characters. See Troubleshooting report problems.

Chapter 9. Initial login and password information

To get started after installing IBM Security Identity Manager, you need to know the login URL and the initial user ID and password.

Note: For security reasons, change the IBM Security Identity Manager ID and password on your system after the initial login.

Login URL

The login URL enables you to access the IBM Security Identity Manager web interface.

The login URL for the IBM Security Identity Manager administrative console is:
`http://ip-address:port/itim/console/main/`

Where *ip-address* is the IP address or DNS address of the IBM Security Identity Manager server, and *port* is the port number. The default port for new installations of IBM Security Identity Manager is 9080.

The login URL for the IBM Security Identity Manager self-service console is:
`http://ip-address:port/itim/self`

Where *ip-address* is the IP address or DNS address of the IBM Security Identity Manager server, and *port* is the port number. The default port for new installations of IBM Security Identity Manager is 9080.

The login URL for the IBM Security Identity Manager Identity Service Center is:
`http://ip-address:port/itim/ui/Login.jsp`

Where *ip-address* is the IP address or DNS address of the IBM Security Identity Manager server, and *port* is the port number. The default port for new installations of IBM Security Identity Manager is 9080.

Initial user ID and password

The initial user ID and password to authenticate to IBM Security Identity Manager is:

Table 12. Initial user ID and password for IBM Security Identity Manager

User ID	Password
itim manager	*secret*

Chapter 10. Accessibility features for IBM Security Identity Manager

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The following list includes the major accessibility features in IBM Security Identity Manager.

- Supports interfaces commonly used by screen readers. This feature applies to applications on Windows operating systems only.
- Can be operated by using only the keyboard.
- Communicates all information independently of color.
- Supports interfaces commonly used by screen magnifiers. This feature applies to applications on Windows operating systems only.
- Allows the user to access the interfaces without inducing seizures due to photosensitivity.

IBM Security Identity Manager uses the latest W3C Standard, WAI-ARIA 1.0, to ensure compliance with US Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0. To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by IBM Security Identity Manager.

The IBM Security Identity Manager online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help.

Keyboard navigation

This product uses standard navigation keys.

Interface information

The IBM Security Identity Manager user interfaces do not have content that flashes 2 - 55 times per second.

The IBM Security Identity Manager web user interface relies on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The IBM Security Identity Manager web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility.

Index

S

schema   58
security
   lifecycle   33
   model   60
   system   60
self-care user interface   41
separation of duty policies   65
service definition file   58
services   58
   manual   59
   prerequisite   58
   selection policies   65
   types   58
software requirements
   IBM Cognos report server   11
   Java Runtime Environment   7
   JRE   7
   operating system   5
static role   44
supported languages   69
system security   60

T

troubleshooting
   known limitations   31

U

user access   60
user interface
   Identity Service Center   41
   new   41
user interfaces   40
users   55

V

views, default   63
virtualization, supported products   6

W

workarounds   31
workflows
   entitlement   67
   operation   67

IBM ®

Printed in USA