# IBM Security Identity Manager

*Glossary*

# Contents

# Chapter 1. Glossary

**A**

**access**
The ability to read, update, delete, or otherwise use a resource. Access to protected resources is typically controlled by system software.

The ability to use data that is stored and protected on a computer system.

A group or role, which is configured as an access in Security Identity Manager. After the access is configured, users can request the group or role access.

**access control**
The process of ensuring that users can access only those resources of a computer system for which they are authorized.

**access control list**
A list that is associated with a resource that identifies all the principals that can access the resource and the permissions for those principals. See also permission and principal.

**access control item (ACI)**
Data that identifies the permissions of principals and is assigned to a resource.

**account**
An entity that contains a set of parameters that define the application-specific attributes of a principal, which include the identity, user profile, and credentials.

**account defaults**
The settings or attributes for an account that Security Identity Manager automatically assigns at the time of creation.

**ACI target**
The resource for which you define the access control items. For example, an ACI target can be a service.

**activity**
In a workflow, the smallest unit of work. When a request requires approval, information, or more actions, the workflow for that request generates the appropriate activities. These activities are added to the to-do lists of the appropriate user. See also workflow.

**adapter**
A set of software components that communicate with an integration broker and with applications or technologies. The adapter does tasks, such as running application logic or exchanging data.

A not apparent, intermediary software component that enables different software components with different interfaces to work together.

**administrative domain**
A logical collection of resources that is used to separate responsibilities and manage permissions. Also referred to as an Admin Domain in the user interface. See also permission.

**adopt**
To assign an orphan account to the appropriate owner. See also orphan account.

**adoption policy**
The set of rules that determine which orphan accounts belong to which owners. See also orphan account.

**agent**
A process that manages target resources on behalf of a system such that the system can respond to requests.

**agent adapters**
A process that resides on the target system. This process enables Security Identity Manager to manage the remote accounts and resources of the target system.

**agent-less adapter**
A process that resides on the IBM® Security Directory Integrator server. This process enables Security Identity Manager to manage target system accounts and resources remotely. See also Directory Integrator adapter

**aggregate message**
A collection of notification messages that are combined into a single email, along with optional user-defined text.

**alias**
In Identity Management, an identity for a user, which might match the user ID. The alias can be used in an adoption rule, such that during reconciliation, the adoption rule is used to determine who owns the account. A person can have several aliases, such as `GSmith`, `GWSmith`, and `SmithG`.

**appliance dashboard**
A web page that can contain one or more widgets that graphically depict state of appliance nodes. It can control service lifecycle events such as start or stop, and can contain easy navigation links to product web interfaces.

**application server**
A server program in a distributed network that provides the execution environment for an application program.

**application user administrator**
A type of person who uses IBM Security Identity Manager to set up and administer the services that are managed by Security Identity Manager or to set up and administer the Security Identity Manager users of those services.

**approval**
A type of workflow activity that allows someone to approve or reject a request. See also workflow.

**attribute**
In BI Modeling, a characteristic of an entity, which is descriptive rather than a unique identifier or aggregating measure.

**audit trail**
A chronological record of events or transactions. You can use audit trails for examining or reconstructing a sequence of events or transactions, managing security, and for recovering lost transactions.

**authentication**
The process of verifying that an entity is the entity that it claims to be, often by verifying a user ID and password combination. Authentication does not identify the permissions that a person has in the system. See also authorization.

**authentication factor**
A piece of information that is used to authenticate or verify an identity for security purposes.

**authorization**
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

**authorization owner**
A user who can manage access control items (ACIs) for a resource.

**authentication provider**
The communication mechanism to an external authentication source. Functions, such as user authentication, group membership, and namespace searches, are made available through authentication providers.

## B

**business unit**
Logically a grouping of people within a business. For example, an organization, organizational unit, location, Business Partner unit, or administration domain. These units can be used to partition users, services, policies, access controls, entitlements, and other entities.

