

CA Identity Manager

Administration Guide

r12



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2007 CA. All rights reserved.

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

Chapter 1: Overview of Identity Manager 15

User Management and Application Access	15
Role-Based Entitlements	16
Admin Roles for User Account Management	17
Profile Management at the Attribute Level	18
Workflow Approval of Admin Tasks	19
User-defined Custom Attributes for Roles	20
Provisioning Roles for Additional Accounts	21
Delegated Administration Through Roles	21
Identity Policies for Rule-based Identity Management	22
Self Service Options for Users	22
Password Management	23
Compliance Support	23
Identity Manager and Business Application Integration	24
Identity Manager Customization and Extensibility	24

Chapter 2: Role Planning 27

Role Decisions	27
Types of Roles	27
Purpose of Roles	28
Delegated Administration	28
Delegation Steps	29
Delegation Example	30
Role Characteristics	30
Role Profile	31
Tasks for the Role	31
Account Templates	31
Member, Admin, and Owner Rules	32
Scope Rules	33
Common Guidelines about Rules	36
Add and Remove Actions	37
Member Policies	38
Admin Policies	39
Role Planning Checklist	39

Chapter 3: Admin Roles for User Management 41

Admin Roles and Admin Tasks	41
Admin Roles and Identity Manager Environments	41
Admin Roles and the Identity Manager User Console	42
Create an Admin Role	42
Begin Admin Role Creation	43
Define the Admin Role Profile	43
Select Admin Tasks for the Role	43
Define Member Policies for an Admin Role	45
Define Admin Policies for an Admin Role	46
Define Owner Rules for an Admin Role	46
Verify an Admin Role	47
User-defined Custom Attributes for Roles	47
Configure Custom Attributes in Profile Tab for Roles	48
Add Custom Attributes to Search Screen of Roles	49
Allow Users to Self-Assign Roles	50

Chapter 4: Admin Tasks 53

Admin Task Planning	53
A Sample Admin Task	54
Admin Task Usage Options	57
Admin Task Processing	58
How to Create an Admin Task	58
Define the Profile of the Task	60
Admin Task Profile Tab	60
Task Categories	64
Choose Tabs for the Task	65
Tab Controllers	65
List of Default Tabs	67
Profile Tabs and Profile Screens	71
List Screens	99
Account Tabs	102
Schedule Tab	104
Object-Task Navigation	106
Define the Task Scope	108
Search Screen Configuration	109
View Fields in the Task	116
Assign Workflow Processes for Events	116
Active Directory Prerequisites	116
The sAMAccountName Attribute	116
Group Type and Scope	117

External Tasks for Application Functions	118
The External Tab	119
The External URL Tab	119
Advanced Task Components	120
Configure Task-Level Validation	121
Create Business Logic Task Handlers	122

Chapter 5: Access Roles 125

Access Roles in Identity Manager	125
How Access Roles Manage Entitlements	125
Example: Indirect Profile Attribute Modification	126
Create an Access Role	126
Begin Access Role Creation	126
Define the Profile of an Access Role	127
Define Member Policies for an Access Role	127
Define Admin Policies for an Access Role	128
Define Owner Rules for an Access Role	128

Chapter 6: Identity Policies 129

Identity Policies	129
Identity Policy Set Planning Worksheet	130
Create an Identity Policy Set	131
Define the Profile for the Identity Policy Set	131
Create an Identity Policy	131
Specify Owners for the Identity Policy Set	140
Manage an Identity Policy Set	140
How Users and Identity Policies Are Synchronized	141
Configure Automatic User Synchronization	142
Synchronize Users Manually	143
Verify User Synchronization	144
Identity Policy Sets in an Identity Manager Environment	145
Example: Automatically Populating User Attributes	145
Example: Allocating Resources and Entitlements	146
Example: Enforcing Compliance	148
Example: Enforcing Segregation of Duties	149

Chapter 7: Self-Service Tasks 151

Identity Manager Self-Service Tasks	151
How to Configure Self-Service Tasks	152
Configure the Self-Registration Task	153

Set Up a Default Organization for Self-Registered Users	154
Add Verification Questions and Answers	154
Configure the Forgotten Password Reset and Forgotten User ID Tasks	156
The Forgotten Password Reset Task	156
The Forgotten User ID Task	156
Custom Forgotten Password Reset and Forgotten User ID Tasks	157
Collect Question and Answer Pairs for User Verification	157
Set Up the Forgotten Password Reset or User ID Task	158
Design Identification Screens	159
Design Verification Screens	160
Lock the Forgotten Password Reset or Forgotten User ID Task	163
Determine How Users Reset Passwords	165
Determine How Users Retrieve a Forgotten User ID	166
Customize Self-Service Tasks	166
Restrict Access to the Self Manager Role	167
Access Self Service Tasks	167
Configure Multiple Self-Service Tasks	168

Chapter 8: Password Management **171**

Password Management in Identity Manager	171
Password Policies	172
Create a Password Policy	173
Manage Password Policies	173
Configure Password Composition	174
Specify Regular Expressions	175
Configure Advanced Password Options	177
Password Policies with SiteMinder	178
Reset Password or Unlock Account	188
Install the GINA or Credential Provider	188
Configure the GINA	189
Configure the Credential Provider	190
Settings in the Registry	191
Reset a Password for a Windows Login	194

Chapter 9: Users **195**

Create a User	195
Manage a User	195
Modify a User	196
Assign Roles to a User	197
Assign Roles with the Modify Role Members/Administrators Task	197
Assign Roles with the Modify User Task	198

Chapter 10: Groups	201
Create a Static Group	201
Create a Dynamic Group	202
Dynamic Group Query Parameters	203
Create a Nested Group	204
Static, Dynamic, and Nested Groups Example	206
Group Administrators	207
 Chapter 11: Compliance Support	 209
Compliance Support in Identity Manager	209
User Entitlement Certification	209
How the Certification Process Works	210
How User Certification is Configured	210
Start the User Certification Process	215
Send Reminder Notifications	215
Use the Certify User Task	216
End the Certification Process	216
 Chapter 12: Workflow	 217
Workflow Overview	217
WorkPoint Process Diagram	218
Workflow and Email Notification	218
WorkPoint Documentation	219
How to Enable Workflow	219
Starting WorkPoint Designer	220
Workflow Control Methods	220
Template Method	221
How to Use the Template Method	222
Process Templates	222
Tasks and Events	226
Participant Resolvers: Template Method	231
Workflow Example: Create User	237
WorkPoint Method	239
How to Use the WorkPoint Method	239
WorkPoint Processes	240
Workflow Activities	245
Participant Resolvers: WorkPoint Method	247
Processes in WorkPoint Designer	256
Jobs and Process Instances	259
Performing Workflow Activities	261

Online Requests	263
Online Request Tasks	264
Online Request Process	265
Online Request History	266
Using Online Requests	267
Workflow Action Buttons	267
Workflow Buttons in Approval Tasks.....	268
Button Configuration In Identity Manager.....	269
Adding Workflow Action Buttons	270
Work Lists and Work Items	272
Displaying a Work List.....	273
Reserving Work Items.....	274
Delegating Work Items	275
Reassigning Work Items.....	279

Chapter 13: Email Notifications **283**

Email Content	283
Enable Email Notification	284
Configure an Event or Task To Send Email	285
Email Templates	286
Template Directories	288
Create Email Templates	289
Custom Email Templates	289
Template Elements	290
Identity Manager Tag Extensions	290
Email Template API	292
Additional Methods.....	305
Javadoc Reference	307
Email Template Deployment.....	307
Template Sets	307
Template Names.....	308

Chapter 14: Reporting **311**

How to Generate Reports	311
Configure Reporting.....	312
Create a Snapshot Definition	313
Capture Snapshot Data.....	321
Associate Snapshots with Report Tasks	321
Run Reports	322
View Reports	323
How to Create Custom Reports	323

Create a report in Crystal Reports	324
Create the Report Parameter XML File	324
Upload Report and Report Parameter XML File	325
Create the Report Tasks	326
Sample Reports	330

Chapter 15: System Tasks 333

Default System Tasks	333
Task Status in Identity Manager	334
How Identity Manager Determines Task Status	335
The View Submitted Tasks Tab	335
Search for Submitted Tasks	336
View Task Details	339
View Event Details	340
Customize the View Submitted Tasks Tab	341
User History Tab	344
Search Attributes for Viewing User History	344
Customize the User History Tab	345
The View User Activity Task	349
Bulk Loader	349
Add Bulk Loader Task to Admin Roles	349
How to Use the Bulk Loader	350
Enable Email Notification for Feeder Tasks	352
Modify Parser File for Bulk Loader	352
Web Service Support for Bulk Loader	353
Bulk Loader Memory Considerations	353
Custom Data for Select Boxes	354
How to Populate Fields Using Select Box Data	354
Create a Select Box Data XML File	355
Import the Select Box Data XML File	358
Configure Fields to Use Select Box Data XML Files	359
Logical Attribute Handlers	361
Create a Logical Attribute Handler	362
Copy a Logical Attribute Handler	362
Create a ForgottenPasswordHandler Logical Attribute Handler	363
Delete a Logical Attribute Handler	363
Modify a Logical Attribute Handler	364
View a Logical Attribute Handler	364
Connection Management	364
Create Connection	365
Connection for Reports	365

Appendix A: Events and Tasks **367**

Identity Manager Events	367
Event List	368
How Identity Manager Determines Task Status	371
Admin Tasks and Events	372
Tasks and Associated Events	372
Events Generated for Unmodified Profiles	379

Appendix B: Default Tasks and Roles **381**

Default Self-Service Tasks	381
Self Registration	381
Forgotten Password	381
Forgotten Password Reset	382
Forgotten User ID	382
Password Services	382
Default Admin Tasks	382
Home	383
Access Roles	385
Admin Roles	387
Certification	389
Groups	389
Organizations	391
Policies	392
Provisioning Roles	394
Reports	395
System	395
Users	397
Default Admin Roles	398
Access Role Manager	399
Admin Role Manager	399
Certification Process Manager	400
Certify Manager	400
Delegation Manager	400
Group Manager	401
Organization Manager	401
Password Manager	402
Provisioning Role Manager	402
Provisioning Synchronization Manager	403
Security Manager	403
Self Delegator	403
Self Manager	404

System Manager	404
User Manager	405
Default Workflow Approval Roles	405

Appendix C: FIPS 140-2 Compliance **407**

FIPS Overview	407
Communications	407
Installation	408
Connecting to SiteMinder	408
Key File Storage	409
The Password Tool	409
FIPS Mode Detection	410
Encrypted Text Formats	410
Encrypted Information	411
FIPS Mode Logging	411

Index **413**

Chapter 1: Overview of Identity Manager

This section contains the following topics:

[User Management and Application Access](#) (see page 15)
[Role-Based Entitlements](#) (see page 16)
[Admin Roles for User Account Management](#) (see page 17)
[Provisioning Roles for Additional Accounts](#) (see page 21)
[Delegated Administration Through Roles](#) (see page 21)
[Identity Policies for Rule-based Identity Management](#) (see page 22)
[Self Service Options for Users](#) (see page 22)
[Password Management](#) (see page 23)
[Compliance Support](#) (see page 23)
[Identity Manager and Business Application Integration](#) (see page 24)
[Identity Manager Customization and Extensibility](#) (see page 24)

User Management and Application Access

The typical Information Technology (IT) department faces a constant demand to maintain user accounts. IT administrators must address urgent needs of users, such as resetting forgotten passwords, creating new accounts, and providing supplies and office equipment.

Simultaneously, IT administrators must provide users with various levels of access to applications. For example, a department manager generates purchase orders and needs an account in a financial application.

To address the escalating demands on IT, Identity Manager provides an integrated method of managing users and their access to applications, including:

- Assignment of privileges through roles. Specifically:
 - Roles that enable administrators to create and maintain user accounts
 - Roles that provision additional accounts to existing users (requires provisioning support)
- Delegation of the management of users and application access
- Self-service options so users can manage their own accounts
- Integration of business applications with Identity Manager
- Options to customize and extend Identity Manager

Role-Based Entitlements

With Identity Manager, you assign privileges to users by assigning roles. A *role* contains tasks that correspond to application functions in Identity Manager or account templates that correspond to additional accounts. When you assign a role to a user, that user can perform the tasks contained in the role or use the accounts associated with the role.

Identity Manager provides these types of roles:

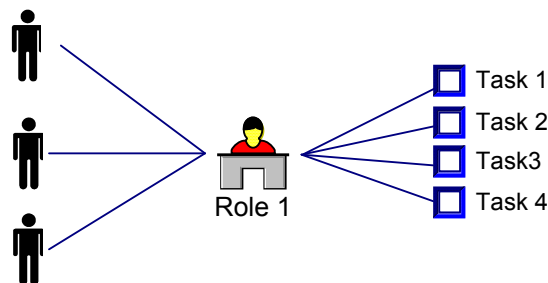
- User management roles are called *admin roles*.
- Account assignment roles are called *provisioning roles*.

Roles simplify privilege management. Instead of associating a user with each task that he performs or each account that he needs, you can assign a role to the user. The user can perform the tasks in the role or use the accounts associated with the role.

You can then edit the role by adding tasks or account templates, which define the accounts. Every user who has the role can now perform the new task or use the new account. If you remove a task or account template from a role, the user can no longer perform that task or use the account.

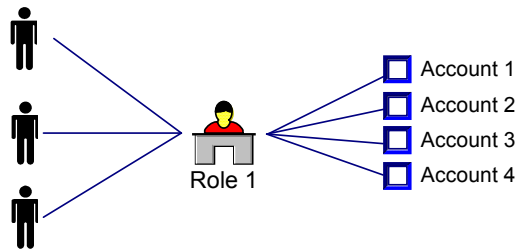
Tasks enable users to perform Identity Manager functions, such as modifying a profile.

The following illustration shows several tasks which are combined into a single admin role and assigned to multiple users:



For a provisioning role, you combine several accounts, such as an email account, a database account, and an Active Directory account. You can assign the role to several users, who each need these accounts.

The following illustration shows several accounts which are combined into a single provisioning role and assigned to multiple users.



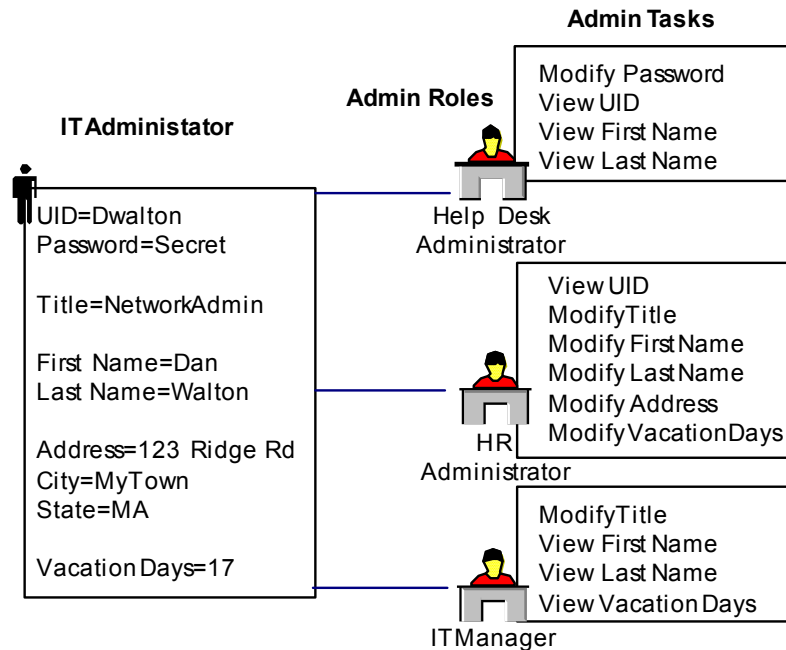
Note: In this figure, each user receives four accounts, when you assign the provisioning role to that user.

Admin Roles for User Account Management

In Identity Manager, you manage user store objects (users, groups, and organizations) through admin roles. You also use admin roles to manage the roles and tasks through which you manage user store objects. For example, you use admin roles to modify profile attributes of users, give users options for managing their own accounts, and to approve tasks that use workflow.

Profile Management at the Attribute Level

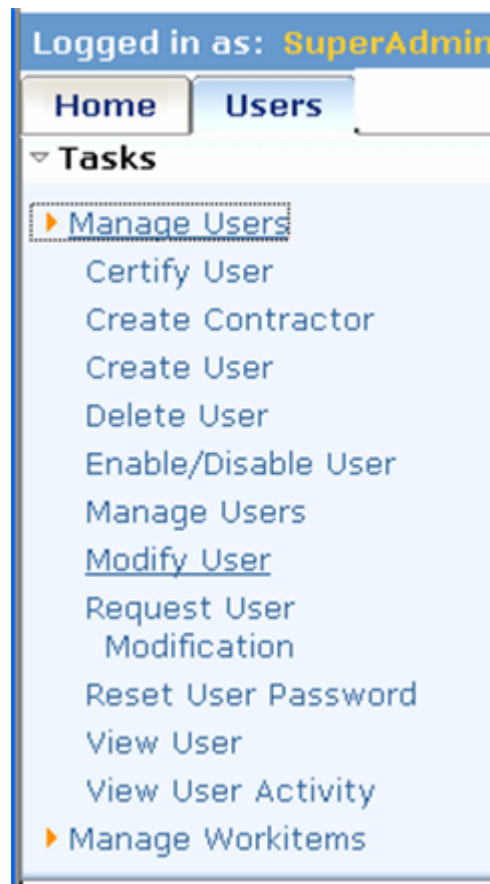
You can create admin roles for different administrators who need to read or write different profile attributes. For example, a company may have several employees who perform operations on user profiles, each accessing different attributes. The following figure shows three roles and their associated tasks. Each role has different access to profile attributes.



In this example, three roles can manage different attributes for the same user, Dan Walton:

- A Help Desk administrator views user names and addresses and resets user passwords.
- A Human Resources administrator modifies user IDs, user names, addresses, titles, and number of vacation days.
- An IT manager modifies the title of users and views their name and number of vacation days.

Whatever roles you have when you log in to Identity Manager, a series of tabs, called categories, appear based on the admin role assigned to your Identity Manager account. You click a tab to see the tasks that you can perform in that category as shown in the following figure:



The categories and the tasks in those categories that a user sees are determined by the user's admin roles.

Workflow Approval of Admin Tasks

To help automate business processes, you can design an admin task to generate a workflow process. A *workflow process* automates a well-defined procedure that a company repeats frequently. Identity Manager includes the WorkPoint workflow engine.

Workflow processes are triggered by Identity Manager events which are part of an admin task. For example, the Create User task includes events called `CreateUserEvent` and `AddToGroupEvent`. When an event occurs, the workflow engine can:

- **Require approvals**--An approver must approve an event, such as modifying a user profile, before Identity Manager updates a user store. Approvers are administrators who have the Approver role for a particular task.
- **Send notifications**--The workflow engine can notify users of an event's status at different stages of a process, such as when a user initiates an event or when an event is approved.
- **Generate work lists**--Work lists specify the tasks that a particular user must perform. The workflow engine updates administrators' work lists automatically.

For common events, you can use the workflow processes supplied with Identity Manager. Alternatively, you can create custom workflow processes.

User-defined Custom Attributes for Roles

Identity Manager supports user-defined custom attributes that allow you to filter roles in your organization effectively. For example, in your corporate environment you may have the need to create more than a thousand roles. You might want to categorize these roles by business units or by geographical locations. If you want to search for roles that are specific to a particular geographical location, you can use the custom attributes to filter the roles in your organization.

You can use custom attributes in the Create, Modify, and View tasks for the following roles:

- Access Roles
- Admin Roles

You must perform the following steps to add custom attributes to admin tasks and search screens.

1. Add custom attributes to any of the admin tasks that are defined for roles.
2. Configure the search screens for roles with custom attributes.

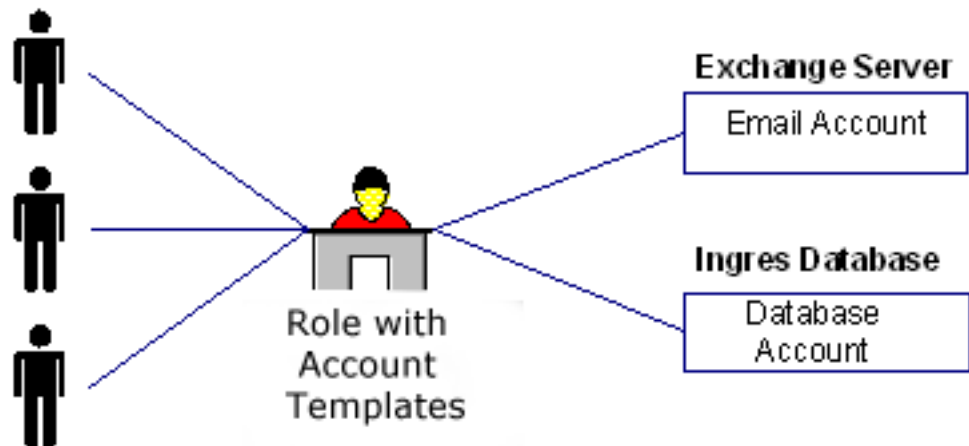
More Information:

[Configure Custom Attributes in Profile Tab for Roles](#) (see page 48)

[Add Custom Attributes to Search Screen of Roles](#) (see page 49)

Provisioning Roles for Additional Accounts

In Identity Manager, you provide additional accounts to users by using provisioning roles. Provisioning roles contain account templates, which define accounts that exist in managed endpoints, such as an email server. Once you have users in Identity Manager, you can assign provisioning roles to some of those users. The user receives the accounts defined by the templates in the role.



The account templates define the characteristics of the account. For example, an account template for an Exchange account might define the size of the mailbox. The account templates also define how user attributes are mapped to accounts.

To be able to use provisioning roles, you must install the Provisioning Server with the Identity Manager server. Then, you create account templates in the Provisioning Manager, a user interface for managing the Provisioning Server.

Delegated Administration Through Roles

As an Identity Manager user, you can personally manage users and their access to applications or you can delegate this work. *Delegated administration* is the use of roles to share the work of managing users and granting application access.

For delegated administration to work, each role contains rules that describe which users can modify, assign, or use the role. By dividing these functions between users, you delegate the work necessary to use and maintain roles.

Identity Policies for Rule-based Identity Management

Using identity policies, you can define a set of business changes that occurs when a user meets a certain condition or rule. You can use identity policies to:

- Automate certain identity management tasks, such as assigning roles and group membership, allocating resources, or modifying user profile attributes.
- Enforce segregation of duties. For example, you can create an identity policy that prohibits members of the Check Signer role from having the Check Approver role, and restricts anyone in the company from writing a check over \$10,000.
- Enforce compliance. For example, you can audit users who have a certain title and make more than \$100,000.

Identity policies that enforce compliance are called *compliance policies*.

The business changes associated with an identity policy include:

- Assigning or revoking roles, including provisioning roles (if you are using a provisioning directory)
- Assigning or revoking group membership
- Updating attributes in a user profile
- Identifying a particular scenario, such as having two mutually exclusive roles, for auditing purposes

Self Service Options for Users

To further reduce the IT workload, Identity Manager includes features for registering new users and supplying a forgotten password. These features require no administrator involvement. The user gains access to Identity Manager through a *public console*, which requires no login account. Through this console, a user can self-register at a site or request a reminder about a forgotten password.

To save the time of IT administrators, Identity Manager users can manage their own accounts. Because users have a self-management role, they can:

- Maintain personal information
- Change their own password
- Join self-subscribing groups

Password Management

Identity Manager includes several features for managing user passwords:

- Password Policies—These policies manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage.
Note: For advanced password policies, configure integration with SiteMinder. For more information, see the *Installation Guide*.
- Password Managers—Administrators who have the Password Manager role can reset a password when a user calls the Help desk.
- Self-Service Password Management—Identity Manager includes several self-service tasks that allow users to manage their own passwords. These tasks include:
 - Self Registration—Users specify a password when they register at a corporate web site.
 - Change My Password—Users can modify their passwords without help from IT or Help Desk personnel
 - Forgotten Password—Users can reset or retrieve a forgotten password after Identity Manager verifies their identity.
 - Forgotten User ID—Users can retrieve a forgotten user ID after Identity Manager verifies their identity.
- Password Synchronization (for use with provisioning only)—Password changes are synchronized in Identity Manager and in accounts on target systems called endpoints. New passwords are verified against Identity Manager password policies.

Compliance Support

Compliance is a corporate governance that includes a wide range of procedures that ensure a company and its employees comply with business policies. These compliance procedures often involve documenting, automating, and auditing the allocation of entitlements to applications and systems.

Identity Manager includes the following features, which support compliance management:

- Identity policies--You can create a compliance policy, a type of identity policy, which prohibits users from having certain privileges if they have other privileges. For example, you can prohibit users who can approve checks from issuing checks.

Compliance policies enforce a segregation of duties in your environment.

- User entitlement certification--Forces users, such as managers, to review and certify the roles of the users they manage.
- Compliance reports--Identity Manager includes sample reports that display the compliance status for users in your environment. Using this report, you can see which users are not compliant with your business policies.

Identity Manager and Business Application Integration

From Identity Manager, you can perform a task that executes a function in a business application. This task is called an *external task*. For example, an Identity Manager administrator may view a report generated by an application, such as a financial application.

Unlike an access task, an external task is used from the Identity Manager user interface. The administrator clicks an external task link, which opens a URL for the application.

To make the external task available, you include it in an admin role, which ensures that only privileged administrators can use the task.

Identity Manager Customization and Extensibility

You customize these Identity Manager features:

- The Identity Manager directory, which describes a user store structure to Identity Manager.
- The appearance and functionality of the user interface.
- User entry screens, which determine the fields and layout of each task screen.
- Validation of user data entry, through regular expression, JavaScript, or Java implementations.
- Workflow, which defines automated workflow processes. Create or modify processes by linking approvers and actions in the WorkPoint Process Designer.
- Email messages, which inform users of a task's status.
- Task submission, which can be sent by a third-party application to the Identity Manager Task Execution Web Service (TEWS). TEWS processes the remote task request. Remote task requests comply with WSDL standards.

You can extend Identity Manager's functionality using the following APIs:

- Logical Attribute API—Enables you to display an attribute differently than how it is stored physically in a user directory.
- Business Logic Task Handler API—Allows you to perform custom business logic during data validation or transformation operations.
- Workflow API—Provides information to a custom script in a workflow process. The script evaluates the information and determines the path of the workflow process accordingly.
- Participant Resolver API—Enables you to specify the list of participants who are authorized to approve a workflow activity.
- Event Listener API—Enables you to create a custom event listener that listens for a specific Identity Manager event or group of events. When the event occurs, the event listener can perform custom business logic.
- Notification Rule API—Lets you determine the users who should receive an email notification.
- Email Template API—Includes event-specific information in an email notification.

Note: For more information on the Identity Manager APIs, see the *Programming Guide for Java*.

When Identity Manager includes provisioning, you can also extend provisioning functionality as follows:

- Custom connectors—Enable communication between a Provisioning Server and an endpoint system. The code that makes up a connector can include a GUI plug-in, server plug-in, and agent plug-in.

A dynamic connector can be generated by Connector Xpress, and a custom static connector can be developed in Java or C++.
- Program exits—Let you reference custom code from the Provisioning Server process flow.

Note: For more information about extending provisioning functionality, see the *Programming Guide for Provisioning*.

Chapter 2: Role Planning

To plan your roles, you decide what kind of roles your business or organization needs and how you will delegate the management of users and their application access. Based on these decisions, you determine each role's characteristics.

This section contains the following topics:

[Role Decisions](#) (see page 27)

[Delegated Administration](#) (see page 28)

[Role Characteristics](#) (see page 30)

[Role Planning Checklist](#) (see page 39)

Role Decisions

The following section includes information to help you make informed role decisions.

Types of Roles

To decide what types of roles that you need, see the following table:

Type of Role	Purpose
Admin role	Contains the tasks that you perform in the Identity Manager User Console: ■ <i>Admin tasks</i>, which you use to manage users, organizations, groups, roles, and tasks. ■ <i>External tasks</i>, which perform functions in business applications, such as passing user attributes to a reporting application
Provisioning role	Contains account templates that define accounts that exist in managed endpoints, such as an email system. The account templates also define how user attributes are mapped to accounts.
Access role	Provides an additional way to provide entitlements in Identity Manager or another application.

You manage roles in an *Identity Manager environment*, which is a view of a management namespace where you manage users, groups, and organizations and the associated tasks and roles. To create an Identity Manager environment, see *CA Identity Manager Configuration Guide*.

For every Identity Manager environment, you need admin roles. You need provisioning roles only if you need to assign additional accounts to existing users. provide an additional way to provide entitlements in Identity Manager or another application.

Purpose of Roles

To use roles effectively, consider these types of questions about user needs and administrator responsibilities:

- Which departments and organizations have users to be managed?
- What additional accounts in managed endpoints will users need?
- Which users should be administrators of other users?
- Who should manage the administrators?
- What admin and access tasks are needed in each role?
- Who should create roles and tasks?
- How can I use roles to delegate work?

The last question concerns sharing the work of managing users and granting application access. More information about the delegation model exists in [Delegated Administration](#) (see page 28).

Based on your answers to these questions, you can decide how many and what kind of roles are needed.

Delegated Administration

As an Identity Manager user, you can personally manage users and their access to applications or you can delegate this work. *Delegated administration* is the use of roles to share the work of managing users and granting application access.

For delegated administration, each role contains rules that describe which users perform the functions in the following figure:

Function	Definition
Role Owner	Modifies the role
Role Administrator	Assigns the role to users and other role administrators
Role Member	Uses the role to perform admin or access tasks

By dividing these functions between users, you can have lower-level administrators manage users and higher-level administrators assign or modify the role.

Note: An *administrator* is an Identity Manager user who can assign roles or use admin roles. A *user* is any Identity Manager user; that user may have admin roles, access roles, or both.

For a provisioning role, you can create administrator and owner rules, so that you can delegate administration. However, you cannot create member rules for provisioning roles in Identity Manager. Instead, you use Modify Provisioning Role Members/Administrators to add or remove role members.

Delegation Steps

After you decide about your use of roles based on Purpose of Roles, delegated administration occurs as follows:

1. An administrator creates the role with rules for who is a role owner, administrator, or member.
2. A role owner modifies the role, when changes are needed.
3. A role administrator:
 - Assigns more role administrators (optional).
 - Assigns more role members (optional).

Some users are already role administrators or members by meeting rules defined in the role.

4. A role member uses the role:
 - An admin role member manages users and other objects in the Identity Manager environment.
 - An access role member performs functions in business applications.
 - A provisioning role member uses the accounts defined by policies in the role.

Delegation Example

You can create a role with rules for who can be a member or administrator. You can then assign the role, so that other users (who do not already meet the rules) can become a role member or administrator.

Consider the following example of administrators who manage the business application rights of end users:

- Jeff is a role owner for the Accountant role; so when the role requires changes, Jeff modifies the role.
- David and Lisa are role administrators for that role. They assign regional users as role members.
- Other users are role members without being assigned as role members. Instead, they meet the rule to be role members.

The role members use the Accountant role to generate purchase orders and perform other tasks in financial applications.

The section Role Characteristics provides details on rules and other characteristics of a role.

Role Characteristics

When you create a role, you define the characteristics shown in the following table:

Characteristics	Definition
Role Profile	General characteristics of the role.
Tasks	Tasks for an admin role.
Account Templates	Templates that define accounts in managed endpoints for a provisioning role.
Member Rules, Member Policies	A member rule defines conditions for a user to be a role member. A member policy combines a member rule with scope rules. Note: Provisioning roles have no member rules and policies. To make a user a member, you use Modify Provisioning Role Members/Administrators.

Characteristics	Definition
Admin Rules, Admin Policies	■ An admin rule defines conditions for a user to be a role administrator. ■ An admin policy combines an admin rule with a scope rule and administrator privileges for assigning the role.
Owner Rules	Conditions for a user to be a role owner.
Scope Rules	Limits on which objects can be managed by the role.
Add Actions, Remove Actions	Changes to a user profile when a user is added or removed as a role member or administrator.

The following sections explain these characteristics.

Role Profile

The role profile is the name and description of the role and whether or not the role is enabled. If enabled, the role is available for use as soon as it is created.

Tasks for the Role

For an admin role, you can choose one or more admin tasks, including external tasks, from one or more categories.

Account Templates

Each provisioning role contains account templates. They define the accounts that exist in managed endpoints. For example, an endpoint for an Exchange account might define the size of the mailbox. The account templates also define how user attributes are mapped to accounts.

You can choose one or more endpoints for each endpoint type. A user who is assigned the role receives an account in the endpoint.

Member, Admin, and Owner Rules

Each role includes rules about who can be a member, administrator, or owner of that role. Therefore, a user could be a member of one role, several roles, or no roles.

Member, admin, and owner rules use the conditions in the following table:

Rule Condition	Example	Rule Syntax
The user must match one attribute value.	Users where title starts with senior	where <user-filter>
The user must match multiple attribute values.	Users where title=manager and locality=east	where <user-filter>
The user must belong to named organizations.	Users in organization sales and lower	in <org-rule>
The user must belong to organizations that meet a condition specified by attributes on the organization.	Users in organizations where Business Type=gold or platinum	in organizations where <org-filter>
The user must belong to specific organizations and match specific user attributes.	Users where title=manager and locality=east and who are in organization sales or marketing	where <user-filter> and who are in <org-rule>
The user must belong to a specific group.	Users who are members of 401K group	who are members of group [set the product group or family]
The user must be a member of a role.	Users who are members of the Help Desk role	who are members of <role-rule>
The user must be an administrator of a role.	Users who are administrators of the Sales Manager role	who are administrators of <role-rule>
The user must be an owner of a role.	Users who are owners of the User Manager role	who are owners of <role-rule>
The user must belong to a group which meets a condition specified by attributes on the group.	Users who are members of groups where owner=CIO	who are members of group <group-filter>

Rule Condition	Example	Rule Syntax
The user must meet a condition based on an LDAP query.	(Use an LDAP directory for situations where a query created in the Identity Manager User Console is insufficient)	user returned by the query ldap_query

Some rules may involve comparing a value to a multi-valued attribute. For the rule to apply, at least one value in a multi-valued attribute must satisfy the rule. For example, if the rule is Attribute A EQUALS 1, and the value of attribute A is 1, 2, 3 for User X, then User X satisfies the criteria.

The user who creates the role may be unable to modify the role. To be able to modify the role, that user must meet the conditions in the owner rules.

Note: In large implementations, it may take significant time to evaluate member, admin, and owner rules. To reduce the evaluation time for rules that include user-attributes, you can enable the in-memory evaluation option. For more information, see the *Configuration Guide*.

Scope Rules

You combine member and admin rules with scope rules. *Scope rules* limit objects on which the role can be used.

- For a role member, scope rules control which objects can be managed with the role.
- For a role administrator, scope rules control which users can become role members and administrators.

The objects include the primary object of the task and any secondary objects. For example, a Create User task that includes a group tab has a primary object of user and a secondary object of group.

For most object types, you can specify the types of scope rules in the following table.

Rule Condition	Example	Rule Syntax
All	Role members can manage all objects	All
The object must match one or more attribute values.	Users where title starts with senior	where <filter>

When you select the filter option, Identity Manager displays two types of filters:

<attribute> <comparator><value>

An attribute in the object's profile must match a specific value.

<attribute> <comparator> admin's <user-attribute>

An attribute in the object's profile must match an attribute on the administrator's profile. For example: Users where manager = admin's UserID.

Additional options, which are described in the following tables, are available for user, group, and organization objects.

Note: The following user scope rules are examples. You can create other rules to handle different relationships between the administrator and the users that the administrator can manage.

Rule Condition	Example	Rule Syntax
The user must match one attribute value.	Users where member of group sales or cell phone does not equal null	where <user-filter>
The user must match multiple attribute values.	Users where title=manager and locality=USA	where <user-filter>
The user must belong to named organizations.	Users in organization Australia or New Zealand Note: Organization scope rule apply to suborganizations of the organization that meets the rule. For example, if the organization rule is "in Organization1", the scope rule applies to Organization1.1 and Organization1.2, but does not apply to Organization1.	in <org-rule>
The user must belong to organizations that meet a condition specified by attributes on the organization.	Users in organizations where Business Type=gold or platinum	in organizations where <org-filter>

Rule Condition	Example	Rule Syntax
The user must belong to specific organizations and match specific user attributes.	Users where title=manager and locality=east and who are in organization sales or organization marketing	where <user-filter> and who are in <org-rule>
The attribute on a user's profile must match an attribute on the administrator's profile.	Users where manager = admin's UserID	where <user-attribute> <comparator> admin's <user-attribute> Note: Do use the Not Equal To comparator with a multi-valued attribute.
The user is in the same organization as the administrator.	Users in the organization where Jeff (the administrator) is a member	admin's organization
The user is in an organization which is listed on the administrator's attribute.	Users in sales or marketing	organization that is a value in admin's <admin-attr>

Note: The following group scope rules are only examples. You can create other rules to handle different relationships between the administrator and the groups that the administrator can manage.

Rule Condition	Example	Rule Syntax
The group must match one attribute value.	Group name where Group name = 401K	where <group-filter>
The groups must belong to named organizations.	Groups in organization accounting and lower	in <org-rule>
The group must match one attribute value and belong to named organizations.	Groups where BusinessType = finance and who are in organization sales and lower	where <group-filter> and who are in <org-rule>

Rule Condition	Example	Rule Syntax
The group must be listed in an attribute of the administrator.	Groups where Description = Engineering	where <group-attribute> <comparator> admin's <user-attribute> Note: Do use the Not Equal To comparator with a multi-valued attribute.

Note: The following organization scope rules are only examples. You can create other rules to handle different relationships between the administrator and the organizations that the administrator can manage.

Rule Condition	Example	Rule Syntax
The organization must match one attribute value.	organizations where org Name=finance	where <org-filter>
The organization must belong to named organization.	organizations in finance and lower	in <org-rule>
The organization must match one attribute value and must belong to named organization	organizations where org Name=finance and are in finance and lower	where <org-filter> and are in <org-filter>

More information:

[Common Guidelines about Rules](#) (see page 36)

Common Guidelines about Rules

Whatever type of rule that you create, you should understand how Identity Manager processes them.

Evaluation of Operators

In creating rules for a role, you may include $\geq$, $\leq$, $<$, and $>$ operators. However, these operators are evaluated as strings by the LDAP directory or relational database. Most user stores compare strings based on the alphabet. Therefore, in comparing 500 to 1100, the user store may determine that 500 is greater because 5 is greater than 1.

You may be able to change the way strings are compared in the user store. Consult the documentation for the LDAP directory service or relational database software.

Case-Insensitivity of Rules

When you create admin or access roles, the rules that you create may be evaluated in a case-insensitive or case-sensitive manner depending on the user store.

However, at the end of a create or modify operation, the rules are evaluated internally in a case-insensitive manner before committing the changes to the user store. For example, if a rule has a condition where `title=manager`, the rule matches the user store object, whether it has a title value of `manager` or `Manager`.

Add and Remove Actions

You must specify an Add and Remove Action for Identity Manager to correctly manage a role's membership when an administrator grants or revokes the role.

- The Add Action must make the user meet the criteria in one of the role's member rules. For example, if the member rule for the User Manager role states that role members have "User Manager" as a value of their Admin Roles attribute, the Add Action must add "User Manager" to the Admin Roles attribute.
- The Remove Action should alter the profile of a user so that the user no longer matches the member rule when the rule is revoked.

Each role can have two *add actions* and two *remove actions*.

If administrators can add and remove members of the role, you define add and remove actions. Otherwise, the user has the role by meeting the member rule, such as by belonging to the RoleAdmins group. For example:

- Role A can be assigned by an administrator, so add or remove actions will be defined.
- Role B has a rule that all members of Group "finance" have the role. This role cannot be assigned, so it has no add or remove action.

When you define add and remove actions, consider using the Admin Role attribute, which Identity Manager can use to store a list of user's roles. For example, you can configure an add action that adds Employee to a user's Admin Role attribute when that user is added as a member of the Employee role. When an administrator assigns the Employee role to a manager who already has the Self Administrator and User Manager roles, the manager's Admin Role attribute would contain the following values: Self Administrator, User Manager, Employee.

To use the Admin Role attribute, the %ADMIN_ROLE_CONSTRAINT% well-known attribute must be mapped to a multi-valued attribute in user profiles. For more information, see the *CA Identity Manager Configuration Guide*.

Important! When defining an add action, avoid setting up a rule that refers to the role you are defining. For example, do not define the add action that makes a member of Role A by being a member of Role A. This will create a recursive error that will cause the policy server to restart.

Member Policies

A *member policy* indicates that if a user meets the member rule, that user has the scope defined in that policy. The following figure shows a role that has two member policies.

- The first policy indicates that if a role member has the Manager Jones, that member can use the role on users in the Sales Office and manage them as members of the 401k group.
- The second policy indicates that if a role member is in the city Bend, that role member can use the role on users in the state of Oregon and manage them as members of the groups that have the Group Admin of Smith.

Member Policies

	Member Rule	User Scope Rule	Group Scope Rule
▶	where (Manager = "Jones")	where (Office = "Sales")	where (Group Name = "401K")
▶	where (City = "Bend")	where (State = "OR")	where (Group Admin = "Smith")

Admin Policies

An *admin policy* indicates that if a user meets the admin rule, that user has the user scope and administrator privileges defined in that policy. The user scope defines where the role is used. The administrator privileges determine if the role administrator can manage members or manage administrators of the role.

The following figure shows a role that has two admin policies, which are defined as follows:

- For the first policy, an IT Admin can add and remove role members and administrators from the users in the Boston.
- For the second policy, an administrator in Sales can add and remove members in the state of Ohio.

Admin Policies

	Admin Rule	User Scope Rule	Manage Members	Manage Administrators	
▶	where (Employee Type = "IT Admin")	where (City = "Boston")	☒	☒	⊖
▶	where (Office = "Sales")	where (State = "Ohio")	☒	☒	⊖

Role Planning Checklist

Before creating a role, use this checklist of role characteristics.

Role Characteristic	Details
Role Profile	Define a name and description for the role and set Enabled status.
Tasks	Include admin or access tasks.
Account Templates	Include account templates that define accounts that exist in endpoints (provisioning roles only).

Role Characteristic	Details
Member Policies	For each member policy, define: ■ Member Rules -- Who can use the role ■ Scope Rules -- Which objects can a role member manage ■ Add Action -- What happens to the profile of a user who becomes a member ■ Remove Action -- What happens to the profile of a user who is removed as a member
Admin Policies	For each admin policy: ■ Admin Rules -- Who can manage the users as members or administrators ■ Scope Rules -- Which users can the administrator manage as members or administrators ■ Add Action -- What happens to the profile of a user who becomes an administrator ■ Remove Action -- What happens to the profile of a user who is removed as an administrator
Owner Rules	Define who can modify the role.

Chapter 3: Admin Roles for User Management

This section contains the following topics:

[Admin Roles and Admin Tasks](#) (see page 41)

[Create an Admin Role](#) (see page 42)

[Verify an Admin Role](#) (see page 47)

[User-defined Custom Attributes for Roles](#) (see page 47)

[Allow Users to Self-Assign Roles](#) (see page 50)

Admin Roles and Admin Tasks

You create roles that contain tasks for managing objects based on your individual business requirements. For example, you might create several roles with tasks that manage users and other roles with tasks that manage the roles you create.

Alternatively, you might create separate roles with:

- Tasks for administrators to manage users
- Tasks that manage the administrators
- Tasks to manage admin roles
- Tasks to manage access roles

Note: You can also use the default admin roles supplied with Identity Manager. These roles have tasks that are grouped in categories similar to the preceding list.

Admin Roles and Identity Manager Environments

When you log into an Identity Manager environment, your user account has one or more admin roles. Each admin role contains tasks, such as Create User, that you use in that Identity Manager environment.

For example, in the *central* Identity Manager environment, an admin role, *Help Desk*, has tasks for resetting passwords. The role has a member rule that the user must be an IT employee. When IT employees log into the *central* Identity Manager environment, they have the *Help Desk* role and can reset the passwords of users in that Identity Manager environment.

Admin Roles and the Identity Manager User Console

An Identity Manager environment is viewed through the Identity Manager user console. Your assigned admin roles determine what you see in that console as shown in the following table:

Assigned Roles	Format of the Identity Manager User Console
System Manager role	The category list for all objects and all default admin tasks for managing those objects
Roles for managing more than one type of object	The category list with one item for each type of object you can manage
Roles for managing one type of object, such as Users	The tasks for that object (such as Modify User) <i>without</i> a category list
An approval role	The Work list screen Appears if the administrator has tasks pending approval (for example, self-registering users need approval)

If you can manage more than one object, the category list appears and shows the objects that you can modify, such as Users and Groups as tabs across the top of the screen. Select a tab to see tasks in your assigned roles.

Note: If your internet browser does not support Cascading Style Sheets (CSS), the Identity Manager User Console uses a different format. To control that format, see the *Configuration Guide*.

Create an Admin Role

You can create an admin role once you know the role requirements. These requirements concern who will use this role, what objects it will manage, and which Environment has the objects to be managed.

Begin Admin Role Creation

You create an admin role from the User Console.

To create an admin role

1. Log into an Identity Manager account that has a role with tasks for creating admin roles.

For example, the first user of an Environment has the System Manager role, which has the Create Admin Role task.

2. Under Roles and Tasks, select Admin Roles, Create Admin Role.
3. Choose the option to create a new role or a copy of a role.

The Profile tab appears where you begin defining the admin role.

4. Define the Admin Role Profile.

Define the Admin Role Profile

On the Profile tab, you define basic characteristics of the role.

To define the profile

1. Enter a name and description, and complete any other custom attributes that are defined for the role.
2. Select Enabled if you are ready to make the role available for use as soon as you create it.
3. [Select Admin Tasks for the Role](#) (see page 43).

More Information:

[Profile Tabs and Profile Screens](#) (see page 71)

Select Admin Tasks for the Role

On the Tasks tab, you select the admin tasks to include in the role.

To select admin tasks

1. Select the category, then the task.

You can include tasks from different categories or copy tasks used in another role. You can also add or remove tasks by clicking icons.

In creating a role or task, you see icons for adding, editing, and removing items. They are defined in the following list:



Go forward or select the current item to view or edit it.

If JavaScript is disabled, press the forward button to select from a drop down list.



Go back or undo a previous selection.



Insert an element, such as a task or rule.



Delete the current task or, in a rule, the expression that follows.



Move the current item up in the list.



Move the current item down in the list.

2. Define Member Policies for an Admin Role.

Define Member Policies for an Admin Role

On the Members tab, you create member policies, which determine who can be a role member.

To define member policies

1. Click Add to define member policies. A member policy contains these rules:
 - A member rule which defines the requirements for a user to be a role member.

Note: The following operators treat numbers as characters in member rules:

 - Less than (<)
 - Less than or equal to (<=)
 - Greater than (>)
 - Greater than or equal to (=>)

For example, '10' will come after '1' but before '2'.
 - Scope rules which limit the primary and secondary objects available to tasks in the role.

For example, if the role contains a task that modifies users by assigning them to groups, the user scope rule limits the users (primary object) that can be found and the group scope rule limits the groups (secondary object) that can be assigned.

Note: Be sure to enter an answer to at least one scope question. The scope rules limit the primary and secondary objects available to tasks in the role. For example, if the role contains a task that modifies users by assigning them to groups, the user scope rule limits the users (primary object) that can be found and the group scope rule limits the groups (secondary object) that can be assigned.
2. Verify that the Member Policy appears on the Members tab.
 - To edit a policy, click the right arrow symbol on the left.
 - To remove it, click the minus sign icon.
3. On the Members tab, enable the checkbox labeled “Administrators can add and remove members of this role,” unless users should only become members by meeting a member rule.

Once you enable this feature, the screen expands.

4. In the expanded area, define the [Add Action and Remove Action](#) (see page 37) for when a user is added or removed as a role member.

Important! When defining an add action, avoid setting up a rule that refers to the role you are defining. For example, do not define the add action that makes a member of Role A by being a member of Role A. This may cause errors.

5. [Define Admin Policies for an Admin Role](#) (see page 46).

Define Admin Policies for an Admin Role

On the Administrators tab, you define who can add or remove users as members and administrators of this role.

To define admin policies

1. If you want to make the Manage Administrators option available, enable the check box labeled "Administrators can add and remove administrators of this role."

Once you enable this feature, the screen expands.

2. In the expanded area, define the Add Action and Remove Action for when a user is added or removed as an administrator of the role.
3. Define admin policies, which contain admin and scope rules and at least one administrator privilege (Manage Members or Manage Administrators).

Note: You can add several admin policies with different rules and different privileges for administrators who meet the rule.

4. To edit a policy, click the arrow symbol on the left. To remove it, click the minus sign icon.
5. [Define Owner Rules for an Admin Role](#) (see page 46).

Define Owner Rules for an Admin Role

On the Owners tab, you define rules about who can be an owner of the role, a user who can modify the role.

To define owner rules

1. Define owner rules, which determine which users can modify the role.
2. Click Submit.

A message appears to indicate the task has been submitted. A momentary delay may occur before a user can use the role.

If you selected Enabled when you created this role, the role is available to be used. If a user meets conditions in the member rule, that user can now log into the Identity Manager environment and use the tasks in the role.

Verify an Admin Role

To check that the role was created, choose Admin Roles, View Admin Role, then select the name of the role.

Alternatively, you can choose System, View Submitted Tasks to see if the role creation task has completed.

User-defined Custom Attributes for Roles

Identity Manager supports user-defined custom attributes that allow you to filter roles in your organization effectively. For example, in your corporate environment you may have the need to create more than a thousand roles. You might want to categorize these roles by business units or by geographical locations. If you want to search for roles that are specific to a particular geographical location, you can use the custom attributes to filter the roles in your organization.

You can use custom attributes in the Create, Modify, and View tasks for the following roles:

- Access Roles
- Admin Roles

You must perform the following steps to add custom attributes to admin tasks and search screens.

1. Add custom attributes to any of the admin tasks that are defined for roles.
2. Configure the search screens for roles with custom attributes.

More Information:

[Configure Custom Attributes in Profile Tab for Roles](#) (see page 48)

[Add Custom Attributes to Search Screen of Roles](#) (see page 49)

Configure Custom Attributes in Profile Tab for Roles

Identity Manager allows you to configure up to 10 custom attributes to suit your requirements. The custom attributes are added to the Profile tab of the admin tasks that are defined for the roles in Identity Manager.

To configure custom attributes in the Profile tab

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.

The Select Admin Task page appears.

2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Submit.

Identity Manager displays the admin tasks that satisfy the search criteria.

3. Select any of the admin tasks that are defined for the following roles, and click Select.

- Access Roles
- Admin Roles

Identity Manager displays the task details for the selected admin task.

4. Click the Tabs tab.

The tabs that are configured to be displayed with this admin task appear.

5. Click  to edit the Profile tab that will be used for the Modify Admin task.

The Configure Profile screen appears.

6. Select the custom fields and enter the labels for each of the custom fields that you want to display on the Profile tab and click OK.

The custom attributes will be available in the Profile tab of the modified task after you submit the task. To make the roles searchable based on the custom attributes, you must configure the search screen to display these custom attributes.

Add Custom Attributes to Search Screen of Roles

When you want to filter roles in Identity Manager, you can only use the attributes that are available in the search screen. To filter the roles based on the custom attributes that you have defined, you must add the custom attributes to the search screen of the roles.

To add Custom Attributes to the Search Screens of roles

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.

The Select Admin Task page appears.

2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Submit.

Identity Manager displays the admin tasks that satisfy the search criteria.

3. Select any of the admin tasks that are defined for the following roles, and click Select.

- Access Roles
- Admin Roles

Identity Manager displays the task details for the selected admin task.

4. Click the Search tab in the Modify Admin Role screen.

The search screen details appear.

5. Click ellipses button  to locate search screens.

The Select Screen Definition page appears.

6. Select the corresponding Manage Roles Search screen, and click Edit.

The Configure Standard Search Screen appears.

7. Add the custom attributes defined for this role to the following tables:

- Select the fields that a user can search on
- Select the fields that appear in the search results

Note: The labels for the custom attributes have values such as Custom 1, Custom 2, etc,. To make search easier, you must change the labels of these custom attributes to the same labels that were used in the Profile tab. For more information about selecting custom attributes in search screens, see [Search Fields and Search Results](#) (see page 111).

8. Click OK.

The edits are saved to the search screen and the Select Screen Definition page appears.

9. Select All Admin Roles from the Search Options list.

10. Click Submit.

The Admin Roles are modified to use the custom attributes. You can search, scope and filter your admin roles based on the new custom attributes.

Allow Users to Self-Assign Roles

There may be some roles in an environment that users can assign to themselves. For example, you may want to allow users to sign up for the Delegation Manager role so that they can delegate the work items of one user to another user.

To control the roles that users can assign to themselves, you configure criteria in the Roles Self-Manager task.

To allow users to assign roles to themselves

1. Modify the Roles Self-Manager task as follows:

- a. Select Roles and Tasks, Modify Admin Task, and search for the Roles Self-Manager task.
- b. Select the Tabs tab.

Identity Manager displays the list of tabs that apply to the task.

- c. Select the right arrow icon next to the Roles Self Manager tab to edit it.
- d. Complete the following fields:

Show only Admin Roles Meeting the Following Rules

Specifies the criteria that Identity Manager will use to determine which roles to allow users to assign to themselves.

To add additional rules, click the plus (+) icon.

User to be used as Admin Role Administrator

Specifies the administrator for roles that users can assign to themselves.

The roles that users can assign to themselves must have the user you select in this field as an administrator *and* meet the criteria you specified in the Show Only Admin Roles Meeting the Following Rules field.

List Screen

Specifies the columns and format for the list of roles that a user can select to self-assign a role.

- e. Click OK, then click Submit.
2. Add the Roles Self-Manager task to a role, and assign that role to users who should have this capability.

Chapter 4: Admin Tasks

This section contains the following topics:

[Admin Task Planning](#) (see page 53)
[How to Create an Admin Task](#) (see page 58)
[Define the Profile of the Task](#) (see page 60)
[Choose Tabs for the Task](#) (see page 65)
[Define the Task Scope](#) (see page 108)
[View Fields in the Task](#) (see page 116)
[Assign Workflow Processes for Events](#) (see page 116)
[Active Directory Prerequisites](#) (see page 116)
[External Tasks for Application Functions](#) (see page 118)
[Advanced Task Components](#) (see page 120)

Admin Task Planning

Admin roles consist of admin tasks, which represent granular capabilities for managing objects. For example, you could manage a user object by using these admin tasks:

- Create User
- View User
- Modify User
- Reset User Password

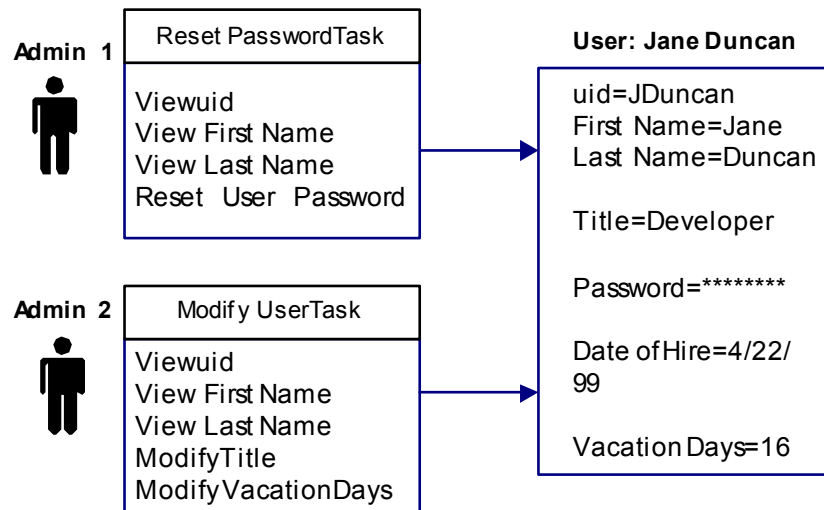
Admin tasks include *events*, actions that Identity Manager performs to complete the task. A task may include multiple events. For example, the Create User task may include events that create the user's profile, adds the user to a group, and assigns roles.

You create or modify each task to match your exact requirements. Then, you combine the appropriate admin tasks into admin roles, which you assign to administrators. With these roles, administrators have the exact privileges they need to manage objects.

To plan admin task creation, decide which objects you need to manage (user, group, organization, role, or task) and which administrators will use these tasks. For example:

- To manage users, help desk administrators need tasks that manage user attributes, such as a user ID or title.
- To manage users' access to applications, other administrators need tasks that make users members of access roles.
- To manage the roles used by help desk administrators, higher-level administrators need tasks that manage admin roles.

For one type of object, such as users, you can create tasks so that different administrators manage different attributes. For example, the following figure shows a user who is managed by two administrators.



- Admin 1 has the Reset User Password task; that administrator can view the employee's user ID and name or reset her password.
- Admin 2 has the Modify User task; that administrator can view the employee's user ID and name or modify her title and vacation days.

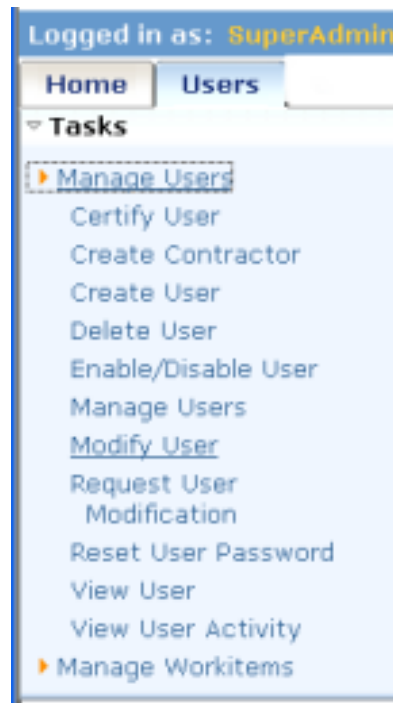
A Sample Admin Task

When you create an admin task, you define the content and layout of screens in the task, including:

- The name of the task
- The category where the task appears

- The tabs and fields to use in the task, and field display properties
- The attributes on the Profile tab
- The fields an administrator can use in a search query, and the fields displayed in the search results

To understand the elements of a task, consider the Modify User task. Choose Users, Manager Users, Modify User. In this task, Users is the category, Manage Users is a subcategory, and Modify User is the task. You create the category and task names when you create a task.



When you choose Modify User, a search screen appears. A *search screen* provides options for finding the object to view or modify. Each option is called a *filter*, which is a limit to the objects found by the search.

After you fill in the search screen, a screen with tabs appears. For example, the following figure shows the tabs for the Modify User task. The Profile tab appears first and shows user attributes; the other tabs show role and group privileges for the user.

For the task you create, you decide which tabs to include and determine their order and content.

Modify User: *SalesMgr*

Profile	Access Roles	Admin Roles	Groups	Delegate Workitems

Organization Employee

User ID SalesMgr

Enabled ☒

• **First Name** Sales

• **Last Name** Manager

• **Full Name** Sales Manager

Email

For example, using the Modify User task as a template, you could create a Modify Contractor task, which has changes to:

- The fields on the Profile tab
- The tabs to include in the task and their content
- The category under which the task appears

You might create this task under a new category, Contractor.



The Modify Contractor task includes some of the fields on the Profile tab in the Modify User task plus other fields, such as the start date of the contract and the contractor's company. Administrators can search for a contractor by searching on the contractor's name, company, and start date.

Modify Contractor: *jhansen*

Profile	Groups	Contractor Roles
User ID jhansen		
Enabled ☒		
• First Name	Julia	
• Last Name	Hansen	
Email	jhansen@wxyz.com	
Start Date	10/19/2007	
Company		

The new task also includes a Contractor Roles tab where you add roles for contractors.

Admin Task Usage Options

Identity Manager provides two ways to use admin tasks:

- **Select the task**

You select a category and task, and then search for the object to which the task applies.

For example, to modify a user profile, you select the Users category, and then select the Modify User task. You then search for the user to modify.

■ Select the object

You use "Manage" tasks, such as Manage Users or Manage Groups to search for an object. Once you select the object, you can display a list of tasks that you can use to manage that object. This method is called *object-task navigation*.

For example, to modify a user using this method, you select the User category, then select the Manage User task. You search for and select the user that you want to manage. In the search results, you click an icon to see a list of tasks that you can use to manage the selected user. From that list, you can select Modify User or any other appropriate task.

You can also configure task lists in tasks other than Manage tasks. For example, you can add a task list to a Membership tab. In this case, a task list is available for each member that appears on the Membership tab.

Note: Only tasks that the current administrator can use appear in the task list for an object.

Admin Task Processing

The time it takes to process a task depends on the steps involved. When a task is submitted for processing, Identity Manager performs the following steps:

1. Identity Manager validates the data being submitted.
2. If the task requires approval, Identity Manager sends the task to the workflow engine.
 - a. The workflow engine determines approvers, and places the approval task in the approvers' work lists.
 - b. Optionally, Identity Manager sends email notifying approvers of the pending work item.
 - c. An approver reserves the work item (which removes the item from the work lists of other approvers), and approves or rejects the item.
 - d. Optionally, Identity Manager sends email notifying involved users of the task's status.
3. Identity Manager carries out the task, if the task was not rejected.

