CA Identity Manager

Glossary

r12

CA Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory, also known as CA Directory

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Glossary Entries

This section contains the following topics:

A

access role

An *access role* controls user privileges in applications other than Identity Manager.

add action

An *add action* occurs when a user is added as a member or administrator of a role. You define the add action when you create or modify the role.

admin policy

An *admin policy* defines admin rules, scope rules, and administrator privileges for a role. You can define several admin policies for a role. Each policy indicates that if an administrator meets the condition in the admin rule, that administrator has the scope and administrator privileges defined for the policy.

admin role

An *admin role* enables Identity Manager administrators to manage objects, such as organizations, groups, users, roles, and tasks in an Identity Manager environment.

admin rule

An *admin rule* defines who is an administrator of a role. You define an admin rule as part of an admin policy for the role.

admin task

An *admin task* is an administrative function that a user can perform in Identity Manager. Examples of admin tasks include Create User, Modify Group, and View Role Membership.

administrative tools

Administrative tools allow you to configure and use Identity Manager. The tools and samples include configuration files, scripts, utilities, and the jar files that you need to compile custom objects with Identity Manager APIs and API samples. The Administrative tools are in your Identity Manager installation directory.

administrator

An *administrator* is an Identity Manager user who can use or assign admin roles. *User* is a general term for any Identity Manager account, which may have admin roles, access roles, or both.

alias

An *alias* is a unique string that is added to the URL for access to an Identity Manager environment. There are two types of aliases:

- protected alias—Added to the URL for accessing protected tasks in the User Console.

  For example, if the protected alias for an environment is employees, the URL for accessing that environment is:

  http://<myserver.mycompany.org>/idm/employees

  where <myserver.mycompany.org> is the fully qualified domain name of the server where Identity Manager is installed.

- public alias—Added to the URL for accessing public tasks, such as self-registration and forgotten password tasks.

  For example, if the public alias is public, the URL for accessing a public task is:

  http://<myserver.mycompany.org>/idm/public/index.jsp?task.tag=<tasktag>

  where <tasktag> is the tag for the task to invoke.

  You specify the task tag when you create the task in the Identity Manager User Console.

You specify a protected and public alias when you create an Identity Manager environment in the Identity Manager Management Console.

Apache Ant

Apache Ant is a software tool for automating software build processes. It is similar to make but is written in Java, and is best suited to building Java projects.

Apache Directory Server (ApacheDS)

The *Apache Directory Server (ApacheDS)* is an embeddable LDAP server written in Java.

approval

An *approval* is an action that must be performed before Identity Manager can complete certain tasks. In a simple approval example, a manager must approve a new title before Identity Manager changes the title in a user's profile. In Identity Manager, an approval is associated with a workflow approval task. In the workflow engine's user interface, an approval is associated with a workflow activity.

C

connector

A *connector* is the software that enables communication between a Provisioning Server and an endpoint system. A dynamic connector can be generated by Connector Xpress, and a custom static connector can be developed in Java or C++.

C++ Connector Server

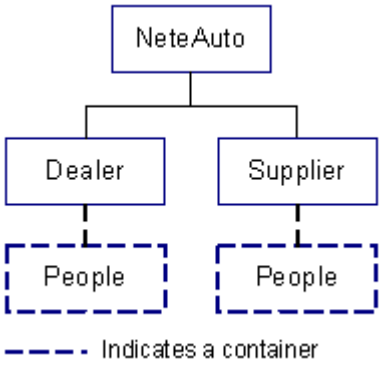
The *C++ Connector Server* is a connector server that manages C++ connectors. It can be installed on the Provisioning Server or on a remote system. The C++ Connector Server provides an object-oriented application framework that simplifies development of connectors, which are responsible for communication between the C++ Connector Server and the endpoint.