## C

**cardinality**

1. For relational data sources, a numerical indication of the relationship between two query subjects, query items, or other model objects.
2. For OLAP data sources, the number of members in a hierarchy. The cardinality property for a hierarchy is used to assign solve orders to expressions.

**Cascading Style Sheets**
A language that defines a hierarchical set of style rules for controlling the rendering of HTML or XML files in browsers, viewers, or in print.

**certificate**
In computer security, a digital document that binds a public key to the identity of the certificate owner. This document enables the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also Certificate Authority (CA).

**Certificate Authority (CA)**
An organization that issues certificates. The CA authenticates the certificate owner's identity and the services that the owner is authorized to use. The CA issues new certificates, renews existing certificates, and revokes certificates that belong to users who are no longer authorized to use them.

**challenge-response authentication**
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question. They must provide an answer (response) to either receive a new password or receive a hint for specifying the correct password.

**child role**
A role that is a member of another role (parent). The child role is a static organizational role that inherits permissions from all of its parent roles in a hierarchical relationship. A child role can have multiple parent roles.

**cluster**
A group of servers that are connected by a network and configured in highly available network that ensures at least one cluster member is available to process a user request.

**cluster member**
An active member of the current cluster, which can share resources with other cluster members and provide services both to other cluster members and to clients of the cluster.

**cluster manager**
An application server configuration profile that manages the nodes and clusters within a group.

**comma-separated values (CSV) file**
See CSV file.

**common criteria**
A standardized method, which is used by international governments, the United States federal government, and other organizations, for expressing security requirements. These requirements assess the security and assurance of technology products.

**Common Gateway Interface (CGI)**
An Internet standard for defining scripts that pass information from a web server to an application program, through an HTTP request, and vice versa.

**connector**
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships. See also adapter.

**contact**
A named email address to which reports and agent emails can be sent. Contacts are never authenticated.

**content store**
The database that contains the data that is needed to operate, such as report specifications, published models, and security rights.

**credential**
A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication and principal.

A credential represents the ID and authenticators (such as a password) for a resource. See also shared access

**credential pool**
Credential pools are a group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

**credential vault**
The vault is a configured repository that stores credentials for shared access management.

**CSV file**
A common type of file that contains data that is separated by commas.

**D**

**DAML**
See Directory Access Markup Language (DAML).

**data model**
A description of the organization of data in a manner that reflects the information structure of an enterprise.

**data source**
The source of data itself, such as a database or XML file, and the connection information necessary for accessing the data.

**data source connection**
The named information that defines the type of data source, its physical location, and any sign-on requirements. A data source can have more than one connection.

**data warehouse**
A subject-oriented collection of data that is used to support strategic decision making.

A central repository for all or significant parts of the data that the business systems of an organization collect.

**deployment archive**
A file that is used for deployment. A deployment archive contains the data from the content store that is being moved.

**delegate (noun)**
The user who is designated to approve requests or provide information for requests for another user.

**delegate (verb)**
To assign all or a subset of administrator privileges to a user. The user can then perform all or a subset of administrator activities for a specific set of users.

To designate a user to approve requests or provide information for requests for another user.

**delegate administrator**
The user who has all or a subset of administrator privileges over a specific set of users.

**delegate administration**
The ability to apply all or a subset of administrator privileges to another user (the delegate administrator). The user can then perform all or a subset of administrator activities for a specific set of the users.

**deprovision**
To remove an account from a target resource. See also provision.

**digital certificate**
An electronic document that is used to identify an individual, server, company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certificate authority and is digitally signed by that authority. See also Certificate Authority (CA).

**Directory Access Markup Language (DAML)**
An XML specification that extends the functions of Directory Services Markup Language (DSML) 1.0 to represent directory operations. In Security Identity Manager, DAML is used for server to agent communications. See also Directory Services Markup Language v2.0 (DSMLv2)..

**Directory Integrator adapter**
A software component that connects to the Security Directory Integrator environment to interact with target data sources such as LDAP servers. Customized adapters are typically written in Java™ or JavaScript. See also agent-less adapter

**directory server**
A server that can add, delete, change, or search directory information for a client. For example, an LDAP server.