How to Create an 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.

When you create an admin task, you complete the following steps:

Note: The section [Active Directory Prerequisites](#) (see page 116) includes additional considerations if Identity Manager is managing an Active Directory user store.

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Create Admin Task.

Identity Manager asks if you want to create a new task or create a task based on an existing task.

For example, select the Modify User task as the basis of the new task.

2. Select a creation option, and click OK.
3. Once you select Ok, you see a screen with the following five tabs:

Tab	Purpose	See this Topic
Profile	Define the profile of the task being created	Define the Profile of the Task (see page 60)
Search	Limit the range of objects that are managed by the task	Define the Task Scope (see page 108)
Tabs	Choose and design the tabs for the task	Choose Tabs for the Task (see page 65)
Fields	Show the fields used on all tabs	View Fields in the Task (see page 116)
Events	Select a workflow process for each event if the Identity Manager environment and the task uses workflow	Assign Workflow Processes for Events (see page 116)

Define the Profile of the Task

The Profile tab includes general settings for the task.

To define the profile of the task

1. Choose the type of object for the task, which is called the primary object, and the action to perform on it.
2. Complete the required fields and select the appropriate check boxes as needed for the task.

Note: If you are creating a task that has similar profile settings as an existing task, click Copy Profile From Another Task. This option populates the profile settings for the task you are creating with the profile settings from any existing task that you select. You then add a name and description for the new task.

3. (Optional) Associate a business logic task handler with the task.
4. Once you complete this tab, proceed to the next step, [Define the Task Scope](#) (see page 108).

Admin Task Profile Tab

The Admin Task Profile Tab lets you define general settings for an admin task.

This tab contains the following fields:

- **Name**

Defines the name of the task.

- **Tag**

Defines a unique identifier for the task. It is used in URLs, web services or properties files. It must consist of letters, numbers, or underscores, beginning with a letter or underscore.

- **Description**

Specifies an optional note about the purpose of the task.

- **Task Order**

Specifies the display order for the task. If no order is specified, the tasks are displayed in alphabetical order.

- **Category**

Specifies a category for the task. Categories are displayed as tabs at the top of the screen.

- **Category Order**

Specifies the order in which the category tab appears. For example, if you set the category order to 3, the category you specified will appear as the third tab.

- **Category 2**

Specifies the second level category, which appears as a link below the list of category tabs. The second level category appears only when the tab for the first level category is selected. For example, if you created a task with the first level category of Employee and a second level category of Employee Management, the Employee Management category would appear only after you select the Employee tab.

- **Category 2 Order**

Specifies the order in which the second level category appears, if more than one second level category exists in a primary category.

- **Category 3**

Specifies the third level category, which appears in the left navigation pane. Tasks are listed under the third level category. For example, in a default environment, a user with the System Manager or User Manager role sees the third level category Manage Users when he selects the Users tab.

- **Category 3 Order**

Specifies the order in which the third level category appears.

- **Primary Object**

Specifies the object that the task operates on.

- **Action**

Specifies the operation to perform on the object.

■ **User Synchronization**

Specifies whether the task synchronizes user accounts with identity policies. You can select one of the following options:

– **Off** (default)

Specifies that this task does not trigger user synchronization.

– **On Task Completion**

Specifies that Identity Manager starts the user synchronization process after all of the events in a task complete. This setting is the default synchronization option for the Create User, Modify User, and Delete User tasks. The default setting for all other tasks is Off.

Note: If you select the On Task Completion option for a task that includes multiple events, Identity Manager does not synchronize users until all of the events in the task complete. If one or more of those events require workflow approval, this may take several days. To prevent Identity Manager from waiting to apply identity policies until all events complete, select the On Every Event option.

– **On Every Event**

Specifies that Identity Manager starts the [user synchronization process](#) (see page 141) when each event in a task completes.

For tasks with a primary and secondary event for the same user, setting user synchronization to On Every Event may result in more identity policies being applied to a user than if the On Task Completion option is selected.

■ **Account Synchronization**

Synchronizes accounts that exist in the Provisioning Server, if you have provisioning enabled.

– **Off** (default)

Specifies that this task does not trigger account synchronization.

– **On Task Completion**

Specifies that Identity Manager starts the account synchronization process after all of the events in a task complete.

– **On Every Event**

Specifies that Identity Manager starts the account synchronization process when each event in a task completes.

Note: For best performance, select On Task Completion. However, if you select the On Task Completion option for a task that includes multiple events, Identity Manager does not synchronize accounts until all of the events in the task complete. If one or more of those events require workflow approval, this may take several days. To prevent Identity Manager from waiting to synchronize accounts until all events complete, select the On Every Event option.

■ **Hide in Menus**

Prevents the task from appearing in menus. Enable this control if the task is only invoked by a URL or by another task.

■ **Public Task**

Makes the task available to users who have not logged into Identity Manager. The default public tasks are forgotten password and self-registration.

■ **Enable Auditing**

Records information about the task in an auditing database. Audit information can be used to generate reports. See the *Configuration Guide*.

■ **Enable Workflow**

Enables the Identity Manager events associated with the task to trigger workflow processes, if you have the workflow engine installed. For example, the events associated with the Delete Group task may trigger a workflow process that includes an approval step.

■ **Enable Web Services**

Marks the task as one for which Web Services Description Language (WSDL) output can be generated from the Management Console. Enable this control if you want to use remote task submission. For more information, see the *Programming Guide for Java*.

■ **Workflow Process**

Enables configuration for task-level workflow instead of event-level workflow. Task-level workflow occurs before any task activity is processed. No events or nested tasks execute before the workflow process job begins.

■ **Task Priority**

Determines the order in which Identity Manager executes tasks. Tasks with a High priority are executed before tasks with a Medium or Low priority. The default priority for a task is Medium.

Note: You can use the View Submitted Tasks task to search for tasks with a specific priority, and then display their status.

- **Business Logic Task Handlers**

Associates a [business logic task handler](#) (see page 122) with the task.

- **Workflow Action Buttons**

Add custom action buttons to workflow approval tasks.

- **Copy Profile from another task**

Copies data from the Profile tab of another task.

For example, you might copy the Profile tab settings from the Modify User task, then add a name and description.

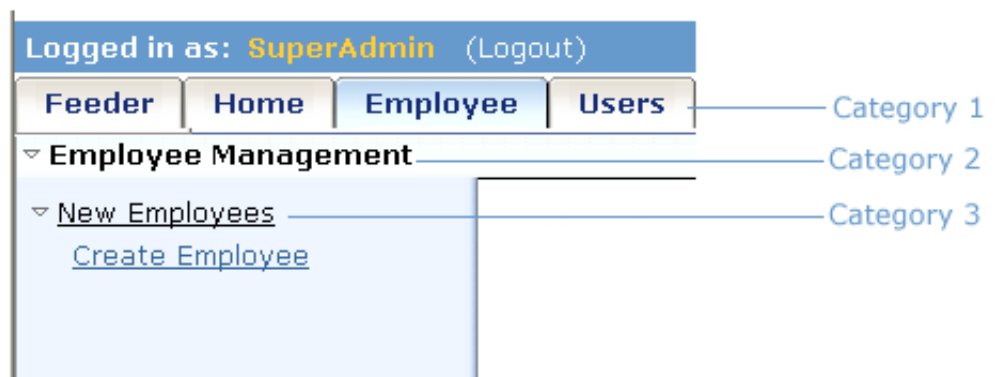
Task Categories

Task categories allow you to organize tasks to make them easier to locate and search for in the User Console.

You can specify three task categories:

- Category 1 is the top level category for tasks. These categories are displayed as tabs across the top of the User Console.
- Category 2 is a second level category. This category enables you group related tasks in a top-level category. If you do not specify a second level category, the default category is Tasks.
- Category 3 contains the tasks that administrators use. When administrators click the Category 3 name in the User Console, a list of tasks in that category is displayed.

Within each category, you can control the order in which the items in that category are displayed by specifying a category order. For example, in the following illustration, the Employee tab has a category order of 3.



Note: When a category contains multiple tasks, the category order that is specified in the profile for each task must be the same. If the category order is different, multiple instances of that category tab will appear. For example, the Employee category contains two tasks: Create Employee and Modify Employee. If the category order in the Create Employee task is 3 and the category order in the Modify Employee is 6, the Employee category appears as two tabs.

Choose Tabs for the Task

On the Tabs tab, name and configure the tabs; each one is a set of fields that you include in the task. You can include default tabs or create new ones. For example, the Modify User task includes the following tabs:

- Profile
- Access Roles
- Admin Roles
- Groups
- Delegate Work Items

To edit the definition of a tab, click the right arrow next to the tab name.

Tab Controllers

A tab controller determines how the tabs in a task are displayed. You select one of the following tab controllers:

- **Standard Tab Controller**

Displays the tabs for the task as independent tabs. Users can use the tabs in the task in any order.

This is the default tab controller.

Create Contractor:

The screenshot shows a web form titled "Create Contractor:". At the top, there are four tabs: "Profile" (selected), "Access Roles", "Admin Roles", and "Groups". Below the tabs, there are four input fields, each with a yellow dot icon to its left: "Organization" with the value "Employee", "User ID" with the value "kmiddleton", "Password" with masked characters "*****", and "Confirm Password" with masked characters "*****".

■ Wizard Tab Controller

Displays the tabs in a task as a wizard. Administrators use each tab in order.

Create Contractor: Profile

The screenshot shows a wizard interface with four steps: 1 Profile, 2 Access Roles, 3 Admin Roles, and 4 Groups. The 'Profile' step is active, indicated by a yellow background and a yellow arrow. Below the steps, there are four input fields: 'Organization' with the value 'Employee', 'User ID' with the value 'kmiddleton', 'Password' with masked characters, and 'Confirm Password' with masked characters.

■ Sequence Tab Controller

Displays one tab, which is displayed as a single page, at a time. Users complete one tab and then click a custom button or link to move to the next tab.

The sequence of tabs and the buttons and links that are displayed are determined programmatically by JavaScript that you write when you configure the sequence tab controller.

In the custom JavaScript, you can specify the appearance and order of tabs based on user input. For example, if a user selects an option on the first tab, Identity Manager displays one page. If a user selects a different option, a different page is displayed.

The screenshot shows a single-page interface for the 'Create Contractor: Profile' task. It contains four input fields: 'Organization' with the value 'Employee', 'User ID' with the value 'kmiddleton', 'Password' with masked characters, and 'Confirm Password' with masked characters.

Select a Tab Controller

When you create or modify an admin task, you select a tab controller, which determines how the tabs in a task are displayed.

To select a tab controller

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for and select the admin task to modify.
Identity Manager displays the tabs to configure the task you selected.
3. Select the Tabs tab.
4. Select a tab controller from the list box.
5. (Optional) Configure the tab controller.

Identity Manager configures the tabs for the task based in the tab controller you select.

Configure a Tab Controller

To configure a tab controller, you specify a JavaScript method that determines whether a tab is displayed. The JavaScript is executed on the server side and has access to the subject of the task and all of the tabs.

To configure a tab controller

1. [Select a tab controller](#) (see page 67).
2. Click the right arrow icon to configure the tab controller.
3. Enter custom JavaScript in the Tab Display JavaScript.

Sample Javascript for Tab Controllers

Identity Manager includes sample Java Script files for Tab Display JavaScript and Active Tab JavaScript.

These files are installed in *im_admin_tools\CA\IAM Suite\IdentityManager\tools\samples\WizardSequencerScripts*

List of Default Tabs

Access Role Administrators

Lets you add, view, or remove administrators of the current access role.

Access Role Membership

Lets you add, view, or remove members of the current access role.

Access Role Profile

Defines the profile for access roles.

Access Role Tasks

Lets you view a role's access tasks, or add or remove access tasks. You can select access tasks from different applications.

Access Roles

Lets you view, add, or remove the roles for the selected user and view that user's privileges.

Access Task Profile

Defines the profile for access tasks.

Accounts

Lists accounts in managed endpoints for users who have been assigned provisioning roles. Typically, this tab is added to tasks that allow you to view or modify a user.

Account Templates

Lets you add, remove, or view account templates associated with a provisioning role.

Admin Role Administrators

Lets you add, view, or remove administrators of the current admin role.

Admin Role Membership

Lets you add, view, or remove members of the current admin role.

Admin Role Profile

Defines the profile for admin tasks.

Admin Role Tasks

Lets you view a role's admin tasks, add or remove admin tasks, and select admin tasks from different categories.

Admin Roles

Lets you view, add, or remove admin roles for a selected user and view that user's member and administrator privileges.

Admin Task Profile

Defines the Profile tab for admin tasks.

Administrators

Lets you add, edit, or remove admin policies.

Approvers

Lists all participants who can approve or reject the work item. It also allows reassignment of the work item.

Approve Task

Displays information about individual approval tasks in a work list.

Approve Event

Displays information about individual approval tasks in a work list.

Certify User

Lets you certify or revoke a user's roles.

Currently Matched Policies/Policies Already Applied

Displays the synchronization status for users.

Events

Lets you select and configure a workflow process for each event that the task initiates.

Execute Explore and Correlate

Lets you select an explore and correlate definition to execute.

Execute Explore and Correlate Profile

Displays the containers in an endpoint that you can explore or correlate.

External Tab (ExternalTab)

Displays the contents of a URL within the tab in a task.

Fields

Lets you view the fields contained in the task. The fields are the attributes defined on the associated profile screen.

Group Administrators

Adds or removes administrators of the current group.

Group Membership

Adds or removes users as group members or adds or removes nested groups to this group.

Group Profile

Allows you to define or view the profile of the group.

Groups

Lets you view, add, or remove the groups for a selected user and view that user's privileges.

Identity Policy Set Owners

Lets you add owner rules, which are rules about who can modify the identity policy set.

Identity Policy Set Profile

Defines the profile of the identity policy set.

JSP

Displays custom information. See your system administrator for details.

Manage System or Orphan Accounts

Assigns a global user to a system or orphan account.

Members

Lets you add, edit, or remove member policies.

Organization Profile

Lets you create, modify, or view the profile of an organization.

Owners

Lets you add, edit, or remove owner policies.

Policies

Creates or modifies an identity policy.

Profile (AdminTaskProfile)

Lets you define the profile of the admin task.

Profile (Generic) (ObjectProfile)

Lets you define the profile for any managed object.

Provisioning Role Administrators

Lets you add, view, or remove administrators of the current provisioning role.

Provisioning Role Membership

Lets you add, view, or remove members of the current provisioning role.

Provisioning Role Profile

Defines the profile of the provisioning role.

Recurrence Tab

Controls the schedule for when the explore and correlate action should occur.

Scope (TaskScope)

Lets you limit the scope of the task. If the task has no primary object, or if the action is self-modify, self-view, or approve, the Search tab does not appear.

Schedule

Lets you automate the execution of a task at a later date.

Synchronization Summary

Displays the synchronization status for users.

Tabs (TaskTab)

Lets you select a tab controller, which determines how the tabs in a task are displayed, and view, add or remove the tabs included in the task.

User History

Displays a history of all the tasks that are initiated, approved, executed on, and performed by any user.

Work List

Displays a list of work items (or approval tasks) that appears in the Identity Manager User Console of the participant authorized to approve the task.

User Profile

Defines or displays the profile of a user.

This tab includes additional functionality, such as generating separate events for password changes, that is specific to user objects.

Profile Tabs and Profile Screens

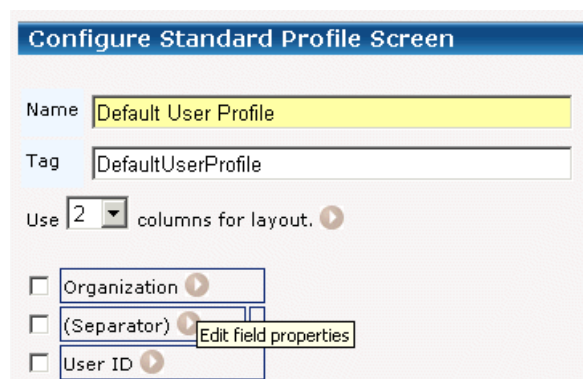
For most tasks, you include a Profile tab, which shows you the attributes for the primary object of the task. The *primary object* is the object to be created, viewed, or modified by the task. For example:

- For Modify User, the primary object is a user. The Profile tab includes user attributes, such as User ID and Last Name.
- For Modify Admin Task, the primary object is a task. The Profile tab includes task attributes, such as Task Name, Public Task, and Enable Workflow.

When you configure a profile tab, you define basic characteristics of that tab and you specify a profile screen. The *profile screen* is the user-visible part of the tab. It controls which attributes of the primary object appear on the tab and their display properties.

Note: You can use the same profile screen on the Profile tab of several tasks.

In the Profile screen definition, you select the fields for the task. The fields correspond to profile attributes. For example, the value entered in the User ID field of the Create User task is stored in a user profile attribute.



The screenshot shows a 'Configure Standard Profile Screen' window. It has a title bar and a main area with several fields. The 'Name' field contains 'Default User Profile' and the 'Tag' field contains 'DefaultUserProfile'. Below these is a 'Use' dropdown set to '2' with the text 'columns for layout.' to its right. Underneath are three items, each with a checkbox and a right-pointing arrow icon: 'Organization', '(Separator)', and 'User ID'. The 'User ID' checkbox is checked. A tooltip box with the text 'Edit field properties' is positioned over the 'User ID' checkbox.

For admin tasks, Identity Manager allows you to add up to 10 custom attributes to the Profile tab. You can use the custom attributes to refine and search for roles.

More Information:

[Field Properties on a Profile Screen](#) (see page 75)

[History Display Field Properties](#) (see page 89)

[History Editor Field Properties](#) (see page 87)

Modify a Profile Screen

You can modify an existing profile screen definition to:

- Add or remove fields
- Change the layout of fields
- Edit field properties
- Add help text by creating separators that are of type HTML anywhere on the profile screen

To modify a profile screen definition

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for and select the admin task to modify.
Identity Manager displays the tabs to configure for the task you selected.
3. Select the Tabs tab, then select the Profile tab.
4. Click the ellipses (...) button for the Screen field.

Identity Manager displays a list of existing profile screen definitions.

5. Select the profile screen definition that you want to modify or copy and then click one of the following buttons:

- **Select**

Adds the selected screen definition to the tab you are configuring

- **Edit**

Opens a new screen where you can change the settings, including fields, field properties, and layout for the selected screen definition

- **Delete**

Deletes the selected screen definition

- **New**

Opens a new screen where you can create a screen definition. The new screen definition does not include any default fields.

- **Copy**

Creates a new screen definition using the settings from an existing screen definition. To create a new screen which is based on an existing screen, you add a new name and tag to the screen definition, and modify the settings as needed.

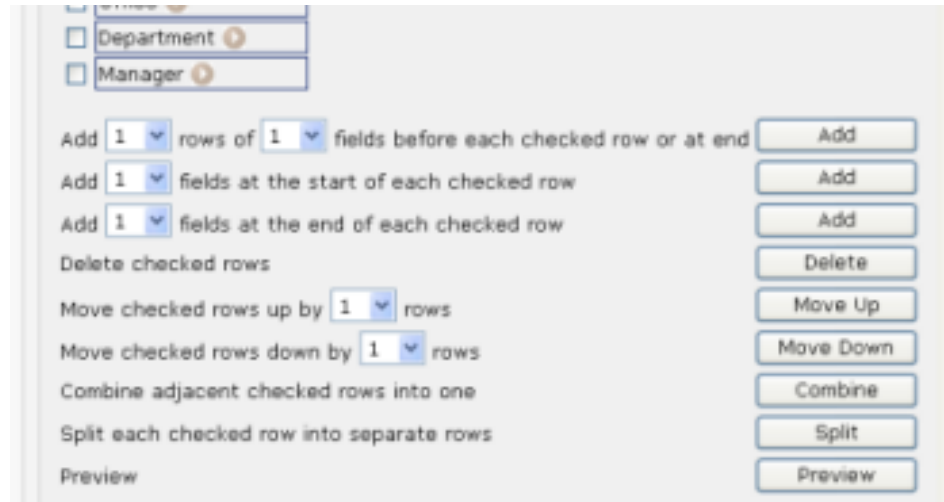
- **Cancel**

Returns you to the Tab configuration screen.

If you selected Edit, New, or Copy, Identity Manager opens a new screen where you can create or modify a profile screen definition.

Format of the Profile Screen

The default profile screens include all attributes for the object in the order used in the directory.xml file. To remove or rearrange attributes, scroll down to the bottom part of the screen.

A screenshot of a software interface for formatting profile screens. At the top, there are two checkboxes labeled 'Department' and 'Manager', each with a small circular icon to its right. Below these, there are several rows of controls. Each row consists of a text label, a dropdown menu (all showing the number '1'), and a button. The rows are: 'Add 1 rows of 1 fields before each checked row or at end' with an 'Add' button; 'Add 1 fields at the start of each checked row' with an 'Add' button; 'Add 1 fields at the end of each checked row' with an 'Add' button; 'Delete checked rows' with a 'Delete' button; 'Move checked rows up by 1 rows' with a 'Move Up' button; 'Move checked rows down by 1 rows' with a 'Move Down' button; 'Combine adjacent checked rows into one' with a 'Combine' button; 'Split each checked row into separate rows' with a 'Split' button; and 'Preview' with a 'Preview' button.

Note: When you edit the field properties on the profile screen, you may find it easier to manipulate rows of multiple fields as follows:

1. Click Split to place the fields on separate rows.
2. Manipulate the fields on separate rows.
3. Click Combine to return the fields to a single row.

To add text or images at the beginning or end of the profile screen, enter HTML in the text fields shown in the following figure:

Field Properties on a Profile Screen

You select a field to edit its properties. Each field has different properties. For example, the Last Name field uses some common properties, which are shown in the following figure:

The screenshot shows a 'Field properties' dialog box with the following fields and values:

- Attribute Name:** Last Name (dropdown menu)
- Style:** Text (dropdown menu)
- Name:** Last Name (text input)
- Permission:** Read/Write Required (dropdown menu)
- Label span:** 1 (dropdown menu) columns
- Field span:** 1 (dropdown menu) columns
- CSS Class:** (empty text input)
- CSS Style:** (empty text input)
- Size:** (empty text input)
- Max Length:** (empty text input)
- Default:** (empty text input)

You can set the following properties for a field:

Note: The fields that are displayed in the Field Properties screen are determined by the option you select in the Style field. You may not see all of the fields described in this list.

- **Attribute Name**

Specifies the name of the attribute in the directory.xml file.

- **Style**

Determines the presentation of the field.

[Style Options](#) (see page 81) lists styles that you can select for a field.

- **Name**

Specifies the label you want for this attribute in the task.

- **Permission**

Determines the privilege level for the field.

Note: If a field is required by the user store, choose a Required setting. Required fields are indicated by a yellow dot in the screen.

- **Read**

Specifies that an administrator can view but not modify the field.

- **Read/Write**

Specifies that an administrator can see the current value of the field (if one exists), and can enter a value for the field.

- **Read/Write Required**

Specifies that a field is required, but otherwise functions as the Read/Write setting.

- **Write**

Specifies that an administrator cannot see the current value of the field (if there is one), but can enter a value.

For example, an administrator can change a user's password, but cannot view the user's current password.

- **Write Required**

Specifies that a field is required, but otherwise functions as the Write setting.

- **Label span**

Specifies the number of columns that the label will span.

- **Field span**

Specifies the number of columns that the field will span (excluding the label)

- **Date Display Pattern**

Determines the format of dates displayed in a field and in the Date Picker control. Specify the date display pattern using Java conventions. For example, the following Java expression is displayed as Oct 2007:

MMM yyyy

For more information about Java date formats, see the documentation for the Java™ 2 Platform Std. Ed. v1.4.2 at the Sun website (<http://java.sun.com/j2se/1.4.2/docs>). Search for SimpleDateFormat.

Note: The Date Display Pattern field appears only when the Date Picker style is selected.

- **CSS Class**

Specifies the Cascading Style Sheet class that controls the presentation of this field.

- **CSS Style**

Determines field properties and style defined using HTML property tags.

You can use this field to set the width of a field. For example, to set the width of a field with the Drop Down style to 300 pixels, you specify the following in the CSS Style field:

CSS Style	{width: 300px}
Selection Options	<i>Enter options on separate value;display-value".</i> Boston New York City Portland San Francisco

Note: By default, the width of fields that include a list of values, such as a drop down or multi-selector box, is set to auto ({width:auto}). This setting sizes the field to accommodate the largest value in the field. For example, if the largest value in the City option selector field is San Francisco, the option list is sized to display the entire value.

You can also use the CSS Style field to control other display properties, such as text size and background color.

- **Rows**

Specifies the number of rows that a text area for user input should include.

For example, you may want to define a text area for the Description field, which allows users to enter four rows of text.

Note: This field is available only when you select the Text Area style.

- **Columns**

Specifies the number of columns in a task screen that a text area for user input should span.

For example, you may want to define a text area for the Description field, which allows user comments to span all of the columns on the text screen.

Note: This field is available only when you select the Text Area style.

- **Checked Value**

Specifies the value of a field when its checkbox is selected. For example, the checked value for the Enabled field is true.

The default value is true.

Note: This field is visible when the checkbox style is selected.

- **Unchecked Value**

Specifies the value of a field when its check box is cleared. For example, the unchecked value for the Enabled field is false.

The default value is false.

Note: This field is visible when the checkbox style is selected.

- **Allow Other Unchecked Values**

When unchecked, sets the value of the attribute to false in the user store if the attribute is empty. When checked, Identity Manager allows the attribute to be empty.

Use this field to automatically set empty attributes to false in the user store.

- **Default**

Sets the default value (true or false) for the field.

- **Size**

Specifies the size of the field. Enter a number based on the style of field. For text and password, enter the number of characters. For drop-down, select, multi-select, and multi-text, enter the number of rows.

- **Source of Selection Options**

Specifies how a field that contains multiple options is populated.

- **None**

Identity Manager will not use an external source for selection options.

- **Select Box Data**

Specifies that Identity Manager will populate the options in the field using a Select Box Data XML file.

- **Simple List**

Allows you to enter a list of options in a text box. If you select this option the following field appears:

Selection Options

Enter options on separate rows. If the option has separate display and storage values, enter them as "storage-value;display-value".

- **Depends on the value of another field**

Specifies that Identity Manager will populate the options in the field based on options in a other field on the task screen.

Dependency on another field is defined in a Select Box Data XML file.

- **Javascript**

Specifies JavaScript that contains the options for the field. If you select this option, the following field appears:

Selection Options (JavaScript)

This JavaScript must contain a function with the signature "function getOptions(FieldContext)" and return a pipe delimited string of options. If the option has separate display and storage values, enter as "storage-value;display-value"

- **Preserve non-options**

Specifies if Identity Manager will preserve the user defined options in a select based control field that is populated using Select Box Data. For example, a drop down combo box 'City' allows a user to add custom values to the field. The other options for the field 'City' are populated using Select Box Data. The setting for Preserve non-options will determine if Identity Manager will retain the user defined value set to the field 'City' or force the user to use only the values populated using Select Box Data. The Preserve non-options should be enabled to allow the user to add custom data to the select based controls.

- **Default**

Disabled. Identity Manager will force the user to select only the valid options.

- **Max Length**

Sets the maximum number of characters that can be entered for this field.

- **Current Values Label**

Sets the text that appears above the list box that contains selected items in the object selector.

- **Available Values Label**

Sets the text that appears above the list box that contains the items that are available for selection in the option selector.

- **Default**

Indicates the value that is displayed by default, and that is stored in the profile if no other value is provided.

Note: For a checkbox, enter true to make the default enabled; enter false to make the default disabled.

[Task-Level Validation](#) (see page 121) describes validation properties.

- **Default JavaScript**

Enables you to use JavaScript to set the default value for a field. Using JavaScript, you can set the value dynamically. For example, you can set a default value based on other attributes.

Use this field for Create tasks only.

- **Initialization JavaScript**

Enables you to use JavaScript to set the default value for a field. Use this field for any task type.

Note: The JavaScript in this field executes after the JavaScript in the Default JavaScript field.

- **Validation Expression**

Contains a regular expression that performs task-level validation

- **Validation Java Class**

Contains the fully-qualified name of a Java class that performs the validation, for example:

`com.mycompany.MyJavaValidator`

Identity Manager expects the class file to be located in the root directory designated for custom Java class files.

- **Validation JavaScript**

Contains the complete JavaScript code that performs the validation.

You must provide JavaScript code in this field. With task-level validation, you cannot reference a file containing JavaScript code.

- **Disable AutoComplete**

Disables the AutoComplete feature in Internet Explorer. If this check box is selected, Internet Explorer does not attempt to provide suggestions for field values based on previous entries.

For more information on the AutoComplete feature, see the documentation for Internet Explorer.

Style Options

The Style field enables you to specify how a field is displayed on a Profile screen. You can select the following styles:

- **Check Box**

Adds a check box next to the field name, which enables or disables a setting. For example, use a check box for the Enable User field. If the check box is selected, the user account is enabled. If the check box is clear, the user account is disabled.

- **Check Box Multi-Select**

Adds a check box next to each option for a field. Users can select multiple options from the option list.

- **Date Picker**

Displays a calendar icon next to a date field, such as Start Date. Administrators click the calendar icon to display a calendar control where they can select the date they want.

- **Drop Down**

Allows the user to select a value for the field. Only one value is visible. Users click an arrow to see additional values in the list.

The user can select a single value from the list.

- **Drop Down Combo**

Provides the same choice of values displayed by a Drop Down style, but adds a text box where the user can enter a new value.

- **Group Selector**

Displays a control for selecting a group.

- **Hidden**

Retrieves the field's value from the user store, but the field's label and value are not displayed on the task screen.

Hidden fields are used for logical attributes. (See the chapter on Logical Attributes in the *Programming Guide for Java*.)

- **Multi-Select**

Displays a list of values for a field.

In a Multi-Select box, the possible values for the field are visible in the list box. Users can select multiple values from the list.

A Multi-Select box can be used only to display fields associated with a multi-valued attribute.

- **Multi-Text**

Allows the user to enter multiple values in a text box.

- **Option Selector**

Displays two list boxes, which show the available and current values for the field. The user clicks buttons to add or remove current values.

- **Option Selector Combo**

Displays the two list boxes used for an Option Selector style plus a text box where the user can enter a new value.

- **Organization Selector**

Displays a control for selecting an organization.

- **Password**

Displays the field's value as a series of asterisks. For example, the password secret is displayed as *****.

- **Radio Button Single Select**

Displays a list of values for a field. A radio button appears next to each value.

In a Single Select box, the possible values for the field are visible in the list box. Users can select a single value from the list.

- **String**

Displays the field's value as read only. If no value exists, the field is blank.

- **Text**

Displays a box where the user can enter a value for the field.

If the field's permission is read only, the value is displayed as a label.

- **TextArea**

Displays a box where the user can enter values that are longer than a text field. For example, a description may require a text area.

- **UserSelector**

Displays a control for selecting a user.

Note: The values for drop down menus, drop down combo boxes, multi-select boxes, option selector, option selector combo boxes, and single-select boxes are determined by select box data.

Date Picker Options

The Date Picker style allows you to add a calendar icon to a field on a Profile screen. Users can click the icon to open a calendar that they can use to select a date. The selected date is stored in the profile attribute that is associated with the field. For example, you could add the calendar control to a Start Date field on the Profile tab for a Create Contractor task. When an administrator selects the first day of the contract, Identity Manager stores that date in the user's profile.

The Date Picker style has the following configuration settings:

- **Date Display Pattern**

Determines the format of dates displayed in a field and in the Date Picker control. Specify the date display pattern using Java conventions. For example, the following Java expression is displayed as Oct 2007:

MMM yyyy

For more information about Java date formats, see the documentation for the Java™ 2 Platform Std. Ed. v1.4.2 at the Sun website (<http://java.sun.com/j2se/1.4.2/docs>). Search for SimpleDateFormat.

Note: The Date Display Pattern field appears only when the Date Picker style is selected.

- **Date Storage Pattern**

Determines how the date is stored in the user store. Specify the date using Java conventions. See the description of the Date Display Pattern for more information.

- **Show Time Picker**

Adds a clock control to a field on a Profile screen. Users can use this control to select a time. The time is stored in the user store.

- **Time Picker Format**

Determines whether Identity Manager displays time in a 12 or 24 hour format.

- **Show Time Zone**

Specifies the time zone of the stored date and time.

Note: If you want to store time zone information, be sure to specify a Date Storage Pattern format that includes the time zone.

Note: The Date Storage Pattern, Show Time Picker, Time Picker Format, and Show Time Zone fields appear only when the attribute that you selected does not have the date valueType in the directory.xml file.

Screen-Defined Logical Attributes

Screen-defined logical attributes are fields on a Profile tab that are defined locally for the current task. You can use these screen-defined logical attributes to manipulate objects in a task screen or *modify* physical attributes that are stored in the user store.

Screen-defined logical attributes are defined, initialized, validated, populated, and implemented using JavaScript.

For example, a user profile has the following attributes--First Name, Last Name, Company, Email ID, and Organization. The Email ID should have the format First Name.Last Name@Company. You can create a screen-defined logical attribute called |Email ID| that uses JavaScript to calculate the Email ID using the values of the other fields in the task. You can use JavaScript to also update the physical attribute Email ID that is stored in the user store.

Note: Attributes enclosed within '|' are identified as screen-defined logical attributes.

You can use screen-defined logical attributes in User Console fields such as:

- Check Box Multi-Select
- Dropdown
- Dropdown Combo
- Multi-Select
- Option Selector
- Option Selector Combo
- Radio Button Single-Select
- Single-Select

The screen-defined logical attributes are useful when you are creating generic tasks that are not bound to any primary object. In this case, you create the fields on the Profile tab using only screen defined logical attributes. You cannot specify physical attributes.

Add Screen-Defined Logical Attributes

Any field on a profile task can be defined as a screen-defined logical attribute. You can use these screen-defined logical attributes to manipulate objects locally within the scope of that profile screen or modify physical attributes in the object store. For example, you can use screen-defined logical attributes to display a note or a warning on a profile screen, or set the Email address for a user in the object store.

To define fields as Screen-Defined Logical Attributes

1. [Modify Profile Screen](#) (see page 72) to add or modify fields to use screen-defined logical attribute.
2. Create or update field properties with the screen-defined logical attribute-specific values:

Attribute Name

Select (Screen Logical Attributes) in the Attribute Name field.

|Attribute Name|

Identifies the attribute name for the field.

Multi-valued

Specifies that the screen-defined logical attribute is multi-valued.

Note: By default, this option is disabled. If this field is disabled, then the attribute is only single-valued.

Name

Enter the display name for the screen-defined logical attribute name. The display name is enclosed within '|' on the User Console to distinguish screen-defined logical attributes from other attributes.

Note: If the screen-defined logical attribute has the same name as a Logical Attribute Handler, the screen defined logical attribute will override the Logical Attribute Handler.

3. Complete all the necessary [field properties](#) (see page 75).

Screen-Defined Logical Attributes in View Submitted Tasks

When you submit a task that contains screen-defined logical attributes, the original and updated values for the screen-defined logical attributes are displayed in the Task Details screen from the View Submitted Tasks tab.

Note: If you have defined any screen-defined logical attributes without binding them to any primary object, only the changed values for the attribute will be displayed in the Task Details screen in the View Submitted Tasks task. The original values will not be displayed. For example, you have created a generic task for which the Primary Object option in the Profile Tab is set to 'None', and added a screen-defined logical attribute 'Name' to the task. Update the value of the field 'Name' from 'John' to 'Joe' and submit the task. If you view the tasks details for this task from the View Submitted Tasks tab, you will see only 'Joe' listed in the 'Attributes Changed' table.

Select Box Data

You can populate the options that are available in the following fields:

- Check Box Multi-Select
- Dropdown
- Dropdown Combo
- Multi-Select
- Option Selector
- Option Selector Combo
- Radio Button Single-Select
- Single-Select

These options are stored in Select Box Data XML files. For example, you can use the Select Box Data XML files to populate options for a City or State drop down box on a Profile tab for the Create User task.

You can also use the Select Box Data XML file to configure a dependency between two fields in an admin task. For example, the options that are available in the City field may depend on the option a user chooses in the State field.

Note: [Custom Data for Select Boxes](#) (see page 354) provides more information on creating the Select Box Data XML file and using that file to populate select boxes.

History Editor Field Properties

The history editor is a text area which creates new history entries, if this text area contains text when the task is submitted. The history editor can include an optional submit button, which allows the creation of history entries without submitting the task.

The history editor has the following field property settings:

- **Attribute Name**

The name of the attribute in the directory.xml file.

Note: The Attribute Name can only be associated with the (Separator) attribute name because it is not compatible with a real or logical attribute.

- **Style**

The presentation of the field. This should be set to "HistoryEditor".

- **Name**

The label you want for this attribute in the task.

- **Label span**

The number of columns that the label will span.

- **Field span**

The number of columns that the field will span (excluding the label)

- **CSS Class**

The Cascading Style Sheet class that controls the presentation of this field.

- **CSS Style**

Field properties and style defined using HTML property tags.

Use this to set the width of a field. For example, to set the width of a field with the Drop Down style to 300 pixels, specify the following in the CSS Style field: {width: 300px}

By default, the width of fields that include a list of values, such as a drop down or multi-selector box, is set to auto ({width:auto}). This setting sizes the field to accommodate the longest string in the field.

Note: You can also use the CSS Style to control other display properties, such as text size and background color.

- **Label**

The label text which appears over or to the left of the text area. This can be a string or a localization key, specified according to Identity Manager localization rules.

- **Stakeholder**

This is a label attached to history log entries which describes the role of the user who created the log entry. For example, the following description would appear in the "Source" column of a history display for a user with an "Approver" stakeholder label:

User comment by SalesMgr (John Doe) acting as Approver

This can be a string or a localization key, specified according to Identity Manager localization rules. The stakeholder type is blank by default, and is optional.

- **Rows**

The number of rows in the history text area.

- **Columns**

The number of columns in the history text area.

- **History Level**

Status level information:

- **Task Level**—For approval tasks it is the task belonging to the event being approved. For non-approval tasks, this is the current task.
- **Event Level**—For approval tasks, this is the event being approved. For non-approval tasks, this returns no results.

- **Add Button Label**

The text to label for the submission button. This can be a string or a localization key, specified according to Identity Manager localization rules. If it is blank (the default value), then the button label is "Add History Event".

- **Add Button CSS Class**

These strings will be included in the <input> element in the profile screen, as the contents of the 'style' and 'class' elements respectively.

- **Add Button CSS Style**

These strings will be included in the <input> element in the profile screen, as the contents of the 'style' and 'class' elements respectively.

- **Enable Add Button**

If checked, the history editor includes its own independent submission button. This button submit only the new history entry, not the entire task.

More Information:

[History Display Field Properties](#) (see page 89)

History Display Field Properties

The history display is a list of text entries created using the history editor. The history display can appear on any profile screen, regardless of subject type.

The history display has the following field property settings:

- **Attribute Name**

The name of the attribute in the directory.xml file.

Note: The Attribute Name can only be associated with the (Separator) attribute name because it is not compatible with a real or logical attribute.

- **Style**

The presentation of the field. This should be set to "HistoryDisplay".

- **Label**

Text for the label which appear on top of the history display. If blank (default) the label text is "History".

- **History Level**

This can be set to one of the following:

- **Task Level**—For approval tasks it is the task belonging to the event being approved. For non-approval tasks, this is the current task.
- **Event Level**—For approval tasks, this is the event being approved. For non-approval tasks, this returns no results.

- **Show Entry Types**

This can be set to one of the following:

- **User Created Entries Only**—Show only runtime entries created using the history editor.
- **All Entries**—Show all entries, including those created by workflow or the task controller.

More Information:

[History Editor Field Properties](#) (see page 87)

Organization Field

If the user store that Identity Manager manages includes organizations, the default Create User task includes an Organization field. An administrator must search for and select the appropriate organization before creating a user profile.

To simplify the Create User task, you can configure Identity Manager to populate the Organization field dynamically, based on the administrator who is executing the task. In this case, the administrator does not have to specify an organization. The user is created in the organization where the administrator's profile exists. For example, if an administrator, whose profile exists in the Employees organization, creates a user profile for a new hire, Identity Manager creates the new profile in the Employees organization. If an administrator in the Suppliers organization uses the same Create User task, the profile for the new user that the second administrator creates would exist in the Suppliers organization.

Configure a Dynamic Organization Field

When you configure a dynamic organization field for the Create User task, Identity Manager creates new users in the organization where the profile for the administrator who is creating the user exists.

To configure a dynamic organization field

1. In the User Console, go to Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for and select the Create User task.
3. On the Tabs tab, click the right arrow icon to edit the Profile tab.
4. In the Screen field, click the ellipses (...) button to display a list of screens to edit.
5. Select the Create User Profile screen and click Edit.
6. Locate the Organization and click the right arrow icon to edit its properties.
7. Set Style to Hidden.
8. In the Default JavaScript field, enter the following:

```
function defaultValue(blthContext)
{
    return blthContext.getAdministrator().getOrg(null).getUniqueName();
}
```
9. Click Apply.
10. Click the left arrow next to Field Properties to return to the screen definition.

Layout of the Profile Screen

You can change the layout of a Profile screen by using the Separator field attribute. To add a Separator attribute to a screen definition, you add a new row with a Separator field. Once you select the Separator field, you can select one of the following styles for that field:

Binary (for LDAP user directories only)

Allows you to add a binary file, such as a certificate or other document, to the Profile screen.

HTML

Displays HTML on a Profile screen.

History Display

Displays a read-only table containing details of previous history entries in chronological order.

History Editor

Displays a text box for entering new history entries and a optional button for submitting the new entry.

Page Section

Allows you to divide the profile screen into multiple sections, which can have a different number of columns than other page sections on the same screen.

For example, the Page Section style allows you to create a profile screen that has an initial page section with a single column, and another page section with two columns.

Picture (for LDAP user directories only)

Allows you to add an image to a Profile screen.

Space

Adds a blank space to the screen to visually separate a set of fields.

Task

Adds a link to a different task to the Profile tab.

Add a Binary Attribute or Picture to a Profile Screen

You can configure Identity Manager to include a binary file or display a picture on a Profile screen. For example, you can configure a user profile screen to allow users to attach a document, such as a certificate, to the Profile screen or display a digital photograph of the user being managed.

Note: This functionality is available for LDAP user stores only.

To add a binary attribute or picture to a Profile screen

1. [Modify the profile screen definition](#) (see page 72).
2. Select the field below the row where you want to add the picture and click the Add button to add one row with one field above the row you selected.
Identity Manager adds a new field above the field you selected.
3. Click the right arrow icon to edit the new field.
The Field Properties dialog opens.
4. Select the (Separator) attribute in the Attribute Name field.
5. Select one of the following options in the Style field:
 - Binary
 - Picture

Identity Manager displays new configuration fields in the Field Properties dialog.

6. Complete the following fields as needed:

- **Name**

The label you want for this attribute in the task.

- **Permission**

The privilege level for the field.

Note: If a field is required by the user store, choose a Required setting. Required fields are indicated by a yellow dot in the screen.

- **Read**

An administrator can view but not modify the field.

- **Read/Write**

An administrator can see the current value of the field (if one exists), and can enter a value for the field.

- **Read/Write Required**

A required field, but otherwise functions as the Read/Write setting.

- **Write**

An administrator cannot see the current value of the field (if there is one), but can enter a value.

For example, an administrator can change a user's password, but cannot view the user's current password.

- **Write Required**

A required field, but otherwise functions as the Write setting.

- **Label span**

The number of columns that the label will span.

- **Field span**

The number of columns that the field will span (excluding the label)

- **CSS Class**

The Cascading Style Sheet class that controls the presentation of this field.

Note: This field is available for picture attributes only.

- **CSS Style**

Field properties and style defined using HTML property tags.

You can use this field to set the width of a field. For example, to set the width of the field where the picture will display to 300 pixels, you specify the following in the CSS Style field:



Note: This field is available for picture attributes only.

- **Binary Attribute Name**

Specifies the name of the attribute that stores the image. This attribute must exist in the user store, but should not be defined in the directory configuration file (directory.xml).

- **Content Type**

Specifies the type of image that will be displayed. For example, for a binary file, you may specify application/octet-stream. For a picture, you may specify image/gif or image/jpg.

- **Alternate Content**

Specifies the URI of an alternate image that Identity Manager displays when an image is not available for a certain user.

Identity Manager includes a default image that is displayed when another image is not available; however, you can use this field to override the default image.

The default image is located in

IdentityMinder.ear\user_console.war\ui\images\user_photo_default.jpg

IdentityMinder.ear is the deployed location of Identity Manager on the application server.

Specify the path to alternate image, which has the same content type as the attribute, relative to user_console.war.

Note: This field is only available when you select the Picture style.

7. Click Apply, then click OK to save changes.

Add Page Sections

Page sections allow you to visually separate a set of fields within a profile screen by adding a header and applying a different number of columns to part of a profile screen. The page section layout applies until another page section is defined for the profile screen.

The following sample profile tab shows two page sections.

Create Contractor:

The screenshot shows a profile screen for 'Create Contractor' with the following layout:

- Tabs:** Profile (selected), Access Roles, Admin Roles, Groups, Delegate Workitems, Schedule.
- Page Section 1:**
 - Organization (dropdown menu)
 - User ID (text field)
 - First Name (text field)
 - Last Name (text field)
 - Full Name (text field)
- Page Section 2 (Contractor Information):**
 - Employee Type (text field)
 - Employee Number (text field)
 - Title (text field)
 - Office (text field)
 - Department (text field)
 - Manager (text field)

To add a page section

1. [Modify the profile screen definition](#) (see page 72).
2. Select the first field that will appear in the page section you are creating and add one row with one field before the checked field.

Identity Manager adds a new field above the field you selected. This field will indicate where the page section starts.

3. Click the right arrow icon to edit the new field.

The Field Properties dialog opens.

4. Select the (Separator) attribute in the Attribute Name field.
5. Select Page Section in the Style field.

Identity Manager adds additional fields to the Field Properties dialog.

6. Specify values for the following fields:

- **Columns for Layout**

Specifies the number of columns that the page section will contain.

After specifying the number of columns, click the right arrow icon to apply the changes. Once the changes are applied, additional fields appear that enable you to specify the width of each column.

Note: Each field includes two columns: one column for the field label, and one column for field values. To display two fields on a single row, add four columns.

- **Table Header**

Specifies the text that appears above the page section as a heading.

- **Enable Hide/Show Buttons**

Determines whether users can choose to hide a page section. When this option is selected, Identity Manager adds an arrow icon in the table header that allows them to show or hide the page section.

- **Hide Initially**

Specifies that a page section is hidden by default.

If users should be able to use the page section, be sure to select the Enable Hide/Show Buttons option when you select the Hide Initially option to allow users to show the page section.

- **Specify Column Widths**

Determines the width of each column in the page section. Each column width is specified as a percentage of the profile screen.

For example, to add four columns of equal width, you would specify each column width as 25%.

Note: The total width of columns must be 100%.

7. Click OK to save the changes to the field properties.

8. Click Select to choose the screen definition that you edited or copied.

9. Click OK, then click Submit to save changes to the task.

Add a Nested Task

A nested task is an admin task that can be opened from the Profile tab of another task. Users of the first task open the nested task by clicking a link or button. For example, you can add a Delete User button to the Modify User task. If the user account is no longer valid, an administrator can click the Delete User button to remove the account without having to return to the navigation pane to select a new task.

Note: The nested task does not appear if the administrator does not have adequate privileges to access it.

To add a nested task

1. [Modify the profile screen definition](#) (see page 72).
2. Select the field below the row where you want to add the nested task and click the Add button to add one row with one field above the row you selected.

Identity Manager adds a new field above the field you selected.

3. Click the right arrow icon to edit the new field.

The Field Properties dialog opens.

4. Select the (Separator) attribute in the Attribute Name field.
5. Select Task in the Style field.

Identity Manager displays new configuration fields in the Field Properties dialog.

6. Complete the following fields as needed:

- **Field Span**

The number of columns that the field will span (excluding the label)

- **Default Task**

Specifies the task that is added to the existing task.

- **Override Task Name**

Specifies the name of the task link or button that will appear in the Profile screen for the active task.

- **Task link**

Determines whether the nested task appears as a link or a button.

- **Use current object as task subject**

When this option is selected, Identity Manager uses the subject of the active task as the subject of the nested task. For example, suppose the Modify User task includes a link to the Delete User task. An administrator uses the Modify User task to modify John Smith's profile. The administrator decides that John Smith's profile is no longer necessary, so she uses the Delete User link to open the Delete User task. When the task opens, Identity Manager asks the administrator if she wants to delete John Smith's profile. She does not need to search for the profile to delete.

- **Task Behavior**

Determines how Identity Manager opens the nested task.

- **Replace active task**

Opens the nested task before the active task completes. The nested task replaces the previous task. When the nested task completes, users are not returned to the original task.

- **Nest task within active task**

Opens the nested task before the active task completes. When users complete the nested task, they are returned to the original task.

- **Nest task within active task and execute when only after the active task completes**

Opens the nested task after the original task completes. This is called a post-task.

Add Help Text to Profile Screens

You can add text anywhere in a profile screen to provide additional information, such as help text for a field, to users.

To add help text to a profile screen

1. [Modify the profile screen definition](#) (see page 72).
2. Select the field below the row where you want to add the picture and click the Add button to add one row with one field above the row you selected.
Identity Manager adds a new field above the field you selected.
3. Click the right arrow icon to edit the new field.
The Field Properties dialog opens.
4. Select the (Separator) attribute in the Attribute Name field.
5. Select HTML in the Style field.
The HTML field appears.

6. Enter the text that you want to appear in HTML tags, for example:
`<h1>Add your help text here</h1>`
7. Click OK.

List Screens

In configuring tabs, you often need to show a list of items, such as a list of users or roles. The list appears on the tab that you are configuring. In these situations, create a List Screen to control the columns and sorting of the objects on the tab.

You can configure the following fields for a List Screen:

Name

Defines the name of the task.

Tag

Defines a unique identifier for the task. It is used in URLs, web services or properties files. It must consist of letters, numbers, or underscores, beginning with a letter or underscore.

Field

Specifies the attributes that appear as fields in the search results.

Name

Specifies the label for the field in the search results.

Style

Determines the format of the field in the search results.

Boolean Display Name

Displays the name of the field for all results that are true. For example, if you enter Enabled as the name of the attribute that indicates a user's account status, "Enabled" would appear in the search results for all active user accounts.

Checkmark

Displays the value as a selected or deselected checkmark based on the value of the attribute. For example, if you select the checkmark style to represent the Enabled/Disabled state of user accounts, Identity Manager displays a selected checkmark for all active accounts.

Multi-Value String

Displays the values in a multi-value attribute on separate lines. The values are listed alphabetically.

Read-Only Checkbox

Displays the value as a read only checkbox.

String

Displays the value as a text string.

Task

Adds a task list to a field. Users click a right arrow icon to see a list of tasks that they can perform on the object associated with the search field. For example, if you add a task list to a Last Name field in the search results, users can click on the arrow icon in that field to see a list of tasks they can perform on the user they select.

Sortable

Determines whether users can sort search results based on the selected field.

Descending

Determines the order in which search results are displayed. When the Descending checkbox is selected, the search results are sorted alphabetically in descending order. The results are sorted in the order in which they appear in the list.

Results per page

Indicates the number of search results to display in the search results.

Enter HTML to appear before the list

Specifies text that appears above the list of search results.

Enter HTML to appear after the list

Specifies text that appears below the list of search results.

You can also add text above and below a list screen.

Once you create the tabs for the task, you can check what fields are used in this task. See the next section, [View Fields in the Task](#) (see page 116).

Add a Task List

A task list is a menu of tasks that you access from a list of objects, such as a list or search results screen. Task lists allow you to view and use all of the tasks that apply to an object without having to search for that object each time you use a new task. For example, you can configure Identity Manager to display a task menu for each role member listed on the Membership tab of the Modify Admin Role Members task. Administrators can use the task menus to manage role members without having to perform a new search for each role member.

To add a task list

1. Complete *one* of the following steps:
 - Select Modify Admin Task from Roles and Tasks, Admin Tasks. Search for and select the admin task to modify.
 - Select Create Admin Task from Roles and Tasks, Admin Tasks. Then, select Create a copy of an Admin Task and search for a task to copy.

Identity Manager displays the tabs to configure for the task you selected.

2. Select the tab where you want to add the task list.

Typically, this will be a tab that includes a search or list screen, such as the Membership tab.

3. Edit the list or search screen by clicking the ellipses (...) button.
4. Select the field that will include a task list from the list of fields that appear in search results.
5. Select Task in the Style field.
6. Click the right arrow icon to open a Field Properties section where you can configure the task list.
7. Complete the following fields as needed:

- **Default Task**

Specifies the task that opens when a user clicks a value in the field. When you configure a field to support task lists, and specify a default task, the field value appears in blue text, indicating that it is a link.

For example, if you configure the Last Name field to include a task list, an administrator can click a user's last name to open the default task.

- **Alternate Task**

Specifies the task that opens when a user clicks the field value and does not have privileges to use the default task.

- **Enable popup task menu**

Displays a right arrow icon next to the field. Users click the icon to view the list of tasks they can perform on that object in that field.

When you select this checkbox, the following options appear:

- **Include all tasks that the administrator can perform on the object**
- **Include all tasks that the administrator can perform on the object unless hidden in menus**

- **Include only the specified tasks**

Displays only tasks that you select in the Task field.

Note: Users will not see a specified task if they do not have privileges to use it.

- **Exclude the specified tasks**

Displays all of the tasks that an administrator can perform on the object *except* tasks listed in the Task field.

- **Task**

Specifies the tasks that appear or do not appear in a task list, depending on whether the Include Only Specified Tasks or Exclude the Specified Tasks checkbox is selected.

- **Nest Task**

When checked, specifies that Identity Manager should open the task as a nested task. When a user completes the nested task, he is returned to the original task.

If this option is not selected, the new task replaces the original task.

8. Click OK.

Account Tabs

The Accounts tab lists accounts in managed endpoints for users who have been assigned provisioning roles. Typically, this tab is added to tasks that allow you to view or modify a user.

View User: *ken.davis*

Profile
Admin Roles
Provisioning Roles
Accounts

Search for an Account of Endpoint Type Windows NT

where + Name = * - + Search Clear

☐ Select	▲ Name	Endpoint Type	Endpoint	EndPoint Description	Container	Suspended	Locked
☐	ken.davis	Windows NT	aj-joy-vm.ca.com	Windows NT Endpoint.	aj-joy-vm.ca.com	Active	Unlocked
☐	ken.davis	Windows NT	iam-fw-wl9	test	iam-fw-wl9	Active	Unlocked

When the Accounts tab is added to a Modify User task, administrators can perform other actions on the user's accounts. For example:

- Suspend or resume an account
- Unlock an account that has been automatically locked because of incorrect or inappropriate access. For example, an account may be locked when a user exceeds the acceptable number of failed login attempts set in an Identity Manager password policy.
- Change the user's password in one or more accounts.
- Assign and unassign accounts to a user.

For details on the other options you can provide on the Accounts tab, see the user console help for the Configure Accounts tab.

Prerequisite for Using the Accounts Tab

To use the Accounts tab, Identity Manager must be configured with provisioning support, and the Identity Manager environment must include a provisioning directory.

Note: To configure provisioning support for an environment, see the *Configuration Guide*.

Fields on the Accounts Tab

The Accounts tab displays details about the accounts the user has on endpoint systems.

The following are some of the more significant fields:

- Account Name--The login name, email name, or other name for the account.
- Endpoint Type--The type of endpoint, such as an LDAP directory, that is associated with the account.
- Container--The LDAP container, if one is used, where the account exists. For example, the container ou=People indicates the account exists in the People container.
- Endpoint--The specific endpoint that is associated with account.
- Source--Description of how the account was created: either the user received a provisioning role or the account was created in the Provisioning Server.

Note: This attribute may take significant time to display. You can configure the Accounts tab to remove this field if it is not required. See the online help for the Configure Accounts page for instructions on adding or removing fields on this tab.

- **Suspended Status**--Indicates whether an administrator has enabled or disabled the account.
- **Locked Status**--Shows if the account is locked. Locking occurs automatically when a user makes several attempts to log into the account with the wrong password.

Additional Functions on the Accounts Tab

When the Accounts tab is included in a task that modifies a user, administrators can use that task can perform functions on the user's accounts. The available functions are determined by the tab configuration.

You can select which functions are available by using the Modify Admin Task on a user task, such as Modify User. You edit the Accounts tab to determine if functions such as Assign Account and Unassign Account are available in the task you are modifying.

See the online help for the Configure Accounts tab for more information.

Schedule Tab

Scheduling lets you automate the execution of a task at a later date. If you schedule a task that is associated with a workflow, Identity Manager executes all the tasks as defined in that workflow. The status of the scheduled tasks can be viewed in the View Submitted Tasks page.

A scheduled task that is not yet executed by Identity Manager can be rescheduled or cancelled through the View Submitted Tasks page.

Identity Manager provides the scheduler as a special tab. To access the scheduler, you must configure a task with the Schedule tab.

Add the Schedule Tab to an Admin Task

Identity Manager lets you schedule your tasks for execution at a specific date and time. To schedule a task, you must add the Schedule tab to an admin task.

Note: You cannot add a Schedule tab to all the admin tasks in Identity Manager. If the task cannot be scheduled, the schedule tab will not be available in the Modify Admin Task screen.

To add the Schedule tab to an admin task

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.
The Select Admin Task page appears.
2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Search.
Identity Manager displays the admin tasks that satisfy the search criteria.
3. Select an admin task, and click Select.
Identity Manager displays the task details for the selected admin task.
4. Click Tabs.
The tabs that are configured for the selected admin task are displayed.
5. Select Schedule from the Which tabs should appear in this task drop down, and click .
The Schedule tab is added to the list of tabs that will appear in the selected admin task.
6. Click Submit.
The Schedule tab is added to the selected admin task.

Object-Task Navigation

Object-task navigation is a method that allows users to select an object 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.

For example, to modify a user using this method, you select the Users category, then select the Manage Users task. You search for and select the user that you want to manage. In the search results, you click an icon to see a list of tasks that you can use to manage the selected user. From that list, you can select Modify User or any other appropriate task.

Identity Manager includes the following default admin tasks that are configured for object-task navigation:

- Manage Users
- Manage Groups
- Manage Organizations
- Manage Access Roles/ Manage Access Tasks
- Manage Admin Roles / Manage Admin Tasks
- Manage Provisioning Roles / Manage Provisioning Tasks

You can also add pop-up task menus to list and search results screens to enable object-task navigation in existing tasks. For example, you can add object-task navigation to the Modify Admin Role Members task to display a pop-up task menu for each role member. Administrators can use the task menus to manage role members without having to perform a new search for each role member.

Configure Object-Task Navigation

Tasks that are configured for object-task navigation include a search screen only. Users search for an object to manage, and then use pop-up task menus to view all of the tasks that they can perform on that object.

When you configure object-task navigation, note the following:

- The action for the admin task on the Profile tab must be Search.
- The admin task cannot contain tabs.
- If you want to configure all admin tasks to use object-task navigation, you may want to create nested tasks for creating objects and for deleting multiple objects. These actions are not supported in the object-task navigation model.

To configure object-task navigation

1. Complete *one* of the following steps:

- Select Modify Admin Task from Roles and Tasks, Admin Tasks. Search for and select the admin task to modify.
- Select Create Admin Task from Roles and Tasks, Admin Tasks. Then, select Create a copy of an Admin Task and search for a task to copy.

Note: To simplify configuration, consider creating a copy of an existing Manage task, such as Manage User. The default Manage tasks include the configuration settings required for object-task navigation.

Identity Manager displays the tabs to configure for the task you selected.

2. Configure the settings for the Profile tab as needed. Set the Action for the task to Search.
3. Select the Search tab and click the ellipses (...) button next to the Search Screen field to configure the search screen for the task.

Identity Manager displays a list of search screen definitions that you can apply to this task.

4. Select the search screen definition that you need.

Note: To simplify configuration, consider creating a copy of an existing Manage search screen definition, such as Manage Users Search. The default Manage search screens are configured to support object-task navigation.

5. Complete the fields in the search screen configuration screen as needed.

Note: If your environment does not include separate tasks for creating a new object or deleting multiple objects from a single screen, which are accessible from the main task navigation, you can add links to those tasks from the task you are creating. Specify the task in the Add Task Button or Add Multi-Delete Button fields and optionally specify a label for those tasks.

Define the Task Scope

On the Search tab, you define the task scope, which limits the objects available to the task. For example, if the object of a task is users, you might define the scope as users who are contractors.

Note: If the task has no primary object, or if the action is self-modify, self-view, or approve, the Search tab does not appear.

You configure the following settings on the Search tab:

Search Screen

The search screen limits the scope of the task based on filters. Click the ... (ellipses) button to see available search screen options.

Note: You may want to create [your own search screen](#) (see page 109). To create a modified version of an existing search screen, select the search screen and click Copy. You can then modify the search screen without changing the original search screen definition. To create a new search screen, click New.

Search Options

The search options appear only when the object is a role or group.