Connector Xpress

Connector Xpress is a utility for managing dynamic connectors, mapping dynamic connectors to endpoints, and establishing routing rules for endpoints.

container

A *container* is a set of objects of a specific type stored in an organization. If you specify a container in the directory configuration file, Identity Manager manages only entries in the container. For example, if you specify a user container called People, Identity Manager manages users in the People container. You cannot specify containers for organizations.



converter

A *converter* is a Java class used by the Java CS infrastructure for converting data to and from endpoint-specific formats.

D

delegated administration

Delegated administration is the management of users and their application access by having different Identity Manager users perform the functions of modifying, assigning, and using a role. For example, the administrator sets up an Identity Manager environment and creates roles with rules about who can be an owner, administrator, or member of the role.

deployment

Deployment describes two different actions, saving metadata from Connector Xpress to an endpoint in the Provisioning Server or making a new connector implementation available to the Java CS by placing its jcs-connector-*.jar file into the <jcs_home>/lib directory.

directory configuration file (directory.xml)

The *directory configuration file* describes the content and structure of a user store to Identity Manager. You use the directory configuration file to create an Identity Manager directory.

Identity Manager provides directory configuration templates for each type of supported user store.

directory information tree (DIT)

A *directory information tree* (DIT) is a tree of objects presented to clients by an LDAP server in which the clients can directly name and manipulate those objects by issuing LDAP commands.

Distinguished Name (DN)

A *Distinguished Name (DN)* is a unique name for an entry in a directory service. In LDAP, this consists of its *Relative Distinguished Name (RDN)* constructed from some attributes in the entry, followed by the parent entry's DN. The DN is analogous to a full filename, and the RDN is analogous to a relative filename.

dynamic connector

A *dynamic connector* has metadata that is generated and maintained by end users using Connector Xpress. The metadata drives the behavior of the dynamic connector at runtime.

E

email template

An *email template* is an HTML file used to generate dynamic email messages containing boilerplate text plus case-specific text.

email template object

An *email template object* is an Identity Manager-provided object that is available to email templates and that allows case-specific text to be inserted into a dynamic email message. For example, in an email notification resulting from an administrator adding a user to an organization, methods in the _eventContextInformation object can insert the administrator’s name, the user’s name, and the organization name.

endpoint

An *endpoint* is a specific installation of a platform or application, such as Active Directory or Microsoft Exchange, which communicates with the Provisioning Server to synchronize information. An endpoint is managed by a connector server using a specific connector.

endpoint account

An *endpoint account* is a user's identity in an endpoint managed by the provisioning server. An account provides users with access to additional resources, such as email or databases. Identity Manager administrators can provide users with accounts by assigning a provisioning role.

endpoint Type

An *endpoint type* is a logical grouping of endpoints. There is one connector for each endpoint type, but there can be multiple endpoint systems for each connector.

eTrust Admin Server

See *Provisioning Server*.

event

An *event* is an Identity Manager-detectable occurrence that Identity Manager generates for a task. Multiple events can be generated for a task. If one or more of a task's events are mapped to a workflow process, the task is workflow-controlled. Identity Manager cannot complete a workflow-controlled task until workflow processes mapped to the task's events are completed.