**Directory Services Markup Language v1.0 (DSMLv1)**
An XML implementation that describes the structure of data in a directory and the state of the directory. DSML can be used to locate data into a directory. DSMLv1 is an open standard that is defined by OASIS. See also Directory Services Markup Language v2.0 (DSMLv2).

**Directory Services Markup Language v2.0 (DSMLv2)**
An XML implementation that describes the operations that a directory can perform and results of those operations. Such descriptions include how to create, modify, and delete data. Whereas DSMLv1 can be used to describe the structure of data in a directory, DSMLv2 can be used to communicate with other products about that data. DSMLv2 is an open standard that is defined by OASIS. See also Directory Services Markup Language v1.0 (DSMLv1).

**distinguished name (DN and dn)**
The name that uniquely identifies an entry in an LDAP directory. A distinguished name is made up of name-component pairs. For example:

```
cn=John Doe,o=My Organization,c=US
```

**domain administrator**
The owner of an administrative domain organizational unit. That relationship grants a set of permissions to the administrator to manage resources in that administrative domain. See also administrative domain.

**dynamic content tags**
A set of XML tags that enables the administrator to provide customized information in a message, notification, or report. These tags are based on the XML Text Template Language (XTTL) schema. See also XML Text Template Language (XTTL).

**dynamic organizational role**
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role. See also organizational role.

## E

**entitlement**
The capability-based reason that a user is given a permission or set of permissions to access IT resources (services).

**entity**
An object about which you want to store information or manage. For example, a person and an account are both entities.

**entity type**
Categories of managed objects. See also entity.

**escalation**
The process that defines what happens and who acts when an activity was not completed in the specified amount of time.

**escalation limit**
The amount of time, for example, hours or days, that a participant must respond to a request before an escalation occurs. See also escalation.

**event**
The encapsulated data that is sent as a result of an occurrence, or situation, in the system. An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

**export**
The process that involves preserving system data in a file so that the data can later be restored in a system. Security Identity Manager uses a JAR file. See also import.

## F

**failover**
An automatic operation that switches to a redundant or standby system during a software, hardware, or network interruption.

**FESI**
See Free ECMAScript Interpreter.

**FESI extension**
A Java extension that can be used to enhance JavaScript code and then be embedded within a FESI script.

**Free ECMAScript Interpreter (FESI)**
An implementation of the ECMAScript scripting language, which is an ISO standard scripting language that is like the JavaScript scripting language.

**form**
In Security Identity Manager, a customizable user interface window from which you can create, view, and modify account, service, or user attributes.

## G

**gateway**
An extension of a web server program that transfers information from the web server to another server. Gateways are often CGI programs, but can follow other standards such as ISAPI and Apache modules.

**group**
A collection of users on a service.

**grouping**
In reporting, the process of organizing common values of query items together and displaying only the value once.

**group management**
The use of lifecycle operations (create, remove, add members, remove members) on groups.

## H

**help desk assistant**
A person who uses Security Identity Manager to assist users and managers with managing their accounts and passwords.

**hierarchy**
The organization of a set of entities into a tree structure, with each entity (except the root) having one or more parent entities and an arbitrary number of child entities.

**high availability**
The process of monitoring system resources and applications for errors and recovering from those errors to maintain availability of those resources for consumers.

**hosted service**
A hosted service is shown as a logically distinct service in Security Identity Manager. The hosted service references a nonhosted service (sometimes called a concrete service because it represents a managed resource or target) within another organization.

## I

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

**identity feed**
The automated process of creating one or more identities from one or more common sources of identity data (for example, identity data can be fed from an HR system by using a DSML file).

**identity governance**
A set of rules that define the access privileges of a user.

**identity policy**
The policy that defines the user ID to be used when an account is created for a user.

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

**IIOP (Internet Inter-ORB Protocol)**
A protocol that is used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

**import**
The process that involves restoring or migrating system data that was preserved in a file (for Security Identity Manager the file is a JAR file) to a system. See also export.