- The first option limits the search based on fields that are defined on the search screen. Within these limits, the search locates all groups or roles in the administrator's scope.
- Other options limit the search as indicated.

Note the following:

- By default, the group search screens support filtering. This means that administrators can specify criteria to limit the scope of group searches. To remove the filtering capability, create a new search screen that does not contain any fields to include in a search query.
- *Filtering not supported*, which appears on the Search tab when the object is a role, means that the task displays all of the roles that meet the criteria in the option you select. Search fields that are configured on the search screen are ignored.

Modified objects must remain in administrator's scope

When this check box is selected, Identity Manager displays an error if changes to the task cause the administrator to lose scope over the primary object. For example, an administrator may use Modify User to change a user's Employee Type attribute to Manager. This change may put the user outside the administrator's scope.

Search Screen Configuration

You configure a search screen to limit the scope of the task and control the fields that users can search on. Search screens apply to two types of objects:

- A *primary object* -- The object to be modified or viewed by the task.
- A *secondary object* -- The object that is used by the primary object.

For example, if you include a group tab on a create user task, the user is the primary object and the group is the secondary object. The group tab needs a search screen for groups.

Note: After configuring a search screen, you can use it for any task to search for a primary or secondary object.

Search Filters

Search filters limit which objects are found by the search. For example, if the object is users, you might limit the search to find only contractors. You can configure a filter to find users with the Employee Type of Contractor.

You can configure the following fields for searches:

Show only objects meeting the following rules

Defines additional criteria to be combined with the configured filter to constrain the search.

Note: Due to limitations with provisioning roles searches, these criteria will overwrite filter fields with the same name configured in the search.

Default search filter

Defines a filter that appears when an administrator uses the search screen. For example, if you are configuring a search screen for the Modify Contractor task and you know that administrators typically search for contractors based on the contract firm's name, you can set the default filter to Contract Firm = *. Administrators can override the default filter by specifying different search criteria. Setting a default filter improves performance by limiting the number of results returned if an administrator does not specify a filter before beginning a search.

Auto select all search results when used with multi-select tasks

Specifies that all search results are selected by default. If you check this box, all of the objects in the search results list will appear with a checked box next to the object name.

Automatically perform search

Specifies that a search criteria box will be displayed along with the search results.

Automatically set subject of task when there is only a single search result

Sets the primary object of the task automatically when only one object matches the search filter.

For example, suppose that this option is selected for a user search screen which is associated with the Modify User task. When an administrator opens the Modify User task and enters a search filter that returns only one user, Identity Manager opens the Modify User task for that user. The administrator does not have to select the user to open the Modify User task.

Save search filter

Specifies that the search filter for the task will be saved. The next time a user searches in the task, the saved search filter will be displayed.

Search in organization

Displays an organization filter on the search screen. If this checkbox is selected, administrators can specify a filter that limits the organizations in which Identity Manager searches for an object. You can specify defaults for the organization search filter by specifying a search screen definition in the Organization Search field.

Save search organization

Specifies that the organization for the task will be saved if an organization was established for the search. The next time a user searches in the task, the organization will be displayed.

Single expression search

Defines the type of search filter that appears on the search screen. When you select this checkbox, users can specify a single search filter, such as <attribute><comparator><value>. When you clear this checkbox, users can specify multiple search filters. For example, <attribute1><comparator><value1> AND <attribute2><comparator><value2>. Objects that meet the conditions in all of the filters are returned in the search results. In the previous example, objects that include <value1> and <value2> would be returned as search results.

Display the number of results

Displays the number of matching search results. If this checkbox is selected, all searches will return the message, "There are X number of results".

Add task button for <task name>

Adds a link to another task to the search screen. The link is displayed as a button.

This field is typically used to add a Create task to a search screen that is configured for object-task navigation.

Optional label

Specifies a label for the task that you selected in the previous field. This label appears on the button for the task.

Add multi-delete button for <task name>

Adds a link to a task that allows administrators to select multiple objects to delete. The link is displayed as a button.

This field is typically with object-task navigation.

Search Fields and Search Results

On another part of the search screen, you select fields that an administrator can use in a search query and fields to display in search results.

Select the fields that a user can search on

Select the fields that an administrator can use to create a search query.

To add additional fields, select the fields in the list box below the search fields table, and click the plus (+) icon.

After selecting the fields, you can change the order in which they appear by using the up and down arrow icons to the right of the field.

Note: If you do not specify fields that an administrator can search on, Identity Manager starts the search automatically.

Select the fields that appear in the search results

Select the fields that Identity Manager displays in the search results. You can select fields that are not available in the search query.

To add additional fields, select the fields in the list box below the search fields table, and click the plus (+) icon.

Style

When you select a field to display in the search results, you can select one of the following style options:

- **Boolean Display Name**

Displays the name of the field for all results that are true. For example, if you enter Enabled as the name of the attribute that indicates a user's account status, "Enabled" would appear in the search results for all active user accounts.

- **Checkmark**

Displays the value as a selected or deselected checkmark based on the value of the attribute. For example, if you select the checkmark style to represent the Enabled/Disabled state of user accounts, IdentityMinder displays a selected checkmark for all active accounts.

- **Multi-Value String**

Displays the values in a multi-value attribute on separate lines. The values are listed alphabetically.

- **Read-Only Checkbox**

Displays the value as a read only checkbox.

- **String**

Displays the value as a text string.

- **Task**

Adds a task list to a field. Users click a right arrow icon to see a list of tasks that they can perform on the object associated with the search field. For example, if you add a task list to a Last Name field in the search results, users can click on the arrow icon in that field to see a list of tasks they can perform on the user they select.

If you select the Task style, a right arrow icon appears next to the Style column. Click the arrow to open a Field Properties dialog. Use this dialog to configure a [task list](#) (see page 100).

Sortable

Select this checkbox to allow administrators to sort search results by a field or fields.

Set the default sort order for the search results

Specifies the order in which search results are displayed. Search results are sorted initially by the first field in the list and then by each additional field in the order in which they appear. Select the Descending checkbox to sort the results in descending order.

Select objects with changes to field *field name*

Specifies that only objects that have changed field names will be used.

Return *N* results per page

Select the number of results to display per page. When search results exceed the number you specify, Identity Manager displays a link to each page of results.

User-Defined Help on Search Screens

If you want to add custom text to your search screen, you can define text in the corresponding HTML text box. You can add text in the following areas:

- Beginning or end of the page
- Before or after the create
- Before or after the results

Types of Search Screens

Identity Manager includes these pre-configured search screens.

Access Role Search Screen

The Access Role Search Screen lets you configure search filters to find access roles that match specific criteria.

Access Task Search Screen

The Access Task Search Screen lets you configure search filters to find access tasks that match specific criteria. This search screen is used to find an access task to view or modify, or to add a task to an access role.

Admin Role Search Screen

The Admin Role Search Screen lets you configure search filters to find admin roles that match specific criteria.

Admin Task Search Screen

The Admin Task Search Screen lets you configure search filters to find admin tasks that match specific criteria. This search screen is used to find an admin task to view or modify, or to add a task to an admin role.

Approval Search Screen

The Approval Search Screen lets you configure the display that appears at the top of an approval task.

Begin Certification User Search Screen

The Begin Certification User Search Screen lets you configure search filters to find users to set to require certification. Users selected will have their certification status set to *requiring certification*.

Certify User Search Screen

The Certify User Search Screen lets you configure the search filters to find users who require certification.

Delegation Search Screen

The Delegation Search Screen lets you configure search filters to find additional users to add as delegates. A delegate is another user that you can temporarily grant permission to view and resolve your workflow work items.

Enable/Disable User Search Screen

The Enable/Disable User Search Screen lets you configure search filters to enable/disable users who match specific criteria.

EndCertification User Search Screen

The EndCertification User Search Screen lets you configure search filters to identify users whose certification cycle should be completed.

End User License Agreement Search Screen

The End User License Agreement Search Screen lets you configure the Self Registration task with a page that is specific to your identity-based application.

Explore and Correlate Search

The Explore and Correlate Search Screen lets you configure search filters for explore and correlate definitions that match specific criteria.

Feeder File Upload Search

The Feeder File Upload Search Screen lets you browse for the feeder file to upload. A feeder file is used to automate repeated actions performed on large number of managed objects.

Forgotten Password Search Screen/Forgotten User ID Search Screen

The Forgotten Password Search Screen lets you configure the Forgotten Password task to prompt users for information that verifies their identity.

Group Search Screen

The Group Search Screen lets you configure search filters for groups, such as groups within the finance organization.

Identity Policy Set Search Screen

The Identity Policy Set Search Screen lets you configure search filters to find identity policy sets that match specific criteria.

Logical Attribute Handler Search Screen

The Logical Attribute Handler Search Screen lets you configure search filters to find logical attribute handlers. This search screen is used to find a logical attribute handler to view or modify its configuration.

Manage Reports Search Screen

The Manage Reports Search Screen lets you configure search filters to find a report to view or delete.

NonCertified User Search Screen

The NonCertified User Search Screen lets you configure search filters to find users who were not certified by the end of the certification period.

Organization Search Screen

The Organization search screen lets you configure search filters to limit the choice of organizations to certain sub-organizations.

Provisioning Role Search Screen

The Provisioning Role Search Screen lets you configure the search filters for retrieving provisioning roles.

Account Template Search Screen

The Account Template Search Screen lets you configure the search filters for retrieving account templates.

Password Policy Search Screen

The Password Policy Search Screen lets you configure the search filters to find password policies that match specific criteria.

Snapshot Definition Search Screen

The Snapshot Definition Search Screen lets you configure the search filters to find a snapshot definition to view, modify, or delete.

Standard Search Screen

The Standard Search Screen lets you configure filters to find custom managed objects.

User Search Screen

The User search screen lets you configure search filters to find users that match specific criteria. For example, you can search for users who are contractors.

Once you complete the Scope tab, Choose Tabs for the Task.

View Fields in the Task

On the Fields tab, you view the fields that apply to this task. These fields are those created on the tabs for this task. To change the fields used, return to the Tabs tab and select the tab that requires the change.

Once you complete this tab, proceed to the next step, [Assign Workflow Processes for Events](#) (see page 116).

However, if this Identity Manager environment does not use workflow, you can now click Submit. A message appears indicating if the task succeeded. If it succeeds, you can add the task to a role, so that role members can start using the task.

Assign Workflow Processes for Events

If you enabled workflow for this Identity Manager environment, use the Events tab to select a workflow process for each event that the task initiates. The workflow process that you select overrides the one selected by default in the Identity Manager Management Console.

For more detail on default workflow mappings, see the Advanced Settings chapter of the *Configuration Guide*.

To complete the creation of this task, click Submit. A message appears indicating if the task succeeded. If it succeeds, you can add the task to a role, so that role members can start using the task.

Active Directory Prerequisites

If Active Directory is the user store, before creating admin tasks, you may need to configure certain Active Directory features.

The sAMAccountName Attribute

The sAMAccountName attribute applies to users and groups. This attribute is required, and must be included on task screens used to create users and groups.

Note: When creating users, the value of the sAMAccountName attribute cannot exceed 20 characters. This restriction does not apply to groups.

You can write a custom logical attribute handler that generates a unique sAMAccountName automatically when a user or group is created. In this case, you can include the sAMAccountName attribute as a hidden field on Create User and Create Group screens.

See the Logical Attributes chapter in the *Programming Guide for Java* for more information.

Group Type and Scope

In Active Directory, there are two types of groups:

- Security--Listed in Access Control Lists (ACLs), which define permissions for resources and objects.
- Distribution--Used to group objects, such as users and groups. Distribution groups cannot be used to grant privileges in Active Directory.

Each type of group has a scope that determines the following:

- Member location--Where potential members can reside
- Permissions--Where the group can be used for access privileges (if the group is a security group)
- Group Membership in Other Groups--The location of groups to which the group can belong

Each type of group can have one of the following scopes:

Scope	Member Location	Permissions	Group Membership in Other Groups
Universal	Group members can be Universal groups, Global groups, and users from any domain in the forest.	Can be used to grant access in any domain in a forest.	Can be members of Domain Local and Universal groups in any domain in the forest.
Global	Group members can be Global groups and users located in the same domain as the group.	Can be used to grant access in any domain in a forest.	Can be members of Global, Domain Local, and Universal groups in any domain in the forest.

Scope	Member Location	Permissions	Group Membership in Other Groups
Domain Local	Group members can be Universal groups, Global groups, and users from any domain in the forest. Members can also be Domain Local groups from the same domain.	Can only be used to grant access to the domain where the group resides.	Can only be a member of other Domain Local groups within the domain.

Group type and scope are not required attributes; however, if you do not specify group type and scope, Active Directory creates a security group with global scope.

To create groups of a different type, you can create a custom logical attribute handler. See the chapter on Logical Attributes in the *Programming Guide for Java*.

Once you have configured these Active Directory features, proceed to the next step: Create an Admin Task.

External Tasks for Application Functions

An external task:

- Allows an administrator to perform a function in an application other than Identity Manager from the Identity Manager User Console
- Optionally passes information to the application to generate user-, group-, 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.

Two tabs are available for External tasks. These tabs are configured in the same way; however, they function differently.

- The External tab is a visual tab, which means that the task displays the contents of the URL within a tab.
- External URL is a non-visual tab, which means that the task redirects to the URL entered.

The External Tab

An external tab can be added to any Create, View, or Modify task to make it an external task. For example, if you add an External tab to a Create User task, the tab appears on that task.

For an External tab:

- No events are generated for an external task.
- You can optionally use managed objects.
- In the External URL field, you can specify the address of the application as:
 - A complete address, including the fully qualified domain name--for example:
`http://server1.mycompany.org/report/viewUserReport`
 - A relative path--for example:
`/report/viewUserReport`
If you specify the relative path, Identity Manager automatically appends the fully qualified domain name of the server where Identity Manager is installed.
- You configure the attributes to pass to the application on the Profile tab.

The External URL Tab

You can add an external URL tab to a view task, such as View User. When you use the View User task, you are redirected to the web site identified by the URL. No other tabs are visible.

For an External URL tab:

- The external URL tab must be the only tab in the task. If there are other tabs associated with the same task, the external tab will not redirect users to the specified URL.
- The task can generate events which can be audited.

- In the External URL field, you can specify the address of the application as:
 - A complete address, including the fully qualified domain name--for example:
`http://server1.mycompany.org/report/viewUserReport`
 - A relative path--for example:
`/report/viewUserReport`
If you specify the relative path, Identity Manager automatically appends the fully qualified domain name of the server where Identity Manager is installed.
- You can optionally use managed objects.
- You can configure attributes to pass to the URL.
Supply a URL for the application that you want to start and include the attributes that you want to pass to the application.

Advanced Task Components

Advanced task components allow you to specify custom processing for a task:

- [Task-Level Validation](#) (see page 121) validates an attribute value against other attributes in the task. For example, you might validate that the area code in a user-supplied phone number is appropriate for the user's city and state.
- [Business Logic Task Handlers](#) (see page 122) perform custom business logic before an Identity Manager task is submitted for processing. Typically, the custom business logic validates data. For example, a business logic task handler may check a group's membership limit before Identity Manager adds a new member to the group. If the group membership limit is reached, the business logic task handler displays a message informing the group administrator that the new member could not be added.

Configure Task-Level Validation

You configure task-level validation in the Identity Manager User Console, when defining field properties on a profile task screen.

1. On the profile screen, select the field to be validated and click Field properties.

You define a Profile screen as part of defining tabs for the task.

2. Specify a value in one of the following fields, depending on how the validation rule is to be implemented:
 - Validation Expression--Contains a regular expression that performs the validation.
 - Validation Java Class--Contains the fully qualified name of a Java class that performs the validation--for example:
`com.mycompany.MyJavaValidator`
Identity Manager expects the class file to be located in the root directory designated for custom Java class files. For information on deploying Java class files, see the *Programming Guide for Java*.
 - Validation JavaScript--Contains the complete JavaScript code that performs the validation.

JavaScript code must be provided in this field. With task-level validation, you cannot reference a file containing JavaScript code.

3. Enable Validate On Change, so that the field validation occurs as soon as it is changed.
4. (Optional) For a user, group, or organization, you can use a Validate button on the profile tab. The Validate button is hidden by default. To make this button visible, clear the Hide Validate button option when you configure the task's profile tab.

If Validate On Change is enabled on a field and the value of that field changes, the Validate button updates other fields on the screen.

Note: The Validate button also executes Logical Attribute Handlers that include the validate method. For more information about Logical Attribute Handlers, see the *Programming Guide for Java*.

Directory-Level Validation validates fields based on the content of the `directory.xml` file. For more information on Directory-Level Validation or understanding the default validation included with Identity Manager, see the *Configuration Guide*.

Create Business Logic Task Handlers

You define a business logic task handler's fully qualified class name as follows:

1. Create or modify an admin task.
2. On the Admin Profile tab, click Business Logic Task Handlers.

The Business Logic Task Handlers screen appears. This screen lists any existing business logic task handlers assigned to the task. Identity Manager executes the handlers in the order in which they appear in the list.

3. Click Add.

The Business Logic Task Handler Detail screen appears.

Use the Business Logic Task Handler Detail screen to define the following information for the business logic task handler you are assigning to the task:

Name

The name you are assigning to the business logic task handler.

Description

An optional description of the business logic task handler.

Java Class

If the business logic task handler is implemented in Java, the fully qualified business logic task handler class name--for example:

`com.mycompany.MyJavaBLTH`

Identity Manager expects the class file to be located in the root directory designated for custom Java class files. For information on deploying Java class files, see the *Programming Guide for Java*.

JavaScript Filename

If the business logic task handler is implemented in JavaScript, and the JavaScript code is contained in a file, specify the file name in this field. For example, you might want to put the JavaScript in a file if the business logic task handler is to be used by several task screens.

Identity Manager expects the file to be located in the root directory designated for custom JavaScript files. For information on deploying JavaScript files, see the *Programming Guide for Java*.

If you store the file in a subdirectory of the root, include the subdirectory name when you specify the JavaScript file name--for example:

`JavaScriptSubDir\MyJavaScriptBLTH.js`

The slashes must be appropriate for the platform where the JavaScript file is deployed.

JavaScript

You can implement a JavaScript business logic task handler by typing the complete JavaScript code in this field instead of in a file. For example, you might want to put the JavaScript in this field if the script is very short or if it is to be used with no other task screens.

Property and Value

With Java implementations, these fields are optional name/value pairs of data that are passed into the `init()` method of the Java business logic task handler, to be used in any way that the handler's business logic requires.

To add a user-defined property, specify a property name and value, and then click Add.

Note: If you add a Java business logic task handler, you restart the application server for the handler to be loaded.

Chapter 5: Access Roles

This section contains the following topics:

[Access Roles in Identity Manager](#) (see page 125)

[Create an Access Role](#) (see page 126)

Access Roles in Identity Manager

Access roles provide an additional way to provide entitlements in Identity Manager or another application. For example, you can use access roles to accomplish the following:

- Provide indirect access to a user attribute
- Create complex expressions
- Set an attribute in a user profile, which is used by another application to determine entitlements

Access roles are similar to identity policies in that they apply a set of business changes to a user or group of users. However, when you use an access role to apply business changes, you can see which users the changes apply to by viewing the members of the access role.

Access roles are not associated with tasks.

How Access Roles Manage Entitlements

You can use access roles to manage entitlements by specifying change actions, which occur when a user is added or removed as a member or administrator of a role.

To use access roles, you complete the following steps:

1. An administrator creates an access role.
2. On the Members tab, the administrator specifies add or remove actions, which determine the actions that Identity Manager takes when the access role is assigned to a user.
3. The administrator specifies administrator and owner policies, as needed, and submits the task to create the access role.
4. Access role administrators assign the access role to users.
5. Identity Manager completes the add actions specified in the role.

Example: Indirect Profile Attribute Modification

To indirectly change an attribute, you set the change actions for the access role. When an administrator assigns the role, the change action can make one or more changes to an attribute in the user's profile.

To use an access role to indirectly modify an attribute, do the following:

1. Create an access role.
2. On the Members tab, select the Administrators Can Add or Remove Members of this Role checkbox, and click the arrow icon.
Identity Manager displays additional Add Action and Remove Action fields.
3. In the Add Action or Remove Action fields, select an action from the list box.
Identity Manager displays additional fields based on the option you selected.
4. Configure the Add or Remove actions as needed.
5. Select the Administrator tab to specify the administrators who can add members to the access role you are creating.
6. Select the Owners tab to specify the administrators who can modify the access role definition.
7. Click Submit to complete the access role creation.
8. Assign the access role to users, as needed.

Create an Access Role

Creating an admin role involves these steps:

- [Begin Access Role Creation](#) (see page 126)
- [Define the Profile of an Access Role](#) (see page 127)
- [Define Member Policies for an Access Role](#) (see page 127)
- [Define Admin Policies for an Access Role](#) (see page 128)
- [Define Owner Rules for an Access Role](#) (see page 128)

Begin Access Role Creation

1. Log into an Identity Manager account with a role that includes a task for creating access roles.

For example, the first user of an Identity Manager environment has the System Manager role, which has the Create Admin Role task.

2. Click Access Roles, Create Access Role.
Choose the option to create a new role or a copy of role. If you select Copy, search for the role.
3. Continue with next section, Define the Profile of an Access Role.

Define the Profile of an Access Role

To define the profile of an access role

1. Enter a name, description, and complete any custom attributes defined for the role.
2. Select Enabled if you are ready to make the role available for use as soon as you create it.
3. Continue with the next section, [Define Member Policies for an Access Role](#) (see page 127).

More Information:

[Profile Tabs and Profile Screens](#) (see page 71)

Define Member Policies for an Access Role

On the Members tab:

1. Select Add to define the member policies.
2. (Optional) On the Member Policy page, optionally define a member rule for who should be able to use this role.

This automatically assigns the role to users who match the criteria in the member policy.
3. Verify that the Member Policy appears on the Members tab.

To edit a policy, click the arrow symbol on the left. To remove it, click the minus sign icon.
4. On the Members tab, enable the Administrators can add and remove members of this role check box.

Once you enable this feature, you define the Add Action and Remove Action. These actions define what happens when a user is added or removed as a member of the role.
5. Continue with the next section, [Define Admin Policies for an Access Role](#) (see page 128).

Define Admin Policies for an Access Role

On the Administrators tab:

1. If you want to make the Manage Administrators option available, enable the Administrators can add and remove administrators of this role check box.

Once you enable this feature, define the actions for when a user is added or removed as an administrator of the role.

2. On the Administrators tab, add admin policies that include admin and scope rules and administrator privileges. Each policy needs at least one privilege (Manage Members or Manage Administrators).

You can add several admin policies with different rules and different privileges for administrators who meet the rule.

3. To edit a policy, click the arrow symbol on the left. To remove it, click the minus sign icon.
4. Continue with the next section, [Define Owner Rules for an Access Role](#) (see page 128).

Define Owner Rules for an Access Role

On the Owners tab:

1. Define owner rules, which determine which users can modify the role.
2. Click Submit.

A message appears to indicate that the task has been submitted. A momentary delay may occur before a user can use the role.

Chapter 6: Identity Policies

This section contains the following topics:

[Identity Policies](#) (see page 129)

[Identity Policy Set Planning Worksheet](#) (see page 130)

[Create an Identity Policy Set](#) (see page 131)

[Manage an Identity Policy Set](#) (see page 140)

[How Users and Identity Policies Are Synchronized](#) (see page 141)

[Identity Policy Sets in an Identity Manager Environment](#) (see page 145)

Identity Policies

An Identity policy is a set of business changes that occurs when a user meets a certain condition or rule. You can use identity policy sets to:

- Automate certain identity management tasks, such as assigning roles and group membership, allocating resources, or modifying user profile attributes.
- Enforce segregation of duties. For example, you can create an identity policy set that prohibits members of the Check Signer role from having the Check Approver role, and restricts anyone in the company from writing a check over \$10,000.
- Enforce compliance. For example, you can audit users who have a certain title and make more than \$100,000.

Identity policies that enforce compliance are called *compliance policies*.

The business changes associated with an identity policy include:

- Assigning or revoking roles, including provisioning roles (if you are using a provisioning directory only)
- Assigning or revoking group membership
- Updating attributes in a user profile

For example, a company may create an identity policy which states that all Vice Presidents belong to the Country Club Member group and have the role Salary Approver. When a user's title changes to Vice President and that user is synchronized with the identity policy, Identity Manager adds the user to the appropriate group and role. When a Vice President is promoted to CEO, she no longer meets the condition in the Vice President identity policy so the changes applied by that policy are revoked, and new changes based on the CEO policy are applied.

The change actions that occur based on an identity policy contain events which can be placed under workflow-control and audited. In the previous example, the Salary Approver role grants significant privileges to its members. To protect the Salary Approver role, the company can create a workflow process that requires a set of approvals before the role is assigned, and they can configure Identity Manager to audit the role assignment.

To simplify identity policy management, Identity policies are grouped together in an identity policy set. For example, the Vice President and CEO policies may be part of the Executive Privileges identity policy set.

Identity Policy Set Planning Worksheet

An identity policy set contains one or more identity policies. Before you create an identity policy set, use the following worksheet to plan each identity policy in the set.

Question	Your Response
What name do you want to give the identity policy?	
Which users does the identity policy apply to?	
When an identity policy is applied to a user, what actions should Identity Manager perform?	
When an identity policy that once applied to a user no longer applies, what actions should Identity Manager perform?	
Should Identity Manager apply the changes in an identity policy multiple times or only the first time a user meets the conditions in the policy?	

After you complete this worksheet for each identity policy in a policy set, verify that the policies do not conflict with other policies. For example, make sure that a policy does not grant a privilege that another policy revokes.

Create an Identity Policy Set

To create an identity policy set, you must have the System Manager role, or a role that includes the Create Identity Policy Set task.

To create an identity policy set, complete the following steps:

1. [Define the Profile for the Identity Policy Set](#) (see page 131)
2. [Create an Identity Policy](#) (see page 131)
3. [Specify Owners for the Identity Policy Set](#) (see page 140)

Note: To use an identity policy set that you create, you must enable identity policies in the Identity Manager Management Console. See the *Configuration Guide* for more information.

Define the Profile for the Identity Policy Set

1. Select Policies, Create Identity Policy Set from the Identity Manager User Console.
2. Enter a name for the identity policy set.
3. Enter a category for the identity policy set.
The category groups identity policy sets with similar purposes for reporting. The Category field is required.
4. Optionally, enter a description for the identity policy set.
5. [Create an Identity Policy](#) (see page 131) in the identity policy set.

Create an Identity Policy

After you define the profile for the Identity Policy Set, you can define the identity policies in that policy set.

Note: In large implementations, it make take significant time to evaluate identity policy rules. To reduce the evaluation time for rules that include user-attributes, you can enable the in-memory evaluation option. For more information, see the *Configuration Guide*.

To create an identity policy

1. Select the Policies tab.
2. Enter a name for the identity policy.
3. Select the Apply Once check box if Identity Manager should apply the policy only when a user first meets the policy.

4. Select the Compliance check box to flag this policy as a compliance policy.
If this check box is selected:
 - Identity Manager can generate reports for users that are not synchronized with compliance policies.
 - The Compliance Violation action is visible in the Action on Apply/Remove Policy list box.
5. Identify the users to which the policy applies in the Policy Condition section.
6. In the Action on Apply Policy section, define the actions that Identity Manager takes when the identity policy is applied to a user.
7. In the Action on Remove Policy section, define the actions that Identity Manager takes when a user no longer meets the conditions for the identity policy.
8. Click OK.

Note: Before you can use the identity policy set that you created, you must enable identity policies in the Management Console. See the *Configuration Guide* for more information.

The Apply Once Setting

Identity Manager applies an identity policy differently, based on the Apply Once setting.

Enabling the Apply Once Setting

If the Apply Once setting is enabled, Identity Manager applies the changes associated with the identity policy when a user *first* meets the condition defined in the policy. The change actions associated with the policy occur only once. Therefore, Identity Manager does not apply policy updates to users, if the policy was previously applied.

When a user no longer meets the condition defined in the policy, Identity Manager executes the policy's remove actions.

The Apply Once setting is typically used when provisioning resources. For example, you may have a policy that assigns a cell phone to managers. When a user first becomes a manager, that user is assigned a cell phone. Identity Manager only issues the cell phone once, not each time the policy is evaluated. If the cell phone policy is updated to include a newer cell phone model, Identity Manager does not issue new cell phones to existing managers.

Note: Resource provisioning is available when Identity Manager integrates with a Provisioning Server.

Disabling the Apply Once Setting

If the Apply Once setting is not enabled, the change actions associated with the identity policy are applied each time an identity policy is evaluated. This means that Identity Manager applies change actions for every user who meets the condition in the policy, regardless of whether the change actions were applied previously.

Typically, you disable the Apply Once setting in an identity policy that enforces compliance. For example, you can create an identity policy that restricts managers' spending authority to \$5,000. If Identity Manager encounters a manager whose spending authority is set to \$10,000, it resets the spending authority to \$5,000. Each time a manager is synchronized with the identity policy, Identity Manager checks to make sure the spending authority is set correctly.

If a manual change that conflicts with a change action is made to a user profile, Identity Manager overwrites the change when the user is synchronized with the policy.

In the previous example, if someone manually increases a manager's spending authority to \$10,000, Identity Manager resets the spending authority to \$5,000 when the manager is synchronized with the policy.

The following table summarizes the effects of enabling or disabling the Apply Once setting.

If Apply Once is...	Then...
Enabled	■ Change Actions associated with the identity policy are applied only once ■ Manual changes made after the identity policy is applied are preserved ■ Updates are not applied to users who meet the condition in an identity policy, if Identity Manager applied the policy previously ■ When a user no longer meets the condition in an identity policy, Identity Manager executes the remove actions

If Apply Once is...	Then...
Disabled	■ Change actions associated with the identity policy are applied every time a user is synchronized with the policy ■ Manual changes are overwritten when the identity policy is applied ■ Updates to the policy are applied when a user is synchronized ■ When a user no longer meets the condition in an identity policy, Identity Manager executes the remove actions

Policy Conditions

Policy conditions are the rules that determine the set of users to which an identity policy applies.

The following table describes the available options.

Syntax	Condition	Example
(all)	The identity policy applies to all users.	
where <user-filter>	The user must match one or more attribute values.	Users where title=manager and locality=east

Syntax	Condition	Example
in <org-rule>	The user must belong to named organizations. Note: When you select this option, Identity Manager displays a new list box where you can select the following options: ■ organization <organization> [and lower]-- Use an organization search screen to select an organization and, optionally, include the organization's child organizations. ■ Organizations where <org-filter> [and lower]-- Specify a filter that selects one or more organizations.	Users in organization sales and lower
where <user-filter> and who are in <org-rule>	The user must match specific user attributes and belong to a specific organization.	title=manager and organization=Sales *
who are members of <group-member-rule>	The user must belong to a group which meets a condition specified by attributes on the group. Note: When you select this option, Identity Manager displays a new list box where you can select the following options: ■ group [set the product group or family]--Use a group search screen to select a group. ■ group where <group-filter>--Specify a filter that selects one or more groups.	Users who are members of groups where owner=CIO

Syntax	Condition	Example
who are members of <role-rule>	The user must be a member of a role. The role can be an: ■ access role ■ admin role ■ provisioning role Note: To use provisioning roles, Identity Manager must integrate with a Provisioning Server. See the <i>Installation Guide</i> for more information.	Users who are members of the Help Desk role
who are administrators of <role-rule>	The user must an administrator for a role. The role can be an: ■ access role ■ admin role ■ provisioning role Note: To use provisioning roles, Identity Manager must integrate with a Provisioning Server. See the <i>Installation Guide</i> for more information.	Users who are administrators of the Sales Manager role
who are owners of <role-rule>	The user must be an owner for a role. The role can be an: ■ access role ■ admin role ■ provisioning role Note: To use provisioning roles, Identity Manager must integrate with a Provisioning Server. See the <i>Installation Guide</i> for more information.	Users who are owners of the User Manager role
returned by the query <LDAP-query>	The user must meet a condition based on an LDAP query.	(Use an LDAP directory for situations where a query created in the Identity Manager User Console is insufficient)

Syntax	Condition	Example
in <administrative-union-constraint>	The user must meet at least one of the conditions in a list of conditions. You can include the following types of filters in an administrative union constraint: - Member of access/admin/provisioning role - Administrator of access/admin/provisioning role - owner of access/admin/provisioning role - member of a group	Users who are a member of the Certify Manager role, <i>or</i> who are an owner of the Certify Manager role.
in <administrative-intersection-constraint>	The user must all of the conditions in a list of conditions. You can include the following types of filters in an administrative union constraint: - Member of access/admin/provisioning role - Administrator of access/admin/provisioning role - owner of access/admin/provisioning role - member of a group	Users who are members of the Contract Initiator role <i>and</i> the Contract Approver role.

Actions on Apply/Remove Policies

You can define change actions that Identity Manager performs when it evaluates the identity policy. The actions include:

- Actions on Apply Policy--A set of actions that Identity Manager performs when a user meets the conditions in the policy conditions.
- Actions on Remove Policy--A set of actions that Identity Manager performs when a user no longer meets the conditions in the policy conditions.

The actions that Identity Manager can perform when identity policies are applied or removed are the same. See the following table for more information.

Change Action	Description
Add to group <group-name> [...]	Adds users to a group. When you select this option, Identity Manager presents a screen where you can search for the group you want.
Add to <group-name> in user's organization	Adds users to a local group. When you select this option, Identity Manager presents a text box where you can enter the name of the group that you want.
Set <single-value-user-attribute> to value	Sets the value of an attribute in a user profile. If there is an existing value, Identity Manager overwrites it with the value specified in the change action.
Add <value> to <multi-value-user-attribute>	Adds a value to a multi-value user attribute. This option does not overwrite existing values.
Make member of access role	Assigns users to an access role.
Make administrator of access role	Make users administrators of an access role
Make member of admin role	Makes users members of an admin role
Make administrator of admin role	Makes users administrators of an admin role
Make member of provisioning role	Makes users members of a provisioning role, which creates associated endpoint accounts. Note: To use provisioning roles, Identity Manager must integrate with a Provisioning Server. See the <i>Installation Guide</i> for your application server.
Make administrator of provisioning role	Makes users administrators of a provisioning role. Note: To use provisioning roles, Identity Manager must integrate with a Provisioning Server. See the <i>Installation Guide</i> for your application server.

Change Action	Description
Remove from group <group-name> [...]	Removes users from a group. When you select this option, Identity Manager presents a screen where you can search for the group you want.
Remove from <group-name> in user's organization	Removes users from a local group. When you select this option, Identity Manager presents a text box where you can enter the name of the group that you want.
Remove <value> from <multi-value-user-attribute>	Removes a value from a multi-value user attribute.
Remove member from access role	Revokes an access role.
Remove administrator from access role	Revokes administrator privileges for a specific access role
Remove member from admin role	Revokes an admin role.
Remove administrator from admin role	Revokes administrator privileges for a specific admin role
Remove member from provisioning role	Revokes a provisioning role.
Remove administrator from provisioning role	Revokes administrator privileges for a specific provisioning role.
Send audit message	Sends a message that you create to the audit database. This message may appear in a report that you create.
Compliance violation	Sends a message that you create to the audit database. If you create a compliance report, the message appears each time the identity policy is applied/removed from a user. See the <i>Configuration Guide</i> for more information about auditing. Note: You must enable the Compliance check box on the Profile tab for the Identity Policy Set to use the Compliance Violation option.

Specify Owners for the Identity Policy Set

On the Owners tab, you define rules about who can be an owner of the identity policy set. An identity policy set owner can modify the basic information about the policy set, and can add, change, or remove identity policies in the set.

To complete the Owners tab:

1. Define owner rules, which determine which users can modify the identity policy set.
2. Click Submit.

Manage an Identity Policy Set

Identity Manager includes the following tasks for managing an identity policy set:

- View Identity Policy Set
- Modify Identity Policy Set
- Delete Identity Policy Set

By default, when an administrator uses one of these tasks, Identity Manager displays a list of all identity policy sets for which that administrator is an owner. The administrator can then choose the policy set he needs from the list.

In an Identity Manager environment that includes many identity policy sets, you may want to customize the View, Modify, and Delete Identity Policy Set tasks to allow administrators to search for an identity policy set, instead of displaying them in a list.

To customize these tasks:

1. In the Identity Manager User Console, select Admin Roles, Modify Admin Task.

The Select Admin Task screen opens.

2. Search for and select the task that you want to customize.
3. On the Scope tab, select All Identity Policy Sets.

When you select this option, Identity Manager uses the Default Identity Policy Set Search screen definition.

4. Click Submit.

How Users and Identity Policies Are Synchronized

When using identity policies, it is important to understand how Identity Manager evaluates and applies the policies to users. Without a thorough understanding of the user synchronization process, you may configure identity policy sets that yield unexpected results.

The following procedure describes how Identity Manager evaluates and applies identity policies:

1. The user synchronization process begins:
 - **Automatically**—You can configure Identity Manager tasks to automatically trigger user synchronization
 - **Manually**—Use the Synchronize User task in the Identity Manager User Console to synchronize a user.
2. Identity Manager determines the set of identity policies that apply to a user.
3. Identity Manager compares the set of identity policies that apply to a user with the list of policies that have already been applied to that user.

Note: The list of policies that have been applied to a user is stored in the %IDENTITY_POLICY% well-known attribute in the user profile. For information on configuring this attribute, see the *Configuration Guide*.

 - If an identity policy is on the list of applicable policies, *and* the policy has *not* been applied to the user previously, then Identity Manager adds the policy to an allocation list.
 - If an identity policy is on the list of applicable policies, the policy has been previously applied to the user, and the Apply Once setting for the policy is disabled, Identity Manager adds the policy to a reallocation list.
 - An identity policy is not on the list of applicable policies, and the policy has been applied to the user, the user no longer matches the policy condition. Identity Manager adds these policies to a deallocation list.
4. After Identity Manager evaluates all of the policies for a user, it applies policies in the following order:
 - a. Identity policies from the deallocation list
 - b. Identity policies from the allocation list
 - c. Identity policies from the reallocation list

5. After the identity policies have been applied, Identity Manager reevaluates the policies to see if any additional changes are needed based on changes that occurred in the first synchronization process (steps 2-4).

This is to ensure that changes made by applying identity policies did not trigger other identity policies.

6. Identity Manager continues to reevaluate and apply identity policies until the user is synchronized with all applicable policies, or until Identity Manager reaches the maximum recursion level, which is defined in the Identity Manager Management Console.

For example, an identity policy may change a user's department when the user is assigned a role. The new department triggers another identity policy. However, if the recursion level is set to 1, the subsequent change is not made until the user is synchronized again.

For more information about setting the recursion level, see the *Management Console Online Help*.

Configure Automatic User Synchronization

Identity Manager can automatically synchronize user accounts with identity policies at different points during a task's lifecycle.

An Identity Manager task generates *events*, detectable activities that occur during task processing. For example, the default Create User task generates the CreateUserEvent, AddUserToGroupEvent, and the AssignAccessRoleEvent. You can configure Identity Manager to synchronize users after a task completes, or when each event completes.

Note: The section [Synchronize Users with Identity Policies](#) (see page 141) provides more information on the user synchronization process.

To configure a task to trigger user synchronization

1. Log into Identity Manager as a user who can modify admin tasks.
2. Select Roles and Tasks, Admin Tasks, Modify Admin Task.
Identity Manager displays a search screen.
3. Search for and select the admin task that will trigger user synchronization.

4. Select one of the following options in the User Synchronization field on the Profile tab for the task:

- **Off**—This task will not trigger user synchronization.
- **On Task Completion**—Identity Manager starts the user synchronization process after all of the events have completed. This setting is the default synchronization option for the Create User, Modify User, and Delete User tasks. The default setting for all other tasks is Off.

Note: If you select the On Task Completion option for a task that includes multiple events, Identity Manager does not synchronize users until all of the events in the task complete. If one or more of those events require workflow approval, this may take several days. To prevent Identity Manager from waiting to apply identity policies until all events complete, select the On Every Event option.

- **On Every Event**—Identity Manager starts the user synchronization process when each event in a task completes.

For tasks with a primary and secondary event for the same user, setting user synchronization to On Every Event may result in more evaluations for which policies apply to a user than if the On Task Completion option is selected.

Synchronize Users Manually

You may want to manually synchronize a user with an identity policy set to ensure that a user account has the right privileges, or complies with a compliance policy.

You can manually synchronize a user by using the Synchronize User task in the Identity Manager User Console.

Note: For the Synchronize User task to work properly, the User Synchronization option must be set to Off, and the Account Synchronization option must be set to On Task Completion or On Every Event. For better performance, choose the On Task Completion option. These options are set in the Profile tab for the Synchronize User task.

The Synchronize User task includes the following tabs:

- **Currently Matched Policies**—Displays a list of identity policies that Identity Manager will apply to the user when the Synchronize User task is submitted.

Note: The Currently Matched Policies tab displays only the identity policies that apply to the user at the time you access the Synchronize User task. When the user is synchronized with those policies, changes may occur that trigger other identity policies. To prevent Identity Manager from applying the new policies until you have reviewed them, set the recursion level for identity policy sets to 1 in the Identity Manager Management Console. After submitting the Synchronize User task, access it again to review the policies.

- **Policies Already Applied**—Displays a list of identity policies that have already been applied to the user.
- **Synchronization Summary**—Displays all of the identity policies that apply to the user and the change actions for those policies.

To synchronize a user account

1. Log into Identity Manager as a user who can use the Synchronize User task. (By default, users with the System Manager role can use this task.)
2. Select Policies, Synchronize User.
The Synchronize User task opens.
3. Select the Synchronization Summary tab.
4. Review the policies and associated actions that Identity Manager will apply to the user, then click Submit.

Verify User Synchronization

To verify that the appropriate changes take place when a user is synchronized with identity policies, check the Policies Already Applied tab in the Synchronize User task.

1. Log into Identity Manager as a user who can use the Synchronize User task. (By default, users with the System Manager role can use this task.)
2. Select Policies, Synchronize User.
The Synchronize User task opens.
3. Select the Policies Already Applied tab.
4. Review the policies and associated actions that Identity Manager applied to the user.

Identity Policy Sets in an Identity Manager Environment

The following sections describe different ways to use identity policies:

- [Example: Automatically Populating User Attributes](#) (see page 145)
- [Example: Allocating Resources and Entitlements](#) (see page 146)
- [Example: Enforcing Compliance](#) (see page 148)
- [Example: Enforcing Segregation of Duties](#) (see page 149)

Example: Automatically Populating User Attributes

You can use an identity policy set to automatically assign user attribute values based on another attribute value or user entitlement. For example, you can create an identity policy set that automatically fills in a user's mailing address based on the user's home office.

To configure an identity policy set for employee addresses, create an identity policy with the following settings for each office location:

Setting	Value
Policy Condition	office = <office_location>
Action on Apply Policy	set Street Address = <some_street_address> set City = <some_city> Set State/Province = <some_state_or_province> Set Postal Code = <some_postal_code>

The following figure shows sample policies in the Employee Addresses identity policy set.

Create Identity Policy Set: *Employee Addresses*

Profile

Policies

Owners

Policy Set

Select identity policy:

	Policy Name	Policy Condition	Action on Apply Policy
▶	New York	where (Office = "New York")	Set Street Address to 601 5th Ave Set City to New York Set State / Province to NY Set Postal Code to 10017
▶	Boston	where (Office = "Boston")	Set Street Address to 201 Jones Rd Set City to Waltham Set State / Province to MA Set Postal Code to 02451
▶	San Francisco	where (Office = "San Francisco")	Set Street Address to 2 Smith St Set City to San Francisco Set State / Province to CA Set Postal Code to 94111

Example: Allocating Resources and Entitlements

Identity policies can automatically assign resources, such as domain accounts, or grant entitlements, such as making a user a member of a role, when users meet the policy condition. For example, you can create a set of identity policies that assign resources and roles based on a user's title.

To create an identity policy set for allocating resources and roles, create an identity policy with the following settings for each of the titles in your organization:

Setting	Value
Policy Condition	title = <some_title>
Action on Apply Policy	Any actions that allocate resources or entitlements to users who meet the policy condition, for example: ■ make member of <some_group> ■ make member of admin role <some_admin_role> ■ make member of provisioning role <some_provisioning_role>
Action on Remove Policy	Any actions that remove resources or entitlements when a user no longer meets the policy condition. For example, if Identity Manager made the user a member of a role when the identity policy was applied, you may want to configure Identity Manager to revoke the role when the user no longer meets the policy condition.

The following figure illustrates sample policies in the Employee Resources identity policy set:

Create Identity Policy Set: *Employee Resources*

Profile Policies Owners

Policy Set

Select identity policy:

	Policy Name	Policy Condition	Action on Apply Policy	Action on Remove Policy
▶	Managers	where (Title = "Manager")	Make member of admin role User Manager Make member of provisioning role Corporate NT Domain Role	Remove member from admin role User Manager
▶	Human Resources	where (Title = "HR Administrator")	Add to group HR Department Make member of admin role User Manager Make member of provisioning role Corporate NT Domain Role	Remove from group HR Department Remove member from admin role User Manager

Example: Enforcing Compliance

You can configure identity policies to define conditions that must or must not exist, and to take certain actions based on the evaluation of those conditions. For example, you can define a compliance policy that states that managers must have a spending limit of \$5,000. If a manager has a spending limit of \$10,000, Identity Manager can reset the manager's spending limit, and record a compliance violation for auditing purposes.

To create a compliance policy set for enforcing spending limits, create an identity policy with the following settings:

Setting	Value
Apply Once	Not enabled
Compliance	Enabled
Policy Condition	Any conditions that define compliance or a compliance violation--for example: title=<some_title> AND Spending Limit > <some spending limit>
Action on Apply Policy	The actions that Identity Manager should take when the policy condition applies--for example: ■ Compliance violation message: Spending limit exceeded ■ Set spending limit to <some_value>

The following figure shows the sample compliance policy described in this example.

Create Identity Policy Set: *Spending Limits*

Profile

Policies

Owners

Policy Set

Select identity policy:

	Policy Name	Policy Condition	Action on Apply Policy
▶	Managers	where (Title = "Manager" and Spending limit > "5000")	Compliance violation message: spending limit exceeded Set Spending limit to 5000

Example: Enforcing Segregation of Duties

Identity policies can define roles that are mutually exclusive and cannot be granted to the same user concurrently. For example, you can prevent a user manager who can grant raises from also being a salary approver.

To create an identity policy set that enforces segregation of duties, create an identity policy with the following settings:

Setting	Value
Apply Once	Not enabled
Compliance	Enabled
Policy Condition	Use the "in <administrative-intersection-constraint>" option to define a set of conditions that violate a business policy. If a user meets all of the conditions, Identity Manager takes the actions in the Action on Apply Policy field. For example, set the policy condition as follows: intersection (who are members of <some_role>) and who are members of <some_other_role>)

Setting	Value
Action on Apply Policy	The actions that Identity Manager should take when the policy condition applies--for example: ■ Compliance violation message: User has mutually exclusive roles ■ Remove member from <some_role>

The following figure illustrates the identity policy in this example.

Create Identity Policy Set: *Salary Approver*

Profile
Policies
Owners

Policy Set

Select identity policy:

	Policy Name	Policy Condition	Action on Apply Policy
1	restrictions	<pre> intersection (who are members of (admin role "User Manager") and who are members of (admin role "Salary Approver")) </pre>	Compliance violation message: <i>user has mutually exclusive roles</i> Remove member from admin role <i>Salary Approver</i>

Chapter 7: Self-Service Tasks

This section contains the following topics:

[Identity Manager Self-Service Tasks](#) (see page 151)

[How to Configure Self-Service Tasks](#) (see page 152)

[Configure the Self-Registration Task](#) (see page 153)

[Configure the Forgotten Password Reset and Forgotten User ID Tasks](#) (see page 156)

[Customize Self-Service Tasks](#) (see page 166)

[Restrict Access to the Self Manager Role](#) (see page 167)

[Access Self Service Tasks](#) (see page 167)

[Configure Multiple Self-Service Tasks](#) (see page 168)

Identity Manager Self-Service Tasks

Self-service tasks are Identity Manager tasks that users can use to manage their own profiles. These tasks are divided into two types:

- **Public tasks**--Tasks that users can access without providing login credentials. Examples of public tasks are self-registration, forgotten password, and forgotten user ID tasks.
- **Protected tasks**--Tasks for which users provide valid credentials. Examples include tasks for changing passwords or profile information. To gain access to these tasks, users must be given a role, such as the Self Manager role.

The following table lists the default self-service tasks, which are available when Identity Manager is installed.

Task Type	Tasks
Public Task	■ Self-registration--Allows users to register at a corporate Web site ■ Forgotten Password Reset--Allows users to reset a forgotten password ■ Forgotten Password--Displays a temporary password that users can use to login to Identity Manager. When the users log in, they are prompted to enter a new password ■ Forgotten User ID--Retrieves or resets a forgotten user ID

Task Type	Tasks
Protected Task	■ Change My Password--Allows users to reset their password ■ Modify My Profile--Maintains profile information, such as address and phone number ■ Modify My Groups--Enables users to subscribe to groups ■ View My Roles--Displays a user's roles ■ View My Submitted Tasks--Displays Identity Manager tasks that the user initiated

How to Configure Self-Service Tasks

The following table describes the steps to configure self-service tasks for an Identity Manager environment. Some of the steps are optional.

✓	Step	Refer to...
	1. Configure a public alias in the Identity Manager Management Console to allow users to access public tasks, such as the self-registration, forgotten password reset, and forgotten user ID tasks.	<i>Configuration Guide</i>
	2. Configure the self-service tasks that apply in your environment.	■ Configure the Self-Registration Task (see page 153) ■ Configure the Forgotten Password Reset and Forgotten User ID Tasks (see page 156)
	3. Customize the self service tasks for your environment.	Customize Self-Service Tasks (see page 166)

-
4. Configure the Self Manager role. (Optional)	Restrict Access to the Self Manager Role (see page 167)

By default, the Self Manager role is assigned to all users. Complete this step only if you want to restrict the users who have access to the role.

-
5. Add links for accessing self service tasks to your corporate Web site.	Access Self Service Tasks (see page 167)
-

Configure the Self-Registration Task

To provide self-registration for users, first make sure that you have an alias for public tasks for the Identity Manager environment. (See the *Configuration Guide*). Then, configure the self-registration task.

Note: To avoid overwriting the default Self Registration task, create a copy of the task. Customize the new task as needed.

1. In the Identity Manager User Console, choose Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Select the Self Registration task.
3. On the Search tab, select the End User License Agreement screen by clicking the ... (ellipses) button.

Edit the screen to present an appropriate title and a Message URL.

For the Message URL, use a page that you create to request that new users agree to license restrictions for your application.

4. On the Tabs tab, edit the Profile and Groups tabs as needed:
 - If the Identity Manager environment supports organizations, [supply a default organization where self-registered users' profiles are stored.](#) (see page 154)
 - If the default tasks do not suit your business requirements, customize the profile and list screens.
 - If the Identity Manager environment includes forgotten passwords or forgotten User ID support, [add fields for collecting password questions and answers](#) (see page 154).

Set Up a Default Organization for Self-Registered Users

If your Identity Manager environment supports organizations, you can specify the organization where Identity Manager creates accounts for self-registered users.

Note: To store profiles for different types of users, such as customers and suppliers, in different environments, create multiple self-registration tasks with different default organizations. For example, if customers self-register in the customers organization, and suppliers register in the supplier organization, create two self-registration tasks, such as Customer Registration and Supplier Registration. In each task, define the appropriate default organization.

1. Navigate to the Configure Profile screen for the Self-Registration task if necessary:
 - a. In the Identity Manager User Console, choose Roles and Tasks, Admin Tasks, Modify Admin Task.
 - b. Select the Self Registration task.
 - c. Select the Tabs tab.
 - d. Click the right arrow next to the Profile tab.
2. On the Configure Profile screen, click the ... (ellipses) button next to Default Organization.
3. Select the organization where new users should be created.
4. Save your changes.

Add Verification Questions and Answers

To enable users to specify question and answer pairs, which can be used to retrieve a forgotten password or user ID, add question and answer fields to the self registration screen.

Note: Before adding question and answer fields to collect verification information, make sure that the logical attributes for the question and answer pairs are configured in the forgotten password logical attribute handler. You configure logical attribute handlers in the Identity Manager User or Management Console. For more information, see the online help in the console that you want to use.

1. Navigate to the Configure Profile screen for the Self-Registration task if necessary.
 - a. In the Identity Manager User Console, choose Roles and Tasks, Admin Tasks, Modify Admin Task.
 - b. Select the self registration task.
 - c. Select the Tabs tab.
 - d. Click the right arrow next to the Profile tab.

2. On the Configure Profile screen, click the ... (ellipses) button next to the Screen field.

The Select Screen Definition screen opens.

3. Select the Self Registration Profile and click Copy.
4. Supply a new name and tag for the custom self registration profile screen that you are creating.
5. Add the number of rows and fields that you want to appear for the verification questions and answers.

For example, if users should supply two question/answer pairs, add two rows of two fields.

6. In the field properties for the first question, select |Question 1| from the list of available attributes. Configure the field properties as needed.

Note: If the ForgottenPasswordHandler logical attribute handler is configured to display a list of questions that users can select, specify the Option Selector style.

7. Repeat step 6 for each of the new fields that you added.
8. Click Apply.

The Select Screen Definition screen opens again.

9. Make sure that the screen definition is selected and click Select.

The Configure Profile screen appears.

10. Click OK to close the Configure Profile screen and return to the Tabs tab.

Configure the Forgotten Password Reset and Forgotten User ID Tasks

Identity Manager includes default tasks for users who cannot access their accounts due to a forgotten password or user ID:

- [The Forgotten Password Reset Task](#) (see page 156)
- [The Forgotten User ID Task](#) (see page 156)

You can use these tasks as installed or customize them to suit your needs.

The Forgotten Password Reset Task

The Forgotten Password Reset task enables a user to reset a password after Identity Manager verifies his identity. Identity Manager uses two types of questions to verify a user's identity:

- Identification questions--Determine who a user is. Examples include a user's full name, user ID, or email address.
- Verification questions--Confirm a user's identity. Depending on how Identity Manager is configured, users can specify their own verification questions, or they can select questions from a predefined list.

In the default Forgotten Password Reset task, a user must provide a user ID and answer three verification questions. Each verification question, which is presented on a separate screen, is randomly chosen from a list of five questions that the user supplies during registration.

Once Identity Manager verifies a user's identity, a screen where the user can enter a new password is displayed.

The Forgotten User ID Task

In the default Forgotten User ID task, a user must provide an email address and answer one verification question to view their user ID in the Identity Manager User Console. The verification question, which is presented on a separate screen, is randomly chosen from a list of five questions that the user supplies during registration.

Custom Forgotten Password Reset and Forgotten User ID Tasks

You can use the Forgotten Password Reset or User ID task as installed, or customize the task for your environment. You can:

- Specify the number of [questions](#) (see page 157) users must answer successfully to verify their identity.
- Determine whether users supply their own [verification questions](#) (see page 157), or whether they select questions from a pre-defined list.
- [Define the presentation](#) (see page 160) of the verification questions on the screen.
- Require users to provide additional information, such as a social security number, to [verify their identity](#) (see page 162).
- Determine how users receive their [password](#) (see page 165) or [user ID](#) (see page 166).
- Specify criteria, such as failing more than three verification attempts, for [locking a user out of the task](#) (see page 163).

Collect Question and Answer Pairs for User Verification

Users must supply the question and answer pairs that are used to verify their identity.

You can allow users to create their own questions, or require them to select predefined questions from a list.

To configure Identity Manager to collect question and answer pairs, complete the following actions:

- Add fields for collecting the questions and answers to the Self Registration, Modify My Profile, and Change My Password [tasks](#) (see page 153).
- Configure the ForgottenPasswordHandler handler in the Identity Manager User Console or Management Console. For configuration instructions, see the online help in the console that you want to use.

Set Up the Forgotten Password Reset or User ID Task

The configuration for the Forgotten Password Reset and Forgotten User ID tasks is very similar.

To configure these tasks

1. Verify that the following items are configured in the Identity Manager Management Console:
 - Public alias--A text string that Identity Manager adds to the URL for accessing public tasks, including the Forgotten Password Reset and Forgotten User ID tasks. See the *Configuration Guide* for more information.
 - ForgottenPasswordHandler--A logical attribute handler that enables users to create one or more verification questions, or choose questions from a predefined list. (See the *Programming Guide for Java* for more information.)

Note: You can also configure the ForgottenPasswordHandler in the User Console. Click the Help button in the User Console for more information.

2. To configure the Forgotten User ID task in an Identity Manager environment that was created before Identity Manager v6.0 SP 1, complete the following steps.

Note: If you are configuring the Forgotten Password Reset task, skip to step 3.

- a. In the Identity Manager Management Console, select the Identity Manager environment.
- b. Click Roles and Tasks and import this file:

```
<im_admin-tools-dir>/RoleDefinitionUpdates/RoleDefinitionsFUID.xml
```

- c. Click Continue to exit.

3. In the Identity Manager User Console, do one of the following:
 - To create a copy of the Forgotten Password Reset or Forgotten User ID task (recommended), choose Admin Roles, Create Admin Task. Select Create a copy of an admin task, and search for the task to copy.
 - To modify the default task, choose Admin Roles, Modify Admin Task. Search for the task to modify.

Identity Manager displays the tasks that match the criteria you entered.

4. Select the Forgotten Password Reset or Forgotten User ID task.
5. On the Scope tab, click the ... (ellipses) button to display a list of screens to edit.

6. Select one of the following screens, and click Edit:
 - Forgotten Password Search
 - Forgotten User ID Search
7. Configure the following based on your needs:
 - Identification screen--Determines who a user is. This is the first screen that users see when they access the Forgotten Password Reset or Forgotten User ID tasks.
 - Verification screen(s)--Presents one or more verification questions to users.
8. Enter the number of questions users must answer to verify their identity.

Note: If you configure Identity Manager to display multiple verification questions on a single screen, the number of questions is determined by the logical attribute handler associated with the task. The Number of Questions setting does not apply.
9. Configure the criteria for locking the Forgotten User ID or Password task.
10. Submit the task.

Design Identification Screens

The identification screen is the first screen that users see when they access the Forgotten Password Reset or User ID task.

The default identification screen prompts users to supply a user ID. You can add or change the fields on the identification screen to suit your needs.

The default identification screen resembles the following:

Identification prompt	Forgotten Password Reset: Please enter the following to identify yourself	
Profile screen for identification	User ID*	

To customize the identification screen:

1. Navigate to the Configure Forgotten Password Search screen or the Forgotten User ID Search screen in the Identity Manager User Console, if necessary:
 - a. Choose Roles and Tasks, Admin Tasks, Modify Admin Task.
 - b. Select the Forgotten Password Reset or User ID task.

- c. On the Scope tab, click the ... (ellipses) button to display a list of screens to edit.
 - d. Select one of the following screens, and click Edit:
Forgotten Password Search
Forgotten User ID Search
2. Enter the text that will appear above the area where users supply account information in the Prompt field.
 3. Select the appropriate screen in the Profile Screen for Identification field.
 4. Modify the screen to include your choice of attributes that users must enter.

Design Verification Screens

After a user successfully completes the identification screen, he is redirected to a verification screen where he must provide information to verify his identity. The user may be required to answer one or more questions, or provide an attribute, such as a social security number.

If users must answer multiple verification questions, Identity Manager can display those questions on the same screen, or on separate screens.

The default verification screen resembles the following:

Forgotten Password: Please enter the following to verify your identity	
User ID	dgoodman
First Name	Diane
Last Name	Goodman
Password Hint	What is your dog's name
Answer*	

Display Multiple Verification Questions At One Time

If users answer multiple questions to verify their identity, you can display those questions on a single screen.

Note: If a single screen displays multiple questions, the number of questions that a user has to answer is determined by the number of question and answer pairs that you add to the profile screen for primary verification, not the number of questions that you configure in the search screen for the task.

To display multiple verification questions on a single screen

1. Configure the Forgotten Password Logical Attribute Handler for multiple question and answer pairs.

You can configure the ForgottenPasswordHandler in the Identity Manager User Console or the Management Console. For instructions, see the online help in the console that you want to use.

Add |VerifyQuestion1| , |VerifyAnswer1| pairs depending upon the number of questions you want to set.

2. Navigate to the Configure Forgotten Password Search screen or Configure Forgotten User ID Search screen, if necessary.
3. Enter the text that appears above the area where users supply verification information in the Prompt for Primary Verification Screen field.
4. In the Profile Screen for Primary Verification field, select a screen definition, such as the Forgotten Password Verify screen.
5. Modify the screen definition to include the Logical Attributes for each of the verification question and answer pairs that should appear on the screen. For example, add fields as follows:

|VerifyQuestion1| - Read only.

|VerifyAnswer1| - Write Required.

Note: For more information, see the online help for the ForgottenPasswordLogical Attribute Handler.

6. Make sure that the Prompt for Secondary Verification Screen and Profile Screen for Secondary Verification fields are blank in the Configure Forgotten Password Search or Configure Forgotten User ID Search screen.
7. Enter the number of questions that user must answer correctly in the Number of Questions field.
8. Click OK.