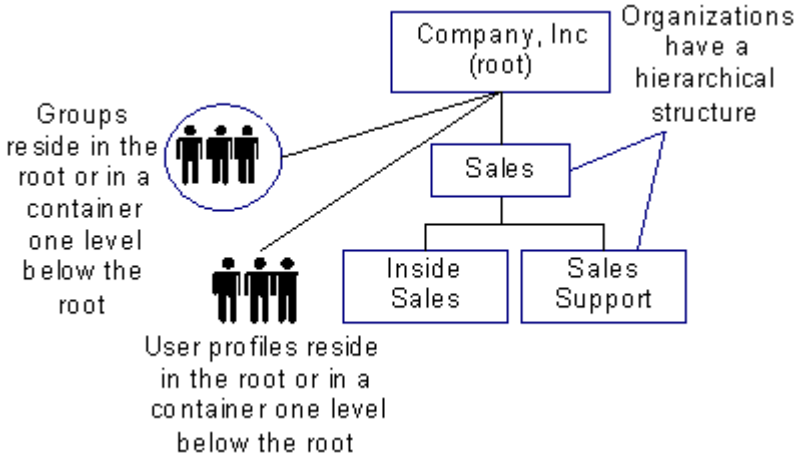
external task

An *external task* performs a function in a business application. External tasks can pass information to an application to generate user-specific, group-specific, or organization-specific tasks. For example, an external task may pass information about an organization to an application that generates purchase orders. The administrator performing the task can view open purchase orders for the organization from the Identity Manager User Console.

F

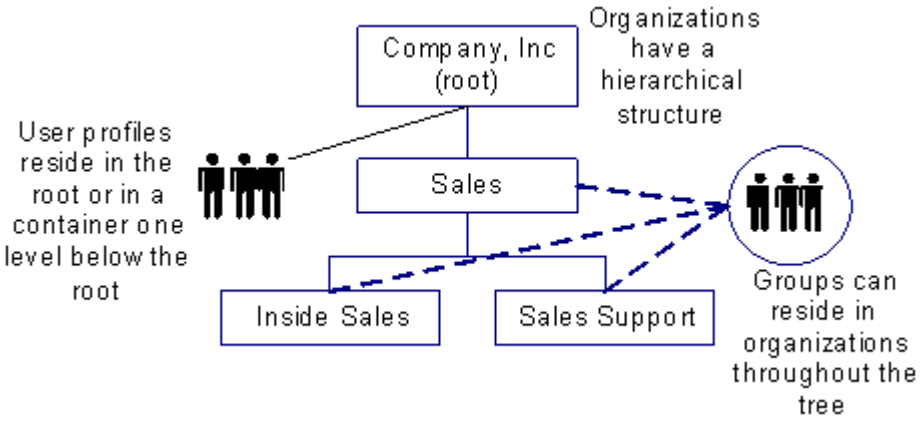
flat directory

A *flat directory* is an LDAP directory in which users and groups are stored at the root (as defined in the SiteMinder user directory connection) or in a container below the root. To facilitate user management and delegation in flat directory structures, users and groups belong to logical organizations. The logical organization is stored as an attribute in user and group profiles.



flat user directory

A *flat user directory* is an LDAP directory in which organizations and groups are stored hierarchically, but users are stored at the root or in a container one level below the root. In flat user directory structures, users belong to logical organizations. A user's logical organization is stored as an attribute in a user's profile.



G

global user

A *global user* is an object maintained by the Provisioning Server which corresponds to one person or other identity that needs access to the Provisioning Server or the endpoints that it manages. A global user object contains information such as the person's name, global user name, account name, password settings, job title, phone number, and address. The primary purpose of a global user is to tie together a person's accounts.

group

A *group* associates users who have something in common. Users from different organizations may belong to the same group—for example, members of the Sales, Marketing, Engineering, and Documentation organizations can form a Product Team. Groups also can be used to establish access privileges. If the user store is an LDAP directory, groups can be nested or dynamic.

