IBM Security Identity Manager
Version 7.0.0.2

Product Overview Topics

IBM Security Identity Manager
Version 7.0.0.2

Product Overview Topics

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 centralizes the process of provisioning and accessing user accounts on the operating systems and applications in your organization. IBM Security Identity Manager provides a mechanism to initially set up a semi-passive virtual appliance and a high availability solution for providing an all-in-one identity virtual appliance. The virtual appliance helps to decrease the amount of time the user spends in deploying and configuring in their own product environment.

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. More 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.

IBM Security Identity Manager virtual appliance overview

The IBM Security Identity Manager virtual appliance is a network appliance-based identity-management solution. IBM Security Identity Manager offers a virtual appliance to reduce the overall Time To Value (TTV) and greatly reduce the deployment time of the product. You can configure the virtual appliance for a cluster environment. You can configure a virtual appliance to connect to external database servers, directory servers, and other supported appliances. You can manage the configuration interfaces and capabilities to deploy and configure the products on the virtual appliance.

The IBM Security Identity Manager virtual appliance cluster is made of one primary node and other member nodes. All configuration changes such as hardware and software are done only on the primary node. There is only one primary node in the cluster. Even if the primary node itself goes down or must be taken down, the other nodes can continue to do the IBM Security Identity Manager functions. Changes to configuration details are not allowed until the primary node is reconnected in the cluster.

Note: IBM Security Identity Manager V7.0.0.2 on the virtual appliance does not support a direct upgrade or migration from previous versions of the IBM Security Identity Manager product.

The important features of the IBM Security Identity Manager virtual appliance are as follows:

- IBM Security Identity Manager now has Identity Governance capabilities through the IBM Security Identity Governance (SIG) adapter.
- A configuration wizard for the first time configuration of the IBM Security Identity Manager solution in stand-alone or cluster mode.
- A dashboard for viewing system status such as system notifications, cluster status, component and application status, deployment statistics, and disk usage.
- Analysis and diagnostics tools such as memory statistics, CPU usage, and performance metrics and service statistics for IBM Security Identity Manager.
- Centralized management of IBM Security Identity Manager settings such as data tier components or external entities, and log files.
- Control of system settings such as host name, date or time, and network settings.
- Most of the features are configurable by using the graphical management interface.
- Add member nodes that point to the primary node to process large number of IBM Security Identity Manager requests.
- Remove a node from the cluster for any maintenance such as applying fix packs, upgrades, or failures.
- Synchronization between two nodes.
- Backing up a primary node for disaster recovery purposes.
- External middleware components such as database server and directory server.
- Manage application server certificates, upload feed files, configure mail server, configure Security Directory Integrator server, or Oracle server.
- Configure Single Sign On to authorize the user to use multiple applications with the single sign-on facility.
- Configure an external user registry with IBM Security Identity Manager to grant users of external user registry the authority to log on to IBM Security Identity Manager application.
- Upload, download, or update files on the virtual appliance by using the **Custom File Management** feature from the **Appliance Dashboard**.
- Upload library files and custom workflow extensions that can be used in IBM Security Identity Manager.
- Update IBM Security Identity Manager properties by using the **Update Property** feature from the **Appliance Dashboard**.
- Monitoring the status of all the nodes and the individual applications in the IBM Security Identity Manager virtual appliance cluster.
- IBM Security Identity Manager Mobile App to manage accounts by using a mobile phone to communicate your requests from the IBM Security Identity Manager virtual appliance.
- Send system audit events over emails.
- SNMP monitoring can be used to monitor the IBM Security Identity Manager virtual appliance.
- Enabling and simplifying workflow extension configuration.
- Configure an external library.

- Enable separate application interfaces for the virtual appliance and the application consoles.
- Use of log file management.
- Export and import configurations. You can also export, import, access, or download report files.
- Download and view core dumps to diagnose or debug virtual appliance errors.
- Manage hosts file.
- Configure static routes.

Chapter 2. Getting started

An overview about how to get started with the IBM Security Identity Manager virtual appliance is described here.

The following table describes the main stages or tasks that you can manage by using IBM Security Identity Manager virtual appliance and IBM Security Identity Manager.