Display One Verification Question at a Time

For increased security, you can display only one verification question at a time. Subsequent questions are displayed only after the preceding question is answered successfully.

To display each verification question on a separate page, define a Primary Verification Screen and a Secondary Verification Screen.

The Primary Verification Screen is displayed after users provide valid identification, such as a user ID. When the user successfully answers one question on the primary verification screen, Identity Manager displays the secondary verification screen for each remaining question.

To configure the primary and secondary configuration screens:

1. Make sure that the |VerifyQuestion| and |VerifyAnswer| logical attributes are configured in the ForgottenPasswordHandler logical attribute handler. See the *Programming Guide for Java*.
2. Navigate to one of the following screens, if necessary:
 - Configure Forgotten Password Search Screen
 - Configure Forgotten User ID Search Screen
3. Enter the text that appears above the area where users supply verification information in the Prompt for Primary Verification Screen field.
4. In the Profile Screen for Primary Verification field, select a screen definition, such as the Forgotten Password Verify screen.
Note: Modify the screen definition to include the Logical Attributes for each of the question and answer pairs that should appear on the screen.
5. Enter the text that appears above the area where users supply verification information in the Prompt for Secondary Verification Screen field.
6. Select the Forgotten Password Secondary Verify screen in the Profile Screen for Secondary Verification field.
Modify the screen to include |VerifyQuestion| and |VerifyAnswer| logical attributes.
Note: To use a secondary verification screen, you must configure a primary verification screen.
7. Enter the number of questions that user must answer correctly in the Number of Questions field.
8. Click OK.

Verify a User Attribute

Identity Manager can verify a user's identity by requiring the user to supply one or more profile attributes. You can require these attributes in addition to verification questions, or instead of them.

The verification screen in the following figure prompts for an Employee ID.

Modified Forgotten Password: Please enter the following information:

Employee Number*

To use user attributes in the verification process:

1. Configure the verification screen as described in one of the following sections:
 - [Display Multiple Verification Questions At One Time](#) (see page 160)
 - [Display One Verification Question at a Time](#) (see page 161)
2. Add one or more fields to collect the user attribute in the Forgotten Password Verify screen, or in a custom primary verification screen, if you designed one.

For example, to collect a user's employee number in addition to a user ID, modify the Forgotten Password Identify profile screen. Add one row containing a single field before or after the user ID field. Click the right arrow for the new field to define its properties.

Lock the Forgotten Password Reset or Forgotten User ID Task

To secure the Forgotten Password Reset or Forgotten User ID task, you can limit the number of failed verification attempts a user makes. Once a user exceeds the failed attempt limit, the task locks, and the user can no longer access it.

You can determine what Identity Manager considers a failed verification attempt. The definition of a failed attempt may be very strict, such as answering one verification question incorrectly, or more lenient to allow for mistakes, such as mis-typing an answer.

Note: You can also configure Identity Manager to lock the Forgotten Password Reset or Forgotten User ID task after a specified number of [successful verification attempts](#) (see page 164). This prevents users from using the Forgotten Password Reset or Forgotten User ID task instead of remembering login credentials.

Configure a Failed Attempt Limit

To configure Identity Manager to lock the Forgotten Password Reset or Forgotten User ID task after failed verification attempts:

1. Navigate to the Configure Forgotten Password Search Screen, if necessary.
2. Configure the criteria for verification failure, as needed:
 - Number of acceptable incorrect answers--The number of incorrect answers a user can provide before Identity Manager records a verification failure.

- Verification page timeout--The amount of time a user has to answer all of the questions on a page.

Verification page attempt limit--The number of times a user can attempt to answer the questions on a page.

If only one question appears per page, the Verification page attempt limit is the number of times a user can try to answer that question.

Note: Specify 0 for the options that do not apply.

If a user exceeds any of the specified criteria, Identity Manager records a verification failure.

3. In the Failed Attempt Limit field, enter the number of consecutive times a user can fail the verification process before they are locked out of the task.

Identity Manager locks the user out of the task, and optionally disables the user's account, if the user attempts to verify his identity after the Failed Attempt Limit has been reached. For example, if the failed attempt limit is 3, the user is locked and disabled on the fourth failed attempt.

4. Select the Disable User check box to disable a user's account in addition to locking the task when the failed attempt limit is exceeded.
5. In the Failed Attempt Lockout Length field, enter the number of days that a user is locked out of the task if she exceeds the failed attempt limit.

Note: The attribute you specify must be defined in the directory configuration file (directory.xml) for the Identity Manager environment.

6. Select the attribute that Identity Manager will use to track verification attempts in the Attempt Tracking Attribute field.

Configure a Successful Attempt Limit

Limiting the number of successful verification attempts prevents users from misusing the Forgotten Password Reset or Forgotten User ID task. For example, a user may rely on the Forgotten Password Reset task to reset a password instead of having to remember a password that conforms to a strict password policy.

To limit successful verification attempts:

1. Navigate to the Configure Forgotten Password Search Screen, if necessary.
2. Select the attribute that Identity Manager will use to track verification attempts in the Attempt Tracking Attribute field.
3. Enter the number of days that users must wait before using the task in the Successful Attempt Limit field.

Determine How Users Reset Passwords

Once Identity Manager verifies a user's identity in the Forgotten Password task, it performs *one* of the following actions:

- Redirects users to a screen where they can enter a new password. (default)
- Emails or displays a temporary password. Users can use the temporary password to log into Identity Manager, where they are forced to set a new password.

To configure Identity Manager to display or email a temporary password, use the Forgotten Password task instead of the Forgotten Password Reset task.

The Forgotten Password task is associated with a business logic task handler, a Java object that forms custom business logic, which generates a temporary password.

By default, the Forgotten Password task displays the temporary password in the Identity Manager User Console.

To configure the Forgotten Password task to email the temporary password:

1. In the Identity Manager Management Console, configure email notifications for the Identity Manager environment. See the *Configuration Guide* for instructions.
2. In the Identity Manager User Console, choose Roles and Tasks, Admin Tasks, Modify Admin Task.
3. Select the Forgotten Password task.
4. On the Profile tab, click Business Logic Task Handlers.
The Business Logic Task Handlers screen opens. The BLTHGenerateTemporaryPassword handler should appear in the list of handlers.
5. Click the right arrow icon to edit the properties for the handler.
6. In the Property field, click the minus icon to delete the ShowPwdOnScreen property.
7. In the Property field, type in ShowPwdOnScreen again.
8. In the Value field, enter:
false
9. Click Add.

Determine How Users Retrieve a Forgotten User ID

Once Identity Manager successfully verifies a user's identity, it displays the user's ID on the screen.

For additional security, you can configure Identity Manager to email the user's ID. To configure Identity Manager to email a user ID:

1. [Configure the Identity Manager environment to support email notifications](#) (see page 212).
2. Choose Roles and Tasks, Admin Tasks, Modify Admin Task.
3. Select the Forgotten User ID task.
4. On the Profile tab, click Business Logic Task Handlers.

The Business Logic Task Handlers screen opens.

5. Click the minus sign () icon next to the BLTHDisplayUserID handler to delete it.

Deleting the BLTHDisplayUserID handler prevents Identity Manager from displaying the user ID in the User Console. If you want Identity Manager to display the user ID in the User Console *and* email the user ID, do not delete the BLTHDisplayUserID handler.

Customize Self-Service Tasks

Identity Manager includes pre-configured self-services tasks, listed in [Identity Manager Self-Service Tasks](#) (see page 151), that you can customize to suit your business needs.

The following table lists some common customizations that you can apply to the default tasks.

Customization	See...
Fields on a task screen, including: ■ Changing the fields that appear on a screen ■ Defining attributes ■ Modifying the layout ■ Applying validation rules	Choose Tabs for the Task

Customization	See...
Branding, colors, and font	The chapter, "Customizing the User Console" in the <i>Configuration Guide</i> .
Workflow for self-service tasks	WorkPoint Workflow (see page 217)
Localization	The chapter, "Identity Manager Localization" in the <i>Configuration Guide</i> .

Restrict Access to the Self Manager Role

By default, the Self Manager role, which allows users to manage their profile information and view their roles and submitted tasks, is assigned to all users.

To give the Self Manager role to a subset of users, delete the existing member policy and create a new policy as described in Define Member Policies for an Admin Role.

Access Self Service Tasks

Once you have configured the self service tasks for your Identity Manager environment, you can add URLs for these tasks to a corporate Web site.

URLs for self service tasks have the following format:

`http://<domain>/ldm/<im>/index.jsp?task.tag=<task_tag>`

where:

- `<domain>` is the fully qualified domain name of the system where Identity Manager is running
- `<im>` is the public alias of the Identity Manager environment
- `<task_tag>` is the unique identifier for the task.

For the default Forgotten Password Reset task, the task tag is `ForgottenPasswordReset`.

`http://<domain>/ldm/<im>/index.jsp?task.tag=ForgottenPasswordReset`

For the default Forgotten User ID task, the task tag is `ForgottenUserID`:

`http://<domain>/ldm/<im>/index.jsp?task.tag=ForgottenUserID`

Configure Multiple Self-Service Tasks

You can create multiple self-service tasks for different types of users. For example, you can create one task to register new employees, and another task to register customers. By using different self-registration tasks, you can:

- Collect different information
- Register users in different organizations
- Redirect users to different logout pages after they register
- Use different branding

The following figures show the self-registration task for new employees and customers, respectively.

Employee Self Registration

Welcome to MyCompany.Com! **Thanks for joining our team.**

First Name*	
Last Name*	
E-Mail	
Office	
Password*	
Confirm Password*	
Question 1	
Answer 1	

Customer Self Registration

Thanks for your interest in MyCompany.Com! To receive information about our products, please provide the following information:

First Name*	
Last Name*	
Company	
Title	
E-Mail	
Password*	
Confirm Password*	

To configure multiple self-service tasks of the same type, specify a unique tag when you create the task. The Tag field is located on the Configure Profile screen for the task.

When you add the link for accessing the task to a web site, you append the task tag, creating a unique URL.

For example, you might create two tasks as follows:

Task	Tag	URL
Register as a new employee	selfregistration_employee	http://<domain>/idm/<im>/index.jsp?task.tag=SelfRegistration_employee
Register as a customer	selfregistration_customer	http://<domain>/idm/<im>/index.jsp?task.tag=SelfRegistration_customer

Chapter 8: Password Management

This section contains the following topics:

[Password Management in Identity Manager](#) (see page 171)

[Password Policies](#) (see page 172)

[Reset Password or Unlock Account](#) (see page 188)

Password Management in Identity Manager

Identity Manager includes several features for managing user passwords:

- Password Policies--These policies manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage.
- Password Managers--Administrators who have the Password Manager role can reset a password when a user calls the Help desk.
- Self-service password management--Identity Manager includes several self-service tasks that allow users to manage their own passwords. These tasks include:
 - Self Registration--Users specify a password when they register at a corporate Web site.
 - Change My Password--Users can modify their passwords without help from IT or helpdesk personnel
 - [Forgotten Password](#) (see page 156)--Users can reset or retrieve a forgotten password after Identity Manager verifies their identity.
 - [Reset Password or Unlock Account](#) (see page 188)--Users can reset or retrieve a forgotten password or unlock a windows account on a system where they access Identity Manager.
 - [Forgotten User ID](#) (see page 156)--Users can retrieve a forgotten user ID after Identity Manager verifies their identity.
- Password synchronization on endpoint accounts--Password changes are synchronized in Identity Manager, the Provisioning Server, and its target systems. New passwords are verified against Identity Manager password policies.

Note: For more information on password synchronization, see the *Provisioning Guide*.

- Password authentication on endpoint accounts--Authenticates passwords so users can employ their passwords on endpoint accounts to log on the Provisioning Manager.

Note: For more information on password validation, see the *Provisioning Guide*.

Password Policies

A password policy is a set of rules and restrictions that determines how passwords are created and when they expire.

In a password policy, you can configure the following settings:

- Password composition--Specify the content requirements for new passwords. For example, you can configure settings that require users to create passwords which are at least eight characters long and contain a number and a letter.
- Regular expressions--Provide an expression that determines the format of a valid password. You can specify whether passwords must match or must not match that format.
- Advanced password options--Specify actions that Identity Manager should take, such as making passwords lower case, before processing a password. You can also specify the priority of a password policy, if multiple password policies apply.

Note: You configure a password policy in an Identity Manager environment; however, the policy applies to the user store associated with the environment. If a user directory is associated with multiple environments, a password policy defined in one environment may apply in other environments, as well.

When Identity Manager integrates with SiteMinder, you can configure additional rules and restrictions for password management:

- Password expiration--Define events, such as a number of days elapsing or a number of failed login attempts, that cause a password to expire. When a password expires, the user account is disabled.
- Password restrictions--Set limits on password reuse. For example, users must wait 90 days before reusing a password.

Note: SiteMinder users can also configure password policies in the SiteMinder Administrative user interface. These policies appear in the Identity Manager User Console.

Create a Password Policy

To create a password policy

1. In the User Console, choose Policies, Manage Password Policies, Create Password Policy.
2. Enter a unique name and an optional description for the password policy.
3. Select the Enabled checkbox to use the password policy in an Identity Manager environment.
4. Select the task to which users are redirected if they are forced to reset their passwords. (Users may be forced to reset a password if their password expires or a change occurs in a password policy.)

By default, Identity Manager redirects users to the Change My Password task.

The task you specify can be a public or protected task. Any user can access a public task, such as the default Password Services task. Users must have a role, such as the Self Manager role, to access a protected task.

5. Configure the password policy settings you need as described in the following sections:
 - [Configure Password Composition](#) (see page 174)
 - [Specify Regular Expressions](#) (see page 175)
 - [Configure Advanced Password Options](#) (see page 177)
6. Configure additional password policy settings, if Identity Manager integrates with SiteMinder:
 - [Configure Password Expiration](#) (see page 181)
 - [Set Password Restrictions](#) (see page 185)

Manage Password Policies

Administrators with the appropriate privileges can manage password policies using the View, Modify, and Delete Password Policy tasks. By default, these tasks appear in the Policies category.

When you access one of these tasks, Identity Manager displays a list of password policies that apply to the user store associated with the current Identity Manager environment. If Identity Manager integrates with SiteMinder, the list may include password policies that are created in the SiteMinder Administrative User Interface using Password Services. You can manage password policies that are created in Identity Manager or SiteMinder.

For more information about SiteMinder Password Services, see *CA SiteMinder Web Access Manager Policy Server Configuration Guide*.

Configure Password Composition

You can specify rules that determine the character composition of newly created passwords.

Note: When configuring password composition settings, consider the maximum password length when determining values for character requirements. If the total number of letters and/or numbers required exceed the maximum password length then all passwords will be rejected. For example, if Letters is set to 6 and Digits is set to 6, all passwords must contain at least 12 characters (6 letters and 6 digits). In this example scenario, if a maximum password length of 8 characters is specified, all passwords will be rejected.

Password composition settings include:

Minimum password length

Specify a minimum length for user passwords.

Maximum password length

Specify the maximum length for user passwords.

Maximum repeating characters

Determines the maximum number of identical characters that can appear consecutively in a password.

For example, if this value is set to 3, then "aaaa" can not appear anywhere in the password. However, "aaa" is acceptable within a password. You should set this value to ensure that users cannot enter passwords made up entirely of a single character.

Upper case letters

Specifies whether to allow upper case alphabetic characters and, if so, the minimum number a password must contain.

Lower case letters

Specifies whether to allow lower case alphabetic characters and, if so, the minimum number a password must contain.

Letters

Specifies whether to allow letters and if so, the minimum number a password must contain.

Note: The Letters check box is automatically selected if you allow upper or lower case letters.

Digits

Specifies whether to allow numbers and, if so, the minimum number a password must contain.

Letters and Digits

Specifies whether to allow letters and digits, and if so, the minimum number a password must contain. If this setting is set in conjunction with Digits, characters can satisfy both requirements. For example, if this setting and Digits are set to 4, the password "1234" is a valid password.

Note: The Letters and Digits check box is automatically selected if you allow upper or lower case letters, or numbers.

Punctuation

Specifies whether to allow punctuation marks, and if so, the minimum number a password should contain. These can be periods, commas, exclamation marks, slashes, dashes, and hyphens.

Non-printable

Specifies whether to allow non-printable characters, and if so, the minimum number a password should contain. These characters cannot be displayed on a computer screen.

Note: Certain browsers do not support non-printable characters.

Non-alphanumeric

Specifies whether to allow non-alphanumeric characters such as punctuation marks and other symbols located on the keyboard ("@", "\$", and "*") and if so, the minimum number a password should contain. Non-printable characters are also included. A non-alphanumeric character also satisfies Punctuation and Non-printable character requirements.

Specify Regular Expressions

Reviewer: W/o SM you can type in two types of expressions Must Match and Must Not Match. With SM, can you still name the expression and add multiples? Password regular expression matching allows you to specify regular expressions (text patterns used for string matching) that each password must match or not match in order to be valid. This can be useful, for example, if you want to require that the first character in the password is a digit, but that a digit not be the last character.

To configure multiple expressions for a single password policy, Identity Manager must integrate with SiteMinder. If you create multiple expressions, acceptable passwords must match *all* specified expressions.

To add a new required expression

1. Type a descriptive tag for the expression (no white space) in the Name field.
2. Type a regular expression using the syntax described in [Regular Expressions Syntax](#) (see page 176) in the Must Match field.
3. If the password must not match the regular expression, select the check box in the Must Not Match column.

Note: If Identity Manager integrates with SiteMinder, you can specify multiple expressions by clicking the plus (+) sign to add the expression.

Example: The following regular expression definition could be used to require that all passwords start with an upper or lower case letter: Name: MustStartAlpha

Expression: [a-zA-Z].*

Regular Expressions Syntax

This section describes the syntax you should use to construct regular expressions for password matching. This syntax is consistent with the regular expression syntax supported for resource matching when specifying realms.

Characters	Results
\	Used to quote a meta-character (like '*')
\\	Matches a single '\' character
(A)	Groups subexpressions (affects order of pattern evaluation)
[abc]	Simple character class (any character within brackets matches the target character)
[a-zA-Z]	Character class with ranges (any character range within the brackets matches the target character)
[^abc]	Negated character class
.	Matches any character other than newline
^	Matches only at the beginning of a line

Characters	Results
\$	Matches only at the end of a line
A*	Matches A 0 or more times (greedy)
A+	Matches A 1 or more times (greedy)
A?	Matches A 1 or 0 times (greedy)
A*?	Matches A 0 or more times (reluctant)
A+?	Matches A 1 or more times (reluctant)
A??	Matches A 0 or 1 times (reluctant)
AB	Matches A followed by B
A B	Matches either A or B
\1	Backreference to 1st parenthesized subexpression
\n	Backreference to <i>n</i> th parenthesized subexpression

All closure operators (+, *, ?) are greedy by default, meaning that they match as many elements of the string as possible without causing the overall match to fail. If you want a closure to be reluctant (non-greedy), you can simply follow it with a '?'. A reluctant closure will match as few elements of the string as possible when finding matches.

Configure Advanced Password Options

Advanced password policy options allow you to configure pre-processing of submitted passwords prior to validation and storage (for example, forcing all characters to upper case) and to assign the policy a priority to allow predictable evaluation of multiple password policies that apply to the same user directory or namespace.

Do Not Force Case | Force Upper Case | Force Lower Case

Determine whether passwords should be forced to upper or lower case before processing and storage. Choose a case forcing option by clicking the Force Upper Case or Force Lower Case radio button. Otherwise ensure that the Do Not Force Case radio button (the default) is selected.

Important! Be careful to ensure that any case forcing option that you specify is consistent with any [case-related composition requirements you have defined](#) (see page 174).

Remove Leading White Space

Select to remove leading white space from passwords before processing.

Remove Trailing White Space

Select to remove trailing white space removed from passwords before processing.

Remove Embedded White Space

Select to remove all embedded white space before processing.

Note: Some user directory implementations automatically strip leading and/or trailing white space from attribute values (in which user passwords are stored) before storing them regardless of the settings you specify in your password policy.

Evaluation Priority

Specifies the evaluation priority for the password policy. The value should be in the range 0 (the default) to 999. Applicable policies are evaluated in descending order (999 first; 0 last).

Apply Lower Priority Password Policies

Determines whether lower priority password policies are applied after this one.

Note: This field is available only when Identity Manager integrates with SiteMinder.

Password Policies with SiteMinder

Identity Manager enables you to create basic password policies that manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage.

If Identity Manager integrates with SiteMinder, you can create advanced password policies that enable you to define these additional rules and restrictions:

- Directory filters
- Password expiration:
 - Track failed or successful logins
 - Authenticate on login
 - Password expiration if not changed
 - Password inactivity
 - Incorrect password
 - Multiple regular expressions

- Password restrictions:
 - Minimum days before reuse
 - Minimum number of passwords before reuse
 - Percent different from last password
 - Ignore sequence when checking for difference
 - Profile attribute matching
 - Dictionary matching

Password Policies and Relational Databases

If you configure a password policy that applies to a relational database, you must use the following format to configure the Password Data attribute for the SiteMinder User Directory:

tablename.columnname

To avoid syntax problems during execution, we recommend that this field reside in the primary table.

Apply a Password Policy to a Set of Users

If Identity Manager integrates with SiteMinder for advanced password policies, you can specify rules that determine the set of users to which a password policy applies. This allows you to have one password policy for general employees, and a stricter policy for high-level managers.

To specify a rule for a password policy

1. Create or modify a password policy in the User Console.
2. Select the type of filter to configure in the Directory Filter field.

See the following table for a description of each filter type.

Note: The options for filter type that appear in the Directory Filter list box are determined by the type of user store to which the password policy applies. Some filter types are not available for relational databases and eTrust Directory user stores.

3. Specify a condition by selecting an attribute and operator, and entering a value.
4. To add additional conditions, click the plus sign.

The following table describes the options for directory filter types, and provides examples of each filter type.

Type of Filter	Use this filter to...	Example
Entire Directory	Apply a password policy to all users in a user store.	N\A
In a group	Search for a specific group	Name=Product Team
A user	Search for and select a single user	User ID=jsmith
User filter (Not available for relational databases)	Specify a filter for users.	Employee Type = Contractor
User Search Expression	Enter a search query for users Note: See the <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i> for information about the LDAP search expression.	uid=*smith
Group Filter (Not available for relational databases and Provisioning Server user stores)	Specify a filter for groups	Self Subscribing = *
Group Search Expression (Not available Provisioning Server user stores)	Enter a search query for groups Note: See the <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i> for information about the LDAP search expression.	cn=Sales*

Type of Filter	Use this filter to...	Example
Organization Filter (Not available for relational databases and Provisioning Server user stores)	Specify a filter for organizations Note: See the <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i> for information about the LDAP search expression.	Organization name = *Marketing
Organization Search Expression (Not available for relational databases and Provisioning Server user stores)	Enter a search query for organizations Note: See the <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i> for information about the LDAP search expression.	ou=Boston
Search	Specify a query that is not included in the other options for filter type. Note: See the <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i> for information about the LDAP search expression.	(&(uid=*smith)(ou=Boston))

Configure Password Expiration

To help manage user access, administrators can define events such as multiple failed login attempts or account inactivity, when Identity Manager integrates with SiteMinder. When those events are triggered, the user account that triggered the event is disabled, and optionally, the user is redirected to a new Web page.

You can configure the following settings for password expiration:

- Track Failed/Successful Logins Check Box
- Authenticate on Login Tracking Failure Check Box
- Password Expires if Not Changed Settings
- Incorrect Password Settings
- Password Expires from Inactivity Settings

Track Failed/Successful Logins Check Box

Note: To track failed or successful logins, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

This check box enables and disables tracking of user login attempts, including the time of the last login attempt. If you enable this check box, Identity Manager writes login information to an attribute in the user store.

When the Track Failed Logins check box is enabled, the Incorrect Password section and the Authenticate on Login Tracking Failure Check Box are active.

When the Track Successful Logins check box is enabled, the Password Expires from Inactivity section and the Authenticate on Login Tracking Failure Check Box are active.

If you disable login details, and you have multiple password policies, you must ensure that all applicable password policies disable login details. Otherwise, a single policy which enables the tracking of login details may cause password policies to behave incorrectly.

Authenticate on Login Tracking Failure Check Box

Note: To disable logins, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

This check box enables and disables logins when user tracking fails. By default, this check box is disabled and if user activity cannot be written to the user directory, users are not allowed to login. However, if you enable this check box, users may login, even if password data cannot be written to the user directory.

Note: To enable this check box, you must also enable the Track Failed Logins or Track Successful Logins check box.

Password Expires if Not Changed Settings

Note: To configure password expiration settings, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

In the Password Expires if Not Changed fields, you can configure behavior for passwords that have expired and have not been changed by the owner. Optionally, you can specify how far in advance users are warned that their password will expire.

You can configure the following fields:

After *<number>* Days

Determines the number of days after a password expires that Identity Manager waits before disabling the user or forcing a password change.

Note: Identity Manager does not disable the user account until the user attempts to login after the specified number of days has elapsed.

Disable User

If this radio button is selected, when a user's password expires, Identity Manager disables the user. Disabled users can be enabled by using:

- The Enable/Disable User task in the User Console. (The default System Manager, Organization Manager, and Security Manager roles include the Enable/Disable User task.)
- The SiteMinder administrative user interface.

Note: For more information, see the *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Force Password Change

If this radio button is selected, when a user's password expires, Identity Manager forces a password change when the user next attempts to log in.

Issue expiration warnings for *<number>* days

Allows you to specify how many days in advance a user is notified that a password will expire.

Password Expires from Inactivity Settings

Note: To configure password inactivity settings, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

The Password Expires from Inactivity settings allow you to specify a period of time between user login attempts after which a user account is considered inactive. You can also use this section to specify an action should a user whose account is considered inactive successfully log in.

Note: To configure settings in the Password Expires from Inactivity section, enable the Track login details check boxes.

The Password Expires from Inactivity section contains the following:

- After *<number>* Days--Determines the number of days of inactivity after which a user's password expires.
- Disable User--If this radio button is selected, when a user's password expires due to inactivity, the user account is disabled. Disabled users must then be enabled using the Enable/Disable Users task.
- Force Password Change--If this radio button is selected, when a user's password expires due to inactivity, the Policy Server forces a password change when the user next attempts to log in.

Incorrect Password Settings

Note: To configure incorrect password settings, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

In the Incorrect Password settings, you can specify how many failed logins are allowed before a user account is disabled. Additionally, you can specify how long the account is disabled before a user can attempt to log in again.

Note: This section applies only if the Track Failed Logins check box is enabled.

The Incorrect Password section contains the following fields:

Account disabled after *<number>* successive incorrect passwords

Determines the number of consecutive failed log in attempts a user can make before the user account is disabled. Limiting the number of unsuccessful attempts protects against programs designed to access a resource by repeatedly trying passwords until the correct one is found. If a user fails to login correctly after the specified number of attempts, the user's account is disabled. An administrator must re-enable the account.

After <number> minutes

Determines the length of time (in minutes) that a user must wait before he or she is allowed another login attempt or their account is re-enabled (see below). If the user enters another incorrect password, Identity Manager disables the account again. The user must wait the specified amount of time before trying again.

Allow one login attempt

If this radio button is selected, when a user enters an incorrect password, they are allowed one additional login attempt after the specified number of minutes.

Re-enable account

If this radio button is selected, when a user account is disabled due to incorrect passwords, their account is re-enabled after the specified number of minutes.

Set Password Restrictions

Note: To set password restrictions, Identity Manager must integrate with SiteMinder. See the *Implementation Guide* for more information.

Using password policies, you can place restrictions on password usage. The restrictions include how long a user must wait before reusing a password and how different the password must be from ones previously selected. You can also prevent users from specifying words that you determine are a security risk or contain users' personal information.

The Restriction section includes the following fields:

Minimum number of days before reuse

Determines how many days a user must wait before reusing a password.

Minimum number of passwords before reuse

Determines how many passwords must be used before a password can be reused.

Note: If you specify a length of time and number of passwords, both criteria must be satisfied before a password can be reused. For example, you can configure a password policy which requires users to wait 365 days and specify 12 passwords before reusing a password. After a year, if only six passwords have been used, another six would have to be used before the user can reuse the first password.

Percent different from last password

The percentage of characters a new password must contain that differ from characters in the previous password. If the value is set to 100, the new password may contain no characters that were in the previous password, unless Ignore sequence when checking for differences is deselected. For examples of how this parameter works with Ignore sequence when checking for differences, see the following table.

Ignore sequence when checking for differences

Ignores the position of the characters in the password when determining the percentage.

For example, if a user's initial password is BASEBALL12 and the Ignore sequence when checking for differences check box is selected, a user cannot choose 12BASEBALL as the new password. If the check box is deselected, 12BASEBALL is an acceptable password because each letter occurs in a different position. For examples of how this parameter works with Percent different from last password, see the following table.

For increased security, Ignore sequence when checking for differences check box should be selected.

Passwords	Percent different	Ignore sequence	Accepted
BASEBALL12 (Old)	0	Selected	Y
12BASEBALL		Deselected	Y
BASEBALL12 (Old)	100	Selected	N
12BASEBALL		Deselected	Y
BASEBALL12 (Old)	0	Selected	Y
12SOFTBALL		Deselected	Y
BASEBALL12 (Old)	90	Selected	N
12SOFTBALL		Deselected	Y
BASEBALL12 (Old)	100	Selected	N
12SOFTBALL		Deselected	N

Profile Attributes

Configuring the Match Length field prevents users from using personal information in their passwords. The Match Length field determines the minimum sequence length the password policy compares to attributes in the user's directory entry. For example, if this value is set to 4, Identity Manager checks to see that the password is not composed of the last four digits of the user's telephone number.

Dictionary

Specifies a list of strings that cannot be used in passwords.

Note: The last line of the dictionary file used by Password Services must be followed by a carriage return or it will not be included in the dictionary search.

The Dictionary settings include the following fields:

- Path--Contains the full path and name of the dictionary file.
- Match Length--Controls the length of strings compared against values in the dictionary file. The comparison ignores the case (upper/lower) of the strings. If the Match Length field is left blank or set to zero, only passwords that match a string in the dictionary exactly will be rejected. If the match length is greater than zero, password entries will be rejected if both of the following are true:

The password includes a substring which starts with the same series of characters as a dictionary entry.

The number of consecutive matching characters is greater than or equal to the number specified in the Match Length field.

For example, consider a dictionary file that contains the following:

lion

tiger

bear

If the Match Length field is set to 4, the following will result:

"TeddyBear" will be rejected because Bear matches the bear entry in the dictionary file.

"prestige" will be rejected because "tige" matches the first four characters of the tiger entry in the dictionary file.

"Geiger Counter" will be accepted since "iger" does not include the first letter of the tiger entry in the dictionary file.

Reset Password or Unlock Account

In the case users forget their passwords on Windows systems, you can configure Self-Service to prompt the user from the Windows logon screen. You can use this feature by installing one of these components:

- The Graphical Identification and Authorization (GINA) component, for Windows 2000, 2003, and XP systems
- The Credential Provider, for Windows VISTA and 2008 systems

With this feature, the user is logged into Self Service through the Cube web browser where a password change request page appears. After filling in this page, the user clicks Return to go back to the Windows Logon screen.

Install the GINA or Credential Provider

You can install the GINA or the Credential Provider on any Windows system from which a user accesses an Identity Manager environment.

To install the GINA or the Credential Provider

1. Locate the Identity Manager Provisioning Components download or other installation media.
2. Start the Product Explorer.
3. Choose Install Products, Infrastructure.
4. Choose one of the following:
 - Provisioning GINA for Windows (for Windows 2000, 2003, and XP systems)
 - Provisioning Credential Provider for Windows Vista (for Windows Vista or 2008 systems)
5. Follow the wizard prompts to answer the questions.
6. Once this component is installed, configure it using the appropriate procedure:
 - [Configure GINA](#) (see page 189)
 - [Configure the Credential Provider](#) (see page 190)

Configure the GINA

You can use GINA configuration tool to edit default GINA values and export them to a registry (.reg) file for repackaging. The settings can also be applied to the current system.

To configure GINA

1. In Windows Explorer, go to the following directory:

`C:\Program Files\CA\Identity Manager\Provisioning GINA`

2. Double-click the following executable:

`ginaconfig.exe`

3. Enter information in the GINA settings fields:

Link1 Command

The complete command line that will be executed when a user clicks on the Forgot Password link. This link should be a URL to a web interface for password resetting.

For example, the command could be:

`http://eastern.local:8080/idm/pub/ca/index.jsp?task.tag=ForgottenPassword`

For this URL, self enrollment must be working on the environment. Also, check to make sure the Self Service URL for the Identity Manager environment works from the system where you are installing the GINA.

Link2 Command

The complete command line that will be executed when a user clicks on the Unlock Account link. This link should be a URL to a web interface allowing a user to unlock an account.

Domain

The Provisioning domain name.

4. Fill in the Secure Browser Settings fields as follows:

Default URL

The default page to navigate to when no command line is given for the `link1_cmd` or `link2_cmd`.

Allow List

A regular expression pattern matching URLs to which access should always be allowed.

Deny List

A regular expression pattern matching URLs to which access should always be denied.

5. (Optional) Click Export to export your settings to another system.
6. Click OK to save your settings.
7. Restart the system.

Configure the Credential Provider

You can use a configuration tool to configure a system where you installed the Credential Provider.

To configure the Credential Provider

1. In Windows Explorer, go to the following directory:

`C:\Program Files\CA\Identity Manager\Credential Provider`

2. Double-click the following executable:

`CAIMCredProvConfig.exe`

3. Fill in the Credential Provider Settings fields as follows:

Link1 Command

The complete command line that will be executed when a user clicks on the Forgot Password link. This link should be a URL to a web interface for password resetting.

For example, the command could be:

`http://eastern.local:8080/idm/pub/ca/index.jsp?task.tag=ForgottenPassword`

For this URL, self enrollment must be working on the environment. Also, check to make sure the Self Service URL for the Identity Manager environment works from the system where you are installing the Credential Provider.

Link2 Command

The complete command line that will be executed when a user clicks on the Unlock Account link. This link should be a URL to a web interface allowing a user to unlock an account.

Domain

The Provisioning domain name.

4. Fill in the Secure Browser Settings fields as follows:

Default URL

The default page to navigate to when no command line is given for the link1_cmd or link2_cmd.

Allow List

A regular expression pattern matching URLs to which access should always be allowed.

Deny List

A regular expression pattern matching URLs to which access should always be denied.

5. (Optional) Click Export to export your settings to another system.
6. Click OK to save your settings.
7. Restart the system.

Settings in the Registry

While configuration tools exist to set up the GINA or Credential Provider, you can edit the Windows registry to provide the same values.

GINA Registry Settings

If you choose not to use the GINA configuration tool, you can edit the Windows registry settings in the following key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\GINAUNLOCK]

gina

This holds the value of the current chained GINA. Usually, this would be MSGINA.DLL, the default Microsoft Windows GINA, unless you were integrating with a product such as eTrust SSO or Novell.

link1_cmd

This is the complete command line to execute for link 1 on the Logon dialog.

link2_cmd

This is the complete command line to execute for optional link 2 on the Logon dialog. For example, you could add a link that would lead to a website for unlocking accounts.

If the link2_cmd is blank, only the link1_cmd appears in the Logon Dialog Window.

domain

The Provisioning domain name.

langdir

The location of the localized language DLLs.

configdir

The full directory path to where the GINA is installed.

Credential Provider Registry Settings

If you choose not to use the Credential Provider configuration tool, you can edit the Windows registry settings in the following key:

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]

link1_cmd

This is the complete command line to execute for link 1 on the Logon dialog.

link2_cmd

This is the complete command line to execute for optional link 2 on the Logon dialog. For example, you could add a link that would lead to a website for unlocking accounts.

If the link2_cmd is blank, only the link1_cmd appears in the Logon Dialog Window.

domain

The Provisioning domain name.

langdir

The location of the localized language DLLs.

disablepwdcp

The Disable Microsoft Password Credential Provider option. 1 is disabled. 0 is enabled.

CredentialProviderInstallPath

The full directory path to where the Credential Provider is installed.

configdir

The full directory path to where the Credential Provider is installed.

Cube Browser Registry Settings

The Cube secure browser component has several registry values which control its behavior. The Cube Values are in the following Registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Cube]

404

The path to a standard HTML document to be displayed if the machine cannot contact the remote Provisioning Server at startup.

default

The default page to navigate to when no URL is included in Link1 Command or Link2 Command.

allow

Explicit Allow ACL. A regular expression pattern matching URL that is always allowed. For more information, see [Cube Access Control Lists](#) (see page 193).

deny

Explicit Deny ACL. A regular expression pattern matching URLs that should always be denied access. For more information, see [Cube Access Control Lists](#) (see page 193).

langdir

The location of the localized language DLLs.

Cube Access Control Lists

Cube ACLs are regular expression patterns that explicitly allow or deny permission to navigate to a selected URL. ACLs evaluate in the following order:

1. Allow (Permission is automatically allowed first)
2. Deny (Denied URLs are checked second)

GINA Access Control List Examples

"allow"=".pdf"

Allow all PDF documents to be displayed.

"deny"=".doc|.xls"

Deny access to Microsoft Word and Excel documents.

Reset a Password for a Windows Login

After the GINA or Credential Provider is installed on a Windows system, a Forgot Password link appears on the standard Microsoft Windows logon dialog. Use this link to reset your password or see clues to help you remember it.

To reset a password for a Windows login

1. Click Login from the Windows Security dialog. The Windows Login dialog appears.
2. Enter a valid user name.
3. Click Forgot Password.

The Identity Manager Password Clue page appears.

If you remember your password, return to the login dialog to continue. Otherwise, perform step 4 to authenticate to Identity Manager Self Service.

4. Type the answers to the authentication questions.

Note: If you do not know the answers to all questions, click Request so that your password can be reset by an administrator.

5. If you succeed in answering the questions, click Log In.

The system logs you in and opens Self Service.

6. Change your password.
7. Return to the login dialog and log in with the new password.

Chapter 9: Users

This section contains the following topics:

[Create a User](#) (see page 195)

[Manage a User](#) (see page 195)

[Modify a User](#) (see page 196)

[Assign Roles to a User](#) (see page 197)

Create a User

Use this procedure to create a user profile. Depending on how the Create User task is configured in your Identity Manager environment, you may also use this task to add a user to a group, or make the user a member of an admin or provisioning role.

To create a user

1. Log into the User Console as a user with user management privileges.

The default User Manager role gives users the appropriate privileges.

2. Select Users, Manage Users, Create User.

The Create User task opens.

3. Complete the fields on the Profile tab, as needed.
4. Complete the fields on the other tabs in the task, if applicable.
5. Click Submit.

Identity Manager creates the user.

Manage a User

You can use the Manage User task to search for a user to manage. Once you select the user, Identity Manager displays the list of tasks that you can use to manage that user.

For example, to modify a user using this method, you select the User category, then select the Manage User task. You search for and select the user that you want to manage. In the search results, you click an icon to see a list of tasks that you can use to manage the selected user. From that list, you can select Modify User or any other appropriate task.

To manage a user

1. Select Users, Manage Users, Manage Users.
A search screen that enables you to search for a user opens.
2. Enter search criteria and click Search.
Identity Manager displays a list of users who match the criteria in the search filter.
3. Click the right arrow icon next to the user to manage.
Identity Manager displays a list of tasks that you can perform on that user.
4. Select the task that you want to use.
5. Complete the task and click Submit.

Modify a User

Use the Modify User task to make changes to a user's profile information, or, depending on how the Modify User task is configured in your environment, to manage the user's group and role membership.

To modify a user

1. Log into the User Console as a user with user management privileges.
The default User Manager role gives users the appropriate privileges.
2. Select Users, Manage Users, Modify User.
The Modify User task opens.
3. Change fields on the Profile tab, as needed.
4. Change the fields on the other tabs in the task, if applicable.
5. Click Submit.
Identity Manager modifies the user profile.

Assign Roles to a User

You can assign a role to a user using one of the following methods:

- Use the Modify Role Members/Administrators task to add or remove multiple users from a role.
- Use the Admin Roles, Provisioning Roles, or Access Roles tab on the Modify User task to assign additional admin, provisioning, or access roles to a single user.
- Modify the member policy on the Members tab for the role.

Modifying the member policy changes the criteria that Identity Manager uses to automatically assign the role to users. For example, a member policy may state that all users who have the title Manager have the User Manager role.

Note: For more information on member policies, see [Member, Admin, and Owner Rules](#) (see page 32).

Assign Roles with the Modify Role Members/Administrators Task

The Modify Role Members/Administrators task allows you to add and remove users as members or administrators of a role.

This task lets you add or remove multiple users at the same time.

To modify role members or administrators

1. Log into the User Console as a user with role administrator privileges.
2. Select Roles and Tasks, Admin Tasks, Modify Admin Members/Administrators.

Identity Manager displays the list of roles that you can manage. For a role to appear in the list, you must be an administrator of the role, and the role must have the following options selected, as needed:

Administrators can add and remove members of this role

Administrators can add and remove administrators of this role

3. Select the Membership or Administrators tab, depending on whether you want to modify the role's members or administrators.

Identity Manager displays a list of existing members or administrators.

4. To remove a member or administrator from the role, clear the check box next to the user's name. Then, click Submit.

5. To add a new user, complete the following:
 - a. Click the Add a User button.
Identity Manager opens a user search screen.
 - b. Search for and select the user or users to add as members or administrators.
Identity Manager adds the selected users to the list of members or administrators.
6. Click Submit.

Assign Roles with the Modify User Task

Use the Admin Roles, Provisioning Roles, or Access Roles tab of the Modify User task to assign additional admin, provisioning, or access roles to a single user.

Note: You can also use these tabs in the Create User task.

To modify a user

1. Log into the User Console as a user with user management privileges.
The default User Manager role gives users the appropriate privileges.
2. Select Users, Manage Users, Modify User.
The Modify User task opens.

3. Select one of the following tabs, as needed:

- Admin Roles
- Provisioning Roles
- Access Roles

Identity Manager displays the selected tab.

4. Click on of the following buttons:

- Add a *role-type* role

role-type represents admin, provisioning or access roles.

When you click this button, Identity Manager opens a search screen where you can search for and select roles to add. Identity Manager displays the list of roles that you can manage. For a role to appear in the list, you must be an administrator of the role, and the role must have one or more of the following options selected, as needed:

Administrators can add and remove members of this role

Administrators can add and remove administrators of this role

- Copy from a user

When you select this button, Identity Manager opens a search screen where you can search for and select a user that has the roles the current user needs.

5. Click Submit.

Identity Manager adds the user as a member or administrator of the specified roles.

Chapter 10: Groups

You can create several types of groups, or a combination of these types:

- Static group--A list of users who are added interactively
- Dynamic group--Users belong to the group if they meet an LDAP query (Requires an LDAP directory as the user store)

Note: The Dynamic Group Query field is not included in the Create Group task or other group tasks even if this field exists in the directory.xml for a group. You include Dynamic Group Query field in the task by editing the associated profile screen.

- Nested group--A group containing other groups (Requires an LDAP directory as the user store)

Note: To view the static, dynamic, and nested groups to which a user belongs, use the Groups tab for the User object. This tab appears in the View and Modify User tasks by default.

This section contains the following topics:

[Create a Static Group](#) (see page 201)

[Create a Dynamic Group](#) (see page 202)

[Dynamic Group Query Parameters](#) (see page 203)

[Create a Nested Group](#) (see page 204)

[Static, Dynamic, and Nested Groups Example](#) (see page 206)

[Group Administrators](#) (see page 207)

Create a Static Group

You can associate a collection of users in a *static group*. You manage the static group by adding or removing individual users from the group's membership list. To see the list of members for a group, use the Membership tab, which is included with the View and Modify Group tasks by default.

Note: The Membership tab displays only the members who are explicitly added to the group. It does not display members who are added dynamically.

To create a static group:

1. In the Identity Manager User Console, select Groups, Create Group.
2. Choose to create a new group or a copy of a group and click **OK**.
3. On the Profile tab, enter a group name, group organization, description, and group administrator name.
4. Click the Membership tab.
5. Click Add a user.
6. Search for users to include.
7. Put a check next to the users and click Select.
8. Click Submit.

Create a Dynamic Group

You can create a *dynamic group* by defining an LDAP filter query using the Identity Manager User Console to dynamically determine group membership at runtime without having to search and add users individually.

For example, if you wanted to generate a group that lists all U.S. employees of NeteAuto, you could define an LDAP search filter similar to the following in the Dynamic Group Query field of the Identity Manager User Console:

```
ldap:///cn=Employees,o=NeteAuto,c=US??sub
```

You could also modify this query to locate employees outside the United States.

[Static, Dynamic, and Nested Groups Example](#) (see page 206) shows an example of a group created by static, dynamic, and nested groups.

Note: You include Dynamic Group Query field in the task by editing the associated profile screen. It is not included by default in the Create Group task.

To create a dynamic group:

1. In the Identity Manager User Console, select Groups, Create Group.
2. Choose to create a new group or a copy of a group and click **OK**.
3. On the Profile tab, enter a group name, group organization, description, and group administrator name.

Use the Validate button to check these fields were used correctly.

Note: The Validate button does not check the content of the Dynamic Group Query field.

4. Enter an LDAP search filter like the following example in the Dynamic Group Query field:

ldap:///cn=Employees,o=NeteAuto,c=US??sub?

5. Click Submit.

Note: Only an administrator with the Modify Group task can change a group's dynamic membership.

Dynamic Group Query Parameters

You can use the following dynamic query parameters in the search:

ldap:///<search_base_DN>??<search_scope>?<searchfilter>

- <search_base_DN> is the point from where you begin the search in the LDAP directory. If you do not specify the base DN in the query, then the group's organization is the default base DN.
- <search_scope> specifies the extent of the search and includes:
 - sub -- Returns entries at the base DN level and below
 - one -- Returns entries one level below the base DN you specify in the URL. This is the default value.
 - base -- Uses one instead, ignoring base as a search option

Using one or base obtains only the users in the Base DN organization.

Using sub obtains all users under the Base DN organization and all sub-organizations in the tree.

- <searchfilter> is the filter that you want to apply to entries within the scope of the search. When you enter a search filter, use the standard LDAP query syntax as follows:

(<logical operator> <comparison> <comparison...>)

- <logical operator> is one of the following:
 - Logical OR: |
 - Logical AND: &
 - Logical NOT: !
- <comparison> indicates <attribute><operator><value>

For example:

(&(city=boston)(state=Massachusetts))

The default search filter is (objectclass=*).

Note the following when creating a dynamic query:

- The "ldap" prefix must be lower case, for example:
ldap:///o=MyCorporation??sub?(title=Manger)
- You cannot specify the LDAP server's host name or port number. All searches occur within the Identity Manager LDAP directory that you configured for your Identity Manager environment.

The following are sample LDAP queries:

Description	Query
All users who are managers.	ldap:///o=MyCorporation??sub?(title=Manger)
All managers in the New York West branch office	ldap:///o=MyCorporation??one?(&(title=Manager) (roomNumber=NYWest))
All technicians with a cell phones	ldap:///o=MyCorporation??one?(&(employeetype=technician) (mobile=*))
All employees whose employee numbers are between 1000 and 2000	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
All help desk administrators who have been employed at the company for more than 6 months	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22)) Note: This query requires that you create a DOH attribute for the user's date of hire.

Note: The > and < (greater than and less than) comparisons are lexicographic, not arithmetic. For details on their use, see the documentation for your LDAP directory server.

Create a Nested Group

If the user store is an LDAP directory, you can add a group as a member of another group. The group is called a *nested group*.

The group containing the nested group is called a *parent group*. Members of the nested group become members of the parent group. However, members of the parent group do not become members of a nested group.

Nested groups are similar to email distribution lists where one list can be a member of another. With nested groups, you can add groups and users as members in the group. By nesting a group in another group's membership list, you could include all nested groups members.

For example, if you created separate groups for the manufacturing, design, shipping, and accounting divisions of a company, you can construct a parent group for the entire company by nesting all the separate division groups as members of the company parent group. As a result, any changes you made to the manufacturing, design, shipping, and accounting nested groups would be automatically reflected in the nested group for the entire company. A group that is nested within another group can be dynamic and/or contain other nested groups.

The figure in [Static, Dynamic, and Nested Groups Example](#) (see page 206) shows a parent group created by static, dynamic, and nested groups.

Be aware of the following before creating a nested group:

- Only an administrator with the Modify Group Members task can add or change nested groups from the group's static member list in the Identity Manager User Console.
- Only users with the appropriate administrator privileges can modify, add, or remove members from a group.

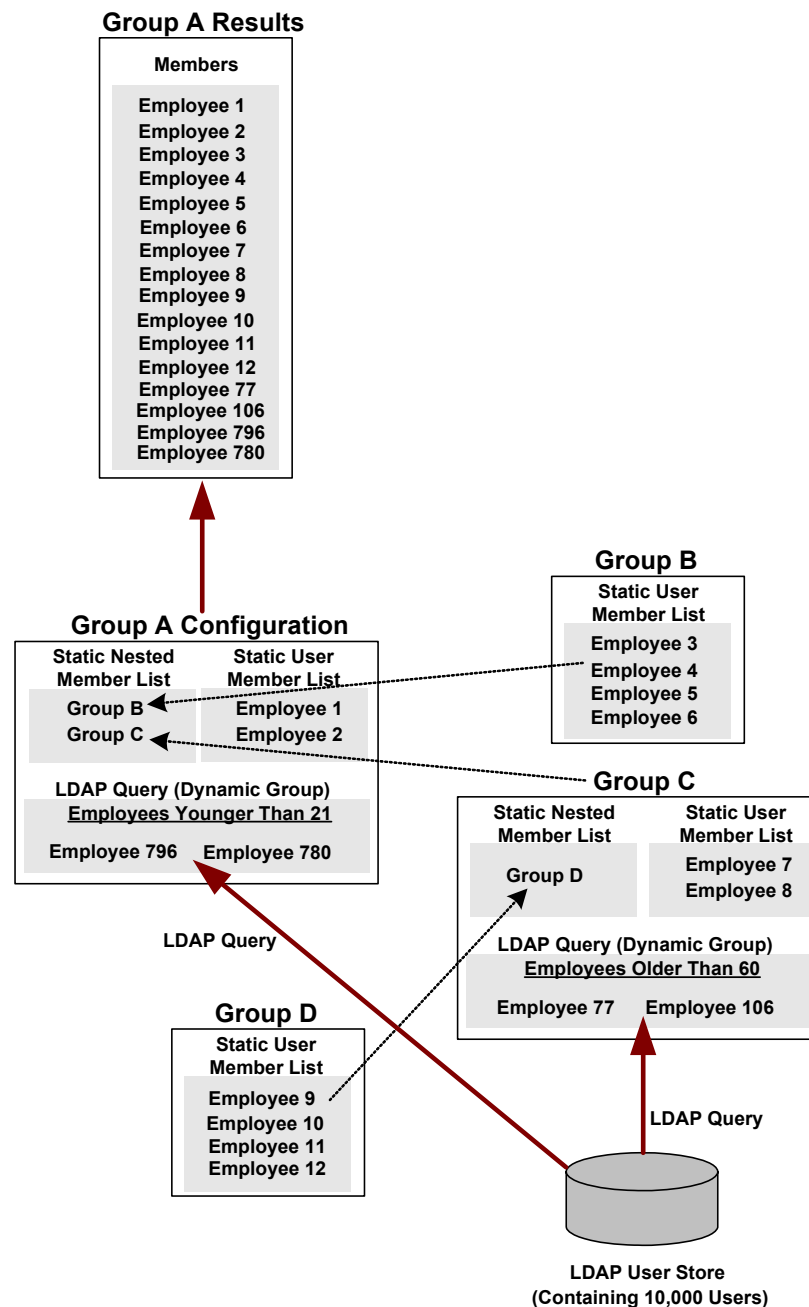
For example, if parent Group A is created by nested groups B and C, the Group A administrator can only modify the members of Group A and not B and C. Groups B and C can only be modified by their appropriate administrators.

To create a nested group:

1. In the Identity Manager User Console, select Groups, Create Group.
2. Choose to create a new group or a copy of a group and click **OK**.
3. On the Profile tab, enter a group name, group organization, description, and group administrator name.
4. On the Membership tab:
 - a. Click Add a group to add a nested group to this group.
 - b. Search for an existing group.
 - c. Put a check next to the group and click Select.
 - d. Click Submit.

Static, Dynamic, and Nested Groups Example

Groups can be complex, consisting of a combination of dynamic, static, or nested groups. The following figure shows an example of a parent group created by static, dynamic, and nested groups.



In the previous figure:

- Parent Group A contains nested groups B and C, two static users, and a dynamic LDAP query that lists all employees who are younger than 21 years old.
- Group B is composed of four static users.
- Parent Group C contains nested Group D, two static users, and a dynamic LDAP query that lists all employees who are older than 60 years old.
- Group D contains four static users.
- The top of the figure lists the Group A members that result from the nested groups, dynamic queries, and static user member lists from Groups B, C, and D.

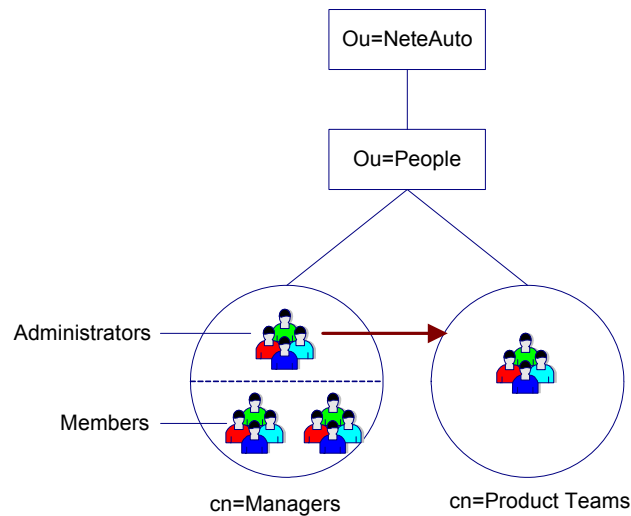
Group Administrators

On the Administrators tab of the Create or Modify Group tasks, you can specify users and groups as administrators of a group. When you assign a user as a group administrator, make sure that the administrator has a role with appropriate scope for managing the group. For example:

1. Use Modify Group to assign a user as an administrator of a group.
2. Assign that user an admin role with group management tasks, such as Modify Group Members, or user management tasks with a Groups tab.
3. Check that the role has appropriate scope over the group.
 - a. Use View Admin Role on the role that you assigned with group management tasks.
 - b. On the Members tab, verify a policy exists with the following:
 - A member rule that the group administrator meets
 - A scope rule that includes the group
 - A scope rule that includes some users to be added to the group

Note: To enable groups to be administrators of other groups in an IdentityMinder environment, configure group administrator support in the directory configuration file. For information, see the *Configuration Guide*.

When you assign a group as an administrator, only administrators of that group will be administrators of the group you are creating or modifying. Members of the administrator group you specify will not have privileges to manage the group. The following illustration shows a group as an administrator of another group.



In this example:

- The group Managers is an administrator of the group Product Teams.
- Administrators of the Managers can manage the Product Teams group. Members of the Managers group cannot.

Chapter 11: Compliance Support

This section contains the following topics:

[Compliance Support in Identity Manager](#) (see page 209)

[User Entitlement Certification](#) (see page 209)

Compliance Support in Identity Manager

Compliance is a corporate governance that includes a wide range of procedures that ensure a company and its employees comply with business policies. These compliance procedures often involve documenting, automating, and auditing the allocation of entitlements to applications and systems.

Identity Manager includes the following features, which support compliance management:

- Identity policies--You can create a compliance policy, a type of identity policy, which prohibits users from having certain privileges if they have other privileges. For example, you can prohibit users who can approve checks from issuing checks.
Compliance policies enforce a segregation of duties in your environment.
- Compliance reports--Identity Manager includes sample reports that display the compliance status for users in your environment. Using this report, you can see which users are not compliant with your business policies.
- User entitlement certification--Forces users, such as managers, to review and certify the roles of the users they manage.

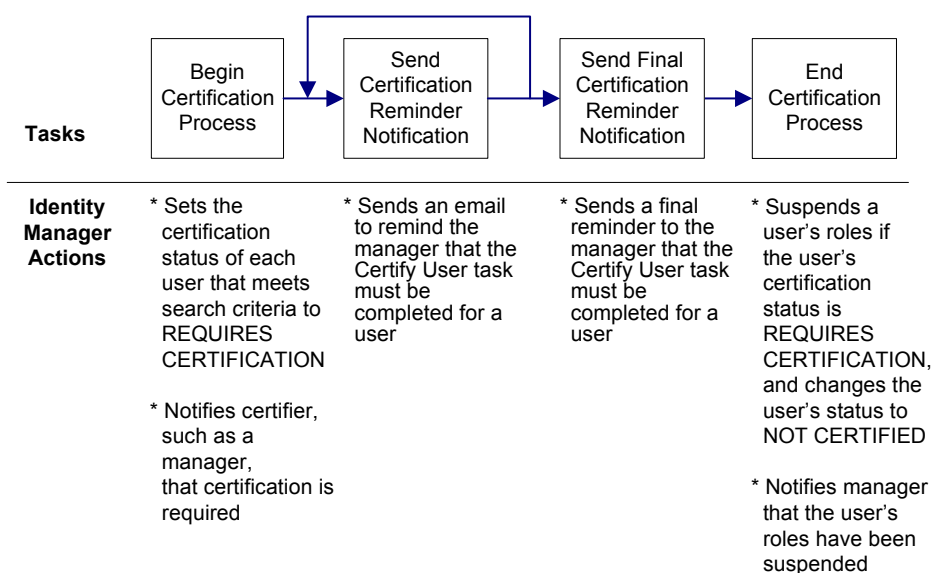
User Entitlement Certification

User certification requires business managers to periodically review and approve the roles of the users they manage. Using the certification tasks, administrators can:

- 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 he has 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

How the Certification Process Works

The following figure describes the steps in the user certification process, and illustrates the actions that Identity Manager takes at each step.



How User Certification is Configured

The user certification feature is configured by default when Identity Manager is installed. Once the prerequisites described in Prerequisites for the User Certification Feature are met, no additional configuration is required.

To customize the default implementation to suit your business requirements, see the following sections:

- [Configure Search Screens](#) (see page 211)
- [Determine Certifiers](#) (see page 212)
- Configure Email Notifications
- [Configure Identity Manager Actions for Non-Certified Users](#) (see page 214)
- [Require Approvals](#) (see page 214)
- [Schedule Certification Tasks](#) (see page 215)

Prerequisites for the User Certification Feature

Before you configure the user certification feature, verify the following:

- [Email notifications are enabled and configured correctly](#) (see page 283).
- The %CERTIFICATION_STATUS% and %LAST_CERTIFIED_DATE% well-known attributes are configured in the directory configuration file (directory.xml)

For more information, see the *CA Identity Manager Configuration Guide*.

Configure Search Screens

Each task in the user certification process allows you to search for a user or group of users on which to perform the task. The default search screens are configured to search for users based on first name, last name, or user ID.

To change the options available on the search screen

1. In the Identity Manager user console, select Roles and Tasks, Admin Tasks, Modify Admin Task.

A search screen opens.

2. Search for and select the task that you want to modify.
3. Select the Search tab.
4. In the Search Screen field, select the ellipses (...) button.

In the Select Screen Definition field, the search screen for the task is selected.

5. Do one of the following:
 - To modify a copy of the default search screen (recommended), click Copy.

Note: If you create a copy of the default screen definition, you must change the name and tag for the screen.

- To edit the default search screen, click Edit.
6. In the section for selecting the fields that a user can search on, add or remove fields as needed.

To add a field, select the field from the list box below the existing fields, and click the plus icon.

To remove a field, click the delete button () next to the appropriate field.

Note: For the Send (Final) Reminder Notification, Certify User, and End Certification Process tasks, do not modify the certification status rules in the Show Only Objects Meeting the Following Rules section.

7. Click OK and then Select to return to the task screen.

Determine Certifiers

Certifiers are users who use the Certify User task to certify or reject user roles. Typically, a certifier is a manager.

To specify certifiers:

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Role.

Identity Manager displays a list of roles.

Note: To avoid overwriting the default Certify Manager role, create and modify a copy of the role.

2. Select the Certify Manager role.
3. Select the Members tab.
4. Add a member policy that selects the users who will act as certifiers.
5. Define a scope rule that specifies the users for which the certifier is responsible.
6. Click OK.

Configure Email Notifications

When you use any certification task, Identity Manager sends an email to certifiers about actions that the certifier must take, or actions that Identity Manager has performed. For example, when the Send Reminder Notification task is executed, Identity Manager sends a reminder to a manager that the Certify User task must be completed for an employee.

You can configure:

- When Identity Manager sends email notifications
- The users to whom Identity Manager sends email messages
- The content of the email messages

Configure When Email Notifications Are Sent

By default, Identity Manager is configured to send email notifications for the following events:

- CertificationRequiredNotification
- CertificationRequiredReminderNotification
- CertificationRequiredFinalReminderNotification
- CertificationNonCertifiedActionPendingNotification
- CertificationNonCertifiedActionCompletedNotification

If you do *not* want Identity Manager to send email notifications for these events, modify the email notification configuration in the Identity Manager Management Console.

