Sun Java™ System

Identity Manager 6.0 2005Q4M3 Administration

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-4481-10

Contents

Contents

Identity Manager Overview

Getting Started with Identity Manager

User and Account Management

Administration

Configuration

Data Synchronization and Loading

Security

Reporting

Task Templates

PasswordSync

lh Reference

Advanced Search for Online Documentation

Preface

This guide describes how to use the Sun Java™ System Identity Manager software to provide secure user access to your enterprise information systems and applications. It illustrates procedures and scenarios to help you perform regular and periodic administrative tasks with the Identity Manager system.

How to Find Information in this Guide

The guide is organized in these chapters:

- Chapter 1. *Identity Manager Overview* — Provides high-level information about the Identity Manager product and objects.
- Chapter 2. *Getting Started with Identity Manager* — Introduces the Identity Manager interfaces and guides you to basic Identity Manager tasks.
- Chapter 3. *User and Account Management* — Details user management concepts and tasks.
- Chapter 4. *Administration* — Discusses delegated administration and provides procedures for working with Identity Manager administrators, organizations, and virtual organizations.
- Chapter 5. *Configuration* — Provides additional information and procedures about configuring Identity Manager objects such as roles, resources, policies, capabilities, and admin roles.
- Chapter 6. *Data Synchronization and Loading* — Discusses Identity Manager facilities for synchronizing data and loading groups of users.
- Chapter 7. *Security* — Describes Identity Manager security features and offers recommendations for best practices while using Identity Manager.
- Chapter 8. *Reporting* — Details the Identity Manager system's full-service reporting and risk analysis capabilities.
- Chapter 9. *Task Templates* — Shows you how to use the Administrator interface to configure certain workflow behaviors, as an alternative to writing customized workflows.
- Chapter 10. *PasswordSync* — describes the PasswordSync feature, which enables Windows systems to securely change and reset user passwords and synchronize them through Identity Manager.

Related Documentation and Help

Sun provides additional documentation and information to help you install, use, and configure Identity Manager.

- *Identity Manager Installation*

  Step-by-step instructions and reference information to help you install and configure Identity Manager and associated software.
- *Identity Manager Upgrade*

  Step-by-step instructions and reference information to help you upgrade and configure Identity Manager and associated software.
- *Identity Manager Administration*

  Procedures, tutorials, and examples that describe how to use Identity Manager to provide secure user access to your enterprise information systems.
- *Identity Manager Technical Deployment Overview*

  Conceptual overview of the Identity Manager product (including object architectures) with an introduction to basic product components.
- *Identity Manager Workflows, Forms, and Views*

  Reference and procedural information that describes how to use the Identity Manager workflows, forms, and views — including information about the tools you need to customize these objects.
- *Identity Manager Deployment Tools*

  Reference and procedural information that describes how to use different Identity Manager deployment tools; including rules and rules libraries, common tasks and processes, dictionary support, and the SOAP-based Web service interface provided by the Identity Manager server.
- *Identity Manager Resources Reference*

  Reference and procedural information that describes how to load and synchronize account information from a resource into Identity Manager.
- *Identity Manager Audit Logging*

  Reference and procedural information that describes how to load and synchronize account information from a resource into Identity Manager.
- *Identity Manager Tuning, Troubleshooting and Error Messages*

  Reference and procedural information that describes Identity Manager error messages and exceptions, and provide instructions for tracing and troubleshooting problems you might encounter as you work.

- *Identity Manager Help*

  Online guidance and information that offer complete procedural, reference, and terminology information about Identity Manager. You can access help by clicking the Help link from the Identity Manager menu bar. Guidance (field-specific information) is available on key fields.

Product Support

If you have problems deploying or using Identity Manager, use one of these mechanisms to contact customer support:

- The online support Web site at http://www.sun.com/service/online/us
- The telephone dispatch number associated with your maintenance contract

We'd Like to Hear from You!

We would like to know what you think of this guide and other documentation provided with Identity Manager. If you have feedback - positive or negative - about your experiences using this product and documentation, please send us a note.

Sun Microsystems.
5300 Riata Park Court
Austin, TX 78727
Attn: Identity Manager Information Development

Email: idm-idd@sun.com

1 Identity Manager Overview

The Sun Java™ System Identity Manager system enables you to securely and efficiently manage access to accounts and resources. By giving you the capabilities and tools to quickly handle periodic and daily tasks, Identity Manager facilitates exceptional service to internal and external customers.

The Big Picture

Today's businesses require increased flexibility and capabilities from its IT services. Historically, managing access to business information and systems required direct interaction with a limited number of accounts. Increasingly, managing access means handling not only increased numbers of internal customers, but also partners and customers beyond your enterprise.

The overhead created by this increased need for access can be substantial. As an administrator, you must effectively and securely enable people – both inside and outside your enterprise – to do their jobs. And after you provide initial access, you face continuing detailed challenges, such as forgotten passwords, and changed roles and business relationships.

Identity Manager was developed specifically to help you manage these administrative challenges in a dynamic environment. By using Identity Manager to distribute access management overhead, you facilitate a solution to your primary challenges: How do I define access? And once defined, how do I maintain flexibility and control?

A secure, yet flexible design lets you set up Identity Manager to accommodate the structure of your enterprise and answer these challenges. By mapping Identity Manager objects to the entities you manage – users and resources – you significantly increase the efficiency of your operations.

Goals of the Identity Manager System

The Identity Manager solution lets you:

- Manage account access to a large variety of systems and resources.
- Securely manage dynamic account information for each user's array of accounts.
- Set up delegated rights to create and manage user account data.
- Handle large numbers of enterprise resources, as well as an increasingly large number of extranet customers and partners.

- Securely authorize user access to enterprise information systems. With Identity Manager, you have fully integrated functionality to grant, manage, and revoke access privileges across internal and external organizations.
- Keep data in sync by *not* keeping data. The Identity Manager solution supports two key principles that superior systems management tools should observe:
  - The product should have minimal impact on the system it is managing, and
  - The product should not introduce more complexity to your enterprise by adding another resource to manage.

Defining User Access

Users in your extended enterprise can be anyone with a relationship to your company, including employees, customers, partners, suppliers, or acquisitions. In the Identity Manager system, users are represented by *user accounts*.

Depending on their relationships with your business and other entities, users need access to different things, such as computer systems, data stored in databases, or specific computer applications. In Identity Manager terms, these things are *resources*.

Because users often have one or more identities on each of the resources they access, Identity Manager creates a single, *virtual identity* that maps to disparate resources. This allows you to manage users as a single entity.

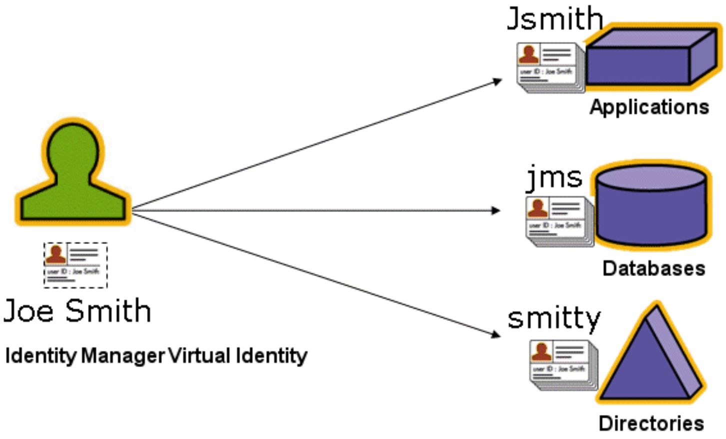


Figure 1. Identity Manager User Account | Resource Relationship

To effectively manage large numbers of users, you need logical ways to group them. In most companies, users are grouped into functional departments or divisions. Each of these departments typically requires access to different resources. In Identity Manager terminology, this type of group is called an *organization*.

Another way to group users is by similar characteristics, such as company relationships or job functions. Identity Manager recognizes these groupings as *roles*.

Within the Identity Manager system, you assign roles to user accounts to facilitate efficient enabling and disabling of access to resources. Assigning accounts to organizations enables efficient delegation of administrative responsibilities.

Identity Manager users are also directly or indirectly managed through the application of *policies*, which set up rules, and password and user authentication options.

Delegating Administration

To successfully distribute responsibility for user identity management, you need the right balance of flexibility and control. By granting select Identity Manager users *administrator* privileges and delegating administrative tasks, you reduce your overhead and increase efficiency by placing responsibility for identity management with those who know user needs best, such as a hiring manager. Users with these extended privileges are called Identity Manager *administrators*.

Delegation only works, however, within a secure model. To maintain an appropriate level of control, Identity Manager lets you assign different levels of *capabilities* to administrators. Capabilities authorize varying levels of access and actions within the system.

The Identity Manager workflow model also includes a method to ensure that certain actions require approval. Using workflow, Identity Manager administrators retain control over tasks and can track their progress. For detailed information about workflow, see *Identity Manager Workflows, Forms, and Views*.

Identity Manager Objects

A clear picture of Identity Manager objects and how they interact is crucial to successful management and deployment of the system. These are:

- User accounts
- Roles
- Resources and resource groups
- Organizations and virtual organizations
- Capabilities
- Admin roles

User Accounts

Identity Manager user accounts:

- Provide users access to one or more resources, and manage user account data on those resources.
- Assign roles, which set user access to various resources.
- Are part of an organization, which determines how and by whom user accounts are administered.

The user account setup process is dynamic. Depending on the role selection you make during account setup, you may provide more or less resource-specific information to create the account. The number and type of resources associated with the assigned role determine how much information is required at account creation.

You grant users administrative privileges to manage user accounts, resources, and other Identity Manager system objects and tasks. Identity Manager administrators manage organizations, and are assigned a range of capabilities to apply to objects in each managed organization.

Roles

A role is an Identity Manager object that represents Identity Manager user types and allows resources to be grouped and assigned to users. Typically, roles represent user job functions. In a financial institution, for example, roles might correspond to job functions like bank teller, loan officer, branch manager, clerk, accountant, or administrative assistant.

Roles define a base set of resources and resource attributes for users. They also can define relationships between other roles; for example, roles that contain or exclude other roles.

Users with the same role share access to a common base group of resources. You can assign one or more roles to each user, or no role.

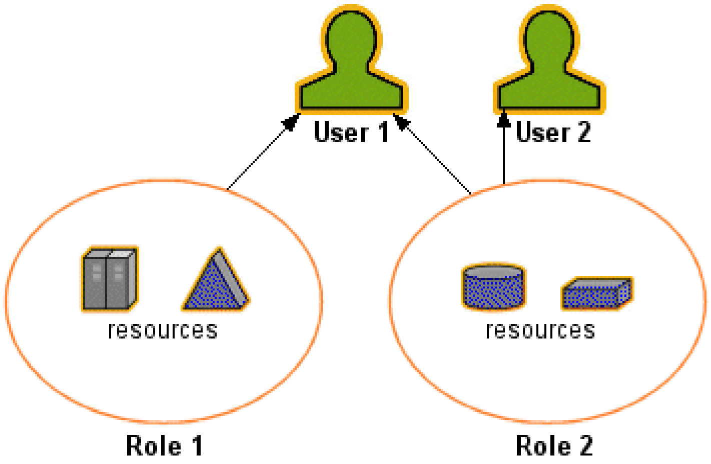


Figure 2. User Account, Role, Resource Relationship

As shown in the previous figure, User 1 and User 2 share access to the same set of resources through assignment of Role 2. User 1, however, has access to additional resources through the assignment of Role 1.

Resources and Resource Groups

Identity Manager resources store information about how to connect to a resource or system on which accounts are created. Resources to which Identity Manager provides access include:

- Mainframe security managers
- Databases
- Directory services (such as LDAP)
- Applications
- Operating systems
- ERP systems (such as SAP™)
- Messaging platforms (such as Microsoft® Exchange)

Information stored by each Identity Manager resource is categorized in several major groups:

- Resource parameters
- Account information (including account attributes and identity template)
- Identity Manager parameters

Identity Manager user accounts are provided access to resources through:

- Role-based assignment – By assigning roles to a user, you indirectly assign the user to one or more resources connected to that role.
- Individual assignment – You can assign individual resources directly to user accounts.

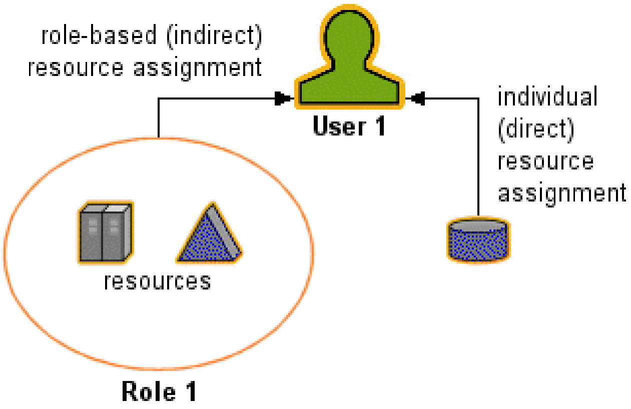

role-based (indirect) resource assignment
User 1
individual (direct) resource assignment
resources
Role 1

Figure 3. Resources Assignment

A related Identity Manager object, a *resource group*, can be assigned to user accounts in the same way resources are assigned. Resource groups correlate resources so that you can create accounts on resources in a specific order.

Organizations

Organizations are Identity Manager containers used to enable administrative delegation. They define the scope of entities that an Identity Manager administrator controls or manages.

Organizations can also represent direct links into directory-based resources; these are called *virtual organizations*. Virtual organizations allow direct management of resource data without loading information into the Identity Manager repository. By mirroring an existing directory structure and membership through a virtual organization, Identity Manager eliminates duplicate and time-consuming setup tasks.

Organizations that contain other organizations are *parent* organizations. You can create organizations in a flat structure or arrange them in a hierarchy. The hierarchy can represent departments, geographical areas, or other logical divisions by which you manage user accounts.

Capabilities

Each user can be assigned capabilities, or groups of rights, to enable him to perform administrative actions through Identity Manager. Capabilities allow the administrative user to perform certain tasks in the system and act on Identity Manager objects.

Typically, you assign capabilities according to specific job responsibilities, such as password resets or account approvals. By assigning capabilities and rights to individual users, you create a hierarchical administrative structure that provides targeted access and privileges without compromising data protection.

Identity Manager provides a set of default capabilities for common administrative functions. Capabilities meeting your specific needs can also be created and assigned.

Admin Roles

Admin roles enable you to define a unique set of capabilities for each set of organizations that are managed by an administrative user. An admin role is assigned capabilities and controlled organizations, which can then be assigned to an administrative user.

Capabilities and controlled organizations can be assigned directly to an admin role. They also can be assigned indirectly (dynamically) each time the administrative user logs in to Identity Manager. Identity Manager rules control dynamic assignment.

Object Relationships

The following table provides a quick glance at Identity Manager objects and their relationships.

Identity Manager object	**What is it?**	**Where does it fit?**
User account	An account on Identity Manager and on one or more resources. User data may be loaded into Identity Manager from resources. A special class of users, Identity Manager administrators, have extended privileges.	*Role* Generally, each user account is assigned to one or more roles. *Organization* User accounts are arranged in a hierarchy as part of an organization. Identity Manager administrators additionally manage organizations. *Resource* Individual resources can be assigned to user accounts. *Capability* Administrators are assigned capabilities for the organizations they manage.
Role	Profiles a class of users and defines the collection of resources and resource attributes on which accounts are managed.	*Resource and resource group* Resources and resource groups are assigned to roles. *User account* Roles group user accounts with similar characteristics. *Role* Defines relationships between other roles (inclusion or exclusion).
Resource	Stores information about a system, application, or other resource on which accounts are managed.	*Role* Resources are assigned to roles; a user account “inherits” resource access from its role assignments. *User account* Resources can be individually assigned to user accounts.
Resource Group	Ordered group of resources.	*Role* Resource groups are assigned to roles; a user account “inherits” resource access from its role assignments. *User account* Resource groups can be directly assigned to user accounts.

Identity Manager object	**What is it?**	**Where does it fit?**
Organization	Defines the scope of entities managed by an administrator; hierarchical.	*Resource* Administrators in a given organization may have access to some or all resources. *Administrator* Organizations are managed (controlled) by users with administrative privileges. Administrators may manage one or more organizations. Administrative privileges in a given organization cascade to its child organizations. *User account* Each user account can be assigned to an Identity Manager organization and one or more directory organizations.
Admin role	Defines a unique set of capabilities for each set of organizations assigned to an administrator.	*Administrator* Admin roles are assigned to administrators. *Capabilities and organizations* Capabilities and organizations are assigned, directly or indirectly (dynamically) to admin roles.
Capability	Defines a group of system rights.	*Administrator* Capabilities are assigned to administrators.
Policy	Sets password and authentication limits.	*User account* Policies are assigned to user accounts. *Organization* Policies are assigned to or inherited by organizations.

Table 1. Identity Manager Object Relationships

Identity Manager Terms

Identity Manager interfaces and guides define these terms as follows:

admin role

Unique set of capabilities for each set of organizations assigned to an administrative user.

administrator

Person who sets up Identity Manager or is responsible for operational tasks, such as creating users and managing access to resources.

administrator interface

Primary administrative view of Identity Manager.

approver

User with administrative capabilities responsible for approving or rejecting access requests.

business process editor (BPE)

Graphical view of Identity Manager forms, rules, and workflow.

capability

Group of access rights for user accounts that governs actions performed in Identity Manager; low-level access control within Identity Manager.

form

Object associated with a Web page that contains rules about how a browser should display user view attributes on that page. Forms can incorporate business logic, and are often used to manipulate view data before it is presented to the user.

identity template

Defines the user’s resource account name.

organization

Identity Manager container used to enable administrative delegation. Organizations define the scope of entities (such as user accounts, resources, and administrator accounts) an administrator controls or manages. Organizations provide a “where” context, primarily for Identity Manager administrative purposes.

policy

Establishes limitations for Identity Manager accounts. *Identity Manager policies* establish user, password, and authentication options, and are tied to organizations or users. *Resource password* and *account ID* policies set rules, allowed words, and attribute values, and are tied to individual resources.

resource

In Identity Manager, stores information about how to connect to a resource or system on which accounts are created. Resources to which Identity Manager provides access include mainframe security managers, databases, directory services, applications, operating systems, ERP systems, and messaging platforms.

resource adapter

Identity Manager component that provides a link between the Identity Manager engine and the resource. This component enables Identity Manager to manage user accounts on a given resource (including create, update, delete, authenticate, and scan capabilities) as well as utilize that resource for pass-through authentication.

resource adapter account

Credentials used by an Identity Manager resource adapter to access a managed resource.

resource group

Collection of resources used to order the creation, deletion, and update of user resource accounts.

resource wizard

Identity Manager tool that steps through the resource creation and modification process, including setup and configuration of resource parameters, account attributes, identity template, and Identity Manager parameters.

role

In Identity Manager, a template or profile for a class of users. Each user can be assigned to one or more roles, which define account resource access and default resource attributes.

rule

Object in the Identity Manager repository that contains a function written in XPRESS, XML Object, or JavaScript languages. Rules provide a mechanism for storing frequently used logic or static variables for reuse within forms, workflows, and roles.

schema

List of user account attributes for a resource.

schema map

Map of resource account attributes to Identity Manager account attributes for a resource. Identity Manager account attributes create a common link to multiple resources and are referenced by forms.

user

Person who holds an Identity Manager system account. Users can hold a range of capabilities in Identity Manager; those with extended capabilities are Identity Manager *administrators*.

user account

Account created using Identity Manager. Refers either to an Identity Manager account or accounts on Identity Manager resources. The user account setup process is dynamic; information or fields to be completed depend on the resources provided to the user directly or indirectly through role assignment.

user interface

Limited view of the Identity Manager system. Specifically tailored to users without administrative capabilities, it allows them to perform a range of self-service tasks such as changing passwords and setting answers to authentication questions.

workflow

A logical, repeatable process during which documents, information, or tasks are passed from one participant to another. Identity Manager workflows comprise multiple processes that control creation, update, enabling, disabling, and deletion of user accounts.

2 Getting Started with Identity Manager

Read this chapter to learn about the Identity Manager graphical interfaces and how you can quickly begin using Identity Manager. Topics covered here include:

- Identity Manager interfaces
- Help and Guidance
- Tasks you can perform and where to begin

Identity Manager Interfaces

The Identity Manager system includes three primary graphical interfaces through which users perform tasks:

- Administrator Interface
- User Interface
- Business Process Editor (BPE)

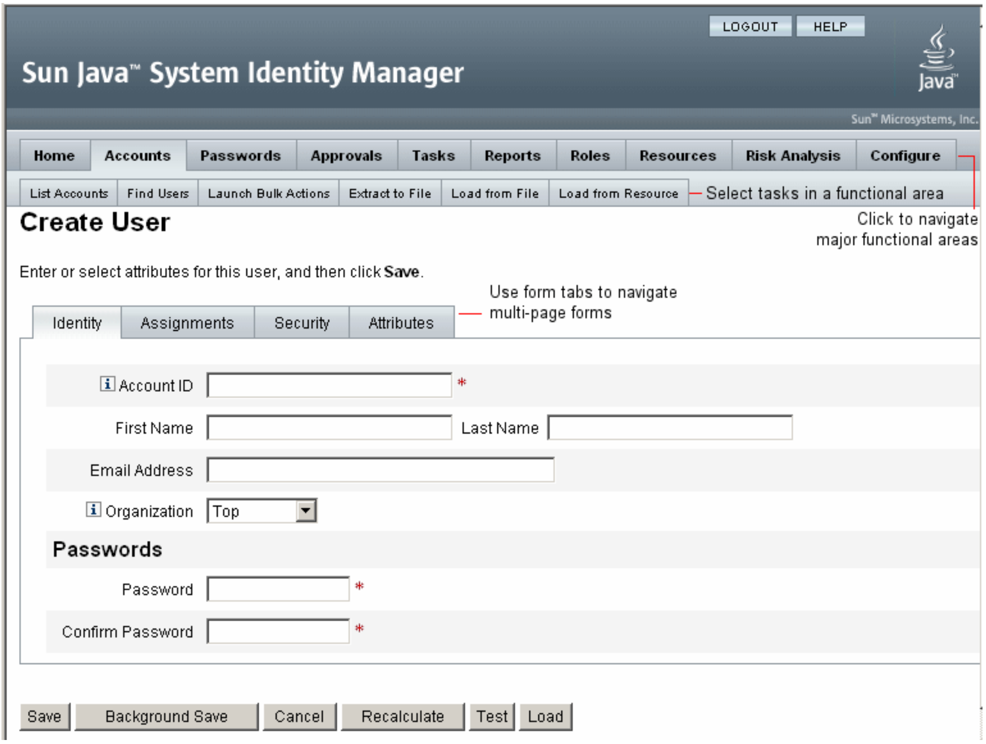
Identity Manager Administrator Interface

The Identity Manager Administrator Interface serves as the primary administrative view of the product. Through this interface, Identity Manager administrators manage users, set up and assign resources, and define rights and access levels in the Identity Manager system.

Interface organization is represented by:

- **Navigation bar tabs** — Located at the top of each interface page, these tabs let you navigate major functional areas.
- **Subtabs or menus** — Depending on your specific implementation, you may see secondary tabs or menus below each navigation bar tab. These subtab or menu selections let you access tasks within a functional area.

In some areas, such as Accounts, *tabbed forms* divide longer forms into one or more pages, enabling you to navigate them more easily.



Select tasks in a functional area

Click to navigate major functional areas

Create User

Enter or select attributes for this user, and then click **Save**.

Use form tabs to navigate multi-page forms

Organization: Top

Figure 1. Identity Manager Administrator Interface

Identity Manager User Interface

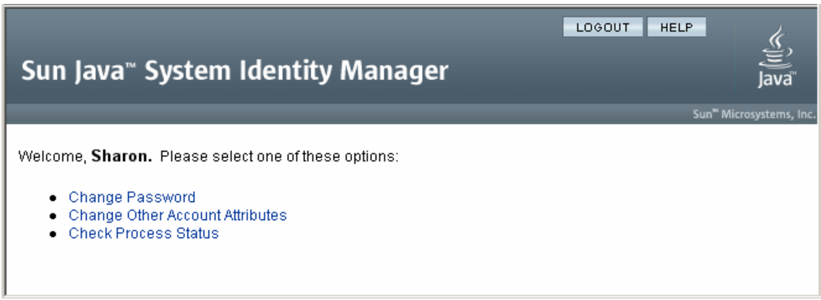
The Identity Manager User Interface presents a limited view of the Identity Manager system. This view is specifically tailored to users without administrative capabilities.

From the User Interface, users can:

- Change their passwords
- Perform self-provisioning tasks
- Manage profile information associated with their accounts

This interface is often customized to present a unique, company-specific view and offer custom selections.

Tip For detailed information about customizing and branding the User Interface, read *Identity Manager Technical Deployment Overview*.



Sun Java™ System Identity Manager

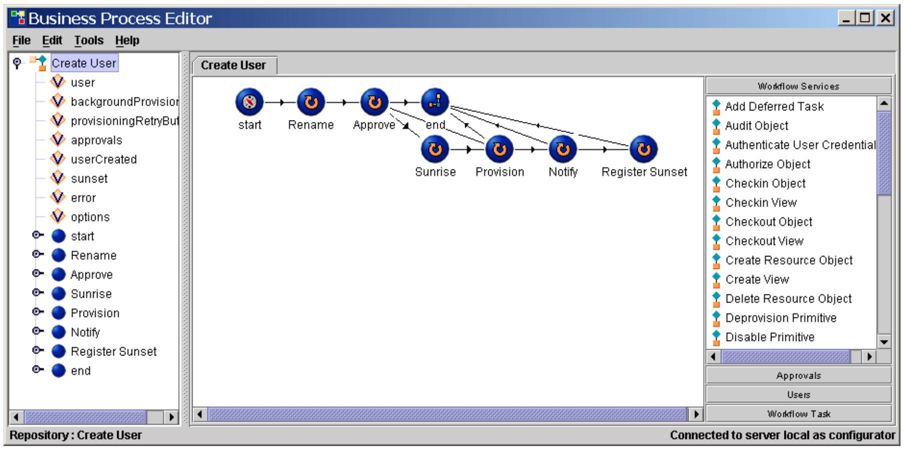
Welcome, **Sharon.** Please select one of these options:

- Change Password
- Change Other Account Attributes
- Check Process Status

Figure 2. Identity Manager User Interface

Identity Manager Business Process Editor

The Business Process Editor (BPE), also referred to as the Configuration Editor, provides a graphical view of Identity Manager forms, rules, and workflows. Using the BPE, you create and edit forms that establish the features available on each Identity Manager page. You also modify Identity Manager *workflows*, which define the sequence of actions followed or tasks performed when working with Identity Manager user accounts.



Repository : Create User

Connected to server local as configurator

Figure 3. Business Process Editor (Configuration Editor)

For more information about the BPE and using it to work with Identity Manager workflows, see *Identity Manager Workflows, Forms, and Views*.

Help and Guidance

To successfully complete some tasks, you may need to consult Help and Identity Manager *guidance* (field-level information and instructions). Help and guidance are available from the Identity Manager Administrator and User interfaces.

Identity Manager Help

For task-related help and information, click the **Help** button, which is located at the top of each Administrator and User Interface page.

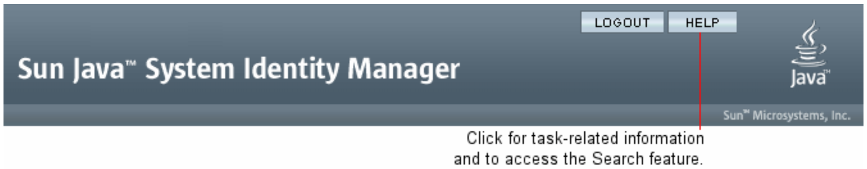

LOGOUT
HELP
Sun Java™ System Identity Manager
Java™
Sun™ Microsystems, Inc.
Click for task-related information and to access the Search feature.

Figure 4. Help

At the bottom of each Help window is a Contents link that guides you to other Help topics and the Identity Manager terms glossary.

Finding Information

Use the search feature in the Help window to locate topics and information included in Identity Manager Help and documentation. To search:

1. Enter one or more terms in the search area.
2. Select to search one of two documentation types. By default, the feature searches online help.
   - **Online Help** — In general, online information provides steps to help you perform a task or complete a form.
   - **Documentation** (Guides) — Identity Manager Guides primarily offer information to help you understand concepts and system objects, as well as complete reference information.
3. Click **Search**.

The search returns linked search results. Use the Previous/Next or First/Last buttons to page through the listed results.

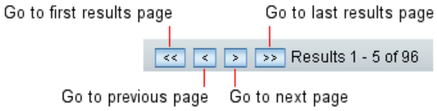


Figure 5. Search Results Navigation

Clicking **Reset** clears the contents of the Help window.

Search Behavior

If you search for more than one word, the search feature returns results that include each word, both words, and variants.

For example, if you enter to search for:

```
resource adapter
```

then the returned results will include matches to the words:

- `resource` (and variants)
- `adapter` (and variants)
- `resource` and `adapter` (in any order), with 0 to *n* intervening words

However, if you include search terms in quotations (for example, `“resource adapter”`), then the search feature returns only exact matches to that phrase.

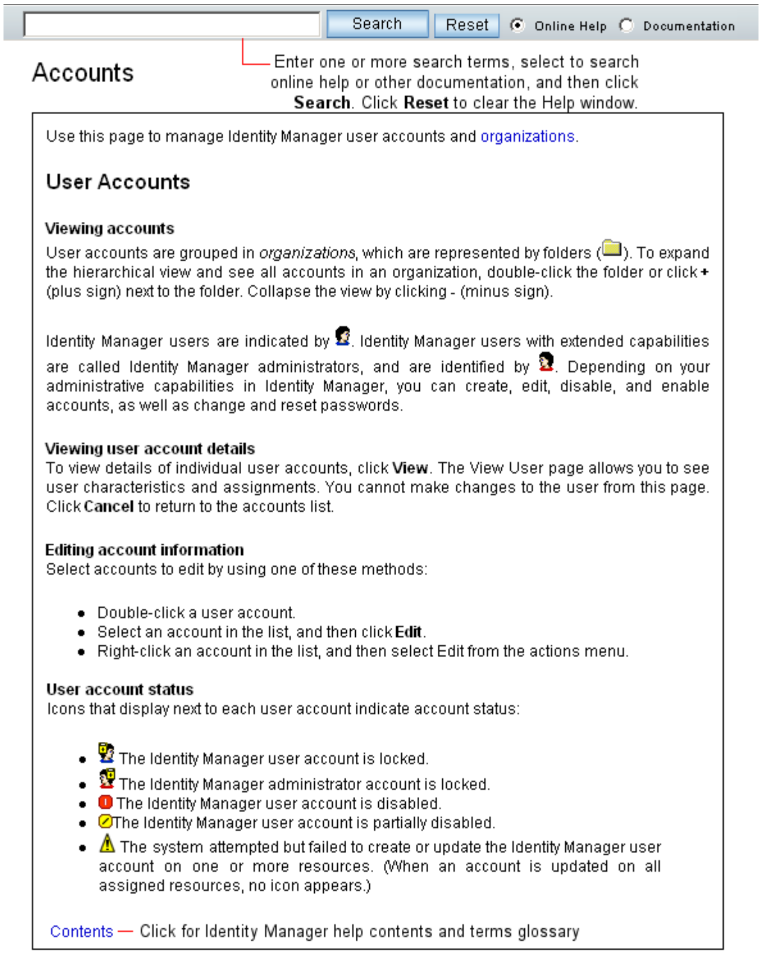
Alternatively, you can use advanced query syntax to specifically include, exclude, or order query elements.

Advanced Query Syntax

The Search feature supports advanced query syntax, including:

- **Wildcard characters** (? and *), which allow you to specify spelling patterns rather than complete words or phrases
- **Query operators** (AND or OR), which let you determine how to combine query elements

See *Advanced Search for Online Documentation* in this guide for more information about Identity Manager’s advanced documentation search features.



Enter one or more search terms, select to search online help or other documentation, and then click **Search**. Click **Reset** to clear the Help window.

Accounts

Use this page to manage Identity Manager user accounts and organizations.

User Accounts

Viewing accounts

User accounts are grouped in *organizations*, which are represented by folders ( ). To expand the hierarchical view and see all accounts in an organization, double-click the folder or click **+** (plus sign) next to the folder. Collapse the view by clicking - (minus sign).

Identity Manager users are indicated by . Identity Manager users with extended capabilities are called Identity Manager administrators, and are identified by . Depending on your administrative capabilities in Identity Manager, you can create, edit, disable, and enable accounts, as well as change and reset passwords.

Viewing user account details

To view details of individual user accounts, click **View**. The View User page allows you to see user characteristics and assignments. You cannot make changes to the user from this page. Click **Cancel** to return to the accounts list.

Editing account information

Select accounts to edit by using one of these methods:

- Double-click a user account.
- Select an account in the list, and then click **Edit**.
- Right-click an account in the list, and then select Edit from the actions menu.

User account status

Icons that display next to each user account indicate account status:

- The Identity Manager user account is locked.
- The Identity Manager administrator account is locked.
- The Identity Manager user account is disabled.
- The Identity Manager user account is partially disabled.
- ⚠ The system attempted but failed to create or update the Identity Manager user account on one or more resources. (When an account is updated on all assigned resources, no icon appears.)

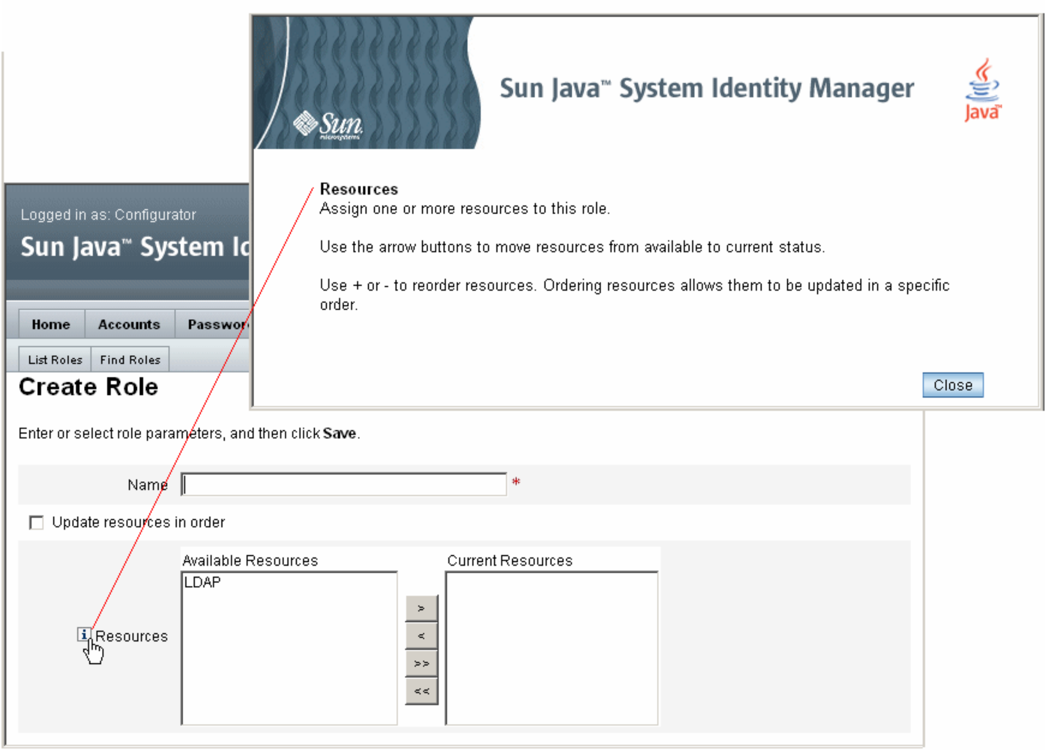
Contents — Click for Identity Manager help contents and terms glossary

Figure 6. Identity Manager Help

Identity Manager Guidance

Identity Manager guidance is brief, targeted help that appears next to many page fields. Its goal is to help you enter information or make selections as you move through a page to perform a task.

This symbol displays next to fields with guidance: ℹ. Click the symbol to open a window and display its associated information.



Sun Java™ System Identity Manager

Resources
Assign one or more resources to this role.

Use the arrow buttons to move resources from available to current status.

Use + or - to reorder resources. Ordering resources allows them to be updated in a specific order.

Logged in as: Configurator

Sun Java™ System Id

Create Role

Enter or select role parameters, and then click **Save**.

Name *

□ Update resources in order

Available Resources: LDAP

Current Resources

Figure 7. Identity Manager Guidance

Identity Manager Tasks

The following tasks matrix provides a quick reference to commonly performed Identity Manager tasks. It shows the primary Identity Manager interface location where you will go to begin each task, as well as alternate locations or methods (if available) that you can use to perform the same task.

Managing Identity Manager Users		
To do this:	Go to:	Or:
Create and edit users	**Accounts** tab, **List Accounts** selection	**Accounts** tab, **Find Users** selection (User Account Search Results page)
Approve user account creation	**Approvals** tab	
Set up user authentication (policies)	**Configure** tab, **Policies** selection	
Change user passwords	**Passwords** tab, **Change User Password** selection	• **Accounts** tab, **List Accounts** selection • **Accounts** tab, **Find Users** selection (User Account Search Results page) • Identity Manager User Interface
Reset user passwords	Passwords tab, Reset User Password selection	• **Accounts** tab, **List Accounts** selection • **Accounts** tab, **Find Users** selection (User Account Search Results page)
Find users	**Accounts** tab, **Find Users** selection	**Passwords** tab, **Change User Password** selection
Enable or disable users	**Accounts** tab, **List Accounts** selection	**Accounts** tab, **Find Users** selection (User Account Search Results page)
Unlock users	**Accounts** tab, **List Accounts** selection	**Accounts** tab, **Find Users** selection (User Account Search Results page)

Managing Identity Manager Administrators	
To do this:	**Go to:**
Set up delegated administration (through organizations)	**Accounts** tab, **List Accounts** selection, Create User page
Assign capabilities	**Accounts** tab, **List Accounts** selection, Create User page
Assign capabilities (through admin roles)	**Accounts** tab, **List Accounts** selection, Create User page
Set up approvers (to validate account creation)	• **Accounts** tab, **List Accounts** selection, Create Organization page • **Roles** tab, Create Roles page
Configuring Identity Manager	
To do this:	**Go to:**
Create and manage resources (Resource Wizard)	**Resources** tab
Manage resource groups	**Resource** tab, **List Resource Groups** selection
Create and manage roles	**Roles** tab
Find roles	**Roles** tab, **Find Roles** selection
Edit capabilities	**Configure** tab, **Capabilities** selection
Create and edit admin roles	**Configure** tab, **Admin Roles** selection, Create/Edit Admin Role page
Set up email templates	**Configure** tab, **Email Templates** selection
Set up password, account, and naming policies; assign policies to organizations	**Configure** tab, **Policies** selection
Configure Identity Attributes	**Configure** tab, **Identity Attributes** selection
Configure ChangeLogs	**Configure** tab, **ChangeLogs** selection

Loading and Synchronizing Accounts and Data		
To do this:	**Go to:**	
Import data files (such as XML-format forms)	**Configure** tab, **Import Exchange File** selection	
Load resource accounts	**Account** tab, **Load from Resource** selection	
Load accounts from file	**Account** tab, **Load from File** selection	
Compare Identity Manager users with resource accounts	**Resources** tab, **Reconcile with Resources** selection	
Auditing, Risk Analysis, and Reporting		
To do this:	**Go to:**	**To do this:**
Set up audit events to capture	**Configure** tab, **Audit Events** selection	Set up audit events to capture
Run and manage reports	**Reports** tab	Run and manage reports
Define and run risk analysis reports	**Risk Analysis** tab	Define and run risk analysis reports

Table 1. Identity Manager Interface Task Reference

Where to Go from Here

After you become familiar with Identity Manager interfaces and ways you can find information, you may want to focus on one of the following topics. They are presented by chapter in this guide:

- Chapter 3. *User and Account Management*
- Chapter 4. *Administration*
- Chapter 5. *Configuration*
- Chapter 6. *Data Synchronization and Loading*
- Chapter 7. *Security*
- Chapter 8. *Reporting*
- Chapter 9. *Task Templates*
- Chapter 10. *PasswordSync*

3 User and Account Management

This chapter provides information and procedures for managing users from the Identity Manager Administrator interface. You will learn about Identity Manager users and account management tasks, including:

- User account data, and how it is stored
- Accounts area of the Identity Manager Administrator Interface
- Account creation and editing capabilities, and other account-related tasks
- User account search features
- Password policies and user account passwords
- User self-service
- User authentication
- Bulk account actions

About User Account Data

A user is anyone who holds an Identity Manager system account. Identity Manager stores a range of data for each user. Collectively, this information forms a user's Identity Manager identity.