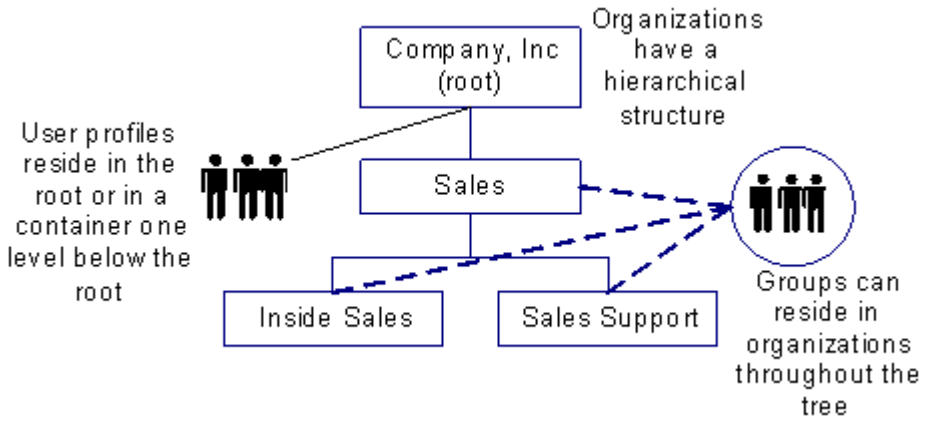
H

handler

A *handler* is a Java object that processes logical attribute data or that performs custom business logic. You can write custom logical attribute handlers and business logic task handlers.

hierarchical directory

A *hierarchical directory* is an LDAP directory that contains a parent organization (root) and suborganizations. The suborganizations may also have suborganizations, which creates a multi-level structure. Users and groups can exist at any level within the directory.



I

Identity Manager directory

An *Identity Manager directory* is a component of an Identity Manager environment. An Identity Manager directory is a user store plus metadata that describes how objects are stored in the user store and represented in the Identity Manager User Console.

Identity Manager environment

An *Identity Manager environment* is a view of a management namespace that allows an Identity Manager administrator to manage different types of objects, such as users, groups, and organizations, with a set of associated roles and tasks. An Identity Manager environment includes an Identity Manager directory, a system manager, default task and role definitions, self-service tasks, and workflow definitions.

Identity Manager Management Console

The *Identity Manager Management Console* is a Web-based tool for creating an Identity Manager directory, configuring an Identity Manager environment, assigning a system manager, and enabling custom features.

Identity Manager User Console

The *Identity Manager User Console* is a Web-based user interface that Identity Manager administrators use to perform admin tasks.

Identity Manager user store

The *Identity Manager user store* is the authoritative source for various types of users required for business operations. These users can be employees, consultants, customers or partners. This user store also contains information about groups, and organizations (if supported). In an Identity Manager deployment that includes provisioning, some users may have a corresponding account in a provisioning directory.

identity policy

An *identity policy* is a set of business changes that occurs when a user meets a certain condition or rule. These changes can include assigning or revoking roles, assigning or revoking group membership, and updating attributes in a user profile.

J

Java Connector Server (Java CS)

The *Java Connector Server (Java CS)* is a server component, written in Java, which handles hosting of, routing to, and aggregation of Java connectors. The Java CS is architecturally and functionally similar to the C++ Connector Server.

JDBC (Java DataBase Connectivity)

JDBC (Java Database Connectivity) is a Java API for executing SQL statements against relational databases.

JDK (Java Development Kit)

JDK (Java Development Kit) is a software development kit for producing Java applications.

JIAM (Java Identity and Access Management)

JIAM (Java Identity and Access Management) is a Java front end to the Provisioning Server.

JNDI (Java Naming and Directory Interface)

JNDI (Java Naming and Directory Interface) is a Java API that enables access to naming and directory services such as LDAP servers.

JVM (Java Virtual Machine)

JVM (Java Virtual Machine) is an execution environment that converts Java bytecode to machine language and executes it.

L

LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol) is a software protocol for locating organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. An LDAP directory is a simple tree hierarchy which distributed among many servers.

list screen

The *list screen* controls the columns and sorting of a list of items on a tab in an admin task, such as a list of roles or users.

Log4j

Log4j is a popular Java logging library used primarily as a debugging tool, and in Java CS custom connector development.

logical attribute

A *logical attribute* is data that is presented to the user on a task screen, but that is not written to the data store. Logical attribute data is managed by a logical attribute handler.