Table 1. Main stages or tasks that you can manage by using IBM Security Identity Manager virtual appliance and IBM Security Identity Manager

	Tasks	**Action by**
1.	Deploy and configure the Identity Management System.	IBM Security Identity Manager virtual appliance Administrator
2.	Configure system-wide organizational structure and roles, and policies for password.	IBM Security Identity Manager Administrator
3.	Create roles. **Note:** Skip this task if the role exists.	IBM Security Identity Manager Administrator
4.	On-board Administrators.	IBM Security Identity Manager Administrator
5.	On-board Users.	IBM Security Identity Manager Administrator
6.	On-board service types, service instances, and accounts.	IBM Security Identity Manager Administrator
7.	Assign users to role.	IBM Security Identity Manager Administrator

Personas and use cases

Different personas are involved with the setup and usage of the IBM Security Identity Manager. Each persona is responsible for a set of tasks or is identified to do specific workflows.

Persona: Virtual Appliance Administrator

The Virtual Appliance Administrator is responsible for the following tasks.

Table 2. Virtual Appliance Administrator tasks

Tasks	Subtasks and reference
Deploy and configure the Identity Management System.	1. Database installation and configuration 2. Installation and configuration of a directory server 3. Setting up the virtual machine 4. Installing the IBM Security Identity Manager virtual appliance 5. Setting up the initial IBM Security Identity Manager virtual appliance 6. Configuring the IBM Security Identity Manager by using the initial configuration wizard a. Managing the database server configuration b. Managing the directory server configuration c. Managing the mail server configuration 7. Setting up an IBM Security Identity Manager member node from the initial configuration wizard
Back up and restore the virtual appliance by using snapshots	Managing the snapshots
Applying Fix Pack	Use the `fixpack` command in the IBM Security Identity Manager virtual appliance command line interface commands for IBM Security Identity Manager.
Upgrade Firmware	Use the `firmware_update` command in the IBM Security Identity Manager virtual appliance command line interface commands.
Reconfigure the virtual appliance	• Reconfiguring the data store connection • Reconfiguring the directory server connection

Persona: IBM Security Identity Manager Administrator

The IBM Security Identity Manager administrator is responsible for the following tasks.

Table 3. IBM Security Identity Manager Administrator tasks

Tasks	Subtasks and reference
Configure system-wide organizational structure and roles, and policies for password.	1. Create a node in an organization tree. See Creating a node in an organization tree. 2. Define password policies for the Identity account. For example, Set password expiry. See Enabling password expiration. For other policies, see Password administration.
Create roles. **Note:** Skip this task if the role exists.	See Creating roles.
On-board Administrators.	1. Create an Identity Administrator profile. See Creating user profiles. 2. (Optional) Assign the user to an Identity Administrator role if the role is already defined. See Adding users to membership of a role. 3. Add user to the pre-defined Identity Administrator group. See Adding members to groups. 4. (Optional) Add an Administrator domain and make the Identity Administrator user as Administrator to the Admin domain. See Creating a node in an organization tree.
On-board Users.	1. Create an Identity User profile. See Creating user profiles. 2. (Optional) Assign the user to an Identity User role if needed or if the role is already defined. See Adding users to membership of a role.
On-board service types, service instances, and accounts. If the service type is not yet pre-configured	Create a Service Type by importing a service type profile. See Creating service types. By default, these pre-configured service type profiles are imported in IBM Security Identity Manager. • POSIX AIX® • POSIX HP-UX • POSIX Linux • POSIX Solaris • Windows Local • Windows Active Directory • IBM Security Privileged Identity Manager

Table 3. IBM Security Identity Manager Administrator tasks (continued)

Tasks	Subtasks and reference
On-board service types, service instances, and accounts. If the service type is already pre-configured	1. Create a specific Identity Administrator Role. See Creating roles. 2. Create a Service instance. See Creating services. 3. Reconcile the accounts for the Service by using filters like **erposixsecondgroup** (for Linux) and **erntlocalgroups** (for Windows) where appropriate. See Reconciling accounts immediately on a service.
Assign users to role.	See Adding users to membership of a role.
(Optional) Update user roles	See Modifying roles.
(Optional) Update user group	See Modifying groups.

Persona: Identity Administrator

The Identity Administrator is responsible for the following tasks.

Table 4. Identity Administrator tasks

Tasks	Subtasks and reference
Assign users to role.	See Adding users to membership of a role.
(Optional) Update user roles	See Modifying roles.
(Optional) Update user group	See Modifying groups.

Persona: Identity User

The Identity User uses the IBM Security Identity Manager self-service UI for the following tasks.