Viewed from the Create User page (**Accounts** tab) of the Administrator Interface, Identity Manager categorizes user data in four areas:

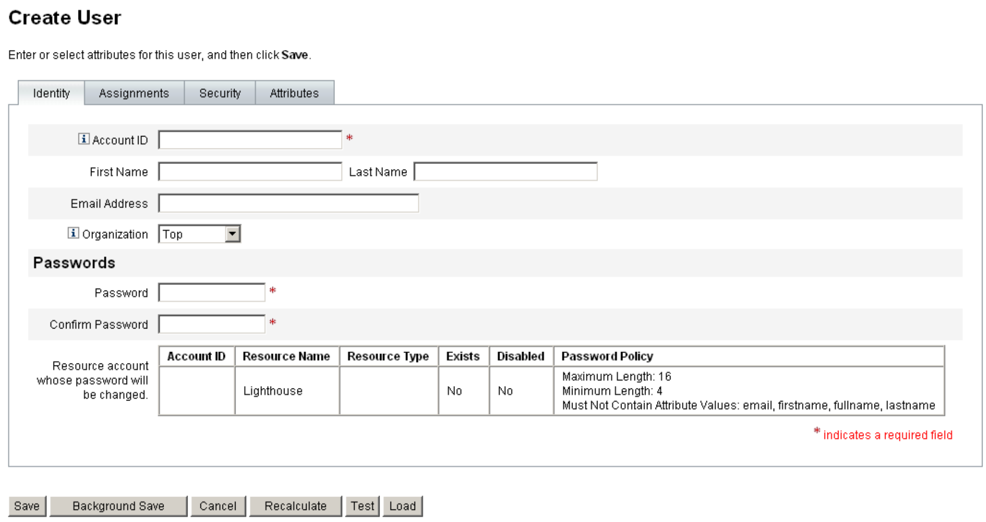
- Identity
- Assignments
- Security
- Attributes

Identity

The Identity area defines a user's account ID, name, contact information, governing organization, and Identity Manager account password. It also identifies the resources to which the user has access, and the password policy governing each resource account.

Note For information about setting up account password policies, read the section in this chapter titled *Setting Password Policies*.

The following figure illustrates the Identity area of the Create User page.



Create User

Enter or select attributes for this user, and then click **Save**.

Account ID *

First Name

Last Name

Email Address

Organization: Top

Passwords

Password *

Confirm Password *

Resource account whose password will be changed.

Account ID	Resource Name	Resource Type	Exists	Disabled	Password Policy
	Lighthouse		No	No	Maximum Length: 16 Minimum Length: 4 Must Not Contain Attribute Values: email, firstname, fullname, lastname

* indicates a required field

Figure 1. Create User - Identity

Assignments

The Assignments area sets limits for access to Identity Manager objects, such as resources.

Click the **Assignments** form tab to set up:

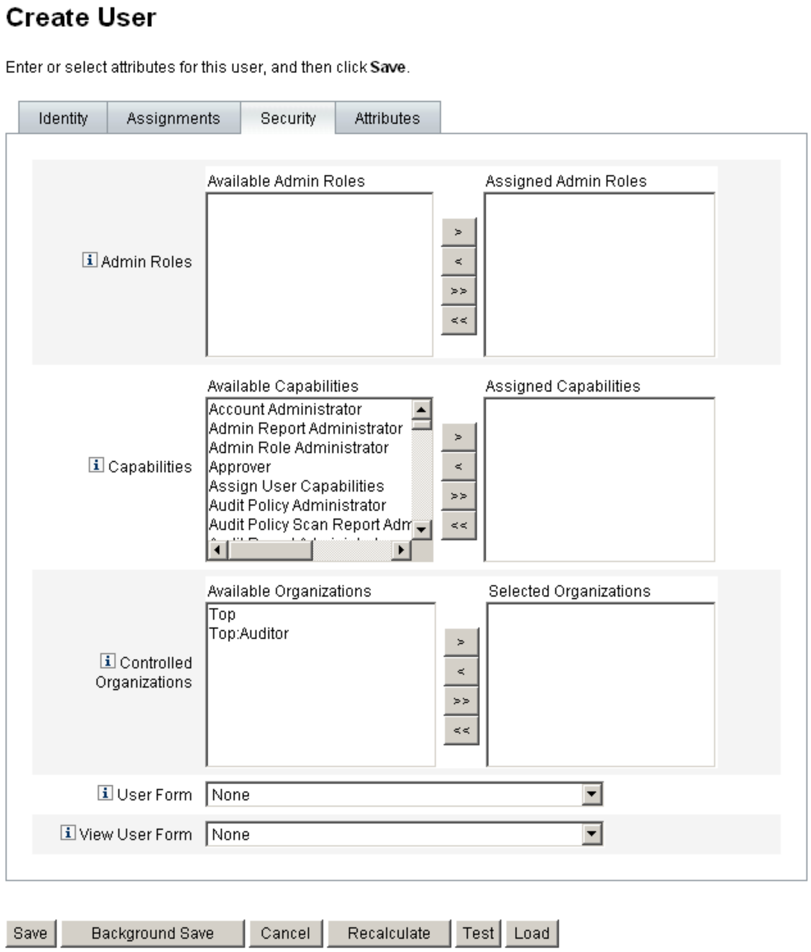
- **Identity Manager account policy** assignment — Establishes password and authentication limits.
- **Roles** assignment — Profiles a class of users. Roles define user access to resources through indirect assignment.
- **Resources and resource groups** access — Shows available resources and resource groups that can be directly assigned to the user, and resources that can be excluded from user access. These supplement resources that are indirectly assigned to the user through role assignment.

Security

In Identity Manager terminology, a user who is assigned extended capabilities is an Identity Manager *administrator*. The Security area establishes these extended administrative capabilities for the user, through assignment of:

- **Admin roles** — Combine a specific, unique set of capabilities and controlled organizations, facilitating coordinated assignment to administrative users.

- **Capabilities** — Enable rights in the Identity Manager system. Each Identity Manager administrator is assigned one or more capabilities, frequently aligned with job responsibilities.
- **Controlled organizations** — Assigns organizations that this user has rights to manage as an administrator. He can manage objects in the assigned organization and in any organizations below that organization in the hierarchy.



Create User

Enter or select attributes for this user, and then click **Save**.

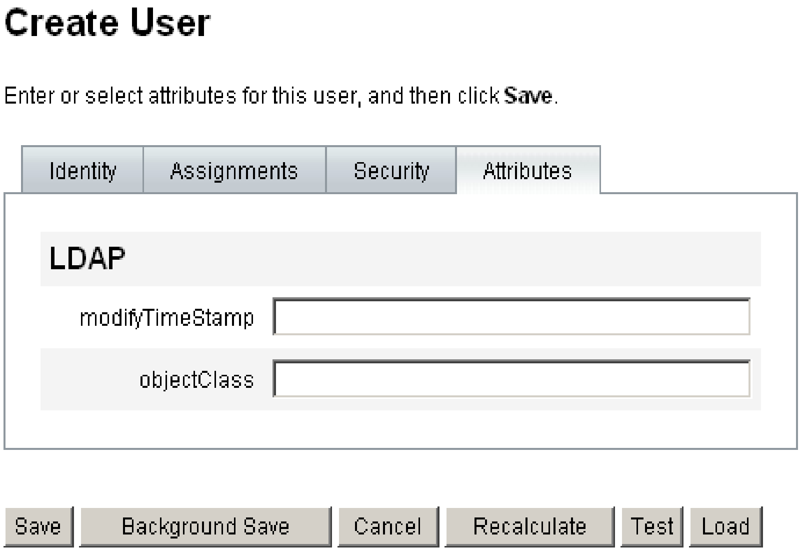
User Form: None

View User Form: None

Figure 2. Create User - Security

Attributes

The Attributes area defines account attributes associated with assigned resources. Listed attributes are categorized by assigned resource, and differ depending on which resources are assigned.



Create User

Enter or select attributes for this user, and then click **Save**.

Figure 3. Create User - Attributes

Accounts Area

The Identity Manager accounts area lets you manage Identity Manager users. To access this area, select **Accounts** from the Administrator Interface.

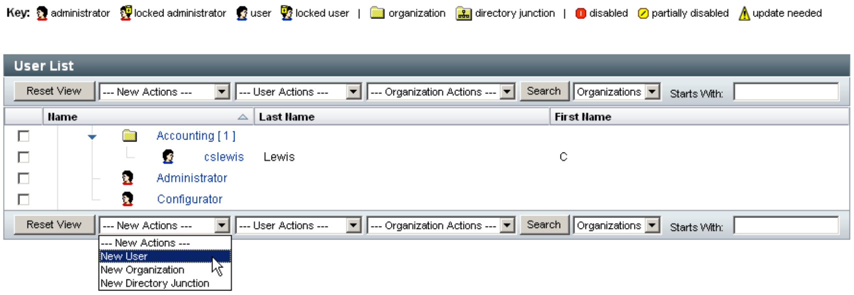
The accounts list shows all Identity Manager user accounts. Accounts are grouped in organizations and virtual organizations, which are represented hierarchically in folders.

You can sort the accounts list by full name (Name), user last name (Last Name), or user first name (First Name).

Click the header bar to sort by a column. Clicking the same header bar toggles between ascending and descending sort order.

Note When you sort by full name (the Name column), then all items in the hierarchy, at all levels, are sorted alphabetically.

To expand the hierarchical view and see accounts in an organization, click the triangular indicator next to a folder. Collapse the view by clicking the indicator again.


Key: administrator locked administrator user locked user | organization directory junction | disabled partially disabled update needed
User List
Reset View
--- New Actions ---
--- User Actions ---
--- Organization Actions ---
Search
Organizations
Starts With:
--- New Actions ---
New User
New Organization
New Directory Junction

	Name	Last Name	First Name
□	Accounting [1]		
□	cslewis	Lewis	C
□	Administrator		
□	Configurator		

Figure 4. Accounts List

Actions Lists in the Accounts Area

Use the actions lists (located at the top and bottom of the accounts area) to perform a range of actions. Actions list selections are divided among:

- **New Actions** — Create users, organizations, and directory junctions.
- **User Actions** — Edit, view, and change status of users; change and reset passwords; delete, enable, disable, unlock, move, update, and rename users; and run a user audit report.
- **Organization Actions** — Perform a range of organization and user actions.

Searching in the Accounts Area

Use the accounts area search feature to locate users and organizations. Select Organizations or Users from the list, enter one or more characters in the search area, and then click **Search**.

User Account Status

Icons that display next to each user account indicate current, assigned account status:

Indicator	Status
🔒	The Identity Manager user account is locked. This means that a user is locked out of a resource account because unsuccessful login attempts have exceeded the limit established for the resource.
🔒	The Identity Manager administrator account is locked.
⛔	The account is disabled on all assigned resources and on Identity Manager. (When an account is enabled, no icon appears.)
⊘	The account is partially disabled, meaning that it is disabled on one or more assigned resources.
⚠	The system attempted but failed to create or update the Identity Manager user account on one or more resources. (When an account is updated on all assigned resources, no icon appears.)

Working with User Accounts

From the Administrator Interface Accounts area, you can perform a range of actions on these system objects.

- **Users** — View, create, edit, move, rename, deprovision, enable, disable, update, unlock, delete, unassign, unlink, and audit
- **Passwords** — Change and reset
- **Organizations** — Create, edit, refresh, and delete
- **Directory Junctions** — Create

Users

View

To view user account details, select a user in the list, and then select View from the User Actions list.

The View User page displays a subset of the identity, assignments, security, and attributes information selections made when editing or creating the user. The information on the View User page cannot be edited. Click **Cancel** to return to the Accounts list.

Create (New Actions List, New User Selection)

To create a user account, select New User from the New Actions list.

Tip If you want to create a user in an organization other than Top, select an organization folder, and then select New User from the New Actions list.

Selections available in one area may depend on selections you make in another.

The Create User page (also called the *user form*) is a multi-page form that lets you set up the user's:

- **Identity** — Name, email, organization, and password details
- **Assignments** — Account policy, roles, and resources
- **Security** — Organizations and capabilities
- **Attributes** — Specific attributes for assigned resources

Note To better reflect your business processes or specific administrator capabilities, you can configure the user form specifically for your environment, For more information about the user form, see *Identity Manager Workflows, Forms, and Views*.

Click form tabs to navigate the Create User page. You can move among form tabs in any order. When your selections are complete, you have two options for saving a user account:

- **Save** — Saves the user account. If you assign a large number of resources to the account, this process could take some time.
- **Background Save** — This process saves a user account as a background task, which allows you to continue working in Identity Manager. A task status indicator displays on the Accounts page, the Find User Results page, and the Home page, for each save in progress.

Status Indicator	Status
↻	The save process is in progress.
⌛	The save process is suspended. Often, this means that the process is waiting for approval.
✓	The process completed successfully. This does not mean that the user was successfully saved; rather that the process completed with no errors.
?	The process has not yet started.
⚠	The process completed with one or more errors.

Tip By moving your mouse over the user icon that displays within the status indicator, you can see details about the background save process.

Creating Multiple User Accounts (Identities)

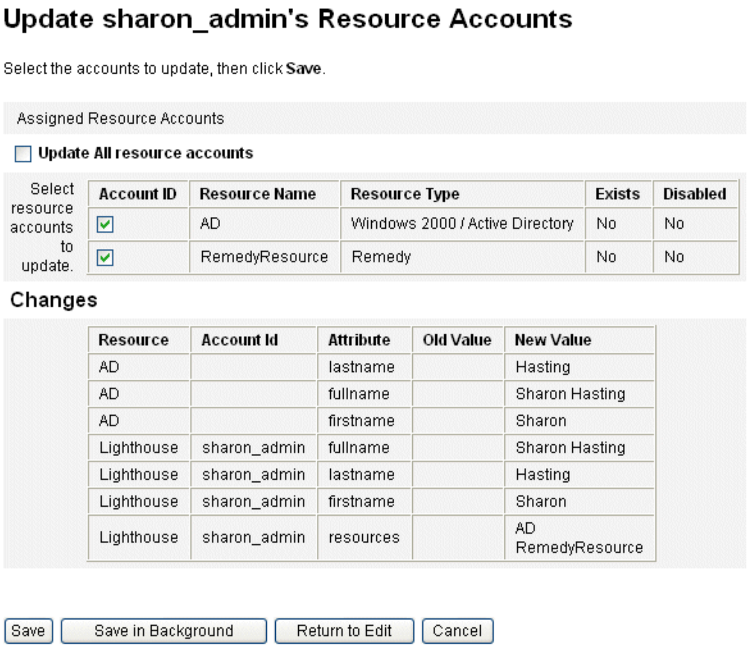
You can create more than one user account on a single resource. When you create (or edit) a user, and then assign the user one or more resources, you can also request and define an additional account on that resource.

Edit

To edit account information, choose one of these actions:

- Click a user account in the accounts list.
- Select a user account in the list, and then select Edit from the User Actions list.

After you make and save changes, Identity Manager displays the Update Resource Accounts page. This page shows resource accounts assigned to the user and the changes that will apply to the account. Select Update All resource accounts to apply changes to all assigned resources; or individually select none, one, or more resource accounts associated with the user to update.



Update sharon_admin's Resource Accounts

Select the accounts to update, then click **Save**.

Assigned Resource Accounts

□ **Update All resource accounts**

Select resource accounts to update.

Account ID	Resource Name	Resource Type	Exists	Disabled
☑	AD	Windows 2000 / Active Directory	No	No
☑	RemedyResource	Remedy	No	No

Changes

Resource	Account Id	Attribute	Old Value	New Value
AD		lastname		Hasting
AD		fullname		Sharon Hasting
AD		firstname		Sharon
Lighthouse	sharon_admin	fullname		Sharon Hasting
Lighthouse	sharon_admin	lastname		Hasting
Lighthouse	sharon_admin	firstname		Sharon
Lighthouse	sharon_admin	resources		AD RemedyResource

Figure 5. Edit User (Update Resource Accounts)

Click **Save** again to complete the edit, or click **Return to Edit** to make further changes.

Move Users (User Actions)

The Change Organization of User task allows you to remove a user from his currently assigned organization and then reassign, or move, the user to a new organization.

To move users to a different organization, select one or more user accounts in the list, and then select Move from the User Actions list.

Rename (User Actions)

Typically, renaming an account on a resource is a complex action. Because of this, Identity Manager provides a separate feature to rename a user’s Identity Manager account or one or more resource accounts that are associated with that user.

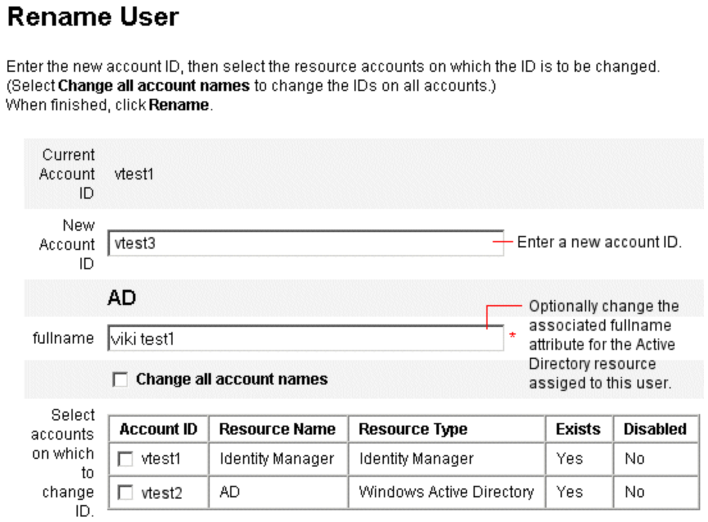
To use the rename feature, select a user account in the list, and then select the Rename option from the User Actions list.

The Rename User page allows you to change the user account name, associated resource account names, and resource account attributes associated with the user's Identity Manager account.

Note Some resource types do not support account renaming.

As shown in the following figure, the user has an assigned Active Directory resource. During the renaming process, you can change:

- Identity Manager user account name
- Active Directory resource account name
- Active Directory resource attribute (fullname)



Rename User

Enter the new account ID, then select the resource accounts on which the ID is to be changed.
(Select **Change all account names** to change the IDs on all accounts.)
When finished, click **Rename**.

Current Account ID	vtest1
New Account ID	vtest3
	AD
fullname	viki test1 *
	□ **Change all account names**

Enter a new account ID.

Optionally change the associated fullname attribute for the Active Directory resource assiged to this user.

Select accounts on which to change ID.

Account ID	Resource Name	Resource Type	Exists	Disabled
□ vtest1	Identity Manager	Identity Manager	Yes	No
□ vtest2	AD	Windows Active Directory	Yes	No

Figure 6. Rename User

Disable Users (User Actions, Organization Actions

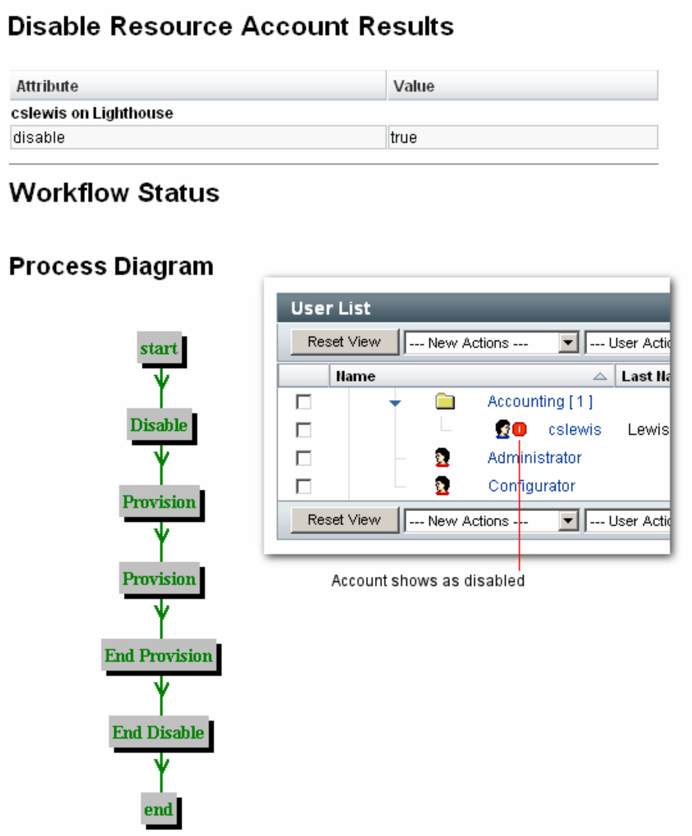
When you disable a user account, you alter that account so that the user can no longer log in to Identity Manager or to his assigned resource accounts.

Note For assigned resources that do not support account disabling, the user account is disabled through assignment of a new, randomly generated password.

Disabling Single User Accounts

To disable a user account, select it in the list, and then select Disable from the User Actions list.

On the displayed Disable page, select the resource accounts to disable, and then click **OK**. Identity Manager displays the results of disabling the Identity Manager user account and all associated resource accounts. The accounts list indicates that the user account is disabled.



Disable Resource Account Results

Attribute	Value
cslewis on Lighthouse	
disable	true

Workflow Status

Process Diagram

Account shows as disabled

Figure 7. Disabled Account

Disabling Multiple User Accounts

You can disable two or more Identity Manager user accounts at the same time. Select more than one user account in the list, and then select Disable from the User Actions list.

Note When you choose to disable multiple user accounts, you cannot select individually assigned resource accounts from each user account. Rather, this process disables all resources on all user accounts you select.

Enable Users (User Actions, Organization Actions)

User account enabling reverses the disabling process. For resources that do not support account enabling, Identity Manager generates a new, random password. Depending on selected notification options, it also displays that password on the administrator’s results page.

The user can then reset his password (through the authentication process), or a user with administrator privileges can reset it.

Enabling Single User Accounts

To enable a user account, select it in the list, and then select Enable from the User Actions list.

On the displayed Enable page, select the resources to enable, and then click **OK**. Identity Manager displays the results of enabling the Identity Manager account and all associated resource accounts.

Enabling Multiple User Accounts

You can enable two or more Identity Manager user accounts at the same time. Select more than one user account in the list, and then select Enable from the User Actions list.

Note When you choose to enable multiple user accounts, you cannot select individually assigned resource accounts from each user account. Rather, this process enables all resources on all user accounts you select.

Update Users (User Actions, Organization Actions)

In an update action, Identity Manager updates the resources that are associated with a user account. Updates performed from the accounts area send any pending changes that were previously made to a user to the resources selected. This situation may occur if:

- A resource was unavailable when updates were made.
- A change was made to a role or resource group that needed to be pushed to all users assigned to that role or resource group. In this case, you should use the Find User page to search for users, and then select one or more users on which to perform the update action.

When you update the user account, you can:

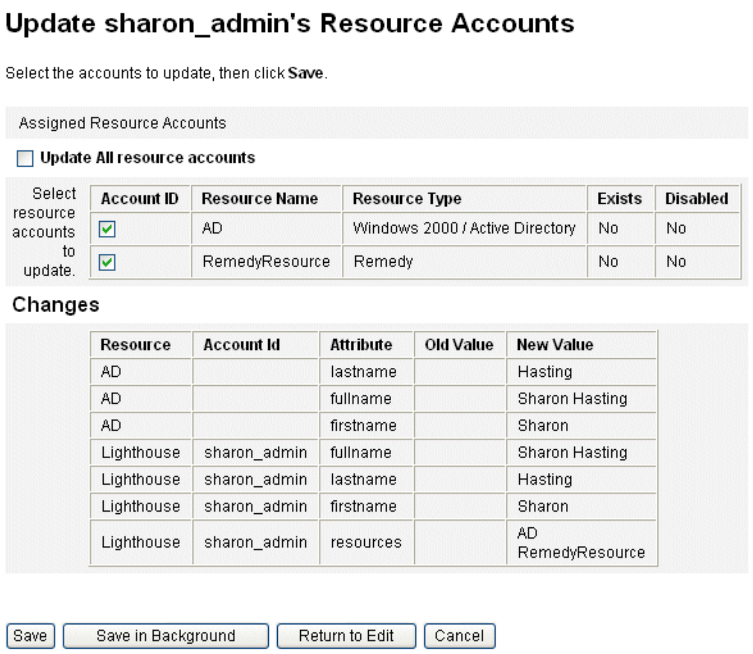
- Choose whether assigned resource accounts will receive the updated information.
- Update all resource accounts, or select individual accounts from a list.

Updating Single User Accounts

To update a user account, select it in the list, and then select Update from the User Actions list.

On the Update Resource Accounts page, select one or more resources to update, or select Update All resource accounts to update all assigned resource accounts. When finished, click **OK** to begin the update process. Alternatively, click **Save in Background** to perform the action as a background process.

A confirmation page confirms the data sent to each resource.



Update sharon_admin's Resource Accounts

Select the accounts to update, then click **Save**.

Assigned Resource Accounts

□ **Update All resource accounts**

Select resource accounts to update.

Account ID	Resource Name	Resource Type	Exists	Disabled
☑	AD	Windows 2000 / Active Directory	No	No
☑	RemedyResource	Remedy	No	No

Changes

Resource	Account Id	Attribute	Old Value	New Value
AD		lastname		Hasting
AD		fullname		Sharon Hasting
AD		firstname		Sharon
Lighthouse	sharon_admin	fullname		Sharon Hasting
Lighthouse	sharon_admin	lastname		Hasting
Lighthouse	sharon_admin	firstname		Sharon
Lighthouse	sharon_admin	resources		AD RemedyResource

Figure 8. Update Resource Accounts

Updating Multiple Accounts

You can update two or more Identity Manager user accounts at the same time. Select more than one user account in the list, and then select Update from the User Actions list.

Note When you choose to update multiple user accounts, you cannot select individually assigned resource accounts from each user account. Rather, this process updates all resources on all user accounts you select.

Unlock Users (User Actions, Organization Actions)

A user can be locked out of one or more resource accounts because his login retry attempts have exceeded the login limits established for that resource. The user's effective Lighthouse account policy establishes the maximum number of failed password or question login attempts that can be made.

When a user is locked because he exceeds the maximum number of failed password login attempts, then he is not allowed to authenticate to any Identity Manager application interface, including the User interface, Administrator interface, Forgot My Password, BPE, SOAP, and console. If he is locked because he exceeds the maximum number of failed question login attempts, then he can authenticate to any Identity Manager application interface except Forgot My Password.

Failed Password Login Attempts

If locked due to failed password login attempts, a user account will remain locked until:

- An administrative user unlocks it. To successfully unlock the account, the administrator must be assigned the Unlock User capability, and must have administrative control of the user's member organization.
- The current date and time is later than the user's lock expiration date and time, if a lock expiration date and time was set. (The Lock Timeout value in the LIghthouse Account Policy sets lock expiration.)

Failed Question Login Attempts

If locked due to exceeding the maximum number of failed question login attempts, a user account will remain locked until:

- An administrative user unlocks it. To successfully unlock the account, the administrator must be assigned the Unlock User capability, and must have administrative control of the user's member organization.
- The locked user, or a user with appropriate capabilities changes or resets the user's password.

An administrator with appropriate capabilities can perform these operations on a user in locked state:

- Update (including resource re-provisioning)
- Change or reset password
- Disable or enable
- Rename
- Unlock

A user in locked state cannot log in to any Identity Manager application, including the Administrator interface, User interface, and BPE. This limitation applies irrespective of whether the user attempts to log in with his Identity Manager user ID and password, by providing his user ID and answers to authentication questions, or by passthrough to one or more resources.

To unlock accounts, select one or more user accounts in the list, and then select Unlock Users from the User Actions or Organization Actions list.

Deletion (User Actions, Organization Actions)

Delete actions include several options that remove Identity Manager user account access from a resource:

- **Delete** — For each resource selected, Identity Manager deletes the associated resource account. The selected resources are also unlinked from the Identity Manager user.
- **Unassign** — For each resource selected, Identity Manager removes the associated resource from the user's list of assigned resources. The selected resources are unlinked from the user. The associated resource account is not deleted.
- **Unlink** — For each resource selected, Identity Manager removes the associated resource account information from the Identity Manager user.

Note If you unlink an account that has been indirectly assigned to the user through a role or resource group, the link may be restored when the user is updated.

To begin a delete action, select a user account, and then select the appropriate deletion action from the User Actions or Organization Actions list.

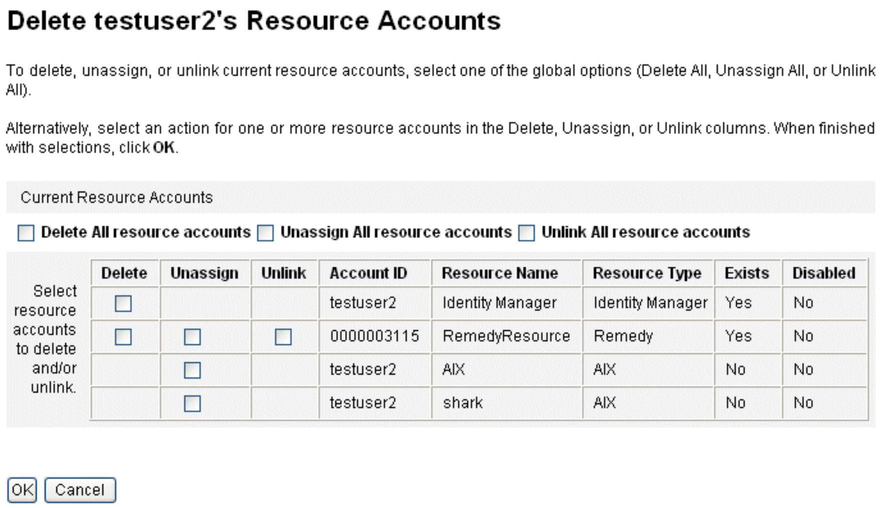
Identity Manager displays the Delete Resource Accounts page.

Deleting the User Account and Resource Accounts

To delete an Identity Manager user account or resource accounts, make selections in the Delete column, and then click **OK**. To delete all resource accounts, select the Delete All resource accounts option, and then click **OK**.

Unassigning or Unlinking Resource Accounts

To unassign or unlink resource accounts from the Identity Manager user account, make individual selections in the Unassign or Unlink columns, and then click **OK**. To unassign all resource accounts, select the Unassign All resource accounts or Unlink All resource accounts option, and then click **OK**.



Delete testuser2's Resource Accounts

To delete, unassign, or unlink current resource accounts, select one of the global options (Delete All, Unassign All, or Unlink All).

Alternatively, select an action for one or more resource accounts in the Delete, Unassign, or Unlink columns. When finished with selections, click **OK**.

Current Resource Accounts

□ **Delete All resource accounts** □ **Unassign All resource accounts** □ **Unlink All resource accounts**

	Delete	Unassign	Unlink	Account ID	Resource Name	Resource Type	Exists	Disabled
Select resource accounts to delete and/or unlink.	□			testuser2	Identity Manager	Identity Manager	Yes	No
	□	□	□	0000003115	RemedyResource	Remedy	Yes	No
		□		testuser2	AIX	AIX	No	No
		□		testuser2	shark	AIX	No	No

Figure 9. Delete User Account and Resource Accounts

Finding Accounts

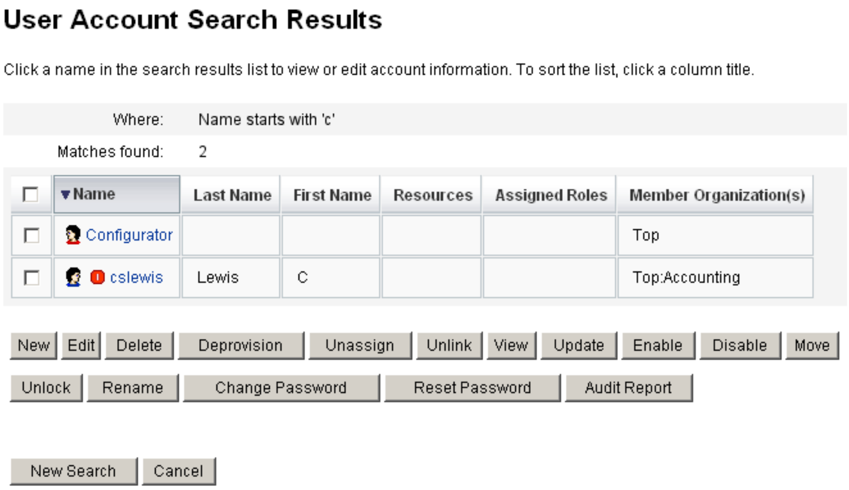
The Identity Manager find feature lets you search for user accounts. After you enter and select search parameters, Identity Manager finds all accounts that match your selections.

To search for accounts, select **Accounts** from the menu bar, and then select **Find Users**. You can search for accounts by one or more of these search types:

- Account detail, such as user name, email address, or last name, or first name. These choices depend on your institution's specific Identity Manager implementation.
- Resource account status, including:
  - **Disabled** — User cannot access any Identity Manager or assigned resource accounts.
  - **Partially Disabled** — User cannot access one or more assigned resource accounts.
  - **Enabled** — User has access to all assigned resource accounts.
- User account status, including:
  - **Locked** — User account is locked because the maximum number of failed password or question login attempts exceeds the maximum allowed.
  - **Not Locked** — User account access is not restricted
- Update status, including:
  - **no** — User accounts that have not been updated on any resource.
  - **some** — User accounts that have been updated on at least one, but not all, assigned resources.
  - **all** — User accounts that have been updated on all assigned resources.
- Assigned resource
- Role
- Organization
- Organizational control
- Capabilities
- Admin role

The search results list shows all accounts that match your search. From the results page, you can:

- Select user accounts to edit. To edit an account, click it in the search results list; or select it in the list, and then click **Edit**.
- Perform actions (such as enable, disable, unlock, delete, update, or change/reset passwords) on one or more accounts. To perform an action, select one or more accounts in the search results list, and then click the appropriate action.
- Create user accounts.



User Account Search Results

Click a name in the search results list to view or edit account information. To sort the list, click a column title.

Where: Name starts with 'c'

Matches found: 2

☐	▾Name	Last Name	First Name	Resources	Assigned Roles	Member Organization(s)
☐	Configurator					Top
☐	cslewis	Lewis	C			Top:Accounting

Figure 10. User Account Search Results

Setting Password Policies

Resource password policies establish the limitations for passwords. You can edit a password policy to set or select values for a range of characteristics.

To begin working with password policies, select **Configure** from the menu bar, and then select **Policies**.

To edit a password policy, select it from the Policies list. To create a password policy, select String Quality Policy from the New list of options.

Creating a Policy

Password policies are the default type for string quality policies. After naming and providing an optional description for the new policy, you will select options and parameters for the rules that define it.

Length Rules

Length rules set the minimum and maximum required character length for a password. Select to enable the rule, and then enter a limit value for the rule.

Character Type Rules

Character type rules establish the minimum and maximum characters of certain types and number that can be included in a password. These include:

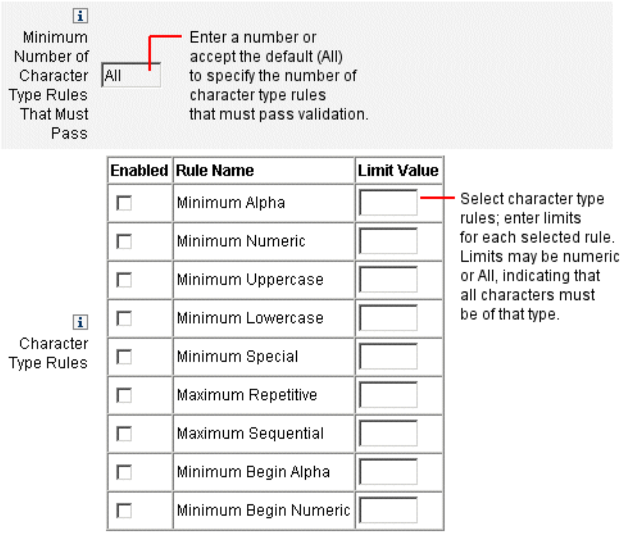
- Minimum and maximum alphabetic, numeric, uppercase, lowercase, and special characters
- Minimum and maximum embedded numeric characters
- Maximum repetitive and sequential characters
- Minimum beginning alphabetic and numeric characters

Enter a numeric limit value for each character type rule; or enter All to indicate that all characters must be of that type.

Minimum Number of Character Type Rules

You also can set the minimum number of character type rules that must pass validation. The minimum number that must pass is 1. The maximum cannot exceed the number of character type rules that you have enabled.

Tip To set the minimum number that must pass to the highest value, enter All.



Minimum Number of Character Type Rules That Must Pass: All

Enter a number or accept the default (All) to specify the number of character type rules that must pass validation.

Character Type Rules

Enabled	Rule Name	Limit Value
□	Minimum Alpha	
□	Minimum Numeric	
□	Minimum Uppercase	
□	Minimum Lowercase	
□	Minimum Special	
□	Maximum Repetitive	
□	Maximum Sequential	
□	Minimum Begin Alpha	
□	Minimum Begin Numeric	

Select character type rules; enter limits for each selected rule. Limits may be numeric or All, indicating that all characters must be of that type.

Figure 11. Password Policy (Character Type) Rules

Dictionary Policy Selection

You can choose to check passwords against words in a dictionary. Before you can use this option, you must:

- Configure the dictionary
- Load dictionary words

You configure the dictionary from the Policies page. For more information about how to set up the dictionary, read the chapter titled Configuring Dictionary Support in *Identity Manager Deployment Tools*.

Password History Policy

You can prohibit re-use of passwords that were used immediately preceding a newly selected password.

In the Number of Previous Passwords that Cannot be Reused field, enter a numeric value greater than one to prohibit re-use of the current and preceding passwords. For example, if you enter a numeric value of 3, the new password cannot be the same as the current password or the two passwords used immediately before it.