**ITIM group**
A list of Security Identity Manager accounts. Membership within an ITIM group determines the access to data within Security Identity Manager.

**ITIM user**
A user who has a Security Identity Manager account.

## J

**Java Database Connectivity**
See JDBC.

**JDBC (Java Database Connectivity)**
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call-level API for SQL-based and XQuery-based database access. Database vendors provide a JDBC interface implementation specific to their platform that enable Java programs to interact with the database.

**join directive**
The set of rules that define how to handle attributes when two or more provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

## L

**layout**
The arrangement of printed matter on a screen or page, including margins, line spacing, type specification, header and footer information, indents, and more.

**LDAP (Lightweight Directory Access Protocol)**
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. This protocol does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

**LDAP Data Interchange Format**
See LDIF.

**LDAP directory**
A type of repository that stores information about people, organizations, and other resources and that is accessed by using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

**LDAP filter**
A search filter that narrows the results from an LDAP search.

**LDIF (LDAP Data Interchange Format)**
A file format that is used to describe directory information and changes that need to be applied to a directory. This format enables the exchange of directory information between directory servers that are using LDAP.

**level**
A set of entities or members that form one section of a hierarchy in a dimension and represent the same type of object. For example, a geographical dimension might contain levels for region, state, and city.

**life cycle**
Passage or transformation through different stages over time. For example, markets, brands and offerings have life cycles.

The life cycle of entities in Security Identity Manager encompasses the create, read, update, and delete operations that are required to manage those entities. By extending those operations, you can customize the lifecycle of entities in Security Identity Manager. For example, customers typically extend the delete operation and change it to suspend only the account. Suspending the account enables auditors to see when the account was deactivated and last accessed.

**life cycle rules**
A life cycle rule contains an LDAP filter, an operation, and a schedule. The rule determines which operations to use when automatically handling commonly occurring events on a set schedule. For example, suspending an account that is inactive for some time.

**Lightweight Directory Access Protocol**
See LDAP.

**Load Balancer**
A tool that acts as a reverse proxy and distributes network or application traffic across a number of servers to increase capacity and reliability.

**locale**
A setting that identifies language or geography and determines formatting conventions such as collation, case conversion, character classification, the language of messages, date and time representation, and numerical representation.

**location**
An organizational unit that is a subdivision of an organization, typically based on geographical area.

## M

**mail**
A type of workflow activity that sends an email notification to one or more users about a request.

**mailbox-enabled**
A mailbox-enabled user can send and receive messages, and store messages on the Exchange server mailboxes.

**mail-enabled**
An Active Directory user account that has an email address that is associated with it, but has no mailbox on the Exchange server. A mail-enabled user can send and receive email by using another messaging system. If you send messages to a mail-enabled user account, then these messages pass through the Exchange server, and are forwarded to an external email ID of that user account.

**managed resource**
An entity that exists in the runtime environment of an IT system and that can be managed (typically named a service).

**manager**
A type of person who uses Security Identity Manager to manage their own accounts and passwords or the accounts and passwords of those people that they supervise.

**manual service**
A type of service that requires manual intervention by the service owner to complete the provisioning request.

**member node**
A cluster node that can process a user request.

**model**
A physical or business representation of the structure of the data from one or more data sources. A model describes data objects, structure, grouping, relationships, and security. In Cognos BI, a model is created and maintained in Framework Manager. The model or a subset of the model must be published to the IBM Cognos server as a package for users to create and run reports.

## N

**namespace**
The set of unique names that a service recognizes.

Space that is reserved by a file system to contain the names of its objects.

**nested group**
A group that is contained within another group. See also group.

**notification**
An email message that is sent to users or systems that indicates that a change was made that might be of interest to the receiver.

## O

**object**
In Report Studio, an empty information container that can be dragged to a report from the toolbox tab and then filled with data. Reports are made up of objects, which include cross-tabs, text items, calculations, graphics, and tables.