1. In the Identity Manager Management, select the Identity Manager environment that you want to modify.
2. Click Advanced Settings, E-mail.
3. In the Event section, select the events that you do not want to trigger email notifications and click Delete.

Determine Who Receives Email Notifications

By default, Identity Manager sends email notifications to the manager of a user who requires certification.

Identity Manager uses the [USER_MANAGER notification rule](#) (see page 292) in the email templates for user certification to determine the user's manager.

Modify the Email Message

The content of the email messages that Identity Manager sends is determined by an email template, which includes static text (such as the phrase "requires certification") and variable text specific to a given context (such as the name of the user who requires certification).

You can use a default template as installed or customize it to suit your needs.

Configure Identity Manager Actions for Non-Certified Users

By default, Identity Manager disables user accounts for users who are not certified when the End Certification Process task is executed. You can modify the action that Identity Manager takes by modifying the End Certification Process task. You can configure Identity Manager to:

- Do nothing
- Disable the user (default)
- Revoke membership/administrative role rights
- Revoke membership/administrative role rights and remove provisioning accounts

To configure the End Certification Process task

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Task.

Identity Manager displays a search screen for tasks.

2. Search for and select the End Certification Process task.
3. Select the Tabs tab.

Identity Manager displays the tab that appears in the End Certification Process task.

4. Click the right arrow next to the Action Type tab.

Identity Manager displays the Configure Non-Certified User Action screen.

5. Select one of the following options:
 - Do nothing--Identity Manager takes no action.
 - Disable the user (default)--Identity Manager disables accounts of users who are not certified.
 - Revoke membership/administrative role rights--Identity Manager revokes the roles for users who are not certified.
 - Revoke membership/administrative role rights and remove user accounts--Identity Manager revokes the roles for users who are not certified, and deletes their provisioning accounts.
6. Click OK to return to the Tabs tab. Then, click Submit.

Require Approvals

For additional security, you can require a set of approvers to approve all certified roles. To require approvals, associate the CertifyRole event with a workflow approval process.

Schedule Certification Tasks

You can use a third-party scheduler to schedule certification tasks. The scheduler can invoke the tasks using the Identity Manager Task Execution Web Service (TEWS).

For more information about TEWS, see the *Programming Guide for Java*.

Start the User Certification Process

Use the Begin Certification Process task to select users that require certification. Once you select the users, Identity Manager sets the users' certification status to REQUIRES CERTIFICATION, and sends an email to the appropriate certifier, informing him that he has pending certifications.

To begin the certification process:

1. Log into an Identity Manager account that has a role, such as the Certification Process Manager role, with tasks for configuring the certification process.
2. Select Certification, Begin Certification Process.
3. Search for the users that require certification.

Identity Manager returns all of the users who match the search criteria.

By default, all of the users are selected. To deselect all of the users, select the Select check box in the header.

4. Review the list of users to be certified, and click Yes to begin the certification process.

Send Reminder Notifications

Use the Send Reminder Notification and Send Final Reminder Notification tasks to send emails to certifiers, reminding them that they have pending certifications.

To configure these tasks:

1. Log into an Identity Manager account that has a role, such as the Certification Process Manager role, with tasks for configuring the certification process.
2. In the Certification category, select one of the following tasks:
 - Send Certification Reminder Notification
 - Send Final Certification Reminder Notification

3. Search for the users that require certification.

Identity Manager returns all of the users who match the search criteria and who do *not* have the certification status CERTIFIED.

By default, all of the users are selected. To deselect all of the users, select the Select check box in the header.

4. Review the list of users to be certified, and click Yes to send the reminder notifications.

Use the Certify User Task

The Certify User task allows users, such as managers, to certify a user's admin, access, and provisioning roles. The user can be a role member or administrator.

1. Log into an Identity Manager account that has a role with tasks for certifying users.

For example, the default Certification Manager role includes the Certify User task.

2. Select Users, Certify User.
3. Search for the user to certify.
4. Select the Certify Roles tab.

Identity Manager displays the list of roles where the user is a member or an administrator.

Note: Only roles that allow administrators to add or remove members or administrators are displayed.

5. Select one of the following options for each role:
 - Certify--The user continues to be a member/administrator of the role.
 - Remove--The user is no longer a member/administrator for the role.
6. Click Submit.

End the Certification Process

Use the End Certification Process task to:

- Disable the user accounts that have the certification status: REQUIRES CERTIFICATION.
- Send notification to certifiers that the user accounts have been disabled.

Chapter 12: Workflow

The Identity Manager workflow feature allows a Identity Manager task to be controlled by a workflow process.

This section contains the following topics:

[Workflow Overview](#) (see page 217)

[Template Method](#) (see page 221)

[WorkPoint Method](#) (see page 239)

[Online Requests](#) (see page 263)

[Workflow Action Buttons](#) (see page 267)

[Work Lists and Work Items](#) (see page 272)

Workflow Overview

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

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

A workflow process consists of one or more steps, called *activities*, that must be performed in order to accomplish some business task, such as creating or modifying an employee user account. Typically, a workflow process includes one or more manual activities which require an authorized user, or participant, to approve or reject the task.

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. A *participant resolver* is a rule or set of criteria for determining who the participants are.

The individual manual activities in a workflow are called *work items* in Identity Manager.

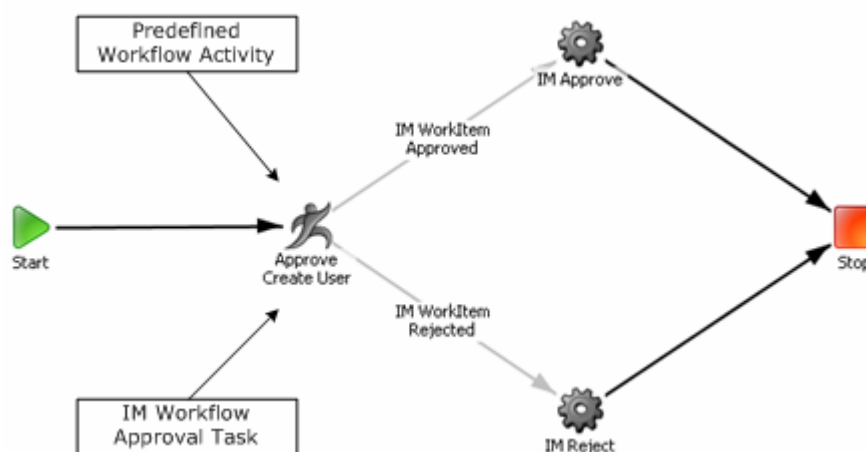
A *work list* is a workflow-generated list of approval tasks, or *work items*, that appears in the Identity Manager User Console of the participant authorized to approve the task.

WorkPoint Process Diagram

In general, Identity Manager tasks trigger Identity Manager events. For example, to create a user, an administrator selects a Create User task. When this task is initiated, the event `CreateUserEvent` is triggered.

The following diagram is an example of a simple workflow process (the predefined process `CreateUserApproveProcess`) as it appears in WorkPoint Designer. This process is invoked by a `CreateUserEvent` if the Create User task is under workflow control.

The process includes a manual activity, Approve Create User, which corresponds to an Identity Manager workflow approval task of the same name. The participant must approve or reject the approval task, typically by clicking a button in the Identity Manager User Console, before the task under workflow control can run to completion.



Workflow and Email Notification

When you initiate a task, Identity Manager submits the task for processing and displays an acknowledgement message similar to this:

Task has been submitted for processing on Friday, August 10, 2007. The status is complete.

However, if the task is under workflow control and requires approval, the message is similar to this:

Task has been submitted for processing on Friday, August 10, 2007. The status is pending.

In addition to on-screen messages, Identity Manager can automatically generate email notifications when:

- An event or task requiring approval or rejection by a workflow approver is pending.
- An approver approves an event or task.
- An approver rejects an event or task.
- An event or task is completed.

More Information:

[Email Notifications](#) (see page 283)

WorkPoint Documentation

For general information about workflow concepts and for instructions about workflow processes, activities, and jobs in WorkPoint Designer, see the WorkPoint documentation. To do so, open the following HTML page:

`<im_admin_tools_dir>\WorkPoint\docs\designer\default.htm`

where `<im_admin_tools_dir>` is the installation directory of the Identity Manager administrative tools. The default installation directory is:

- **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager
- **UNIX:** `<home_directory>/CA/IAM Suite/Identity Manager`

How to Enable Workflow

You must have workflow enabled before you can use it to control Identity Manager tasks. By default, workflow is disabled.

To enable workflow

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain_name>/idmmanage`

where `<domain_name>` is the fully qualified domain name of the server where Identity Manager is installed. For example, `myserver.mycompany.com:port`.

2. Click Environments, then select the name of the appropriate Identity Manager environment.

3. Click Advanced Settings, and then click Workflow.
4. Select the Enabled check box, and then click Save.

Note: The Event Mappings on this screen apply only if you use the WorkPoint method to configure workflow. If you use the template method (recommended), do not map events to processes using this Management Console screen.

More Information:

[Workflow Control Methods](#) (see page 220)

[Map a Process to an Event Globally](#) (see page 242)

Starting WorkPoint Designer

To start WorkPoint Designer, run the following file:

- **Windows:** <im_admin_tools_dir>\WorkPoint\bin\Designer.bat
- **UNIX:** <im_admin_tools_dir>/WorkPoint/bin/Designer.sh

where <im_admin_tools_dir> is the installation directory of the Identity Manager administrative tools. The default installation directory is:

- **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager\tools
- **UNIX:** <home_directory>/CA/IAM Suite/Identity Manager/tools

Note: You must have workflow components installed configured before you can run WorkPoint Designer. For instructions, see the *Installation Guide* for your application server.

Workflow Control Methods

Identity Manager provides two methods of placing tasks under workflow control:

Template Method

Identity Manager includes workflow process templates you can use to place tasks under workflow control. The *template method* lets you use these templates to configure and manage workflow entirely from within the Identity Manager User Console. Introduced in Identity Manager r12, these generic process templates can be configured to control most Identity Manager tasks and events.

The template method enables new features such as:

- Both task-level and event-level workflow control
- Simplified participant resolver configuration for workflow approvers
- Work item delegation, which covers “out of the office” scenarios by allowing a user to delegate another user to approve work items
- Work item reassignment, which allows a running task to be reassigned to another user for approval

WorkPoint Method

Identity Manager also includes a set of predefined workflow processes with default event mappings that correspond to specific Identity Manager tasks. The *WorkPoint method* requires you to configure and customize these processes from within WorkPoint Designer. These predefined processes are compatible with releases prior to Identity Manager r12.

Note: For greater flexibility and ease of use, CA recommends that you use the template method whenever possible.

More Information:

[Template Method](#) (see page 221)

[WorkPoint Method](#) (see page 239)

Template Method

Introduced in Identity Manager r12, the template method allows you to configure workflow process templates in the Identity Manager User Console, without having to open WorkPoint Designer.

Template method advantages are:

- Multi-stage process templates can address most workflow needs without requiring customization within WorkPoint Designer.
- Templates support both task-level and event-level workflow control.
- The same workflow process template can be configured for use with many different tasks while the process design itself remains unchanged.
- Participant resolvers can be specified easily in the User Console.
- Work item delegation can be performed in the Identity Manager User Console.

How to Use the Template Method

This section lists the high-level steps involved with placing admin tasks under workflow control using the template method. For more information about each step, see the appropriate section in this chapter.

To use the template method

1. In the Identity Manager User Console, open the Modify (or Create) Admin Task screen for the task you want under workflow control.
2. To implement task-level workflow:
 - a. On the Profile tab, click the Workflow Process button.
 - b. On the task-level workflow configuration tab, select a process template and configure participant resolvers.
3. To implement event-level workflow:
 - a. On the Events tab, select one or more events.
 - b. On the event-level workflow configuration tab, select a process template and configure participant resolvers.
4. After workflow control is configured, the user with the appropriate role performs the admin task.
5. The designated workflow participant approves or rejects the task or event.

More Information:

[Event-Level Workflow](#) (see page 228)

[Task-Level Workflow](#) (see page 226)

[Participant Resolvers: Template Method](#) (see page 231)

Process Templates

A workflow process template has the following characteristics:

- It is defined in WorkPoint Designer.
- It has manual activities, which correspond to Identity Manager approval tasks.
- It includes special attributes which contain information to identify participants (also called approvers).

Workflow process templates include no information for selecting specific participants. This is provided by Identity Manager after a user configures a workflow and its participant resolvers. This information is mapped to an event for event-level workflow control, and to a task for task-level workflow control.

When using the template method, all workflow and participant configuration is done within the Identity Manager User Console.

There are two process templates for use with the template method:

- SingleStepApproval
- TwoStageApprovalProcess

How a Process Template Works

A workflow process template contains a number of places where it requests lists of participants. When the template is mapped to an Identity Manager task or event, you need to configure participant resolvers for these lists.

At runtime, as shown in the following figure, Identity Manager provides the participant lists to the workflow process based on your configured information.

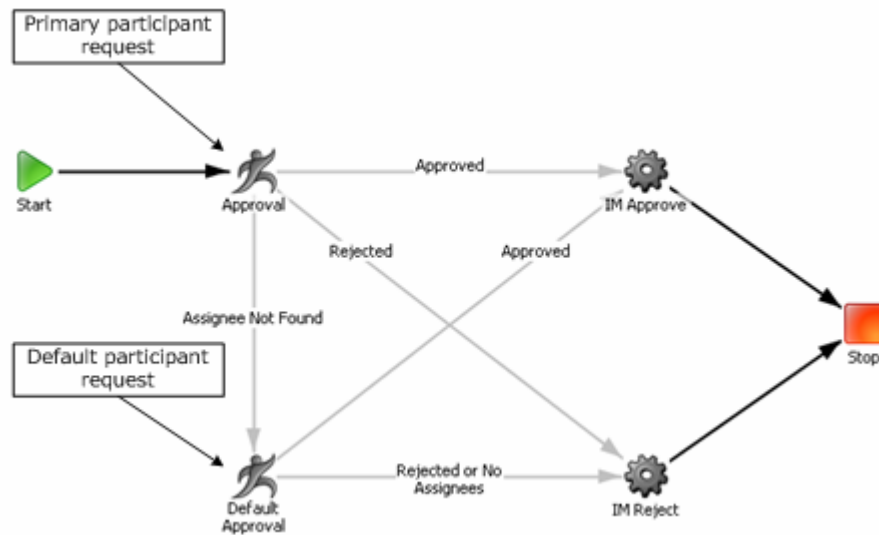


Single Stage Template Diagram

The following diagram illustrates the SingleStageApproval process template as it appears in WorkPoint Designer. The process template includes two manual activities:

- An approval node for the primary participant. If this user approves or rejects the request, the process runs to completion.

- An approval node for a default participant. This user can approve or reject the task if the primary participant is not found or fails to respond.

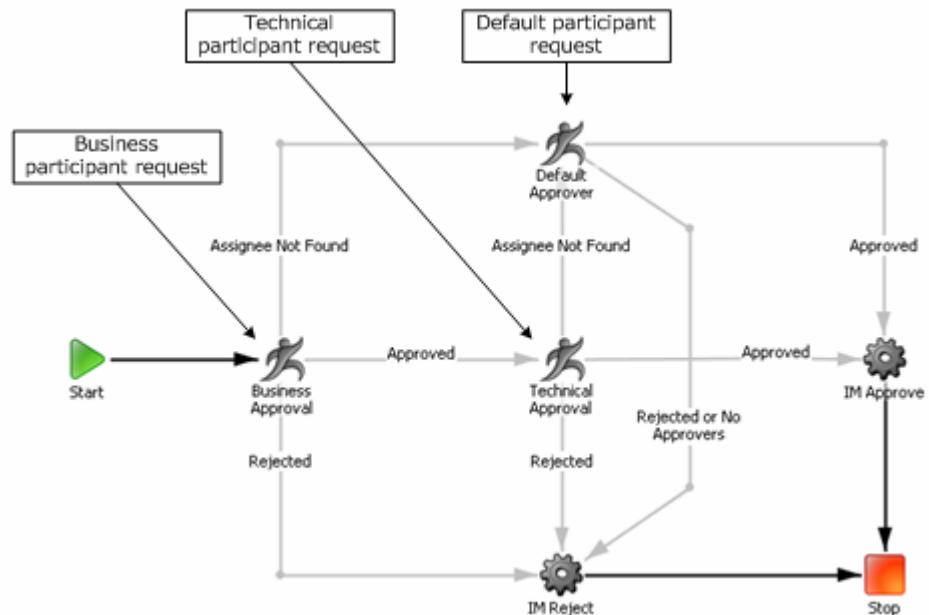


Two Stage Template Diagram

The following diagram illustrates the TwoStageApproval process template as it appears in WorkPoint Designer. The TwoStageApproval process template includes three manual activities:

- An approval node for the business participant. If this user approves or rejects the request, the process proceeds to the technical approver.
- An approval node for the technical participant. If this user approves or rejects the request, the process runs to completion.

- An approval node for a default participant. This user can approve or reject the task if either the business or technical participant is not found or fails to respond.



Process Template Attributes

Workflow processes that support the template method all have the following special user data attributes:

- **PARTICIPANT_ID**—This is unique key for the participant request. If not set, the node is not considered a participant request.
- **PARTICIPANT_NAME**—This is a friendly name for the request. It can be a text string or a localization key. If not set, the name of the WorkPoint node is used instead.
- **PARTICIPANT_DESCRIPTION**—This is a longer description of the request. It can be a text string or a localization key. If not set, the description of the WorkPoint node is used instead.

Note: These attributes are defined in the manual activity node properties in WorkPoint Designer. The attribute values are created when participant resolvers are configured from the Identity Manager User Console.

Tasks and Events

Identity Manager lets you associate workflow processes with either tasks or events. This means that participants can approve or reject either an entire Identity Manager task, or a specific event within a task.

For example, some Identity Manager tasks generate several events, and an approver may need to review all events before deciding to approve or reject a request. This is possible under task-level workflow. When a workflow process is associated with a specific event within a task, an approver cannot see the overall task context within which a request is made.

Task-Level Workflow

Task-level workflow allows approvers to review all events before deciding to approve or reject a request.

Task-level workflow occurs before any task activity is processed. No events or nested tasks execute before the workflow process job begins.

If task-level workflow is rejected, no part of the task is executed.

You configure task-level workflow mapping and participant resolvers in the Profile tab for Modify Admin Task or Create Admin Task.

Note: A task that is configured for task-level workflow control can also be configured for event-level workflow control at the same time. Concurrent event-level workflow may be applied globally or for a specific task.

More Information

[Event-Level Workflow](#) (see page 228)

[Global Process to Event Mapping](#) (see page 241)

Task-Level Process Attribute

Workflow processes that are compatible with task-level workflow all have a special attribute defined within WorkPoint Designer. This process level user data attribute, called TASK_LEVEL, is set to true by default in the following process templates:

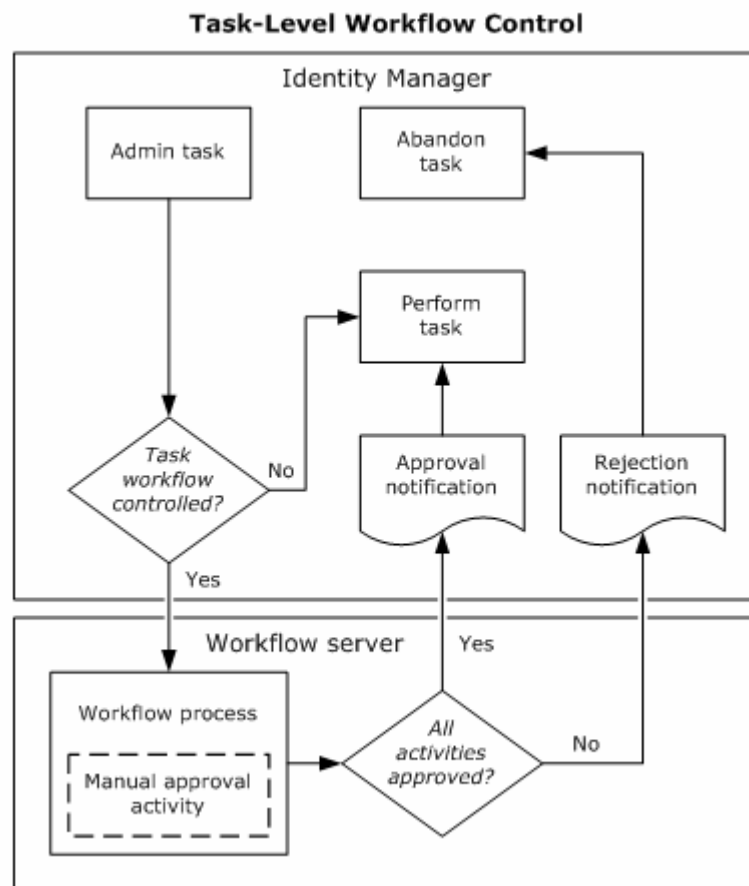
- SingleStepApproval
- TwoStageApprovalProcess

When you select an admin task for task-level workflow, only these process templates are available.

Note: Although TASK_LEVEL is set to true, the process templates can still be used for event-level workflow. Do not change this TASK_LEVEL attribute value.

Task-Level Control Diagram

The following diagram illustrates the interaction between Identity Manager and workflow server when a typical task-level workflow process is initiated.



More Information:

[Event-Level Control Diagram](#) (see page 231)

How to Configure Task-Level Workflow

Task-level workflow occurs before any task activity is processed. No events or nested tasks execute before the workflow process job begins.

To Configure Task-Level Workflow

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify (or Create) Admin Tasks.
A Select Admin Task screen appears.
2. Search for the task you want under workflow control, and click Select.
A Modify (or Create) Admin Task screen appears.
3. On the Profile tab, click the Workflow Process button.
The Task Level Workflow Configuration tab appears.
4. Select one of the following process templates from the Workflow Process list:
 - SingleStepApproval
 - TwoStageApprovalProcessThe Task Level Workflow Configuration tab expands.
5. Configure participant resolvers as required by the process template.
The participant requests are added to the process.
6. Click OK.
Identity Manager saves your task-level workflow configuration.
7. Click Submit.
Identity Manager processes the task modification.

More Information:

[Participant Resolvers: Template Method](#) (see page 231)

Event-Level Workflow

An Identity Manager event can be mapped to a workflow process. When an event that is mapped to a workflow process is triggered, the workflow process begins. The task that triggered the event is placed in a pending state and is considered under workflow control.

A workflow process may require an Identity Manager participant to approve or reject an event or task before the process can be complete. A task that requires manual workflow approval by a participant takes longer to complete than a task not under workflow control.

After all activities in a workflow process have been carried out, the event mapped to the workflow process is released from workflow control. When all events triggered by a given task are released from workflow control, the workflow-controlled task is complete.

While the task is under workflow control, the contents of the task screens are saved in the task persistence database. The workflow job state (workflow-relevant data) is stored in the WorkPoint database.

You configure event-level workflow mapping and participant resolvers in the Events tab for Modify Admin Task or Create Admin Task.

Note: The Events tab lists the events that are generated by each tab in a task. After adding a new tab to a task, you must submit the task and then reopen it using Modify Admin Task before the new events are displayed on the Events tab.

How to Configure Event-Level Workflow

Event-level workflow begins when an event that is mapped to a workflow process is triggered. The task that triggered the event is placed in a pending state until the participant approves or rejects the task.

To Configure Event-Level Workflow

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify (or Create) Admin Task.
A Select Admin Task screen appears.
2. Search for the task you want under workflow control, and click Select.
A Modify (or Create) Admin Task screen appears.
3. On the Events tab, select an event to map to a process template.
The workflow mapping screen appears.
4. Select one of the following process templates from the Workflow Process list:
 - SingleStepApproval
 - TwoStageApprovalProcessThe workflow mapping screen expands.
5. Configure participant resolvers as required by the process template.
The participant requests are added to the process.
6. Click OK.
Identity Manager saves your event-level workflow configuration.

7. Repeat steps 3 - 6 for each event you want under workflow control.
8. Click Submit.

Identity Manager processes the task modification.

Note: The Workflow Process list includes processes for use with both the template method and the WorkPoint method:

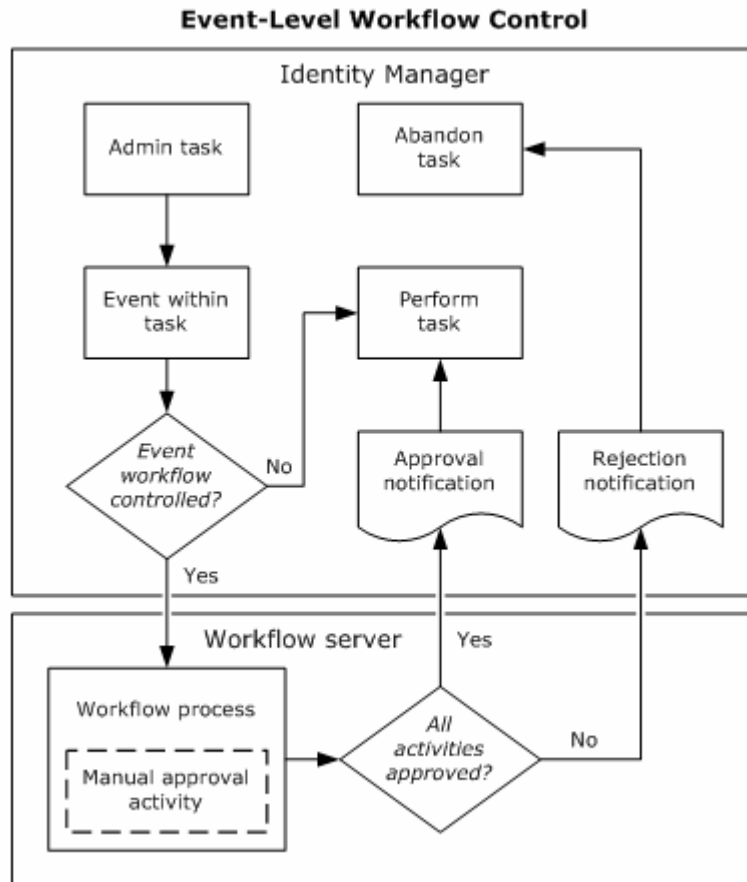
- When a template method process is selected (either SingleStepApproval or TwoStageApprovalProcess), the page expands to enable participant resolver configuration.
- When a WorkPoint method process is selected, the page does not expand. Participant resolvers are configured in WorkPoint Designer.

More Information:

[Participant Resolvers: Template Method](#) (see page 231)

Event-Level Control Diagram

The following diagram illustrates the interaction between Identity Manager and the workflow server when a typical event-level workflow process is initiated.



More Information:

[Task-Level Control Diagram](#) (see page 227)

Participant Resolvers: Template Method

To specify participants using the process template method, you define the following activity properties in the Identity Manager User Console:

- The name of the approval task
- The type of participant resolver
- Additional information as required by the participant resolver

Participant resolvers are configured on the following User Console screens:

- **Task-level workflow**—Workflow configuration screen, selected from the Modify (or Create) Admin Task Profile tab.
- **Event-level workflow**—Workflow mapping screen, selected from the Modify (or Create) Admin Task Events tab.

Types of Participant Resolvers

For the template method, there are seven types of participant resolvers:

Approval Task Role Members

Participants are members of roles that grant access to the approval task.

User List

Participants are a specified list of users.

Group Members

Participants are members of a specified list of groups.

Admin Role Members

Participants are members of a specified list of admin roles.

Admin Task Members

Participants are members of admin roles associated with a specified list of admin tasks.

Dynamic Resolver

Participants are dynamically selected depending on the task or event being approved.

Null Resolver

This resolves to a null list with no users.

Custom

Participants are determined by a custom participant resolver.

Approval Task Role Members

This resolver assigns the activity to all members of all Identity Manager roles that grant access to the approval task. This resolver requires no further configuration.

To configure an approval task role members resolver

1. On the User Console workflow configuration screen, select Approval Task Role Members from the Participant Resolver list.

The workflow configuration screen changes according to the participant resolver selection.

2. Click OK to save the participant resolver configuration.
The admin task profile tab reappears.
3. Click Submit to save your admin task workflow changes.

User List

This resolver assigns the work item to a specified list of users.

Scoping is not enforced. Any user may be added to or removed from the list by anyone who has access to the workflow configuration screen.

This resolver has the following validation rules:

- At least one user name must be provided.
- The user names must be those of a currently existing users.

To configure a user list resolver

1. On the User Console workflow configuration screen, select User List from the Participant Resolver list.
The workflow configuration screen changes according to the participant resolver selection.
2. Click Add User to add a participant to the list.
A select user screen appears.
3. Search for and select one or more participants.
The participants are added to the user list.
4. Click OK to save the participant resolver configuration.
The admin task profile tab reappears.
5. Click Submit to save your admin task workflow changes.

Group Members

This resolver assigns the work item to all members of all groups specified in the group list.

Evaluation of who the group members are is performed at the time the work item is created, not at the time the participant resolver is specified.

Scoping is not enforced. Any group may be added to or removed from the list by anyone who has access to the workflow configuration screen.

This resolver has the following validation rules:

- At least one group must be specified
- The group names must be those of currently existing groups

To configure a group members resolver

1. On the User Console workflow configuration screen, select Group Members from the Participant Resolver list.

The workflow configuration screen changes according to the participant resolver selection.

2. Click Add Groups to add a group to the list.

A select group screen appears.

3. Search for and select one or more groups.

The groups are added to the group list.

4. Click OK to save the participant resolver configuration.

The admin task profile tab reappears.

5. Click Submit to save your admin task workflow changes.

Admin Role Members

This resolver assigns the work item to all members of the admin roles specified in the admin role list.

Evaluation of who the role members are is performed at the time the work item is created, not at the time the participant resolver is specified.

Scoping is not enforced. Any role may be added to or removed from the list by anyone who has access to the workflow configuration screen.

This resolver has the following validation rules:

- At least one admin role must be specified.
- The admin role names must be those of currently existing admin roles.

To configure an admin role members resolver

1. On the User Console workflow configuration screen, select Admin Role Members from the Participant Resolver list.

The workflow configuration screen changes according to the participant resolver selection.

2. Click Add Admin Roles to add a role to the list.

A select role screen appears.

3. Search for and select one or more roles.
The roles are added to the role list.
4. Click OK to save the participant resolver configuration.
The admin task profile tab reappears.
5. Click Submit to save your admin task workflow changes.

Admin Task Members

This resolver assigns the work item to all members of all admin roles associated with the admin tasks specified in the admin task list.

Scoping is not enforced. Any task may be added to or removed from the list by anyone who has access to the workflow configuration screen.

Evaluation of who the role members are and what roles are present on the tasks is performed at the time the work item is created, not at the time the participant resolver is specified.

This resolver has the following validation rules:

- At least one admin task must be specified.
- The admin task names must be those of currently existing admin tasks.

To configure an admin task members resolver

1. On the User Console workflow configuration screen, select Admin Task Members from the Participant Resolver list.
The workflow configuration screen changes according to the participant resolver selection.
2. Click Add Admin Task to add a task to the list.
A select task screen appears.
3. Search for and select one or more tasks.
The tasks are added to the task list.
4. Click OK to save the participant resolver configuration.
The admin task profile tab reappears.
5. Click Submit to save your admin task workflow changes.

Dynamic Resolver

This resolver returns a list of users according to a dynamic rule resolved at run-time. Use the following selection to set dynamic rule constraints:

Approvers

The type of user to approve this task.

Note: This only shows those objects that can contain users (or approvers).

User or Object

The user or object where the approvers can be found.

- Object associated with the event—The event under workflow control.
- Initiator of this task—The user who initiated the admin task.
- Primary object of this task—The user being modified by the task.

Attribute

The attribute that contains the approvers.

Note: By default, this is the User ID attribute in the object.

Event Object Type

The type of object from the event.

Note: This appears only if "Object associated with the event" is selected.

Null Resolver

The null resolver returns no users. Depending on how the workflow process is designed, this can cause the process to skip the approval entirely. The null resolver requires no further configuration.

To configure a null resolver

1. On the User Console workflow configuration screen, select Null Resolver from the Participant Resolver list.

The workflow configuration screen changes according to the participant resolver selection.

2. Click OK to save the participant resolver configuration.

The admin task profile tab reappears.

3. Click Submit to save your admin task workflow changes.

Custom Participant Resolver

The custom participant resolver is a Java object that determines workflow activity participants and returns a list to Identity Manager, which then passes the list to the workflow engine. Typically, you write a custom participant resolver only if the standard participant policies cannot provide the list of participants that an activity requires.

Note: You create a custom participant resolver using the Participant Resolver API. For information, see the *Programming Guide for Java*.

To configure a custom participant resolver

1. On the User Console workflow configuration screen, select Custom: `<resolverName>` from the Participant Resolver list.

The workflow configuration screen changes according to the participant resolver selection.

2. Add input parameters as required by your custom participant resolver.
3. Click OK to save the participant resolver configuration.
The admin task profile tab reappears.
4. Click Submit to save your admin task workflow changes.

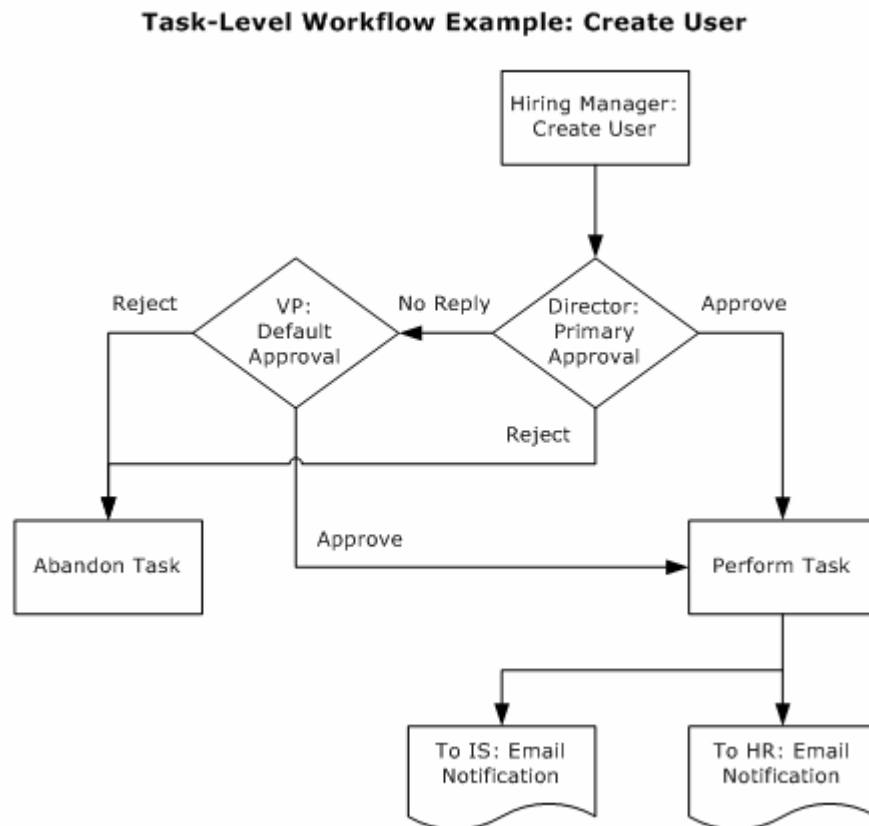
Workflow Example: Create User

A company's Identity Manager administrator needs to define a workflow and user roles to handle the following scenario:

- The company Sales Manager hires a new Sales Representative. The Sales Manager must be able to create an Identity Manager user for the new hire.
- To streamline the hiring process, the participants want to perform only a single work item to approve (or reject) the task.
- The Sales Director should be primary approver for all new hires. If the Sales Director is unable to do this for any reason, the VP of Sales should be the default approver.
- If the new hire is approved, Identity Manager should send new user email notifications to both the Human Resources (HR) and Information Services (IS) departments.

Create User Control Diagram

The following diagram illustrates the logic flow for the create user scenario:



Workflow Example Implementation

To implement this example scenario, the administrator needs to perform the following tasks:

- Ensure that the task initiator is a member of the required admin role:
The Sales Manager needs to be a member of the User Manager admin role. This role gives the Sales Manager the required authority to initiate the Create User admin task for the new hire Sales Representative.
- Enable task-level workflow for the Create User admin task:
Task-level workflow guarantees that only one work item is generated to complete the Create User task. Because there are several individual events associated with the Create User task, event-level workflow would generate several work items, and also would be harder to configure.

- Configure the participant resolvers:

The number of possible participant resolvers is determined by the selected workflow process template. The SingleStageApproval template includes primary and default approvers, other templates allow for more.

Because only this scenario requires only two individuals approvers, the User List participant resolver provides the simplest solution. This resolver allows individual approvers to be selected by name, rather than multiple users to be selected by role or group.

- Configure email notification:

The Management Console allows email notification for specific tasks and events. For this scenario, task email is enabled and email notifications are sent when the Create User task completes.

A custom email template is required to send email to the HR and IS departments with the appropriate subject line and message text.

More Information

[How to Use the Template Method](#) (see page 222)

[How to Configure Task-Level Workflow](#) (see page 228)

[Participant Resolvers: Template Method](#) (see page 231)

[Email Notifications](#) (see page 283)

WorkPoint Method

The WorkPoint method applied to Identity Manager releases prior to r12. There are 14 predefined WorkPoint workflow processes that by default are mapped to specific Identity Manager events. You must use WorkPoint Designer to configure participant resolvers and otherwise modify workflow processes.

The WorkPoint method also requires you to use the Identity Manager Management Console to map a workflow process to an approval event to place the corresponding task under workflow control at a global level within the environment.

How to Use the WorkPoint Method

This section lists the high-level steps involved with placing admin tasks under workflow control using the WorkPoint method. For more information about each step, see the appropriate section in this chapter.

Note: For greater flexibility and ease of use, CA recommends that you use the template method whenever possible.

To use the WorkPoint method

1. Do the following in the Identity Manager Management Console:
 - a. Make sure workflow is enabled.
 - b. For global event mapping, associate one or more events to the appropriate predefined workflow process. (optional)
 - c. If necessary, restart the Identity Manager environment.
2. Do the following in the Identity Manager User Console:
 - a. For task-specific event mapping, associate one or more events to the appropriate predefined workflow process. (optional)
3. Do the following in WorkPoint Designer:
 - a. Associate an approval task with a workflow process (optional).
 - b. Configure participant resolvers with a workflow process (optional).
4. Do the following in the Identity Manager User Console:
 - a. After workflow control is configured, the user with the appropriate role performs the admin task.
 - b. The designated workflow participant approves or rejects the event.

More Information:

[Mapping Processes to Events](#) (see page 241)

[Associate a Workflow Activity with an Approval Task](#) (see page 246)

[Participant Resolvers: WorkPoint Method](#) (see page 247)

WorkPoint Processes

Identity Manager includes a number of workflow processes which are predefined in WorkPoint Designer. You can use the predefined processes with their default event mappings, map the workflow processes to other events, modify workflow processes by adding or removing activities, and create new workflow processes.

Global Process to Event Mapping

This table shows the default global workflow process and event mappings, specified in the Management Console.

Important: These are global mappings. The mapped workflow process executes whenever the corresponding event is generated by any task in the environment.

Workflow Process	Mapped Event
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyIdentityPolicySetApproveProcess	ModifyIdentityPolicySetEvent
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
ModifyUserApproveProcess	ModifyUserEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Note: Workflow processes marked with an asterisk (*) are not mapped to events by default.

More Information:

[Map a Process to an Event Globally](#) (see page 242)

[Map a Process to an Event in a Specific Task](#) (see page 243)

Mapping Processes to Events

You create and modify workflow processes in WorkPoint Designer. When you create a workflow process for Identity Manager, you do so with a particular Identity Manager task in mind. The execution of this task is controlled by the workflow process.

In addition to creating the workflow process, you must also:

- Identify the event that is generated by the Identity Manager task, described in Admin Tasks and Events. You can create a workflow process for any Identity Manager task that generates an event.
- Map the workflow process to an event by doing one of the following:
 - Assign a Workflow Process to an Event Globally.

With this global mapping, the workflow process occurs whenever the event is generated in the environment, regardless of the task that generates the event.
 - Assign a Workflow Process to an Event Generated by a Specific Task.

With this task-specific mapping, the workflow process occurs only when the specified task generates the event.

Note: If you map an event to a workflow process both globally and to a specific task, the workflow process associated with the specific task takes precedence.

- Specify a participant resolver for the workflow activity in the workflow process.
- Associate a workflow activity with an approval task.

More Information:

[Map a Process to an Event Globally](#) (see page 242)

[Map a Process to an Event in a Specific Task](#) (see page 243)

[Workflow Activities](#) (see page 245)

[Participant Resolvers: WorkPoint Method](#) (see page 247)

Map a Process to an Event Globally

You map a workflow process to an event globally so the workflow process executes when the event is generated by any task in the environment.

To map a workflow process to an event globally

1. Open the Identity Manager Management Console by entering the following URL in a browser:
`http://<domain_name>/idmmanage`
where <domain_name> is the fully qualified domain name of the server where Identity Manager is installed. For example, `myserver.mycompany.com:port`.
2. Click Environments, then select the name of the appropriate Identity Manager environment.
3. Click Advanced Settings, and then click Workflow.

4. Do the following to map an event to a workflow process:
 - a. Select an event from the Event list box.
 - b. Select a workflow process from the Approve Process list box.
 - c. Click Add.
5. After you finish mapping events to workflow processes, click Save.
6. Restart the Identity Manager environment for changes to take effect.

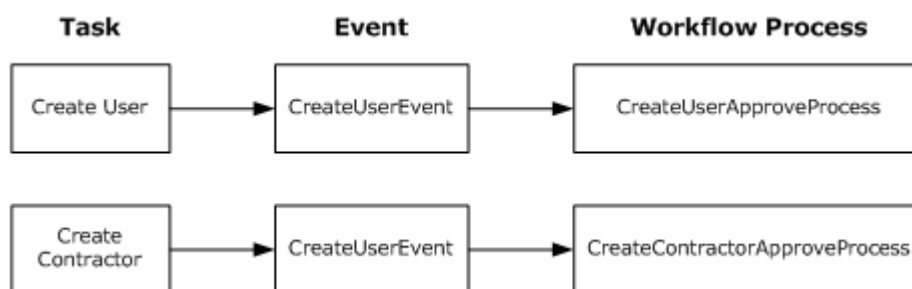
More Information:

[Global Process to Event Mapping](#) (see page 241)

Map a Process to an Event in a Specific Task

You can assign a workflow process to an event that is generated by a particular task. In this case, the workflow process occurs only when the mapped event is generated by the specified task.

Task-specific mapping provides variable control over the workflow processes that can be executed for the same event. For example, the following diagram shows two different tasks generating the same event but triggering two different workflow processes:



In this diagram, each task uses a different workflow process:

- **Create User**—This default admin task triggers CreateUserEvent, which is mapped to CreateUserApproveProcess, a default workflow process.
- **Create Contractor**—This is a custom task based on Create User. In this case, CreateUserEvent is mapped to CreateContractorApproveProcess, a custom workflow process created for approving new contractor accounts.

To map a workflow process to an event in an existing task

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for an administrator task.

3. Select a task (for example, the Modify User or Create User tasks) and click Select.
4. On the Events tab, select a workflow process for the event in the task.
Note: Workflow must be enabled for the event names and the workflow process drop-down menu to appear on this tab.
5. Using the Workflow Process drop-down menu, assign a workflow process to the event name and click OK.
6. Click Submit.
7. Open the IM Management Console and restart the Identity Manager environment for the changes to take effect.

To map a workflow process to an event in a new task

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Create Admin Task.
Note: Be sure you select an existing workflow approval task (such as Approve Create Group or Approve Create User) as the template for your new workflow approval task.
2. On the Profile tab, enter the information in the appropriate fields.
3. On the Events tab, select a workflow process for the event in the task.
Note: Workflow must be enabled for the event names and the workflow process drop-down menu to appear on this tab.
4. Using the Workflow Process drop-down menu, assign a workflow process to the event name and click OK.
5. Click Submit.
6. Open the IM Management Console and restart the Identity Manager environment for the changes to take effect.

Note: The Workflow Process list includes processes for use with both the template method and the WorkPoint method:

- When a template method process is selected (either SingleStepApproval or TwoStageApprovalProcess), the page expands to enable participant resolver configuration.
- When a WorkPoint method process is selected, the page does not expand. Participant resolvers are configured in WorkPoint Designer.

More Information:

[Global Process to Event Mapping](#) (see page 241)

Workflow Activities

Identity Manager includes a number of workflow activities that are predefined in the WorkPoint Designer. These activities are assigned to predefined workflow processes.

The predefined workflow processes are single-step processes—that is, each process contains a single predefined activity.

Each predefined activity corresponds to a workflow approval task with the same name that is predefined in Identity Manager. You can use the predefined activities in other workflow processes, and you can create new activities.

You can use the predefined workflow processes without modification or add more activities to them. For information about adding an activity to a workflow process, see the WorkPoint documentation.

Processes, Tasks, and Activities

The table below lists the predefined workflow activities and the predefined workflow process that each activity is assigned to by default.

Note: The predefined workflow activities and their corresponding workflow approval tasks have the same name.

Workflow Process	Workflow Task/Activity
CertifyRoleApprovalProcess**	Approve Certify Role
Consultation Process*	
CreateGroupApproveProcess	Approve Create Group
CreateOrganizationApproveProcess	Approve Create Organization
CreateUserApproveProcess	Approve Create User
DeleteGroupApproveProcess	Approve Delete Group
DeleteOrganizationApproveProcess	Approve Delete Organization
DeleteUserApproveProcess	Approve Delete User
ModifyAccessRoleMembershipApproveProcess	Approve Modify Access Role Membership
ModifyAdminRoleMembershipApproveProcess	Approve Modify Admin Role Membership
ModifyGroupMembershipApproveProcess	Approve Modify Group Membership

Workflow Process	Workflow Task/Activity
ModifyIdentityPolicySetApproveProcess	Approve Modify Identity Policy Set
ModifyOrganizationApproveProcess	Approve Modify Organization
ModifyUserApproveProcess	Approve Modify User
SelfRegistrationApproveProcess	Approve Self Registration
SingleStepApproval*	
TwoStageApprovalProcess*	

Note: Workflow processes marked with one asterisk (*) are designed for use with the template method. They are configured in the User Console, and therefore have no default associated tasks or activities. The CertifyRoleApprovalProcess (**) is a sample process demonstrating a custom participant resolver.

Associate a Workflow Activity with an Approval Task

To associate a workflow activity with a workflow approval task, you define a name/value pair in WorkPoint Designer.

Note: If a name/value pair is not defined for a workflow activity, by default Identity Manager uses a task with a name that matches the approval task.

To associate a workflow activity with an approval task

1. Start WorkPoint Designer.
2. Click File, Open, Process.
3. Select a workflow process and click Open.
4. Right click the activity node in the process, and click Properties.
5. Enter the following in the User Data tab:
 - **Name**—TASK_TAG.
 - **Value**—Approval Task Tag name.
6. Click Add.
7. Click OK to save your changes.

Participant Resolvers: WorkPoint Method

To specify participants using the WorkPoint method, you define the following activity properties in WorkPoint Designer:

- The name of the predefined Identity Manager script which enables communication between Identity Manager and the workflow server. The script issues a request to Identity Manager for activity participants, and then supplies that list to the workflow server.
- References to one or more participant resolvers.

Types of Participant Resolvers

Rather than entering a specific list of participants in workflow activity properties, the participants are referenced by an arbitrary name that is mapped to a *participant resolver*.

For the predefined process model, there are four types of participant resolvers:

Role Participant Resolver

Participants are members of a particular role.

Group Participant Resolver

Participants are members of a particular group.

Custom Participant Resolver

Participants are determined by a custom participant resolver.

Filter Participant Resolver

Participants are selected through a search filter.

Role Participant Resolvers

With role type participant resolvers, Identity Manager retrieves all of the members for that role and returns those members as participants.

If no resolver type is specified in the UserData parameter of the Activity dialog box, the role type resolver is used by default.

If you do not specify any participant resolvers in the User Data tab of the WorkPoint Activity Properties dialog box, by default, Identity Manager finds all available roles containing this approval task and returns back those role members as participants.

To configure Role Participant Resolvers

1. Start WorkPoint Designer.
2. Click File, Open, Process.

3. Select a workflow process and click Open.
4. Right click the activity node in the process, and click Properties.
5. Enter the following in the User Data tab:
 - **Name**—APPROVER_ROLE_NAME
 - **Value**—The name of an Identity Manager role (for example, Security Manager)
6. Click Add.

Note: This role does not need to contain any approval tasks.
7. In the User Data tab, enter the following name/value pair (optional):

Value—APPROVERS_REQUIRED

Value—YES.
8. Click Add.

Note: The default approval setting is APPROVERS_REQUIRED=NO. In this case, an activity is approved automatically if no participants are found.

If APPROVERS_REQUIRED=YES and Identity Manager can find no participants, the activity cannot be successfully completed.
9. Click OK to save your changes.

Group Participant Resolvers

With group type participant resolvers, Identity Manager retrieves all of the members for that group and returns those members as participants.

To configure Group Participant Resolvers

1. Start WorkPoint Designer.
2. Click File, Open, Process.
3. Select a workflow process and click Open.
4. Right click the activity node in the process, and click Properties.
5. Enter the following in the User Data tab:
 - **Name**—APPROVER_GROUP_UNIQUENAME
 - **Value**—The name of an Identity Manager group
6. Click Add.
7. In the User Data tab, enter the following name/value pair (optional):
 - **Name**—APPROVERS_REQUIRED
 - **Value**—YES.
8. Click Add.

Note: The default approval setting is APPROVERS_REQUIRED=NO. In this case, an activity is approved automatically if no participants are found.

If APPROVERS_REQUIRED=YES and Identity Manager can find no participants, the activity cannot be successfully completed.

9. Click OK to save your changes.

Custom Participant Resolvers

The custom participant resolver is a Java object that determines workflow activity participants and returns a list to Identity Manager, which then passes the list to the workflow engine. Typically, you write a custom participant resolver only if the standard participant policies cannot provide the list of participants that an activity requires.

Note: You create a custom participant resolver using the Participant Resolver API. For information, see the *Programming Guide for Java*.

To Configure a Custom Participant Resolver

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain_name>/idmmanage`

where <domain_name> is the fully qualified domain name of the server where Identity Manager is installed. For example, myserver.mycompany.com:port.

2. Click Environments, then select the name of the appropriate Identity Manager environment.
3. Click Advanced Settings, and then click Workflow Participant Resolver.
4. On the WorkFlow Participant Resolver screen, click New and enter:
 - **Name**—Custom participant resolver name. For example:
APPROVER_CUSTOMRESOLVER_NAME
 - **Description**—A description of the custom participant resolver.
 - **Class**—The Java class name. For example:
com.netegrity.samples.GroupFinder
5. Click Save.
6. Start WorkPoint Designer.
7. Click File, Open, Process.
8. Select a workflow process and click Open.
9. Right click the activity node in the process, and click Properties.

10. Enter the following in the User Data tab:

- **Name**—The custom participant resolver name. This must match the name you entered on the Custom Type Participant Resolver screen in the Identity Manager Management Console, for example:

APPROVER_CUSTOMRESOLVER_NAME

- **Value**—A unique name for the custom resolver. For example, GroupFinder.

11. Click Add.

Note: The default approval setting is APPROVERS_REQUIRED=NO. In this case, an activity is approved automatically if no participants are found.

If APPROVERS_REQUIRED=YES and Identity Manager can find no participants, the activity cannot be successfully completed.

12. Click OK to save your changes.

Filter Participant Resolvers

A filter participant resolver enables Identity Manager to search for users or groups that match the filter criteria. You specify a search filter in WorkPoint Designer, and Identity Manager returns matching approvers for the corresponding workflow activity.

You create a filter participant resolver on the User Data tab of the WorkPoint Activity Properties dialog box.

Participant Resolvers Filter Syntax

There are three required attributes that combine to make a search filter:

- Approver attribute (for example, title)
- Approver attribute operation (for example, equals)
- Approver attribute value (for example, manager)

The required search filter attributes combine together in the following order:

<attribute> <operation> <value>

For example:

“title equals manager” or “department contains payroll”

Required Participant Resolver Filter Attributes

The following are required participant resolver filter attributes.

Note: For each filter, n is a positive integer indicating the search filter number. The default is 1.

APPROVER_FILTER_n_ATTRIBUTE

The approver attribute. For example, Title, Department, User ID. (Approver attribute name strings must match Identity Manager user attribute name strings.)

Required: Yes

APPROVER_FILTER_n_OP

The operation associated with the approver attribute. For example, equals, not_equals, or contains. (Operation keywords are not case-sensitive.)

Valid entries for this filter are:

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

Required: Yes

APPROVER_FILTER_n_VALUE

The value associated with the approver. For example, manager, payroll, engineering.

Required: Yes

Optional Participant Resolver Filter Attributes

The following are optional participant resolver filter attributes.

APPROVER_OBJECTTYPE

USER or GROUP (not case-sensitive)

The default is USER.

Required: No

APPROVER_ORG_UNIQUENAME

A unique name for an approver's organization. (Organization name strings must match Identity Manager organization name strings.)

The default is root.

Required: No

APPROVER_ORG_AND_LOWER

The approver's organization or sub-organizations:

- 0 means search in the approver's organization.
- 1 means search in all sub-organizations of the approver's organization.

The default is 1.

Required: No

APPROVER_FILTER_NO

The number of search filter that you are using. If you have two filters, then this number would be 2.

The default is 1.

Required: Yes, if the number of filters is greater than one. No, if there is only one filter.

APPROVER_FILTER_n_CONJ_TYPE

You can combine search filters using OR or AND conjunction types. For example, you can specify the AND conjunction type if you are searching for "title equals manager" AND "department equals development."

Note: n is a positive integer greater than 1 indicating the search filter number.

Note: Filters separated by the OR conjunction take precedence over those separated by AND.

Required: No

Add a Participant Resolver Filter

To configure Participant Resolver Filters

1. Start WorkPoint Designer.
2. Click File, Open, Process.
3. Select a workflow process and click Open.
4. Right click the activity node in the process, and click Properties.

5. Enter the following in the User Data tab:

- **Name**—APPROVER_FILTER_1_ATTRIBUTE
- **Value**—A unique role identifier (for example, title).

6. Click Add.

7. Repeat steps 5 and 6 for each attribute in the search filter.

Note: The default approval setting is APPROVERS_REQUIRED=NO. In this case, an activity is approved automatically if no participants are found.

If APPROVERS_REQUIRED=YES and Identity Manager can find no participants, the activity cannot be successfully completed.

8. Click OK to save your changes.

Example: Filter Participant Resolver

The user store in the following table contains four users—Holly, Sarah, John, and Dave—with user ID, job title, and department attributes.

User	ID	Title	Department
Holly	admin1	sysadmin	administration
Sarah	test1	sysadmin	development
John	admin2	manager	development
Dave	admin3	sysadmin	accounting

Identity Manager applies the three filters defined in the following table against the preceding user store:

Name	Value
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	equals
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	department
APPROVER_FILTER_2_OP	equals
APPROVER_FILTER_2_VALUE	administration
APPROVER_FILTER_3_CONJ_TYPE	OR

Name	Value
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	equals
APPROVER_FILTER_3_VALUE	sysadmin

Identity Manager applies the filters in the following sequence:

1. Evaluates the second and third filters connected by the OR conjunction:
"department equals administration" OR "title equals sysadmin"
This excludes John and returns Holly, Sarah, and Dave.
2. Evaluates the first and second filters connected by the AND conjunction
(where * is a wild card character:
"uid equals admin*" AND "department equals administration"
This excludes Sarah, and returns Holly and Dave.

The final users returned from the user store are Holly and Dave.

Participant Resolver Order of Precedence

If you do not specify any participant resolvers, by default Identity Manager identifies all available roles containing the approval task and returns those role members as participants.

If you specify more than one participant resolver, Identity Manager evaluates them using this order of precedence:

1. Custom
2. Role
3. Filter
4. Group

Identity Manager identifies and applies the first resolver in this order of precedence, and ignores any subsequent remaining resolvers.

You should only have one resolver at a time. Also, make sure that the resolver is configured properly so that Identity Manager correctly identifies participants.

Specify Workflow Resource Script

Identity Manager is shipped with a script, named IM Approvers, that passes information between Identity Manager and the workflow server.

When a list of participants is required for a workflow activity, the script passes to Identity Manager the activity name, the participant identifier provided on the User Data tab of the WorkPoint Activity Properties dialog box, and any other information provided on the User Data tab. Identity Manager searches for the participants and passes the list back to the script. The script then provides the list to the workflow server.

When you have a new workflow process definition and the workflow process activity is an Identity Manager workflow approval task, the IM Approvers script must be specified in the Resources tab of the WorkPoint Activity Properties dialog box.

To specify the IM Approvers script in WorkPoint Designer

1. In the Resources tab, click Select.
2. In the Select Resources dialog box, select Rule from the drop-down list. This action lists the rules (scripts) that you can associate with the activity.
3. Select the script name IM Approvers and click Add.
4. Click OK, and then click Apply on the Activity Properties dialog box.

Note: Do not modify the IM Approvers script.

Specify Participants for Certify User Tasks

Certify User tasks generate the event CertifyRoleEvent. This event can be subject to workflow approval through the predefined process CertifyRoleApproveProcess.

Identity Manager also includes the predefined participant resolver CertifyRoleParticipantResolver, which appears in your environment by default. Participants for activities in a CertifyRoleApprovalProcess are specified through CertifyRoleParticipantResolver.

To provide participant configuration information

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain_name>/idmmanage`

where <domain_name> is the fully qualified domain name of the server where Identity Manager is installed. For example, myserver.mycompany.com:port.

2. Click Environments, then select the name of the appropriate Identity Manager environment.
3. Click Advanced Settings and then click Miscellaneous.
4. Define name/value pairs that specify the approvers for each role to be certified:
 - In the Property field, use the format: *role-type.role-name*
role-type must be one of these roles: admin, access, provisioning.
role-name is the name of any existing role.
The role-name and role-type must be separated by a period (.).
 - In the Value field, specify the IDs of the approvers, and separate the IDs with a semi-colon (;).

In the following example, user certification can be approved for the following roles and by the following participants:

- jsmith01 and ajones19 can approve certification for the User Manager role
- plewis12 is the only approver for the System Manager role
- rtrevor8 and pkitt3 can approve certification for My Access Role

Property	Value
admin.User Manager	jsmith01;ajones19
admin.System Manager	plewis12
access.My Access Role	rtrevor8;pkitt3

Note: Any unspecified roles will not have approvers for a CertifyRoleEvent.

Processes in WorkPoint Designer

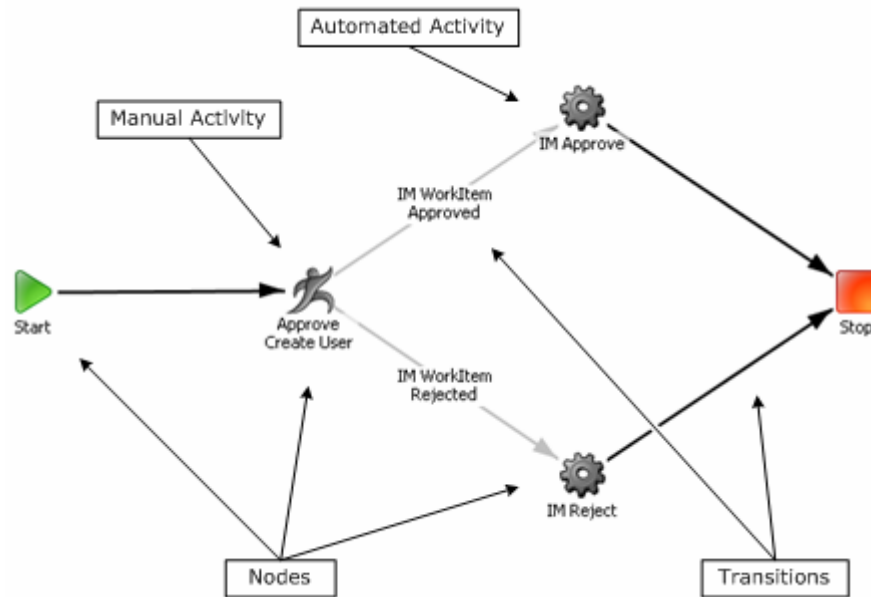
In WorkPoint Designer, you can customize the default workflow processes and activities that come with Identity Manager, and you can create new ones.

This document presents WorkPoint workflow information that is specific to Identity Manager. For complete information, see the WorkPoint Designer documentation.

Note: When creating a workflow process, consider doing so by making a copy of an existing Identity Manager process, and then modifying the new process to suit your needs. A workflow process created in this way includes default Identity Manager-specific elements and nodes such as transition scripts and automated activities.

WorkPoint Process Diagram

The following diagram shows a typical workflow process with the minimum set of components for a process that controls an Identity Manager task. The diagram illustrates the predefined process `CreateUserApproveProcess`, which controls the execution of a Create User task.



WorkPoint Process Components

The workflow process contains the following nodes and transitions:

Start

Every workflow process begins with this node.

Stop

Every workflow process ends with this node.