You can also prohibit re-use of similar characters from passwords used previously. In the Maximum Number of Similar Characters from Previous Passwords that Cannot be Reused field, enter the number of consecutive characters from the previous password or passwords that cannot be repeated in the new password. For example, if you enter a value of 7, and the previous password was password1, then the new password cannot be password2 or password3.

If you enter a value of 0, then all characters must be different regardless of sequence. For example, if the previous password was abcd, then the new password cannot include the characters a, b, c, or d.

The rule can apply to one or more previous passwords. The number of previous passwords checked is the number specified in the Number of Previous Passwords that Cannot be Reused field.

Must Not Contain Words

You can enter one or more words that the password may not contain. In the entry box, enter one word on each line.

Note You can also exclude words by configuring and implementing the dictionary policy. For more information, read the chapter titled *Configuration*.

Must Not Contain Attributes

Select one or more attributes that the password may not contain. Attributes include:

- accountID
- email
- firstname
- fullname
- lastname

Note You can change the allowed set of “must not contain” attributes for passwords in the `UserUIConfig` configuration object. The password attributes in `UserUIConfig` are listed in `<PolicyPasswordAttributeNames>`.

Implementing Password Policies

Password policies are established for each resource. To put a password policy in place for a specific resource, select it from the Password Policy list of options, which is located in the Policy Configuration area of the Create or Edit Resource Wizard: Identity Manager Parameters pages.

Working with User Account Passwords

All Identity Manager users are assigned a password. When set, the Identity Manager user password is used to synchronize the user's resource account passwords. If one or more resource account passwords cannot be synchronized (for example, to comply with required password policies), you can set them individually.

Changing User Account Passwords

To change a user account password:

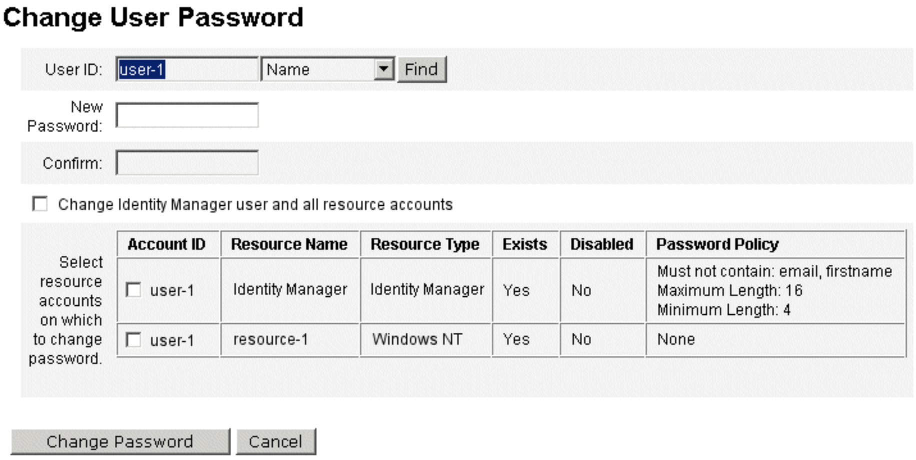
1. From the menu bar, select **Passwords**.

   By default, the Change User Password page appears.

2. Enter or search for the user whose password you want to change. Choose one of these options:

   - Enter the user name, and then click **Change Password**.
   - Type one or more letters of a name in the User ID field, and then click **Find**. Identity Manager returns a list of all users whose IDs contain the entered characters. Click to select a user and return to the Change User Password page.

Enter and confirm new password information, and then click **Change Password** to change the user password on the listed resource accounts. Identity Manager displays a workflow diagram that shows the sequence of actions taken to change the password.



Change User Password

User ID: user-1 Name ▼ Find

New Password:

Confirm:

☐ Change Identity Manager user and all resource accounts

Select resource accounts on which to change password.

Account ID	Resource Name	Resource Type	Exists	Disabled	Password Policy
☐ user-1	Identity Manager	Identity Manager	Yes	No	Must not contain: email, firstname Maximum Length: 16 Minimum Length: 4
☐ user-1	resource-1	Windows NT	Yes	No	None

Figure 12. Change User Password

Resetting User Account Passwords

The process for resetting Identity Manager user account passwords is similar to the change process. The reset process differs from a password change in that you do not specify a new password. Rather, Identity Manager randomly generates a new password (depending on your selections and password policies) for the user account, resource accounts, or a combination of these.

The policy assigned to the user – either by direct assignment or through the user's organization – controls several reset options, including:

- How often a password may be reset before resets are disabled
- Where the new password is displayed or sent. Depending on the Reset Notification Option selected for the role, Identity Manager emails the new password to the user or displays it (on the Results page) to the Identity Manager administrator requesting the reset.

Password Expiration on Reset

By default, when you reset a user password, it is immediately expired. This means that after reset, the first time a user logs in, he must select a new password before gaining access. This default can be overridden in the form, such that the user's password will expire according to the expire password policy set in the Lighthouse Account Policy associated with the user instead.

For example, in the Reset User Password Form, you would set `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword` to a value of `false`.

There are two ways to expire a password via the Reset Option field in the Lighthouse Account Policy:

- **permanent** — The time period specified in the passwordExpiry policy attribute is used to calculate the relative date from the current date when the password is reset, and then set that date on the user. If no value is specified, the changed or reset password never expires.
- **temporary** — The time period specified in the tempPasswordExpiry policy attribute is used to calculate the relative date from the current date when the password is reset, and then set that date on the user. If no value is specified, the changed or reset password never expires. If tempPasswordExpiry is set to a value of 0, then the password is expired immediately.

Note The `tempPasswordExpiry` attribute applies only when passwords are reset (randomly changed); it does not apply to password changes.

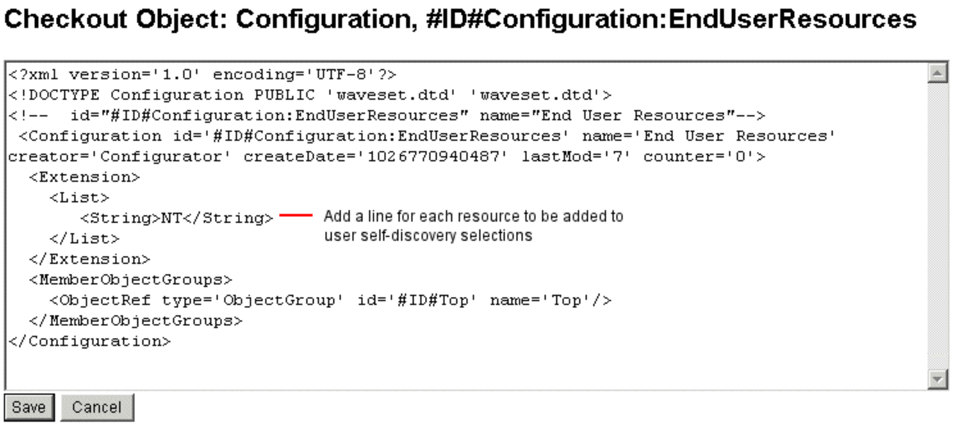
User Self-Discovery

The Identity Manager User Interface allows users to *discover* resource accounts. This means that a user with an Identity Manager identity can associate it with an existing, but unassociated, resource account.

Enabling Self-Discovery

To enable self-discovery, you must edit a special configuration object (End User Resources) and add to it the name of each resource on which the user will be allowed to discover accounts. To do this:

1. Open the Identity Manager System Settings page (`idm/debug`).
2. Select Configuration from the list of Configuration types, and then click **List Objects**.
3. Click **Edit** next to End User Resources to display the configuration object.
4. Add `<String>`***Resource***`</String>`, where ***Resource*** matches the name of a resource object in the repository.



Checkout Object: Configuration, #ID#Configuration:EndUserResources

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<!--  id="#ID#Configuration:EndUserResources" name="End User Resources"-->
 <Configuration id='#ID#Configuration:EndUserResources' name='End User Resources'
creator='Configurator' createDate='1026770940487' lastMod='7' counter='0'>
  <Extension>
    <List>
       <String>NT</String>
    </List>
  </Extension>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Configuration>
```

Add a line for each resource to be added to user self-discovery selections

Figure 13. End User Resources Configuration Object

5. Click **Save**.

When self-discovery is enabled, the user is presented with a new menu item on the Identity Manager User Interface (**Inform Identity Manager of Other Accounts**) This area allows him to select a resource from an available list, and then enter the resource account ID and password to link the account with his Identity Manager identity.

User Authentication

If a user forgets his password or his password is reset, he can answer one or more account authentication questions to gain access to Identity Manager. You establish these questions, and the rules that govern them, as part of an Identity Manager account policy. Unlike password policies, Identity Manager account policies are assigned to the user directly or through the organization assigned to the user (on the Create and Edit User pages).

To set up authentication in an account policy:

1. Select **Configure** from the menu bar, and then select **Policies**.
2. Select Default Lighthouse Account Policy from the list of policies.

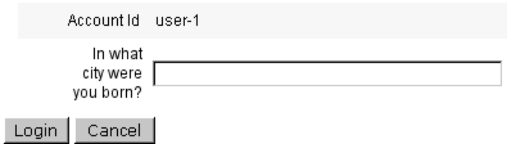
   Authentication selections are offered in the Secondary Authentication Policy Options area of the page.

Important! When first set up, the user should log in to the Identity Manager User Interface and provide initial answers to his authentication questions. If these answers are not set, the user cannot successfully log in without his password.

Depending on the authentication rules set, you can require a user to answer:

- All authentication questions
- Any one of the authentication questions
- Randomly selected questions from the set; the number of questions is determined by a value you specify
- One or more questions selected in sequence from the set

Note You can verify your authentication choices by logging in to the Identity Manager User Interface, clicking **Forgot Your Password?**, and answering the presented question or questions.



Account Id user-1

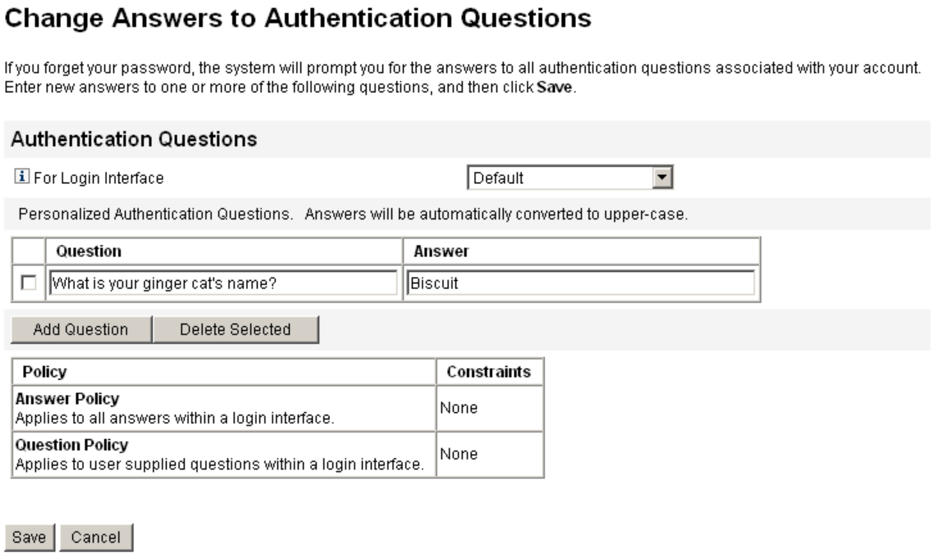
In what city were you born?

Figure 14. User Account Authentication

Personalized Authentication Questions

In the Lighthouse account policy, you can select an option to allow users to supply their own authentication questions in the User and Administrator interfaces. You can additionally set the minimum number of questions that the user must provide and answer to be able to log in successfully by using personalized authentication questions.

Users then can add and change questions from the Change Answers to Authentication Questions page.



Change Answers to Authentication Questions

If you forget your password, the system will prompt you for the answers to all authentication questions associated with your account. Enter new answers to one or more of the following questions, and then click **Save**.

Authentication Questions

For Login Interface: Default

Personalized Authentication Questions. Answers will be automatically converted to upper-case.

	Question	Answer
□	What is your ginger cat's name?	Biscuit

Policy	Constraints
Answer Policy Applies to all answers within a login interface.	None
Question Policy Applies to user supplied questions within a login interface.	None

Figure 15. Change Answers — Personalized Authentication Questions

Bypassing the Change Password Challenge after Authentication

When a user successfully authenticates by answering one or more questions, by default he is challenged by the system to provide a new password. You can configure Identity Manager to bypass the change password challenge, however, by setting the `bypassChangePassword` system configuration property, for one or more Identity Manager applications.

To bypass the change password challenge for all applications following successful authentication, set the `bypassChangePassword` property as follows in the system configuration object:

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='questionLogin'>
          <Object>
            <Attribute name='bypassChangePassword'>
              <Boolean>true</Boolean>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

To disable it for a specific application, set it as follows:

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='user'>
          <Object>
            <Attribute name='questionLogin'>
              <Object>
                <Attribute name='bypassChangePassword'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

Bulk Account Actions

You can perform several *bulk* actions on Identity Manager accounts, which allow you to act on multiple accounts at the same time. Bulk actions you can initiate are:

- **Delete** — Deletes, unassigns, and unlinks any selected resource accounts. Select the Target the Identity Manager Account option to delete each user's Identity Manager account.
- **Delete and Unlink** — Deletes any selected resource accounts and unlinks the accounts from the users.
- **Disable —** Disables any selected resource accounts. Select the Target the Identity Manager Account option to disable each user's Identity Manager account.
- **Enable —** Enables any selected resource accounts. Select the Target the Identity Manager Account option to enable each user's Identity Manager account.
- **Unassign** — Unlinks any selected resource accounts and removes the Identity Manager user account's assignments to those resources. Unassigning does not remove the account from the resource. You cannot unassign an account that has been indirectly assigned to the Identity Manager user through a role or resource group.
- **Unlink** — Removes a resource account's association (link) with the Identity Manager user account. Unlinking does not remove the account from the resource. If you unlink an account that has been indirectly assigned to the Identity Manager user through a role or resource group, the link may be restored when the user is updated.

Bulk actions work best if you have a list of users in a file or application, such as an email client or spreadsheet program. You can copy and paste the list into a field on this interface page, or you can load the list of users from a file.

Many of these actions can be performed on the results of a user search. Search for users on the Find Users page under the **Accounts** tab.

Launching Bulk Account Actions

To launch bulk account actions, select or enter values, and then click **Launch**. Identity Manager launches a background task to perform the bulk actions.

Tip To monitor the status of the bulk actions task, go to the **Tasks** tab, and then click the task link.

Using Action Lists

You can specify a list of bulk actions using comma-separated values (CSV) format. This allows you to provide a mix of different action types in a single action list. In addition, you can specify more complicated creation and update actions.

The CSV format consists of two or more input lines. Each line consists of a list of values separated by commas. The first line contains field names. The remaining lines each correspond to an action to be performed on an Identity Manager user, the user's resource accounts, or both. Each line should contain the same number of values. Empty values will leave the corresponding field value unchanged.

Two fields are required in any bulk action CSV input:

- **user** — Contains the name of the Identity Manager user.
- **command** — Contains the action taken on the Identity Manager user. Valid commands are:
  - **Delete** — Deletes, unassigns, and unlinks resource accounts, the Identity Manager account, or both.
  - **DeleteAndUnlink** — Deletes and unlinks resource accounts.
  - **Disable** — Disables resource accounts, the Identity Manager account, or both.
  - **Enable** — Enables resource accounts, the Identity Manager account, or both.
  - **Unassign** — Unassigns and unlinks resource accounts.
  - **Unlink** — Unlinks resource accounts.
  - **Create** — Creates the Identity Manager account. Optionally creates resource accounts.
  - **Update** — Updates the Identity Manager account. Optionally creates, updates, or deletes resource accounts.
  - **CreateOrUpdate** — Performs a create action if the Identity Manager account does not already exist. Otherwise, it performs an update action.

Delete, DeleteAndUnlink, Disable, Enable, Unassign, and Unlink Commands

If you are performing Delete, DeleteAndUnlink, Disable, Enable, Unassign, or Unlink actions, then the only additional field you need to specify is resources. Use the resources field to specify which accounts on which resources will be affected. It can have the following values:

- **all** — Process all resource accounts including the Identity Manager account.
- **resonly** — Process all of the resource accounts excluding the Identity Manager account.
- *resource_name* [**|** *resource_name ...*] — Process the specified resource accounts. Specify Identity Manager to process the Identity Manager account.

Following is an example of the CSV format for several of these actions:

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create, Update, and CreateOrUpdate Commands

If you are performing Create, Update, or CreateOrUpdate commands, then you can specify fields from the User View in addition to the user and command fields. The field names used are the path expressions for the attributes in the views. See *Identity Manager Workflows, Forms, and Views* for information on the attributes that are available in the User View. If you are using a customized User Form, then the field names in the form contain some of the path expressions that you can use.

Some of the more common path expressions used in bulk actions are:

- **waveset.roles** — A list of one or more role names to assign to the Identity Manager account.
- **waveset.resources** — A list of one or more resource names to assign to the Identity Manager account.
- **waveset.applications** — A list of one or more role names to assign to the Identity Manager account.
- **waveset.organization** — The organization name in which to place the Identity Manager account.
- **accounts**[*resource_name*].*attribute_name* — A resource account attribute. The names of the attributes are listed in the schema for the resource.

Example

Following is an example of the CSV format for create and update actions:

```
command,user,waveset.resources,password.password,password.confi
rmPassword,accounts[Windows Active
Directory].description,accounts[Corporate Directory].location
Create,John Doe,Windows Active Directory|Solaris
Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New
York
CreateOrUpdate,Bill Jones,,,,,California
```

Fields with More Than One Value

Some fields can have multiple values. These are known as multi-valued fields. For example, the `waveset.resources` field can be used to assign multiple resources to a user. You can use the vertical bar (|) character (also known as the “pipe” character), to separate multiple values in a field. The syntax for multiple values can be specified like this:

```
value0 | value1 [ | value2 ... ]
```

When updating multi-valued fields on existing users, replacing the current field's values with one or more new values may not be what you want. You may want to remove some values or add to the current values. You can use field directives to specify how to treat the existing field's values. Field directives go in front of the field value and are surrounded by the vertical bar character:

```
|directive [ ; directive ] | field values
```

You can choose from the following directives:

- **Replace** — Replace the current values with the specified values. This is the default if no directive (or just the List directive) is specified.
- **Merge** — Add the specified values to the current values. Duplicate values are filtered.
- **Remove** — Remove the specified values from the current values.
- **List** — Force the field's value to be handled as if it had multiple values, even if it only has a single value. This directive is not usually needed as most fields are handled appropriately regardless of the number of values. This is the only directive that can be specified with another directive.

Note Field values are case-sensitive. This is important when specifying the Merge and Remove directives. The values must match exactly to correctly remove values or avoid having multiple similar values when merging.

Special Characters in Field Values

If you have a field value with a comma (,) or double quote (“) character, or you want to preserve leading or trailing spaces, you must embed your field value within a pair of double quotes (“field_value”). You then need to replace double quotes in the field value with two double quote (") characters. For example, "John ""Johnny"" Smith" results in a field value of John "Johnny" Smith.

If you have a field value with a vertical bar (|) or backslash (\) character in it, you must precede it with a backslash (\| or \\).

Bulk Action View Attributes

When the Create, Update, or CreateOrUpdate actions are performed, there are additional attributes in the User View that are only used or available during bulk action processing. These attributes can be referenced in the User Form to allow behavior specific to bulk actions. The attributes are as follows:

- **waveset.bulk.fields.***field_name* — These attributes contain the values for the fields that were read in from the CSV input, where *field_name* is the name of the field. For example, the command and user fields are in the attributes with path expressions `waveset.bulk.fields.command` and `waveset.bulk.fields.user`, respectively.
- **waveset.bulk.fieldDirectives.***field_name* — These attributes are only defined for those fields for which a directive was specified. The value is the directive string.
- **waveset.bulk.abort** — Set this Boolean attribute to true to abort the current action.
- **waveset.bulk.abortMessage** — Set this to a message string to display when waveset.bulk.abort is set to true. If this attribute is not set, a generic abort message is displayed.

Correlation and Confirmation Rules

Use correlation and confirmation rules when you do not have the Identity Manager user name available to put in the user field of your actions. If you do not specify a value for the user field, then you must specify a correlation rule when launching the bulk action. If you do specify a value for the user field, then the correlation and confirmation rules will not be evaluated for that action.

A correlation rule looks for Identity Manager users that match the action fields. A confirmation rule tests an Identity Manager user against the action fields to determine whether the user is a match. This two-stage approach allows Identity Manager to optimize correlation by quickly finding possible users (based on name or attributes), and by performing expensive checks only on the possible users.

Create a correlation or confirmation rule by creating a rule object with a subtype of `SUBTYPE_ACCOUNT_CORRELATION_RULE` or `SUBTYPE_ACCOUNT_CONFIRMATION_RULE`, respectively.

Correlation Rules

Input for any correlation rule is a map of the action fields. Output must be one of:

- String (containing user name or ID)
- List of String elements (each a user name or ID)
- List of WSAttribute elements
- List of AttributeCondition elements

A typical correlation rule generates a list of user names based on values of the fields in the action. A correlation rule may also generate a list of attribute conditions (referring to queryable attributes of `Type.USER`) that will be used to select users.

A correlation rule should be relatively inexpensive but as selective as possible. If possible, defer expensive processing to a confirmation rule.

Attribute conditions must refer to queryable attributes of `Type.USER`. These are configured as QueryableAttrNames in the Identity Manager UserUIConfig object.

Correlating on an extended attribute requires special configuration:

- The extended attribute must be specified as queryable in UserUIConfig (added to the list of QueryableAttrNames).
- The Identity Manager application (or the application server) may need to be restarted for the UserUIConfig change to take effect.

Confirmation Rules

Inputs to any confirmation rule are:

- userview — Full view of an Identity Manager user.
- account — Map of action fields.

A confirmation rule returns a string-form Boolean value of true if the user matches the action fields; otherwise, it returns a value of false.

A typical confirmation rule compares internal values from the user view to the values of the action fields. As an optional second stage in correlation processing, the confirmation rule performs checks that cannot be expressed in a correlation rule (or that are too expensive to evaluate in a correlation rule). In general, you need a confirmation rule only when the:

- Correlation rule may return more than one matching user
- User values that must be compared are not queryable

A confirmation rule is run once for each matching user returned by the correlation rule.

4 Administration

This chapter provides information and procedures for performing a range of administrative-level tasks in the Identity Manager system, such as:

- Creating Identity Manager administrators, and delegated administration
- Defining organizations and virtual organizations
- Creating and managing administrators

Understanding Identity Manager Administration

Identity Manager administrators are users with extended Identity Manager privileges. You establish Identity Manager administrators to manage:

- User accounts
- System objects, such as roles and resources
- Organizations

Identity Manager differentiates administrators from users through the assignment of:

- **Extended capabilities**. Administrators apply extended capabilities to accounts, roles, and resources in each managed organization.
- **Controlled organizations**. Once assigned to control an organization, the administrator can manage objects in that organization and in any organizations below that organization in the hierarchy.

Delegated Administration

In most companies, employees with administrative tasks to perform hold specific and varied responsibilities. In many cases, an administrator needs to perform account management tasks that are “transparent” to other users or administrators, or that are limited in scope.

For example, an administrator might be responsible only for creating Identity Manager user accounts. With that limited scope of responsibility, the administrator likely does not need specific information about the resources on which he creates user accounts; or about the roles or organizations that exist within the system.

Identity Manager supports separation of responsibility and this delegated administration model by allowing administrators to “see” and manage only those objects within a specific, defined scope.

Identity Manager implements the ability to delegate individual system activities to administrators by:

- Providing limited control over specific organizations and objects within those organizations
- Filtering administrator views of Identity Manager user create and edit pages
- Giving administrators specific job duties in the form of capabilities

Understanding Identity Manager Organizations

Organizations allow you to:

- Logically and securely manage user accounts and administrators
- Limit access to resources, applications, roles, and other Identity Manager objects

By creating organizations and assigning users to various locations in an organizational hierarchy, you set the stage for delegated administration. Organizations that contain one or more other organizations are called *parent organizations*.

All Identity Manager users (including administrators) are *statically assigned* to one organization. Users also can be *dynamically assigned* to additional organizations.

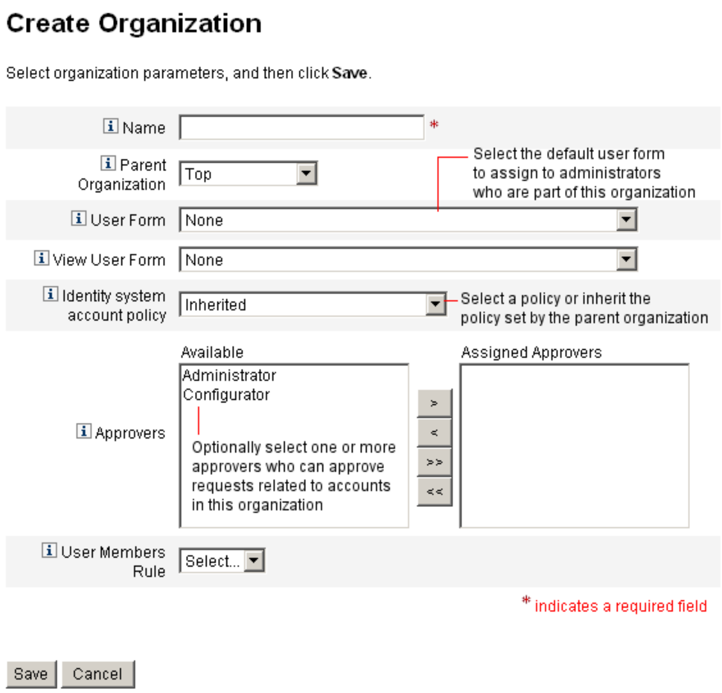
Identity Manager administrators are additionally assigned to *control* organizations.

Creating Organizations

Create organizations in the Identity Manager Accounts area. To create an organization:

1. From the menu bar, select **Accounts**.
2. Select New Organization from the New Actions list on the Accounts page.

Tip To create an organization at a specific location in the organizational hierarchy, select an organization in the list, and then select New Organization from the New Actions list.



Create Organization

Select organization parameters, and then click **Save**.

Name	*
Parent Organization	Top
User Form	None
View User Form	None
Identity system account policy	Inherited
Approvers	Available: Administrator Configurator Assigned Approvers:
User Members Rule	Select...

Select the default user form to assign to administrators who are part of this organization

Select a policy or inherit the policy set by the parent organization

Optionally select one or more approvers who can approve requests related to accounts in this organization

* indicates a required field

Figure 1. Create Organization

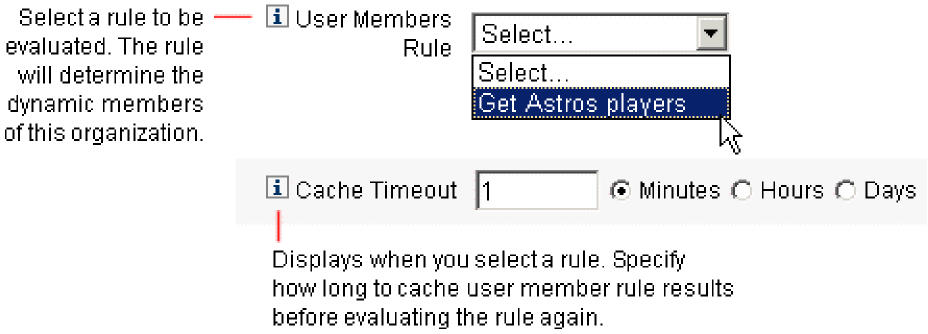
Assigning Users to Organizations

Each user is a static member of one organization, and can be a dynamic member of more than one organization. Organizational membership is determined by:

- **Direct (static) assignment** — Assign users directly to an organization from the Create or Edit User page. (Select the **Identity** form tab to display the Organizations field.) A user must be directly assigned to one organization.
- **Rule-driven (dynamic) assignment** — Dynamically assign users to an organization by assigning a rule to the organization that, when evaluated, returns a set of member users. Identity Manager will evaluate the user member rule when:
  - Listing the users in an organization
  - Finding users (through the Find Users page) that includes searching for users that are in an organization with a user member rule

- Requesting access to a user, and the current administrator controls an organization with a user member rule

Select a user members rule from the User Members Rule field on the Create Organization page.



Select a rule to be evaluated. The rule will determine the dynamic members of this organization.

User Members Rule: Select...
- Select...
- Get Astros players

Cache Timeout: 1 ● Minutes ○ Hours ○ Days

Displays when you select a rule. Specify how long to cache user member rule results before evaluating the rule again.

Figure 2. Create Organization: User Members Rule Selections

The following sample shows how you might set up a user members rule that can dynamically control an organization's user membership.

Note For information about creating and working with rules in Identity Manager, see *Identity Manager Deployment Tools*.

Key Definitions and Inclusions

- For a rule to appear in the User Member Rule option box, its authType must be set as `authType='UserMembersRule'`.
  - The context is the currently authenticated Identity Manager user's session.
  - The defined variable (`defvar`) 'Astros players' gets the dn for each user that is a member of the Windows Active Directory ou 'Houston Astros'.
  - For each user found, the append logic will concatenate the dn of each member user of the 'Houston Astros' ou with the name of the Identity Manager Resource prefixed by a colon (as in ":dogbreath-AD").
  - The results returned will be a list of dn's concatenated with the Identity Manager resource name in the format "<dn>:dogbreath-AD".

Sample User Members Rule

```
<Rule name='Get Astros players'
         authType='UserMembersRule'>
   <defvar name='Astros players'>
      <block>
   <defvar name='player names'>
      <list/>
   </defvar>
   <dolist name='users'>
      <invoke class='com.waveset.ui.FormUtil'
            name='getResourceObjects'>
      <ref>context</ref>
      <s>User</s>
      <s>dogfish-AD</s>
      <map>
         <s>searchContext</s>
         <s>OU=Houston Astros,DC=dev-ad,DC=waveset,DC=com</s>
         <s>searchScope</s>
         <s>subtree</s>
         <s>searchAttrsToGet</s>
         <list>
            <s>distinguishedName</s>
         </list>
      </map>
      </invoke>
      <append name='player names'>
      <concat>
         <get>
            <ref>users</ref>
            <s>distinguishedName</s>
         </get>
            <s>:dogbreath-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Astros players</ref>
</Rule>
```

Assigning Organization Control

Assign administrative control of one or more organizations from the Create or Edit User page. Select the **Security** form tab to display the Controlled Organizations field.

You can also assign administrative control of organizations by assigning one or more admin roles, from the Admin Roles field.

Understanding Directory Junctions and Virtual Organizations

A *directory junction* is a hierarchically related set of organizations that mirrors a directory resource's actual set of hierarchical containers. A *directory resource* is one that employs a hierarchical namespace through the use of hierarchical containers. Examples of directory resources include LDAP servers and Windows Active Directory resources.

Each organization in a directory junction is a *virtual organization*. The top-most virtual organization in a directory junction is a mirror of the container representing the base context defined in the resource. The remaining virtual organizations in a directory junction are *direct* or *indirect* children of the top virtual organization, and also mirror one of the directory resource containers that are children of the defined resource's base context container.

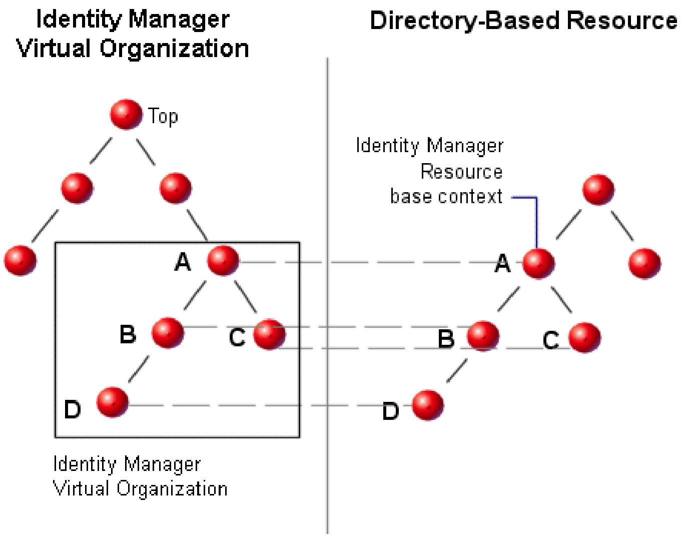

Identity Manager Virtual Organization
Directory-Based Resource
Top
Identity Manager Resource base context
A
B
C
D
A
B
C
D
Identity Manager Virtual Organization

Figure 3. Identity Manager Virtual Organization

Directory junctions can be spliced into the existing Identity Manager organizational structure at any point. However, directory junctions cannot be spliced within or below an existing directory junction.

Once you have added a directory junction to the Identity Manager organizational tree, you can create or delete virtual organizations in the context of that directory junction. In addition, you can refresh the set of virtual organizations comprising a directory junction at any time to ensure they stay synchronized with the directory resource containers. You cannot create a non-virtual organization within a directory junction.

You can make Identity Manager objects (such as users, resource, and roles) members of, and available to, a virtual organization in the same way as an Identity Manager organization.

Setting Up Directory Junctions

You set up directory junctions from the Identity Manager Accounts area:

1. From the Identity Manager menu bar, select **Accounts**.
2. Select an Identity Manager organization in the Accounts list, and then select New Directory Junction from the New Actions list.

   The organization you select will be the parent organization of the virtual organization you set up.

   Identity Manager displays the Create Directory Junction page.
3. Make selections to set up the virtual organization:
   - **Parent organization** — This field contains the organization you selected from the Accounts list; you can, however, select a different parent organization from the list.
   - **Directory resource** — Select the directory resource that manages the existing directory whose structure you want to mirror in the virtual organization.
   - **User form** — Select a user form that will apply to administrators in this organization.
   - **Identity Manager account policy** — Select a policy, or select the default option (inherited) to inherit the policy from the parent organization.
   - **Approvers** — Select administrators who can approve requests related to this organization.

Refreshing Virtual Organizations

This process refreshes and re-synchronizes the virtual organization with the associated directory resource, from the selected organization down. Select the virtual organization in the list, and then select Refresh Organization from the Organization Actions list.

Deleting Virtual Organizations

When deleting virtual organizations, you can select from two delete options:

- Delete the Identity Manager organization only — Deletes the Identity Manager directory junction only.
- Delete the Identity Manager organization and the resource container — Deletes the Identity Manager directory junction and the corresponding organization on the native resource.

Select an option, and then click **Delete**.

Creating Administrators

You “create” an Identity Manager administrator by extending the capabilities of a Identity Manager user. When creating or editing a user, you can give him administrative control by:

- Designating organizations that he can manage
- Assigning capabilities within the organizations he manages
- Selecting the form he will use when creating and editing Identity Manager users (if capabilities are assigned that allow him to perform those actions)
- Selecting an approver to receive pending approval requests (if capabilities are assigned that allow him to approve requests)

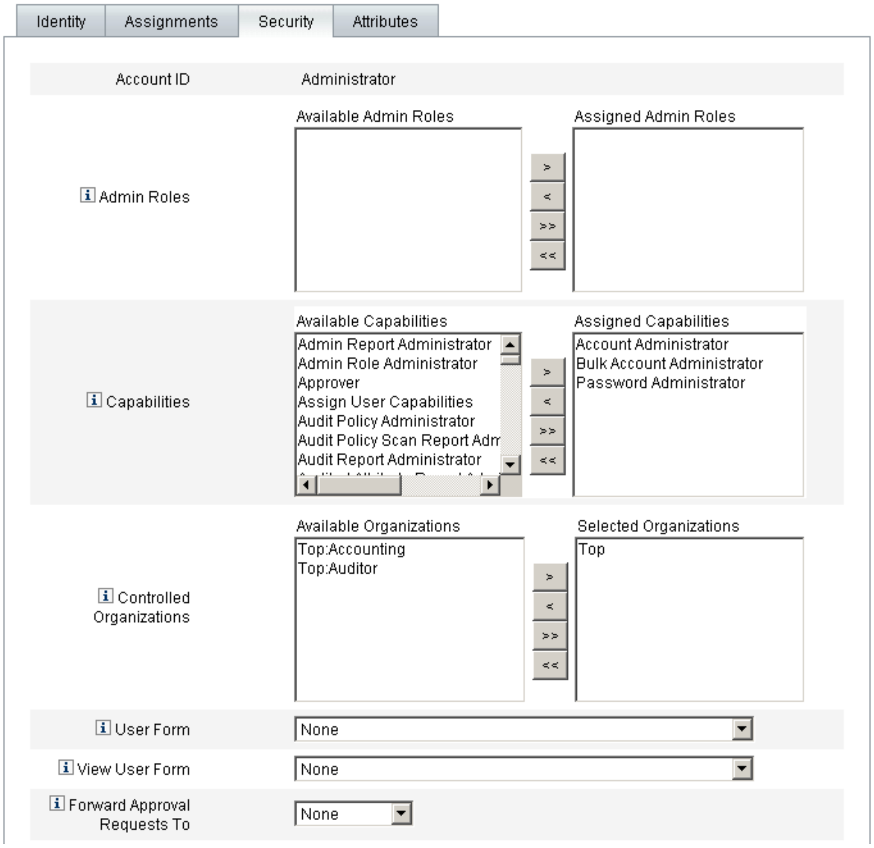
To give a user administrative privileges, select **Accounts** to go to the Identity Manager Accounts area, and then select the **Security** form tab.

Make one or more selections to establish administrative control:

- **Controlled Organizations** — Select one or more organizations. The administrator can control objects in the selected organization and in any organizations beneath it in the hierarchy. The scope of his control is further defined by his assigned capabilities. You must make a selection in this area.

- **Capabilities** — Select one or more capabilities this administrator will have within the organizations he controls. For more information and descriptions of Identity Manager capabilities, read Chapter 5, *Configuration*.
- **User Form** — Select the user form that this administrator will use when creating and editing Identity Manager users (if that capability is assigned). If you do not directly assign a user form, the administrator will inherit the user form assigned to the organization he belongs to. The form selected here supersedes any form selected within this administrator's organization.
- **Forward Approval Requests To** — Select a user to forward all pending approval requests to. This administrator setting also can be set from the Approvals page.

Create Administrator



Account ID: Administrator

Admin Roles
Available Admin Roles:
Assigned Admin Roles:

Capabilities
Available Capabilities:
Admin Report Administrator
Admin Role Administrator
Approver
Assign User Capabilities
Audit Policy Administrator
Audit Policy Scan Report Adm
Audit Report Administrator

Assigned Capabilities:
Account Administrator
Bulk Account Administrator
Password Administrator

Controlled Organizations
Available Organizations:
Top:Accounting
Top:Auditor

Selected Organizations:
Top

User Form: None

View User Form: None

Forward Approval Requests To: None

Figure 4. Create Administrator

Filtering Administrator Views

By assigning user forms to organizations and administrators, you establish specific administrator views of user information. Access to user information is set at two levels:

- **Organization** — When you create an organization, you assign the user form that all administrators in that organization will use when creating and editing Identity Manager users. Any form set at the administrator level overrides the form set here. If no form is selected for the administrator or the organization, Identity Manager inherits the form selected for the parent organization. If no form is set there, Identity Manager uses the default form set in the system configuration.
- **Administrator** — When you assign a user administrative capabilities, you can directly assign a user form to the administrator. If you do not assign a form, the administrator inherits the form assigned to his organization (or the default form set in the system configuration if no form is set for the organization).

Note Chapter 5, *Configuration*, describes built-in Identity Manager capabilities that you can assign.

Changing Administrator Passwords

Administrator passwords may be changed by an administrator with administrative password change capabilities assigned, or by the administrator-owner.

Administrators can change another administrator’s password through:

- **Accounts area —** Select an administrator from the list, and then select Change Password from the User Actions list.
- **Edit User page —** Select the **Identity** form tab, and then enter and confirm a new password.
- **Passwords area —** Enter an administrator name, and then click **Change Password**.

Tip Enter one or more characters, and then click **Find** to list all matches.

An administrator can change his own password from the Passwords area. Select **Passwords**, and then select **Change My Password** to access self-service password fields.

Note The Identity Manager account policy applied to the account determines password limitations, such as password expiration, reset options, and notification selections. Additional password limitations may be set by password policies set on the administrator’s resources.

Challenging Administrator Actions

You can set an option to require that an administrator be challenged for his Identity Manager login password before processing certain account changes. If the password fails, then the account action does not succeed.

Identity Manager pages that support this option are:

- Edit User (account/modify.jsp)
- Change User Password (admin/changeUserPassword.jsp)
- Reset User Password (admin/resetUserPassword.jsp)

Set this option in the account/modify.jsp page as follows:

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"email, fullname, password");
```

where the value of the option is a comma-delimited list of one or more of these user view attribute names:

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname
- organization
- password
- resources
- roles

Set this option in the admin/changeUserPassword.jsp and admin/resetUserPassword pages as follows:

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"true");
```

where the value of the option can be `true` or `false`.

Changing Answers to Authentication Questions

Use the Passwords area to change the answers you have set for account authentication questions. From the menu bar, select **Passwords**, and then select **Change My Answers**.

For more information about authentication, see *User Authentication*.

Customizing Administrator Name Display in the Administrator Interface

You can display an Identity Manager administrator by attribute (such as email or fullname) rather than accountId in some Identity Manager Administrator interface pages and areas. These include:

- Edit User (forward approvals selection list)
- Role table
- Create/Edit Role
- Create/Edit Resource
- Create/Edit Organization/Directory Junction
- Approvals

To configure Identity Manager to use a display name, add to the UserUIConfig object:

```
<AdminDisplayAttribute>
  <String>"attribute_name"</String>
</AdminDisplayAttribute>
```

For example, to use the email attribute as the display name, add to UserUIconfig:

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

Approvals

When a user is added to the Identity Manager system, administrators who are assigned as *approvers* for new accounts must validate account creation. Identity Manager supports three categories of approvals, applied to these Identity Manager objects:

- **Organization** — Approval is needed for the user account to be added to the organization.
- **Role** — Approval is needed for the user account to be assigned to a role.
- **Resource** — Approval is needed for the user account to be given access to a resource.

Note You can configure Identity Manager for digitally signed approvals. For information about this feature, refer to *Signed Approvals* in the chapter titled *Configuration*.

Setting Up Approvers

Setting up approvers for each of these categories is optional, but recommended. At least one approval for each category in which approvers are set up is required for account creation. If one approver rejects a request for approval, the account is not created.

You can assign more than one approver to each category. Because only one approval within a category is needed, you can set up multiple approvers to help ensure workflow is not delayed or halted. If one approver is unavailable, others are available to handle requests. Approval applies only to account creation. By default, account updates and deletions do not require approval; however, you can customize this process to require it.

Identity Manager illustrates the approval process and the status of an account creation request as a workflow diagram. You can customize the workflow by using the Business Process Editor (BPE) to change the flow of approvals, capture account deletions, and capture updates.

For more information about the BPE, workflows, and an illustrated example of altering the approval workflow, see *Identity Manager Workflows, Forms, and Views.*

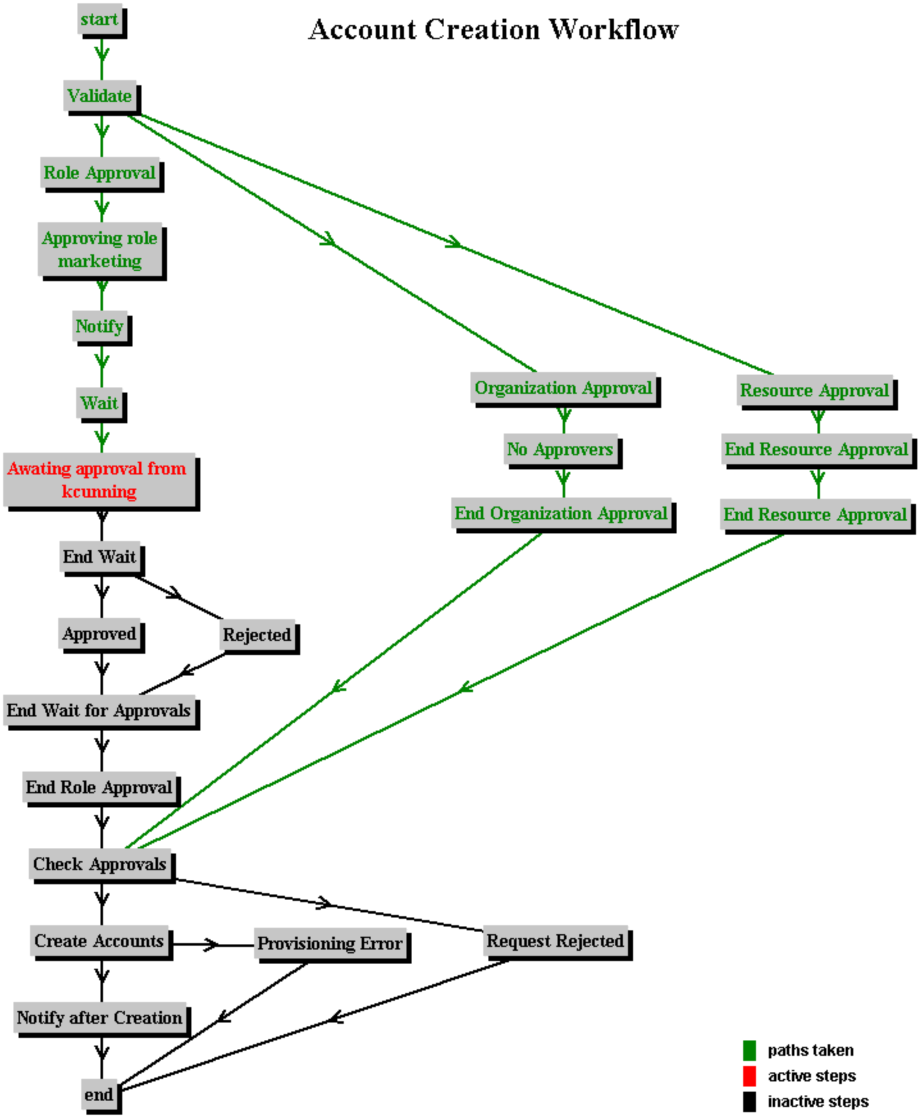


Figure 5. Account Creation Workflow

5 Configuration

This chapter provides information and procedures for using the Administrator Interface to set up Identity Manager objects.

In this chapter, you can learn more about:

- Creating and editing Identity Manager objects, such as:
  - Roles
  - Resources
  - ChangeLogs
  - Policies
  - Capabilities
  - Admin roles
  - Email templates
  - Servers
- Setting up audit configuration groups (audit events)
- Integrating Identity Manager with a Remedy server
- Configuring digitally signed approvals

Understanding Roles

Read this section for information about setting up roles in Identity Manager.

What are Roles?

Identity Manager roles define the collection of resources on which accounts are managed. Roles allow you to profile a class of users, grouping Identity Manager users with similar characteristics.

You can assign each user to one or more roles, or to none. All users assigned to a role share access to the same base group of resources.

All resources associated with a role are *indirectly* assigned to the user. Indirect assignment differs from *direct* assignment, in which resources are specifically selected for the user.

When you create or edit a role, Identity Manager launches the `ManageRole` workflow. This workflow saves the new or updated role in the repository, and allows you to insert approvals or other actions before the role is created or saved.

You assign roles to users through the Administrator Interface Create and Edit User pages.

Creating Roles

To create a role:

1. From the menu bar, select **Roles**.
2. From the Roles list page, click **New**.

The Create Role page allows you to:

- Assign resources and resource groups to the role.
- Select role approvers and make notification selections.

Tip To learn more about the approval process, refer to *Approvals* in the chapter titled *Administration*.

- Exclude roles. This means that if this role is assigned to a user, the excluded role or roles may not also be assigned.
- Select the organizations to which this role will be available for assignment.
- Edit attribute values for resources assigned to the role.

Editing Assigned Resource Attribute Values

Click **Set Attribute Values** from the Assigned Resources area on the Create Role page to display a list of attributes for each resource assigned to the role. From this Edit attributes page, you can specify new values for each attribute and determine how attribute values are set. Identity Manager enables you to directly set values or use a rule to set values; it also provides a range of options for overriding or merging with existing values.

Editing Roles

To make changes to a role:

1. From the menu bar, select **Roles**.
2. From the Roles list page, click a role in the list.

Finding Roles

Use the Find Roles area to search for roles. The search feature returns a list of roles that match your search criteria.

You can search for roles by one or more of these search types:

- Name
- Availability
- Approver
- Resource
- Resource group

Notes:

- If you select more than one search type, the search must meet all specified criteria to successfully return results.
- Search is not case-sensitive.

To search for roles, select **Roles**, and then select **Find Roles**.

Cloning Roles

You can use the selections from an existing role to create a new role. To do this:

1. Select a role to edit.
2. Enter a new name in the Name field, and then click **Save**.

   Identity Manager displays the Create or Rename page.
3. Click **Create** to create the new role.

Renaming Roles

To rename a role:

1. Select a role to edit.
2. Enter a new name in the Name field, and then click **Save**.

   Identity Manager displays the Create or Rename page.
3. Click **Rename** to change the role name.

Synchronizing Identity Manager Roles and Resource Roles

You can synchronize Identity Manager roles with roles created natively on a resource. When synchronized, the resource is assigned, by default, to the role. This applies to roles that are created with the task, as well as existing Identity Manager roles that match one of the resource role names.

From the menu bar, select **Tasks**, and then select **Run Tasks** to access the Synchronize Identity Manager Roles with Resource Roles task page.

Understanding Resources

Read this section for information and procedures to help you set up Identity Manager resources.

What are Resources?

Identity Manager resources store information about how to connect to a resource or system on which accounts are created. Identity Manager resources define the relevant attributes about a resource and help specify how resource information is displayed in Identity Manager.

Identity Manager provides resources for a wide range of resource types, including:

- Mainframe security managers
- Databases
- Directory services
- Operating systems
- Enterprise Resource Planning (ERP) systems
- Messaging platforms

Resources Area

Identity Manager displays information about existing resources on the Resources page.

To access resources, select **Resources** on the menu bar.

Resources are grouped by type, represented in the list by named folders. To expand the hierarchical view and see currently defined resources, click the indicator next to the folder. Collapse the view by clicking the indicator again.

When you expand a resource type folder, it dynamically updates and displays the number of resource objects it contains (if it is a resource type that supports groups).

Some resources have additional objects you can manage, including:

- Organizations
- Organizational units
- Groups
- Roles

Select an object from the resources list, and then make selections from one of these options lists to initiate a management task:

- **Resource Actions** — Perform a range of actions on resources, including edit, active synchronization, rename, and delete; as well as work with resource objects and manage resource connection.
- **Resource Object Actions** — Edit, create, delete, rename, save as, and find resource objects.
- **Resource Type Actions** — Edit resource policies, work with the account index, and configure managed resources.

When you create or edit a resource, Identity Manager launches the `ManageResource` workflow. This workflow saves the new or updated resource in the repository, and allows you to insert approvals or other actions before the resource is created or saved.

Managing the Resources List

The list from which you can select resources to create is managed from the Configure area of the Administrator Interface. Select Configure Managed Resources from the Resource Type Actions options list to choose the resources that will populate the resources list.

On the Managed Resources page, Identity Manager divides resources into two categories:

- **Identity Manager resources** — Resources included in this table are those most commonly managed by Identity Manager. The table shows the resource type and version. Choose one or more resources by selecting the option in the Managed? column, and then click **Save** to add them to the resources list.
- **Custom resources** — Use this page area to add custom resources to the Resources list.

To add a custom resource:

1. Click **Add Custom Resource** to add a row to the table.
2. Enter the resource class path for the resource, or enter your custom-developed resource.
3. Click **Save** to add the resource to the Resources list.

The following table lists custom resource classes.

Custom Resource	Resource Class
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory ActiveSync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustManagerResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter

NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter
PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

Creating Resources

You create resources by using the *Resource Wizard*. The Resource Wizard guides you through the process of creating an Identity Manager resource adapter to manage objects on a resource.

Using the Resource Wizard, you will set up:

- **Resource-specific parameters** — You can modify these values from the Identity Manager interface when creating a specific instance of this resource type.
- **Account attributes** — Defined in the schema map for the resource. These determine how Identity Manager user attributes map to attributes on the resource.
- **Account DN or identity template** — Includes account name syntax for users, which is especially important for hierarchical namespaces.
- **Identity Manager parameters for the resource** — Sets up policies, establishes resource approvers, and sets up organization access to the resource.

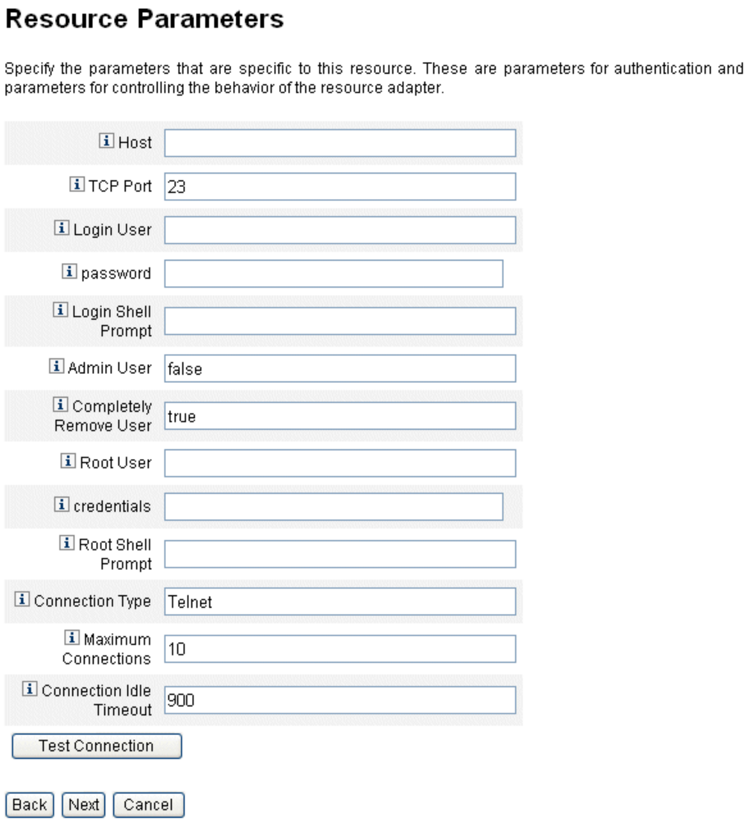
To create a resource:

1. Select New Resource from the Resource Type Actions list of options.

   Identity Manager displays the New Resource page.
2. Select the resource type, and then click **New** to display the Resource Wizard Welcome page.

Note Alternatively, you can select a resource type in the resources list before selecting New Resource from the Resource Type Actions list. In this case, Identity Manager does not display the New Resource page, but immediately launches the Resource Wizard.

3. Click **Next** to begin defining the resource. Resource Wizard steps and pages that display are, in order:
   - **Resource Parameters** — Set up resource-specific parameters that control authentication and resource adapter behavior. Enter parameters, and then click **Test Connection** to ensure the connection is valid. On confirmation, click **Next** to set up account attributes.



Resource Parameters

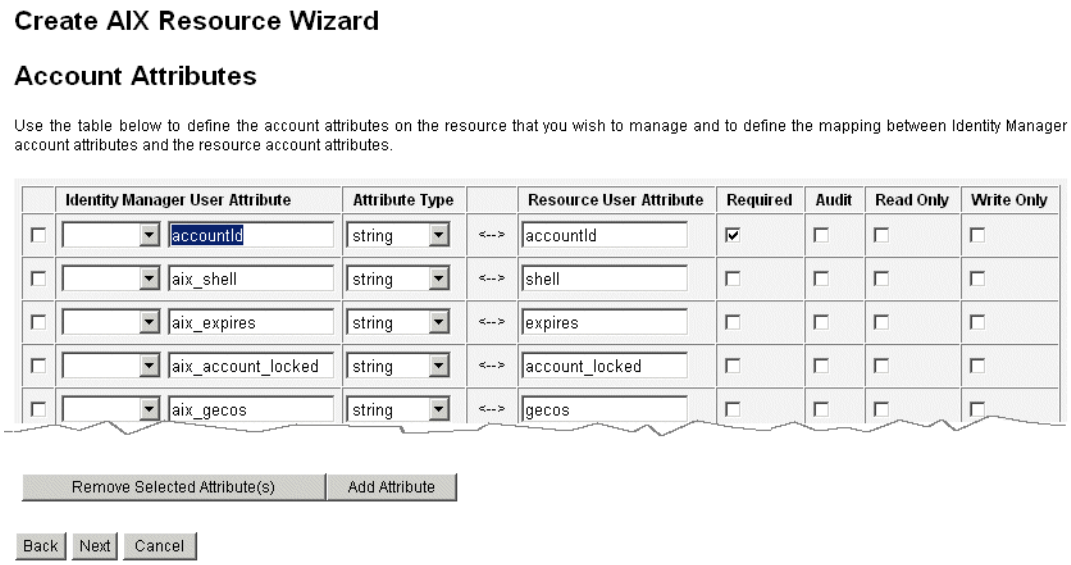
Specify the parameters that are specific to this resource. These are parameters for authentication and parameters for controlling the behavior of the resource adapter.

Host	
TCP Port	23
Login User	
password	
Login Shell Prompt	
Admin User	false
Completely Remove User	true
Root User	
credentials	
Root Shell Prompt	
Connection Type	Telnet
Maximum Connections	10
Connection Idle Timeout	900

Figure 1. Resource Wizard: Resource Parameters

- **Account Attributes (schema map)** — Maps Identity Manager account attributes to resource account attributes.

  To add an attribute, click **Add Attribute**. Select one or more attributes, and then click **Delete Selected Attributes** to delete attributes from the schema map. When finished, click **Next** to set up the identity template.



Create AIX Resource Wizard

Account Attributes

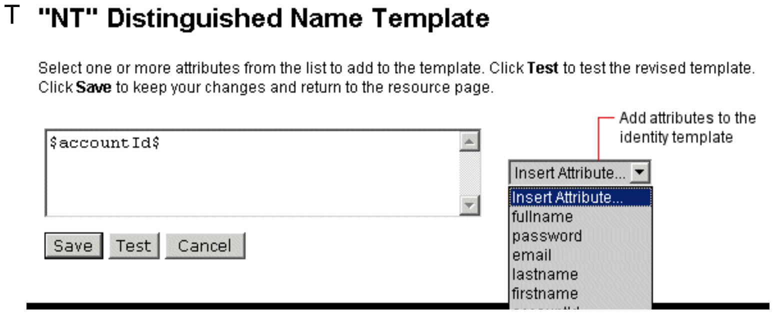
Use the table below to define the account attributes on the resource that you wish to manage and to define the mapping between Identity Manager account attributes and the resource account attributes.

	Identity Manager User Attribute		Attribute Type		Resource User Attribute	Required	Audit	Read Only	Write Only
□		accountId	string	<-->	accountId	☑	□	□	□
□		aix_shell	string	<-->	shell	□	□	□	□
□		aix_expires	string	<-->	expires	□	□	□	□
□		aix_account_locked	string	<-->	account_locked	□	□	□	□
□		aix_gecos	string	<-->	gecos	□	□	□	□

Figure 2. Resource Wizard: Account Attributes (Schema Map)

- **Identity Template** — Defines account name syntax for users. This feature is particularly important for hierarchical namespaces.

  Select attributes from the Insert Attributes list. To delete attributes from the template, click in the list and delete one or more items from the string. Delete the attribute name, as well as the preceding and following $ (dollar sign) characters.



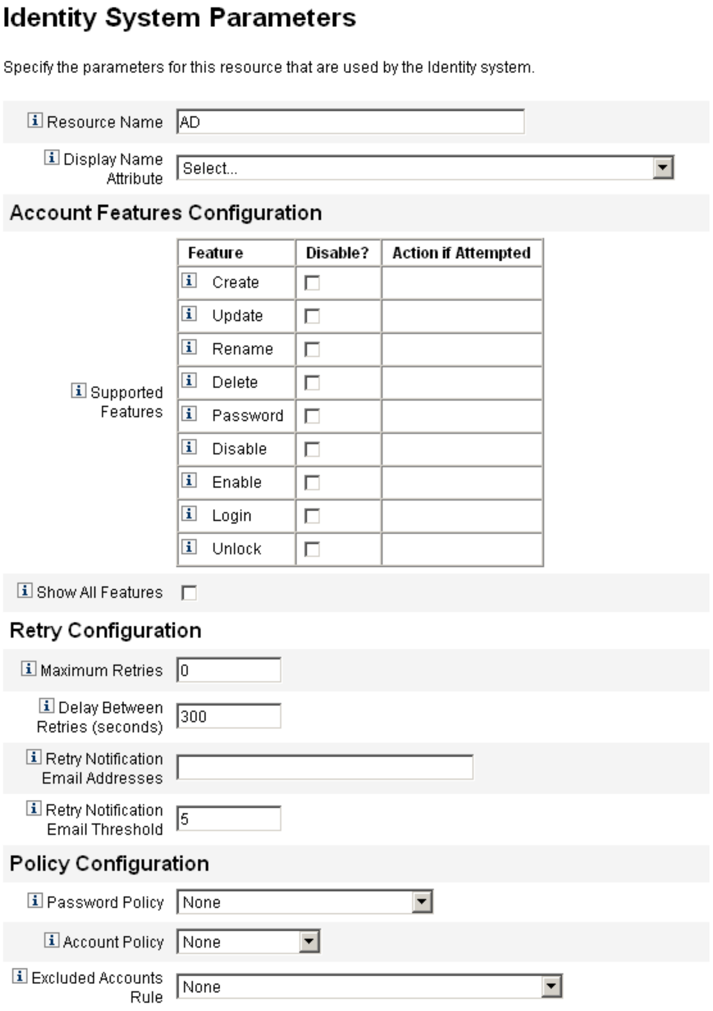
T "NT" Distinguished Name Template

Select one or more attributes from the list to add to the template. Click **Test** to test the revised template. Click **Save** to keep your changes and return to the resource page.

```
$accountId$
```

Figure 3. Resource Wizard: Identity Template

- **Identity System Parameters** — Sets Identity Manager parameters for the resource, including retry and policy configuration.



Identity System Parameters

Specify the parameters for this resource that are used by the Identity system.

Resource Name	AD
Display Name Attribute	Select...

Account Features Configuration

Supported Features

Feature	Disable?	Action if Attempted
Create	□	
Update	□	
Rename	□	
Delete	□	
Password	□	
Disable	□	
Enable	□	
Login	□	
Unlock	□	

Show All Features □

Retry Configuration

Maximum Retries	0
Delay Between Retries (seconds)	300
Retry Notification Email Addresses	
Retry Notification Email Threshold	5

Policy Configuration

Password Policy	None
Account Policy	None
Excluded Accounts Rule	None

Figure 4. Resource Wizard: Identity System Parameters

Use **Next** and **Back** to move among the pages. When you complete all selections, click **Save** to save the resource and return to the list page.

Managing Resources

You can perform a range of edit actions on the resource from the resources list. In addition to editing capabilities on each of the Resource Wizard pages, you can:

- **Delete resources** — Select one or more resources, and then select Delete from the Resource Actions list. You can select resources of several types at the same time. You cannot delete a resource if any roles or resource groups are associated with it.
- **Search for resource objects** — Select a resource, and then select Find Resource Object from the Resource Object Actions list to find a resource object (such as an organization, organizational unit, group, or person) by object characteristics.
- **Manage resource objects** — For some resource types, you can create new objects. Select the resource, and then select Create Resource Object from the Resource Object Actions list.
- **Rename resources** — Select a resource, and then select Rename from the Resource Actions list. Enter a new name in the entry box that appears, and then click **Rename**.
- **Clone resources** — Select a resource, and then select Save As from the Resource Actions list. Enter a new name in the entry box that appears. The cloned resource appears in the resource list with the name you select.

Working with Account Attributes

Identity Manager resources use schema maps to define names and types for attributes coming from the external resource (*resource account attributes*); they then map those attributes to the standard Identity Manager account attributes. By setting up a schema map (on the Account Attributes page of the Resource Wizard), you can:

- Limit resource attributes to only those that are essential for your company
- Create common Identity Manager attribute names to use with multiple resources
- Identify required user attributes and attribute types

To access these values, select the resource from the resources list, and then select Edit Resource Schema from the Resource Actions list.

The left column of the schema map (titled Identity system User Attribute) contains the names of Identity Manager account attributes that are referenced by the forms used in the Identity Manager Administrator and User interfaces. The right column of the schema map (titled Resource User Attribute) contains the names of attributes from the external source.

By defining Identity system attribute names, attributes from difference resources can be defined with common names. For example, on an Active Directory resource, the `lastname` attribute in Identity Manager is mapped to the Active Directory resource attribute `sn`; on GroupWise, the fullname attribute can be mapped to the GroupWise attribute `Surname`. As a result, an administrator is required to complete a value for `lastname` only once; when the user is saved, it is passed to the resources with different names.

Resource Groups

Use the resources area also to manage resource groups, which let you group resources to be updated in a specific order. By including and ordering resources in a group, and assigning the group to a user, you determine the order in which that user's resources are created, updated, and deleted.

Activities are performed on each resource in turn. If an action fails on a resource, the remaining resources are not updated. This type of relationship is important for related resources.

For example, an Exchange 5.5 resource relies on an existing Windows NT or Windows Active Directory account: one of these must exist before the Exchange account can be successfully created. By creating a resource group with (in order) a Windows NT resource and an Exchange 5.5 resource, you ensure the correct sequence when creating users. Conversely, this order ensures that resources are deleted in the correct sequence when you delete users.

Select **Resources**, and then select **List Resource Groups** to display a list of currently defined resource groups. From that page, click **New** to define a resource group. When defining a resource group, a selection area lets you choose and then order chosen resources, as well as select the organizations to which the resource group will be available.

Understanding ChangeLogs

Read this section for information about the Identity Manager ChangeLog feature, and for procedures to help you configure and use ChangeLogs.

What are ChangeLogs?

ChangeLogs provide a view of identity attributes information contained by Identity Manager resources. Each ChangeLog is defined to capture changes to a subset of identity attributes.

As attribute data changes on a resource, ActiveSync adapters capture the information, and then write changes to a ChangeLog. Custom scripts developed specifically to interact with a resource in the enterprise then read the ChangeLogs and update the resource.

The ChangeLogs feature differs from Identity Manager's standard resource active synchronization and reconciliation features because it enables indirect communication to resources from the provisioning system (via custom scripts).

ChangeLogs and Security

Identity Manager's ChangeLog feature requires write access to a designated directory or directories in the local file system. Some Web containers, by default, do not allow local file system access to the hosted Web modules like Identity Manager.

You grant access by editing a Java policy file. If using `/tmp/changelogs` as the directory, your policy file should contain:

```
grant {
    permission java.io.FilePermission "/tmp/changelogs/*",
"read,write,delete";
};
```

You must define a file permission for each ChangeLog directory that you have specified.

The default security policy file for Java can be found at:

```
$JAVA_HOME/jre/lib/security/java.policy
```

Editing that file may be sufficient; however, if you are using your own file (not the default file), then the server is running with options such as:

```
-Djava.security.manager -Djava.security.policy=/path/to/your/java.policy
```

In this case, edit the file identified by the `java.security.policy` system property.

Note You may need to restart the Web container after editing the security policy file.

ChangeLogs Feature Requirements

The ChangeLogs feature requires that you configure identity attributes before configuring a ChangeLog.

Configuring Identity Attributes

Use the following information and procedures to configure Identity Attributes and to select the Identity system applications to which Identity Attributes will be applied.

Working with Identity Attributes

To configure identity attributes, select **Configure**, and then select **Identity Attributes** from the Identity Manager Administrator interface. The Identity Attributes page displays.

To add an Identity Attribute, click **Add Attribute**. Once added to the list, edit an Identity Attribute by clicking its name in the list. To remove one or more Identity Attributes, select them, and then click Remove Selected Attributes.

Note You must click **Save** before the action will take place.

Selecting Applications

Use the Enabled Applications area to select the Identity system applications to which the Identity Attributes will be applied. Select one or more applications from the Available applications area and move them to the Enabled applications area. You must click **Save** before the action will take place.

Note To use the ChangeLog feature, you must enable the ActiveSync application.

Adding and Editing Identity Attributes

From the Add Identity Attributes or Edit Identity Attributes pages, make these selections to add or edit Identity Attributes:

- **Attribute Name** — Select or enter an attribute name. Select from the default values provided (from resource schema map entries, operational Identity Attributes, and user extended attributes); or enter a value in the text box.
- **Sources** — Select one or more sources with which to populate the value for this Identity Attribute. The sources will be evaluated in order, and the Identity Attribute will be set to the first non-null value.
  - **Resource** — The value comes from a selected attribute on a selected resource.
  - **Rule** — The value comes from the evaluation of a selected rule.
  - **Constant** — The value is set to the supplied constant value.

  Click **+** (plus sign) to add a new line to select another source. Click **-** (minus sign) next to a source to delete it.
- **Attribute Properties —** Use this area to set up properties for the Identity Attribute.
  - **Identity Attribute is authoritative** — The value of the Identity Attribute is authoritatively set on all targets. Select this option to cause the value determined by the sources to override any values entered by the user in a form. Typically, this option should be selected.
  - **Store attribute in IDM repository** — Select to store the Identity Attribute locally in the Identity system repository. This should be selected if the Identity system user is to be the authoritative store for the Identity Attribute, or if the attribute should be capable of handling queries.
  - **Set value on all assigned resources** — Select this option if the Identity Attribute should globally be set on all assigned resources that support this attribute.
- **Targets** — Select the target resource on which this Identity Attribute should be set. If no targets are defined, then click **Add Target**. To remove a target from the list, select it, and then click **Remove Selected Targets**.

  Click **OK** to add the Identity Attribute and return to the Identity Attributes page. You must click **Save** on the Identity Attributes page to save the additions.

Adding Target Resources

Tip It is not necessary to set targets for Identity Attributes if they are being used solely for the ChangeLog. You might do this, for example, if you wanted to use the ChangeLog, but also wanted to use the standard "Input Form" to push data through ActiveSync. If there are no targets, then the MetaView just calculates the identity attributes' values; it doesn't set them on any of the other resources.

Make selections to add a target resource for which an Identity Attribute should be set:

- **Target Resource** — Select the target resource on which the selected Identity Attribute should be set.
- **Target Attribute** — Select the name of the attribute on the target resource that will receive the value.
- **Condition** — Select a rule to run to determine if the selected Identity Attribute should be set on this target resource. This rule should return a value of true or false. If the condition is not set, then the target attribute always will be set for the selected event types.
- **Apply To:** — Select the types of events for which the selected Identity Attribute should be set on this target resource. These selections are combined with the Condition to determine if the target attribute should be set.

  Click **OK** to add the target resource and return to the Add or Edit Identity Attribute page.

Removing Target Resources

To remove one or more target resources, select them in the list, and then click **Remove Selected Targets**.

Importing Identity Attributes

Using the Import Identity Attributes feature, you can select one or more forms to import and populate Identity Attributes values. Identity Manager will analyze the imported form values and make a "best guess" at Identity Attributes; however, it may be necessary to edit the Identity Attributes after import.

Make these import selections:

- **Merge with existing Identity Attributes** — If you select this option, then Identity Manager will merge imported values with existing Identity Attributes. If not selected, then the Identity Attributes are cleared before the import occurs.
- **Forms to import** — Select one or more forms from the Available Forms area to populate the Identity Attributes.

  Click **Import** to import the forms. The Identity Attributes page displays with the new or merged Identity Attributes listed.

  Click **Save** to save changes to the Identity Attributes.

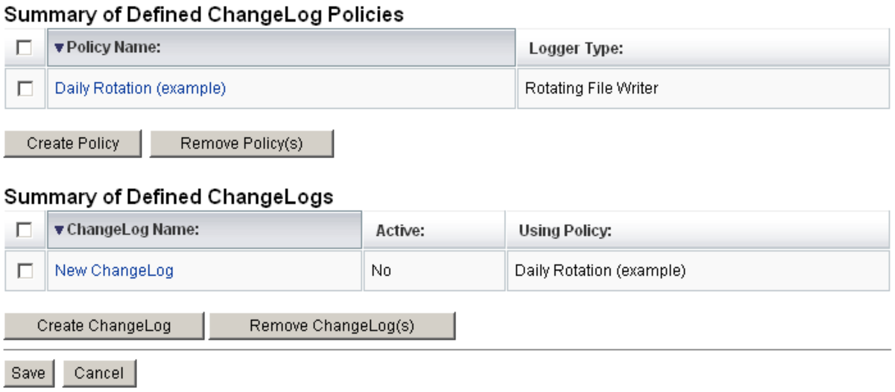
Note If there are Identity Attributes conditions that need to be corrected, then Identity Manager will display a Warning page that lists one or more warnings. Click **OK** to return to the Configure area.

Configuring ChangeLogs

You configure ChangeLogs by creating ChangeLog policies and ChangeLogs. Each ChangeLog must have an associated ChangeLog policy. A ChangeLog defines the subset of changes, detected by ActiveSync and pushed through the Identity Attributes, should be written to a log. Its associated ChangeLog policy defines how the ChangeLog files should be written. The ChangeLog files will be consumed by custom scripts.

To configure ChangeLogs and ChangeLog policies, select **Configure**, and then select **ChangeLogs** from the Administrator interface menu bar.

Identity Manager displays the ChangeLog Configuration page, which displays two summary areas.



Summary of Defined ChangeLog Policies

□	▾Policy Name:	Logger Type:
□	Daily Rotation (example)	Rotating File Writer

Summary of Defined ChangeLogs

□	▾ChangeLog Name:	Active:	Using Policy:
□	New ChangeLog	No	Daily Rotation (example)

Figure 5. ChangeLog Configuration

ChangeLog Policies Summary

The ChangeLog Policies summary area shows currently defined ChangeLog policies. To edit an existing ChangeLog policy, click its name in the list. To create a ChangeLog policy, click Create Policy.

To remove one or more ChangeLog policies, select them in the list, and then click Remove Policy. (No confirmation is needed for this action.)

ChangeLogs Summary

The ChangeLogs summary area shows currently defined ChangeLogs. To edit an existing ChangeLog, click its name in the list. To create a ChangeLog, click Create ChangeLog.

To remove one or more ChangeLogs, select them in the list, and then click Remove ChangeLog. (No confirmation is needed for this action.)

Saving ChangeLog Configuration Changes

Any changes you make to the ChangeLog Configuration — either to ChangeLog policies or defined ChangeLogs — must be saved from the ChangeLog Configuration page. Click **Save** to save changes and return to the Identity Manager Configure page.

Creating and Editing ChangeLog Policies

Provide input and make selections on the Edit ChangeLog Policy page to create or edit ChangeLog Policies:

- **Policy Name** — Enter a unique name for the policy.
- **Daily Start Time** — Establish the time of day used to calculate the times when rotations should start or change over. ChangeLogs using this policy will start new rotations at this time and at increments calculated from this time. For example, if the start time is set to midnight (00:00) with 3 'Rotations Per Day', the prefixes on log files will change at 00:00, 08:00, and 16:00.

  Filenames follow the pattern, 'cl_User_yyyyMMddHHmmss.n.suffix', where 'HHmmss' is the most recent time for a rotation to start. ('.n' is the Sequence number, and .suffix is a suffix provided in the ChangeLog definition.)

  Using '00:00' for the start time with 3 as the number of rotations, if you were to activate a ChangeLog at 9:24 a.m. one morning, the resulting rotation name would include the most recent rotation start time (for example, 08:00). In this case, the filenames would start with cl_User_yyyyMMdd080000. At 16:00, a new rotation (a new prefix on filenames) would start.
- **Rotations Per Day** — Specify the number of times you want to rotate the logs each day. For example, if you want a rotation every 4 hours, enter a value of 6.

  This value is limited to non-negative integers. A value of 0 means to ignore this field. When this field is non-zero, the 'Maximum Age of a Rotation' setting is ignored.

  If you specify the length of rotations in seconds, and if the 'Rotations Per Day' field is 0, then this value is used to determine the period of rotation.

  This is limited to non-negative integer values. If you specify a non-zero number of 'Rotations Per Day', then that value is used (and this one is not). If the value of both of these fields is 0, then only the sequence information is applied. (Even Daily Start Time is unused in this case.)

- **Number of Rotations to Keep** — Specify how many rotations are allowed to accumulate before Identity Manager deletes them. For example, if you are running with 3 rotations per day and want to keep 2 days of changes in the logs, specify a value of 6.
- **Maximum File Size in Bytes** — A new log file (with the same rotation prefix, but with a new sequence number) is started if writing a change to the current file will exceed this limit. A value of 0 indicates that this limit is not used. All of the limit fields (size, lines, age) that are non-zero are used; however, this limit is checked before the others.
- **Maximum File Size in Lines** — If writing a change will cause the current file to have more lines than this limit, then a new sequence file is created and the line is written to the new file. A value of 0 indicates 'no limit.' This limit is checked after the size limit and before the age limit.
- **Maximum File Age in Seconds** — When a change is received and the existing sequence file is now older than the number of seconds specified here, a new sequence file is created before writing the change. A value of 0 indicates that this limit is not used. The other limits, if non-zero, are applied before this one.

Click **OK** to return to the ChangeLog Configuration page. You must click OK from the Configuration page to save the new ChangeLog policy or changes to an existing policy.

Creating and Editing ChangeLogs

Provide input and make selections on the Edit ChangeLogs page to create or edit a ChangeLog:

- **ChangeLog Name** — Enter a unique name for the ChangeLog.
- **Active** — If you select this option, then the ChangeLog will monitor and write changes as they flow through ActiveSync resources and into the Identity Attributes (ActiveSync must be an Identity Attributes application for this to work).
- **Filter** — Enter the name of the ChangeLog filter to use. 'Noop' means use the default filter, which accepts all changes. This should be sufficient for the vast majority of cases. Otherwise, this must name a Java class implementing com.sun.idm.changelog.ChangeLogFilter. The class must be in the classpath of the server, and it must have a public default constructor.
- **Log these Operations** — Log events of the types selected, which includes Creates, Updates, and Deletes. Events not selected are ignored.
- **ChangeLog View** — Define the contents (columns) of the ChangeLog by using this table. Each table row specifies a column in the ChangeLog. Click Add Column to add a ChangeLog column. Each column has a name, a type, and an

Identity Attribute Name. The order of the rows indicates the order of the columns. Use the 'Up' and 'Down' buttons to order columns after they are defined.

Note In every ChangeLog, there will be an implicit first column in the table named 'changeType'. This implicit first column indicates the type of the change. This column's type is 'Text'. The data in the log will be one of the following values: 'ADD', 'MOD', or 'DEL'.

- **Use the Policy Named** — Select a defined ChangeLog policy from the list to use for logging.
- **Output Path** — Enter the name of the directory on the file system that will contain the log files. This can be a network-mounted location; but it is preferable to use a directory that is local to the server. It is also advisable to use a unique location per ChangeLog.
- **Suffix** — Enter a suffix for the ChangeLog files (for example, .csv). The suffix selected may be used to differentiate these files from other ChangeLog files.

Click **OK** to return to the ChangeLog Configuration page. You must click OK from the Configuration page to save the new ChangeLog or changes to an existing ChangeLog.

Example

View this example that details how to set up identity attributes and a ChangeLog to capture a specific set of attributes data.

Example: Define Identity Attributes

In this example, two Identity Manager resources (Resource 1 and Resource 2) provide source data to a third resource (Resource 3). Resource 3 is not directly connected to the Identity Manager system. A ChangeLog is needed to pull and maintain a data subset from Resource 1 and 2 to Resource 3.

Resource 1: EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

Resource2 : OrgInfo
employeeNum*
managerEmpNum
departmentNumber

Resource 3 : PhoneList
empId*
fullname
phone
department

Note * indicates a key to correlate records.

The Identity Attributes are defined as follows.

Attribute	<==	From Resource.Attribute
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber
reportsTo	<==	OrgInfo.managerEmpNum
firstName	<==	EmployeeInfo.givename
lastName	<==	EmployeeInfo.surname
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + “ “ + middleInitial + “ “ + lastName
phoneNumber	<==	EmployeeInfo.phone

Example: Configure the ChangeLog

After defining the identity attributes, define a ChangeLog called PhoneList ChangeLog. Its purpose is to write a subset of the identity attributes to a ChangeLog file.

ChangeLogView in PhoneList ChangeLog

Column Name	Type	Identity Attribute
empId	Text	employee
fullname	Text	fullname
phone	Text	phoneNumber

When records in Resource 1 or Resource 2 are changed, the full set of data (not just the changes) for a ChangeLog record (all data from the identity attributes) is written to the ChangeLog. A custom script reads the information and uses it to populate Resource 3.

CSV File Format

Read this section for information about the format of the comma-separated value (CSV) file written by ChangeLogs.

Think of a ChangeLog file in terms of rows and column, such as a spreadsheet or database table. Each “row” is a line in the file.

The ChangeLog format is self-describing using the first two rows. Together, these two rows define the “schema”; that is, the logical names and logical types of each “cell” (values between commas on a row) in the table.

The first row names the attributes in the file. The second row describes the types of values of the attributes. Additional rows represent all the data for a change-event.

The ChangeLog file is encoded in Java UTF-8 format.

Columns

The first column in the file has special significance. This defines the operation type; for example, whether the change event was a create, modify, or delete action. It is always named changeType, and is always type T (representing Text). Its value is one of the values ADD, MOD, or DEL.

Exactly one column should hold a unique identifier (the primary key) for the entry. This generally is the second column in the file.

Other columns simply name the attribute. The name is taken from the Column Name value in the ChangeLog View table.

Rows

After the first two header rows that define the "schema" of the file, the remaining rows hold the values of the attributes. The values appear in the order of the columns in the first row. The ChangeLog is applied from the Identity Attributes, and therefore contains all data known about the user at the time the change is detected.

In addition, there is no special sentinel value indicating null (or not set). If a value is not present when a change is detected, then the ChangeLog writes an empty string.

Values are encoded according to the type of the column, as specified in the second row of the file. Supported types are:

- T: Text
- B: Binary
- MT: Multi-Text
- MB: Multi-Binary

Text Values

Text values are written as a string, with two exceptions:

- If a value contains a `,` (comma), then Identity Manager escapes the comma within the value by inserting a `\` (backslash) character. For example, if the value for fullname is `Mouse, Mickey`, then Identity Manager writes `Mouse \,Mickey` as the value.
- If a value contains a \ (backslash) character, then Identity Manager escapes it with another \. For example, if a value for `homedir` contains `C:\users\home`, then Identity Manager writes `C:\\users\\home` to the log.

Text values cannot contain a newline. If the file needs newlines, then use the Binary value type.

Binary Values

Binary values are Base64 encoded.

Multi-Text Values

Multi-Text values are written similarly to Text values, but are comma-separated and bracketed (using [and]).

Multi-Binary Values

Multi-Binary values are written like Binary values (Base64 encoded), but also are comma-separated and bracketed (using [and]).

Formatting Examples

The following examples illustrate various output format. Each example is in the form:

```
column1, column2, column3, column4
```

Column 3 of each example shows the example text.

- Text (T) data appear as strings in the file:

  ```
  ADD,account0,some text data,column4
  ```

- Binary (B) data appears base64 encoded.