Table 5. Identity User tasks in the IBM Security Identity Manager self-service UI

Tasks	Subtasks and reference
Change password	See Changing user passwords.
Reset password	See Resetting user passwords.

Persona: Identity User Manager

The User Manager uses the IBM Security Identity Manager self-service UI for the following task.

Table 6. Identity User Manager task in the IBM Security Identity Manager self-service UI

Tasks	Subtasks and reference
Approve role requests	See Approving user requests.

Roadmap to the IBM Security Identity Manager virtual appliance setup

Use the roadmap as a reference for a server deployment, IBM Security Identity Manager installation in the virtual appliance, and initial configuration settings.

Table 7. Server installation by using a virtual appliance roadmap

Procedure	Reference
Prepare the database server	../installing/cpt/cpt_ic_ins_db_inst.dita
Prepare the directory server	Installation and configuration of IBM Security Directory Server
Set up the virtual appliance on VMware ESXi	Setting up the virtual machine
Install IBM Security Identity Manager in the virtual appliance	Installing the IBM Security Identity Manager virtual appliance
Configure the virtual appliance	Setting up the initial IBM Security Identity Manager virtual appliance
Configure the virtual appliance in a stand-alone or a clustered mode.	Managing the index page

Logging on to the IBM Security Identity Manager virtual appliance console

To get started after you install the IBM Security Identity Manager virtual appliance, you need to know the login URL and the user name and password.

About this task

The default user password to log on to the IBM Security Identity Manager virtual appliance console is `admin`. If you changed the password during the virtual machine setup, use that password. If you did not change the password, use the default administrator password, which is `admin`.

Procedure

1. In a web browser, type the URL as `https://`*`isimva_hostname`* to open the **Appliance Dashboard** of the IBM Security Identity Manager virtual appliance. For example, `https://isimva.example.com`.
2. Enter the user name as `admin`.
3. Enter the password as `admin`.
4. Click **Login**.

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 8. Initial user ID and password for IBM Security Identity Manager

User ID	Password
itim manager	*secret*

Chapter 3. 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 4. Hardware and software requirements

The IBM Security Identity Manager virtual appliance has specific hardware and software requirements.

IBM Security Identity Manager, Version 7.0.0.2 virtual appliance server

- VMware ESXi 5.0 and 5.1.
- CPU: 2.2 GHz, four cores (64-bit).
- Minimum 16 GB system memory.
- Disk space: At least 100 GB free hard disk space.
- Network interface cards: At least 3.

Data tier

Components: IBM DB2®, IBM Security Directory Server

- CPU: 2.2 GHz, four cores (64-bit).
- Minimum 16-24 GB [1] system memory. You can use 16 GB of RAM for one database and one directory server instance.
- Disk space: At least 100 GB free hard disk space.

Database and directory server support

- DB2 Universal Database™ Enterprise Server Version 10.5.0.5
- IBM Security Directory Server Version 6.4
- Oracle 12c Standard and Enterprise Edition Release 1

Other external component support

IBM Security Directory Integrator Version 7.1.1 Fix Pack 4. Additionally, 7.1.1-TIV-TDI-LA0022 is required for Java™ 7 support.

Web browser support

- Mozilla Firefox Versions 24.0 ESR and 31.0
- Microsoft Internet Explorer Versions 10.0 and 11.0
- Google Chrome Version 42.0 for the Identity Service Center user interface and the IBM Security Identity Manager virtual appliance user interface only.

Notes:

[1] System Memory (RAM) to allocate for the database and the directory server.

Appliance format

The IBM Security Identity Manager comes in a virtual appliance format.

The IBM Security Identity Manager virtual appliance can be hosted on the VMware ESXi 5.0 virtual hypervisors.

Virtualization support

IBM Security Identity Manager supports virtualization environments.

See Table 9 for a list of the virtualization products that IBM Security Identity Manager supports at the time of product release.

Table 9. Virtualization support.

Product	Applicable operating systems
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

Prerequisites for IBM Cognos report server

Security Identity Manager supports IBM Cognos Business Intelligence Server version 10.2.1 with IBM Cognos fix pack 1.

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

Table 10. Software requirements for IBM Cognos report server

Software	For more information, see
IBM Cognos Business Intelligence Server, version 10.2.1.1	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.

Table 10. Software requirements for IBM Cognos report server (continued)

Software	For more information, see
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 **IBM Cognos Business Intelligence 10.2.1 Supported Software Environments**. 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. Search for **Web Servers** section.
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 **IBM Cognos Business Intelligence 10.2.1 Supported Software Environments**. 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. Search for **Data Sources** section.