**object class**
The specific type of object, or subcategory of classes, that an access control item can protect. For example, if the protection category is account, then the object class can be the type of account, such as an LDAP user account. See also protection category.

An entity that defines the schema for a service or an account.

**operation**
A specific action (such as add, multiply, or shift) that the computer does when requested.

**operational workflow**
A workflow that defines the lifecycle process for accounts, persons, and other entities. The operational workflows include the create, read, update, and delete operations for each entity. See also workflow.

**organization**
A hierarchical arrangement of organizational units, such that each user is included only once. See also organizational unit.

**organization tree**
A hierarchical structure of an organization that provides a logical place to create, access, and store organizational information. Also referred to as an organization structure.

**organizational role**
A logical group of principals that provide a set of permissions. Access to operations is controlled by granting access to a role. An organizational role can also represent a group of principals based on business job title or other business-related attributes. See also dynamic organizational role and static organizational role.

**organizational unit**
A type of organizational container that represents a department or similar grouping of people.

**orphan account**
On a managed resource, an account whose owner cannot be automatically determined by Security Identity Manager.

**ownership type**
A category that classifies ownership accounts in IBM Security Identity Manager. One account can have only one type of ownership. Accounts can be marked with different ownership types that depend on their use. Password management process is affected by the type of ownership. For example, password synchronization provides change of password for accounts that have ownership type, "Individual".

The following are the default ownership types:

- Device
- Personal
- System
- Vendor

As an administrator, you can customize ownership types.

## P

**package**
A subset of a model, which can be the whole model, to be made available to the Cognos server. See also metric package.

**parent role**
A static organizational role where one or more of its members is another role (child role). The parent role grants a set of permissions to the child role in a hierarchical relationship. A parent role can have multiple child roles.

**participant**
In Identity Management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow. See also workflow.

**password**
In computer and network security, a specific string of characters that is used by a program, computer operator, or user to access the system and the information that is stored within it.

**password retrieval**
In Identity Management, the method of retrieving a new or changed password by accessing a designated website and specifying a shared secret. See also shared secret.

**password strength rules**
The set of rules that a password must conform to, such as the length of the password and the type of characters that are allowed (or not allowed) in the password.

**password policy**
A policy that defines the password strength rules. A password strength policy is applied whenever a password is set or modified. See also password strength rules.

**password synchronization**
The process of coordinating passwords across services and systems such that only a single password is needed to access those multiple services and systems.

**permission**
Authorization to do activities, such as reading and writing local files, creating network connections, and loading native code. In Security Identity Manager, permissions to manage objects are encapsulated in ACI.

**person**
An individual in the system that has a person record in one or more corporate directories.

**personal profile**
The data that describes a user within the system, such as the user name, password, contact information, and others.

**plug-in**
A software module that adds function to an existing program or application.

**policy**
A set of considerations that influence the behavior of a managed resource or a user.

**policy enforcement**
The manner in which Security Identity Manager acts on accounts that do not meet provisioning policy requirements for a specific service.

**policy join**
In Identity Management, a directive that defines how attributes are handled when policies conflict. This conflict can occur when multiple policies are defined for the same users or groups of users on the same target service, service instance, or service type.

**post office**
A component that collects notifications from the appropriate workflow activities that have activity group topic IDs defined. The component distributes those notifications to the appropriate workflow participants. The distribution is done in aggregate form.

**primary node**
A cluster node that currently has the principle copy of a cluster resource. All replications of a resilient resource originate from the primary copy of the resource.

**principal**
A person or group that is granted permissions.

An entity that can communicate securely with another entity.

**privilege**
See permission.

**product locale**
The code or setting that specifies which language, regional settings, or both to use for parts of the product interface, such as menu commands.

**profile**
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

**protection category**
The category of classes that an access control item can protect. For example, accounts or persons. See also object class, ACI.

**provision**
In Identity Management, to set up and maintain the access of a user to a system.

In Identity Management, to create an account on a managed resource.