  ```
  ADD,account0,FGResWE23WDE==,column4
  ```

- Multi-Text (MT) appears as:

  ```
  ADD,account0,[one,two,three],column4
  ```

- Multi-Binary (MB) appears as:

  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

Note The Base64 alphabet does not include the , (comma), [(left bracket), or] (right bracket) characters, or a newline.

ChangeLog Filenames

Filenames are of the form:

*servername*_User_*timestamp*.*sequenceNumber*.*suffix*

Where:

- *timestamp* is the time that this log was started or rolled over. Files with the same timestamp are considered to be a "Rotation."
- *sequenceNumber* is a monotonically increasing number, used to partition a rotation into subsets of files, that are controlled by a maximum number of bytes, lines, or seconds. Each of these is known as a "Sequence" file.
- *suffix* is the file extension defined in the ChangeLog config, usually `.csv`.

Configuring Rotations and Sequences

These are defined in ChangeLogPolicy objects and referred to from ChangeLogs.

Example

A policy that defines rotations to:

- begin at 7:00 a.m.
- rotate three times each day for two days

would result in rotation file names similar to the following. (There are two sequence files in each of these rotations.)

```
myServer_User_20060101070000.1.csv
myServer_User_20060101070000.2.csv
myServer_User_20060101150000.1.csv
myServer_User_20060101150000.2.csv
myServer_User_20060101230000.1.csv
myServer_User_20060101230000.2.csv

myServer_User_20060102070000.1.csv
myServer_User_20060102070000.2.csv
myServer_User_20060102150000.1.csv
myServer_User_20060102150000.2.csv
myServer_User_20060102230000.1.csv
myServer_User_20060102230000.2.csv
```

January 1 shows 3 rotations, 8 hours apart, beginning at 07:00:00. January 2 is similar; only the portion of the name that corresponds to the day (20060102) differs.

Writing ChangeLog Scripts

Read this section for information helpful to ChangeLog script writers.

- Scripts likely run continuously, waiting for new data, new files, or sleeping between activity; and then simply read the file and apply the changes for each line to the back-end resource.
- ChangeLogs support delete operations; however, only the accountId value will be included in DEL lines.
- By using Rotations and Sequences, you can decide how often a script runs. For example, you could specify:
  - Rotation at midnight; and then every night run the script against the prior rotation.
  - Rotation every 4 hours, starting at 8:00 a.m., and then run the scripts every four hours (at 8, 12, 16, 20, 24, 4, ...)

    - No rotation, and run the script such that it reads a sequence file when the sequence number bumps. You can control how the sequence number increments; it can be size-based, num-operations based, or time-based.

- Each ChangeLog can be seen as a representation of the records in the back-end system. To keep things simple for the script reading the log, Identity Manager always writes all data for a given record, whether or not it has changed. Scripts can "blindly" apply the data in the records.

  However, they need to ensure that the back-end resource (or the script), especially with regard to ADD and DEL, can either:

    - Handle this idempotently. (*Idempotency* means if you apply the data more than once, then it does nothing.) If the script reads the ChangeLog from start to finish in two passes, then the state of the data records in the resource should be exactly the same after each pass.
    - Does this (at most) one time. For example, if the resource cannot be made idempotent with regard to add and delete actions, then the script must ensure that it applies changes only once, either by reading the log entries only once, or by otherwise tracking its progress.

- A good approach might be to watch for a sequence file to appear, and then apply the previous file. For example, do not apply a .1 file until the .2 file appears. When .3 appears, apply .2. After applying a file, note that you have done so on a disk. This approach allows you to avoid using calls like `fstat` or `tail -f`.

Understanding Policies

Read this section for information and procedures for configuring policies.

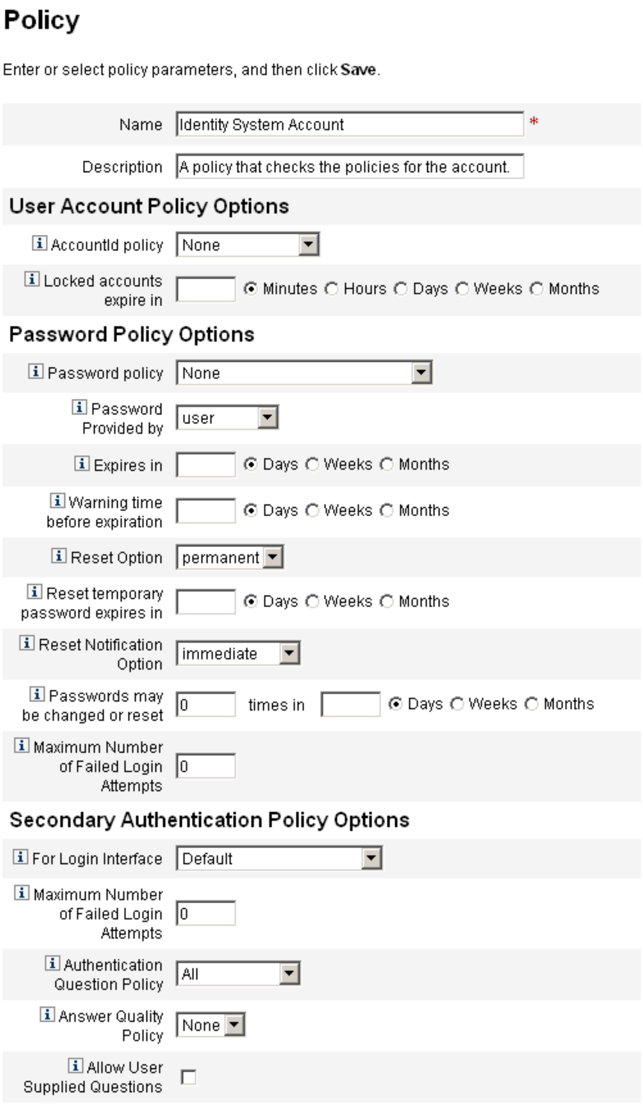
What are Policies?

Identity Manager policies set limitations for Identity Manager users by establishing constraints for Identity Manager account ID, login, and password characteristics.

You create and edit Identity Manager policies from the Policies page. From the menu bar, select **Configure**, and then select **Policies**. From the displayed list page, you can edit existing policies and create new ones.

Policies are categorized as:

- **Identity System Account policies** — Establish user, password, and authentication policy options and constraints. You assign Identity System Account policies to organizations or users, through the Create and Edit Organization and Create and Edit User pages.



Policy

Enter or select policy parameters, and then click **Save**.

Name	Identity System Account *
Description	A policy that checks the policies for the account.

User Account Policy Options

AccountId policy	None
Locked accounts expire in	● Minutes ○ Hours ○ Days ○ Weeks ○ Months

Password Policy Options

Password policy	None
Password Provided by	user
Expires in	● Days ○ Weeks ○ Months
Warning time before expiration	● Days ○ Weeks ○ Months
Reset Option	permanent
Reset temporary password expires in	● Days ○ Weeks ○ Months
Reset Notification Option	immediate
Passwords may be changed or reset	0 times in ● Days ○ Weeks ○ Months
Maximum Number of Failed Login Attempts	0

Secondary Authentication Policy Options

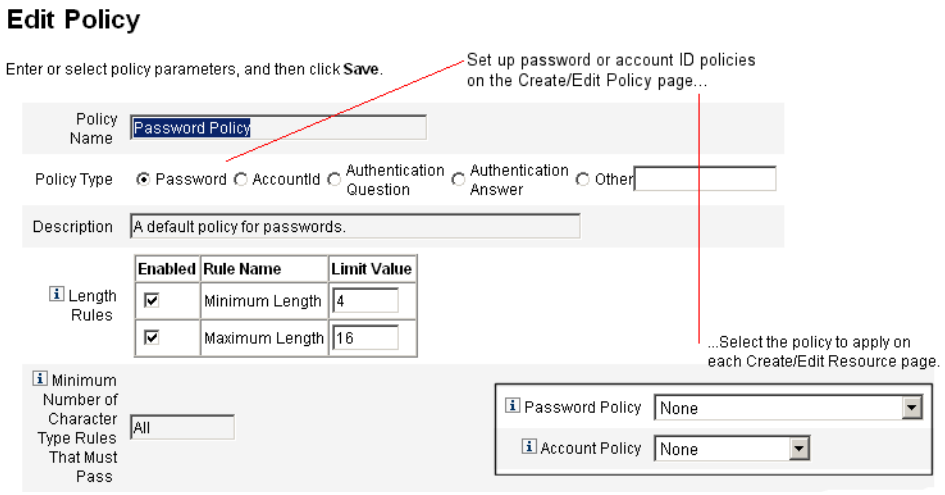
For Login Interface	Default
Maximum Number of Failed Login Attempts	0
Authentication Question Policy	All
Answer Quality Policy	None
Allow User Supplied Questions	□

Figure 6. Identity Manager Policy

Options you can set or select include:

- **User policy options** — Specify how Identity Manager treats user accounts if a user fails to correctly answer authentication questions
- **Password policy options** — Set password expiration, warning time before expiration, and reset options
- **Authentication policy options** — Determine how authentication questions will be presented to the user, whether the user can provide his own authentication questions, and establish the bank of questions (up to 10) that could be presented to a user.

- **String Quality Policies** — String quality policies include policy types such as password, AccountID, and authentication, and set length rules, character type rules, and allowed words and attribute values. This type of policy is tied to each Identity Manager resource, and is set on each resource page.



Edit Policy

Enter or select policy parameters, and then click **Save**.

Set up password or account ID policies on the Create/Edit Policy page...

Policy Name	Password Policy
Policy Type	● Password ○ AccountId ○ Authentication Question ○ Authentication Answer ○ Other
Description	A default policy for passwords.

Length Rules

Enabled	Rule Name	Limit Value
☑	Minimum Length	4
☑	Maximum Length	16

Minimum Number of Character Type Rules That Must Pass: All

...Select the policy to apply on each Create/Edit Resource page.

Password Policy	None
Account Policy	None

Figure 7. Create/Edit Password Policy

Options and rules you can set for passwords and account IDs include:

- **Length rules** — Determine minimum and maximum length.
- **Character type rules** — Set minimum and maximum allowable values for alphabetic, numeric, uppercase, lowercase, repetitive, and sequential characters.

- **Password re-use limits** — Specify the number of passwords preceding the current password that cannot be re-used. When a user attempts to change his password, the new password will be compared to the password history to ensure this is a unique password. For security reasons, a digital signature of the previous passwords is saved; new passwords are compared to this.
- **Prohibited words and attribute values** — Specify words and attributes that cannot be used as part of an ID or password.

Dictionary Policy

The dictionary policy enables Identity Manager to check passwords against a word database to ensure that they are protected from a simple dictionary attack. By using this policy with other policy settings to enforce the length and makeup of passwords, Identity Manager makes it difficult to use a dictionary to guess passwords that are generated or changed in the system.

The dictionary policy extends the password exclusion list that you can set up with the policy. (This list is implemented by the Must Not Contain Words option on the Administrator Interface password Edit Policy page.)

Configuring the Dictionary Policy

To set up the dictionary policy, you must:

- Configure dictionary server support
- Load the dictionary

Follow these steps:

1. From the menu bar, select **Configure**, and then select **Policies**.
2. Click **Configure Dictionary** to display the Dictionary Configuration page.
3. Select and enter database information:
   - **Database Type** — Select the database type (Oracle, DB2, SQLServer, or MySQL) that you will use to store the dictionary.
   - **Host** — Enter the name of the host where the database is running.
   - **User** — Enter the user name to use when connecting to the database.
   - **Password** — Enter the password to use when connecting to the database.
   - **Port** — Enter the port on which the database is listening.
   - **Connection URL** — Enter the URL to use when connecting. These template variables are available:
     - %h - host

    - %p - port
    - %d - database name
  - **Driver Class** — Enter the JDBC driver class to use while interacting with the database.
  - **Database Name** — Enter the name of the database where the dictionary will be loaded.
  - **Dictionary Filename** — Enter the name of the file to use when loading the dictionary.
4. Click **Test** to test the database connection.
5. If the connection test is successful, click **Load Words** to load the dictionary.

Note The load task may take a few minutes to complete.

6. Click **Test** to ensure that the dictionary was loaded correctly.

Implementing the Dictionary Policy

Implement the dictionary policy from the Identity Manager policies area. From the Policies page, click to edit a password policy. On the Edit Policy page, select the Check passwords against dictionary words option. Once implemented, all changed and generated passwords will be checked against the dictionary.

Understanding Capabilities

Capabilities are groups of rights in the Identity Manager system. Capabilities represent administrative job responsibilities, such as resetting passwords or administering user accounts. Each Identity Manager administrative user is assigned one or more capabilities, which provide a set of privileges without compromising data protection.

Not all Identity Manager users need capabilities assigned; only those who will perform one or more administrative actions through Identity Manager. For example, an assigned capability is not needed to enable a user to change his password, but an assigned capability is required to change another user’s password.

Your assigned capabilities govern which areas of the Identity Manager Administrator Interface you can access. All Identity Manager administrative users can access certain areas of Identity Manager, including:

- **Home** and **Help** tabs
- **Passwords** tab (**Change My Password** and **Change My Answers** subtabs only)
- **Reports** (limited to types related to the administrator's specific responsibilities)

Capabilities Categories

Identity Manager defines capabilities as:

- 🔑 **Task-based**. These are capabilities at their simplest task level.
- 🔑📁 **Functional**. Functional capabilities contain one or more other functional or task-based capabilities.

Built-in capabilities (those provided with the Identity Manager system) are *protected*, meaning that you cannot edit them. You can, however, use them within capabilities that you create.

Protected (built-in) capabilities are indicated in the list with a red key (or red key and folder) icon. Capabilities that you create and can edit are indicated in the capabilities list with a green key (or green key and folder) icon.

Working with Capabilities

1. From the menu bar, select **Configure**.
2. Select **Capabilities** to display the list of Identity Manager capabilities.

Create a Capability

To create a capability, click **New**.

Edit a Capability

To edit a non-protected capability, right-click it in the list, and then select **Edit**.

Note You cannot edit built-in capabilities; however, you can save them with a different name to create your own capability, or use them in capabilities you create.

Save and Rename a Capability

To “clone” a capability (save it with a different name to create a new capability):

- Right-click a capability in the list, and then select Save As.
- Enter a new name, and then click **OK**.

You can edit the new capability, even if the copied capability is protected.

Assigning Capabilities

Assign capabilities to a user from the Create and Edit User page.

Note You can also assign capabilities to a user by assigning an admin role, which you set up through the Security area. See *Understanding Admin Roles* for more information.

Capabilities Hierarchy

Task-based capabilities fall within the following functional capabilities hierarchy:

Account Administrator

- Approver
- Assign User Capabilities
- User Account Administrator
  - Create User
  - Delete User
    - Delete IDM User
    - Deprovision User
    - Unassign User
    - Unlink User
  - Disable User
  - Enable User
  - Password Administrator
    - Change Password Administrator
    - Reset Password Administrator
  - Rename User
  - Unlock User
  - Update User
  - View User
  - Import User

Admin Role Administrator

- Connect Capabilities
- Connect Capabilities Rules
- Connect Controlled Organizations Rules

- Connect Organizations

Bulk Account Administrator

- Approver
- Assign User Capabilities
- Bulk User Account Administrator
  - Bulk Create User
  - Bulk Delete User
    - › Bulk Delete IDM User
    - › Bulk Deprovision User
    - › Bulk Unassign User
    - › Bulk Unlink User
  - Bulk Disable User
  - Bulk Enable User
  - Password Administrator
  - Rename User
  - Unlock User
  - View User
  - Import User

Bulk Change Account Administrator

- Approver
- Assign User Capabilities
- Bulk Change User Account Administrator
  - Bulk Disable User
  - Bulk Enable User
  - Bulk Update User
  - Password Administrator
  - Rename User
  - Unlock User
  - View User

Capability Administrator

Change Account Administrator

- Approver
- Assign User Capabilities
- Change User Account Administrator
  - Disable User
  - Enable User
  - Password Administrator
    - › Change Password Administrator
    - › Reset Password Administrator
  - Rename User
  - Unlock User
  - Update User
  - View User

Import/Export Administrator

Login Administrator

Organization Administrator

Password Administrator (Verification Required)

- Change Password Administrator (Verification Required)
- Reset Password Administrator (Verification Required)

Policy Administrator

Reconcile Administrator

- Reconcile Request Administrator

Remedy Integration Administrator

Report Administrator

- Admin Report Administrator
  - Run Admin Report
- Audit Report Administrator
  - Run Audit Report
- Configure Audit
- Reconcile Report Administrator

  - Run Reconcile Report
- Resource Report Administrator
  - Run Resource Report
- Risk Analysis Administrator
  - Run Risk Analysis
- Role Report Administrator
  - Run Role Report
- Task Report Administrator
  - Run Task Report
- User Report Administrator
  - Run User Report

Resource Administrator

- Resource Group Administrator
- Change Active Sync Resource Administrator
- Control Active Sync Resource Administrator

Resource Object Administrator

Resource Password Administrator

- Change Resource Password Administrator
- Reset Resource Password Administrator

Role Administrator

Security Administrator

View Organizations

- List Organizations

View Resources

- List Resources

Waveset Administrator

Capabilities Definitions

The following table describes each of the task-based capabilities and highlights the tabs and subtabs accessible with each capability.

All capabilities grant the user or administrator access to the **Change My Password** and **Change My Answers** subtabs (**Passwords** tab).

Capability	**Allows the Administrator/User to:**	**Can Access These Tabs and Subtabs:**
Account Administrator	Perform all operations on users, including assigning capabilities. Does not include bulk operations.	**Accounts** - **List Accounts**, **Find Users**, **Extract to File**, **Load from File**, **Load from Resource** subtabs **Passwords** - All subtabs **Approvals** - All subtabs **Tasks** - All subtabs
Admin Report Administrator	Create, edit, delete, and run administrator reports.	**Reports** - **Manage Reports**, **Run Reports** subtabs (Administrator report only)
Admin Role Administrator	Create, edit, and delete admin roles.	**Configure** - **Admin Roles** subtab
Approver	Approve or reject requests initiated by other users.	**Approvals** - All subtabs
Assign User Capabilities	Change user capabilities assignments (assign and unassign).	**Accounts** - **List Accounts** (Edit only), **Find Users** subtabs. Must be assigned with another user administrator capability (for example, Create User or Enable User).
Audit Report Administrator	Create, edit, delete, and run audit reports.	**Reports** - Audit reports only
Bulk Account Administrator	Perform regular and bulk operations on users, including assigning capabilities.	**Accounts** - All subtabs **Passwords** - All subtabs **Approvals** - All subtabs **Tasks** - All subtabs
Bulk Change Account Administrator	Perform regular and bulk operations except delete on existing users, including assigning capabilities.	**Accounts** - **List Accounts**, **Find Users**, **Launch Bulk Actions** subtabs. Cannot create or delete users. **Passwords** - All subtabs **Approvals** - All subtabs **Tasks** - All subtabs

Bulk Change User Account Administrator	Perform regular and bulk operations except delete on existing users.	**Accounts** - **List Accounts, Find Users, Launch Bulk Actions** subtabs. Cannot create, delete, or assign capabilities to users. **Passwords** - All subtabs **Tasks** - All subtabs
Bulk Create User	Assign resources and initiate user create requests (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Create only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Delete User	Delete Identity Manager user accounts; deprovision, unassign, and unlink resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Create only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Delete IDM User	Delete existing Identity Manager user accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Delete only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Deprovision User	Delete and unlink existing resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Deprovision only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Disable User	Disable existing users and resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Disable only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Enable User	Enable existing users and resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Enable only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Unassign User	Unassign and unlink existing resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Unassign only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk Unlink User	Unlink existing resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Unlink only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs

Bulk Update User	Update existing users and resource accounts (on individual users and by using bulk operations).	**Accounts** - **List Accounts** (Update only), **Find Users**, **Launch Bulk Actions** subtabs **Tasks** - All subtabs
Bulk User Account Administrator	Perform all regular and bulk operations on users.	**Accounts** - All subtabs **Passwords** - All subtabs **Tasks** - All subtabs
Capability Administrator	Create, modify, and delete capabilities.	**Configure** - **Capabilities** subtab
Change Account Administrator	Perform all operations except delete on existing users, including assigning capabilities. Does not include bulk operations	**Accounts** - All subtabs. Cannot delete users. **Passwords** - All subtabs **Approvals** - All subtabs **Tasks** - All subtabs **Reports** - Create admin and user reports, run and edit admin reports, run auditlog reports in scope. Cannot run admin and user reports on out-of-scope organizations.
Change Active Sync Resource Administrator	Change active sync resource parameters.	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs **Resources** - For Active Sync resources: Edit actions menu, Edit Active Sync Parameters
Change Password Administrator	Change user and resource account passwords.	**Accounts - List Accounts, Find Users** subtabs (Change Password only) **Passwords** - All subtabs **Tasks** - All subtabs. Export Password Scan task only (from **Run Tasks** subtab)
Change Password Administrator (Verification Required)	Change user and resource account passwords following successful validation of the user's authentication question answers.	**Accounts - List Accounts, Find Users** subtabs (Change Password only; verification required before action) **Passwords** - All subtabs **Tasks** - All subtabs. Export Password Scan task only (from **Run Tasks** subtab)

Change Resource Password Administrator	Change resource administrator account passwords.	**Tasks -** All subtabs **Resources - List Resources** subtab. Change resource password only (from **Manage Connection-->Change Password** in the actions menu)
Change User Account Administrator	Perform all operations except delete on existing users. Does not include bulk operations	**Accounts** - **List Accounts, Find Users** subtabs. Cannot create, delete, or assign capabilities to users. **Passwords** - All subtabs **Tasks** - All subtabs
Configure Audit	Configure the activities audited in the system.	**Configure** - **Audit Events** subtab
Control Active Sync Resource Administrator	Control Active Sync resource state (such as start, stop, and refresh)	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** **Resources** - For Active Sync resources: Active Sync actions menu (all selections)
Create User	Assign resources and initiate user create requests. Does not include bulk operations	**Accounts** - **List Accounts** (Create only), **Find Users** subtabs **Tasks** - All subtabs
Delete User	Delete Identity Manager user accounts; deprovision, unassign, and unlink resource accounts. Does not include bulk operations.	**Accounts** - **List Accounts** (Delete only), **Find Users** subtabs **Tasks** - All subtabs
Delete IDM User	Delete Identity Manager user accounts. Does not include bulk operations.	**Accounts** - **List Accounts** (Delete only), **Find Users** subtabs **Tasks** - All subtabs
Deprovision User	Delete and unlink existing resource accounts. Does not include bulk operations.	**Accounts** - **List Accounts** (Deprovision only), **Find Users** subtabs **Tasks** - All subtabs
Disable User	Disable existing users and resource accounts. Does not include bulk operations	**Accounts** - **List Accounts** (Disable only), **Find Users** subtabs **Tasks** - All subtabs

Enable User	Enable existing users and resource accounts. Does not include bulk operations	**Accounts** - **List Accounts** (Enable only), **Find Users** subtabs **Tasks** - All subtabs
Import User	Import users from defined resources.	**Accounts** - **Extract to File**, **Load from File**, **Load from Resource** subtabs
Import/Export Administrator	Import and export all types of objects.	**Configure** - **Import Exchange File** subtab
License Administrator	Set the Identity system product license	Provides `lh license` command access. (No Administrator Interface tabs provided by this capability.)
Login Administrator	Edit the set of login modules for a given login interface.	**Configure** - **Login** subtab
Organization Administrator	Create, edit, and delete organizations.	**Accounts** - **List Accounts** subtab (Edit and create organizations and directory junctions, delete organizations only)
Password Administrator	Change and reset user and resource account passwords.	**Accounts** - **List Accounts** (list, change, and reset passwords only), **Find Users** subtabs **Passwords** - All subtabs **Tasks** - All subtabs
Password Administrator (Verification Required)	Change and reset user and resource account passwords following successful validation of the user's authentication question answers.	**Accounts** - **List Accounts** (list, change, and reset passwords only; verification required before action succeeds), **Find Users** subtabs **Passwords** - All subtabs **Tasks** - All subtabs
Policy Administrator	Create, edit, and delete Policies.	**Configure** - **Policy** subtab
Reconcile Administrator	Edit reconciliation policies and control reconciliation tasks.	**Tasks** - All subtabs (View reconcile task). **Resources** - **List Resources** subtab
Reconcile Report Administrator	Create, edit, delete, and run reconciliation reports.	**Reports** - **Run Reports** (Account Index report only), **Manage Reports** subtabs

Reconcile Request Administrator	Manage reconciliation requests.	**Tasks** - All subtabs **Resources** - **List Resources** subtab (list and reconciliation features only)
Remedy Integration Administrator	Modify Remedy integration configuration.	**Tasks** - All subtabs (view tasks, run role synchronization) **Configure** - **Remedy Integration** subtab
Rename User	Rename existing users and resource accounts.	**Accounts** - List Accounts subtab (list all accounts in scope, rename users)
Report Administrator	Configure audit settings and run all report types.	**Tasks** - All subtabs (view tasks, run role synchronization) **Reports** - All subtabs
Reset Password Administrator	Reset user and resource account passwords.	**Accounts - List Accounts, Find Users** subtabs (Reset Password only) **Passwords** - All subtabs **Tasks** - All subtabs. Export Password Scan task only (from **Run Tasks** subtab)
Reset Password Administrator (Verification Required)	Reset user and resource account passwords following successful validation of the user's authentication question answers.	**Accounts - List Accounts, Find Users** subtabs (Reset Password only; verification required before action succeeds) **Passwords** - All subtabs **Tasks** - All subtabs. Export Password Scan task only (from **Run Tasks** subtab)
Reset Resource Password Administrator	Reset resource administrator account passwords.	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs **Resources - List Resources** subtab. Reset resource password only (from **Manage Connection -->Reset Password** in the actions menu)

Resource Administrator	Create, modify, and delete resources.	**Reports** - Resource user report, resource group report returns error on out-of-scope resources. **Resources** - **List Resources** subtab (edit global policy, edit parameters, resource groups. Cannot manage connection or resource objects).
Resource Group Administrator	Create, edit, and delete resource groups.	**Resources** - **List Resource Groups** subtab
Resource Object Administrator	Create, modify, and delete resource objects.	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs (view tasks involving resource objects). **Resources** - **List Resources** subtab (list and manage resource objects only)
Resource Password Administrator	Change and reset resource proxy account passwords.	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs **Resources - List Resources** subtab. Change resource password only (from **Manage Connection-->Change Password** in the actions menu)
Resource Report Administrator	Create, edit, delete, and run resource reports.	**Reports** - All subtabs (resource reports only)
Risk Analysis Administrator	Create, edit, delete, and run risk analysis.	**Risk Analysis** - All subtabs
Role Administrator	Create, modify, and delete roles.	**Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs (synchronize roles) **Roles** - All subtabs
Role Report Administrator	Create, edit, delete, and run resource reports.	**Reports** - Role reports only
Run Admin Report	Run administrator reports.	**Reports** - Admin reports onlyl
Run Audit Report	Run audit reports.	**Reports** - AuditLog and Usage reports only
Run Reconcile Report	Run reconciliation reports.	**Reports** - AuditLog and Usage reports only
Run Resource Report	Run resource reports.	**Reports** - AuditLog and Usage reports only

Run Risk Analysis	Run risk analysis.	
Run Role Report	Run role reports.	**Reports** - Role reports only
Run Task Report	Run task reports.	**Reports** - Task reports only
Run User Report	Run user reports.	**Reports** - User reports only
Security Administrator	Create users with capabilities; manage encryption keys, login configuration, and policies.	**Accounts** - **List Accounts** (delete, create, update, edit, change and edit passwords), **Find Users** subtabs (audit report) **Passwords** - All subtabs **Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs **Reports** - All subtabs **Resources** - **List Resources** (list and control resource objects) **Configure** - **Policies**, **Login** subtabs
Task Report Administrator	Create, edit, delete, and run task reports.	**Reports** - Create and manage task reports
Unassign User	Unassign and unlink existing resource accounts. Does not include bulk operations.	**Accounts** - **List Accounts** (Unassign only), **Find Users** subtabs **Tasks** - All subtabs
Unlink User	Unlink existing resource accounts. Does not include bulk operations.	**Accounts** - **List Accounts** (Unlink only), **Find Users** subtabs **Tasks** - All subtabs
Unlock User	Unlock existing user’s resource accounts that support unlock. Does not include bulk operations.	**Accounts** - **List Accounts** (Unlock only), **Find Users** subtabs **Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs
Update User	Edit existing users and initiate user update requests.	**Accounts** - Edit and update users **Tasks** - Manage existing tasks (from the **All Tasks** subtab)

User Account Administrator	All operations on users.	**Accounts** - **List Accounts**, **Find Users**, **Extract to File**, **Load from File**, **Load from Resource** subtabs. Cannot assign user capabilities (**Security** form tab on **List Accounts** subtab). **Tasks** - **Find Tasks**, **All Tasks**, **Run Tasks** subtabs
User Report Administrator	Create, edit, delete, and run user reports.	**Reports** - Run user reports.
View User	View individual user details.	**Accounts** - Select users from the list to view individual user account information. No change actions allowed.
Waveset Administrator	Perform system-wide tasks, such as modification of system configuration objects.	**Tasks** - All subtabs. Synchronize roles, edit source adapter template, and schedule reports **Reports** - All subtabs **Resources** - List Resources (list only; no change actions allowed) **Configure** - **Audit Events**, **Email Templates**, **Form and Process Mappings** subtabs

Table 1. Identity Manager Capabilities Descriptions

Understanding Admin Roles

Admin roles enable the assignment of a unique set of capabilities for each set of organizations managed by an administrator. An admin role is assigned capabilities and controlled organizations; it can then be assigned to an administrative user.

The assignment of capabilities and organizations to an admin role can be:

- **Direct** — This option allows you to assign specific capabilities, controlled organizations, or both to the admin role.
- **Dynamic** (indirect) — This option uses capabilities and controlled organizations *rules* to dynamically determine, each time the assigned user logs into Identity Manager, the capabilities and controlled organizations given to him through the admin role.

Note See *Capabilities Rules and Controlled Organizations Rules* for key information about setting up these rules.

You can assign one or more admin roles to each user. An admin role can be assigned to one or more users.

User Admin Role

Identity Manager includes a built-in admin role, titled "User". By default, it contains no capabilities or controlled organization assignments, and it cannot be deleted. This admin role is implicitly assigned to all users (end users and administrators) at login time.

You can edit the User admin role through the Administrator interface (select **Configure**, and then select **Admin Roles**).

Because any capabilities or controlled organizations that are statically assigned through this admin role are assigned to all users, it is recommended that the assignment of capabilities and controlled organizations be done through rules. This will enable different users to have different (or no) capabilities, and assignments will be scoped depending on factors such as who they are, which department they are in, or whether they are managers, which can be queried for within the context of the rules.

The User admin role does not deprecate or replace the use of the `authorized=true` flag used in workflows. This flag is still appropriate in cases where the user should not have access to objects accessed by the workflow, except when the workflow is executing. Essentially, this lets the user enter a "run as superuser" mode.

However, in cases where a user should have specific access to one or more objects outside of and potentially inside of workflows, then dynamic assignment of capabilities and controlled organizations via the User admin role enables dynamic, fine-grain authorization to those objects.

Example

The steps in the following example show how the User admin role can be used in a dynamic environment.

1. Create two Active Directory ou's:
   - "Chicago Cubs" && "New York Yankees"
2. Create three Active Directory users in each ou, with the following attributes set:
   - Chicago Cubs:
     - Dusty Baker (title = 'manager', manager = '')
     - Kerry Woods (title = 'pitcher', manager = 'Dusty Baker')

    - Mark Prior (title = 'pitcher', manager = 'Dusty Baker')
  - New York Yankees
    - Joe Torre (title = 'manager', manager = '')
    - Alex Rodriguiz (title = '3rd', manager = 'Joe Torre')
    - Derek Jeter (title = 'shortstop', manager = 'Joe Torre')

3. Assign the following rules to the User admin role:
   - capabilitesRule ==> If Team Manager Assign Account Admin Capability
   - controlledOrganizationsRule ==> If Team Manager Assign Control of My Team
4. Create an Identity Manager organization named “My Team” and assign:
   - userMembersRule ==> Get My Team

When a user logs in, then:

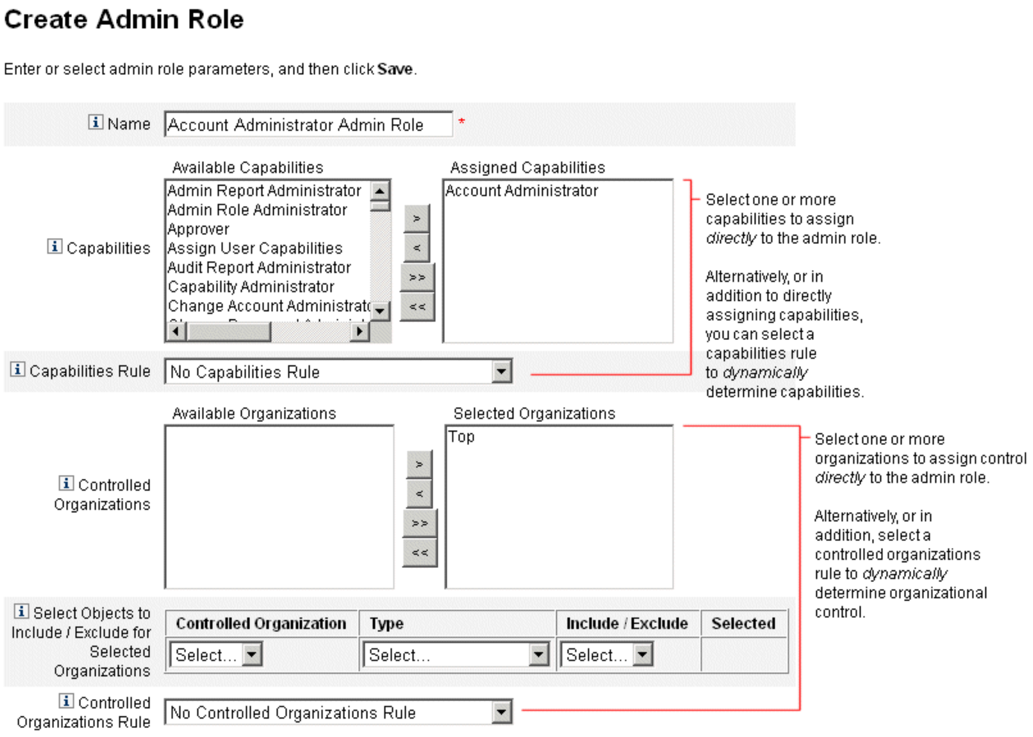
- If his Active Directory user title is 'manager', then he will be assigned the "Account Administrator" capability and assigned control of the "My Team" organization.
- If his AD user title is not 'manager', then he will not be assigned any capabilities or organizations to control.
- If the logged-in user's title is 'manager', then when the "My Team" organization is opened, the "Get My Team" rule will invoke getResourceObjects on the Active Directory resource requesting all users whose 'manager' is the accountInfo.accounts[AD].accountId of the user currently logged in.

This setup will enable managers logged into the User interface to manage their employees, and prevent employees from performing admin functions when logged in to the User interface.

Creating and Editing Admin Roles

To create or edit an admin role, you must be assigned the Admin Role Administrator capability. To access the admin roles area, click **Configure**, and then click **Admin Roles**. The Admin Roles list page allows you to create, edit, and delete admin roles in Identity Manager.

To edit an existing admin role, click a name in the list. Click **New** to create an admin role. Identity Manager displays the Create Admin Role page, where you specify the capabilities and scope of the new admin role.



Create Admin Role

Enter or select admin role parameters, and then click **Save**.

Name: Account Administrator Admin Role *

Capabilities

Available Capabilities: Admin Report Administrator, Admin Role Administrator, Approver, Assign User Capabilities, Audit Report Administrator, Capability Administrator, Change Account Administrato

Assigned Capabilities: Account Administrator

Capabilities Rule: No Capabilities Rule

Select one or more capabilities to assign *directly* to the admin role.

Alternatively, or in addition to directly assigning capabilities, you can select a capabilities rule to *dynamically* determine capabilities.

Controlled Organizations

Available Organizations:

Selected Organizations: Top

Select Objects to Include / Exclude for Selected Organizations

Controlled Organization	Type	Include / Exclude	Selected
Select...	Select...	Select...	

Controlled Organizations Rule: No Controlled Organizations Rule

Select one or more organizations to assign control *directly* to the admin role.

Alternatively, or in addition, select a controlled organizations rule to *dynamically* determine organizational control.

Figure 8. Admin Role: Create Page

Scoping Controlled Organizations

For each directly assigned, controlled organization included in an admin role, you can define the scope of objects on which a user can act. You can choose to include or exclude one or more objects that are generally available to each organization controlled by the user.

For example, you might choose to restrict the access of a user who can create, update, and delete users within an organization that includes a wide range of resources to a specific subset of resources in that organization. To do this, you could create an admin role with these characteristics:

- Name — NT User Administrator
- Capabilities — Create User, Update User, Delete User
- Controlled Organization — *OrganizationName*
- Included Resources — NT

To do this, make selections in the Select Objects to Include / Exclude area of the Create Admin Role page.

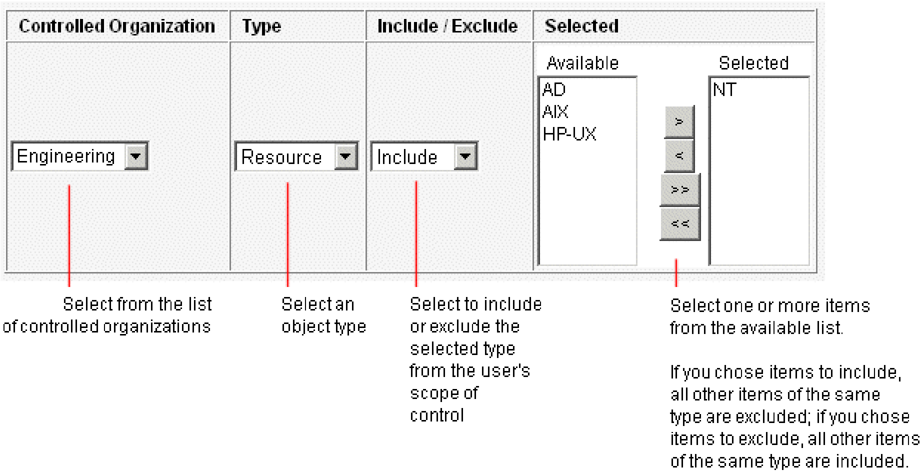

Controlled Organization
Type
Include / Exclude
Selected
Available
Selected
AD
AIX
HP-UX
NT
Engineering
Resource
Include
>
<
>>
<<
Select from the list of controlled organizations
Select an object type
Select to include or exclude the selected type from the user's scope of control
Select one or more items from the available list.
If you chose items to include, all other items of the same type are excluded; if you chose items to exclude, all other items of the same type are included.

Figure 9. Admin Role: Include/Exclude Selections for Controlled Organizations

If you include an item in both an include and an exclude list, it is excluded from the admin role.

Assigning User Forms to an Admin Role

You can specify a user form as an attribute of an admin role. The admin assigned the admin role will use this user form when he creates or edits users in the organizations controlled by that admin role. A user form assigned through an admin role overrides any user form that is inherited from the organization of which the admin is a member. It does not override a user form that is directly assigned to the admin.

The user form that will be used when editing a user is determined in this order of precedence:

- If a user form is assigned directly to the admin, then it is used.
- If no user form is assigned directly to the admin, but the admin is assigned an admin role that:
  - controls the organization of which the user being created or edited is a member, and
  - specifies a user form

  then that user form is used.
- If no user form is assigned directly to the admin, or assigned indirectly through an admin role, then the user form assigned to the admin's member organizations (starting with the admin's member organization and going up to just below Top) is used.
- If none of the admin's member organizations are assigned a user form, then the default user form is used.

If an admin is assigned more than one admin role that controls the same organization but specifies different user forms, then an error is displayed when he attempts to create or edit a user in that organization. If an admin attempts to assign two or more admin roles that control the same organization but specify different user forms, then an error is displayed. Changes cannot be saved until the conflict is resolved.

Capabilities Rules and Controlled Organizations Rules

The following samples show how you might set up a capabilities rule or controlled organizations rule that can dynamically control the assigned capabilities or controlled organizations given to a user assigned an admin role.

Note For information about creating and working with rules in Identity Manager, see *Identity Manager Deployment Tools*.

Capabilities Rule: Key Definitions and Inclusions

- A capabilities rule must include the `authType='CapabilitiesRule'` entry. This is required to ensure that you can select the rule from within the admin role page.
- The context is the currently authenticated Identity Manager user's user view.
- In the following sample rule, the defined variable (`defvar`) `'user groups'` gets the currently authenticated Identity Manager user's account on the Windows Active Directory server named `'ranger-AD'`, and returns the list of groups of which the user is currently a member.

- The conditional logic (`cond`) checks to see if the currently authenticated Identity Manager user is a member of the `'manager'` group. If yes, the user is assigned the Identity Manager capabilities Login Administrator and Resource Administrator. If no, then no Identity Manager capabilities are assigned.

Sample Capabilities Rule

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='CapabilitiesRule' name='If Manager'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
         <ref>context</ref>
            <s>ranger-AD</s>
            <s>User</s>
         <ref>accountInfo.accounts[ranger-AD].accountId</ref>
         <map>
            <s>searchAttrsToGet</s>
               <list>
            <s>memberOf</s>
               </list>
         </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
         <ref>user groups</ref>
            <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
      </contains>
      <list>
         <s>Login Administrator</s>
         <s>Resource Administrator</s>
      </list>
   </cond>
   </block>
   <MemberObjectGroups>
      <ObjectRef type='ObjectGroup'
id='#ID#ObjectGroup:Waveset'        name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

Controlled Organizations Rule: Key Definitions

- A controlled organizations rule must include the `authType='ControlledOrganizationsRule'` entry. This enables you to select the rule from within the admin role page.
- The context is the currently authenticated Identity Manager user's user view.
- In the following sample rule, the defined variable (`defvar`) `'user groups'` gets the currently authenticated Identity Manager user's account on the Windows Active Directory server named `'ranger-AD'` and returns the list of groups of which the user is currently a member.
- The conditional logic (`cond`) checks to see if the currently authenticated Identity Manager user is a member of the `'manager'` group. If yes, the user is assigned control of the Identity Manager `'Waveset'` organization. If no, then no organizational control is assigned.

Sample Controlled Organizations Rule

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='ControlledOrganizationsRule' name='Get managed
departments'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
            <ref>context</ref>
               <s>ranger-AD</s>
               <s>User</s>
            <ref>accountInfo.accounts[ranger-
AD].accountId</ref>
            <map>
               <s>searchAttrsToGet</s>
            <list>
               <s>memberOf</s>
            </list>
            </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
      <ref>user groups</ref>
         <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
   </contains>
      <list>
         <s>Waveset</s>
      </list>
     </cond>
   </block>
   <MemberObjectGroups>
   <ObjectRef type='ObjectGroup' id='#ID#ObjectGroup:Waveset'
       name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

Understanding Email Templates

Identity Manager uses email templates to deliver information and requests for action to users and approvers. The system includes templates for:

- **Account Creation Approval** — Sends notification to an approver that a new account is awaiting his approval. The system sends this notification when the Provisioning Notification Option for the associated role is set to approval.
- **Account Creation Notification** — Sends notification that an account has been created with a particular role assignment. The system sends this notification when one or more administrators are selected in the Notification recipients field on the Create Role or Edit Role pages.
- **Password Reset** — Sends notification of a Identity Manager password reset. Depending on the Reset Notification Option value selected for the associated Identity Manager policy, the system displays notification immediately (in the Web browser) to the administrator resetting the password or emails the user whose password is being reset.
- **Password Synchronization Notice** — Notifies the user that a password change has completed successfully on all resources. The notification lists which resources were updated successfully and indicates the origin of the password change request.
- **Password Synchronization Failure Notice** — Notifies the user that the password change was not successful on all resources. The notification provides a list of errors and indicates the origin of the password change request.

- **Reconcile Account Event**, **Reconcile Resource Event**, **Reconcile Summary** — Called from the Notify Reconcile Response, Notify Reconcile Start, and Notify Reconcile Finish default workflows, respectively. Notification is sent as configured in each workflow.
- **Report** — Sends a generated report to a specified list of recipients.
- **Request Resource** — Sends notification to a resource administrator that a resource has been requested. The system sends this notification when an administrator requests a resource from the Resources area.
- **Retry Notification** — Sends notification to an administrator that a particular operation has been unsuccessfully attempted on a resource a specified number of times.
- **Risk Analysis** — Sends a risk analysis report. The system sends this report when one or more email recipients are specified as part of a resource scan.
- **Temporary Password Reset** — Sends notification to the user or role approver that a temporary password has been provided for the account. Depending on the Password Reset Notification Option value selected for the associated Identity Manager policy, the system displays notification immediately (in the Web browser) to the user, emails the user, or emails the role approvers.

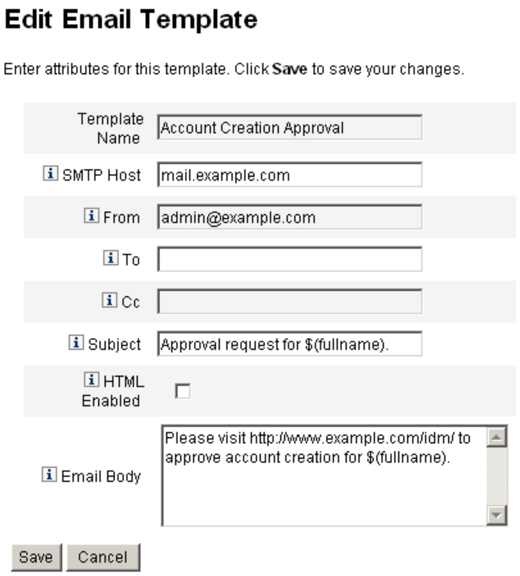
Customizing Email Templates

You can customize email templates to provide specific directions to the recipient, telling him how to accomplish a task or see results. For example, you might want to customize the Account Creation Approval template to direct an approver to an account approval page:

Please go to http://host.example.com:8080/idm/approval/approval.jsp to approve account creation for `$(fullname)`.

To customize the Account Creation Approval template:

1. From the menu bar, select **Configure**.
2. On the Configure page, select **Email Templates**.
3. Click to select the Account Creation Approval template.



Edit Email Template

Enter attributes for this template. Click **Save** to save your changes.

Template Name	Account Creation Approval
SMTP Host	mail.example.com
From	admin@example.com
To	
Cc	
Subject	Approval request for $(fullname).
HTML Enabled	□
Email Body	Please visit http://www.example.com/idm/ to approve account creation for $(fullname).

Figure 10. Customize Email Template

4. Enter details for the template:
   - In the SMTP Host field, enter the SMTP server name so that email notification can be sent.
   - In the From field, customize the originating email address.
   - In the To and Cc fields, enter one or more email addresses or Identity Manager accounts that will be the recipients of the email notification.
   - In the Email Body field, customize the content to provide a pointer to your Identity Manager location.
5. Click **Save**.

Note You can also modify email templates by using the Business Process Editor (BPE). For more information on the BPE, see *Identity Manager Deployment Tools.*

HTML and Links in Email Templates

You can insert HTML-formatted content into an email template to display in the body of an email message. Content can include text, graphics, and Web links to information. To enable HTML-formatted content, select the HTML Enabled option.

Allowable Variables in the Email Body

You can also include references to variables in the email template body, in the form $(*Name*); for example: `Your password $(password) has been recovered.`

Allowable variables for each template are defined in the following table.

Template	Allowable Variables
Password Reset	`$(password)` **– newly generated password**
Update Approval	`$(fullname)` **– user's full name** `$(role)` **– user's role**
Update Notification	`$(fullname)` **– user's full name** `$(role)` **– user's role**
Report	`$(report)` **– generated report** `$(id)` **– encoded ID of the task instance** `$(timestamp)` **– time when email was sent**
Request Resource	`$(fullname)` **– user's full name** `$(resource)` **– resource type**
Risk Analysis	`$(report)` **– risk analysis report**
Temporary Password Reset	`$(password)` **– newly generated password** `$(expiry)` **– password expiration date**

Table 2. Email Template Variables

Audit Group Configuration

Setting up audit configuration groups allows you to record and report on system events you select.

To configure audit configuration groups, select **Configure** from the menu bar, and then select **Audit Events**.

The Audit Events page shows the list of audit configuration groups, each of which may contain one or more events. For each group, you can record successful events, failed events, or both.

Click an audit configuration group in the list to display the Edit Audit Configuration Group page. This page lets you select the types of audit events to be recorded as part of an audit configuration group in the system audit log.

Editing Events in the Audit Configuration Group

To edit events in the group, you can add or delete actions for an object type. To do this, move items in the Actions column from the Available to the Selected area for that object type, and then click **OK**.

Adding Events to the Audit Configuration Group

To add an event to the group, click **New**. Identity Manager adds an event at the bottom of the page. Select an object type from the list in the Object Type column, and then move one or more items in the Actions column from the Available area to the Selected area for the new object type. Click **OK** to add the event to the group.

Remedy Integration

You can integrate Identity Manager with a Remedy server, enabling it to send Remedy tickets according to a specified template.

Set up Remedy integration in two areas of the Administrator interface:

- **Remedy server settings** — Set up Remedy configuration by creating a Remedy resource from the Resources area. After setting up the resource, test the connection to ensure integration is enabled.
- **Remedy template** — After setting up the Remedy resource, define a Remedy template. To do this, select **Configure**, and then select **Remedy Integration**. You will then select the Remedy schema and resource.

Creation of Remedy tickets is configured through Identity Manager workflow. Depending on your preferences, a call can be made at an appropriate time that uses the defined template to open a Remedy ticket. For more information about configuring workflows, see *Identity Manager Workflows, Forms, and Views.*

Configuring Identity Manager Server Settings

You can edit server-specific settings so that Identity Manager servers run only specific tasks. To do this, select **Configure**, and then select **Servers**.

To edit settings for an individual server, select a server in the list on the Configure Servers page. Identity Manager displays the Edit Server Settings page, where you can edit reconciler and scheduler settings.

Reconciler Settings

By default, reconciler settings display on the Edit Server Settings page. You can accept the default value or de-select the Use default option to specify a value:

- **Parallel Resource Limit** — Specify the maximum number of resources that the reconciler can process in parallel.
- **Minimum Worker Threads** — Specify the number of processing threads that the reconciler will always keep alive.
- **Maximum Worker Threads** — Specify the maximum number of processing threads that the reconciler can use. The reconciler will only start as many threads as the workload requires; this places a limit on that number.

Scheduler Settings

Click **Scheduler** on the Edit Server Settings page to display scheduler options. You can accept the default value or de-select the Use default option to specify a value:

- **Scheduler Startup** — Select a startup mode for the scheduler:
  - **Automatic** — Starts when the server is started. This is the default startup mode.
  - **Manual** — Starts when the server is started, but remains suspended until manually started.
  - **Disabled** — Does not start when the server is started.
- **Tracing Enabled** — Select this option to activate scheduler debug tracing to standard output.
- **Task Restrictions** — Specify the set of tasks that can execute on the server. To do this, select one or more tasks from the list of available tasks. The list of selected tasks can be an inclusion or exclusion list depending on the option you select. You can choose to allow all tasks except those selected in the list (the default behavior), or allow only the selected tasks.

Click **Save** to save changes to the server settings.

Editing Default Server Settings

The Default Server Settings feature lets you set the default settings for all Identity Manager servers. The servers inherit these settings unless you select differently in the individual server settings pages. To edit the default settings, click **Edit Default Server Settings**. The Edit Default Server Settings page displays the same options as the individual server settings pages.

Changes you make to each default server setting is propagated to the corresponding individual server setting, unless you have de-selected the Use default option for that setting.

Click **Save** to save changes to the server settings.

Signed Approvals

Use the following information and procedures to set up digitally signed approvals. Steps and examples follow for:

- Configuring signed approvals (server-side and client-side)
- Adding certificates and CRL to Identity Manager
- Signing approvals

Configuring Signed Approvals

Follow these steps to configure signed approvals.

Server-Side Configuration

To enable server-side configuration:

1. In the system configuration, set `security.nonrepudiation.signedApprovals=true`
2. Add your certificate authority (CA)'s certificates as trusted certificates. To do this, you must first obtain a copy of the certificates.

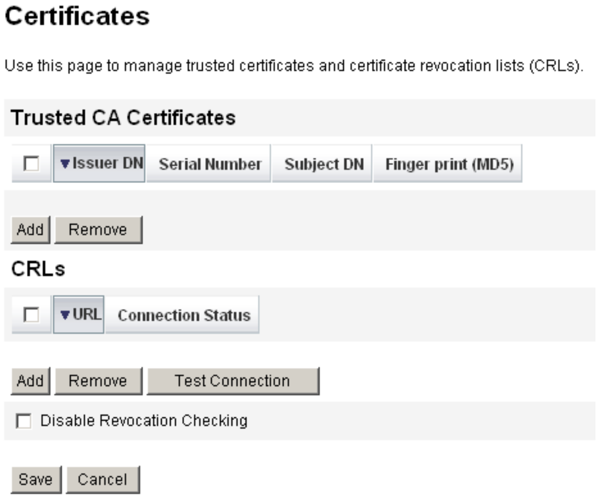
   For example, if you are using a Microsoft CA, follow steps similar to these:

   a. Go to http://***IPAddress***/certsrv and log in with administrative privileges.

   b. Select Retrieve the CA certificate or certificate revocation list, and then click **Next**.

   c. Download and save the CA certificate.
3. Add the certificate to Identity Manager as a trusted certificate:

   a. From the Administrator interface, select **Configure**, and then select **Certificates**. Identity Manager displays the Certificates page.



Certificates

Use this page to manage trusted certificates and certificate revocation lists (CRLs).

Trusted CA Certificates

CRLs

□ Disable Revocation Checking

Figure 11. Certificates

   b. In the Trusted CA Certificates area, click **Add**. Identity Manager displays the Import Certificate page.

   c. Browse to and then select the trusted certificate, and then click **Import**.

   The certificate now displays in the list of trusted certificates.
4. Add your CA's certificate revocation list (CRL):

   a. In the CRLs area of the Certificates page, click **Add**.

   b. Enter the URL for the CA's CRL.

Notes:

- The certificate revocation list (CRL) is a list of certificate serial numbers that have been revoked or are not valid.
- The URL for the CA's CRL may be http or LDAP.
- Each CA has a different URL where CRLs are distributed; you can determine this by browsing the CA certificate's CRL Distribution Points extension.

5. Click **Test Connection** to verify the URL.
6. Click **Save**.
7. Sign applets/ts1.jar using jarsigner.

Note Refer to http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html for more information. The `ts1.jar` file provided with Identity Manager is signed using a self-signed certificate, and should not be used for production systems. In production, this file should be re-signed using a code-signing certificate issued by your trusted CA.

Client-Side Configuration

Follow these steps to enable client-side configuration:

Prerequisites

Your client system must be running a Web browser with JRE 1.4 or higher.

Procedure

Obtain a certificate and private key, and then export them to a PKCS#12 keystore.

For example, if using a Microsoft CA, you would follow steps similar to these:

1. Using Internet Explorer, browse to http://***IPAddress***/certsrv, and then log in with administrative privileges.
2. Select Request a certificate, and then click **Next**.
3. Select Advanced request, and then click **Next**.
4. Click **Next**.
5. Select User for Certificate Template.
6. Select these options:
   a. Mark keys as exportable
   b. Enable strong key protection
   c. Use local machine store
7. Click **Submit**, and then click **OK**.

8. Click **Install this certificate**.
9. Select Run —> mmc to launch mmc.
10. Add the Certificate snap-in:
    a. Select Console—>Add/Remove Snap-in.
    b. Click **Add...**
    c. Select Computer account.
    d. Click **Next**, and then click **Finish**.
    e. Click **Close**.
    f. Click **OK**.
    g. Go to Certificates—>Personal—>Certificates.
    h. Right-click Administrator All Tasks—>Export.
    i. Click **Next**.
    j. Click **Next** to confirm exporting the private key.
    k. Click **Next**.
    l. Provide a password, and then click **Next**.
    m. File ***CertificateLocation***.
    n. Click **Next**, and then click **Finish**. Click **OK** to confirm.

Signing Approvals

Follow these steps to sign an approval.

1. from the Identity Manager Administrator interface, select **Approvals**.
2. Select an approval from the list.
3. Enter comments for the approval, and then click **Approve**.

   Identity Manager prompts you and asks whether to trust the applet.
4. Click **Always**.

   Identity Manager displays a dated summary of the approval.
5. Enter or click Browse to locate the keystore location (the location provided in Step 10m of the server-side configuration procedure).
6. Enter the keystore password (the password provided in Step 10l of the server-side configuration procedure).
7. Click **Sign** to approve the request.

Signing Subsequent Approvals

After signing an approval, subsequent approval actions require only that you enter the keystore password and then click **Sign**. (Identity Manager should remember the keystore location from the previous approval.)

Viewing the Transaction Signature

Follow these steps to view the transaction signature in an Identity Manager AuditLog report.

1. From the Identity Manager Administrator interface, select **Reports**.
2. On the Run Reports page, select AuditLog Report from the New... list of options.
3. In the Report Title field, enter a title (for example, “Approvals”).
4. In the Organizations selection area, select all organizations.
5. Select the Actions option, and then select Approve.
6. Click **Save** to save the report and return to the Run Reports page.
7. Click **Run** to run the Approvals report.
8. Click the details link to see transaction signature information, including:
   - issuer
   - subject
   - certificate serial number
   - message signed
   - signature
   - signature algorithm

6 Data Synchronization and Loading

This chapter provides information and procedures for using Identity Manager data synchronization and loading features.

Topics in this Chapter

In this chapter, you will learn more about:

- Identity Manager data synchronization tools (discovery, reconciliation, and ActiveSync)
- How to use the discovery, reconciliation, and ActiveSync features to keep data current

Data Synchronization Tools: Which to Use?

Follow these guidelines when selecting Identity Manager data synchronization tools to perform a task.

If you want to:	Then choose this feature:
Initially *pull* resource accounts into Identity Manager, without viewing before loading	Load from Resource
Initially *pull* resource accounts into Identity Manager, optionally viewing and editing data before loading	Extract to File, Load from File
Periodically *pull* resource accounts into Identity Manager, taking action on each account according to configured policy	Reconcile with Resources
Push or *pull* resource account changes into Identity Manager	ActiveSync (multiple resource implementations)

Discovery

Identity Manager account discovery features help facilitate rapid deployment and speed account creation tasks. These features are:

- **Extract to File** — Extracts the resource accounts returned by a resource adapter to a file (in CSV or XML format). You can manipulate this file before importing the data into Identity Manager.
- **Load from File** — Reads accounts in a file (in CSV or XML format) and loads them into Identity Manager.
- **Load from Resource** — Combines the other two discovery features, extracting accounts from a resource and loading them directly into Identity Manager.

Using these tools, you can create new Identity Manager users or correlate accounts on a resource with existing Identity Manager user accounts.

Extract to File

Use this feature to extract resource accounts from a resource to an XML or CSV text file. Doing this allows you to view and make changes to extracted data before importing it into Identity Manager.

To extract accounts:

1. From the menu bar, select **Accounts**, and then select **Extract to File**.
2. Select a resource from which to extract accounts.
3. Select a file format for the output account information. You can extract data to an XML file, or to a text file with account attributes arranged in comma-separated value (CSV) format.
4. Click **Download**. Identity Manager displays a File Download dialog, which lets you choose to save or view the extracted file.

Tip If you choose to open the file, you may have to select a program to view it.

Load from File

Use this feature to load resource accounts — either those extracted from a resource through Identity Manager, or from another file source — into Identity Manager. A file created by the Identity Manager Extract to File feature is in XML format. If you are loading a list of new users, the data file typically is in CSV format.

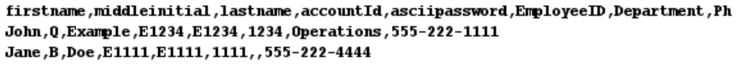
About CSV File Format

Often, accounts to be loaded are listed in a spreadsheet (such as Excel) and saved in comma-separated value (CSV) format for loading into Identity Manager. CSV file contents must follow these format guidelines:

Line 1 — Lists column headings or schema attributes for each field, separated by commas.

Lines 2 to end — Lists values for each attribute defined in line 1, separated by commas. If data does not exist for a field value, that field must be represented by adjacent commas.

For example, the first three lines of a file might look like this:



```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

In this example, the second user (Jane Doe) does not have a department. The missing value is represented by adjacent commas (,,).

To load accounts:

1. From the menu bar, select **Accounts**, and then select **Load from File.**

   Identity Manager displays the Load from File page, which lets you specify load options before continuing:

   - **User Form** — When load creates an Identity Manager user, the user form assigns an organization as well as roles, resources, and other attributes. Select the user form to apply to each resource account.
   - **Account Correlation Rule** — An account correlation rule selects Identity Manager users that might own each unowned resource account. Given the attributes of an unowned resource account, a correlation rule returns a list of names or a list of attribute conditions that will be used to select potential owners. Select a rule to look for Identity Manager users that may own each unowned resource account.
   - **Account Confirmation Rule** — An account confirmation rule eliminates any non-owner from the list of potential owners that the correlation rule selects. Given the full View of an Identity Manager user and the attributes of an unowned resource account, a confirmation rule returns true if the user owns the

account and false otherwise. Select a rule to test each potential owner of a resource account. If you select No Confirmation Rule, Identity Manager accepts all potential owners without confirmation.

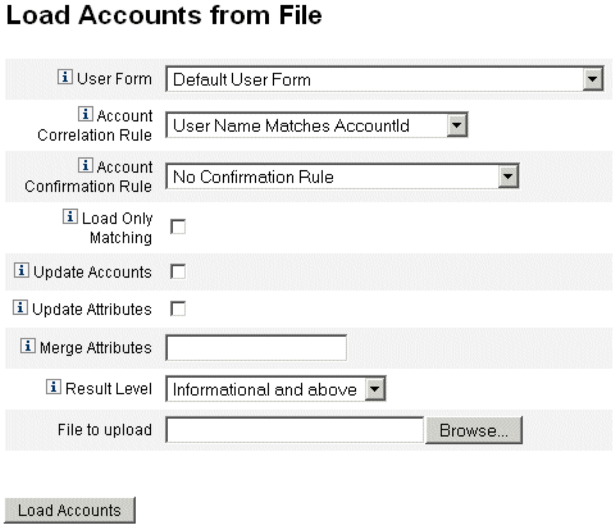
Note In your environment, if the correlation rule will select at most one owner for each account, then you do not need a confirmation rule.

- **Load Only Matching** — Select to load into Identity Manager only those accounts that match an existing Identity Manager user. If you select this option, load will discard any unmatched resource account.
- **Update Attributes** — Select to replace the current Identity Manager user attribute values with the attribute values from the account being loaded.
- **Merge Attributes** — Enter one or more attribute names, separated by commas, for which values should be combined (eliminating duplicates) rather than overwritten. Use this option only for list-type attributes, such as groups and mailing lists. You must also select the Update Attributes option.
- **Result Level** — Select a threshold at which the load process will record an individual result for an account:
  - **Errors only** — Record an individual result only when loading an account produces an error message.
  - **Warnings and errors** — Record an individual result when loading an account produces a warning or an error message.
  - **Informational and above** — Record an individual result for every account. This causes the load process to run more slowly.

2. In the File to Upload field, specify a file to load, and then click **Load Accounts**.

Notes:

- If the input file does not contain a user column, you must select a confirmation rule for the load to proceed correctly.
- The task instance name associated with the load process is based on the input file name; therefore, if you re-use a file name, then the task instance associated with the latest load process will overwrite any previous task instances.



Load Accounts from File

User Form	Default User Form
Account Correlation Rule	User Name Matches AccountId
Account Confirmation Rule	No Confirmation Rule
Load Only Matching	□
Update Accounts	□
Update Attributes	□
Merge Attributes	
Result Level	Informational and above
File to upload	

Figure 1. Load from File

If an account matches (or correlates with) an existing user, the load process will merge the account into the user. The process will also create a new Identity Manager user from any input account that does not correlate (unless Correlation Required is specified).

The `bulkAction.maxParseErrors` configuration variable sets a limit on the number of errors that can be found when a file is loaded. By default, the limit is 10 errors. If the `maxParseErrors` number of errors is found, then parsing stops.

Load from Resource

Use this feature to directly extract and import accounts into Identity Manager according to the load options you specify.

To import accounts, select **Accounts** from the menu bar, and then select **Load from Resource**.

Note Identity Manager lets you specify load options before continuing. Load options available from the Load from Resource page, and the actions that result, are the same as those on the Load from File page.

Reconciliation

Use the reconciliation feature to highlight inconsistencies between the resource accounts on Identity Manager and the accounts that actually exist on a resource, and to periodically correlate account data.

Because reconciliation is designed for ongoing comparison, it:

- Diagnoses account situations more specifically and supports a wider range of responses than the discovery process
- Can be scheduled (discovery cannot)
- Offers an incremental mode (discovery is always full mode).
- Can detect native changes (discovery cannot)

You can also configure reconciliation to launch an arbitrary workflow at each of the following points in processing a resource:

- Before reconciling any account
- For each account
- After reconciling all accounts

Access Identity Manager reconciliation features from the Resources area. The Resources list shows when each resource was last reconciled and its current reconciliation status.

About Reconciliation Policies

Reconciliation policies allow you to establish a set of responses, by resource, for each reconciliation task. Within a policy, you select the server to run reconciliation, determine how often and when reconciliation takes place, and set responses to each situation encountered during reconciliation. You can also configure reconciliation to detect changes made natively (not made through Identity Manager) to account attributes.

Editing Reconciliation Policies

To edit a reconciliation policy:

1. Select **Resources** from the menu bar.
2. Select a resource in the Resources list hierarchy.
3. Select Edit Reconciliation Policy from the Resource Actions options list.

   Identity Manager displays the Edit Reconciliation Policy page, where you can make these policy selections:

   - **Reconciliation Server** — In a clustered environment, each server may run reconciliation. Specify which Identity Manager server will run reconciliation against resources in the policy.
   - **Reconciliation Modes** — Reconciliation can be performed in different modes, which optimize different qualities:
     - **Full reconciliation** — Optimizes for thoroughness at a cost of speed.
     - **Incremental reconciliation** — Optimizes for speed at the expense of some thoroughness.

     Select the mode in which Identity Manager should run reconciliation against resources in the policy. Select Do not reconcile to disable reconciliation for targeted resources.
   - **Full Reconciliation Schedule** — If full mode reconciliation is enabled, it is performed automatically on a fixed schedule. Specify how frequently full reconciliation should be run against resources in the policy. Select the Inherit option to inherit the indicated schedule from a higher-level policy.
   - **Incremental Reconciliation Schedule** — If incremental mode reconciliation is enabled, it is performed automatically on a fixed schedule. Specify how frequently incremental reconciliation should be run against resources in the policy. Select the Inherit option to inherit the indicated schedule from a higher-level policy.

Note Not all resources support incremental reconciliation.

   - **Attribute-level Reconciliation** — Reconciliation can be configured to detect changes made natively (that is, not made through Identity Manager) to account attributes. Specify whether reconciliation should detect native changes to the attributes specified in **Reconciled Account Attributes**.
   - **Account Correlation Rule** — An account correlation rule selects Identity Manager users that might own each unowned resource account. Given the attributes of an unowned resource account, a correlation rule returns a list of names or a list of attribute conditions that will be used to select potential owners. Select a rule to look for Identity Manager users that may own each unowned resource account.

- **Account Confirmation Rule** — An account confirmation rule eliminates any non-owner from the list of potential owners that the correlation rule selects. Given the full View of an Identity Manager user and the attributes of an unowned resource account, a confirmation rule returns true if the user owns the account and false otherwise. Select a rule to test each potential owner of a resource account. If you select No Confirmation Rule, Identity Manager accepts all potential owners without confirmation.

Note In your environment, if the correlation rule will select at most one owner for each account, then you do not need a confirmation rule.

- **Proxy Administrator** — Specify the administrator to use when reconciliation responses are performed. The reconciliation can perform only those actions that the designated proxy administrator is permitted to do. The response will use the user form (if needed) associated with this administrator.

  You can also select the No Proxy Administrator option. When selected, reconciliation results are available to view, but no response actions or workflows are run.

- **Situation Options** (and Response)— Reconciliation recognizes several types of situations. Specify in the Response column any action reconciliation should take:
  - **CONFIRMED** — The expected account exists.
  - **DELETED** — The expected account does not exist.
  - **FOUND** — The reconciliation process found a matching account on an assigned resource.
  - **MISSING** — No matching account exists on a resource assigned to the user.
  - **COLLISION** — Two or more Identity Manager users are assigned the same account on a resource.
  - **UNASSIGNED** — The reconciliation process found a matching account on a resource not assigned to the user.
  - **UNMATCHED** — The account does not match any users.
  - **DISPUTED** — The account matches more than one user.

  Select from one of these response options (available options vary by situation):
  - **Create new Identity Manager user based on resource account** — Runs the user form on the resource account attributes to create a new user. The resource account is not updated as a result of any changes.
  - **Create resource account for Identity Manager user** — Recreates the missing resource account, using the user form to regenerate the resource account attributes.
  - **Delete resource account** and **Disable resource account** — Deletes/disables the account on the resource.

  - **Link resource account to Identity Manager user** and **Unlink resource account from Identity Manager user** — Adds or removes the resource account assignment to or from the user. No form processing is performed.
- **Pre-reconciliation Workflow** — Reconciliation can be configured to run a user-specified workflow prior to reconciling a resource. Specify the workflow that reconciliation should run. Select Do not run workflow if no workflow should be run.
- **Per-account Workflow** — Reconciliation can be configured to run a user-specified workflow after responding to the situation of a resource account. Specify the workflow that reconciliation should run. Select Do not run workflow if no workflow should be run.
- **Post-reconciliation Workflow** — Reconciliation can be configured to run a user-specified workflow after completing reconciliation for a resource. Specify the workflow that reconciliation should run. Select Do not run workflow if no workflow should be run.

Click **Save** to save policy changes.

Starting Reconciliation

Two options are available for starting reconciliation tasks:

- Reconciliation schedule — You can set a reconciliation schedule on the Edit Reconciliation Policy page, which runs reconciliation at regular intervals.
- Immediate reconciliation — Runs reconciliation immediately. To do this, select a resource in the resources list, and then select one of the following options in the Resource Actions list:
  - Full Reconcile Now
  - Incremental Reconcile Now

  Reconciliation will run according to the parameters you have set in the policy. If the policy has a regular schedule set for reconciliation, it will continue to run as specified.

Canceling Reconciliation

To cancel reconciliation, select the resource, and then select Cancel Reconciliation from the Resource Actions list.

Viewing Reconciliation Status

The Status column in the Resources list reports several reconciliation status conditions. These are:

- **unknown** — Status is not known. Results for the latest reconciliation task are not available.
- **disabled** — Reconciliation is disabled.
- **failed** — The latest reconciliation failed to complete.
- **success** — The latest reconciliation completed successfully.
- **completed with errors** — The latest reconciliation completed, but with errors.

Note You must refresh this page to view changes to status (the information does not automatically refresh).

Detailed status information for each account on a resource is available. Select a resource in the list, and then select View Reconciliation Status from the Resource Actions list.

Working with the Account Index

The Account Index records the last known state of each resource account known to Identity Manager. It is primarily maintained by reconciliation, but other Identity Manager functions will also update the Account Index, as needed.

Note Discovery tools do not update the Account Index.

Searching the Account Index

To search the account index, select Search Account Index from the Resource Actions list.

Select a search type, and then enter or select search attributes. Click **Search** to find accounts that match all search criteria.

- **Resource account name** — Select this option, select one of the modifiers (starts with, contains, or is), and then enter part or all of an account name.
- **Resource is one of** — Select this option, and then select one or more resources from the list, to find reconciled accounts that reside on the specified resources.
- **Owner** — Select this option, select one of the modifiers (starts with, contains, or is), and then enter part or all of an owner name. To search for unowned accounts, search for accounts in the UNMATCHED or DISPUTED situation.

- **Situation is one of** — Select this option, and then select one or more situations from the list to find reconciled accounts in the specified situations.

Click **Search** to search for accounts according to your search parameters. To limit the results of the search, optionally specify a number in the Limit results to first field. The default limit is the first 1000 accounts found.

Click **Reset Query** to clear the page and make new selections.

Examining the Account Index

It is also possible to view all Identity Manager user accounts and optionally reconcile them on a per-user basis. To do this, select **Resources**, and then select **Examine Account Index**.

The table displays all of the resource accounts that Identity Manager knows about (whether or not an Identity Manager user owns the account). This information is grouped by resource or by Identity Manager organization. To change this view, make a selection from the Change index view list.

Working with Accounts

To work with the accounts on a resource, select the Group by resource index view. Identity Manager displays folders for each type of resource. Navigate to a specific resource by expanding a folder. Click + or - next to the resource to display all resource accounts that Identity Manager knows about.

Note Accounts that have been added directly to the resource since the last reconciliation on that resource are not displayed.

Depending on the current situation of a given account, you may be able to perform several actions. You can also view account details or choose to reconcile that one account.

Working with Users

To work with Identity Manager users, select the Group by user index view. In this view, Identity Manager users and organizations are displayed in a hierarchy similar to the Accounts List page. To see accounts currently assigned to a user in Identity Manager, navigate to the user and click the indicator next to the user name. The user’s accounts and the current status of those accounts that Identity Manager knows about are displayed under the user name.