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

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)
- Windows Local Account profile
- Active Directory profile
- IBM Security Privileged Identity Manager profile

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_7.0.0.2/com.ibm.itim_pim.doc_7.0/c_adapters_intro.htm

Chapter 5. What's new in this release

Virtual appliance

- A virtual appliance form factor, making it much simpler to deploy IBM Security Identity Manager. As a new customer, use this new form factor. As an existing customer, continue to receive software stack support through IBM Security Identity Manager V6.0.0.x fix packs.
- Expansion of the Identity Service Center user interface to support new user scenarios.
- Improvements to IBM Security Identity Manager adapters include new support for Oracle 12c, Microsoft SQL Server 2014, SharePoint 2013, and Red Hat Enterprise Linux 7.

Note: IBM Security Identity Manager V7.0.0.2 does not include IBM Security Role and Policy Modeler capability.

The new features in the IBM Security Identity Manager virtual appliance are as follows:

- Configure the IBM Security Identity Manager virtual appliance to send system audit events over emails.
- Use SNMP monitoring to monitor the IBM Security Identity Manager virtual appliance.
- Enable and simplify workflow extension configuration.
- Configure an external library in the IBM Security Identity Manager virtual appliance.
- Enable separate application interfaces for the virtual appliance and the application consoles.
- Use of log file management.
- Use export and import configurations. You can also export, import, access, or download report files.
- Download and view core dumps to diagnose or debug virtual appliance errors.
- Configure static routes to the paired protection interfaces on your virtual appliance.
- Manage hosts file.

For information about IBM Security Identity Manager virtual appliance, see Chapter 1, “IBM Security Identity Manager overview,” on page 1.

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.
- The Identity Service Center supports Google Chrome version 42.0.

These functions are new or changed for the Identity Service Center user interface in IBM Security Identity Manager Version 7.0.0.2:

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.

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_7.0.0.2/com.ibm.itim_pim.doc_7.0.0.2/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 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 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

These functions are new or changed for IBM Security Identity Manager Server Version 7.0.0.2:

Virtualization support for VMWare 5.5

IBM Security Identity Manager now supports VMWare 5.5. See "Virtualization support" on page 14.

Java Runtime Environment (JRE) support

The JRE is installed with WebSphere® Application Server. Some JRE versions are not supported. See WebSphere Application Server support.

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.

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

A connector is provided to allow 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.

The technote has been revised for version 7.0.1 of the connector, which enables bidirectional synchronization between IBM Security Identity Manager and IBM Security Identity Governance.

High Availability and Disaster Recovery

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.