**provisioning**
In Identity Management, the process of providing, deploying, and tracking a service or component.

**provisioning policy**
A policy that defines the access to various managed resources (services), such as applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

**publish**
In Cognos BI, to expose all or part of a Framework Manager model or Transformer PowerCube, through a package, to the IBM Cognos server, so that the data can be used to create reports and other content.

## Q

**query**
The simple report specifications that are created and edited by Query Studio.

**query item**
A representation of a column of data in a data source. Query items might appear in a model or in a report and contain a reference to a database column, a reference to another query item, or a calculation.

**query subject**
A named collection of query items that are closely functionally related. Query subjects are defined by using Framework Manager to represent relational data and form the set of available data for authoring reports in Query Studio and Report Studio. A query subject is similar to a relational view in that it can be treated as a table but does not necessarily reflect the data storage.

## R

**recertification**
The process of validating and possibly updating your credentials with a system, typically after a specified time interval.

**recertification policy**
A policy that defines the life cycle rule for automatically validating accounts and users in the provisioning system at a specified frequency. The policy sends approvals to the recertification policy participants to ask if the accounts or users are still to be certified. See also life cycle rules.

**reconciliation**
The process of synchronizing data in Security Identity Manager with data on a managed resource.

**registration**
The process of accessing a system and requesting an account on that system.

**registry**
A repository that contains access and configuration information for users, systems, and software.

**relationship**
A defined association between two or more data entities. This association is used to define Security Identity Manager access control items (ACIs) and to specify workflow participants.

**relevant data**
The data that is used and referenced by workflow activities in a workflow operation. For example, in adding a person operation workflow, the person entity is a relevant data item. See also workflow.

**report**
A set of data that is deliberately laid out to communicate business information.

**report output**
The output that is produced as a result of running a report specification against a data set.

**repository**
A persistent storage area for data and other application resources. Common types of repositories are databases, directories, and file systems.

**request**
The item that initiates a workflow and instigates the various activities of a workflow. See also workflow.

**Request Access wizard**
A form of user assistance where you can change or customize the appearance and content of several Security Identity Manager components such as user cards, access cards, badges, and search control properties.

**request approval workflow**
A workflow that defines the business logic. Typically it contains a series of activities and participants. The workflow is used to approve requests, such as account requests and access requests. See also workflow.

**request for information (RFI)**
A workflow activity that requests additional information from the specified participant. See also workflow.

**resource**
A hardware, software, or data entity. See also managed resource.

**response file**
An ASCII file that can be customized with the setup and configuration data that automates an installation. During an interactive installation, the setup and configuration data must be entered, but with a response file, the installation can proceed without any intervention.

**restore**
To activate an account that was suspended and inactive.

**rights**
See permission.

**role**
A logical group of principals that provide a set of permissions. Access to resources is controlled by using provisioning policy to grant access to a role. A role can also represent a group of principals that is based on business job title or other business-related attributes. See also organizational role.

**role classification**
The identification of a role by its category that differentiates one category from another, such as a system application role from a business role.

**role hierarchy**
A hierarchical structure of inheritance in which a role can be a parent role or child role or both.

**role ownership**
The ability of a user to control membership in a role and to approve users who are assigned to that role. Both users and organization roles can be owners of an organizational role. If a role is assigned as an owner of another role, then all the members of the owner role become owners of that other role.

**role relationship**
The ability to establish parent-child (inheritance) associations between roles. Inheritance between roles can directly affect policies' members, which govern user access.

An example of inheritance that affects a policy's members is a provisioning policy grants the members of the 'Role A' with an Linux account. If the Role A is associated with another role, 'Role B', where Role A is the parent of B; the provisioning policy now grants the members of Role A and Role B (because of inheritance) a Linux account.

**rule**
A set of conditional statements that enable computer systems to identify relationships and run automated responses.

## S

**schema**
The fields and rules in a repository that comprise a profile. See also profile.

**scope**
In Identity Management, the set of entities that a policy or an access control item (ACI) can affect.

**Secure Sockets Layer (SSL)**
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

**security**
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

**security administrator**
A type of person who sets up and administers Security Identity Manager for users, managers, help desk assistants, and application user administrators.