Manual activity

A manual activity requires the approval or rejection of an Identity Manager task by a participant, and must have the same name as an Identity Manager workflow approval task.

A workflow process that controls an Identity Manager task must include at least one manual activity requesting approval for that task.

Automated activity

An automated activity is assigned one of two scripts:

- **Notify IM Approve**—Informs Identity Manager to execute the Identity Manager task under workflow control.
- **Notify IM Reject**—Informs Identity Manager to cancel execution of the Identity Manager task.

In general, the Notify IM Approve script is activated if all manual activities are approved, and the Notify IM Reject script is activated if any manual activity is rejected.

Unconditional transition

An unconditional transition is a path from one node in the workflow process to another, and is not associated with a condition script.

Conditional transition

A conditional transition represents is an alternative path from one node in the workflow process to another, and is associated with a condition script.

A condition script determines whether the transition occurs by evaluating the outcome of the associated activity. If the script returns true, the transition is performed and the process moves to the next indicated node.

It is possible to have two or more condition scripts return true. This allows an activity to be performed in parallel, since each script is associated with a different transition.

Note: You can use custom scripts in conditional transitions. For instructions, see the *Programming Guide for Java*.

Manual Activity Properties

Property settings specific to Identity Manager are listed in the following table. These settings are defined in the specified tabs of the WorkPoint Designer Activity Properties dialog box.

Property Tab	Property Descriptions
Resources	IM Approvers—Specified in the Include list. This script passes information between Identity Manager and the workflow server.
Agents	Nobody Auto Complete—Specified in the Asynchronous list and associated with the Available state. This script determines whether an activity should be considered approved if no activity participants exist.

Property Tab	Property Descriptions
User Data	Define name/value pairs that Identity Manager uses to retrieve activity participants. Optionally, you can also define data to be passed to a custom participant resolver.

Conditional Transition Properties

The following default scripts appear in the in the Condition tab of the Transition Properties dialog box:

IM WorkItem Approved

Returns true if the associated activity is approved. The workflow process flows to the next node indicated by the transition.

IM WorkItem Rejected

Returns true if the associated activity is rejected. The workflow process flows to the next node indicated by the transition.

Jobs and Process Instances

A *workflow process* defines the steps that must take place before Identity Manager can complete a particular task. A *job* is a runtime instance of a workflow process.

For example, the default workflow process `CreateUserApproveProcess` defines the steps that must occur for a new user to be approved. When a new user is actually created in Identity Manager and the task is submitted for approval, a job instance of `CreateUserApproveProcess` is created in WorkPoint Designer.

You can open, view, and modify jobs in WorkPoint Designer using an interface that is very similar to that used for editing workflow processes.

Multiple jobs based on the same process can exist simultaneously.

Filtering Jobs

WorkPoint Designer includes filtering, which lets you search for jobs based on various criteria. For example, you can search for jobs that:

- Are based on one or more selected workflow processes
- Have a user-defined job reference or a unique job ID

- Are in a particular state (such as active, complete, or suspended)
- Were created or were started within a specified date range

Note: For instructions and reference information about job filtering, see the WorkPoint Designer documentation.

Job Status and Properties

When you open a job, the job's workflow diagram is displayed. Workflow activity nodes and transitions are rendered in color indicating whether that have been performed.

You can view, and in some cases modify:

- Properties of a job, including participant and job history information
- The state of an open job, for example whether it has completed
- Properties of individual nodes and transitions in a job

Activity and Work Item Properties

You can view, and in some cases, modify job activity properties and process activity properties, including the following:

- Activity state information
- Activity approval information
- Approval task (called *work item* in WorkPoint Designer) information, for example:
 - If no participant has the work item reserved (which removes the item from the work lists of other approvers), the state is Available, and no participant user ID is displayed.
 - If a participant has reserved but not yet completed the work item, the state is Open, and the participant's user ID and the reservation time are displayed.
 - If the work item has been completed, the state is Complete. The user ID of the participant who approved or rejected the task under workflow control is displayed, along with the time of completion.

Specific work item properties include:

- The work item name and current state
- State history information, including the user IDs of the participants responsible for given states
- Authorized work item participants information

Note: For more information about job, activity, and work item properties, see the WorkPoint Designer documentation.

Performing Workflow Activities

In a workflow process, a manual activity is performed by a person designated as an activity participant, who approves or rejects an event associated with an approval task. Participants perform this activity in Identity Manager.

The following operations take place when an activity associated with an Identity Manager approval task is performed:

1. Identity Manager notifies the participants.
2. A participant approves or rejects the task.
3. The workflow server completes the activity.

Find and Notify the Participants

When a workflow activity associated with an Identity Manager approval task begins, the workflow server passes information about activity participants to Identity Manager. This information is defined in the activity properties. Identity Manager uses this information to retrieve activity participants and alert them that an approval task is pending.

After identifying the participants, Identity Manager adds a new work item (the approval task) to each participant's work list. Optionally, Identity Manager also sends an email notification about the new work item to each participant.

Note: If the APPROVERS_REQUIRED activity property is set to false and no participants are found, the task is considered approved by default.

Note: A circle in the Status column indicates that the approval task is available for any participant to claim. A check mark indicates that the work list owner has accepted the approval task but has not yet completed it.

Accept and Perform the Approval Task

Once participants are found, the activity cannot be completed until one participant accepts the approval task and either approves or rejects the task under workflow control.

A participant accepts an approval task by clicking the work item name in the Workflow Activity Console, and then clicking Reserve Item. (Reserving an item removes it from the work lists of other approvers.)

Once a participant accepts an approval task, he commits to making the approval or rejection decision for the task under workflow control. And, since multiple participants cannot accept the same approval task, the approval task is removed from the work lists of other participants.

After a participant accepts an approval task, an approval screen appears, in which the participant can take one of these actions:

- Approve or reject the task under workflow control immediately.
- Release the approval task to make it available to other participants.
- Close the dialog box and complete the activity later. To reopen the Approve Create User dialog box shown above, the participant clicks the name of the approval task in his work list.

Additionally, the participant can update one or more modifiable fields, if any, on the approval screen. You can make fields on this screen modifiable when you create the task.

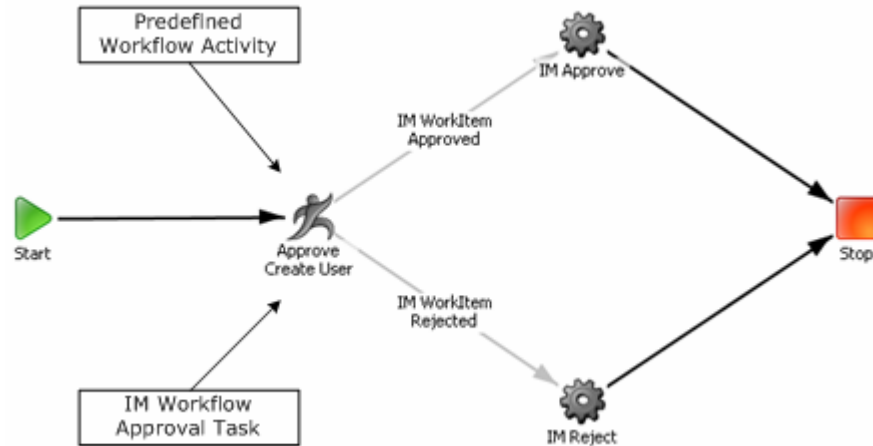
After the participant approves or rejects the task under workflow control, the activity is complete, and the workflow process can continue along the path determined by the outcome of the activity, as described in the next section.

Workflow Server Completes the Activity

A manual activity appears in the Designer window with two or more conditional transitions leading from it.

Each conditional transition is associated with a script. When a participant completes the activity, the scripts evaluate the activity outcome. The result of these evaluations determines the direction of the process flow.

The following illustration shows the Approve Create User activity in the Designer and the corresponding approval task of the same name in Identity Manager.



When the activity participant (or approver) clicks the Approve or Reject button in Identity Manager:

1. The Approve Create User activity in the process job instance ends. The scripts associated with the conditional transitions evaluate the outcome of the activity.
2. The job instance continues, depending on which conditional transition evaluates to true:
 - If the activity is approved, script IM WorkItem Approved returns true. The workflow takes the IM WorkItem Approved transition to the next node. This automated activity, IM Approve, notifies Identity Manager to execute the Create User task.
 - If the activity is rejected, script IM WorkItem Rejected returns true. The workflow takes the IM WorkItem Rejected transition to the next workflow node. This automated activity, IM Reject, notifies Identity Manager to cancel the Create User task.

Online Requests

Identity Manager lets you create general purpose online request tasks. The default online request implementation is comprised of a set of related tasks for both self-modification requests and administrative user modification requests. However, the online request feature could easily be implemented for other Identity Manager request tasks.

A user modification request triggers a workflow process which generates a work item. Workflow participants can either approve and implement the work item, or reject it. The user initiating the task enters a description of the request in the history editor, a text area which Identity Manager uses to maintain a history of the request. This history editor can be configured to allow participants to leave comments about the action they perform on the work item. These comments become part of the cumulative work item history.

New actions in addition to (or in place of) the standard approve and reject actions are also possible. For example, a business participant can clarify or comment on the request, and a technical participant can implement the request. These new activities can be represented by new workflow action buttons like "Clarify" and "Implement" which you can add to the standard "Approve" and "Reject" buttons on the approval task.

Online Request Tasks

There are five tasks that work together to make up the default online request implementation. These tasks demonstrate the use of custom requests, history, and workflow action buttons:

Note: The admin tasks (Change My Account and Create Online Request) are configured by default for event-level workflow using the Consultation Process template.

Change My Account

This is a self-modification admin task that creates a user account change request. It has a Request tab with a history editor for describing the request, and a Profile tab with read-only user details.

Create Online Request

This is a user modification admin task that creates an account change request for a particular user. It has a Request tab with a history editor for describing the request, and a Subject Profile tab with read-only user details.

Approve Online Request

This is an approval task that allows the business participant to approve or reject the task, or to request further clarification of the task. This task has a Request tab with a history display and a history editor for queries or comments, a read-only Subject Profile tab, and an Assignees tab.

Clarify Online Request

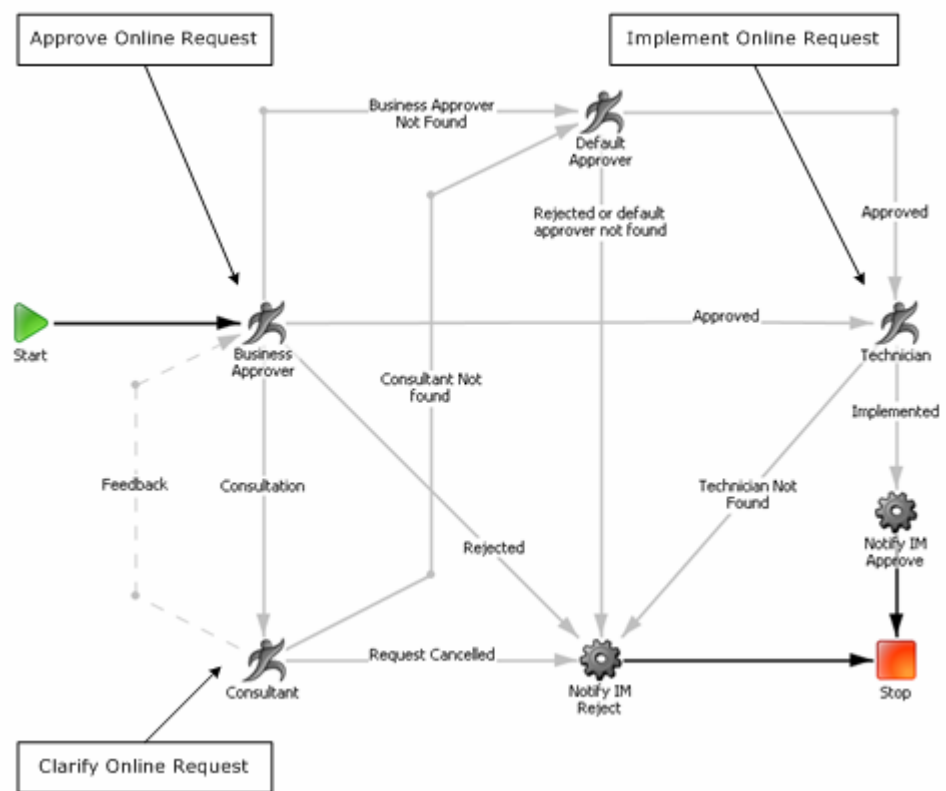
This is an approval task that allows the clarifying participant to respond to a clarification request, and sends the task back to the business participant for approval. It has a Request tab with a history display and a history editor for comments, and a read-only Subject Profile tab.

Implement Online Request

This is an approval task that allows the technical participant to implement the task and to add a comment to the task history. It has an Implement Request tab with a history display and a history editor for comments, a read-only Subject Profile tab, and an Assignees tab.

Online Request Process

The online request tasks are controlled by a workflow process template called Consultation Process, shown as it appears in WorkPoint Designer:



The Consultation Process includes four manual activities which correspond to approval tasks in the online request implementation:

- An activity for the business approver, who rejects the work item, approves the work item and passes it on to the technician, or requests further clarification from the consultant.
- An activity for the consultant, who clarifies the work item and sends it back to the business approver.

- An activity for a default approver, who takes over if either the business approver or consultant cannot be contacted.
- An activity for the technician, who implements the request and completes the work item.

Online Request History

The online request history feature allows participants to create a record of work item actions. As responsibility for the work item passes from one participant to another, the new participant is able to review work item history before taking action.

Two controls are used to implement online request history:

- The history display is a read-only table containing details of previous history entries in chronological order.
- The history editor is a text box for creating new history entries. It also has an optional button for adding multiple entries without submitting the work item.

By default, the history editor and history display appear on the Request tabs for all tasks associated with the online request implementation. The following screen illustrates the history controls in the Clarify Online Request task:

The screenshot shows the 'Clarify Request' tab selected. Below the tabs, there is a text area for user comments. Below that, the 'Request, and history:' section contains a table with three columns: Source, Description, and Time. The table lists three entries. Below the table, the 'Additional Information:' section contains a text box labeled 'History Editor' and a button 'Add History Event'. To the right of the text box is a 'History Display' label with an arrow pointing to the table. At the bottom, there are four buttons: 'Return', 'Cancel the request', 'Reserve Item', and 'Close'.

Source	Description	Time
User comment by superadmin (Super Admin), acting as Requester	Promote "SalesDir" to "SalesVP"	2007-11-01 12:13:46.28
User comment by SalesMgr (Sales Manager), acting as Approver	Why not "SalesVeep" instead?	2007-11-01 12:15:05.967
User comment by SalesCon (Sales Consultant), acting as Initiator	OK, let's go with "SalesVeep".	2007-11-01 12:19:16.813

Using Online Requests

The following steps describe the online request workflow process. For each step, the generated IM task appears in parentheses. At every step in the process, the participant can add a comment in the history editor. This comment appears in the history display to the next participant in the workflow process.

1. The Task Initiator requests a modification to an IM user (Create Online Request).
2. The Business Approver receives a work item, and does one of the following:
 - Approves the work item (Approve Online Request).
 - Rejects the work item and terminates the workflow process. No new task is generated.
 - Requests a clarification from the consultant (Clarify Online Request).
3. The Consultant receives a work item, and does one of the following:
 - Adds a clarification and returns the work item to the Business Approver. No new task is generated.
 - Cancels the work item and terminates the workflow process. No new task is generated.
4. The Technician receives a work item, and implements the request (Implement Online Request).

Workflow Action Buttons

Approval tasks in Identity Manager historically have Approve and Reject action buttons that appear on their corresponding work item screens. Workflow action buttons allow administrators to extend the functionality of Identity Manager tasks and workflows by adding action buttons to approval tasks, and by removing or modifying existing buttons. (The standard Approve and Reject buttons are implemented in the same manner as custom workflow action buttons.)

For example, a workflow process might require an action that allows mid-level participants to escalate certain cases to a more senior participant for final approval or rejection. These mid-level participants could add a comment or recommendation using the history editor, and then send the work item to the senior participant to review and approve or reject.

Adding or removing workflow action buttons requires appropriate changes to the WorkPoint workflow process that provides the business logic for handling these new actions.

More Information:

[Workflow Buttons in Approval Tasks](#) (see page 268)

[Button Configuration In Identity Manager](#) (see page 269)

[Button Configuration in WorkPoint Designer](#) (see page 271)

Workflow Buttons in Approval Tasks

Workflow action buttons correspond to transition nodes pointing away from manual activity nodes on a WorkPoint process diagram. For example, in the Consultation Process, the Technician activity node has a single transition called Implemented. This corresponds to the "Implemented" button on the Implement Online Request approval task, shown in the following figure:

Implement Request | Subject Profile | Assignees

The request described here for changes to the user whose profile is provided has been approved and should now be enacted. Please launch tasks using the provided buttons to implement this request. When this is done, please click 'implemented' to close out the request.

Request, and history:

Source	Description	▲Time
User comment by superadmin (Super Admin), acting as Requester	Change to Sales Rep Australian.	2007-10-17 11:31:01.267
User comment by SalesCon (Sales Consultant), acting as Requester	We need an Aussie rep, so she's moving to Sydney.	2007-10-17 11:35:01.343
User comment by NeteTech (NeteAuto TechSupport), acting as Implementer	Does she cover New Zealand too?	2007-10-23 17:31:50.877

Comments

The SalesRepAsia user account has been implemented as requested.

Add

Use these tasks to implement this request:

Workflow Action Button → **Implemented** Reserve Item Close

Note: The "Reserve Item" and "Close" buttons are governed by Identity Manager programming logic and are not under workflow control.

More Information:

[Workflow Action Buttons](#) (see page 267)

[Button Configuration In Identity Manager](#) (see page 269)

Button Configuration In Identity Manager

To configure a workflow action button, click the button named Workflow Action Buttons on the Profile tab of an Approval task. The following button Profile tab appears:

The screenshot shows the 'Modify Admin Task: Implement User Modification Request' window. The 'Profile' tab is selected, displaying a table of workflow action buttons. The table has four columns: Display Name, Action, Tool Tip, and Description. A single row is visible with the values 'pel.button.implemented', 'implemented', 'implemented.description', and 'implemented.description'. Below the table are buttons for 'Add Button', 'Reset Buttons', 'OK', and 'Cancel'.

Display Name	Action	Tool Tip	Description
pel.button.implemented	implemented	implemented.description	implemented.description

The button Profile tab has a table with a row for each workflow action button. Each button row has the following four properties, which correspond to columns in the table:

Display Name

The name that appears on the button in the approval screen. This is a conditionally localized value, which can be either a string or a key for a localized string in a resource file.

Action

The value passed back to the workflow process when the option is selected. This value is an attribute of the corresponding transition node in the WorkPoint process diagram. This is a non-localized string. The default settings are "approved" and "rejected".

Tool Tip

A short description (or tool tip) of the button action which appears when a user hovers the mouse cursor over the button. This is a conditionally localized value, which can be either a string or a key for a localized string in a resource file.

Long Description

A longer description of the button action which adds a message describing the action on the "View Submitted Task" screen. If this is blank, the message displayed on the "View Submitted Task" screen is the button name. This is a conditionally localized value, which can be either a string or a key for a localized string in a resource file.

More Information:

[Button Configuration in WorkPoint Designer](#) (see page 271)

Adding Workflow Action Buttons

To add a new button to an existing workflow process, perform the following high-level steps:

1. Add the workflow button in Identity Manager.

For instructions, see [How to Add a Workflow Action Button](#) (see page 270).

2. If necessary, add localization keys.

For instructions, see the *Configuration Guide*.

3. Add any new required nodes in WorkPoint Designer.

For instructions, see the WorkPoint Designer online help.

4. Define a script in the WorkPoint Designer transition node.

For instructions, see [Button Configuration in WorkPoint Designer](#) (see page 271).

More Information:

[How to Add a Workflow Action Button](#) (see page 270)

[Button Configuration in WorkPoint Designer](#) (see page 271)

How to Add a Workflow Action Button

You can add workflow action buttons to approval tasks in Identity Manager.

To add a workflow action button to an admin task

1. In the Identity Manager User Console, select Roles and Tasks, Admin Tasks, Modify Admin Task.

The Select Admin Task screen appears.

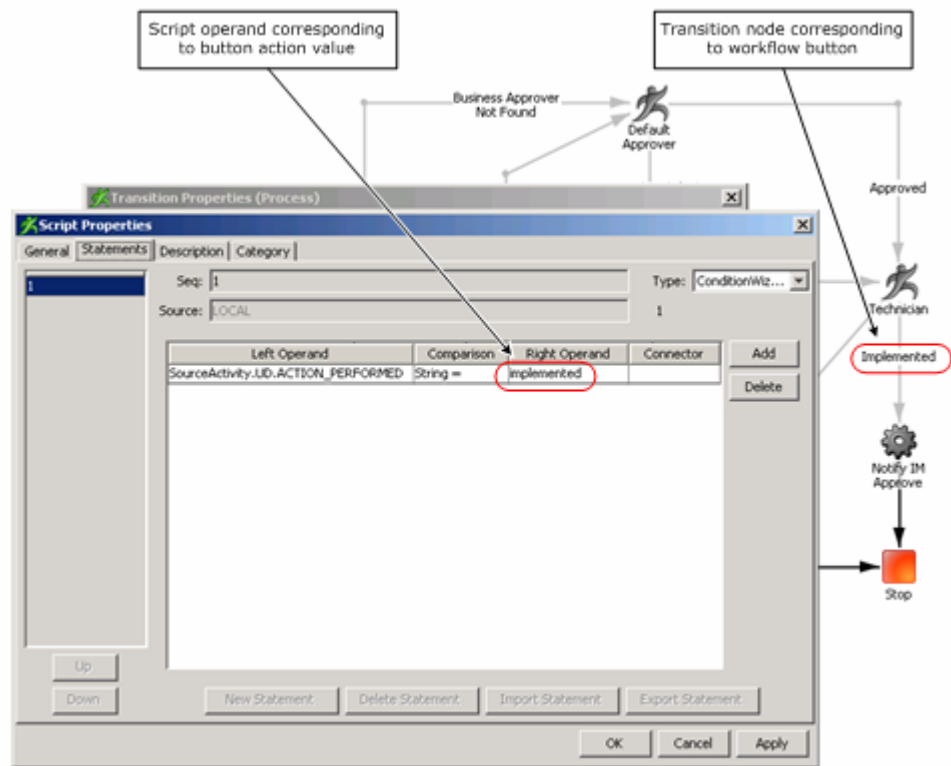
2. Search for the approval task, and click Select.

The Modify Admin Task screen appears.

3. On the Profile tab, click the button named Workflow Action Buttons.
The Workflow Action Button Profile tab appears.
4. Click "Add Button" to add a new button to the approval task.
5. Enter the button property information.
6. Click OK.
Identity Manager saves the new button information.
7. Click Submit.
Identity Manager processes the task modification.

Button Configuration in WorkPoint Designer

In WorkPoint Designer, workflow action buttons are configured using transition node script properties, as shown in the following figure:



By default, workflow action buttons use the following script properties to perform a string comparison:

- Left Operand--ACTION_PERFORMED, which is defined in the User Data properties of the preceding manual activity node.
- Right Operand--The Action value of the button, which is defined in the button profile tab of the Identity Manager User Console.

Note: See the WorkPoint Designer online help for information about activity node and transition node scripts and properties.

More Information:

[Button Configuration In Identity Manager](#) (see page 269)

Work Lists and Work Items

A *work list* is a list of work items (or approval tasks) that appears in the User Console of the participant authorized to approve the task. Work items correspond to manual activities in a workflow process. Work items are represented as rows in the work list.

Work items can be added to a work list in the following ways:

- A participant resolver determining a list of approvers.
- Receiving delegated work items from another user.
- Reassigning it to another user.

Work items can be removed from a work list in the following ways:

- Completing (approving or rejecting) the work item.
- Reassigning it to another user.
- Reserving it. This removes it from the work list of all other participants.

The information tabs that appear on a work item depend on whether the work item was generated by workflow under task-level or event-level control:

- **Profile**—Provides profile information about the object affected by the event (event-level only).
- **Task Details**—Provides detailed information for all events within the task (task-level only).
- **Approvers**—Lists all individual approvers and delegators for the task or event (task-level and event-level)

Displaying a Work List

Your work list appears automatically when you log into the Identity Manager User Console if you have been assigned as a participant to approve tasks (or work items) initiated by other users.

To display your work list manually

1. In the User Console, select Home, View My Work List.

Your work list appears.

2. Click the name of a work item to display it.

The selected work item appears.

Administrators can manage work items for users over whom they have scope.

Note: Managing a user's work items allows administrators to reserve a work item. Viewing a user's work list does not allow work item changes of any kind.

To view the work list of another user

1. In the User Console, select Users, Manage Work Items, View User's Work List.

A select user screen appears.

2. Search for the user whose work list you want to view, and click Select.

The user's work list screen appears.

To manage work items for another user

1. In the User Console, select Users, Manage Work Items, Manage User's Work Items.

A select user screen appears.

2. Search for the user whose work items you want to manage, and click Select.

The user's work list screen appears.

3. Click the name of a work item to display it.

The selected work item appears.

Reserving Work Items

You can reserve a work item to "check it out" and remove it from the work list of other participants. Reserving a work item holds it for the user performing the reservation.

If the reserving user releases the work item, it becomes available again on the work list of other participants. If the reserving user approves or rejects the work item, it is completed, and no longer available to other participants.

More Information:

[Delegation and Reserved Work Items](#) (see page 274)

[Reassignment and Reserved Work Items](#) (see page 274)

Reassignment and Reserved Work Items

If a user has a work item reserved while it is reassigned, the user keeps it reserved. But if the user then releases that work item, he loses access to it.

An administrator can reassign, reserve, or release another user's work item, but cannot approve or reject another user's work item. Only the assigned work item participant can do that.

More Information:

[Reassigning Work Items](#) (see page 279)

Delegation and Reserved Work Items

While a delegation is active, either the delegate or the delegator may reserve a work item. A work item reserved by one user cannot appear on another user's work list.

For example, if a delegate has a work item reserved while the delegation is withdrawn, the delegate keeps the work item reserved. But if the delegate then releases that work item, he loses access to it.

If a user who is a delegate is deleted while the delegate has a work item reserved, the delegate still retains the work item. If the delegate then approves the work item, auditing can no longer determine who delegated it.

If a delegate has a work item reserved while the delegation is withdrawn, the delegate retains access until the work item is completed or released.

More Information:

[Reserving Work Items](#) (see page 274)

[Delegating Work Items](#) (see page 275)

How to Reserve or Release a Work Item

You reserve a work item to "check it out" and remove it from the work list of other participants.

You release a reserved work item to make it available on the work list of other participants.

Note: The only way to free a reserved work item is to explicitly release it.

To reserve or release a work item

1. In the Identity Manager user Console, select Home, View My Work List.
Your work list appears.
2. Select the work item you want to reserve or release.
The expanded work item screen appears.
3. Click Reserve Item or Release Item.
Identity Manager confirms your action.

Delegating Work Items

Work item *delegation* lets a user (the delegator) specify that another user (the delegate) be allowed to approve tasks in the delegator's work list. A delegator can assign work items to another approver during periods when the delegator is "out of the office." Delegators retain full access to their work items during the delegation period.

Delegated work items are not changed in any way. Logging indicates whether a work item was delegated.

Delegation works by allowing the delegate to "impersonate" the delegator and view the items on the delegator's work list. When viewing a work list, delegates see their own work items as well as the delegator's work items.

Delegation is not transitive. A delegate can only see work items that the delegator has assigned directly. For example, If user A delegates work items to user B, and user B delegates work items to user C, user C can only see work items belonging to user B, and not any work items that may have been work items delegated to user B by user A.

More Information:

[Delegation and Reserved Work Items](#) (see page 274)

Delegation Well-Known Attribute

Delegation uses the following well-known attribute:

%DELEGATORS%

This well-known attribute stores the names of users who are delegating to the user with the attribute, as well as the time when the delegation was created.

How to Enable Delegation

You must have workflow approval delegation enabled before you can use a delegate work items to another user. By default, delegation is disabled.

To enable workflow approval delegation

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain_name>/idmmanage`

where <domain_name> is the fully qualified domain name of the server where Identity Manager is installed. For example, `myserver.mycompany.com:port`.

2. Click Environments, then select the name of the appropriate Identity Manager environment.
3. Click Advanced Settings, and then click Workflow Approval Delegation.
4. Select the Enabled check box, and then click Save.

More Information:

[How to Delegate for Yourself](#) (see page 276)

[How to Delegate for Another User](#) (see page 278)

How to Delegate for Yourself

You can delegate work items to another user during periods when you are “out of the office.” Delegators still retain full access to their work items during the delegation period.

To delegate work items for yourself

1. In the Identity Manager User Console, select Home, Out of Office Assistant.

The Out of Office Assistant screen appears.

2. Click Add User.

A select user screen appears.

3. Search for and select one or more users to act as delegate.

The users are added to the delegate list.

4. Click Submit.

The task is submitted and the delegation is saved.

Note: Users who are already delegates do not appear in the search results when adding a delegate.

More Information:

[How to Enable Delegation](#) (see page 276)

Out of Office Assistant Screen

You use the following Out of Office Assistant screen to add and remove delegate for yourself:

Logged in as: Sales Vice President (Logout)

Home

Tasks

Out Of Office Assistant

User ID	Last Name	First Name	Start Date	Has Delegates
SalesDir	Director	Sales	Nov 16, 2007 12:24:07 PM	
SalesMgr	Manager	Sales	Nov 16, 2007 12:24:07 PM	Yes

Add User

Submit Cancel

The Out of Office Assistant screen displays a list of your current delegates. In addition to columns that identify the delegate, two additional columns are included in the list:

Start Date

Displays the date the delegation was created.

Has Delegates

Indicates whether the delegate has delegated work items to another user.

How to Delegate for Another User

Administrators can delegate work items from one user (the delegator) to another. For example, a user may be out of the office unexpectedly, or an administrator may need to assign a large workload to multiple users.

Administrators can only delegate work items for users over whom they have scope. Similarly, they can only add or remove users they manage from the list of delegates.

To delegate work items for another user

1. In the Identity Manager User Console, select Users, Manage Work Items, Delegate Work Items.

A select user screen appears.

2. Search for the user whose work items you want to delegate (the delegator), and click Select.

A delegate work items screen appears.

3. Click Add User.

A select user screen appears.

4. Search for and select one or more users to act as delegate.

The users are added to the delegate list.

5. Click Submit.

The task is submitted and the delegation is saved.

Note: Users who are already delegates do not appear in the search results when adding a delegate.

More Information:

[How to Enable Delegation](#) (see page 276)

How to Remove a Delegation

If a user logs into Identity Manager with delegations in place, Identity Manager displays the following reminder:

You have delegations in place. Please check that they are still required.

To remove a delegation for yourself

1. In the Identity Manager User Console, select Home, Out of Office Assistant.

The Out of Office Assistant screen appears.

2. Click the minus sign (-) for delegates you want to remove.

The delegates disappear from the list.

3. Click Submit.

The task is submitted and the delegation is removed.

To remove a delegation for another user

1. In the Identity Manager User Console, select Users, manage Work Items, Delegate Work Items.

A user search screen appears.

2. Search for and select the user whose delegations you want to remove.

The delegates list appears.

3. Click the minus sign (-) for delegates you want to remove.

The delegates disappear from the list.

4. Click Submit.

The task is submitted and the delegation is removed.

Note: You can only remove a delegate if you have scope over that user.

Reassigning Work Items

Reassignment allows users and administrators to change the assignees of a work item after it is created. An administrator can:

- View another user's work list
- Add and remove work item assignees
- Change the reserve status of work items

For example, an administrator can reassign a work item or release a reserved work item from a user who is not acting on it.

If a user has a work item reserved while it is reassigned, the user keep it reserved. But if the user then releases that work item, he loses access to it.

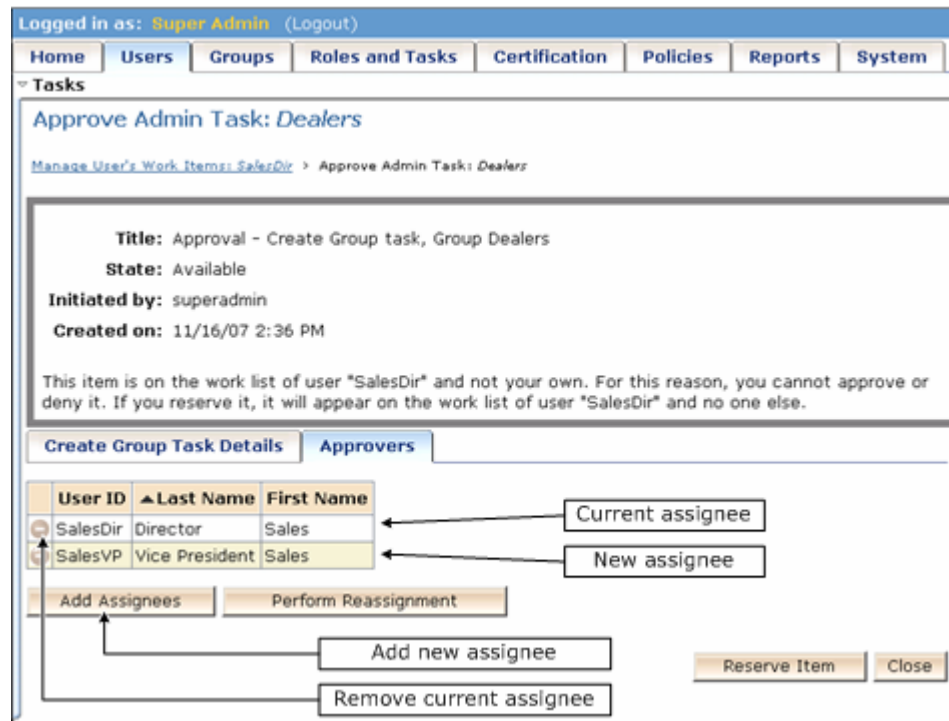
If a delegate has a work item reserved while the delegation is withdrawn, the delegate retains access until the work item is completed or released.

More Information:

[Reassignment and Reserved Work Items](#) (see page 274)

The Approvers Tab

You perform reassignment on the Work Item Approvers tab, which displays a list of current work item approvers (or assignees). When you perform reassignment, you assign the open work item to all approvers in the list. Therefore, to reassign a work item to a new assignee, you also need to explicitly remove the current assignee, as shown in the following figure:



How to Reassign Work Items

Reassigning a work item from one user to another is a two-step process:

- Select a new approver.
- Remove the current approver.

Note: You must have scope over users to whom you want to reassign.

To reassign a work item for yourself

1. Select Home, View My Work List.
Your work list appears.
2. Select a work item to expand it.

3. Select the Approvers tab.

The list of all current approvers appears, including the user whose work list you are managing.

4. Click Add Assignees.

A select user screen appears.

5. Search for and select one or more users to whom you want to reassign.

6. Click the minus sign button (-) to remove yourself as an assignee.

7. Click Perform Reassignment.

The work item appears on the work lists of the reassigned users.

Note: An administrator can reassign, reserve, or release another user's work item, but cannot approve or reject another user's work item. Only the owner of the work item can do that.

To reassign a work item for another user

1. Select Users, Manage Work Items, Manage User's Work Items.

A select user screen appears.

2. Search for the user whose work items you want to reassign, and click Select.

The Manage User's Work Items screen appears.

3. Select a work item to expand it.

4. Select the Approvers tab.

The list of all current approvers appears, including the user whose work list you are managing.

5. Click Add Assignees.

A select user screen appears.

6. Search for and select one or more users to whom you want to reassign.

7. Click the minus sign button (-) to remove the current assignee.

8. Click Perform Reassignment.

The work item appears on the work lists of the reassigned users.

Chapter 13: Email Notifications

Email notifications inform Identity Manager users of tasks and events in the system. Identity Manager can automatically generate email notifications when:

- An event requiring approval or rejection by a workflow approver is pending
- An approver approves an event
- An approver rejects an event
- An event or task is completed
- A user requests a temporary password through the forgotten password feature

This section contains the following topics:

[Email Content](#) (see page 283)

[Enable Email Notification](#) (see page 284)

[Configure an Event or Task To Send Email](#) (see page 285)

[Email Templates](#) (see page 286)

[Create Email Templates](#) (see page 289)

[Custom Email Templates](#) (see page 289)

[Email Template Deployment](#) (see page 307)

Email Content

An email notification consists of a generic template plus task-specific details that are added to the email through the email API. For example, the following information can be inserted into an email for a Create User task:

- The name of the administrator who is executing the task
- The name of the new user
- The user's email address, department name, and other attribute data
- The organization where the user is being created
- Workflow approval status and approval time
- The task name and the names of the events in the task

Enable Email Notification

You can enable or disable email notification for an Identity Manager environment:

If...	Then...
You disable email notification (default)	No emails are sent for that Identity Manager environment. Note: To use the Forgotten Password feature, enable email notification.
You enable email notification	Identity Manager sends email notifications for the events and tasks you specify.

Before enabling email notification, configure the SMTP server. See the *CA Identity Manager Installation Guide*.

To enable email notification:

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain>/idmmanage`

where *<domain>* is the fully qualified domain name of the server where Identity Manager is installed--for example, `myserver.mycompany.com`.
2. Click Environments.
A list of Identity Manager environments is displayed.
3. Click the name of the appropriate Identity Manager environment. Then, click Advanced Settings, Email.
4. Select the Enabled check box.
5. Optionally, configure the events and tasks that trigger email, as described in [Configure an Event or Task To Send Email](#) (see page 285).
6. Click Save.
7. Restart the instance of the application server on which Identity Manager is installed.

Configure an Event or Task To Send Email

If email notification is enabled, you can specify a list of events and tasks that trigger email notifications. For example, you may want emails sent in circumstances such as these:

- To a system administrator, at the completion of a Reset User Password task.
- To a new employee's manager, at the completion of a Create User task. In addition, when the AddToGroupEvent generated within the Create User task is approved, another email can be sent to all members of a group to which the new user is being added.

To specify the events and tasks that trigger email notifications

1. Open the Identity Manager Management Console by entering the following URL in a browser:

`http://<domain>/idmmanage` where *<domain>* is the fully qualified domain name of the server where Identity Manager is installed. For example, `myserver.mycompany.com`.

2. Click Environments.

A list of Identity Manager environments is displayed.

3. Click the name of the appropriate Identity Manager environment. Then, click Advanced Settings, Email.
4. To send email notifications when an event completes or for an event under workflow control, configure email notification for the events that the task generates. Select the event from the Event list box and click Add.
5. In the tasks section, search for the task for which to send an email notification. Select the task from the search results and click Add.

Note: Task-level email notifications are not available for tasks that have the action type View or Self View. To see the action type of a task, go to Modify Admin Task, Select a Task, and check the action field in the task profile.

6. When you finish configuring the tasks and events that trigger email notifications, click Save.
7. Restart the application server on which Identity Manager is installed.

Email Templates

Email notifications are generated from email templates. Identity Manager provides default email templates that you can use as installed, or that you can use to create your own email templates.

Each email template contains the following:

- **Delivery information**--A list of email recipients. Identity Manager automatically generates the list of recipients, based on users involved in the task. For example, an approval email is sent to all Approvers for the task.
- **Subject**--The text used in the message's subject line.
- **Content**--The message body. The body typically contains both static text and variables, which Identity Manager resolves based on the task or event that triggers the email.

The default email templates are located in an emailTemplates directory where the Identity Manager administrative tools are installed. The default installation location for the administrative tools is:

- For Windows--C:\Program Files\CA\CA Identity Manager\
- For UNIX--<home_directory>/CA/CA Identity Manager

The emailTemplates directory contains four folders. Each folder is associated with a task or event state:

Directory	Contents
Approved	defaultEvent.tmpl--Informs recipients that an event has been approved

Directory	Contents
Completed	■ CertificationNonCertifiedActionCompletedNotification.tmpl--Informs the manager that a non-compliance action has been applied to an employee. ■ CertificationNonCertifiedActionPendingNotification.tmpl--Informs the manager that a non-compliance action will be applied to an employee. ■ CertificationRequiredFinalNotification.tmpl--Final reminder to a manager that the Certify User task must be completed for an employee. ■ CertificationRequiredNotification.tmpl--Informs the manager that a certification process has begun for an employee. The manager must complete a Certify User task for this employee. ■ CertificationRequiredReminderNotification.tmpl--Reminds the manager that the Certify User task must be completed for an employee. ■ Certify Employee.tmpl--Informs an administrator that the certification process for an employee is complete. ■ CreateProvisioningUserNotificationEvent.tmpl--Sends a temporary password to a user when that user's account is created in the provisioning directory. ■ defaultTask.tmpl--Informs recipients that Identity Manager has completed a task. ■ ForgottenPassword.tmpl--Sends a temporary password to users who have used the forgotten password feature. ■ ForgottenUserID.tmpl--Sends a user ID to users who have used the forgotten user ID feature. ■ Self Registration.tmpl--Informs a user that a self-registration task has completed successfully.
Pending	■ defaultEvent.tmpl--Informs approvers that a work list item requires attention ■ ModifyUserEvent.tmpl--Same as the default template, but includes methods for retrieving the attributes of the User managed object
Rejected	defaultEvent.tmpl--Informs recipients that an event has been rejected

Use the Identity Manager templates and template directory structure that are installed in the `<im_admin_tools_dir>\Identity Manager\emailTemplates` directory as a base for creating custom email templates.

Template Directories

Each template directory described in [Email Templates](#) (see page 286) is associated with a particular task or event state. For example, if an email is to be sent for an event that has been rejected in a workflow process, Identity Manager looks in a deployed rejected directory for the template to use. Identity Manager then generates the email from the appropriate email template in the directory.

Email Templates in a Directory

Each deployed template directory contains one or more email templates. When a task or event occurs for which email is enabled, Identity Manager searches the appropriate template directory for a template name that is the same as the name of the task or event. If such a template cannot be found, Identity Manager uses the default template in the directory. Default template names are listed in [Email Templates](#) (see page 286). For example, Identity Manager uses defaultEvent.tmpl in the Pending directory to inform approvers that they have a new work list item.

Sets of Template Directories

A set of template directories contains an approved, completed, pending, and rejected directory. You can deploy multiple sets of template directories and specify one set to be used for a given Identity Manager environment.

[Email Template Deployment](#) (see page 307) provides information on deploying sets of template directories.

For information on configuring email template directories so that Identity Manager uses the correct set for a given environment, see the *CA Identity Manager Configuration Guide*.

Create Email Templates

To create custom email messages

1. Open the template that you want to modify.

For example, if you want to create an email message for a pending Create User event, open `defaultEvent.tmpl` in the Pending directory.

2. Save the template in the same directory with a new name. The name must match the name of the event to which the email applies, and have the extension `.tmpl`.

For example, name the message for the pending Create User event as follows:

`CreateUserEvent.tmpl`

See Identity Manager Events for a list of events.

Note: When you create an email template file with a file name using a different language, the operating system session should be operating in a language that supports the character set.

3. Modify the message template as needed, as described in the next section, [Custom Email Templates](#) (see page 289).

Custom Email Templates

An email template is a dynamic file that supports both HTML and embedded server-side JavaScript. A template lets you insert variable values into static text, allowing case-specific messages to be generated from a single template.

The same template can be used any number of times to print out boilerplate static text (such as the phrase has been approved) along with variable text specific to a given context (such as the name of the event being approved).

For example, here is a template for reporting the approval of an event:

```
<!-- Define the E-mail Properties -->
<%
  _to = _util.getNotifiers("ADMIN");
  _cc = "";
  _bcc = "";
  _subject = _eventContextInformation.getEventName() + " approved";
%>
<!-- Start of Body -->
<html>
<body text="Navy">
```

```
Event: <b> <%= _eventContextInformation.getEventName()%> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%= _eventContextInformation.getPrimaryObjectName()%></b><br>
In <%= _eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%= _eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

Note: The Identity Manager objects `_util` and `_eventContextInformation` used in the above example are described in [Email Template API](#) (see page 292).

If an approval is generated for the event `CreateUserEvent`, and user John Jones is created in organization HR, the body of the email notification generated from the approval template might look like this:

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

The following sections describe the syntax and Identity Manager objects that make dynamic email messages possible.

Template Elements

Identity Manager email templates support:

- Standard HTML tags.
- Server-side JavaScript.
- One or more implicit objects that Identity Manager makes available to an instance of the template--that is, to an email message.
- Identity Manager tags that let you embed JavaScript in the template, call the methods in the implicit Identity Manager objects, and insert variable values into the template's static text.

Identity Manager Tag Extensions

Email templates support the following tags:

- `<% %>`. Embeds JavaScript into an email template.
- `<%= %>`. Inserts a variable value into static text.

The tags are described in the following sections.

<% %>

This tag lets you embed JavaScript for in-line execution into an email template.

You can use any JavaScript object within the embedded JavaScript. You can also call Identity Manager implicit object methods within the embedded JavaScript.

For example, the following code modifies the body of the approval template shown in [Custom Email Templates](#) (see page 289). JavaScript is used to determine if a secondary object is involved in the event (such as an ORGANIZATION object when a USER primary object is added). If there is no secondary object, the text relating to the secondary object is omitted from the message:

```
Event: <b> <%= _eventContextInformation.getEventName()%> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%= _eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+ _eventContextInformation.getSecondary
        ObjectName()+" </b><br>");
}
%>
Status: <b>Approved</b>
```

<%= %>

This tag lets you insert a variable value into static text. The value can be:

- A variable defined in some previously executed JavaScript in the template--for example:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
...    // More JavaScript processing
%>
...    // More HTML
The primary object was created in <%=secondaryType%>.
```

- A value returned from a method in an Identity Manager implicit object--for example:

```
Event <%= _eventContextInformation.getEventName()%> is approved.
```

Email Template API

When a message is generated from a template, Identity Manager makes the implicit objects below available to the message. These objects let you insert instance-specific information into a message by calling methods in the Email Template API.

A template can call the methods in any of the following objects:

- `_contentType`. Specifies the `contentType` for the email.
- `_priority`. Specifies the priority for the email.
- `_to`. Adds recipients to the message's To field.
- `_cc`. Adds recipients to the message's cc (send copy to) field.
- `_bcc`. Adds recipients to the message's bcc (send blind copy to) field.
- `_subject`. Specifies the subject of the email.
- `_encoding`. Specifies the encoding for the email.
- `template`. Lets you add a string of text to a message from lines of JavaScript code.
- `_util`. A utility object.
- `_eventContextInformation`. Contains information about the event generated by the current task, such as event name and approval status.
- `_taskContextInformation`. Contains a collection of information about the current task, such as task name, organization name, and constituent events.

These objects are described in the following sections.

`_contentType`

Specifies the `contentType` for the email.

If no `contentType` is specified through `_contentType` variable, the default `contentType` "text/html" applies.

Methods: None.

Example:

```
<% _contentType = "text/html"; %>
```

_priority

Specifies the priority for the email. Specify 0 for no priority (default) and 1 for high priority.

Methods: None.

Example:

```
<% _priority = "1"; %>
```

_to

Adds recipients to the message's To field.

The value of the `_to` variable is a JavaScript string. Multiple recipients are permitted, but the string must conform to JavaScript syntax, as shown in the following example.

Methods: None.

Example:

```
<%  
_to =  
_util.getNotifiers("USER") + ',' +  
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
_cc = "" ;  
_bcc = "" ;  
_subject = "Your new password ";  
%>
```

Note: When emails alert participants that a task is in a Pending state and under workflow control, the `_to` object is pre-populated with the addresses of the participants. You cannot use the `_to` object in a Pending template.

_cc

Adds recipients to the message's cc (send copy to) field.

The value of the `_to` variable is a JavaScript string. Multiple recipients are permitted, but the string must conform to JavaScript syntax, as shown in the following example.

Methods: None.

Example:

```
<%  
_cc =  
_util.getNotifiers("USER") + ';' +  
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
%>
```

_bcc

Adds recipients to the message's bcc (send blind copy to) field.

Email addresses specified in this field do not appear in the email.

The value of the `_to` variable is a JavaScript string. Multiple recipients are permitted, but the string must conform to JavaScript syntax, as shown in the following example.

Methods: None.

Example:

```
<%  
_bcc =  
_util.getNotifiers("USER") + ';' +  
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
%>
```

_subject

Specifies the subject of the email.

Methods: None.

Example:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

`_encoding`

Specifies the encoding for the email.

If no encoding is specified either through `_encoding` or through the `LANG` variable, characters in the email may not be correctly displayed. Be sure to set `_encoding` or `LANG` for the appropriate locale.

Methods: None.

Example:

```
<% _encoding = "UTF-8"; %>
```

`template`

Lets you add a string of text to a message from lines of JavaScript code (that is, lines within the `<% %>` tag). The string can contain HTML tags, static text, and/or variable values returned by methods in Identity Manager implicit objects.

Note: The template object is not preceded by the underscore (`_`) character.

Method:

- `add(String)`

The argument must evaluate to a string, including any calls to methods in an Identity Manager implicit object. In the example below, see `_eventContextInformation.getSecondaryObjectName()`.

Example:

```
<%  
var secondaryType = _eventContextInformation.getSecondaryObjectType();  
if (secondaryType != "") {  
    template.add("In " + secondaryType + ": ");  
    template.add("<b> "+ _eventContextInformation.getSecondary  
        ObjectName()+" </b><br>");  
}  
%>
```

`_util`

Utility object.

Method:

- `getNotifiers(String [,String])`

Returns email IDs based on a notification rule.

The first argument supports the following predefined notification rules, enclosed in quotes:

- "ADMIN". Sends the email to the administrator who initiated the task.
- "USER". Sends the email to the user in the current context.
- "USER_MANAGER". Sends the email to the manager of the user in the current context.

You can also reference a custom notification rule that you create with the Notification Rule API. For information, see the *Programming Guide for Java*.

The second argument is optional. You can use it to pass one or more user-defined name/value pairs into a custom notification rule. Separate each name/value pair with a comma, in the following format:

"name1=value1,name2=value2,..."

Examples:

```
<%  
_to = _util.getNotifiers("ADMIN");  
_cc = "";  
%>  
  
<%  
_to = _util.getNotifiers("MYRULE","type=loan,district=3");  
_cc = "";  
%>
```

Notifying a User's Manager

You can use the USER_MANAGER notification rule to send email to any user's manager. Identity Manager uses this rule in the email templates supporting user entitlement certification.

Note: The USER_MANAGER Notification Rule only applies to events or tasks that create or manage a single user.

Because there are a number of different ways a user-to-manager relationship can be specified within a user directory, the default User Manager Notification Adapter resolves this relationship based on an attribute expression specified in the second parameter of the `getNotifiers()` method.

Example:

```
<%  
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");  
_cc = "";  
%>
```


The User Manager Notification Adapter supports two look-up options:

- `managerattribute = <Manager AttributeName>`- where the User object maintains an attribute that indicates the DN or UserID of that user's manager
- `commonattribute = <AttributeName>` - where the user and the user's manager share a common attribute value, such as "department"

You configure these lookup options in the Miscellaneous Properties for an environment in the Identity Manager Management Console.

To configure the USER_MANAGER notification rule:

1. In the Identity Manager Management Console, select Identity Manager Environments. Then, select the environment for which you are configuring email notification.
2. Select Advanced Settings>Miscellaneous Properties.
3. In the Miscellaneous Properties page, complete the configuration steps for the lookup option that you want to use:
 - To use the `managerattribute=<Manager AttributeName>` lookup option:
 - a. In the Property field, enter `managerattribute`.
 - b. In the Value field, enter the attribute that stores the manager's DN or user ID.
 - c. Click Add.
 - d. Click Save.
 - To use the `commonattribute=<AttributeName>` lookup option:
 - a. In the Property field, enter `commonattribute`.
 - b. In the Value field, enter the attribute that the user and the user's manager have in common.
 - c. Click Add.
 - d. In the Property field, enter `ismanagerfilter`.

- e. In the Value field, enter a search expression using the following syntax:
`<attribute> <operator> <filter>`
For example, title EQUALS manager
- f. Click Add.
- g. Click Save.

You can also write a custom adapter and create your own rules for notifying a user's manager. See the *Programming Guide for Java*.

_eventContextInformation

Contains information about the event generated by the current task, such as event name and approval status. This information is called *context* information for the event.

The `_eventContextInformation` object is created from the `ExposedEventContextInformation` class in package `com.netegrity.imapi`.

This object is available for email messages based on Approved, Pending, and Rejected templates. For information about these templates, see [Email Templates](#) (see page 286).

Methods: All the methods below return a String.

Method	Description
<code>getAdminName()</code>	Returns the name of the person who submitted the task that generated the event. Deprecated in Identity Manager 5.6. Use one of the following inherited methods: ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>
<code>getApprovalStatus()</code>	Returns the approval status of the event. One of these values: <code>APPROVAL_STATUS_APPROVED</code> <code>APPROVAL_STATUS_REJECTED</code>
<code>getApprovalTime()</code>	Returns the time the event was approved.

Method	Description
getEventName()	Returns the name of the event. For a list of event names, see Identity Manager Events.
getOrgName()	Returns the friendly name of the organization where the task is being executed. Deprecated in Identity Manager 5.6. Use the inherited method getObjectOrganizationFriendlyName().
getPassword()	If the primary objects is type USER, returns the user's password.
getPrimaryObjectTypeName()	Returns the type of primary object. Primary object types returned: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

Method	Description
<code>getPrimaryObjectName()</code>	Returns the name of the primary object affected by the event. A <i>primary object</i> is the object directly affected by the event. A <i>secondary object</i> is the object that the primary object is bound to, if any. For example: ■ The primary object type for <code>CreateUserEvent</code> is <code>USER</code>. The secondary object is the object where the user is created--that is, <code>ORGANIZATION</code>. ■ The primary object type for <code>CreateAdminRoleEvent</code> is <code>ADMINROLE</code>. This object is not bound to other objects, so no secondary object exists. With a primary object of type <code>USER</code>, <code>getPrimaryObjectName()</code> might return John Jones.
<code>getSecondaryObjectTypeName()</code>	If a secondary object was affected by the event, returns the object type. Secondary object types returned: <code>ACCESSROLE</code> <code>ACCESSTASK</code> <code>ADMINROLE</code> <code>ADMINTASK</code> <code>GROUP</code> <code>ORGANIZATION</code> <code>USER</code>
<code>getSecondaryObjectName()</code>	If a secondary object was affected by the event, returns the object name. See <code>getPrimaryObjectName()</code> for information about primary and secondary objects. With a secondary object of type <code>ORGANIZATION</code>, the method <code>getSecondaryObjectName()</code> might return HR.

Note: The methods in `_eventContextInformation` are provided through the interface `ExposedEventContextInformation`. Since `ExposedEventContextInformation` inherits methods in the core Identity Manager API, `_eventContextInformation` can also call these methods from an email template, along with the methods in the above table. For more information about these inherited methods, see [Additional Methods](#) (see page 305).

Example--Email notification about a Pending event:

```
<%  
_cc = "" ;  
_bcc = "" ;  
_subject = _eventContextInformation.getEventName() +  
           " Approval Request";  
%>  
<!-- Start of Body -->  
<html>  
<body text="Navy">
```

The following item has been added to your work list for approval:

```
<br><br><br>  
Event: <b><%= _eventContextInformation.getEventName()%></b> <br>  
<%= _eventContextInformation.getPrimaryObjectTypeName()%>:  
<b><%= _eventContextInformation.getPrimaryObjectName()%></b><br>  
In <%= _eventContextInformation.getSecondaryObjectTypeName()%>:  
<b><%= _eventContextInformation.getSecondaryObjectName()%></b><br>  
</body>  
</html>
```

Possible email body:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**

Note: The value of the From field is derived from the email.properties file. To change the value, edit the following file:

`<IdentityMinder.ear>\config\com\netegrity\config\email.properties`

where `<IdentityMinder.ear>` is the installed location of Identity Manager in the application server domain--for example:

For WebLogic:

`<WebLogic_home>\user_projects\<domain>\applications\IdentityMinder.ear`

For JBoss:

`<IdentityManager_home>\jboss-3.2.2\server\default\deploy\IdentityMinder.ear`

For WebSphere:

`<im_admin_tools_dir>\WebSphere-ear\IdentityMinder.ear`

To add additional information about the user affected by the event to the email in the previous example, add text that resembles the following:

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Possible email body:

From: lsmith@security.com [mailto:lsmith@security.com]

To: vimperioso@security.com

Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**

USER: **Richard Ferrigamo**

In ORGANIZATION: **Mortgages & Loans**

User information:

Last Name: Ferrigamo

First Name: Richard

Full Name: Richard Ferrigamo

Email: rferrigamo@mybank.org

Organization Membership: **Mortgages & Loans**

`_taskContextInformation`

Contains a collection of information about the current task, such as task name, organization name, and constituent events. This information is called *context* information for the task.

This object is available for email messages based on Completed templates. For information about this template, see [Email Templates](#) (see page 286).

Methods: All the methods below return a String except for the method `getExposedEventContexts()`, which returns a Java Vector.

Method	Description
<code>getAdminName()</code>	Returns the name of the person submitting the task. Deprecated in Identity Manager 5.6. Use one of the following inherited methods: ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>
<code>getExposedEventContexts()</code>	Returns a Java Vector of all events associated with the task. Each object in the Vector is an event context object. You can use the methods listed in <code>_eventContextInformation</code> to retrieve context information for a given event object. The return object is a standard Java Vector object. You can use any of the Vector object's methods--for example, <code>get()</code> and <code>size()</code>--to manage the elements in the Vector.
<code>getOrgName()</code>	Returns the name of the organization where the task is being executed. Deprecated in Identity Manager 5.6. Use the inherited method <code>getObjectOrganizationFriendlyName()</code>.

Method	Description
getTaskName()	Returns the name of the task being executed. Deprecated in Identity Manager 5.6. Use one of the following inherited methods: ■ getAdminTask() ■ getTaskFriendlyName()

Note: The methods in `_taskContextInformation` are provided through the interface `ExposedTaskContextInformation`. Since `ExposedTaskContextInformation` inherits methods in the core Identity Manager API, `_taskContextInformation` can also call these methods from an email template, along with the methods in the above table. For more information about these inherited methods, see [Additional Methods](#) (see page 305).

Example--Body of an email notification template for a password change:

```
<%  
var imsEventContexts =      _taskContextInformation.getExposedEventContexts();  
if(imsEventContexts != null)  
{  
  for(var i=0;i<imsEventContexts.size();i++)  
  {  
    var eventContext = imsEventContexts.get(i);  
    template.add("Hi "+ eventContext.getPrimaryObjectName() + ",");  
    template.add("<br>Your new password is: <b>" +  
                eventContext.getPassword());</br>  
    template.add("<hr>");  
  }  
}  
%>
```

Possible email body:

Hi Victor Imperioso,
Your new password is: LFH7F1226

Additional Methods

The methods in `_taskContextInformation` and `_eventContextInformation` are provided through the Identity Manager objects `ExposedTaskContextInformation` and `ExposedEventContextInformation`, respectively.

These objects inherit methods in the core Identity Manager API. Consequently, the inherited methods are also available to `_taskContextInformation` and `_eventContextInformation`.

The following methods inherited from the `TaskInfo` object are particularly useful to an email template:

- `getAdministrator()`. Retrieves a `User` object for the administrator who is executing the current task.
- `getAdminTask()`. Retrieves an `AdminTask` object for the current task.

These retrieved objects allow you to insert administrator-specific and task-specific information into an email. For example:

<!-- Define the E-mail Properties -->

```
<%
  _cc = "";
  _bcc = "";
  _subject = _eventContextInformation.getEventName() +
            " Approval Request";
%>
<!-- Start of Body -->
<html>
<body text="Navy">
```

The following item has been added to your work list for approval:


```
User <b><%= _eventContextInformation.getAdministrator().
  getAttribute(Packages.com.netegrity.llsdk6.imsapi.
  managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
from department <b><%= _eventContextInformation.
getAdministrator().getOrg(null).getFriendlyName()
%></b> initiated task <b><%= _eventContextInformation.
getAdminTask().getFriendlyName() %></b>at <b><%=
  _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
```

```
<font color="green">Details: </font><b><%= _eventContextInformation.  
    getEventName()%></b><br>  
<font color="green"><%= _eventContextInformation.  
    getPrimaryObjectTypeName()%></font>  
<b><%= _eventContextInformation.getPrimaryObjectName()%></b>  
    was modified  
<br>  
<font color="green">Updated Attributes:</font>  
<table border="1">  
<tr>  
    <td><b>Name</b></td>  
    <td><b>Value</b></td>  
</tr>  
<%  
    var event = _eventContextInformation.getEvent();  
    if(event instanceof Packages.com.netegrity.imapi.UserEvent) {  
        var user = event.getUser();  
        var attributes = user.getAttributes().keys();  
        while(attributes.hasMoreElements()) {  
            var attr = attributes.nextElement();  
            var value = user.getAttribute(attr);  
            if(user.hasAttributeChanged(attr)) {  
                template.add("<tr><td>" + attr + "</td>");  
                template.add("<td>" + value + "</td></tr>");  
            }  
        }  
    }  
<%>  
</table>  
<br>  
</body>  
</html>
```

Possible email body:

The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**

User: **John Jones** was modified

Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

For more information about the inherited methods that are available to the Email Template API, see the objects `ExposedTaskContextInformation` and `ExposedEventContextInformation` objects in the Identity Manager Javadoc.