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
```

Workflow options

Options have been added to nodes to allow finer control over workflow processing.

The following options have been 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 has been added for loop nodes:

- **Asynchronous Processing of the Loop Body**

See Loop node.

A flow diagram detailing the influence of the properties has been 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

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 7.0.0.2:

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=swg21688806.

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.

Chapter 6. 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.

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

Chapter 7. 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

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:

- Security Identity Manager Cognos® reports. For a list of all the IBM Cognos reports and the formats, see Report descriptions and parameters.
- 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 11. 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
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
- 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.

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 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_7.0.0/com.ibm.itim_pim.doc_7.0/c_adapters_intro.htm.

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, 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 noncompliant. 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.

For nonapproval activities, you are automatically redirected to the self-care user interface.

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

The 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 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.

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 8. 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 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.

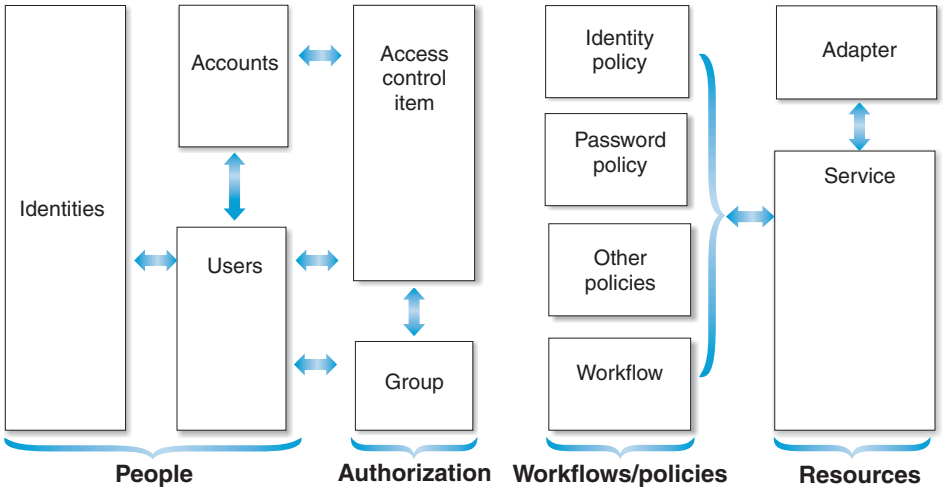

Figure 1. Users, authorization, and resources

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

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:

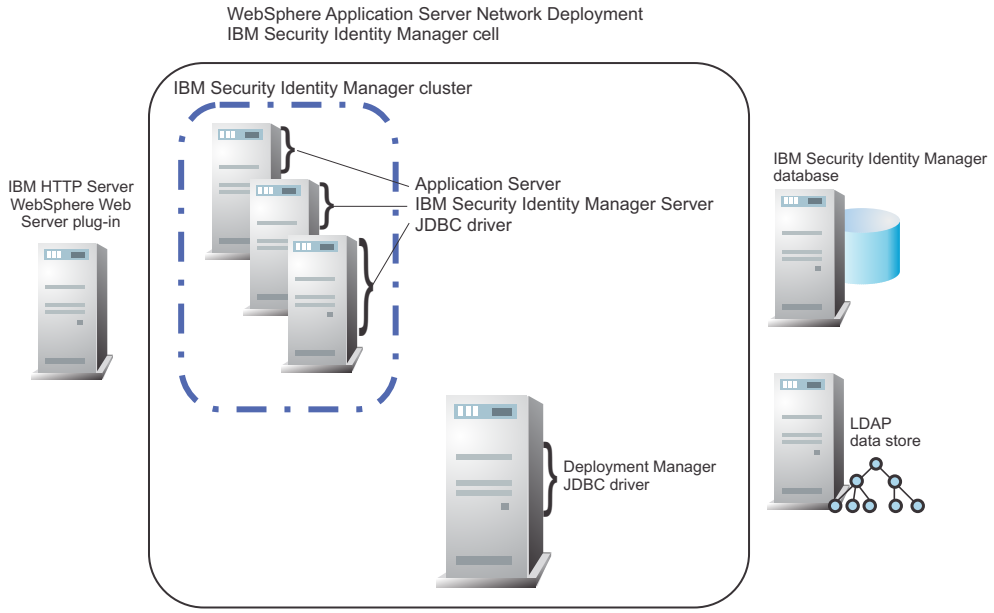

Figure 2. Main components

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 product is IBM DB2 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.

For more information about supported database server products, see Hardware and software requirements.

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 IBM Security Directory Server.