M

managed object

A *managed object* is a user, group, or organization object defined in the Identity Manager directory, or an admin role, admin task, access role, or access task object defined within an Identity Manager environment. A managed object contains a set of attributes that define the object. Using the Identity Manager API, you can access managed objects through a provider or a task session.

member policy

A *member policy* defines a member rule and scope rules for a role. You can define several member policies for one role. For each policy, if a user meets the condition in the member rule, that user has the scope for using the role that is defined in the policy.

member rule

A *member rule* defines who can use a role. You define a member rule as part of a member policy for the role.

metadata

Metadata is XML data that describes the structure of a connector to the Java CS.

N

namespace

A *namespace* is a specific type of endpoint system.
See *endpoint type*.

notification

Notification is an optional workflow feature that informs a set of users when an event occurs, such as when an event is approved.

O

object-task navigation

Object-task navigation is a method that allows users to select an object in the User Console and view all of the tasks that they can perform on that object in a pop-up menu. From the menu, the user can select the task that they want to use. Once the task is complete, users can select another task from the pop-up menu without having to search for the object again.

option

See *Connector.*

organization

An *organization* represents a company's business unit. Organizations are logical groups of user profiles. For example, the sales organization may contain user profiles for a company's sales force.

owner rule

An *owner rule* defines who can modify a role. You can define several owner rules for a role.

P

participant

A *participant* is a person who is authorized to perform a workflow activity. In Identity Manager, participants are also called *approvers*, since they must approve or reject the task under workflow control.

participant resolver

Participant resolver is a Java object that determines the participants in an Identity Manager workflow process.

password policy

The *password policy* is a SiteMinder feature that lets you specify rules for passwords, including expiration dates, constraints, and composition requirements.

physical attribute

A *physical attribute* is data that is written to the data store and that can be displayed on an Identity Manager task screen. A physical attribute can also be represented on a task screen by a logical attribute.

physical directory

The *physical directory* refers to the LDAP user directory that Identity Manager manages. The physical directory stores information about users, groups, and organizations.

primary object

The *primary object* is the target object of a task—for example, a user object in a Create User task. In the Identity Manager API, the primary object is called the subject of the task.

profile screen

The *profile screen* controls the attributes displayed on a profile tab.

profile tab

A *profile tab* controls basic characteristics of the tab for an admin task.

protected alias

A *protected alias* is a unique string that is added to the URL for accessing protected tasks in the User Console. For example, if the protected alias for an environment is employees, the URL for accessing the Identity Manager User Console for that environment is:

http://<myserver.mycompany.org>/idm/employees

where <myserver.mycompany.org> is the fully qualified domain name of the server where Identity Manager is installed.

protected task

A *protected task* is an admin task that a user access in the Identity Manager User Console. Users must provide valid credentials to use protected tasks.

provider

A *provider* is an object in the Identity Manager API that gives you direct access to managed objects (such as user, group, and organization objects). If an object's attributes are modified through a provider, no Identity Manager events are generated, and no workflow approvals, auditing, or security checks are performed.

Provisioning Directory

A *Provisioning Directory* is the directory maintained by the Provisioning Server to manage Exchange accounts, Active Directory accounts, Ingres accounts, or other accounts on endpoints.

If a user in the Identity Manager users store needs an account in the Provisioning Directory, that user must be assigned a provisioning role.

provisioning role

A *provisioning role* has policies that define accounts that users can receive. Accounts When you assign a provisioning role to a user, that user receives the accounts defined by policies in the role. The policies also define how user attributes are mapped to accounts. The accounts exist in managed end points defined by the policies.

Provisioning Server

The *Provisioning Server* handles provisioning of users, delegating to Connector Servers where interaction with endpoint systems is required.

public alias

A *public alias* is a unique string that is added to the URL for accessing public tasks in the Identity Manager environment. For example, if the public alias is public, the URL for accessing a public task is:

http://<*myserver.mycompany.org*>/idm/public/index.jsp?task.tag=<*task_tag*>

where <*task_tag*> is the tag for the task to invoke.

You specify the task tag when you configure a task in the Identity Manager User Console.

public tasks

Public tasks are self-service tasks, such as self-registration or forgotten password tasks. Users do not need to log in to access public tasks.

public user

Public user is the name of an existing user who serves as the public user, if an Identity Manager environment includes public tasks. Identity Manager uses the public user's credentials in place of user-supplied credentials when accessing public tasks.