Java Standard Output Stream

An email message can also make calls to the Java standard output stream from inside the JavaScript tag (`<% %>`). For example, the following call sends the message Done to the server console:

```
<%  
...    // JavaScript processing  
out.println("Done.");  
%>
```

Javadoc Reference

For information about the `ExposedTaskContextInformation` and `ExposedEventContextInformation` objects, including the methods they inherit from the core Identity Manager API, see the Identity Manager Javadoc.

You can access the Javadoc by opening the file `index.html` in the following default location:

```
<doc_install_path>/javadoc-im
```

Email Template Deployment

When Identity Manager is about to send email, it searches for templates from which to generate the email in the following root location within your application server:

```
<IdentityMinder.ear>\custom\emailTemplates
```

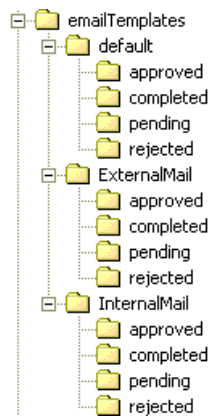
The email templates deployed in this root are contained in template sets that have the same directory structure--that is, there is an `approved`, `completed`, `pending`, and `rejected` directory in each set.

Template Sets

You can deploy several sets of email templates under `emailTemplates`. For example, during installation, the following set of email templates is created under `IdentityMinder.ear\custom\emailTemplates`:

```
default\approved  
default\completed  
default\pending  
default\rejected
```

The default email template set contains the installed templates that are described in [Email Templates](#) (see page 286). You can add custom templates within the default set. You can also deploy other sets of email templates in directory structures that you define at the same level as the default set. For example, IdentityMinder.ear\custom might contain the following deployed email templates:



For information about how Identity Manager chooses a particular email template within a template set, see [Template Directories](#) (see page 288).

How to Specify a Template Set for an Environment

When you configure email for an Identity Manager environment, you specify the email template set that you want to use for that environment. For information about configuring email for an Identity Manager environment, see the *CA Identity Manager Configuration Guide*.

Template Names

The directories in a custom template set should contain default templates with the same name as those that were installed in the default template set. The default names are listed in [Email Templates](#) (see page 286). Identity Manager uses the default templates when it can find no other template with a name that matches the task or event being executed.

Optionally, you can add additional templates to one or more directories in a template set if you want an email to be generated from a particular template. To do so:

- Assign the template the same name as the task or event for which the email will be generated.
- Place the template in the directory associated with the task or event state for which the email will be generated.

For example, if you want emails to be generated from a particular template when a `CreateUserEvent` is rejected, place a template named `CreateUserEvent.tmpl` in the rejected directory of the environment's template set.

Chapter 14: Reporting

This section contains the following topics:

[How to Generate Reports](#) (see page 311)

[How to Create Custom Reports](#) (see page 323)

[Sample Reports](#) (see page 330)

How to Generate Reports

Identity Manager allows you to perform the following reporting tasks through the User Console:

- Define snapshots
- Schedule the generation of reports
- View the reports inside Identity Manager
- Export reports to other formats

The following table describes the steps to set up reporting in Identity Manager:

Step	Refer to...
1. Configure reporting in the Management Console.	Configure Reporting (see page 312)
2. Create a snapshot definition.	Create Snapshot Definition (see page 313)
3. (Optional) Capture the snapshot data.	Capture Snapshot Data (see page 321)
4. Associate snapshots with report tasks.	Associate Snapshots with Reporting Tasks (see page 321)
5. Run the reports.	Run Reports (see page 322)
6. View reports.	View Reports (see page 323)

Configure Reporting

Configure reporting in Identity Manager to add the connections between Identity Manager, the IAM Report Server, and the Reporting Database. This will add default reports and tasks to Identity Manager as well.

Reporting will need to be configured for each environment where you want to use reports.

To configure reporting

1. In the Management Console, go to the Environment and click Advanced Settings.
2. Click Reports.
3. Enter the Reporting Database connection information.

Important! If you used reporting with an earlier version of Identity Manager, run the one of the following upgrade scripts on the Reporting Database:

- **MS SQL:**

```
C:\Program Files\CA\IAM Suite\Identity
Manager\tools\imrexporthdb\sqlserver\ims_mssql_upgrade_6x_to_8.sql
C:\Program Files\CA\IAM Suite\Identity
Manager\tools\imrexporthdb\sqlserver\ims_mssql_upgrade_8_to_r12.sql
```

- **Oracle:**

```
C:\Program Files\CA\IAM Suite\Identity
Manager\tools\imrexporthdb\oracle\ims_oracle_upgrade_6x_to_8.sql
C:\Program Files\CA\IAM Suite\Identity
Manager\tools\imrexporthdb\oracle\ims_oracle_upgrade_8_to_r12.sql
```

Note: For more information on the Reporting Database connection information, see the Management Console Online Help.

4. Enter the IAM Report Server (Business Objects) connection information.

Note the following:

- Ensure that you use the fully-qualified hostname of the server.
- Enter the Tomcat port number in the Business Objects Port field.

Note: For more information on the IAM Report Server connection information, see the Management Console Online Help.

5. Click Submit.

All reporting connections are established, and reporting tasks and default reports are installed.

Create a Snapshot Definition

A snapshot reflects the state of objects in Identity Manager at a given time, and extracts this data, which can be used in one or more reports. You must create a snapshot definition before you can export data to the Reporting Database.

To create a snapshot definition

1. Click Reports, Manage Snapshot Definition, Create Snapshot Definition.
2. Create a new snapshot or copy an existing snapshot.
3. Enter the following details under the Profile tab:

Snapshot Definition Name

Specifies the unique name given for the snapshot definition.

Snapshot Definition Description

Displays any additional information to describe the snapshot.

Enabled

Specifies that Identity Manager will create a snapshot based on the current snapshot definition at the scheduled time.

Note: If this option is not selected, the snapshot will not be captured at the scheduled time. Also, the snapshot definition will not be listed in the Capture Snapshot Data screen.

Identifier

Specifies the [Snapshot Parameters XML file](#) (see page 314) that defines the objects and their attributes, which will be exported into the Reporting Database. ExportAll.xml is the default Identifier file that will export all data for reporting. The sample Identifier files are located in the following directory:

IdentityMinder.ear\config\com\netegrity\config\imreexport\sample

Note: Previously, these files were known as export command files and were used by the imreexport tool. If you used reporting in a previous version of Identity Manager and have existing export command files, move them to the Identifier file directory for management in the User Console.

Keep Last

Specifies the number of successful snapshots to be stored in the Reporting Database.

Note: The number of snapshots should be greater than zero. If you do not specify a value for this field, Identity Manager will store unlimited snapshots.

4. Click the Recurrence tab to schedule the exporting of snapshot data for a later date and time.

The scheduling details for the snapshot definition appear.

Important! Exporting snapshot data can take a long time if you have a large amount of data to export. We recommend you schedule your snapshots with this in mind. If you do not schedule the snapshot, manually export the snapshot data using the [Capture Snapshot Data](#) (see page 321) screen.

5. Click Submit.

Identity Manager is configured to create snapshots of the objects mentioned in the Identifier XML file.

The Snapshot Parameter XML File

Identity Manager reports enable you to see the current state of an Identity Manager environment. You can use this information to ensure compliance with internal business policies or external regulations.

You generate Identity Manager reports from *management data*, which describes the relationship between objects in an Identity Manager environment. Examples of management data include the following:

- A user's profile attributes
- A list of roles that contain a certain task
- The members of a role or group
- The rules that comprise a role

Use the Snapshot Parameter XML file to define the management data you want to use in reports.

Configure the Snapshot Parameter XML File

To control the data that Identity Manager exports, create a Snapshot Parameter XML file. In this file, list the objects to export and, optionally, supply additional export criteria. Only objects that meet the criteria are exported. For example, you can export information about users who have a certain role.

The Snapshot Parameter XML file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>

<IMRExport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="jar:file:imrexport.jar!/schema/ImrExportCmd.xsd">
<export object="">
  <where attr="" satisfy="" ">
    <value> </value>
  </where>
  <exportattr attr="" ">
</export>
</IMRExport>
```

The Snapshot Parameter XML file contains the following elements:

export

Indicates the object to export. For example, the Export element may export user data.

The export element can include one or more exportattr and where elements, which enable you to export only data that meets certain criteria. If there are no exportattr or where elements specified, all of the data for the object is exported. The export element has only the object parameter. The following table lists the possible values for the object parameter and its associated attributes:

Object	Attributes
role	You can use the name filter. name —the roles that satisfy the filter For example, to export a list of roles that include Manager in the name, specify the following: <pre><export object="role"> <where attr="name" satisfy="ANY"> <value op="CONTAINS">Manager</value> </where></pre>
user	Any well-known or physical attribute or any of the following filters: ■ groups —the members of a group ■ roles —the members of a role ■ orgs —users whose profiles exist in organizations that satisfy the filter

group	Any well-known or physical attribute or the following filter: ■ groups —the list of nested groups within a group that satisfies the filter
organization	Any well-known or physical attribute
useraccount	Any well-known or physical attribute or any of the following filters: ■ groups —the members of a group ■ roles —the members of a role ■ orgs —users whose profiles exist in organizations that satisfy the filter For example, to filter by endpoint type, specify the following: <pre><where attr="Namespace" satisfy="ANY"> <value op="EQUALS">*</value> </where></pre> For example, to filter by endpoint, specify the following: <pre><where attr="Endpoint" satisfy="ANY"> <value op="EQUALS">*</value> </where></pre>

exportattr

Indicates a specific attribute to export. Use the exportattr element to export a subset of attributes for the object you are exporting. For example, use the exportattr element to export only a user's ID.

The exportattr element has only the attr parameter. The following table lists the possible values for the attr parameter:

Attribute	Values
role	You can use any of the following filters: ■ tasks —the list of tasks associated with the role ■ rules —the list of member, admin, owner, and scope rules that apply to the role ■ users —the list of members, administrators, and owners for the role ■ rolemembers —the list of role members ■ roleadmins —the list of role administrators ■ roleowners —the list of role owners

Attribute	Values
user	You can use any of the following filters: ■ <code> all_attributes </code>—the list all available user attributes. Alternatively, you can list physical attributes to be returned ■ <code> groups </code>—the list of all groups where the user is a member of or admin ■ <code> roles </code>—the list of roles where the user is a member, admin or an owner of. ■ <code> identitypolicystatus </code>—the list of the identity policies that apply to a specific user or set of users ■ <code> allocations </code>—the list of policies that are to be applied to a user for the first time ■ <code> reallocations </code>—the list of policies that will be reapplied to a user ■ <code> deallocations </code>—the list of policies that no longer apply to a user because the user no longer matches the policy condition
group	You can use any well-known or physical attribute or any of the following filters: ■ <code> all_attributes </code>—all of the attributes that are defined for the Group object in the directory configuration file (<code>directory.xml</code>). Alternatively you can list the physical attributes to be returned ■ <code> groups </code>—the nested groups within the group ■ <code> users </code>—the members of the group ■ <code> groupadmins </code>—the users who are administrators of specified group ■ <code> groupmembers </code>—the users who are members of specified group ■ <code> users </code>—the group administrators and members

Attribute	Values
organization	You can use any well-known or physical attribute or any of the following filters: ■ all_attributes —all of the attributes that are defined for the Organization object in the directory configuration file (directory.xml) ■ orgs —the members of the organization ■ groups —all groups in the organization ■ users —all users in the organization
identityPolicySet	You can use any of the following filters: ■ identitypolicystatus —a list of the identity policies that apply to a specific user or set of users ■ all_attributes —a list of all policy sets, policies, and actions ■ identitypolicyset —exports the details of an identity policy set ■ identitypolicies —the list of policy sets that meet the filter criteria and the policies associated with each policy set

Attribute	Values
useraccounts	You can export any account specific attribute by modifying the mapping file (see page 320) (use imname) or using any of the following filters: ■ accountdata —saving account name, endpoint, container, domain and type ■ statistics —when the account was created and modified ■ assignmentinfo —who created and approved the account and why ■ syncwithroles —whether the account is redundant to user provisioning roles or not ■ entitlementattributes —export all entitlement attributes that exists in the mapping file ■ users —Global users that meets the filter. If you chose to export users you can specify any of user object export attributes ■ all_attributes —will export all available user attributes. ■ groups —friendly name of a group. This search will return group members ■ roles —friendly name of a role. This search will return role members ■ orgs —friendly name of an organization. This search will return organization members ■ allocations —This contains the names of any policies which need to allocated to the user for the first time ■ reallocations —This contains the name of policies which need to be reallocated to the user ■ deallocations —This contains the names of policies which need to be deallocated from the user ■ identitypolicystatus —This will trigger the inclusion of allocations, reallocations, and deallocations in the user

value

Defines a condition that an object or attribute in the corresponding where element meet to be exported.

The value element requires the operator (op) parameter. The operator can be EQUALS or CONTAINS.

where

Filters the data that is exported based on specific criteria. You can specify multiple where elements.

The where and value elements are used to form a search filter. A where element must include at least one value element. For example, you can use where and value elements to export the tasks for enabled roles:

```
<export object="role">
  <where attr="enabled" satisfy="ALL">
    <value op=EQUALS>Yes</value>
  </where>
  <exportattr attr="[tasks]">
</export>
```

You can specify where and value elements for the export and exportattr elements. The following table describes the parameters for the where element:

Parameter	Description
attr	Indicates the attribute to use in a filter. For example, if you specify the enabled attribute, Identity Manager checks the value of the enabled attribute to determine whether or not to export the role.
satisfy	Indicates whether some or all of the value evaluations must be satisfied for the attribute to be displayed. ■ ALL—An attribute or object must satisfy all of the value evaluations. ■ ANY—An attribute or object must satisfy at least one value evaluation.

Control Specific Attributes to be Exported

If you want a snapshot to export an attribute for an endpoint account, edit the endpoint type IM2JIAM mapping file, which is located in the following directory:

IdentityMinder.ear\custom\provisioning\im2jiammapping

Edit the attribute element within the mapping file and set isEntitlementment = "true" and restart the application server.

For example,

```
<attribute imname="createStatistics" etname="createStatistics" type="String" permission="READONLY"
description="Information about account creation" isEntitlementment="true" />
```

Note: You can export as many attributes as you want.

Managing Snapshots

Identity Manager lets you view, modify and delete your snapshot definitions. When you view or modify a snapshot definition, the Profile, Recurrence, and Maintenance tabs are shown. The Maintenance tab will only appear after a snapshot definition has been captured once. From the Maintenance tab, you can delete your snapshots (even if the status of the snapshot is failed).

To view, modify, or delete a snapshot definition, go to Reports, Manage Snapshot Definition and click on the task you want to execute.

Capture Snapshot Data

If you want to capture snapshot data on demand (instead of scheduling a snapshot definition), run the Capture Snapshot Data task to export the data immediately (defined by a snapshot definition) to the Reporting Database.

Important! Exporting snapshot data can take a long time if you have a large amount of data to export. We recommend you [schedule](#) (see page 313) your snapshots when exporting a lot of data.

To capture snapshot data

1. In the User Console, go to Reports, Tasks, Capture Snapshot Data.
2. Choose a snapshot definition.
3. Click Submit.

Snapshot data is exported to the Reporting Database.

Associate Snapshots with Report Tasks

To associate a snapshot definition with a report task

1. Go to Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for the report task you want to associate a snapshot with.
3. Go to the Tabs Tab and click the  next to the Report Snapshot Scheduler tab.
4. Click Add.
5. Search for the snapshot to associate with the report task and click Select.

The snapshot will be associated with that reporting task.

When associating a snapshot definition with a report task, note the following:

- A report can be associated with one or more snapshot definitions.
- A snapshot definition can be associated with more than one report.

Run Reports

You can generate reports within Identity Manager.

To generate a report

1. Go to Reports, Tasks, Run Report.
A list of reports appears in the left frame.
2. Select the report you want to generate.
A Parameters screen appears.
3. Select the snapshot that you want to use and enter the parameter value.
Note: If snapshots are not available for this report, you must first capture a snapshot.
4. Click OK.
The selected value is passed as an input parameter to the report and the scheduler screen appears.
5. Select a schedule for your reports, and click OK.
The report is submitted to the IAM Report Server.

More Information

[Report Scheduler](#) (see page 322)

Report Scheduler

Some reports may take a long time to run, or you may want to view the same report multiple times without re-running the report each time you view it. The report scheduler allows you to schedule the automatic generation of a report to occur at a later time. Once the report is generated, you can view the report multiple times without re-running the report.

You can use the following options to schedule reports. Based on the scheduling option you select, Identity Manager displays more options. Based on the scheduling option you may have to specify the start time, start date, end time, and end date.

Now

Specifies that the report is run immediately.

Once

Specifies that the report is run only once. You must select the start date, end date, start time, and end time when you want to generate the report.

View Reports

To view reports

1. Click View My Reports.

Identity Manager retrieves a list of generated reports.

2. Choose the report you want, and click Select.

The report is displayed in Identity Manager.

3. (Optional) Click Export this report (top left corner) to export the report to the following formats:

- Crystal Report
- Excel
- PDF

How to Create Custom Reports

Identity Manager allows you to create and customize reports to suit your business needs.

The following table describes the steps to create custom reports in Identity Manager:

Step	Refer to...
1. Create a report in Crystal Reports Developer.	Create a report in Crystal Reports (see page 324)
2. Create the Report Parameter XML file.	Create the Report Parameter XML File (see page 324)
3. Upload reports and Report Parameter XML files to the IAM Report Server.	Upload Report and Report Parameter XML File (see page 325)
4. Create the Report Tasks.	Create the Report Tasks (see page 326)
5. Generate Reports in Identity Manager	How to Generate Reports in Identity Manager (see page 311)

Create a report in Crystal Reports

Identity Manager lets you create your own custom reports to meet your business needs. In order to use custom reports in Identity Manager, create a report (RPT file) in Crystal Reports Developer. For more information on how to create a report in Crystal Reports, refer to your Crystal Reports documentation.

Create the Report Parameter XML File

In Identity Manager, reports provide their own search screen so that a user can enter or select required data during the generation of a report. A parameter is one of the fields in a report that can be used to filter reports. You can generate a report by filtering the data using parameters. To allow the customization of the report search screen, each report (RPT file) is associated with a Report Parameter XML file.

The Report Parameter XML file has the following elements:

Product

Identifies the product for which the parameters are used. You can create different parameters for multiple products using the same parameter XML file.

Screen

Identifies the Screen element, which contains the parameters that will be displayed on a specific screen. You can use the screen element to bind the parameters to a specific screen. The screen ID used in this element is used to identify the screens and their parameters.

Parameters

Identifies the start of the Parameters element. The parameters for a specific screen are displayed in this element.

Param ID

Identifies the parameters by the parameter type, name, ID, default value, sql query or java class which retrieves the value for the parameter.

Note: The Report Parameter XML file must have the same name as the report (RPT file) with a .xml extension. For example, if you upload a report called test.rpt into the IAM Report Server, your XML file should be named test.rpt.xml.

Example Report Parameter XML File

The following is an example of the Report Parameter XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<product xmlns="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsi="http://www.example.org/Parameters"
xsi:schemaLocation="http://www.example.org/Parameters
../reporting/src/com/ca/ims/reporting/utls/Parameters.xsd">
  <!--The following is required only if you want to use a database connection that is different from the database
  connection set previously in the Management Console. Use Connection Management tasks to create the new
  connection and provide the ID in the "id" attributes that follow.
  <connection_info id="REPORT_DSN" classification="rpt_dsn_type"/>
  <connection_info id="rptParamConn" conn_type="rptParamConn"
  classification="conn_mo_type" />
  <screen id="1">
    <parameters>
      <param id="param1" displaytext="User" name="User" type="string"/>
    </parameters>
  </screen>
  <screen id="Test">
    <parameters>
      <!--Provide the "conn_id" attribute that follows if you have defined the <connection> element previously.
      Otherwise, this parameter will use the reporting connection information you defined in the Management Console.
      <param id="Test" displaytext="Test" name="Test" type="sqlstr" conn_id="rptParamConn"
      multiselect="true" rows="3"
      sql="select CUSTOMERID, CONTACTNAME from customers where customerid like '##param1##'"
      />
    </parameters>
  </screen>
</product>
```

Upload Report and Report Parameter XML File

After you create the report and the corresponding Report Parameter XML file, upload the reports to the IAM Report Server (Business Objects).

To upload a report and the Report Parameter XML file

1. Log in to the Business Objects Central Management Console.
2. Click on Folders.
3. Select the IM Reports folder.
4. Click on New Object and ensure the object is of type Crystal Reports.
5. Browse for the new report (RPT file) you created.

6. Ensure you have the IM Reports folder selected as the folder to save the report in.
7. Click Submit.
8. Click on IM Reports in the top, left corner.
9. Click on New Object and ensure the object is of type Text.
10. Browse for the new Report Parameter XML you created.
11. Ensure you have the IM Reports folder selected as the folder to save the report in.
12. Click Submit.
13. Go to the IM Reports folder and verify that both new files are available.

Create the Report Tasks

Report tasks are used to create, manage, view, and delete the templates for the reports that are generated in the Identity Manager User Console. The process for creating a report task is similar to creating an admin task in Identity Manager.

To create a task for reports

1. Go to Roles and Tasks, Admin Tasks, Create Admin Task.
2. Select Create a new admin task and click OK.
3. Complete the [profile tab](#) (see page 327).
4. Complete the [search tab](#) (see page 327).
5. Complete the [tabs tab](#) (see page 329).

Note: A report type (RPT file) can only be associated with one reporting task.

More Information:

[Profile Tab for Report Tasks](#) (see page 327)

[Search Tab for Report Tasks](#) (see page 327)

[Tabs Tab for Report Tasks](#) (see page 329)

Profile Tab for Report Tasks

To enter the Profile information for a Report Task, click on the Profile tab and complete the following fields:

Name

Defines the name of the report. Each report task name should be unique.

Tag

Defines a unique identifier for the task. It is used in a URL, a web service, or a properties files. It must consist of letters, numbers, and/or underscores, beginning with a letter or underscore.

Category

Specifies the category to which the current task belongs. Select Reporting as the category for this task.

Category 2

Specifies the sub category to which the current task belongs. Enter any string in this field.

Primary Object

Specifies the object on which the task operates. Select Report Instance as the primary object.

Action

Specifies the action that is performed on the primary object. Select Create.

Search Tab for Report Tasks

The search screen limits the scope of the task and control the fields that users can search. You can configure the search screen for reports based on whether or not you want to pass parameters dynamically to the reports.

You must create separate a search screen for each of the reports. The search screen defines the parameters that you can use to filter the report data. When you generate a report, based on the search screen configuration, Identity Manager prompts you to enter the parameters to be used to filter report data. Based on your input, Identity Manager connects to the Reporting Database and retrieves the data that satisfies your criteria.

To enter the Search information for a Report Task, click the Search tab and select a search screen.

Note: Every report has a search screen associated with it. If you do not find the appropriate search screen for your report, you must create a new search screen. For more information on creating new search screens for reports, see [Create Search Screen for Reports](#) (see page 328).

Create New Search Screen for Report Task

A report search screen is based on the default Report Type Selection screen.

To create a search screen for a report

1. Click  to locate search screens.

The list of available search screens is displayed.

2. Click New.

The Create Screen pane appears.

3. Select Report Type Selection Screen from the list, and click OK.

Identity Manager connects to the IAM Report Server and displays all the reports and their search criteria based on the `suitereports.properties` file.

4. Complete the following fields:

Name

Defines the name of the report. Each report task name should be unique.

Tag

Defines a unique identifier for the task. It is used in a URL or a web service or properties files. It must consist of letters, numbers, numbers, or underscores, beginning with a letter or underscore.

Title

Defines the title of the new search screen. The title must be unique.

Report Type

Identifies the report to associate with the search screen. Choose one of the reports you added to the IAM Report Server.

The new search screen is created for reports.

5. Click Ok.

Tabs Tab for Report Tasks

Tabs organize the fields that are required to execute a task. The Tabs tab in a report allows you to associate a report with a snapshot definition and make a report scheduler available.

To configure the Tabs tab for a report task

1. Click Tabs.

The tabs that will be visible to the user will be displayed.

2. Select the Standard Tab Controller.
3. Select Report Snapshot Scheduler from Which tabs should appear in this task?, and click .

The Report Snapshot Scheduler tab is added to the list of tabs.

4. Click  to edit the Report Snapshot Scheduler tab.

The Configure Report Snapshot Scheduler screen appears.

5. Click Add to associate the report task to a snapshot definition.

A list of available [Snapshot Definitions](#) (see page 314) appear.

6. Select a Snapshot Definition and click OK.

The report task is associated with a Snapshot Definition.

7. Select Report Scheduler from Which tabs should appear in this task?, and click .

8. The Scheduler tab is added to the list of tabs.

9. Click  to edit the Scheduler tab.

10. Click Submit.

The Report Tasks is created.

11. Assign the newly created report task to an Admin Role.

The Identity Manager user who is part of the Admin Role will be able to use the newly created report task.

Report Scheduler

Some reports may take a long time to run, or you may want to view the same report multiple times without re-running the report each time you view it. The report scheduler allows you to schedule the automatic generation of a report to occur at a later time. Once the report is generated, you can view the report multiple times without re-running the report.

You can use the following options to schedule reports. Based on the scheduling option you select, Identity Manager displays more options. Based on the scheduling option you may have to specify the start time, start date, end time, and end date.

Now

Specifies that the report is run immediately.

Once

Specifies that the report is run only once. You must select the start date, end date, start time, and end time when you want to generate the report.

Sample Reports

Identity Manager installs sample reports you can customize to suit your needs. The sample reports are located in the following directory:

MSSQL

C:\Program Files\CA\IAM Suite\Identity Manager\tools\tools\imexport\ReportDefinitions\CR11\Ms-SQL Reports

Oracle

C:\Program Files\CA\IAM Suite\Identity Manager\tools\tools\imexport\ReportDefinitions\CR11\Oracle Reports

The following table describes the sample reports:

Report	Description
Role Members	Displays the roles in the report database and lists the members of those roles.
Roles	Displays the following information for each role in the report database: ■ Tasks associated with the role ■ Member policies and role members ■ Administrator policies and role administrators ■ Owner policies and role owners
Tasks Roles	Displays the tasks in the report database and the roles with which they are associated.
Non-Standard Accounts Trend	Displays non-standard accounts trends for orphan accounts, system accounts, and exception accounts
Non-Standard Accounts	Displays all orphan, system, and exception accounts
Orphan Accounts	Displays all endpoint accounts with no global user in the Provisioning Server
Policies	Displays all identity policies
User Profile	Displays the following information for users: ■ Name ■ User ID ■ Groups where the user is a member or administrator ■ Roles where the user is a member, administrator, or owner

Report	Description
Endpoint Accounts	Displays accounts per endpoint (you can choose which endpoint to view)
Role Administrators	Displays roles and their administrators
Role Owners	Displays roles and their owners
Snapshots	Displays all exported snapshots
User Account	Displays a list of users and their accounts. Note: The list of account attributes presented in this report depends on the attributes exported (see page 320).
User Entitlements	Displays user's roles, groups and accounts. Note: The list of account attributes presented in this report depends on the attributes exported (see page 320).
User Policy Sync Status	Displays the user's status per policy (which policies should be allocated, deallocated or reallocated)

Chapter 15: System Tasks

This section contains the following topics:

[Default System Tasks](#) (see page 333)

[Task Status in Identity Manager](#) (see page 334)

[How Identity Manager Determines Task Status](#) (see page 335)

[The View Submitted Tasks Tab](#) (see page 335)

[User History Tab](#) (see page 344)

[Bulk Loader](#) (see page 349)

[Custom Data for Select Boxes](#) (see page 354)

[Logical Attribute Handlers](#) (see page 361)

[Connection Management](#) (see page 364)

Default System Tasks

Identity Manager includes the following tasks that help administrators to manage an Identity Manager environment:

- **View Submitted Tasks tasks**
Allows administrators to view the status of tasks in the environment.
- **Bulk Loader tasks**
Uploads feeder files that are used to manipulate large numbers of managed objects simultaneously.
- **Select Box Data tasks**
Allows administrators to upload files that are used to populate options in fields, such as select boxes, in admin tasks.
- **Logical Attribute Handler tasks**
Allows administrators to manage logical attributes, which are used to display user store attributes (called physical attributes) in a user-friendly format on task screens.
- **Connection Management tasks**
Configures the database server connection details in Identity Manager.

Task Status in Identity Manager

Administrators may want to track the status of Identity Manager tasks once they are submitted for processing. Identity Manager provides the following methods for viewing task status:

■ View Submitted Tasks Tab

This tab allows you to search for and display Identity Manager tasks that have been submitted for processing.

Administrators can view task details at a high level or view additional levels of detail.

The View Submitted Tasks tab is included in two default tasks:

- View My Submitted Tasks

Allows administrators to search for and display information about tasks that they submitted for processing.

- View Submitted Tasks

Allows administrators to search for and display information about tasks that other administrators have submitted for processing.

■ User History Tab

This tab, which you can add to user tasks, such as View or Modify User, lets administrators view the following information for a selected user:

- Tasks performed on the user
- Tasks performed by the user
- Workflow approvals by the user

■ Reports

Identity Manager reports enable you to see the current state of an Identity Manager environment. You can use this information to ensure compliance with internal business policies or external regulations.

[Reporting](#) (see page 311) provides additional information about setting up and using reports.

■ Logs

Display information about all of the components in an Identity Manager installation, and provide details about all operations in Identity Manager.

See the *Configuration Guide* for more information about Identity Manager logs.

How Identity Manager Determines Task Status

A *task* is an administrative function that a user can perform in Identity Manager. Tasks include *events*, actions that Identity Manager performs to complete the task. A task may include multiple events. For example, the Create User task may include events that create the user's profile, adds the user to a group, and assigns roles.

Identity Manager tasks and events can be associated with a workflow process, which determines how Identity Manager performs the required actions, and other custom business logic. Tasks may also be associated with other tasks, called nested tasks. In this case, Identity Manager processes the nested tasks with the original task.

The status of a task depends on the status of its associated events, workflow processes, nested tasks, and custom business logic.

The View Submitted Tasks Tab

Identity Manager includes a View Submitted Tasks tab that provides information about tasks in an Identity Manager environment. You can use this tab to search for and view high-level details about actions that Identity Manager performs. Detail screens provide additional details about each task and event.

Based on the status of the task, you can cancel or resubmit a task.

The View Submitted Tasks tab allows you to track the processing of a task from beginning to end. For example, if an Identity Manager task includes provisioning role assignment, and that assignment triggers the creation of accounts in other systems, The View Submitted Tasks tab displays all of the details of the original task and the details of the account creations.

Note: For more information about provisioning, see the *Provisioning Guide*.

By default, Identity Manager includes the View Submitted Tasks tab in two tasks:

- View Submitted Tasks
- View My Submitted Tasks

Search for Submitted Tasks

Perform the following steps to search for submitted tasks.

To search for submitted tasks

1. Click System, View Submitted Tasks.

The View Submitted Tasks page appears.

2. Specify search criteria, enter the number of rows to be displayed, and click Search.

The tasks that satisfy your search criteria are displayed.

Note: For more information on specifying attributes in the search criteria, see [Search Attributes for Viewing Submitted Tasks](#) (see page 336).

Search Attributes for Viewing Submitted Tasks

To review tasks that have been submitted for processing, you can use the search feature in View Submitted Tasks. You can search for tasks based on the following criteria:

Initiated By

Identifies the name of the user who has initiated a task as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Approved By

Identifies the name of the task approver as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Note: If you select Approved by criteria to filter the tasks, the Show approval tasks criteria is also enabled by default.

Task Name

Identifies the task name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where Task Name field. For example, you can specify the search criteria "task name equals Create User" by selecting the equals condition, and entering Create User in the text field.

Task Status

Identifies task status as the search criteria. You can select the task status by enabling Where task status equals, and selecting the condition. You can further refine the search based on the following conditions:

- Completed
- In Progress
- Failed
- Rejected
- Partially Completed
- Cancelled
- Scheduled

Note: See [Task Status Description](#) (see page 338) for more information.

Task Priority

Identifies task priority as the search criteria. You can select the task priority by enabling Where task priority equals, and selecting the condition. You can further refine the search based on the following conditions:

Low

Specifies that you can search for tasks that have a low priority.

Medium

Specifies that you can search for tasks that have a medium priority.

High

Specifies that you can search for tasks that have a high priority.

Performed On

Identifies tasks that are performed on the selected instance of the object. If you do not select an instance of the object, the tasks that were performed on all the instances of that object will be displayed.

Note: This field appears only when the Configure Performed On field is populated in the Configure Submitted Tasks screen. You use this screen to configure the Submitted Tasks tab. See the online help for that screen for more information.

Date range

Identifies the dates between which you want to search submitted tasks. You must provide the From and To dates.

Show unsubmitted tasks

Identifies the tasks in the Audited state. Identifies the tasks that have initiated other tasks or tasks that have not been submitted. All such tasks will be audited and displayed if you select this tab.

Show approval tasks

Identifies the tasks that have to be approved as part of a workflow.

More Information:

[Task Status Description](#) (see page 338)

Task Status Description

A submitted task exists in one of the states described below. Based on the state of the task, you can perform actions such as cancelling or resubmitting a task.

Note: To cancel or resubmit a task, you must configure View Submitted Tasks to display the cancel and resubmit buttons based on the tasks status. For more information on cancelling and resubmitting tasks, see [Customize the View Submitted Tasks Tab](#) (see page 341).

In progress

Displayed when any of the following occurs:

- Workflow is initiated but not yet completed
- Tasks, which are initiated before the current tasks, are in progress
- Nested tasks are initiated but not yet completed
- The primary event is initiated but not yet completed
- Secondary events are initiated but not yet completed

You can cancel a task in this state.

Note: Cancelling a task will cancel all the incomplete nested tasks and events for the current task.

Cancelled

Displayed when you cancel any of the tasks or events in progress.

Rejected

Displayed when Identity Manager rejects an event or task that is part of a workflow process. You can resubmit a rejected task.

Note: When you resubmit a task, Identity Manager will resubmit all the failed or rejected nested tasks and events.

Partially Completed

Displayed when you cancel some of the events or nested tasks. You can resubmit a partially completed event or nested task.

Completed

Displayed when a task is completed. A task is completed when the nested tasks and nested events of the current task are completed.

Failed

Displayed when a task, nested task, or event nested in the current task are invalid. This status is displayed when the task fails. You can resubmit a failed task.

Scheduled

Displayed when the task is scheduled to execute at a later date. You can cancel a task in this state.

Audited

Displayed when the current task is audited.

View Task Details

Identity Manager provides task details, such as the status of a submitted task, nested tasks, and events associated with a task.

To view details of a submitted task

1. Click the right arrow icon next to the selected task in the View Submitted Tasks tab.

The task details appear.

Note: Events and nested tasks (if any) are displayed in the Task Details page. You can view the task details for each of the tasks and events.

2. Click Close.

The Task Details tab closes and Identity Manager displays the View Submitted Tasks tab with the tasks list.

View Event Details

Identity Manager provides events details, such as the status of a submitted event, event attributes, and any additional information about the events.

To view details of a submitted event

1. Click the right arrow icon next to an event in the View Task Details page.
The event details appear.
2. Click Close.
The Event Details page is closed.

Description of Event Status

Events in Identity Manager can be in one of the states described below. Based on the event status, you can cancel or resubmit an event for execution.

Note: To allow administrators to cancel or resubmit an event, you must configure View Submitted Tasks to display the Cancel and Resubmit Events buttons. When you configure the task, you can specify which administrators can cancel and resubmit events. For more information on cancelling and resubmitting events, see [Customize the View Submitted Tasks Tab](#) (see page 341).

In progress

Displayed when any of the following occurs:

- Workflow or pre-events are initiated, in progress, or approved
- Identity Manager is executing the event
- Identity Manager executes post events

You can cancel an event in this state.

Rejected

Displayed when Identity Manager rejects an event that is part of the workflow. You can resubmit a rejected event.

Cancelled

Displayed when you cancel any of the events in progress. You can resubmit a cancelled event.

Completed

Displayed when an event is completed.

Failed

Displayed when Identity Manager encounters an exception during execution of an event. You can resubmit a cancelled event.

Note: You cannot resubmit a secondary event until the primary event is in the completed state.

Scheduled

Displayed when the event is scheduled to execute at a later date. You can cancel an event in this state.

Audited

Displayed when the current event is audited.

Customize the View Submitted Tasks Tab

Administrators can customize the View Submitted Tasks tab as follows:

- Specify a different task name and tag.
- Change the default display properties. As installed, users see a search screen where they can enter criteria that determine the tasks that appear in the tab. Administrators can configure the tab to automatically display the submitted tasks for a current day, preventing users from having to enter search criteria.
- Determine whether audit events appear in the Task Details page.
- Add an additional column to the task display.
- Specify the criteria for cancelling or resubmitting tasks and events.

You can configure the View Submitted Tasks tab by modifying the corresponding admin task.

To configure the View Submitted Tasks tab

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.

The Select Admin Task page appears.

2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Search.

Identity Manager displays the admin tasks that satisfy the search criteria.

3. Select View Submitted Tasks, and click Select.

Identity Manager displays the task details for the View Submitted Tasks admin task.

4. Click the Tabs tab.

The tabs that are used for View Submitted Tasks tab are displayed.

5. Click the right arrow icon to edit the Submitted Tasks tab.
The tab details appear.
6. Edit the fields to customize the View Submitted Tasks tab as needed. See [Configuration Settings for the Submitted Tasks tab](#) (see page 342).

Configuration Settings for the View Submitted Tasks Tab

Use the following fields to change the appearance and functionality of the View Submitted Tasks tab.

Name

Defines the name of the task.

Tag

Defines a unique identifier for the task. It is used in URLs, web services or properties files. It must consist of letters, numbers, or underscores, beginning with a letter or underscore.

Hide Tab

Identifies that the tab is visible to the users, but will not be executed. If you select this option, Identity Manager will display an error to the users.

Show task lists on load

Displays the tasks that have been submitted for the current day.

Note: If you have enabled this option, users clicking on View Submitted Tasks will directly see the tasks that were submitted on the same day.

Show audit events

Specifies if audited events are included in tasks in the View Submitted Tasks page.

Allow custom column

Indicates that you can append a custom column to the tasks table that you can view from the View Submitted Tasks tab and the User History tab. For example, you can append a column "User ID" to the tasks table that is displayed on the User History tab.

Custom column heading

Indicates the display name of the custom column.

Custom column attribute

Indicates the attribute that will be used to populate the custom column in the tasks table. For example, if you are searching for tasks that are performed on employees of an organization, you can append an organization column that displays the organization for each of the employees.

Cancel Tasks and Events

Identifies the criteria for canceling tasks or events. You can set the scope for this field by selecting one of the following options:

Task creator must be current user

Identifies that you can cancel or resubmit tasks or events that you have created.

Task creator must be in scope

Identifies that you can cancel or resubmit tasks that have been initiated by other users who match the user scope rules for the admin role that gives you access to the tab.

For example, you received the User Manager role, which includes View Submitted Tasks, because you met the criteria in a membership rule that includes scope over all users in the Employee organization. You can cancel or resubmit tasks that are submitted by all users in the Employee organization.

No restrictions

Identifies that any user can cancel or resubmit a task or event.

Not allowed

Specifies that a task or event cannot be cancelled or resubmitted.

Resubmit Tasks and Events

Identifies the criteria for resubmitting a task or event. You can set the scope of this field by selecting one of the following options:

Task creator must be current user

Identifies that you can cancel or resubmit tasks or events that you have created.

Task creator must be in scope

Identifies that you can cancel or resubmit tasks that have been initiated by other users who match the user scope rules for the admin role that gives you access to the tab.

For example, you received the User Manager role, which includes View Submitted Tasks, because you met the criteria in a membership rule that includes scope over all users in the Employee organization. You can cancel or resubmit tasks that are submitted by all users in the Employee organization.

No restrictions

Identifies that any user can cancel or resubmit a task or event.

Not allowed

Specifies that a task or event cannot be cancelled or resubmitted.

User History Tab

The User History tab allows you to view tasks that are related to a user. The task details that are displayed in this tab can also be viewed in the View Submitted Tasks tab.

Note: You cannot add this tab to create tasks, such as Create User.

You can use this tab to view a history of the following tasks:

- **Tasks performed on the user**

Displays all the tasks that are performed on the selected user.

- **Tasks performed by the user**

Displays all the tasks that are performed by the selected user.

- **Workflow approvals by the user**

Displays all the tasks that the user has approved as part of a workflow.

Note: The type of tasks that you can view in this tab depend on the tab's configuration. [Customize the User History Tab](#) (see page 345) provides more information.

Search Attributes for Viewing User History

To review tasks that have been submitted for processing, you can use the search feature in View Submitted Tasks. You can search for tasks based on the following criteria:

Task Name

Identifies the task name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where Task Name field. For example, you can specify the search criteria, task name equals Create User by selecting the equals condition, and entering Create User in the text field.

Task Status

Identifies task status as the search criteria. You can select the task status by enabling Where task status equals, and selecting the condition. You can further refine the search based on the following conditions:

- Completed
- In Progress
- Failed
- Rejected
- Partially Completed
- Cancelled
- Scheduled

Note: See [Task Status Description](#) (see page 338) for more information.

Task Priority

Identifies task priority as the search criteria. You can select the task priority by enabling Where task priority equals, and selecting the condition. You can further refine the search based on the following conditions:

Low

Specifies that you can search for tasks that have a low priority.

Medium

Specifies that you can search for tasks that have a medium priority.

High

Specifies that you can search for tasks that have a high priority.

Date range

Identifies the dates between which you want to search submitted tasks. You must provide the From and To dates.

Customize the User History Tab

Administrators can customize the User History tab as follows:

- Specify a different task name and tag.
- Change the default display properties. As installed, users see a search screen where they can enter criteria that determines the tasks that appear in the tab. Administrators can configure the tab to automatically display the tasks for a current day, preventing users from having to enter search criteria.

- Determine whether audit events appear in the Task Details page.
- Add an additional column to the task display.
- Specify the criteria for cancelling or resubmitting tasks and events.

To configure the User History tab

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.
The Select Admin Task page appears.
2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Search.
Identity Manager displays the admin tasks that satisfy the search criteria.
3. Select the task that includes the User History tab, and click Select.
Identity Manager displays the task details for the admin task.
4. Click the Tabs tab.
5. Click the arrow icon  next to the User History tab.
The tab details appear.
6. Edit the fields to customize the User History tab.
See

Configuration Settings for the User History Tab

Use the following fields to change the appearance and functionality of the User History tab.

Name

Defines the name of the task.

Tag

Defines a unique identifier for the task. It is used in URLs, web services or properties files. It must consist of letters, numbers, or underscores, beginning with a letter or underscore.

Hide Tab

Identifies that the tab is visible to the users, but will not be executed. If you select this option, Identity Manager will display an error to the users.

Show task lists on load

Displays the tasks that have been submitted for the current day.

Note: If you have enabled this option, users clicking on View Submitted Tasks will directly see the tasks that were submitted on the same day.

Show audit events

Specifies if audited events are included in tasks in the View Submitted Tasks page.

Allow custom column

Indicates that you can append a custom column to the tasks table that you can view from the View Submitted Tasks tab and the User History tab. For example, you can append a column "User ID" to the tasks table that is displayed on the User History tab.

Custom column heading

Indicates the display name of the custom column.

Custom column attribute

Indicates the attribute that will be used to populate the custom column in the tasks table. For example, if you are searching for tasks that are performed on employees of an organization, you can append an organization column that displays the organization for each of the employees.

Cancel Tasks and Events

Identifies the criteria for canceling tasks or events. You can set the scope for this field by selecting one of the following options:

Task creator must be current user

Identifies that you can cancel or resubmit tasks or events that you have created.

Task creator must be in scope

Identifies that you can cancel or resubmit tasks that have been initiated by other users who match the user scope rules for the admin role that gives you access to the tab.

For example, you received the User Manager role, which includes View Submitted Tasks, because you met the criteria in a membership rule that includes scope over all users in the Employee organization. You can cancel or resubmit tasks that are submitted by all users in the Employee organization.

No restrictions

Identifies that any user can cancel or resubmit a task or event.

Not allowed

Specifies that a task or event cannot be cancelled or resubmitted.

Resubmit Tasks and Events

Identifies the criteria for resubmitting a task or event. You can set the scope of this field by selecting one of the following options:

Task creator must be current user

Identifies that you can cancel or resubmit tasks or events that you have created.

Task creator must be in scope

Identifies that you can cancel or resubmit tasks that have been initiated by other users who match the user scope rules for the admin role that gives you access to the tab.

For example, you received the User Manager role, which includes View Submitted Tasks, because you met the criteria in a membership rule that includes scope over all users in the Employee organization. You can cancel or resubmit tasks that are submitted by all users in the Employee organization.

No restrictions

Identifies that any user can cancel or resubmit a task or event.

Not allowed

Specifies that a task or event cannot be cancelled or resubmitted.

Show Tasks

Determines the tasks that appear in the User History tab.

Tasks performed on the user

Displays all the tasks that are performed on the selected user.

Tasks performed by the user

Displays all the tasks that are performed by the selected user.

Workflow approvals by the user

Displays all the tasks that the user has approved as part of a workflow.

The View User Activity Task

User activity is a history of tasks that involve a specific user. Administrators can use the View User Activity task to track the following user information:

- Tasks performed on the user
- Tasks performed by the user
- Workflow approvals performed by the user

To view user activity

1. Click Users, Manage Users, View User Activity.

The Select User screen appears.

2. Search for a user and click Select.

The View User Activity screen appears.

For more information on the user activity displayed, see the *User Console Online Help*.

Bulk Loader

You can use the Bulk Loader tab to upload feeder files that are used to manipulate large numbers of managed objects simultaneously. For example, you can create 1000 users in Identity Manager manually, or you can use the Bulk Loader. The advantage of the Bulk Loader method is that you can automate the process of manipulating a large number of managed objects using an information (feeder) file. The Bulk Loader task can also be mapped to a workflow process.

Note: For more information on how to map a Bulk Loader task to workflow, see the [Workflow Overview](#) (see page 217).

Add Bulk Loader Task to Admin Roles

To manipulate large numbers of primary objects, use the Bulk Loader task. Log in as a System Manager and configure admin roles to use the Bulk Loader task.

To add the Bulk Loader Task to admin roles

1. Login as the System Manager.
2. Click Roles and Tasks.

The tasks for Roles and Tasks appear.

3. Click Admin Roles, Modify Admin Roles.
The Admin Role Search screen appears.
4. Search for the admin role for which you want to add the Bulk Loader Task, and click OK.
The Admin Role details appear.
5. In the Tasks tab, add a new task with the following options:
Category
Select System as the category.
Task
Select Bulk Loader as the task.
6. Click Submit.
The Admin Role is configured with the Bulk Loader task.

How to Use the Bulk Loader

You must perform the following steps to manipulate a large number of users, groups, or organizations.

1. Create a CSV feeder file.
2. Upload the feeder file.
3. Configure the Loader Records Details tab.
4. Select a primary object and identify the action to perform on the object.
5. View and modify the progress of the Bulk Loader task from the View Submitted Tasks tab.

Note: If the Identity Manager server goes down during a long running task, such as uploading a large number of objects, you can restart the task in the View Submitted Tasks tab. When the task restarts, it begins from the last successfully executed record.

Create a Feeder File

Each feeder file contains data that can be used to manage large numbers of primary objects automatically.

To create a feeder file

1. Create a CSV text file using a text editor. Use the appropriate file [format](#) (see page 351).
2. Save the file. You will upload this file into the Environment where you want to manipulate large numbers of primary objects.

Feeder File Format

A Bulk Loader file is used to automate repeated actions performed on a large number of managed objects. When you upload a feeder file, Identity Manager parses and reads the feeder file.

The feeder file must have a CSV extension and should have the following properties:

- The file must contain a header which specifies the physical attributes or well-known attribute names of a managed object.
- Each row in the feeder file is called a record. The records contain the values for each of the attributes specified by the header line. The following options are acceptable values for an attribute:
 - Value—the attribute will be set to the value you specify.
 - ' ' (blank)—the attribute will not be changed.
 - NULL—the attribute will be deleted.
- The header line must include a column that indicates the action that should be performed on the records. The column name and the values themselves can contain any non-empty values.

Example CSV feeder file

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL
create,JD,John,Doe,John Doe,test,Johndoe@a.com
Modify,MD,Jane,Doe,Jane Doe,test,Marydoe@a.com
create,BD,Baby,Doe,Baby Doe,test,Babydoe@a.com
```

In the preceding code, the feeder file has the following properties:

Header

The first line of the code is the header line. The header line has physical attributes or well-known attributes for the managed object 'User'.

Action

The action column identifies the task that should be performed for each record. For example, the preceding file specifies that a 'create' action should be performed on the First Name 'John'.

Enable Email Notification for Feeder Tasks

To set email notifications for Bulk Loader tasks as part of a workflow process, enable email notifications in the Management Console for the BulkLoader Event or the Bulk Loader task.

Note: For more information on Email Notifications, see the Management Console Online Help.

Modify Parser File for Bulk Loader

To modify the parser Identity Manager uses to parse feeder files, and to schedule the implementation of the Bulk Loader task, you must configure the corresponding admin task.

To modify the Bulk Loader admin task

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.
The Select Admin Task page appears.
2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Search.
Identity Manager displays the admin tasks that satisfy the search criteria.
3. Select an admin task, and click Select.
Identity Manager displays the task details for the selected admin task.
4. Choose the Search tab for the Bulk Loader task.
5. Click  to locate search screens.
The list of available search screens is displayed.
6. Select a Search screen from the Select Screen Definition tab, and click Edit.
The Search screen details appear.
7. (Optional) Edit the Parser Fully Qualified Name.
The Parser Fully Qualified Name should match the name of your parser file.

Note: The sample parser provided by Identity Manager is displayed as the default value. The sample parser file is used to parse CSV files. The sample parser file provided by Identity Manager is in the following location:

C:\Program Files\CA\IAM Suite\Identity Manager\tools\samples\feeder

8. (Optional) [Add a Scheduler tab](#) (see page 104) to Bulk Loader.
9. Click Submit.

Web Service Support for Bulk Loader

The Bulk Loader has a Web service API that can be called using the Identity Manager Task Execution Web Service (TEWS) interface. TEWS allows client applications to submit remote tasks to Identity Manager for execution. This interface implements the WSDL and SOAP open standards to provide remote access to Identity Manager.

Identity Manager includes Java client samples that demonstrate calling the Bulk Loader as a Web service. The Java samples are located in the following source file:

```
samples\WebService\Axis\optional\ObjectFeeder.java
```

Data samples and documentation for calling the Bulk Loader as a Web service are located in the following directory:

```
samples\Feeder\
```

Note: For more information about configuring and using TEWS, see the *Programming Guide for Java*.

Bulk Loader Memory Considerations

If you use the Bulk Loader to import a large number of users, you may see out-of-memory exceptions. Additionally, some tasks, which require significant resources, may fail if they run while the Bulk Loader imports a large number of users.

To address these issues, consider the following:

- Add a batch server to your Identity Manager implementation to handle large imports

Note: For more information about adding a batch server, see the *Implementation Guide*.

- Increase the JVM memory settings

Custom Data for Select Boxes

Identity Manager task screens include fields that allow users to select a value. These fields include the following:

- Check Box Multi-Select
- Dropdown
- Dropdown Combo
- Multi-Select
- Option Selector
- Option Selector Combo
- Radio Button Single-Select
- Single-Select

You can specify custom data that you want to use to populate select boxes in XML files. For example, you can use the Select Box Data XML files to populate options for a City or State drop down box on a Profile tab for the Create User task.

You can also use the Select Box Data XML file to configure a dependency between two fields in a task screen. For example, the options that are available in the City field may depend on the option a user chooses in the State field.

How to Populate Fields Using Select Box Data

To populate a field using Select Box Data, you must perform the following tasks:

1. Create a Select Box Data XML file.
2. Import the Select Box Data XML file in Identity Manager.
3. Configure fields to use Select Box Data XML files.

Create a Select Box Data XML File

Each Select Box Data XML file contains data that can be used to populate the options for a Identity Manager User Console control.

To create a Select Box Data XML file

1. Create a text file with an .XML extension using a text or XML editor.
2. Create a file using the format described in [Select Box Data XML File](#) (see page 355).
3. Save the file.

You import this file into an Identity Manager environment to populate the options in Identity Manager User Console controls.

The Select Box Data XML File

The Select Box Data XML file is a tree-based collection of elements and child elements. You can populate fields in any Identity Manager profile screen with elements or child elements in a Select Box Data XML file. After creating the XML file, you can import it using Import Select Box Data task in the User Console.

The following code shows an example of a Select Data XML file that populates the state names and city names when the country is selected as Australia or UK:

```
<places name="places" displayName="places">
  <country name="AU" displayName="Australia">
    <state name="VIC" displayName="Victoria">
      <city name="MEL" displayName="Melbourne"/>
      <city name="GEEL" displayName="Geelong"/>
      <city name="BAL" displayName="Ballarat"/>
    </state>
    <state name="NSW" displayName="New South Wales">
      <city name="SYD" displayName="Sydney"/>
      <city name="NCL" displayName="Newcastle"/>
      <city name="WOD" displayName="Wodonga"/>
    </state>
    <state name="QLD" displayName="Queensland">
      <city name="BRIS" displayName="Brisbane"/>
      <city name="CNS" displayName="Cairns"/>
      <city name="TVL" displayName="Townesville"/>
    </state>
  </country>
```