See Hardware and software requirements.

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.

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_7.0.0/com.ibm.itim_pim.doc_7.0/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:

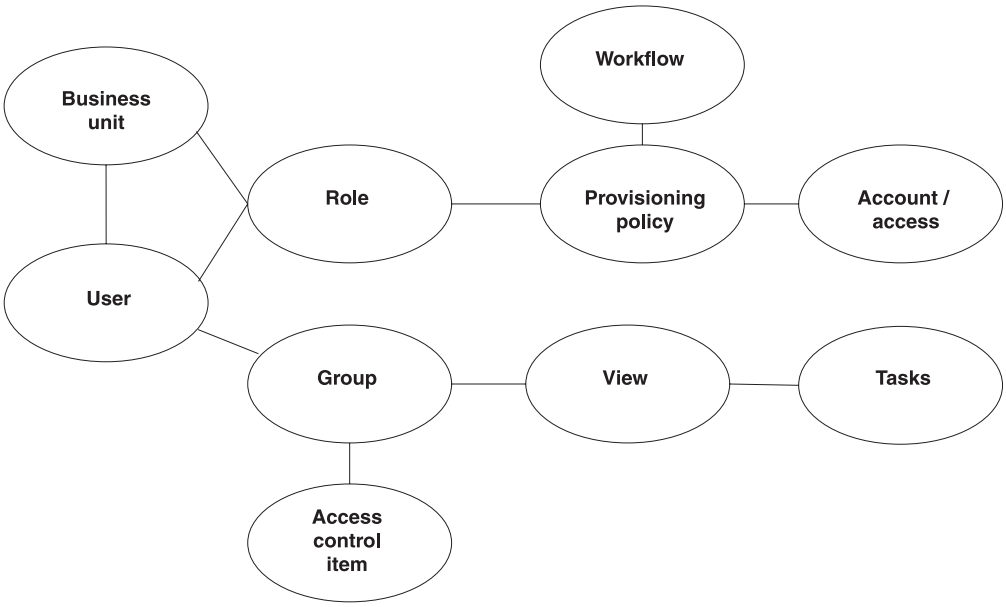

Figure 3. Securing data for user access to resources

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.

Two 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.
- 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 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

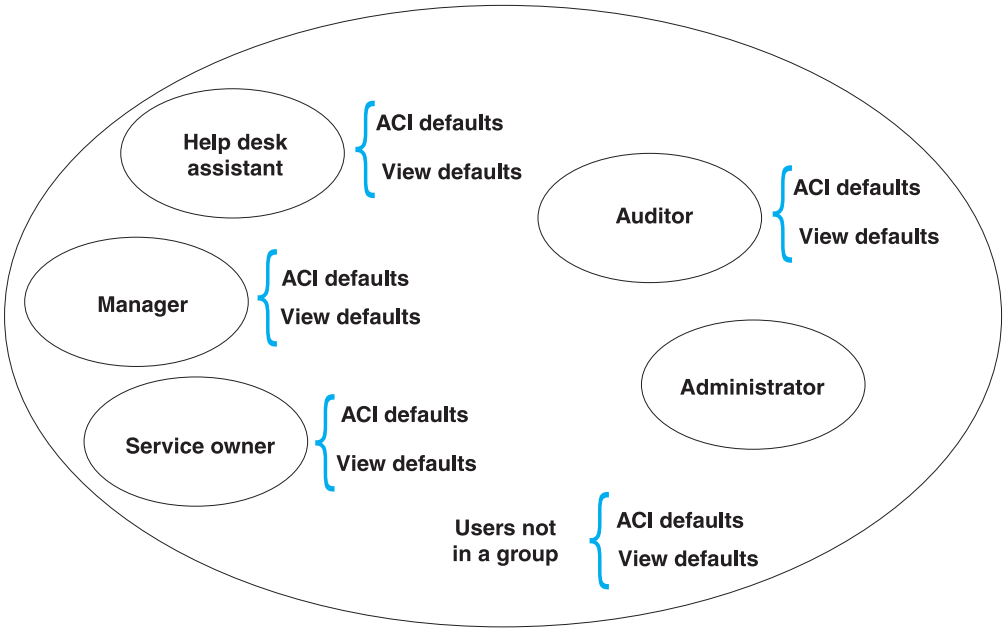

Figure 4. Predefined groups, views, and access control items

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 12. 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 9. Language support

The IBM Security Identity Manager virtual appliance and its integrated products, are translated into the following languages:

Table 13. Supported language per product

Language	IBM Security Identity Manager Version 7.0.0 console	IBM Security Identity Manager Version 7.0 virtual appliance console
Arabic	Yes	No
Chinese (Simplified)	Yes	Yes
Chinese (Traditional)	Yes	Yes
Czech	Yes	Yes
Dutch	Yes	Yes
English (United States)	Yes	Yes
French (Standard)	Yes	Yes
German	Yes	Yes
Greek	Yes	Yes
Hebrew	Yes	No
Hungarian	Yes	Yes
Italian	Yes	Yes
Japanese	Yes	Yes
Korean	Yes	Yes
Polish	Yes	Yes
Portuguese (Brazilian)	Yes	Yes
Russian	Yes	Yes
Spanish	Yes	Yes
Turkish	Yes	Yes

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

Chapter 10. Accessibility features for IBM Security Identity Manager

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

Accessibility features

IBM Security Identity Manager partially conforms to Section 508 standards for accessibility. Detailed compliance information is available by requesting Voluntary Product Accessibility Templates (VPATs) at http://www.ibm.com/able/product_accessibility.

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

Note: The following list of accessibility features might not apply to every page of a user interface.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the IBM Security Identity Manager form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can start any applet, such as the form designer applet, in a separate window. The applet enables Alt+Tab to toggle between that applet and the web interface and for more screen workspace. To start the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes. Themes provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for information about the IBM commitment to accessibility.

Index

T

U

V

W

Printed in USA