R

relationship

A *relationship* is an object that is associated with the subject of a task. For example, during a Create User task, a user might be assigned to relationship objects such as groups and roles. A relationship object is also called a *secondary object*.

remove action

A *remove action* is a user profile change that occurs when a user is removed as a member or administrator of a role. The remove action is defined when a role is created or modified.

role

A *role* is a method of associating users and rights to Identity Manager or other applications. Roles are made up of tasks. A user who has a role can perform its tasks. Users may have multiple roles. For example, a user may have the roles *accountant* and *employee*.

role administrator

A *role administrator* is an Identity Manager administrator who can add and remove role members or other role administrators. A user becomes a role administrator by meeting conditions in an admin rule for the role or when a role administrator assigns the user as a role administrator.

role-based access control

Role-based access control is a method for granting users access to protected resources based on roles.

role member

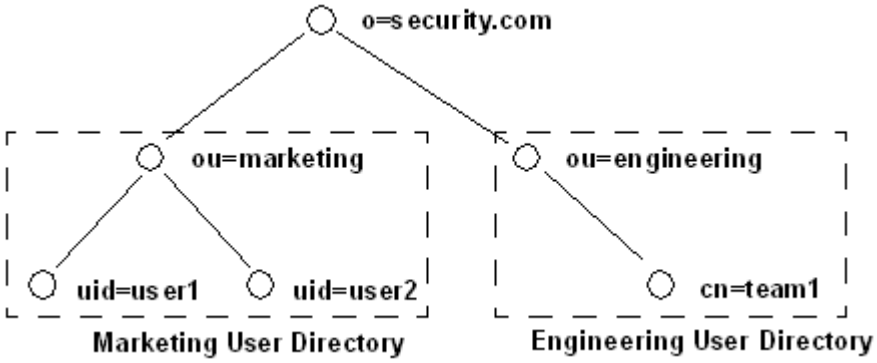
A *role member* is an Identity Manager user who can use a role. A user becomes a role member by meeting conditions in a member rule for the role or when an administrator assigns the role to the user.

role owner

A *role owner* is an Identity Manager administrator who can modify a role.

root

The *root* is the location in an LDAP directory that serves as the starting point for the directory—typically, an organization (o) or organizational unit (ou). In the figure, the root of the Engineering User Directory is ou=engineering.



S

scope

For a role, *scope* determines the objects on which a role member can use the role. For an admin task, *scope* adds additional limits beyond those defined for the role.

search screen

The *search screen* limits the scope of a view or modify admin task. As a result, the task operates only on the objects found by the search screen. For example, if the object is users, you might limit the scope to locate users with the Employee Type of Contractor. The search screen also defines the fields that the user can search on and the results that are displayed.

secondary object

A *secondary object* is associated with the primary object of a task. For example, during a Create User task, a user might be assigned to secondary objects such as groups and roles. A secondary object is also called a relationship object.

self-service

Self-service enables users to register without involvement by the System Manager or other administrators. Self-service users can enter profile information, specify a password, select a challenge question for forgotten password, and subscribe to groups.

SiteMinder user directory

The *SiteMinder user directory* provides a secure connection to an existing user directory.

skin

A *skin* is a set of components that affect the look and feel of the Identity Manager User Console.

SOAP

SOAP is a protocol for exchanging XML-based messages over a computer network using HTTP. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework that more abstract layers can build on. When the standard was created, SOAP was an acronym for Simple Object Access Protocol. However, the full term has since been dropped because it is considered to be misleading.

subject

The *subject* is the target object of a task—for example, a user object in a Create User task. In the Identity Manager User Console, a subject is called a primary object.

SuperAgent

See *C++ Connector Server.*

system manager

The *system manager* is a user with the System Manager role. The system manager has the admin tasks necessary to create the initial roles, tasks, and users for an Identity Manager environment.