**self-registration**
See registration.

**separation of duty policy**
A logical container of separation rules that define mutually exclusive relationships among roles.

**service**
A representation of a managed resource, application, database, or system. In Security Identity Manager specifically, a service represents the user repository for a managed resource.

**service owner**
An individual who uses Security Identity Manager to set up and administer the accounts on the services that are managed by Security Identity Manager. See also service.

**service prerequisite**
A service on which a user must first have an existing account to receive a new account on another service.

**service provider**
An organization that provides services to the user.

**service selection policy**
A policy that determines which service to use in a provisioning policy. See also provisioning policy.

**service type**
A category of related services that share the same schemas. See also service.

**session**
The time during which an authenticated user is logged on.

**shared access**
Access to a resource or application by using a shared credential.

**shared access policy**
Shared access policy authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

**shared secret**
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

**single sign-on (SSO)**
The ability of a user to log on once and access multiple applications without having to log on to each application separately.

**sponsor**
A type of workflow participant who is designated to respond to a workflow manual activity for a Business Partner person or organization. A workflow manual activity can either be an approval activity, request for information activity, or work order activity.

**static organizational role**
An organizational role that is manually assigned to a person. See also organizational role.

**supervisor**
A role that identifies the person who supervises another set of users. This role is often responsible for approving or rejecting requests that are made by those users.

**suspend**
To deactivate an account so that the account owner cannot access the service (managed resource).

**system administrator**
An individual who is responsible for the configuration, administration, and maintenance of Security Identity Manager.

**summary**
In reporting and analysis, an aggregate value that is calculated for all the values of a particular level or dimension. Examples of summaries include total, minimum, maximum, average, and count.

## T

**tenant**
In a hosted service environment, a virtual enterprise instance of an application. Each instance of Security Identity Manager (defined on separate tenant IDs) can share directory servers or relational databases while it remains a separate service instance.

**to-do list**
A collection of outstanding activities. See also activity.

**topic**
The group ID of a notification message set in manual workflow activities in the workflow designer. This ID enables messages to be grouped based on the same task and aggregated to each recipient of the message.

**transfer**
In Identity Management, the process of moving a user from one business unit to a different business unit within the same organization.

**transition**
A connection between two workflow activities. See also workflow.

## U

**universally unique identifier (UUID)**
The 128-bit numerical identifier that is used to ensure that two entities do not have the same identifier. The identifier is unique for all space and time.

**user**
Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system. The individual who uses Security Identity Manager to manage their accounts and passwords. A user represents a person that is managed by Security Identity Manager. An *ITIM user* represents a user who has a Security Identity Manager account and can use Security Identity Manager.

**user recertification policy**
A policy that provides a periodic revalidation process for a user's role memberships, accounts, and group membership of accounts. User recertification combines recertification of multiple resources and memberships into a single activity to be completed by a designated approver. See also recertification policy.

## V

**view**
A collection of various graphical user interfaces for a product that represent the set of tasks that a particular type of user is allowed to do. Administrators can customize views to contain different collections of graphical user interfaces.

**virtual appliance**
An appliance that is installed on a virtual machine. A prepackaged software application that provides some well-defined business workflow, making it easier to deploy a solution with minimal configuration. Many tiers of operating systems and applications can be packaged as a single virtual appliance.

## W

**work area**
The area within a studio that contains the report, analysis, query, or agent currently being used.

**work order**
A workflow activity that requires a participant to do an activity outside of the scope of the system. See also workflow.

**workflow**
The sequence of activities that is done in accordance with the business processes of an enterprise. See also activity.

**workflow notification**
A message sent to a user defined in the workflow, which contains information about the success, failure, or required action of an activity.

## X

**XML Text Template Language (XTTL)**
An XML schema that provides a means for representing dynamic content within a message, notification, or report. The XML tags are also called dynamic content tags. See also dynamic content tags.