```
<country name="UK" displayname="UK">
  <state name="SU" displayname="Surrey">
    <city name="LON" displayname="London"/>
    <city name="READ" displayname="Reading"/>
  </state>
  <state name="WLS" displayname="Wales">
    <city name="CDF" displayname="Cardiff"/>
    <city name="SWN" displayname="Swansea"/>
  </state>
</country>
</places>
```

Note: The Identity Manager Tools include a sample Select Box Data XML file, which is installed in the following location:

IdentityManager_tools\samples\SelectBoxData

IdentityManager_tools is the installed location of the Identity Manager tools. For example, if you installed the tools on a Windows system, the complete path would be the following:

C:\Program Files\CA\IAM
Suite\IdentityManager\tools\samples\SelectBoxData

For more information about the sample, see the readme.txt file in the SelectBoxData directory.

Description of Select Box Data XML File

The Select Box Data XML file is organized as follows:

Root Element

Identifies the Select Box Data XML file. There is only one root element per Select Box Data XML file. The root element is a container for all the elements and child elements. In the example code in the preceding topic, places is the root element. These elements cannot be used to populate the fields.

Provider Element

Specifies the nodes in the tree of a Select Box Data XML file. These elements contain the options that you can use to populate fields in Identity Manager. The provider element does not have a parent element. For example, if you create two dependent fields that have options 'Melbourne' and 'Victoria', the corresponding elements in the Select Box Data XML file must belong to the same provider element. In the illustration below, the city 'Melbourne' is dependent on the state 'Victoria'. The provider element for both the options is 'Australia'.

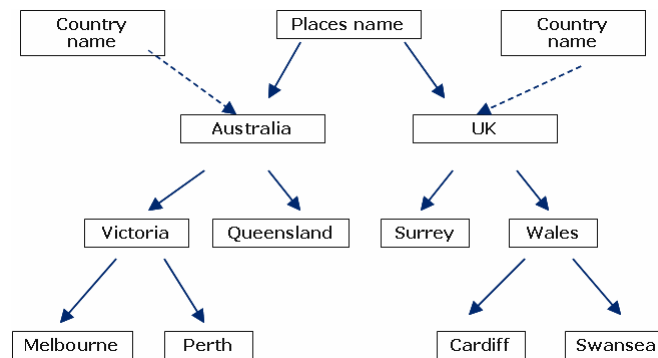
Elements

Any XML element in Select Box Data XML File is identified as an element. An element can be a parent element or a child element. In the following illustration, 'Victoria' is a parent element of 'Melbourne'. Similarly 'Victoria' is a child element of 'Australia'.

Child Elements

All the XML elements that are contained as part of elements higher in the tree structure are called child elements.

The following illustration identifies the Select Box Data structure for the example in the preceding topic.



Each element is identified by the following attributes:

Display Name

Identifies the element name which is displayed when the element appears in the Identity Manager User Console. For example, Melbourne and Queensland are the display names.

Type

Identifies the type of element. In the example in the preceding topic, state name and city name are type elements.

Note: In the Identity Manager User Console Display Name is referred to as Child Name and Type is referred to as Child Type.

Import the Select Box Data XML File

The Select Box Data XML file includes elements that Identity Manager uses as options in select box fields on task screens. You must import the Select Box Data into Identity Manager environment to use the elements.

To import Select Box Data XML file

1. Click System, Tasks, Select Box Data, Import Select Box Data.

The Import Select Box Data page appears.

2. Click Create Provider.

The Create Select Box Data page appears.

3. Complete the following fields:

Name

Identifies the unique name for each of the Select Box Data XML file. The identifier name should be unique. Identity Manager validates the uniqueness of the identifier name.

Description

Identifies more information about the Select Box Data XML file.

Precedence

Identifies the precedence of the Select Box Data XML file compared to other Select Box Data XML files. Precedence should be numeric.

4. Click Browse to search for the XML file, locate the XML file and click Create.

The XML file is imported.

5. Click Close.

The newly imported Select Box Data XML file is displayed in the list.

Configure Fields to Use Select Box Data XML Files

Configure fields in a task screen to use Select Box Data XML files as the source of selection for options fields.

To configure fields to use Select Box Data

1. Click Roles and Tasks, Admin Tasks, Modify Admin Tasks.
The Select Admin Task page appears.
2. Select Name or Category in the Search Admin Task where field, enter the string you want to search, and click Search.
Identity Manager displays the admin tasks that satisfy the search criteria.
3. Select an admin task, and click Select.
Identity Manager displays the task details for the selected admin task.
4. Click the Tabs tab.
The tabs page appears.
5. Click the right arrow icon to edit the Profile tab.
The Profile tab for the admin task appears.
6. Click the ellipses (...) button for the Screen field to display the list of profile screen definitions for this task.
7. Select a profile screen definition and click Edit.
The fields that are configured to be displayed on the profile tab appear.
8. Add or select a field on the profile screen and click the right arrow icon to display the field properties.
9. Complete the properties for the field you have added in step 8. Set Style to one of the following values:
 - Check Box Multi-Select
 - Dropdown
 - Dropdown Combo
 - Multi-Select
 - Option Selector
 - Option Selector Combo
 - Radio Button Single-Select
 - Single-Select

The Source of selection options field appears.

10. Select *one* of the following options for the Source of selection options field.

Select Box Data Options

Specifies that the field will be populated from a Select Box Data XML file. If you select this option, the Edit for the Select Box Data for Options appears.

Click Edit for the Select Box Data for Options and use the following options to select the values that you want to display for this field.

Child Name Filter

Identifies the name of the element or child element in a Select Box Data XML file.

Child Type Filter

Identifies the type of the element or child element in a Select Box Data XML file.

For more information on element name and element types, see [The Select Box Data XML File](#) (see page 355) .

Note: The values you can select from this field are populated from the Select Box Data XML file you have imported into Identity Manager.

Depends on the value of another field

Specifies that the field will be populated based on the values selected in another field. If you have selected this option, see [How to Create Dependent Fields Using Select Box Data](#) (see page 361).

Select an existing field on the form Options source field.

11. Select one of the values for Preserve non-options field.
12. Complete the other necessary field properties and click Apply.
13. Click OK to save the changes.

The fields that you have configured will appear to the user on the profile tab of the selected admin task. The values for select-based controls that are configured to use Select Box Data as source will be populated with the values from the Select Box Data XML file.

How to Create Dependent fields Using Select Box Data

You can create a dependency between two fields on an Identity Manager task screen. The following process describes the steps that you must follow to create dependency between two fields:

1. Create a field that uses an XML file to populate the options.

For example, you can create a field 'State' which takes multiple values as input. Each option in 'State' corresponds to an element or a child element in the Select Box Data XML file. Each of the element in 'State' further has 'City' as child elements.

2. Create another field which is populated based on the option that you have selected in Step 1.

For example, 'City' are also populated from the same XML file as 'State', and are the child elements of the elements used in 'State'.

More Information:

[The Select Box Data XML File](#) (see page 355)

Logical Attribute Handlers

Identity Manager logical attributes allow you to display user store attributes (called physical attributes) in a user-friendly format on task screens. Identity Manager administrators use task screens to perform functions in Identity Manager. Logical attributes do not exist in a user store. Typically, they represent one or more physical attributes to simplify presentation. For example, the logical attribute date may represent the physical attributes month, day, and year.

Logical attributes are processed by logical attribute handlers, which are Java objects that are written using the Logical Attribute API. (See the *Programming Guide for Java*.) For example, when a task screen is displayed, a logical attribute handler might convert physical attribute data from the user store into logical attribute data, which is displayed on the task screen. You can use pre-defined logical attributes and logical attribute handlers included with Identity Manager, or create new ones using the Logical Attribute API.

Note: For more information on logical attributes, see the *Programming Guide for Java*.

In the Identity Manager User Console, the Environment category contains tasks for managing logical attribute handlers. The list includes pre-defined handlers shipped with Identity Manager and any custom handlers defined at your site.

From the Environment task category, you can do the following:

- Create a new logical attribute handler with Identity Manager
- Copy a handler
- Delete a handler
- Modify an existing handler configuration

Note: To change the order of execution for logical attribute handlers, use the Management Console.

Create a Logical Attribute Handler

To create a logical attribute handler

1. Select Environment, Create Logical Attribute Handler.
2. In the Create Logical Attribute Handler screen, select Create Standard Logical Attribute Handler and click OK.
3. In the Create Logical Attribute Handler screen, configure the settings for the logical attribute handler.

For a description of each field, click the Help link from this screen.

4. Click Submit.

The handler is added to the list of handlers on the Logical Attribute Handlers screen.

Note: You do not need to restart the application server after configuring logical attribute handlers using the User Console.

Copy a Logical Attribute Handler

To copy a logical attribute handler

1. Select Environment, Create Logical Attribute Handler.
2. In the Create Logical Attribute Handler screen, select Create a copy of a logical attribute handler definition and click Search.
3. Select a logical attribute handler (for example, ConfirmPasswordHandler) and click OK.

4. In the Create Logical Attribute Handler screen, configure the settings for the logical attribute handler.

For a description of each field, click the Help link from this screen.

5. Click Submit.

The handler is added to the list of handlers on the Logical Attribute Handlers screen.

Note: You do not need to restart the application server after configuring logical attribute handlers using the Identity Manager User Interface.

Create a ForgottenPasswordHandler Logical Attribute Handler

The ForgottenPasswordHandler logical attribute handler uses separate logical attributes for the following:

- configuration
- runtime questions and answers

To create a ForgottenPasswordHandler logical attribute handler

1. Select Environment, Create Logical Attribute Handler.
2. In the Create Logical Attribute Handler screen, select Create Standard Logical Attribute Handler and click Search.
3. Select the ForgottenPasswordHandler and click OK.
4. In the Create Logical Attribute Handler: ForgottenPasswordHandler screen, configure the settings for the logical attribute handler.
For a description of each field, click the Help link from this screen.
5. Click Submit.

The handler is added to the list of handlers on the Logical Attribute Handlers screen.

Note: You do not need to restart the application server after configuring logical attribute handlers using the User Console.

Delete a Logical Attribute Handler

To delete a logical attribute handler

1. Select Environment, Delete Logical Attribute Handler.
2. In the Delete Logical Attribute Handler screen, select the check box to the left of each logical attribute to delete.

3. Click Select.
Identity Manager displays a confirmation message.
4. Click Yes to confirm the deletion.

Modify a Logical Attribute Handler

To modify a logical attribute handler

1. Select Environment, Modify Logical Attribute Handler.
2. In the Modify Logical Attribute Handler screen, select the handler that you want to modify and click Select.
3. Select a logical attribute handler (for example, ConfirmPasswordHandler) and click OK.
4. In the Modify Logical Attribute Handler screen, configure the settings for the logical attribute handler.
For a description of each field, click the Help link from this screen.
5. Click Submit.

Note: You do not need to restart the application server after configuring logical attribute handlers using the User Console.

View a Logical Attribute Handler

To view a logical attribute handler

1. Select Environment, View Logical Attribute Handler.
2. In the View Logical Attribute Handler screen, select the handler that you want to view and click Select.
3. View the logical attribute handler's properties and click Close.

Connection Management

Connection Management is used to configure the database server connection details in Identity Manager. When Identity Manager has to connect to a database server, it uses the Connection details to connect to the database server. Connection Management allows you to create multiple Connections to different database servers under a Connection Type. For each Connection Type you can specify a default connection. You must configure a primary Connection Type for Identity Manager through the Management Console.

Create Connection

Use the following steps to create a connection.

To create a Connection

1. Click Systems, Connection Management, Create Connection.
The Create Connection screen appears.
2. Complete all the necessary fields, and click Submit.
A new Connection is created.

Connection for Reports

Identity Manager allows you to generate report instances and view the report instances through the User Console. The report instances that you have generated are stored in the IAM Report server database. When you view a report instance in Identity Manager, Identity Manager connects to the IAM Report server database, retrieves the report instances, and displays the report instances. For Identity Manager to connect to the IAM Report server database, you must input the connection information using the Connection Management task.

You must create a Connection for reports and include the Infoview server information. The server connection details for infoview are under the `suitereports.properties` file at the following location:

`<App_Server_Deploy Folder>/config/com/netegrity/config`

Note: If you have placed the reports under a folder in Infoview, you must add the folder as an attribute to the Connection.

Appendix A: Events and Tasks

This section contains the following topics:

[Identity Manager Events](#) (see page 367)

[Admin Tasks and Events](#) (see page 372)

Identity Manager Events

An Identity Manager task may represent several smaller and possibly asynchronous operations, called *events*. One or more events are generated whenever an Identity Manager task (other than a workflow approval task) is performed.

Identity Manager audits events, enforces customer-specific business rules associated with events, and, when events are mapped to workflow processes, requires approval for events.

An event can be mapped to a workflow process in the following ways:

- In the Identity Manager Management Console, by clicking Workflow in the Advanced Settings screen.

The event is subject to workflow control whenever it is generated, regardless of the task it is generated within.

- In the Identity Manager User Console, when you are configuring a task on a task screen. To do so, click the Events tab for the task.

The event is subject to workflow control only when that particular task is being executed.

Most events can be mapped to workflow processes. If an event is mapped to a workflow process, the Identity Manager task within which the event occurs can be workflow-controlled.

Event List

The following table lists all Identity Manager events and indicates which events can be mapped to workflow processes.

Event	Workflow Support
AddGrantorOnAccessRoleEvent	Yes
AddGrantorOnAdminRoleEvent	Yes
AddGrantorOnProvisioningRoleEvent	Yes
AddGroupAdminEvent	Yes
AddGroupAdminGroupEvent	Yes
AddGroupToGroupEvent	Yes
AddToGroupEvent	Yes
AssignAccessRoleEvent	Yes
AssignAdminRoleEvent	Yes
AssignProvisioningRoleEvent	Yes
CertificationNonCertifiedActionCompletedNotificationEvent	No
CertificationNonCertifiedActionPendingNotificationEvent	No
CertificationRequiredFinalReminderNotificationEvent	No
CertificationRequiredNotificationEvent	No
CertificationRequiredReminderNotificationEvent	No
CertificationStatusCertifiedEvent	No
CertificationStatusInCertificationEvent	No
CertificationStatusNotCertifiedEvent	No
CertificationStatusRequiresCertificationEvent	No
CertifyRoleEvent	Yes
CreateAccessRoleEvent	Yes
CreateAccessTaskEvent	Yes
CreateAdminRoleEvent	Yes
CreateAdminTaskEvent	Yes

CreateGroupEvent	Yes
CreateIdentityPolicySetEvent	Yes
CreateLAHDefinitionEvent	Yes
CreateOrganizationEvent	Yes
CreatePasswordPolicyEvent	Yes
CreateProvisioningRoleEvent	Yes
CreateProvisioningUserAuditEvent	No
CreateProvisioningUserNotificationEvent	No
CreateUserEvent	Yes
DeleteAccessRoleEvent	Yes
DeleteAccessTaskEvent	Yes
DeleteAdminRoleEvent	Yes
DeleteAdminTaskEvent	Yes
DeleteGroupEvent	Yes
DeleteIdentityPolicySetEvent	Yes
DeleteLAHDefinitionEvent	Yes
DeleteOrganizationEvent	Yes
DeletePasswordPolicyEvent	Yes
DeleteProvisioningRoleEvent	Yes
DeleteProvisioningUserAuditEvent	No
DeleteUserEvent	Yes
DisableUserEvent	Yes
EnableUserEvent	Yes
ExternalTaskEmptyEvent	No
ExternalTaskGroupEvent	No
ExternalTaskOrgEvent	No
ExternalTaskUserEvent	No
ForgottenPasswordAuditEvent	No
ForgottenPasswordEvent	Yes
ForgottenUserIDEvent	Yes

GenericAuditEvent	No
ModifyAccessRoleEvent	Yes
ModifyAccessTaskEvent	Yes
ModifyAdminRoleEvent	Yes
ModifyAdminTaskEvent	Yes
ModifyGroupEvent	Yes
ModifyIdentityPolicySetEvent	Yes
ModifyLAHDefinitionEvent	Yes
ModifyOrganizationEvent	Yes
ModifyPasswordPolicyEvent	Yes
ModifyProvisioningRoleEvent	Yes
ModifyProvisioningUserAuditEvent	No
ModifyUserEvent	Yes
RemoveFromGroupEvent	Yes
RemoveGrantorOnAccessRoleEvent	Yes
RemoveGrantorOnAdminRoleEvent	Yes
RemoveGrantorOnProvisioningRoleEvent	Yes
RemoveGroupAdminEvent	Yes
RemoveGroupAdminGroupEvent	Yes
RemoveGroupFromGroupEvent	Yes
ResetPasswordEvent	Yes
RevokeAccessRoleEvent	Yes
RevokeAdminRoleEvent	Yes
RevokeProvisioningRoleEvent	Yes
SelfRegisterUserEvent	Yes
SetPrimaryObjectAuditEvent	No
SynchronizeUserAccountsEvent	Yes
SynchronizeUserEvent	Yes
SynchronizeUserProvisioningRolesAddAccountsEvent	Yes

SynchronizeUserProvisioningRolesDeleteAccountsEvent	Yes
UserAttributeAddValueEvent	Yes
UserAttributeRemoveValueEvent	Yes
ViewAccessRoleEvent	No
ViewAccessTaskEvent	No
ViewAdminRoleEvent	No
ViewAdminTaskEvent	No
ViewGroupEvent	No
ViewLAHDefinitionEvent	No
ViewOrganizationEvent	No
ViewPasswordPolicyEvent	No
ViewProvisioningRoleEvent	No
ViewUserEvent	No

How Identity Manager Determines Task Status

A *task* is an administrative function that a user can perform in Identity Manager. Tasks include *events*, actions that Identity Manager performs to complete the task. A task may include multiple events. For example, the Create User task may include events that create the user's profile, adds the user to a group, and assigns roles.

Identity Manager tasks and events can be associated with a workflow process, which determines how Identity Manager performs the required actions, and other custom business logic. Tasks may also be associated with other tasks, called nested tasks. In this case, Identity Manager processes the nested tasks with the original task.

The status of a task depends on the status of its associated events, workflow processes, nested tasks, and custom business logic.

Admin Tasks and Events

If multiple events are generated for a task, and the events are mapped to workflow processes, all the workflow processes must be completed before Identity Manager can complete the task.

Generally, events are independent of other events. However, some tasks are associated with a primary event and one or more secondary events:

- A failure of a primary event results in the automatic rejection of all of its secondary events. For example, if a `CreateUserEvent` fails, there is no need for the `AddToGroupEvent` to occur for the user. It also results in the cancelation of the associated task.
- A failure of a secondary event does not affect the success or failure of any other events executed for the task or the execution of the task itself. For example, in a Create User task, an `AddToGroupEvent` may be rejected, meaning that the new user cannot be added to a particular group. But the user can still be created (`CreateUserEvent`) and assigned to access roles (`AssignAccessRoleEvent`), and even be added to other groups.

Tasks and Associated Events

The following table lists the admin tasks that are shipped with Identity Manager, and shows the events that can occur within each task.

Primary events are shown in bold type.

Primary events must be completed before any of its secondary events can begin.

Task	Events Generated for the Task
Begin Certification Process	CertificationRequiredNotificationEvent CertificationStatusRequiresCertificationEvent
Certify User	CertificationStatusCertifiedEvent CertificationStatusInCertificationEvent CertifyRoleEvent ForgottenPasswordEvent ModifyUserEvent RemoveGrantorOnAccessRoleEvent RemoveGrantorOnAdminRoleEvent RemoveGrantorOnProvisioningRoleEvent ResetPasswordEvent RevokeAccessRoleEvent RevokeAdminRoleEvent RevokeProvisioningRoleEvent
Change My Password	ForgottenPasswordEvent ModifyUserEvent ResetPasswordEvent
Create Access Role	CreateAccessRoleEvent
Create Access Task	CreateAccessTaskEvent
Create Admin Role	CreateAdminRoleEvent
Create Admin Task	CreateAdminTaskEvent
Create Group	CreateGroupEvent AddGroupAdminEvent AddGroupAdminGroupEvent AddGroupToGroupEvent AddToGroupEvent
Create Identity Policy Set	CreateIdentityPolicySetEvent
Create Logical Attribute Handler	CreateLAHDefinitionEvent
Create Organization	CreateOrganizationEvent
Create Password Policy	CreatePasswordPolicyEvent
Create Provisioning Role	CreateProvisioningRoleEvent

Create User	CreateUserEvent AddGrantorOnAccessRoleEvent AddGrantorOnAdminRoleEvent AddGrantorOnProvisioningRoleEvent AddGroupAdminEvent AddToGroupEvent AssignAccessRoleEvent AssignAdminRoleEvent AssignProvisioningRoleEvent
Delete Access Role	DeleteAccessRoleEvent
Delete Access Task	DeleteAccessTaskEvent
Delete Admin Role	DeleteAdminRoleEvent
Delete Admin Task	DeleteAdminTaskEvent
Delete Group	DeleteGroupEvent
Delete Identity Policy Set	DeleteIdentityPolicySetEvent
Delete Logical Attribute Handler	DeleteLAHDefinitionEvent
Delete Organization	DeleteOrganizationEvent
Delete Password Policy	DeletePasswordPolicyEvent
Delete Provisioning Role	DeleteProvisioningRoleEvent
Delete User	DeleteUserEvent
Enable/Disable User	DisableUserEvent EnableUserEvent
End Certification Process	CertificationNonCertifiedActionCompletedNotificationEvent CertificationNonCertifiedActionPendingNotificationEvent CertificationStatusNotCertifiedEvent
External Task	ExternalTaskEmptyEvent
External Group Task	ExternalTaskGroupEvent
External Organization Task	ExternalTaskOrgEvent
External User Task	ExternalTaskUserEvent
Forgotten Password	ForgottenPasswordEvent
Forgotten User ID	ForgottenUserIDEvent
Modify Access Role	ModifyAccessRoleEvent

Modify Access Role Members/Administrators	AddGrantorOnAccessRoleEvent AssignAccessRoleEvent RemoveGrantorOnAccessRoleEvent RevokeAccessRoleEvent
Modify Access Task	ModifyAccessTaskEvent
Modify Admin Role	ModifyAdminRoleEvent
Modify Admin Role Members/Administrators	AddGrantorOnAdminRoleEvent AssignAdminRoleEvent RemoveGrantorOnAdminRoleEvent RevokeAdminRoleEvent
Modify Admin Task	ModifyAdminTaskEvent
Modify Group	AddGroupAdminEvent AddGroupAdminGroupEvent AddGroupToGroupEvent AddToGroupEvent ModifyGroupEvent RemoveFromGroupEvent RemoveGroupAdminEvent RemoveGroupAdminGroupEvent RemoveGroupFromGroupEvent
Modify Group Members	AddGroupToGroupEvent AddToGroupEvent RemoveFromGroupEvent RemoveGroupFromGroupEvent
Modify Identity Policy Set	ModifyIdentityPolicySetEvent
Modify Logical Attribute Handler	ModifyLAHDefinitionEvent
Modify My Groups	AddGroupAdminEvent AddToGroupEvent RemoveFromGroupEvent RemoveGroupAdminEvent
Modify My Profile	ModifyUserEvent
Modify Organization	ModifyOrganizationEvent
Modify Password Policy	ModifyPasswordPolicyEvent
Modify Provisioning Role	ModifyProvisioningRoleEvent
Modify Provisioning Role Members/Administrators	AddGrantorOnProvisioningRoleEvent AssignProvisioningRoleEvent RemoveGrantorOnProvisioningRoleEvent RevokeProvisioningRoleEvent

Modify User	ModifyUserEvent AddGrantorOnAccessRoleEvent AddGrantorOnAdminRoleEvent AddGrantorOnProvisioningRoleEvent AddGroupAdminEvent AddToGroupEvent AssignAccessRoleEvent AssignAdminRoleEvent AssignProvisioningRoleEvent ForgottenPasswordEvent RemoveFromGroupEvent RemoveGrantorOnAccessRoleEvent RemoveGrantorOnAdminRoleEvent RemoveGrantorOnProvisioningRoleEvent RemoveGroupAdminEvent ResetPasswordEvent RevokeAccessRoleEvent RevokeAdminRoleEvent RevokeProvisioningRoleEvent
Provisioning Create User	CreateUserEvent AddGrantorOnAccessRoleEvent AddGrantorOnAdminRoleEvent AddGrantorOnProvisioningRoleEvent AddGroupAdminEvent AddToGroupEvent AssignAccessRoleEvent AssignAdminRoleEvent AssignProvisioningRoleEvent
Provisioning Enable/Disable User	DisableUserEvent EnableUserEvent

Provisioning Modify User	ModifyUserEvent AddGrantorOnAccessRoleEvent AddGrantorOnAdminRoleEvent AddGrantorOnProvisioningRoleEvent AddGroupAdminEvent AddToGroupEvent AssignAccessRoleEvent AssignAdminRoleEvent AssignProvisioningRoleEvent ForgottenPasswordEvent RemoveFromGroupEvent RemoveGrantorOnAccessRoleEvent RemoveGrantorOnAdminRoleEvent RemoveGrantorOnProvisioningRoleEvent RemoveGroupAdminEvent ResetPasswordEvent RevokeAccessRoleEvent RevokeAdminRoleEvent RevokeProvisioningRoleEvent
Reset Access Role Owners	ModifyAccessRoleEvent
Reset Admin Role Owners	ModifyAdminRoleEvent
Reset Provisioning Role Owners	ModifyProvisioningRoleEvent
Reset User Password	ModifyUserEvent ForgottenPasswordEvent ResetPasswordEvent
Self Registration	SelfRegisterUserEvent
Send Certification Reminder Notification	CertificationRequiredReminderNotificationEvent
Send Final Certification Reminder Notification	CertificationRequiredFinalReminderNotificationEvent

Synchronize User	ModifyUserEvent AddGrantorOnAccessRoleEvent AddGrantorOnAdminRoleEvent AddGrantorOnProvisioningRoleEvent AddGroupAdminEvent AddToGroupEvent AssignAccessRoleEvent AssignAdminRoleEvent AssignProvisioningRoleEvent ForgottenPasswordEvent RemoveFromGroupEvent RemoveGrantorOnAccessRoleEvent RemoveGrantorOnAdminRoleEvent RemoveGrantorOnProvisioningRoleEvent RemoveGroupAdminEvent ResetPasswordEvent RevokeAccessRoleEvent RevokeAdminRoleEvent RevokeProvisioningRoleEvent
View Access Role	ViewAccessRoleEvent
View Access Role Members/Administrators	ViewAccessRoleEvent
View Access Task	ViewAccessTaskEvent
View Admin Role	ViewAdminRoleEvent
View Admin Role Members/Administrators	ViewAdminRoleEvent
View Admin Task	ViewAdminTaskEvent
View Group	ViewGroupEvent
View Identity Policy Set	No associated event
View Logical Attribute Handler	ViewLAHDefinitionEvent
View My Roles	ViewUserEvent
View My Submitted Tasks	No associated event
View Organization	ViewOrganizationEvent
View Password Policy	ViewPasswordPolicyEvent
View Provisioning Role	ViewProvisioningRoleEvent
View Provisioning Role Members/Administrators	ViewProvisioningRoleEvent

View Submitted Tasks	No associated event
View User	ViewUserEvent

Events Generated for Unmodified Profiles

User, group, and organization objects each contain a set of physical attributes that are stored in the user directory. If a physical attribute of one of these objects is changed on a profile tab, Identity Manager generates a Modify... event after the user submits the task. For example, if a *Title* attribute is changed on a User Profile tab, Identity Manager generates the event ModifyUserEvent.

If a user, group, or organization object is represented on a profile tab, but no physical attributes have been changed when the user clicks Submit, Identity Manager does not generate a Modify... event. Instead, the corresponding View... event is generated, as follows:

- ViewUserEvent is generated instead of ModifyUserEvent
- ViewGroupEvent is generated instead of ModifyGroupEvent
- ViewOrganizationEvent is generated instead of ModifyOrganizationEvent

Appendix B: Default Tasks and Roles

An Identity Manager environment includes a set of default tasks and roles that you can use or modify for an environment.

This section contains the following topics:

[Default Self-Service Tasks](#) (see page 381)

[Default Admin Tasks](#) (see page 382)

[Default Admin Roles](#) (see page 398)

[Default Workflow Approval Roles](#) (see page 405)

Default Self-Service Tasks

Identity Manager includes the following self-service tasks:

- [Self Registration](#) (see page 381)
- [Forgotten Password](#) (see page 381)
- [Forgotten Password Reset](#) (see page 382)
- [Forgotten User ID](#) (see page 382)
- [Password Services](#) (see page 382)

These tasks are public tasks, which users can access without providing login credentials.

Self Registration

The Self Registration task allows users to register at a corporate Web site without administrator involvement. Users can enter profile information, set a password, and subscribe to groups.

Forgotten Password

The Forgotten Password task provides a user with a temporary password that she can use to log into Identity Manager. When the user logs in, she is immediately prompted to enter a new password.

Forgotten Password Reset

The Forgotten Password Reset task enables a user to reset a password after Identity Manager verifies his identity.

In the default Forgotten Password Reset task, a user must provide a user ID and answer three verification questions. Once Identity Manager verifies a user's identity, a screen where the user can enter a new password is presented.

Forgotten User ID

The Forgotten User ID task allows a user to retrieve a forgotten user ID. In the default task, a user must provide an email address and answer one verification question to receive an email containing the user's ID.

Password Services

The Password Services task changes your password after you enter your current password. Users are automatically directed to the Password Services task if they are forced to change their password as the result of a password policy or a SiteMinder authentication failure.

This task does not appear as a task in the User Console.

Default Admin Tasks

When you create an admin role, you can include any of the default admin tasks, which appear in the user interface under these categories:

- [Home](#) (see page 383)
- [Access Roles](#) (see page 126)
- [Admin Roles](#) (see page 387)
- [Certification](#) (see page 389)
- [Groups](#) (see page 389)
- [Organizations](#) (see page 391)
- [Policies](#) (see page 392)
- [Provisioning Roles](#) (see page 394)

- [Reports](#) (see page 395)
- [System](#) (see page 395)
- [Users](#) (see page 397)

Note: Any task that appears in Identity Manager, but is omitted from the tasks defined here, is a task created by an Identity Manager administrator.

Depending on the admin roles assigned to you, you see only certain admin tasks. For example, if you have the default Group Manager role, you see five tasks under Groups.

Note: After using a task, you may see a Task Submitted for Processing message, indicating that changes may not be in effect. For details on this processing, see [Admin Task Processing](#) (see page 58).

Home

The My Account tab provides these tasks for viewing or modifying the profile, roles, groups, and password of the current user.

- [Change My Account](#) (see page 383)
- [Change My Password](#) (see page 383)
- [Modify My Groups](#) (see page 384)
- [Modify My Profile](#) (see page 384)
- [Out of Office](#) (see page 384)
- [View My Roles](#) (see page 384)
- [View My Submitted Tasks](#) (see page 384)
- [View My Work List](#) (see page 384)

Change My Account

Change my account lets you make a request to change the details of a user.

Change My Password

Change My Password changes your password after you enter your current password. This task is different from Reset User Password, which modifies another user's password without requiring the current password.

Modify My Groups

Modify My Groups allows you to join or leave any self-subscribing group. The Groups tab displays the groups that are assigned to you and self-subscribing groups that you have joined.

To join more self-subscribing groups, click Add More. To leave a group, click the Remove check box; it appears next to each self-subscribing group.

Modify My Profile

Modify My Profile enables you to change personal information, such as name, phone numbers, and title.

Out of Office

Out of Office allows a user (the delegator) to specify that another user (the delegate) be allowed to approve tasks in the delegator's work list. The delegator can assign work items to another approver during periods when the delegator is "out of the office."

View My Roles

View My Roles displays a list of roles for which you are a role member or a role administrator.

View My Submitted Tasks

View My Submitted Tasks enables you to view the status of tasks that you have submitted for processing. When performing this task, you can:

- View all of the tasks that you initiated or you can view only the tasks that meet certain criteria--for example, you can search for and display tasks that you submitted during a certain period of time.
- View details about the events that a task generates.

Note: This task cannot be used by Task Execution Web Service (TEWS).

View My Work List

View My Work List enables you to see any tasks you received through the workflow process. Typically, these tasks require an approval action to continue through the workflow process.

Access Roles

You use the Access Role Management category to create or manage access roles and tasks. You create access tasks to provide access to functions in applications and then create access roles that include those tasks.

The category contains these tasks:

- [Create Access Role](#) (see page 385)
- [Create Access Task](#) (see page 385)
- [Delete Access Role](#) (see page 385)
- [Delete Access Task](#) (see page 385)
- [Modify Access Role](#) (see page 386)
- [Modify Access Role Members/Administrators](#) (see page 386)
- [Modify Access Task](#) (see page 386)
- [Reset Access Role Owners](#) (see page 386)
- [View Access Role](#) (see page 386)
- [View Access Role Members/Administrators](#) (see page 386)
- [View Access Task](#) (see page 386)

Create Access Role

Create Access Role creates a role that contains access tasks. Each task provides access to a function in an application other than Identity Manager.

Create Access Task

Create Access Task creates a task that can be included in an access role. The task corresponds to a function in an application.

Delete Access Role

Delete Access Role removes the selected access role from the Environment. The role can no longer be used. Before deleting the role, consider removing members from the role.

Delete Access Task

Delete Access Task removes the selected access task.

Note: If a user is performing the task when it is deleted, the user can complete the task.

Modify Access Role

Modify Access Role changes the properties of the selected access role, including its enabled or disabled status.

A role can be enabled for immediate use, or disabled if it is not ready for use or if it protects an application feature that is unavailable. Disabled roles can be assigned to users; however, a disabled role will not appear in a list of roles that a user has.

Note: If you modify a role while a role member is performing a task, the role member can complete that task.

Modify Access Role Members/Administrators

Modify Access Role Members/Administrators adds or removes members of the access role that you select. When performing this task, you can select any role for which you have the Manage Members or Manage Administrators privilege.

Modify Access Task

Modify Access Task makes changes to the selected access task.

Reset Access Role Owners

Reset Access Role Owners redefines the owner rules that control who are owners for the selected access role. Owners can modify the role.

View Access Role

View Access Role displays the characteristics of the selected access role.

View Access Role Members/Administrators

View Access Role Members/Administrators lists members and administrators of the selected access role. When performing this task, you can select any access role for which you are an administrator.

View Access Task

View Access Task displays the characteristics of an access task that you select.

Admin Roles

You use the Admin Role Management category to create or manage admin roles and [admin tasks](#) (see page 41).

The category contains these tasks:

- [Create Admin Role](#) (see page 387)
- [Create Admin Task](#) (see page 387)
- [Delete Admin Role](#) (see page 387)
- [Delete Admin Task](#) (see page 387)
- [Modify Admin Role](#) (see page 388)
- [Modify Admin Role Members/Administrators](#) (see page 388)
- [Modify Admin Task](#) (see page 388)
- [Reset Admin Role Owners](#) (see page 388)
- [View Admin Role](#) (see page 388)
- [View Admin Role Members/Administrators](#) (see page 388)
- [View Admin Task](#) (see page 388)

Create Admin Role

Create Admin Role creates a role that contains admin tasks.

Create Admin Task

Create Admin Task creates a task that can be included in an admin role.

Delete Admin Role

Delete Admin Role removes the selected admin role from the Environment. The role can no longer be used.

Before deleting the role, consider removing members from the role. If you delete an admin role, role members can complete the role's task, which is currently in use. Once the task is complete, they cannot perform it again.

Delete Admin Task

Delete Admin Task removes an admin task that you select.

Note: Users who are performing the task when the task is deleted can complete the task.

Modify Admin Role

Modify Admin Role changes the properties of the selected admin role including the role's enabled or disabled status.

A role can be enabled for immediate use, or it can be disabled if it is not ready for use. Disabled roles can be assigned to an administrator; however, a disabled role will not appear in a list of roles that a user has.

Note: If a role member is performing a role's task when the role is modified, the role member can complete the task.

Modify Admin Role Members/Administrators

Modify Admin Role Members/Administrators adds or removes members or administrators of the selected admin role. When performing this task, you can select any admin role for which you have the Manage Members or Manage Administrators privilege.

Modify Admin Task

Modify Admin Task makes changes to the selected admin task.

Reset Admin Role Owners

Reset Admin Role Owners redefines the owner rules that control who are owners for the selected admin role. Owners can modify the role.

View Admin Role

View Admin Role displays the characteristics of the selected admin role.

View Admin Role Members/Administrators

View Admin Role Members lists all members or administrators of the selected admin role.

You can select any role for which you have the Manage Members or Manage Administrators privilege.

View Admin Task

View Admin Task displays the characteristics of the selected admin task.

Note: To use View My Submitted Tasks, database task persistence must be enabled. See the Identity Manager system administrator for assistance.

Certification

The Certification category manages the user certification process. This category includes the following tasks:

- [Begin Certification Process](#) (see page 389)
- [End Certification Process](#) (see page 389)
- [Send Certification Reminder Notification](#) (see page 389)
- [Send Final Certification Reminder Notification](#) (see page 389)

Begin Certification Process

The Begin Certification Process task allows you to select users that require certification. Once you select the users, Identity Manager sets the users' certification to REQUIRES CERTIFICATION, and sends an email to the appropriate certifier, notifying her that she has pending certifications.

End Certification Process

The End Certification Process task disables users who have not been certified, and informs the appropriate certifiers.

Send Certification Reminder Notification

The Send Certification Reminder Notification task sends an email to certifiers reminding them that they have pending certifications.

Send Final Certification Reminder Notification

The Send Final Certification Reminder Notification task is similar to the [Send Certification Reminder Notification](#) (see page 389) task except that the email sent to certifiers informs them that they will not receive additional reminders.

Groups

The Groups category creates or manages groups. This category includes these tasks:

- [Create Group](#) (see page 390)
- [Delete Group](#) (see page 390)
- [Modify Group](#) (see page 390)
- [Modify Group Members](#) (see page 390)
- [View Group](#) (see page 391)

Create Group

Create Group creates a group in the current organization. When you use this task, you can:

- Provide profile information
- Specify the organization in which to create the group
- Assign administrators and static members by selecting from a list of users who exist in the current organization

You see the following tabs when you perform this task:

- **Members**--Adds static members to the group. You select members whose profiles exist in organizations where you have the Modify Group task.
- **Administrators**--Adds administrators for the group. You select group administrators whose profiles exist in organizations where you have the Modify Group task.

On the Administrators tab, you can specify users and groups as administrators. If you specify a group, administrators of that group will be administrators of the group you are modifying. Members of the group you specify will not have privileges to manage the group you are creating.

Note: The Dynamic Group Query field is not included in the Create Group task or other group tasks even if this field exists in the directory.xml for a group. You include Dynamic Group Query field in the task by editing the associated profile screen.

Delete Group

Delete Group removes the group that you select from the current organization.

Modify Group

Modify Group makes changes to the profile, to the list of group administrators, or to the list of static members of the selected group.

Note: If you specify a group as an administrator, only administrators of that group can manage the group you are modifying. Members of the administrator group will not have privileges to manage the group you are modifying.

Modify Group Members

Modify Group Members adds or removes static members to a group. To add or remove group administrators, use Modify Group.

View Group

View Group displays the group profile and the administrators and members of a group.

You see the following tabs when you perform this task:

- **Members**--Lists the all of the static members (users and groups) of the group.
- **Administrators**--Lists the group administrators.

If a group is listed as an administrator, only users who are administrators of that group can manage the group you are viewing. Members of the administrator group do not have privileges to manage the group you are viewing.

Organizations

The Organization category is intended for a user store that is an LDAP directory or a relational database that includes organizations. This category contains these tasks, which you use to create or manage an organization.

- [Create Organization](#) (see page 391)
- [Delete Organization](#) (see page 391)
- [Modify Organization](#) (see page 391)
- [View Organization](#) (see page 391)

Create Organization

Create Organization creates a suborganization in the organization that you select.

Delete Organization

Delete Organization removes the organization that you select. All users and groups in the organization are also deleted.

Modify Organization

Modify Organization makes changes to the organization that you select.

View Organization

View Organization displays the characteristics of the organization that you select.

Policies

The Policies category manages Identity Policy Sets and Password Policies. This category contains the following tasks:

- [Create Identity Policy Set](#) (see page 392)
- [Delete Identity Policy Set](#) (see page 392)
- [Modify Identity Policy Set](#) (see page 392)
- [View Identity Policy Set](#) (see page 393)
- [Synchronize User](#) (see page 393)
- [Create Password Policy](#) (see page 393)
- [Delete Password Policy](#) (see page 393)
- [Modify Password Policy](#) (see page 393)
- [View Password Policy](#) (see page 393)

Create Identity Policy Set

Create Identity Policy Set allows you to configure a set of business changes that occur when a user meets a certain condition or rule. The business changes can include:

- Assigning or revoking roles, including provisioning roles
- Assigning or revoking group membership
- Updating attributes in a user profile

Delete Identity Policy Set

Delete Identity Policy Set removes the policy sets that you select. Deleting an identity policy set deletes the associated identity policies.

Modify Identity Policy Set

Modify Identity Policy Set makes changes to the identity policy set that you select.

View Identity Policy Set

View Identity Policy Set displays the characteristics of the identity policy set that you select, including:

- Basic information about the identity policy set, such as name, category, and description
- The identity policies in the set
- The owner policies for the set

Synchronize User

Synchronize User synchronizes a user that you select with identity policies.

The Synchronize User task includes the following tabs:

- **Currently Matched Policies**--Displays a list of identity policies that will be applied to the user when synchronization takes place.
- **Policies Already Applied**--Displays a list of identity policies that have already been applied to the user.
- **Synchronization Summary**--Displays all of the identity policies that apply to the user and the change actions for those policies.

Create Password Policy

Create Password Policy enables you to configure a set of rules and restrictions that determine how passwords are created and when they expire.

Delete Password Policy

Delete Password Policy removes the password policy that you select.

Modify Password Policy

Modify Password Policy makes changes to the password policy that you select.

View Password Policy

View Password Policy displays the characteristics of the password policy you select.

Provisioning Roles

You use the Provisioning Roles category to create and manage provisioning roles, which can be assigned to users. This category contains the following tasks:

- [Create Provisioning Role](#) (see page 394)
- [Delete Provisioning Role](#) (see page 394)
- [Modify Provisioning Role](#) (see page 394)
- [Modify Provisioning Role Members/Administrators](#) (see page 394)
- [Reset Provisioning Role Owners](#) (see page 394)
- [View Provisioning Role](#) (see page 394)
- [View Provisioning Role Members/Administrators](#) (see page 395)

Create Provisioning Role

Create Provisioning role creates a provisioning role for which users can be made members or administrators.

Delete Provisioning Role

Delete Provisioning Role removes a role from the Environment.

Modify Provisioning Role

Modify Provisioning Role makes changes to the provisioning role that you select.

Modify Provisioning Role Members/Administrators

Modify Provisioning Role Members/Administrators adds or removes members or administrators of the selected provisioning role.

Reset Provisioning Role Owners

Reset Provisioning Role Owners redefines the owner rules that control who are owners for the selected provisioning role. Owners can modify the role.

View Provisioning Role

View Provisioning Role displays the characteristics of the selected provisioning role.

View Provisioning Role Members/Administrators

View Provisioning Role Members/Administrators lists the members and administrators of the selected provisioning role.

Reports

You can use the Reports category to view and manage your reports. This category involves the following tasks:

Task	Description
View My Reports	This task lets you view the report instances you have generated.
Delete My Reports	This task lets you delete any of the report instances you have generated.
Set Reporting Options	This task lets you manage the options for generating report instances. For example, you can limit the number of report instances you can generate for each report type.

System

You can use the System category to monitor the status of tasks and events that have been submitted for processing. This category involves the following tasks:

Task	Description
Connection Management	Connection Management is used to configure database server connection details in Identity Manager.
Select Box Data	This task lets you populate the options for select based controls in the User Console from an XML file.
Bulk Loader	The Bulk Loader is used to upload feeder files that are used to manipulate large numbers of managed objects simultaneously.

Task	Description
View Submitted Tasks	This task displays the status of tasks that have been submitted for processing in the current Environment. Note: This task cannot be used by Task Execution Web Service (TEWS).
Logical Attribute Handlers	This tasks lets you create the following: ■ Logical attributes--Data that is presented to the user on a task screen, but that is not written to the data store. ■ Logical Attribute Handlers-- Java objects that process logical attribute data.

Create Logical Attribute Handler

The Create Logical Attribute Handler task allows you to create logical attribute handlers, which are Java objects that process logical attribute data and are written using the Logical Attribute API. For example, when performing this task, you can create a logical attribute handler that can convert physical attribute data from the user store into logical attribute data that can be displayed on the task screen.

Delete Logical Attribute Handler

The Delete Logical Attribute Handler task allows you to delete existing logical attribute handlers. Deleting logical attribute handlers deletes the Java objects that process logical attribute data but does not affect the data store.

Modify Logical Attribute Handler

The Modify Logical Attribute Handler task allows you to modify and update existing logical attribute handlers.

View Logical Attribute Handler

The View Logical Attribute Handler task allows you to view the properties of existing logical attribute handlers.

Users

The User category creates or manages user accounts. This category includes these tasks:

- [Create User](#) (see page 397)
- [Delegate Work Items](#) (see page 397)
- [Delete User](#) (see page 397)
- [Enable/Disable User](#) (see page 397)
- [Modify User](#) (see page 398)
- [Reset User Password](#) (see page 398)
- [View User](#) (see page 398)

Create User

Create User creates an Identity Manager account. When you create a user, you can:

- Select the organization in which to create the user's profile
- Assign access roles or admin roles if you are an administrator of the role to be assigned
- Assign a user to a group if you are an administrator for that group

Note: If you cannot make changes on a certain tab, you will not see that tab. For example, if you are not a group administrator, you will not see the Groups tab.

Delegate Work Items

Delegate Work Items allows a user with the Delegation Manager role to act on behalf of another user (the delegator) and delegate work item approval tasks to a third user (the delegate).

Delete User

Delete User removes the selected user account from Identity Manager. That user may be an administrator or an end user.

Enable/Disable User

Enable/Disable User controls whether or not a user account is active.

Modify User

Modify User makes changes to a user account. Changes affect the user's profile and membership in roles and groups for which you are an administrator.

You can also view other roles that the user has been assigned or has received by meeting the role constraint.

Reset User Password

Reset User Password changes the password of a user account without requiring entry of the current password.

View User

View User displays the profile, roles, and groups of a user. That user may be an administrator or an end user. This task displays all roles that the user has been assigned or has received by meeting the role constraint.

Note: If you use the System Manager role, you can view any user in the Environment.

Default Admin Roles

The following sections define the default roles that are installed with Identity Manager.

- [Access Role Manager](#) (see page 399)
- [Admin Role Manager](#) (see page 399)
- [Certify Manager](#) (see page 400)
- [Certification Process Manager](#) (see page 400)
- [Delegation Manager](#) (see page 400)
- [Group Manager](#) (see page 401)
- [Organization Manager](#) (see page 401)
- [Password Manager](#) (see page 402)
- [Provisioning Role Manager](#) (see page 402)
- [Provisioning Synchronization Manager](#) (see page 402)
- [Security Manager](#) (see page 403)
- [Self Delegator](#) (see page 403)

- [Self Manager](#) (see page 403)
- [System Manager](#) (see page 404)
- [User Manager](#) (see page 405)

Note: If you have modified a default role, use View Admin Role to see the tasks in the role.

Access Role Manager

Creates, modifies, and deletes access tasks and roles and determines who are members or administrators of the role. The role includes these tasks:

Access Role Management

■ Create Access Role	■ Modify Access Task
■ Create Access Task	■ View Access Role
■ Delete Access Role	■ View Access Role Members/Administrators
■ Delete Access Task	■ View Access Task
■ Modify Access Role	
■ Modify Access Role Members/Administrators	
-

Note: This role grants significant privileges. You may want to limit the number of administrators with this role.

Admin Role Manager

Creates, modifies, and deletes admin tasks and roles and determines who are members or administrators of the role. The role includes these tasks:

Admin Role Management

■ Create Admin Role	■ Modify Admin Role Members/Administrators
■ Create Admin Task	■ Modify Admin Task
■ Delete Admin Role	■ View Admin Role
■ Delete Admin Task	■ View Admin Role Members/Administrators
■ Modify Admin Role	■ View Admin Task
-

Note: This role grants significant privileges. You may want to limit the number of administrators with this role.

Certification Process Manager

Selects users for certification, sends reminders to certifiers about pending certifications, and ends the certification process, which disables the accounts of users who are not certified.

The role includes these tasks:

Certification

- Begin Certification Process
 - End Certification Process
 - Send Certification Reminder Notification
 - Send Final Certification Reminder Notification
-

Certify Manager

Certifies user entitlements by certifying or rejecting users' roles.

The role includes this task:

User Management

- Certify User
-

Delegation Manager

A Delegation Manager can act on behalf of another user (the delegator) and delegate work item approval to tasks a third user (the delegate).

This role has scope over all users.

This role includes the following task:

[Delegate Workitems](#) (see page 397)

Group Manager

Creates, modifies, and deletes groups in organizations where the administrator has management privileges, and assigns group administrators. The role includes these tasks:

Group Management

- Create Group
 - Delete Group
 - Modify Group
 - View Group
-

Organization Manager

Creates, modifies, and deletes groups, users, administrators, and organizations. The role includes these tasks:

Organization Management

- Create Organization
- Delete Organization
- Modify Organization
- View Organization

Group Management

- Create Group
- Delete Group
- Modify Group
- View Group

User Management

- Create User
 - Delete User
 - Enable/Disable User
 - Modify User
 - Reset User Password
 - View User
-

Admin Role Management

- Modify Admin Role Members/Administrators
- View Admin Role
- View Admin Role Members/Administrators

Access Role Management

- Modify Access Role Members/Administrators
 - View Access Role
 - View Access Role Members/Administrators
-

Password Manager

Resets user passwords. This role is useful for help desk personnel. The role includes these tasks:

User Management

- Reset User Password
 - View User
-

Provisioning Role Manager

Creates, modifies, and deletes admin tasks and roles and determines who are members or administrators of the role. The role includes these tasks:

Provisioning Roles

- Create Provisioning Role
 - Delete Provisioning Role
 - Modify Provisioning Role
 - Modify Provisioning Role
Members/Administrators
 - View Provisioning Role
 - View Provisioning Role
Members/Administrators
-

Provisioning Synchronization Manager

Updates the user store used by Identity Manager with user changes made on the Provisioning Server. This role is used internally by Identity Manager. The role includes these tasks:

Provisioning Synchronization

- Provisioning Create User
 - Provisioning Enable/Disable User
 - Provisioning Modify User
-

Security Manager

Enables and disable a user's account, and resets user passwords. The role includes these tasks:

User Management

- Enable/Disable User
 - Reset User Password
 - View User
-

Self Delegator

A Self Delegator (the delegator) can specify that another user (the delegate) be allowed to approve tasks in the delegator's work list.

This role has scope over all users.

This role includes the following task:

[Out of Office](#) (see page 384)

Self Manager

Changes your own profile, including your password, requests membership to self subscribing groups, and views your own roles. The role includes these tasks:

My Account

- Change My Password
 - Modify My Groups
 - Modify My Profile
 - View My Roles
 - View My Submitted Tasks
 - View My Work List
-

System Manager

Sets up initial top-level administrators, tasks, and roles in an Environment. The role includes all default admin tasks.

Organization Management

- Create Organization
- Delete Organization
- Modify Organization
- View Organization

User Management

- Create User
- Delete User
- Modify User
- View User

System Management

- View Submitted Tasks

Access Role Management

- Reset Access Role Owner

Admin Role Management

- Create Admin Role
 - Create Admin Task
 - Delete Admin Role
 - Delete Admin Task
 - Modify Admin Role
 - Modify Admin Task
 - Reset Admin Role Owner
 - View Admin Role
 - View Admin Task
-

User Manager

Creates, modifies, and deletes users in organizations and controls membership in roles and groups. The role includes these tasks:

User Management

- Create User
- Delete User
- Modify User
- View User

Group Management

- Modify Group Members

Access Role Management

- Modify Access Role Members/Administrators
- View Access Role Members/Administrators

Default Workflow Approval Roles

Note: The approval tasks for role or group membership approve changes to who is a member or an administrator of the role or group.

Approval Role Name	Tasks for Approval
Access Role Membership Approver	■ Approve Modify Access Role Membership
Admin Role Membership Approver	■ Approve Modify Admin Role Membership
Group Approver	■ Approve Create Group ■ Approve Delete Group
Group Membership Approver	■ Approve Modify Group Membership
Organization Approver	■ Approve Create Organization ■ Approve Delete Organization ■ Approve Modify Organization
Provisioning Role Membership Approver	■ Approve Modify Provisioning Role Membership
Self Registration Approver	■ Approve Self Registration
User Approver	■ Approve Create User ■ Approve Delete User ■ Approve Modify User

Appendix C: FIPS 140-2 Compliance

This section contains the following topics:

[FIPS Overview](#) (see page 407)
[Communications](#) (see page 407)
[Installation](#) (see page 408)
[Connecting to SiteMinder](#) (see page 408)
[Key File Storage](#) (see page 409)
[The Password Tool](#) (see page 409)
[FIPS Mode Detection](#) (see page 410)
[Encrypted Text Formats](#) (see page 410)
[Encrypted Information](#) (see page 411)
[FIPS Mode Logging](#) (see page 411)

FIPS Overview

The Federal Information Processing Standards (FIPS) 140-2 publication is a security standard for the cryptographic libraries and algorithms a product should use for encryption. Encryption affects the storage and verification of passwords, as well as the communication of all sensitive data between components of CA products and between CA products and third-party products. FIPS 140-2 specifies the requirements for using cryptographic algorithms within a security system protecting sensitive, unclassified data.

CA Identity Manager uses the Advanced Encryption Standard (AES) adapted by the US government. CA Identity Manager incorporates the RSA Crypto-J v3.5 and Crypto-C ME v2.0 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules.

Communications

FIPS encryption covers all data communications between Identity Manager and the following components:

- Identity Manager Server
- Provisioning Server
- Provisioning Manager and Clients
- C++ Connector Servers
- C++ Connector Server endpoints (if supported by endpoint)
- Java Connector Servers

- Java Connector Server endpoints (if supported by endpoint)
- Connector Xpress (if supported by endpoint)
- Windows Password Synchronization Agents
- Java Identity and Access Management (JIAM)
- Service Provisioning Markup Language (SPML)

Note: CA Directory r12 is not certified with Identity Manager Provisioning Server r12.

Installation

The Identity Manager installer allows you to configure FIPS 140-2 during installation.

All components in an Identity Manager environment need to be FIPS 140-2 enabled in order for Identity Manager to support FIPS 140-2. You need a FIPS encryption key to enable FIPS 140-2 during installation. A Password Tool (pwdtools.bat/pwdtools.sh) for generating a FIPS key is included in the following location:

C:\Program Files\CA\IAM Suite\Identity Manager\tools\PasswordTool\pwdtools.bat

Important! Use the same FIPS 140-2 encryption key in all installations, and ensure that you safeguard the key file generated by the Password Tool.

Connecting to SiteMinder

When connecting to CA SiteMinder during Identity Manager installation, be aware that FIPS mode and product version configurations are supported only as listed in the following table:

Identity Manager r12	SiteMinder	SiteMinder Version
FIPS-only mode	FIPS-only mode	r12
FIPS-only mode	FIPS-compatible mode	r12
Non-FIPS mode	FIPS-compatible mode	r12
Non-FIPS mode	Non-FIPS mode	r6

Key File Storage

Identity Manager uses the file system for FIPS encryption key storage. The Identity Manager administrator is responsible for protecting that file from unauthorized access by setting the directory access permissions for specific group or user types, such as the user who is authorized to run Identity Manager.

The Password Tool

The FIPS-compliant password tool utility, `pwdtools.bat` (or `pwdtools.sh`), can generate the encryption key during Identity Manager installation, from the command line.

Before using the password tool, edit the `pwdtools.bat/pwdtools.sh` file and set the `JAVA_HOME` variable as required.

Important! Because Identity Manager r12 does not support data migration or re-encryption, you should not change encryption keys after installation.

This command has the following syntax:

```
pwdtools -[FIPSKEY|JSAFE|FIPS] -p [plain text] -k [key file location]
```

JSAFE

Encrypt a plain text value using non-FIPS algorithm.

Example:

```
pwdtools -JSAFE -p firewall
```

FIPSKEY

Create a FIPS key file.

Example:

```
pwdtools -FIPSKEY -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the Identity Manager FIPS key directory.

FIPS

Encrypt a plain text value using a FIPS key file. This uses the existing FIPS key file.

Example:

```
pwdtools -FIPS -p firewall -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the Identity Manager FIPS key directory.

Important! Because Identity Manager uses the FIPS key file to check whether the application is to start in FIPS mode or non-FIPS mode, the key file must be named `FIPSKey.dat` with the following application server deployment path:

`IdentityMinder.ear\config\com\netegrity\config\keys\FIPSkey.dat`

where `IdentityMinder.ear` is in the application server deployment directory, for example:

`jboss_home\server\default\deploy`

FIPS Mode Detection

The following key file determines whether or not Identity Manager is in FIPS mode or non-FIPS mode:

`/config/com/netegrity/config/keys/FIPSkey.dat`

If this file exists, Identity Manager is operating in FIPS mode.

The `FIPSkey.dat` key file is created by the password tool utility, `pwdtools.bat` (or `pwdtools.sh`), during Identity Manager installation.

More Information:

[The Password Tool](#) (see page 409)

Encrypted Text Formats

The algorithm name is added to the encrypted text as a prefix. This informs Identity Manager which algorithm was used for encryption.

In FIPS mode, the prefix is `{AES}`. For example, if you encrypt the text "password", the encrypted text is similar to this:

`{AES}:eolQCTq1CGPyg6qe++0asg==`

In non-FIPS mode (or JSAFE mode), the prefix is `{PBES}`. For example, if you encrypt the text "password", the encrypted text is similar to this:

`{PBES}:gSex2/BhDGzEKWvFmzca4w==`

Encrypted Information

The following Identity Manager information is encrypted:

- Passwords in the datasource configuration for Jboss
- Forgotten password recovery information
- Any other attributes that are flagged as sensitive
- Provisioning Server callback secret
- Workflow session information
- Policy Server connection information
- Data in provisioning components

FIPS Mode Logging

The following CA Identity Manager components indicate in log files whether FIPS mode is enabled:

- Identity Manager Server
- Provisioning Server
- C++ Connector Server
- Java Connector Server
- Provisioning Manager
- Password Synchronization Agent

In all cases, the log entry indicating that FIPS mode is enabled ends with the following string:

FIPS 140-2 MODE: ON

Index

<

<% %> HTML tag extension • 294

<%= %> HTML tag extension • 294

A

access roles

 Delete Access Role • 391

 Modify Access Role • 392

 View Access Role • 392, 394, 400

Access Roles category

 about • 391

ACCESSROLE object type • 296

ACCESSTASK object type • 296

Actions on Apply/Remove policies • 134, 137

Active Directory

 creating task screens • 116

 sAMAccountName requirements • 116

add() • 296

Add/Remove Action • 37

ADMIN notification rule • 296

admin roles

 Create Admin Role • 393

 Delete Admin Role • 393

 Modify Admin Role • 394

 Modify Admin Role Members/Administrators • 394

 View Admin Role Members/Administrators • 394

Admin Roles category

 about • 393

admin tasks

 Access Roles category • 391

 Active Directory considerations • 116

 Admin Roles category • 393

 Change My Password • 389

 Create Access Task • 391

 Create Admin Role • 393

 Create Admin Task • 393

 Create Group • 396

 Create Organization • 397

 Create User • 403

 Delete Access Role • 391

 Delete Admin Role • 393

 Delete Admin Task • 393

 Delete Group • 396

 Delete Organization • 397

 Delete User • 403

 Enable/Disable User • 403

 Groups category • 395

 inserting into email • 309

 Modify Access Role • 392

 Modify Access Role Members/Administrators • 392

 Modify Access Tasks • 392

 Modify Admin Role • 394

 Modify Admin Role Members/Administrators • 394

 Modify Admin Task • 394

 Modify Group • 396

 Modify Group Members • 396

 Modify My Groups • 390

 Modify My Profile • 390

 Modify Organization • 397

 Modify User • 404

 Organizations category • 397

 Reset User Password • 404

 System category • 401

 View Access Role • 392, 394, 400

 View Access Role Members/Administrators • 392

 View Access Task • 392

 View Admin Task • 394

 View Group • 397

 View My Roles • 390

 View My Submitted Tasks • 390

 View Organization • 397

 View Submitted Tasks • 401

 View User • 404

administrators

 inserting into email • 296, 309

ADMINROLE object type • 296

ADMINTASK object type • 296

API

 Email Template • 296

 inheriting methods from Identity Manager API • 309

application functions and external tasks • 118

Apply Once setting • 132

approval status in email • 296

APPROVAL_STATUS_APPROVED • 296

APPROVAL_STATUS_REJECTED • 296

Approved template • 290
retrieving information for • 296

B

_bcc email template object • 296

C

categories

- Access Roles • 391
- Admin Roles • 393
- default • 388
- Organizations • 397
- System • 401

_cc email template object • 296

certification

- about • 211
- configuring • 212
- determining certifiers • 214
- prerequisites • 213
- starting the certification process • 217

CertificationNonCertifiedActionCompletedNotification.tpl • 290

CertificationNonCertifiedActionPendingNotification.tpl • 290

CertificationRequiredFinalNotification.tpl • 290

CertificationRequiredNotification.tpl • 290

CertificationRequiredReminderNotification.tpl • 290

certifiers

- specifying • 214

Certify Employee.tpl • 290

Certify User task • 218

Change My Password • 389

commonattribute

- in User Manager Notification Adapter • 296

Completed template • 290

- retrieving information for • 296

compliance

- certifying user entitlements • 211

compliance check box

- in identity policy sets • 131

configuring

- password composition requirements • 174
- user certification • 212

configuring email notifications for certification • 214

context information

events • 296

tasks • 296

Create Access Task • 391

Create Admin Role • 393

Create Admin Task • 393

Create Group • 396

Create Organization • 397

Create User • 403

CreateProvisioningUserNotificationEvent.tpl • 290

customizing Identity Manager

- email generation • 289

- email templates • 293

D

default tasks • 388

defaultEvent.tpl • 290

defaultTask.tpl • 290

delegation

- worklist • 390

Delete Access Role • 391

Delete Access Task • 391

Delete Admin Role • 393

Delete Admin Task • 393

Delete Group • 396

Delete Organization • 397

Delete User • 403

deploying email templates • 311

description

- dynamic groups • 204

- nested groups • 206

- parent groups • 206

- static groups • 203

dynamic email messages • 293

dynamic groups

- description • 204

- example • 208

E

email notifications

- about • 287

- configuring for user certification • 214

- Email Template API • 296

- enabling for a task • 289

- enabling for an event • 289

- enabling for the environment • 288

- generated from templates • 290

- when generated • 287

Email Template API • 296

- inheriting Identity Manager API methods • 309
- email templates
 - about • 293
 - Approved template • 290
 - changing the From value • 296
 - Completed template • 290
 - contents • 290
 - customizing • 293
 - default • 290, 311
 - deploying • 311
 - elements • 294
 - Email Template API • 296
 - event states • 290
 - Java output stream • 311
 - JavaScript • 294
 - location • 290
 - names • 312
 - notification rules • 296
 - objects • 296
 - Pending template • 290
 - Rejected template • 290
 - sets of • 311
 - specifying for an environment • 312
 - tag extensions • 294
 - variables • 294
- email.properties • 296
- emailTemplates directory • 290, 311
- Enable/Disable User • 403
- _encoding email template object • 296
- _eventContextInformation email template object • 296
- events
 - context information for email • 296
 - inserting into email • 296
 - states, and email templates • 290
 - triggering email notifications • 289
- examples
 - identity policy sets • 145
- ExposedEventContextInformation class • 296
- ExposedEventContextInformation interface • 296
- ExposedTaskContextInformation interface • 296

F

- Forgotten Password Reset task
 - about • 156
 - customizing • 157

- Forgotten User ID task
 - customizing • 157
- ForgottenPassword.templ • 290

G

- getAdminFriendlyName() • 296
- getAdministrator() • 296, 309
- getAdminName() • 296
- getAdminTask() • 296, 309
- getApprovalStatus() • 296
- getApprovalTime() • 296
- getEventName() • 296
- getExposedEventContexts() • 296
- getNotifiers() • 296
- getObjectOrganizationFriendlyName() • 296
- getOrgName() • 296
- getPassword() • 296
- getPrimaryObjectName() • 296
- getPrimaryObjectTypeName() • 296
- getSecondaryObjectName() • 296
- getSecondaryObjectTypeName() • 296
- getTaskFriendlyName() • 296
- getTaskName() • 296
- GROUP object type • 296
- group type and scope in Active Directory • 117
- groups
 - Create Group • 396
 - Delete Group • 396
 - Modify Group • 396
 - Modify Group Members • 396
 - View Group • 397

I

- identification screens
 - designing • 159
- Identity Manager
 - email template objects • 296
- identity policies
 - about • 129
 - Action on Apply Policy • 137
 - creating • 131
 - synchronizing users • 141
- identity policy sets
 - about • 130
 - about the apply one setting • 132
 - Action on Apply/Remove Policy settings • 134
 - creating • 131
 - defining change actions • 137

- defining policy conditions • 134
- examples • 145
- managing • 140
- planning • 130

implicit message objects • 296

J

Java standard output stream • 311
Javadoc reference • 311
JavaScript in email templates • 294

M

managerattribute
 in User Manager Notification Adapter • 296
Modify Access Role • 392
Modify Access Task • 392
Modify Admin Role • 394
Modify Admin Role Members/Administrators • 394
Modify Admin Task • 394
Modify Group • 396
Modify Group Members • 396
Modify My Groups • 390
Modify Organization • 397
ModifyUserEvent.tmp • 290

N

nested groups
 creating • 206
 description • 206
 example • 208
notification rules • 296
notification templates
 See email templates • 293

O

objects for email templates • 296
ORGANIZATION object type • 296
organizations
 adding to email • 296
 Create Organization • 397
 Delete Organization • 397
 Modify Organization • 397
 View Organization • 397
Organizations category • 397
owner rules
 for an access role • 128
 for an admin role • 46

P

parent groups • 206
 description • 206
password policies
 about • 172
 composition • 174
 expiration • 181
passwords
 inserting into email • 296
Pending template • 290
 retrieving information for • 296
policy conditions
 in identity policy sets • 134
primary objects in email • 296
protected tasks
 list of • 151
public tasks
 list of • 151

R

Rejected template • 290
 retrieving information for • 296
remote task submission
 See also Task Execution Web Service • 217
Reset User Password • 404

S

secondary objects in email • 296
self registration
 adding verification questions • 154
 setting up a default organization • 154
Self Registration.tmp • 290
Self-Registration task
 configuring • 153
self-service tasks
 understanding • 151
standard output stream • 311
static groups
 creating • 203
 description • 203
 example • 208
_subject email template object • 296
Synchronize User task • 143
System category
 about • 401

T

tags for email templates • 294

- task execution
 - remote task submission • 217
- Task Execution Web Service
 - about • 217
- task screens
 - Active Directory considerations • 116
 - adding sAMAccountName • 116
- _taskContextInformation email template object
 - 296
- tasks
 - context information for email • 296
 - default categories • 388
 - inserting into email • 296
 - remote task submission • 217
 - self-service • 166
 - triggering email notifications • 289
 - validation • 121
- _template email template object • 296
- templates for email messages
 - See email templates • 293
- _to email template object • 296

U

- user interface
 - default categories • 388
- User Manager Notification Adapter • 296
- USER notification rule • 296
- USER object type • 296
- user synchronization
 - and identity policies • 141
 - automatic synchronization • 142
 - manual synchronization • 143
 - verifying • 143
- USER_MANAGER notification rule • 214, 296
- users
 - certifying entitlements for • 211
 - Create User • 403
 - Delete User • 403
 - Enable/Disable User • 403
 - Modify User • 404
 - Reset User Password • 404
 - synchronizing with identity policies • 141
 - View User • 404
- _util email template object • 296

V

- validation
 - task-level • 121
- variables in email templates • 294

- verification screens
 - designing • 160
- View Access Role • 392, 394, 400
- View Access Role Members/Administrators • 392
- View Access Task • 392
- View Admin Role Members/Administrators • 394
- View Group • 397
- View My Roles • 390
- View My Submitted Tasks • 390
- View Organization • 397
- View Submitted Tasks • 401
- View User • 404

W

- web services. See Task Execution Web Service
 - 217
- workflow
 - description • 19