T

tag

A *tag* is a unique identifier for a task or tab. It is used in URLs, web services, or properties files. It may consist of letters, numbers, or underscores, beginning with a letter or underscore.

task

A *task* is an administrative function that a user can perform in Identity Manager.

Task Execution Web Service (TEWS)

Task Execution Web Service (TEWS) allows third-party applications to send remote task requests to Identity Manager for execution. Requests and responses are SOAP documents.

U

user

A *user* represents a user in an enterprise. A user has profile information, such as name and user ID, which is managed in Identity Manager. A user may also belong to groups, and have access roles.

user certification

User certification requires business managers to periodically review and approve the roles of the users they manage. Administrators use certification tasks to do the following:

- Identify a set of users that require certification
- Specify a certification period, such as a fiscal quarter, in which all users must be certified
- Notify a user, such as a manager, that there are pending certifications
- Allow a privileged user, such as a manager, to certify or remove privileges
- Disable privileges for users who have not been certified after a certain period of time

user directory

A *user directory* stores information about users, organizations, and groups. Identity Manager manages user directories.

user synchronization

User synchronization evaluates and applies identity policies to users. You can synchronize users automatically by configuring a task to initiate the synchronization process, or manually by using the Synchronize User task

V

validation rule

A *validation rule* verifies input supplied through the user interface or programmatically. For example, a validation rule can verify that a value supplied to an Order Number field falls within a valid range. Validation rules can be implemented as regular expressions, JavaScript, or Java classes.

validation rule set

A *validation rule set* contains one or more validation rules. The rules are executed in the order in which they are listed in the rule set. Output from one rule can be used as input to the subsequent rule.

validator

A *validator* is a Java class that checks the validity of individual values, attributes, or an entire object class. The Java CS uses validators to ensure that data values meet specific requirements before being passed to or from the endpoint system for processing.

W

Web Service Description Language (WSDL)

The *Web Service Description Language (WSDL)* is an XML-based file describing how to communicate using the web service, including all necessary protocol bindings and message formats.

work item delegation

Work item delegation allows an administrator to delegate work items from one user to another using an Identity Manager task. Administrators may want to delegate another user's work items if that user is out of the office unexpectedly or to assign a large workload to multiple users. First you must identify the delegator, or the user with the work items to be delegated. Then you add one or more delegates, other user(s) who will have access to the delegator's work items. Once the delegation is in place, all work items appear in the delegator and the delegate.

work item

A *work item* is an approval task that appears in the work list of the participant authorized to complete the task. Work items correspond to manual activities in a workflow process.

work list

A *work list* is a workflow-generated list of tasks that appear in the Identity Manager User Console. For example, a task may appear to request approval of a create user task.

workflow

A *workflow* is one or more steps that must be performed before Identity Manager can complete a task that is under workflow control.

workflow activity

A *workflow activity* is an operation that must be performed before a task (such as the creation of a new user) can be completed. With Identity Manager, an activity involves the approval or rejection of the task under workflow control.

workflow approval task

A *workflow approval task* is an Identity Manager task that is associated with a workflow activity. When an Identity Manager user performs a workflow approval task (for example, approves the creation of a new user), the result is reported to the associated workflow activity, and the workflow process can then continue to the next workflow element. The workflow approval task and its associated workflow activity must have the same name.

workflow job

A *workflow job* is a runtime instance of a workflow process.

workflow process

A *workflow process* is one or more steps that must be performed before Identity Manager can complete the task under workflow control. The workflow process defines the required steps. A runtime instance of a workflow process definition is called a workflow job.

workflow-controlled task

A *workflow-controlled task* generates one or more events that are mapped to a workflow process.

WorkPoint Designer

WorkPoint Designer is software from Insession Technologies that is integrated with Identity Manager. WorkPoint Designer lets you manage workflow processes and workflow jobs.