Depending on the current situation of a given account, you may be able to perform several actions. You can also view account details or choose to reconcile that one account.

ActiveSync Adapters

The Identity Manager ActiveSync feature allows information that is stored in an *authoritative external resource* (such as an application or database) to synchronize with Identity Manager user data. Setting up active synchronization for an Identity Manager resource enables it to “listen” or poll for changes to the authoritative resource.

Setting Up Active Synchronization

Use the Active Sync Wizard in the Identity Manager resources area to set up active synchronization. This wizard leads you through a varying set of steps, depending on the choices you make, to set up active synchronization for a resource.

To launch the Active Sync Wizard, select a resource in the resources list, and then select Active Sync Wizard from the Resource Actions list of options.

The Active Sync Wizard Synchronization Mode page appears.

Synchronization Mode

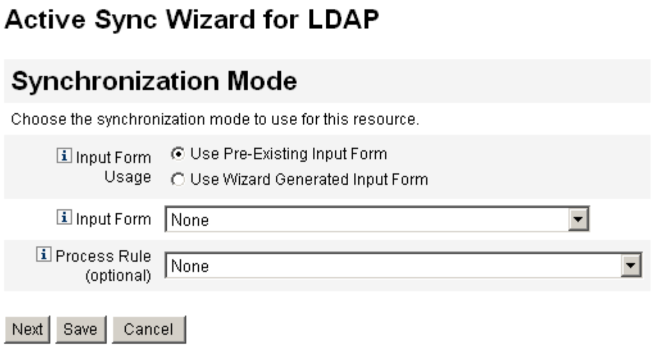
The Synchronization Mode page lets you determine the range of configuration options you can choose during active synchronization setup.

Select from these options:

Input Form Usage — Select the mode to use when setting up active synchronization. You can choose to use a pre-existing form, which limits configuration choices for this resource. Alternatively, you can use a form that is generated by the Active Sync Wizard, which offers a complete set of configuration choices.

- If you select Pre-Existing Input Form (the default), then make selections for these options:
  - › **Input Form** — Select an input form that will process data updates. This optional configuration item allows attributes to be transformed before they are saved on the accounts.

- › **Process Rule** — Optionally select a process rule to run for each incoming account. This selection overrides all other options. If you specify a process rule, the process will be run for every row, regardless of other settings on the resource. It can be either a process name, or a rule evaluating to a process name.



Active Sync Wizard for LDAP

Synchronization Mode

Choose the synchronization mode to use for this resource.

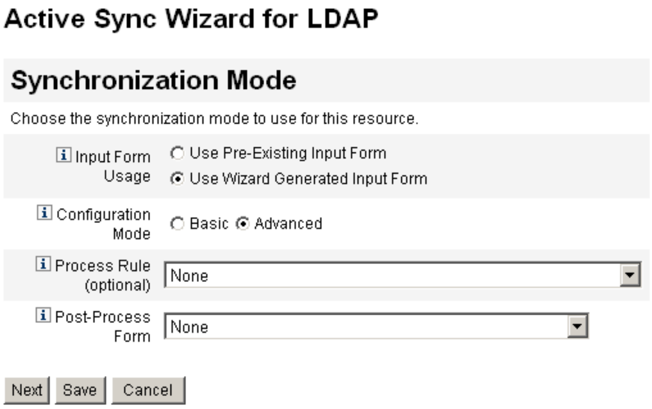
Input Form Usage: ● Use Pre-Existing Input Form ○ Use Wizard Generated Input Form

Input Form: None

Process Rule (optional): None

Figure 2. Active Sync Wizard: Synchronization Mode, Pre-Existing Form Selections

- If you select Use Wizard Generated Input Form, then make selections for these options:
  - **Configuration Mode** — Select whether to use basic or advanced mode within the Active Sync Wizard. Basic mode is the default option. If you select advanced mode, you can define event types and set process rules.
  - **Process Rule** — (Displays with advanced configuration mode only.) Optionally select a process rule to run for each incoming account. This selection overrides all other options. If you specify a process rule, the process will be run for every row, regardless of other settings on the resource. It can be either a process name, or a rule evaluating to a process name.
  - **Post-Process Form** — (Displays with advanced configuration mode only.) Optionally select a form to run, in addition to the form generated by the Active Sync Wizard. This form overrides any settings from the Active Sync Wizard.



Active Sync Wizard for LDAP

Synchronization Mode

Choose the synchronization mode to use for this resource.

Input Form Usage: ○ Use Pre-Existing Input Form ● Use Wizard Generated Input Form

Configuration Mode: ○ Basic ● Advanced

Process Rule (optional): None

Post-Process Form: None

Figure 3. Active Sync Wizard: Synchronization Mode, Wizard Generated Form Selections

Click **Next** to continue with the wizard. The Active Sync Running Settings page appears.

Running Settings

This page lets you establish settings for active sync:

- Startup
- Polling
- Logging

Startup Settings

Make selections for active sync startup:

- **Startup Type** — Select one of:
  - **Automatic** or **Automatic with failover** — Starts the authoritative source when the Identity system is started.
  - **Manual** — Requires that an administrator start the authoritative source.
  - **Disabled** — Disables the resource.
- **Proxy Administrator** — Select the administrator who will process updates. All actions will be authorized through capabilities assigned to this administrator. You should select a proxy administrator with an empty user form.

Polling Settings

If you set a polling start date and time that is in the future, then polling will begin when specified. If you set a polling start date and time that is in the past, then Identity Manager determines when to begin polling based on this information and the polling interval. For example:

- You configure active synchronization for the resource on July 18, 2005 (Tuesday)
- You set the resource to poll weekly, with a start date of July 4, 2005 (Monday) and time of 9:00 a.m.

In this case, the resource will begin polling on July 25, 2005 (the following Monday).

If you do not specify a start date or time, then the resource will poll immediately. However, setting a start date and time is recommended; otherwise, each time the application server is restarted, all resources configured for active synchronization will begin polling immediately.

Make selections to set up polling:

- **Poll Every** — Specify how often to poll. Enter a number, and then select the unit of time (Days, Hours, Minutes, Months, Seconds, or Weeks). Minutes is the default unit.
- **Polling Start Date** —- Enter the day that the first scheduling interval should start, in yyyyMMdd format.
- **Polling Start Time** — Enter the time of day that the first scheduling interval should start, in `HH:mm:ss` format.

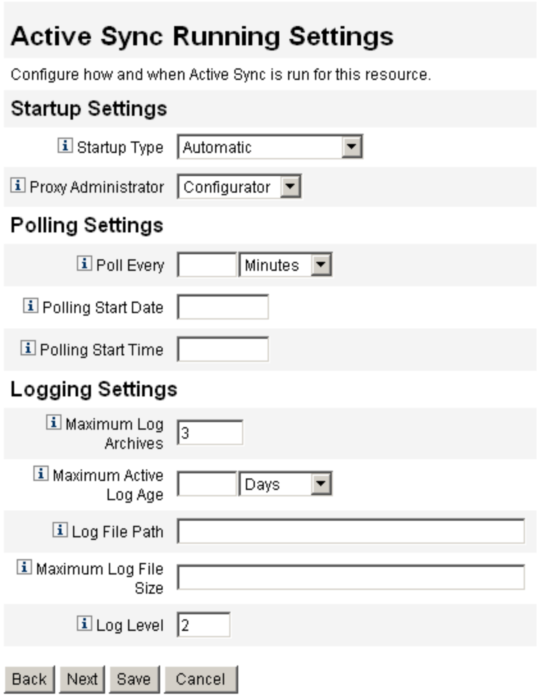
Logging Settings

Make selections to set up logging information and levels:

- **Maximum Log Archives** — If greater than zero, then retain the latest N log files. If zero, then a single log file is re-used. If -1, then log files are never discarded.
- **Maximum Active Log Age** — After this period of time has elapsed, the active log will be archived. If the time is zero, then no time-based archival will occur. If Maximum Log Archives is zero, then the active log will instead be truncated and re-used after this time period. This age criteria is evaluated independently of the time criteria specified by Maximum Log File Size.

  Enter a number, and then select the unit of time (Days, Hours, Minutes, Months, Seconds, or Weeks). Days is the default unit.
- **Log File Path** — Enter the path to the directory in which to create the active and archived log files. Log file names begin with the resource name.

- **Maximum Log file Size** — Enter the maximum size, in bytes, of the active log file. The active log file will be archived when it reaches maximum size. If Maximum Log Archives is zero, then the active log will instead be truncated and re-used after this time period. This size criteria is evaluated independently of the age criteria specified by Maximum Active Log Age.
- **Log Level** — Enter the level of logging:
  - 0 — no logging
  - 1 — error
  - 2 — information
  - 3 — verbose
  - 4 — debug



Active Sync Running Settings

Configure how and when Active Sync is run for this resource.

Startup Settings

Startup Type: Automatic

Proxy Administrator: Configurator

Polling Settings

Poll Every: Minutes

Polling Start Date:

Polling Start Time:

Logging Settings

Maximum Log Archives: 3

Maximum Active Log Age: Days

Log File Path:

Maximum Log File Size:

Log Level: 2

Figure 4. Active Sync Wizard: Running Settings

Click **Next** to continue with the wizard. The General Active Sync Settings page appears.

General Active Sync Settings

Use this page to specify general active sync configuration parameters.

Resource Specific Settings

Note Available resource-specific settings vary depending on resource type. One or more of the following selections may not appear. The following settings apply to an LDAP resource.

- **Object Classes to Synchronize** — Enter the object classes to synchronize. The change log is for all objects; this filters updates only to the listed object classes.
- **LDAP Filter for Accounts to Synchronize** — Enter an optional LDAP filter for the objects to synchronize. The change log is for all objects; this filter updates only objects that match the specified filter. If you specify a filter, an object will be synchronized only if it matches the filter and includes a synchronized object class.
- **Attributes to synchronize** — Enter the attribute names to synchronize. This ignores updates from the change log if they do not update any of the named attributes. For example, If only department is listed, then only changes that affect department will be processed. All other updates are ignored. If blank (the default), then all changes are processed.
- **Change Log Blocksize** — Enter the number of change log entries to fetch per query. The default number is 100.
- **Change Number Attribute Name** — Enter the name of the change number attribute in the change log entry.
- **Filter Changes By** — Enter the names (RDNs) of directory administrators to filter from the changes. Changes with the attribute modifiersname that match entries in this list will be filtered.

The standard value is the administrator's name used by this adapter, to prevent loops. Entries should be in the format `cn=Directory Manager`.

Common Settings

- **Correlation Rule** — Optionally specify a correlation rule to override the correlation rule specified in the resource's reconciliation policy. Correlation rules correlate resource accounts to Identity system accounts.
- **Confirmation Rule** —- Optionally specify a confirmation rule to override the confirmation rule specified in the resource's reconciliation policy.
- **Resolve Process Rule** — Optionally specify the name of a TaskDefinition to run in case of multiple matches to a record in the feed. This should be a process that prompts an administrator for manual action. It can be a process name or a rule evaluating to a process name.
- **Delete Rule** — Optionally specify a rule, which returns true or false, that will be evaluated for each incoming user update to determine if a delete operation should occur.

- **Create Unmatched Accounts** — When true, the adapter will attempt to create accounts that it does not find in the Identity system. When false, the adapter will run the account through the process returned by the Resolve Process Rule.
- **Assign Active Sync resource on create events —** When this option is selected, the Active Sync source resource will be assigned to the user that is created when a create event is detected.
- **Populate Global** — All attributes in the incoming accounts will always be available to the form under the ActiveSync namespace. If this option is selected, then all attributes (except accountId) will be available on the global namespace also.
- **When reset, ignore past changes** — When the adapter is started for the first time or reset, select to ignore past changes. To reset the adapter, delete the configuration object `IAPI_resourceName`. This option is not available for all adapters.
- **Pre-Poll Workflow** — Select an optional workflow to be executed immediately before each poll.
- **Post-Poll Workflow** — Select an optional workflow to be executed immediately after each poll.

Click **Save** or **Next** to save changes to general settings for the resource:

- If you are using the pre-existing input form, click **Save** to complete the wizard selections and return to the Resources list.
- If you are using the wizard generated input form, click **Next** to continue.
  - › If you are using *basic* configuration mode, the Target Resources page appears. (Skip forward in this chapter to *Target Resources*.)
  - › If you are using *advanced* configuration mode, the Event Types page appears.

Event Types

Use this page to configure a mechanism to determine whether a certain type of change event has occurred on the active sync resource.

About Events

An active synchronization event is defined as a change that occurs on an active sync resource. The event types listed for each resource depend on the type of resource and the object affected by the change event. Some event types are create, delete, update, disable, enable, and rename.

Ignoring Events

You can select a mechanism to determine whether to ignore an active sync event. Options are:

- **None** — No active sync events will be ignored.
- **Rule** — Use a rule to determine whether to ignore the active sync event. If you select this option, then you must additionally select a rule from the options list.
- **Condition** — Use a condition to determine whether to ignore the active sync event. After selecting this option, click Edit Condition to use the Condition Panel to define the condition.

Options for determining event types are:

- **None** — There is no method for determining the event type.
- **Rule** — Use a rule to determine the event type. If you select this option, then you must additionally select a rule from the options list.
- **Condition** — Use a condition to determine the event type. After selecting this option, click Edit Condition to use the Condition Panel to define the condition.

Click **Next** to continue in the wizard. The Process Selection page appears.

Process Selection

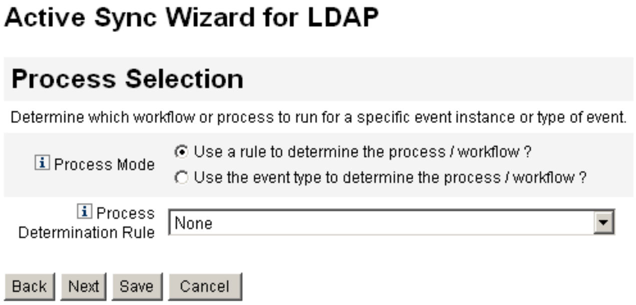
Use this page to set up a workflow or process to run when the user view is checked in for a specific active sync event instance or type of active sync event.

Process Mode

You can select from two modes that determine which workflow or process will run when an active sync event occurs:

- **Rule** — You can use a specific rule to determine which workflow or process to run for each active sync event instance. This means that the rule is executed each time an event occurs.

  After selecting this option, select a rule (process determination rule) from the list.



Active Sync Wizard for LDAP

Process Selection

Determine which workflow or process to run for a specific event instance or type of event.

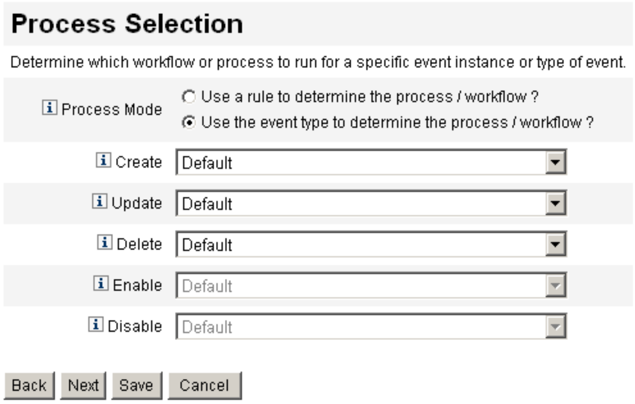
Process Mode
● Use a rule to determine the process / workflow ?
○ Use the event type to determine the process / workflow ?

Process Determination Rule: None

Figure 5. Active Sync Wizard: Process Selection (Rule)

- **Event Type** — You can run a workflow or process based on the event type of each event instance. This is the default selection.

  After selecting this option, select a workflow or process to run for each event type listed.



Process Selection

Determine which workflow or process to run for a specific event instance or type of event.

Process Mode
○ Use a rule to determine the process / workflow ?
● Use the event type to determine the process / workflow ?

Create: Default

Update: Default

Delete: Default

Enable: Default

Disable: Default

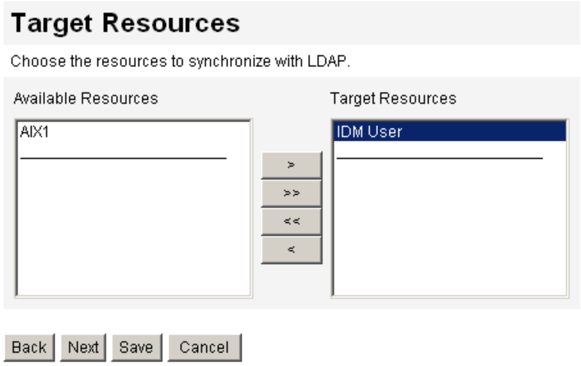
Figure 6. Active Sync Wizard: Process Selection (Event Type)

Click **Next** to continue in the wizard. The Target Resources page appears.

Target Resources

Use this page to specify target resources to synchronize with this resource.

Select one or more resources from the Available Resources area, and then move them to the Target Resources area.



Target Resources

Choose the resources to synchronize with LDAP.

Available Resources: AIX1

Target Resources: IDM User

Figure 7. Active Sync Wizard: Target Resources

Click **Next** to continue. The Target Attribute Mappings page appears.

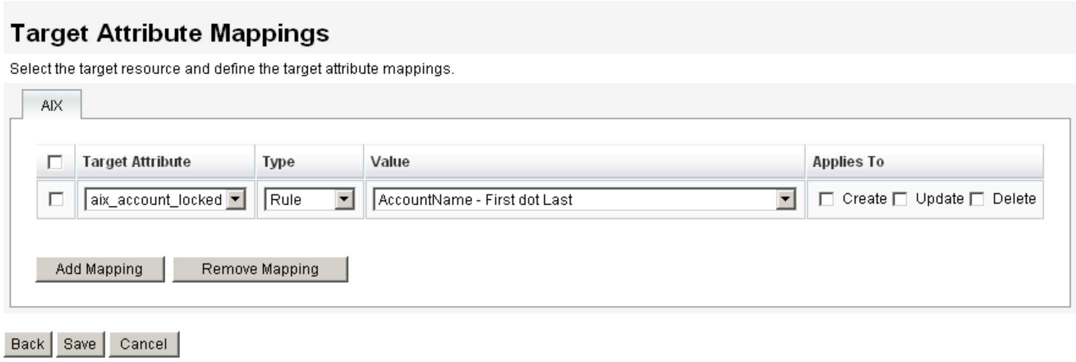
Target Attribute Mappings

Use this page to define the target attribute mappings for each target resource.

Select a target resource from the options list. To add a target attribute to the list, click **Add Mapping**.

Select the attribute, type, and attribute value for each target attribute. In the Applies To column, select one or more actions (Create, Update, or Delete) to which the mapping will apply.

Repeat Steps 1-3 for each target resource. To remove an attribute row from the list, select the row, and then click **Remove Mapping**.



Target Attribute Mappings

Select the target resource and define the target attribute mappings.

AIX

☐	Target Attribute	Type	Value	Applies To
☐	aix_account_locked	Rule	AccountName - First dot Last	☐ Create ☐ Update ☐ Delete

Figure 8. Active Sync Wizard: Target Attribute Mappings

Click **Save** to save the attribute mappings and return to the resources list.

Editing ActiveSync Adapters

Before editing an ActiveSync adapter, you should stop active synchronization. From the Running Settings page, select Disable as Startup Type. A warning message will appear to indicate that active synchronization is disabled.

Note Disabling active synchronization for a resource will result in stopping the active sync task when the resource is saved.

Active Synchronization in a Clustered Environment

The Error status indicator is present only on the Identity Manager server that performs active synchronization for the resource.

Tuning ActiveSync Adapter Performance

Since active synchronization is a background task, ActiveSync adapter configuration can affect server performance. Tuning ActiveSync adapter performance involves these tasks:

- Changing polling intervals
- Specifying the host where the adapter will run
- Starting and stopping
- Managing adapter logs

Manage ActiveSync adapters through the resources list. Select an ActiveSync adapter, and then access start, stop, and status refresh controls actions from the Resource Actions list.

Changing Polling Intervals

- The polling interval determines when the ActiveSync adapter will start processing new information. Polling intervals should be determined based on the type of activity being performed. For example, if the adapter reads in a large list of users from a database and updates all users in Identity Manager each time, consider running this process daily in the early morning hours. Some adapters may have a quick search for new items to process and could be set to run every 10 seconds.

Specifying the Host Where the Adapter Will Run

To specify the host where the adapters will run, edit the `waveset.properties` file. In this file, you can edit either:

- Set `sources.hosts=hostname1,hostname2,hostname3`. This lists the hostnames of machines to run ActiveSync adapters. The adapter will run on the first available host in this field.

  or

- `Set sources.hosts=localhost`

Setting the latter causes the adapter to run on the server on which the adapter was configured.

Note In a cluster you should use the first option if you need to specify a specific server.

ActiveSync adapters that require more memory and CPU cycles can be configured to run on dedicated servers to help load balance the systems.

Starting and Stopping

ActiveSync adapters can be disabled, manually started, or automatically started just like services in NT. They also have to be assigned to run as an Identity Manager administrator. This administrator will scope the access of what the ActiveSync adapter can do, and will be listed in the audit log as the admin that made the changes. Optional attributes include log file size and path, log level.

When an adapter is set to automatic, the adapter restarts when the application server does. When you start an adapter, it will run immediately and execute at the specified polling interval. When you stop an adapter, the next time the adapter checks for the stop flag, it will stop.

Adapter Logs

Adapter logs capture information about the adapter current processing. The amount of detail that the log captures depends upon the logging level of the logging you have set. Adapter logs are useful for debugging problems and watching the adapter process progress.

Each adapter has its own log file, path, and log level. You specify these values on the Running Settings page.

Deleting Adapter Logs

Adapter logs should be deleted only when adapter has been stopped. In most cases, make a copy of the log for archive purposes before deleting a log.

7 Security

This chapter provides information about Identity Manager security features, and details steps you can take to further reduce security risks.

Security Features

Identity Manager features help reduce security risks by providing:

- *Instant disabling of account access* – Identity Manager lets you disable organizations or individual access rights with a single action.
- *Active risk analysis* – Identity Manager scans constantly for security risks such as inactive accounts and suspicious password activity.
- *Comprehensive password management* – Complete and flexible password management capabilities ensure complete access control.
- *Auditing and reporting to monitor access activities* – You can run a full range of reports to deliver targeted information on access activities. (See *Reporting* for more information about reporting features.)
- *Server key encryption* – Identity Manager allows you to create and manage server encryption keys through the Tasks area.

In addition, system architecture seeks to reduce security risks wherever possible. For example, once logged out, you cannot access previously visited pages through your browser's “Back” feature.

Password Management

Identity Manager offers password management at multiple levels:

- **Administrative change management**
  - Change a user's password from multiple locations (**Edit User**, **Find User**, or **Change Password** pages)
  - Change passwords on any one of a user's resources with granular resource selection
- **Administrative password resets**
  - Generate random passwords
  - Display passwords to the end user or the administrator

- **User change password**
  - Provide self-service to the end user for password changes at http://*localhost*:8080/idm/user
  - Optionally customize the self-service page to match the end user's environment
- **User update data**
  - Set up any user schema attribute to be managed by the end user
- **User access recovery**
  - Use authentication answers to grant a user access to change his password
  - Use pass-through authentication to grant a user access by using one of several passwords

Pass-through Authentication

Use pass-through authentication to grant user and administrator access through one or more different passwords. Identity Manager manages authentication through the implementation of:

- *Login applications* (collection of login module groups)
- *Login module groups* (ordered set of login modules)
- *Login modules* (sets authentication for each assigned resource and specify one of several success requirements for authentication)

About Login Applications

Login applications define a collection of login module groups, which further define the set and order of login modules that will be used when a user logs in to Identity Manager. Each login application comprises one or more login module groups.

At login, the login application checks its set of login module groups. If only one login module group is set, then it is used, and its contained login modules are processed in the group-defined order. If the login application has more than one defined login module group, then Identity Manager checks the *login constraint rules* applied to each login module group to determine which group to process.

Login Constraint Rules

Login constraint rules are applied to the login module groups defined in a login application. For each set of login module groups in a login application, only one cannot have a login constraint rule applied to it.

When determining which login module group of a set to process, Identity Manager evaluates the first login module group's constraint rule. If it succeeds, then it processes that login module group. If it fails, then it evaluates each login module group in turn, until a constraint rule succeeds or a login module group with no constraint rule is evaluated (and subsequently used).

Note If a login application will contain more than one login module group, then the login module group with no login constraint rules should be placed in the last position of the set.

Example Login Constraint Rule

In the following example of a location-based login constraint rule, the rule gets the IP address of the requester from the header, and then checks to see if it is located on the 192.168 network. If 192.168. is found in the IP address, then the rule will return a value of true, and this login module group is selected.

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
  <match>
    <ref>remoteAddr</ref>
    <s>192.168.</s>
  </match>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='All'/>
  </MemberObjectGroups>
</Rule>
```

Editing Login Applications

From the menu bar, select **Configure**, and then select **Login** to access the Login page.

The login application list shows:

- Each Identity Manager login application (interface) defined
- Login module groups comprising the login application
- The Identity Manager session timeout limits set for each login application

From the Login page you can:

- Create custom login applications
- Delete custom login applications
- Manage login module groups

To edit a login application, select it from the list.

Setting Identity Manager Session Limits

From the Modify Login Application page, you can set a timeout value (limits) for each Identity Manager login session. Select hours, minutes, and seconds, and then click **Save**. The limits you establish display in the login application list.

Disabling Access to Applications

From the Create Login Application and Modify Login Application pages, you can select the Disable option to disable a login application, thereby preventing users from logging in. If a user tries to log in to a disabled application, then the interface redirects him to an alternate page, indicating that the application is currently disabled. You can edit the message that displays on this page by editing the custom catalog.

Login applications remain disabled until you de-select the option. As a safeguard, you cannot disable administrator login.

Editing Login Module Groups

The login module group list shows:

- Each Identity Manager login module group defined
- Login modules that each login module group contains
- Whether a login module group contains constraint rules

From the Login Module Groups page you can create, edit, and delete login module groups. Select one of the login module groups from the list to edit it.

Editing Login Modules

Enter details or make selections for login modules as follows. (Not all options are available for each login module.)

- **Login success requirement** — Select a requirement that applies to this module. Selections are:
  - **Required** — The login module is required to succeed. Irrespective of whether it succeeds or fails, authentication proceeds to the next login module in the list. If it is the only login module, the administrator is successfully logged in.
  - **Requisite** — The login module is required to succeed. If it succeeds, authentication proceeds to the next login module in the list. If it fails, authentication does not proceed.

  - **Sufficient** — The login module is not required to succeed. If it does succeed, authentication does not proceed to the next login module, and the administrator is successfully logged in. If it fails, authentication continues to the next login module in the list.
  - **Optional** — The login module is not required to succeed. Irrespective of whether it succeeds or fails, authentication continues to the next login module in the list.
- **Login search attributes** — (LDAP only) Specify an ordered list of LDAP user attribute names to be used when attempting to bind (log in) to the associated LDAP server. Each of the LDAP user attributes specified, along with the user's specified login name, is used (in order) to search for a matching LDAP user. This allows a user to log in to Identity Manager, when configured for pass-through to LDAP, via an LDAP cn or email address.

  For example, if you specify:

  ```
  cn
  mail
  ```

  and the user attempts to log in as gwilson, then the LDAP resource will first attempt to find an LDAP user where `cn=gwilson`. If that succeeds, then the bind is attempted with the password specified by the user. If it does not succeed, then the LDAP resource will search for an LDAP user where `mail=gwilson`. If that also fails, then login fails.

  If you do not specify a value, then the default LDAP search attributes are:

  ```
  uid
  cn
  ```

- **Login correlation rule** — Select a login correlation rule to be used for the mapping of login info to the Identity Manager user. The rule you select must have the LoginCorrelationRule authType.
- **New user name rule** — Select a new user name rule to be used when automatically creating new Identity Manager users as part of login.

Click **Save** to save a login module. Once it is saved, you can place the module relative to all other modules in the login module group.

WARNING It is recommended that, if Identity Manager login is configured to authenticate to more than one system, an account's user ID and password should be the same across all systems that are targets of Identity Manager authentication.

If the user ID and password combinations differ, login will fail on each system whose user ID and password do not match the user ID and password entered on the Identity Manager User Login form. Some of these systems may have a lockout policy enforcing the number of failed login attempts before an account is locked; for these systems, user accounts will eventually be locked, even though the user's login via Identity Manager continues to succeed.

Configuring Authentication for Common Resources

If you have more than one resource that is physically or logically the same (for example, two resources defined for the same physical host, or several resources that represent trusted domain servers in an NT or AD domain environment), then you can specify that set of resources in the system configuration object as *common resources*.

By establishing resources as common, you allow a user to authenticate to one of the common resources, but be mapped to his associated Identity Manager user by using another of the common resources. For example, a user may have a resource account linked to his Identity Manager user for resource AD-1. The login module group may define that users must authenticate to resource AD-2. If AD-1 and AD-2 are defined as common resources (in this case, in the same trusted domain), then if the user successfully authenticates to AD-2, Identity Manager can map to the associated Identity Manager user by finding a user with the same accountId on resource AD-1.

The format for specifying this system configuration object attribute is:

```
<Attribute name='common resources'>
    <Attribute name='Common Resource Group Name'>
        <List>
            <String>Common Resource Name</String>
            <String>Common Resource Name</String>
        </List
    </Attribute>
</Attribute>
```

Configuring X509 Certificate Authentication

Use the following information and procedures to configure X509 Certificate Authentication for Identity Manager.

Prerequisites

To support X509 certificate-based authentication in Identity Manager, ensure that two-way (client and server) SSL authentication is configured properly. From the client perspective, this means that an X509-compliant user certificate should have been imported into the browser (or be available through a smart card reader), and that the trusted certificate used to sign the user certificate should be imported into the Web application server's keystore of trusted certificates.

Also, the client certificate used must be selected for client authentication. To verify this:

1. Using Internet Explorer, select **Tools**, and then select **Internet Options**.
2. Select the **Content** tab.
3. In the Certificates area, click **Certificates**.
4. Select the client certificate, and then click **Advanced**.
5. In the Certificate Purposes area, verify that the Client Authentication option is selected.

Configuring X509 Certificate Authentication in Identity Manager

To configure Identity Manager for X509 certificate authentication:

1. Log in to the Administrator Interface as Configurator (or with equivalent permissions).
2. Select **Configure**, and then select **Login** to display the Login page.
3. Click **Manage Login Module Groups** to displays the Login Module Groups page.
4. Select a login module group from the list.
5. Select Identity Manager X509 Certificate Login Module from the Assign Login Module... list. Identity Manager displays the Modify Login Module page.
6. Set the login success requirement. Acceptable values are:
   - **Required** — The login module is required to succeed. Irrespective of whether it succeeds or fails, authentication proceeds to the next login module in the list. If it is the only login module, the administrator is successfully logged in.
   - **Requisite** — The login module is required to succeed. If it succeeds, authentication proceeds to the next login module in the list. If it fails, authentication does not proceed.
   - **Sufficient** — The login module is not required to succeed. If it does succeed, authentication does not proceed to the next login module, and the administrator is successfully logged in. If it fails, authentication continues to the next login module in the list.
   - **Optional** — The login module is not required to succeed. Irrespective of whether it succeeds or fails, authentication continues to the next login module in the list.

7. Select a login correlation rule. This could be a built-in rule or a custom correlation rule. (See the following section for information about creating custom correlation rules.)
8. Click **Save** to return to the Modify Login Module Group page.
9. Optionally, reorder the login modules (if more than one login module is assigned to the login module group, and then click **Save**.
10. Assign the login module group to a login application if it is not yet assigned. From the Login Module Groups page, click Return to Login Applications, and then select a login application. After assigning a login module group to the application, click **Save**.

Note If the `allowLoginWithNoPreexistingUser` option is set to a value of true in the `waveset.properties` file, then when configuring the Identity Manager X509 Certificate Login Module, you are prompted to select a New User Name Rule. This rule is used to determine how to name new users created when one is not found by the associated Login Correlation Rule.

The New User Name Rule has the same available input arguments as the Login Correlation Rule. It returns a single string, which is the user name used to create the new Identity Manager user account.

A sample new user name rule is included in `idm/sample/rules`, named `NewUserNameRules.xml`.

Creating and Importing a Login Configuration Rule

A Login Correlation Rule is used by the Identity Manager X509 Certificate Login Module to determine how to map the certificate data to the appropriate Identity Manager user. Identity Manager includes one built-in correlation rule, named Correlate via X509 Certificate subjectDN.

You can also add your own correlation rules. Each correlation rule must follow these guidelines:

- Its `authType` attribute must be set to `LoginCorrelationRule`. (Set authType='LoginCorrelationRule' in the `<LoginCorrelationRule>` element.)
- It is expected to return an instance of a list of `AttributeConditions` to be used by the login module to find the associated Identity Manager user. For example, the login correlation rule might return an `AttributeCondition` that searches for the associated Identity Manager user by email address.

Arguments passed to login configuration rules are:

- Standard X509 certificate fields (such as `subjectDN`, `issuerDN`, and valid dates)
- Critical and non-critical extension properties

The naming convention for certificate arguments passed to the login correlation rule is:

```
cert.field name.subfield name
```

Example argument names that are available to the rule include:

- `cert.subjectDN`
- `cert.issuerDN`
- `cert.notValidAfter`
- `cert.notValidBefore`
- `cert.serialNumber`

The login configuration rule, using the passed-in arguments, returns a list of one or more `AttributeConditions`. These are used by the Identity Manager X509 Certificate Login Module to find the associated Identity Manager user.

A sample login correlation rule is included in `idm/sample/rules`, named `LoginCorrelationRules.xml`.

After creating a custom correlation rule, you must import it into Identity Manager. From the Administrator Interface, select **Configure**, and then select **Import Exchange File** to use the file import facility.

Testing the SSL Connection

To test the SSL connection, go to the configured application interface's URL via SSL (for example, https//idm007:7002/idm/user/login.jsp). You are notified that you are entering a secure site, and then prompted to specify which personal certificate to send to the Web server.

Diagnosing Problems

Problems authenticating via X509 certificates should be reported as error messages on the login form. For more complete diagnostics, enable trace on the Identity Manager server for these classes and levels:

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

If the client certificate attribute is named something other than `javaxservlet.request.X509Certificate` in the http request, then you will receive a message that this attribute cannot be found in the http request. To correct this:

1. Enable trace for `SessionFactory` to see the complete list of http attributes and determine the name of the X509Certificate.
2. Use the Identity Manager debug facility to edit the `LoginConfig` object.
3. Change the name of the `<AuthnProperty>` in the `<LoginConfigEntry>` for the Identity Manager X509 Certificate Login Module to the correct name.
4. Save, and then retry.

You may also need to remove, and then re-add the Identity Manager X509 Certificate Login Module in the login application.

Cryptographic Use and Management

Cryptography is used to ensure the confidentiality and integrity of server data in memory and in the repository, as well as all data transmitted between the server and gateway.

The following sections provide more information about how cryptography is used and managed in the Identity Manager Server and Gateway, and addresses questions about server and gateway encryption keys.

Cryptographically Protected Data

The following table shows the types of data that are cryptographically protected in the Identity Manager product, including the ciphers used to protect each type of data.

Data Type	**RSA** **MD5**	**NIST** **Triple DES** **168-bit key** **(DESede/ECB/NoPadding)**	**PKCS#5** **Password-Based Crypto** **56-bit key** **(PBEwithMD5andDES)**
Server encryption keys		default	configuration option[1]
Gateway encryption keys		default	configuration option[1]
Policy dictionary words	yes		
User passwords		yes	
User password history		yes	
User answers		yes	
Resource passwords		yes	
Resource password history	yes		
All payload between server and gateways		yes	

[1] Configure via the System Configuration object via the `pbeEncrypt` attribute or the Manage Server Encryption task.

Server Encryption Key Questions and Answers

Read the following sections for answers to frequently asked questions about server encryption key source, location, maintenance, and use.

Where do server encryption keys come from?

Server encryption keys are symmetric, triple-DES 168-bit keys. There are two types of keys supported by the server:

- **Default key** — This key is compiled into the server code.
- **Randomly generated key** — This key can be generated at initial server startup, or any time the security of the current key is in question.

Where are server encryption keys maintained?

Server encryption keys are objects maintained in the repository. There can be many data encryption keys in any given repository.

How does the server know which key to use for decryption and re-encryption of encrypted data?

Each piece of encrypted data stored in the repository is prefixed by the ID of the server encryption key that was used to encrypt it. When an object containing encrypted data is read into memory, Identity Manager uses the server encryption key associated with the ID prefix on the encrypted data to decrypt, and then re-encrypt with the same key if the data changed.

How do I update server encryption keys?

Identity Manager provides a task called Manage Server Encryption. This task allows an authorized security administrator to perform several key management tasks, including:

- Generating a new "current" server key
- Re-encrypting existing objects, by type, containing encrypted data with the "current" server key

See *Managing Server Encryption* in this chapter for more information about how to use this task.

What happens to existing encrypted data if the "current" server key is changed?

Nothing. Existing encrypted data will still be decrypted or re-encrypted with the key referenced by the ID prefix on the encrypted data. If a new server encryption key is generated and set to be the "current" key, any new data to be encrypted will use the new server key.

Note It is very important that any server encryption key referenced by some object's encrypted data not be removed from the repository; otherwise, the server will not be able to decrypt it. If an object containing encrypted data is imported from another repository, then the associated server encryption key must first be imported to ensure the object can be successfully imported.

To avoid these multi-key issues, as well as to maintain a higher level of data integrity, use the Manage Server Encryption task to re-encrypt all existing encrypted data with the "current" server encryption key.

How are server keys protected?

If the server is not configured to use password-based encryption (PBE) - PKCS#5 encryption (set in the System Configuration object via the `pbeEncrypt` attribute or the Manage Server Encryption task), then the default key is used to encrypt the server keys. The default key is the same for all Identity Manager installations.

If the server is configured to use PBE encryption, then a PBE key is generated each time the server is started. The PBE key is generated by providing a password, generated from a server-specific secret, to the PBEwithMD5andDES cipher. The PBE key is maintained only in memory and never persisted. In addition, the PBE key is the same for all servers sharing a common repository.

To enable PBE encryption of server keys, the cipher PBEwithMD5andDES must be available. Identity Manager does not package this cipher by default, but it is a PKCS#5 standard that is available in many JCE providers implementations, such as those provided by Sun and IBM.

Can I export the server keys for safe external storage?

Yes. If the server keys are PBE encrypted, then before they are exported, they will be decrypted and re-encrypted with the default key. This allows them to be imported to the same or another server at a later date, independent of the local server PBE key. If the server keys are encrypted with the default key, then no pre-processing is done before they are exported.

When they are imported into a server, if the server is configured for PBE keys, the keys will be decrypted and then re-encrypted with the local server's PBE key, if that server is configured for PBE key encryption.

What data is encrypted between the server and gateway?

All data (payload) transmitted between the server and gateway is triple-DES encrypted with a randomly generated, per server-gateway session symmetric 168 bit key.

Gateway Key Questions and Answers

Read the following sections for answers to frequently asked questions about gateway source, storage, distribution, and protection.

Where do the gateway keys come from to encrypt or decrypt data?

Each time an Identity Manager Server connects to a gateway, the initial handshake will generate a new random 168-bit, triple-DES session key. This key will be used to encrypt or decrypt all subsequent data transmitted between that server and that gateway. There is a unique session key generated for each server/gateway pair.

How are gateway keys distributed to the gateways?

Session keys are randomly generated by the server and then securely exchanged between server and gateway by encrypting them with the shared secret master key as part of the initial server-to-gateway handshake.

At initial handshake time, the server queries the gateway to determine which mode it supports. The gateway can operate in two modes

- **Default mode** — Initial server-to-gateway protocol handshake is encrypted with the default 168 bit triple-DES key, which is compiled into the server code.
- **Secure mode** — A per shared repository, random, 168-bit key, triple-DES gateway key is generated and communicated from the server to the gateway as part of the initial handshake protocol. This gateway key is stored in the server repository like other encryption keys, and also stored by the gateway in its local registry.

  When in secure mode and a server contacts a gateway, the server will encrypt test data with the gateway key and send it to the gateway. The gateway will then attempt to decrypt the test data, add some gateway unique data to the test data, re-encrypt both, and send the data back to the server. If the server can successfully decrypt the test data and the gateway unique data, the server will then generate the server-gateway unique session key, encrypt it with the gateway key and send it to the gateway. Upon receipt, the gateway will decrypt the session key and retain it for use for the life of the server-to-gateway session. If the server cannot successfully decrypt the test data and gateway unique data, the server will encrypt the gateway key using the default key and send it to the gateway. The gateway will decrypt the gateway key using its compiled in default key and store the gateway key in its registry. The server will then encrypt the server-gateway unique session key with the gateway key and send it to the gateway for use for the life of the server-to-gateway session.

From that point forward, the gateway will only accept requests from servers that have encrypted the session key with its gateway key. On startup, the gateway checks the registry for a key. If there is one, it will use it. If there is not one, it will use the default key. Once the gateway has a key set in the registry, it will no longer allow sessions to be established using the default key. This will prevent someone from setting up a rogue server and establishing a connection to a gateway.

Can I update the gateway keys used to encrypt or decrypt the server-to-gateway payload?

Identity Manager provides a task called Manage Server Encryption that allows an authorized security administrator to do several key management tasks, including generate a new "current" gateway key and update all gateways with the "current" gateway key. This is the key that is used to encrypt the per-session key used to protect all payload transmitted between server and gateway. The newly generated gateway key will be encrypted with either the default key or PBE key, depending on the value of the `pbeEncrypt` attribute in the System Configuration.

Where are the gateway keys stored on the server, on the gateway?

On the server, the gateway key is stored in the repository just like server keys. On the gateway, the gateway key is stored in a local registry key.

How are gateway keys protected?

The gateway key is protected the same way server keys are. If the server is configured to use PBE encryption, the gateway key will be encrypted with a PBE generated key. If the option is false, it will be encrypted with the default key. See the previous section titled *How are server keys protected?* for more information.

Can I export the gateway key for safe external storage?

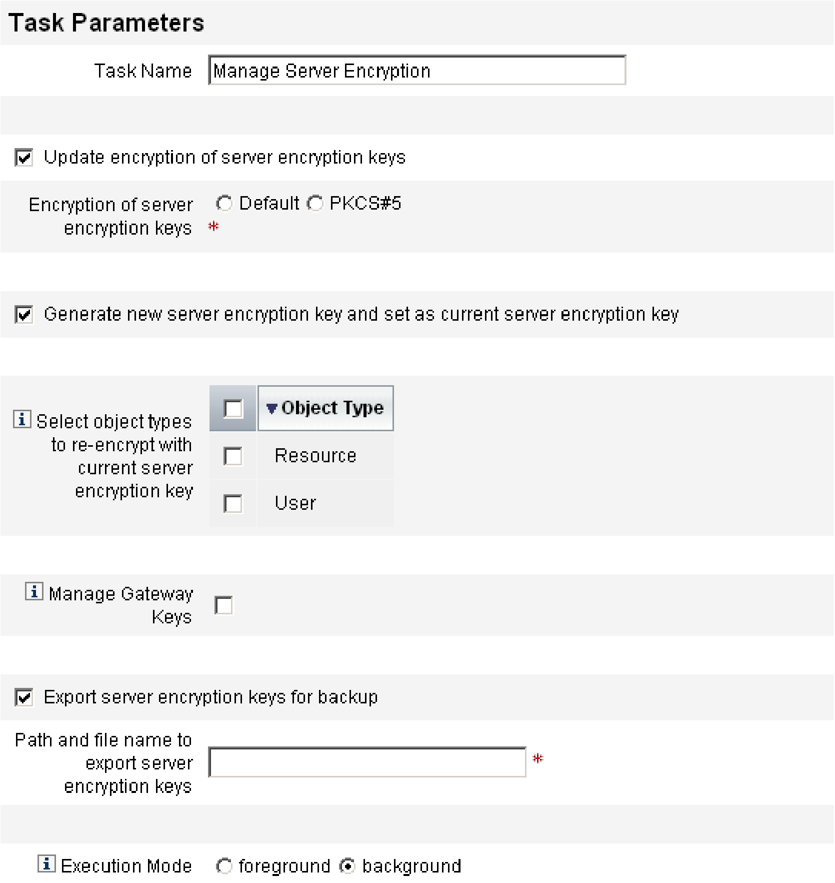
The gateway key can be exported via the Manage Server Encryption task, just as with server keys. See the previous section titled *Can I export the server keys for safe external storage?* for more information.

How are server and gateway keys destroyed?

Server and gateway keys are destroyed by deleting them from the server repository. Note that a key should not be deleted as long as any server data is still encrypted with that key or any gateway is still relying on that key. Use the Manage Server Encryption task to re-encrypt all server data with the current server key and to synchronize the current gateway key to all gateways to ensure no old keys are still being used before they are deleted.

Managing Server Encryption

The Identity Manager server encryption feature allows you to create new 3DES server encryption keys, and then encrypt these keys by using 3DES or PKCS#5 encryption. Only users with Security Administrator capabilities can run the Manage Server Encryption task, which is accessed from the **Tasks** tab.



Task Parameters

Task Name: Manage Server Encryption

☑ Update encryption of server encryption keys

Encryption of server encryption keys * ○ Default ○ PKCS#5

☑ Generate new server encryption key and set as current server encryption key

Select object types to re-encrypt with current server encryption key

□	▼ Object Type
□	Resource
□	User

Manage Gateway Keys □

☑ Export server encryption keys for backup

Path and file name to export server encryption keys ________ *

Execution Mode ○ foreground ● background

Figure 1. Manage Server Encryption Task

Select **Run Tasks**, and then select Manage Server Encryption from the list to configure this information for the task:

- **Update encryption of server encryption keys** — Select to specify whether server encryption keys will be encrypted by using default (3DES) encryption or PKCS#5 encryption. When you select this option, two encryption choices appear (Default and PKCS#5); select one.
- **Generate new server encryption key and set as current server encryption key** — Select to generate a new server encryption key. Each piece of encrypted data generated after you make this selection is encrypted with this key. Generating a new server encryption key does not affect the key applied to existing encrypted data.

- **Select object types to re-encrypt with current server encryption key** — Select one or more Identity Manager object types (such as resources or users) to re-encrypt with the current encryption key.
- **Manage Gateway Keys** — When selected, the page displays these gateway key options:
  - **Generate a new key and synchronize all gateways**
    Select this option when initially enabling a secure gateway environment. This option generates a new gateway key and communicates it to all gateways.
  - **Synchronize all gateways with current gateway key**
    Select to synchronize any new gateways, or gateways that have not communicated the new gateway key. Select this option if you had a gateway that was down when all gateways were synchronized with the current gateway key, or when you want to force a key update for a new gateway.
- **Export server encryption keys for backup** — Select to export existing server encryption keys to an XML-formatted file. When you select this option, Identity Manager displays an additional field for you to specify a path and file name to export the keys.

Note If you are using PKCS#5 encryption and you choose to generate and set a new server encryption key, you should also select this option. In addition, you should store the exported keys on removable media and in a secure location (not on a network).

- **Execution Mode** — Select whether to run this task in the background (the default option) or in the foreground. If you choose to re-encrypt one or more object types with a newly generated key, this task can take some time and is best run in the background.

Security Practices

As an Identity Manager administrator, you can further reduce security risks to your protected accounts and data by following these recommendations, at setup time and after.

At Setup

You should:

- Access Identity Manager through a secure Web server using https.
- Reset the passwords for the default Identity Manager administrator accounts (Administrator and Configurator). To further protect the security of these accounts, you can rename them.

- Limit access to the Configurator account.
- Limit administrators' capability sets to only those actions needed for their job functions, and limit administrator capabilities by setting up organizational hierarchies.
- Change the default password for the Identity Manager Index Repository.
- Turn on auditing to track activities in the Identity Manager application.
- Edit the permissions on files in the Identity Manager directory.
- Customize workflows to insert approvals or other checkpoints.
- Develop a recovery procedure to describe how to recover your Identity Manager environment in the event of emergency.

During Use

You should:

- Periodically change the passwords for the default Identity Manager administrator accounts (Administrator and Configurator).
- Log out of Identity Manager when not actively using the system.
- Set or know the default timeout period for an Identity Manager session.

  If your application server is Servlet 2.2-compliant, the Identity Manager installation process sets the http session timeout to a default value of 30 minutes. You can change this value by editing the property; however, you should set the value lower to increase security. Do not set the value higher than 30 minutes.

  To change the session timeout value:

  1. Edit the `web.xml` file, which is located in the `idm/WEB-INF` directory in your application server directory tree.
  2. Change the number value in the following lines:

  ```
  <session-config>
    <session-timeout>30</session-timeout>
  </session-config>
  ```

8 Reporting

Identity Manager reports on automated and manual system activities. A robust set of reporting features lets you capture and view important access information and statistics on Identity Manager users at any time.

Read this chapter for information and procedures that show how to work with Identity Manager reporting features. You can learn about:

- Identity Manager report types, including AuditLog, Real Time, Summary, SystemLog, and Usage reports
- How to create, edit, run, and email reports
- How to download report information

Working with Reports

In Identity Manager, reports are considered a special category of task. As a result, you work with reports in two areas of the Identity Manager Administrator interface:

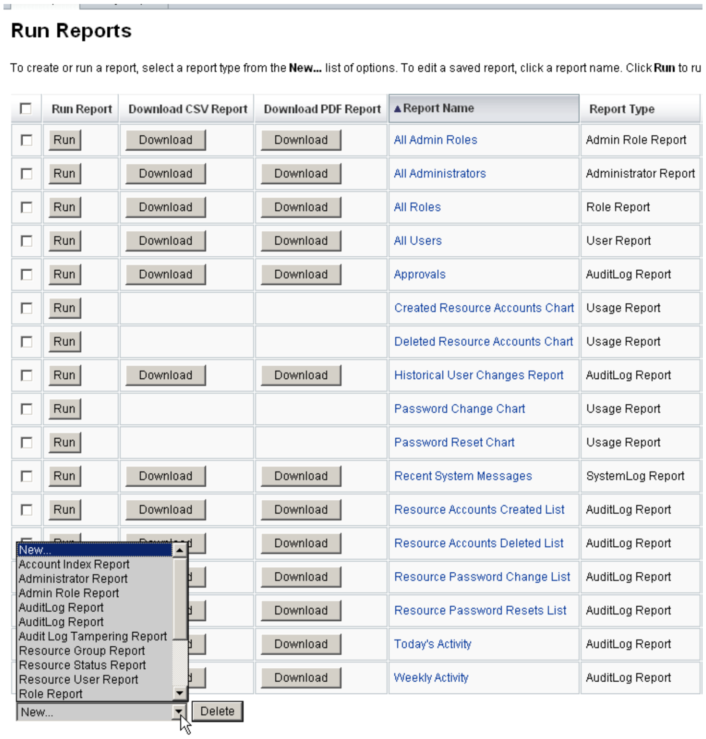
- **Reports** — From here, you define, run, delete, and download reports. You can also manage scheduled reports.
- **Tasks** — Once you define reports, go to the Tasks area to schedule and manipulate report tasks.

Reports

You perform most report-related activities from the Run Reports page, which allows you to:

- Create, modify, and delete reports
- Run reports
- Download report information for use in another application, such as Microsoft Excel.

To view this page, select **Reports** from the menu bar. The **Run Reports** subtab page appears.



Run Reports

To create or run a report, select a report type from the **New...** list of options. To edit a saved report, click a report name. Click **Run** to ru

☐	Run Report	Download CSV Report	Download PDF Report	▲Report Name	Report Type
☐	Run	Download	Download	All Admin Roles	Admin Role Report
☐	Run	Download	Download	All Administrators	Administrator Report
☐	Run	Download	Download	All Roles	Role Report
☐	Run	Download	Download	All Users	User Report
☐	Run	Download	Download	Approvals	AuditLog Report
☐	Run			Created Resource Accounts Chart	Usage Report
☐	Run			Deleted Resource Accounts Chart	Usage Report
☐	Run	Download	Download	Historical User Changes Report	AuditLog Report
☐	Run			Password Change Chart	Usage Report
☐	Run			Password Reset Chart	Usage Report
☐	Run	Download	Download	Recent System Messages	SystemLog Report
☐	Run	Download	Download	Resource Accounts Created List	AuditLog Report
			Download	Resource Accounts Deleted List	AuditLog Report
			Download	Resource Password Change List	AuditLog Report
			Download	Resource Password Resets List	AuditLog Report
			Download	Today's Activity	AuditLog Report
			Download	Weekly Activity	AuditLog Report

Figure 1. Run Reports Page Selections

Begin defining reports by using one of these methods:

- Create a report
- Select a report to modify and save with a new name (also known as report cloning)

Creating Reports

To create a report:

1. Select **Reports** from the menu bar.
2. Select a report type from the **New** list of options.

Identity Manager displays the Define a Report page, where you select and save options to create the report.

Cloning Reports

To clone a report, select a report from the list. Enter the new report name and optionally adjust report parameters, and then click **Save** to save it with the new name.

Emailing Reports

When creating or editing a report, you can select an option to email the report results to one or more email recipients. When you select this option, the page refreshes and prompts for email recipients. Enter one or more recipients, separating addresses with a comma.

You also can choose the format of the report to be attached to the email:

- **Attach CSV Format** — Attaches report results in comma-separated value (CSV) format.
- **Attach PDF Format** — Attaches report results in Portable Document Format (PDF).

Running Reports

After entering and selecting report criteria, you can:

- Run the report without saving — Click **Run** to run the report. Identity Manager does not save the report (if you defined a new report) or the changed report criteria (if you edited an existing report).
- Save the report — Click **Save** to save the report. Once saved, you can run the report from the Run Reports page (the list of reports).

Scheduling Reports

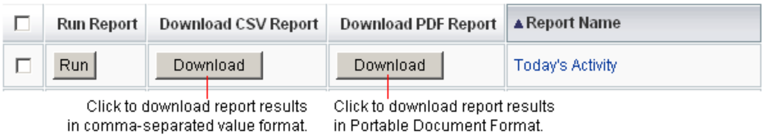
Depending on whether you want to immediately run a report or schedule it to run at regular intervals, you make different selections:

- **Reports → Run Reports** — Allows you to run saved reports immediately. From the list of reports, click **Run**. Identity Manager runs the report and then displays the results in summary and detailed formats.
- **Tasks → Schedule Tasks** — Schedules report tasks to be run. After selecting a report task, you can set report frequency and options. You also can adjust specific report details (as in the Define a Report page in the Reports area).

Downloading Report Data

From the Run Reports page, click **Download** in one of these columns:

- **Download CSV Report** — Downloads audit report output in CSV format. Once saved, you can open and work with the report in another application, such as Microsoft Excel.
- **Download PDF Report** — Downloads audit report output in Portable Document Format.



□	Run Report	Download CSV Report	Download PDF Report	▲Report Name
□	Run	Download	Download	Today's Activity

Click to download report results in comma-separated value format.

Click to download report results in Portable Document Format.

Figure 2. Download Reports

Configuring Fonts for Report Output

For reports generated in portable document format (PDF), you can make selections to determine the fonts to be used in the report.

To configure report font selections, click **Configure**, and then select **Reports**. These selections are available:

- **PDF Font Name** — Select the font to use when generating PDF reports. By default, only fonts available to all PDF viewers are shown. However, additional fonts (such as those needed to support Asian languages) can be added to the system by copying font definition files into the product's fonts/ directory and restarting the server.

  Accepted font definition formats include .ttf, .ttc, .otf, and .afm. If you select one of these fonts, then it must be available at the machine where the report is viewed. Alternatively select the Embed Font in PDF Documents option.
- **Embed Font in PDF Documents** — Select this option to embed the font definition in the generated PDF report. This ensures that the report is viewable in any PDF viewer.

Note Embedding the font can greatly increase the size of the document.

Click **Save** to save report configuration options.

Report Types

Identity Manager several report types, including:

- AuditLog
- Real Time
- Summary
- SystemLog
- Usage

AuditLog

Audit reports are based on events captured in the system audit log. These reports provide information about generated accounts, approved requests, failed access attempts, password changes and resets, and self-provisioning activities, among others.

Note Before running audit logs, you must specify the types of Identity Manager events you want to capture. To do this, select **Configure** from the menu bar, and then select **Audit Events**. Select one or more audit group names to record successful and failed events for each group. For more information about setting up audit configuration groups, see *Audit Group Configuration* in Chapter 5.

To define an AuditLog report, select AuditLog Report from the list of report options on the Run Reports page.

Once you have set and saved report parameters, run the report from the Run Reports list page. Click **Run** to produce a report of all results that match the saved criteria. Included in the report are the date an event occurred, the action performed, and the result of the action.

Real Time

Real Time reports poll resources directly to report real-time information. Real time reports include:

- **Resource Group** — Summarizes group attributes, including user memberships.
- **Resource Status** — Tests the connection status of one or more specified resources by executing the testConnection method against each resource.
- **Resource User** — Lists user resource accounts and account attributes.

To define a Real Time report, select it from the list of report options on the Run Reports page.

Once you have set and saved report parameters, run the report from the Run Reports list page. Click **Run** to produce a report of all results that match the saved criteria.

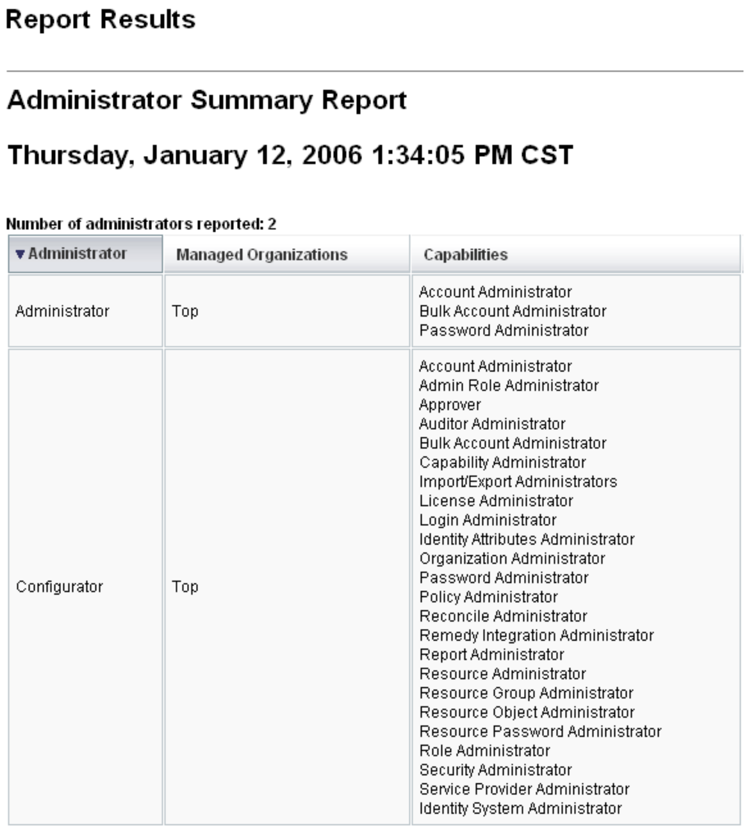
Summary Reports

Summary report types include:

- **Account Index** – Report on selected resource accounts according to reconciliation situation.
- **Administrator** – View Identity Manager administrators, the organizations they manage, and assigned capabilities. When defining an administrator report, you can select administrators to include by organization.
- **Admin Role** – List users assigned to admin roles.
- **Role** – Summarize Identity Manager roles and associated resources. When defining a role report, you can select the roles to include by associated organization.
- **Task** – Report on pending and finished tasks. You determine the depth of information to include by selecting from a list of attributes such as approver, description, expiration date, owner, start date, and state.
- **User** – View users, the roles to which they are assigned, and the resources they can access. When defining a user report, you can select which users to include by name, role, organization, or resource assignment.
- **User Question** – Allows administrators to find users who have not answered the minimum number of authentication questions, as specified by their account policy requirements. The results indicate user name, account policy, the interface associated with the policy, and the minimum number of questions that require answers.

Run summary reports from the Run Reports list page.

As shown in the following illustration, the administrator report lists Identity Manager administrators, the organizations they manage, and their assigned capabilities and admin roles.



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▾Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

Figure 3. Administrator Summary Report

SystemLog

A SystemLog report shows system messages and errors that are recorded in the repository. When setting up this report, you can specify to include or exclude:

- System components (such as Provisioner, Scheduler, or Server)
- Error codes
- Severity levels (error, fatal, or warning)

You also set the maximum number of records you want to display (by default, 3000), and whether you want to display the oldest or newest records if available records exceed the specified maximum.

Note You also can run the `lh syslog` command to extract records from the system log. For detailed command options, read *syslog command* in *lh Reference*.

To define a SystemLog report, select SystemLog Report from the list of report options on the Run Reports page.

Usage Reports

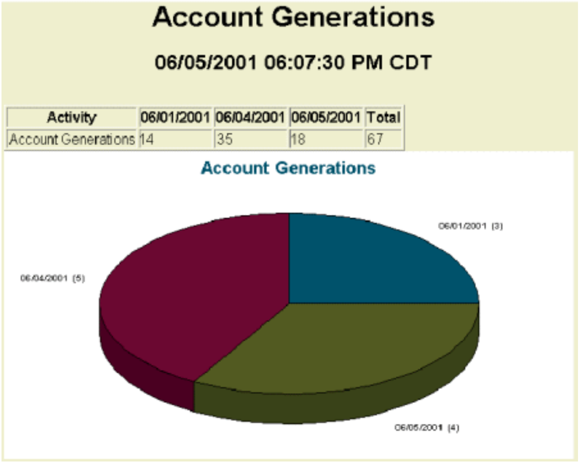
Create and run usage reports to view graphical or tabular summaries of system events related to Identity Manager objects such as administrators, users, roles, or resources. You can display output in pie chart, bar graph, or tabular format.

To define a usage report, select Usage Report from the list of report options on the Run Reports list page.

Once you have set and saved report parameters, run the report from the Run Reports list page.

Usage Report Charts

In the following illustration, the table at the top shows events comprising the report. The chart below shows the same information in graphical format. As you move the mouse pointer over each portion of the chart, the value of that portion appears.



Account Generations

06/05/2001 06:07:30 PM CDT

Activity	06/01/2001	06/04/2001	06/05/2001	Total
Account Generations	14	35	18	67

Figure 4. Usage Report (Generated User Accounts)

You can manipulate portions of a pie chart to highlight them. Right-click and hold a data slice, and then drag it away from center to visually separate it from the other data slices. You can do this with one or more portions of the chart. For most control, click the slice near the center; this allows you to drag it a longer distance from the remaining slices.

You also can rotate the pie chart to your desired view. Click and hold near the edge of the chart, and then move the mouse to right or left to rotate the view.

Risk Analysis

Identity Manager risk analysis features let you report on user accounts whose profiles fall outside certain security constraints. Risk analysis reports scan the physical resource to gather data and show, by resource, details about disabled accounts, locked accounts, and accounts with no owners. They also provide details about expired passwords. Report details vary depending on the resource type.

Note Standard reports are available for AIX, HP, Solaris, NetWare NDS, Windows NT, and Windows Active Directory resources.

Risk analysis pages are controlled by a form and can be configured for your environment. You can find a list of forms under the RiskReportTask object on the `idm\debug` page, and modify these by using the Business Process Editor. See *Identity Manager Technical Reference* for more information about configuring Identity Manager forms.

To create a risk analysis report, click **Risk Analysis** from the menu bar, and then select a report from the New list of options.

You can limit the report to scan selected resources; and depending on the resource type, you can scan for accounts:

- That are disabled, expired, inactive, or locked
- That have never been used
- Do not have a fullname or password
- Do not require a password
- With passwords that have expired or have not changed for a specified number of days

Once defined, you can schedule risk analysis reports to run at specified intervals.

1. Click **Schedule Tasks**, and then select a report to run.
2. On the Create Task Schedule page, enter a name and schedule information, and then optionally adjust other risk analysis selections.
3. Click **Save** to save the schedule.

9 Task Templates

Identity Manager's *task templates* enable you to use the Administrator interface to configure certain workflow behaviors, as an alternative to writing customized workflows.

Identity Manager provides these task templates you can configure:

- **Create User Template** — Configures properties for the create user task.
- **Delete User Template** — Configures properties for the delete user task.
- **Update User Template** — Configures properties for the update user task.

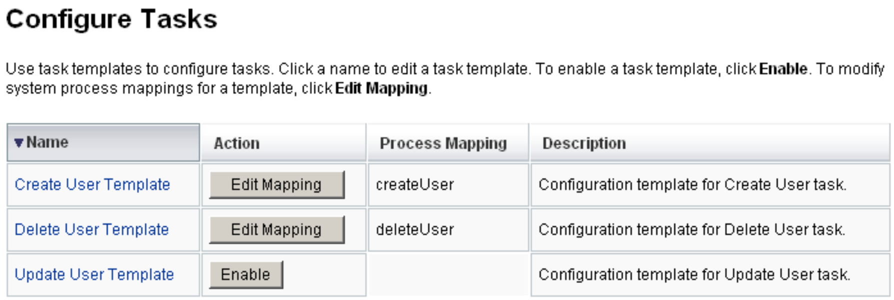
Read the following sections for information about working with task templates:

- Enabling the Task Templates — Describes how to make the task templates available to your system.
- Configuring the Task Templates — Describes how to use task templates to configure workflow behaviors.

Enabling the Task Templates

Before using task templates, you must map the task templates processes. To map process types:

1. From the Identity Manager Administrator interface, select **Tasks**, and then select **Configure Tasks**.



Configure Tasks

Use task templates to configure tasks. Click a name to edit a task template. To enable a task template, click **Enable**. To modify system process mappings for a template, click **Edit Mapping**.

▼Name	Action	Process Mapping	Description
Create User Template	Edit Mapping	createUser	Configuration template for Create User task.
Delete User Template	Edit Mapping	deleteUser	Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

Figure 1. Configure Tasks

The Configure Tasks page contains a table with these columns:

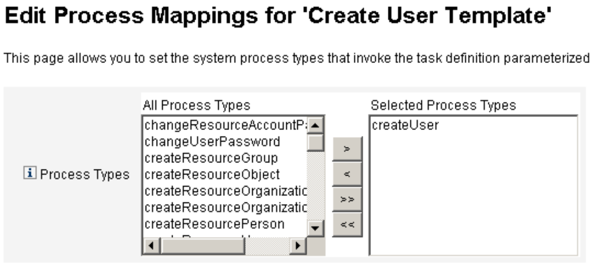
- **Name** — Provides links to the Create User, Delete User, and Update User Templates.

- **Action** – Contains one of the following buttons:
  - **Enable** – Displays if you have not enabled a template yet.
  - **Edit Mapping** – Displays after you enable a template.

  The procedure for enabling and editing process mappings is the same.
- **Process Mapping** – Lists the process type mapped for each template.
- **Description** – Provides a short description of each template.

2. Click **Enable** to open the Edit Process Mappings page for a template.

   For example, the following page displays for the Create User Template:



Edit Process Mappings for 'Create User Template'

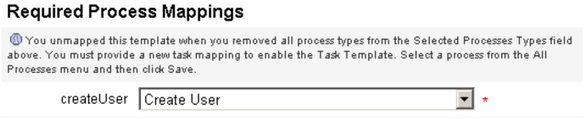
This page allows you to set the system process types that invoke the task definition parameterized by this template.

Process Types

Figure 2. Edit Process Mappings Page

Note The default process type (in this case, `createUser`) automatically displays in the Selected Process Types list. If necessary, you can select a different process type from the menu.

- Generally, you do not map more than one process type for each template.
- If you remove the process type from the Selected Process Types list and do not select a replacement, a Required Process Mappings section displays instructing you to select a new task mapping.



Required Process Mappings

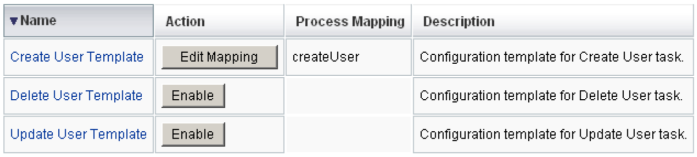
You unmapped this template when you removed all process types from the Selected Processes Types field above. You must provide a new task mapping to enable the Task Template. Select a process from the All Processes menu and then click Save.

createUser: Create User *

Figure 3. Required Process Mappings Section

3. Click **Save** to map the selected process type and return to the Configure Tasks page.

Note When the Configure Tasks page redisplays, an **Edit Mapping** button replaces the **Enable** button and the process name is listed in the Process Mapping column.



▾Name	Action	Process Mapping	Description
Create User Template	Edit Mapping	createUser	Configuration template for Create User task.
Delete User Template	Enable		Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

Figure 4. Updated Configure Tasks Table

4. Repeat the mapping process for each of the remaining templates.

Notes:

- You can verify the mappings by selecting **Configure** > **Form and Process Mappings**. When the Configure Form and Process Mappings page displays, scroll down to the Process Mappings table and verify that the following Process Types are mapped to the Process Name Mapped To entries shown in the table.

Process Type	Process Name Mapped To
`createUser`	`Create User Template`
`deleteUser`	`Delete User Template`
`updateUser`	`Update User Template`

  If the templates were enabled successfully, Process Name Mapped To entries should all include the word *Template*.

- You can also map these process types directly from this page if you type **`Template`** into the Process Name Mapped To column as shown in the table.

After successfully mapping the template process types, you can configure the task templates.

Configuring the Task Templates

To configure the different task templates, follow these steps:

1. Select a Name link in the Task Template table. One of the following pages displays:
   - **Edit Task Template Create User Template** — Open this page to edit the template used to create a new user account.
   - **Edit Task Template Delete User Template** — Open this page to edit the template used to delete or deprovision a user’s account.

- **Edit Task Template Update User Template** — Open this page to edit the template used to update an existing user's information.

Each Edit Task Template page contains a set of tabs that represent a major configuration area for the user workflow.

The following table describes each tab, its purpose, and which templates use that tab.

Tab Name	Purpose	Template
General (*default tab*)	Allows you to define how a task name displays in the task bar located on the Home and Account pages, and in the task instance table on the Tasks page.	Create User and Update User Task Templates only
	Allows you to specify how user accounts are deleted/deprovisioned	Delete User Template only
Notification	Allows you to configure email notifications sent to administrators and users when Identity Manager invokes a process.	All Templates
Approvals	Allows you to enable or disable approvals by type, designate additional approvers, and specify attributes from account data before Identity Manager executes certain tasks.	All Templates
Audit	Allows you to enable and configure auditing for the workflow.	All Templates
Provisioning	Allows you to run a task in the background and to allow Identity Manager to retry a task if the task fails.	Create User Task Template and Update User Task Templates only
Sunrise and Sunset	Allows you to suspend a creation task until a specified date/time (*sunrise*) or to suspend a deletion task until a specified date/time (*sunset*).	Create User Task Template only
Data Transformations	Allows you to configure how user data is transformed during provisioning.	Create User and Update User Task Templates only

2. Select one of the tabs to configure workflow features for the template.

   Instructions for configuring these tabs are provided in the following sections:

   - "Configuring the General Tab" on page 5
   - "Configuring the Notification Tab" on page 7
   - "Configuring the Approvals Tab" on page 12
   - "Configuring the Provisioning Tab" on page 26
   - "Configuring the Sunrise and Sunset Tab" on page 27
   - "Configuring the Data Transformations Tab" on page 32

3. When you are finished configuring the templates, click the **Save** button to save your changes.

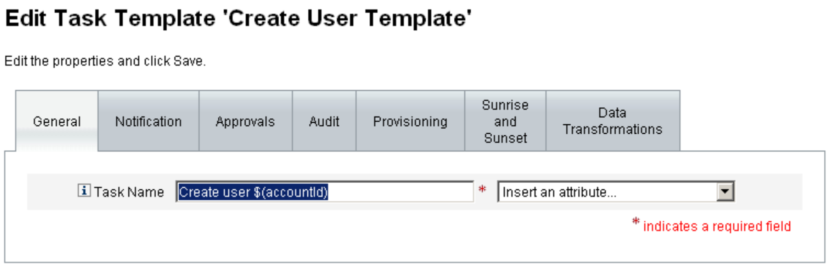
Configuring the General Tab

This section provides instructions for configuring the General tab.

Note The Edit Task Template pages for the Create User Template and Update User Template are identical, so instructions for configuring the tabs are provided in one section.

For the Create User or Update User Templates

When you open the Edit Task Template Create User Template or Edit Task Template Update User Template the General tab page displays by default. This page consists of a Task Name text field and menu, as shown in the following figure.



Edit Task Template 'Create User Template'

Edit the properties and click Save.

Task Name: Create user $(accountId) * Insert an attribute...

* indicates a required field

Figure 5. General Tab: Create User Template

Task names can contain literal text and/or attribute references that are resolved during task execution.

To change the default task name, use the following steps:

1. Type a name into the **Task Name** field.

   You can edit or completely replace the default task name.

2. The **Task Name** menu provides a list of attributes that are currently defined for the view associated with the task configured by this template. Select a attribute from the menu (*optional*).

   Identity Manager appends the attribute name to the entry in the Task Name field. For example:

   ```
   Create user $(accountId) $(user.global.email)
   ```

3. When you are finished, you can

- Select a different tab to continue editing the templates.
- Click **Save** to save your changes and return to the Configure Tasks page.

  The new task name will display in the Identity Manager task bar, located at the bottom of the Home and Accounts tabs.
- Click **Cancel** to discard your changes and return to the Configure Tasks page.

For the Delete User Template

When you open the Edit Task Template Delete User Template, the General tab page displays by default.

To specify how user accounts are deleted/deprovisioned, use the following steps:

1. Use the **Delete Identity Manager Account** buttons to specify whether an Identity Manager account can be deleted during a delete operation, as follows:
   - **Never** — Enable this button to prevent accounts from being deleted.
   - **Only if user has no linked accounts after deprovisioning** — Enable this button to allow user account deletions only if there are no linked resource accounts after deprovisioning.
   - **Always** — Enable this button to always allow user account deletions — even if there are still resource accounts assigned.
2. Use the **Resource Accounts Deprovisioning** boxes to control resource account deprovisioning for *all* resource accounts, as follows:
   - **Delete All** — Enable this box to delete all accounts representing the user on all assigned resources.
   - **Unassign All** — Enable this box to unassign all resource accounts from the user. The resource accounts will not be deleted.
   - **Unlink All** — Enable this box to break all links from the Identity Manager system to the resource accounts. Users with accounts that are assigned but not linked will display with a badge to indicate that an update is required.

Note These controls override the behaviors in the Individual Resource Accounts Deprovisioning table.

3. Use the **Individual Resource Accounts Deprovisioning** boxes to allow a more fine-grained approach to user deprovisioning (compared to Resource Accounts Deprovisioning) as follows:
   - **Delete** — Enable this box to delete the account that represents the user on the resource.
   - **Unassign** — Enable this box and the user will no longer be assigned directly to the resource. The resource account will not be deleted.

- **Unlink** — Enable this box to break the link from the Identity Manager system to the resource accounts. Users with accounts that are assigned but not linked will display with a badge to indicate that an update is required.

Note The **Individual Resource Accounts Deprovisioning** options are useful if you want to specify a separate deprovisioning policy for different resources. For example, most customers do not want to delete Active Directory users because each user has a global identifier that can never be re-created following deletion.

However, in environments where new resources are added, you might not want to use this option because the deprovisioning configuration would have to be updated every time you add a new resource.

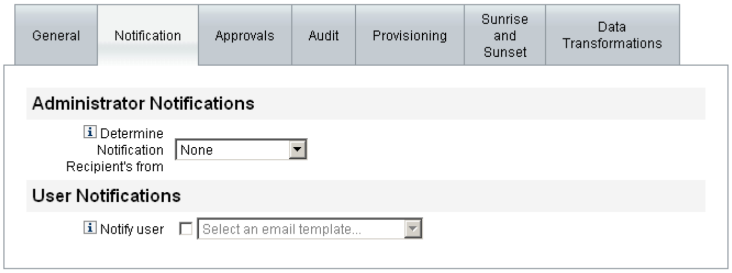
4. When you are finished, you can
   - Select a different tab to continue editing the templates.
   - Click **Save** to save your changes and return to the Configure Tasks page.
   - Click **Cancel** to discard your changes and return to the Configure Tasks page.

Configuring the Notification Tab

All of the Task Templates support sending email notifications to administrators and users when Identity Manager invokes a process — usually after the process has completed. You can use the Notification tab to configure these notifications.

Note Identity Manager uses email templates to deliver information and requests for action to administrators, approvers, and users. For more information about Identity Manager email templates, see the section titled Understanding Email Templates in this guide.

The following figure shows the Notification page for the Create User Template.



Administrator Notifications

Determine Notification Recipient's from: None

User Notifications

Notify user ☐ Select an email template...

Figure 6. Notification Tab: Create User Template

To specify how Identity Manager will determine notification recipients, use the following process:

1. Complete the Administrator Notifications section.
2. Complete the User Notifications section.
3. When you are finished, you can
   - Select a different tab to continue editing the templates.
   - Click **Save** to save your changes and return to the Configure Tasks page.
   - Click **Cancel** to discard your changes and return to the Configure Tasks page.

Configuring Administrator Notifications

Select an option from the **Determine Notification Recipients from** menu to determine the method for notifying administrator recipients.

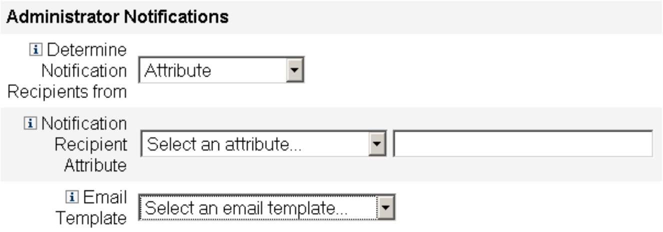
- **None** (default) — No administrators will be notified.
- **Attribute** — Select to derive notification recipients' account IDs from a specified attribute in the user view. Continue to *Specifying Recipients by Attribute* on page 9-8.
- **Rule** — Select to derive notification recipients' account IDs by evaluating a specified rule. Continue to *Specifying Recipients by Rule* on page 9-9.
- **Query** — Select to derive notification recipients' account IDs by formulating a query to a particular resource. Continue to *Specifying Recipients by Query* on page 9-10.
- **Administrator List** — Select to choose notification recipients' explicitly from a list. Continue to *Specifying Recipients from the Administrators List* on page 9-11.

Specifying Recipients by Attribute

To derive notification recipients' account IDs from a specified attribute, use the following steps:

Note The attribute must resolve to a string that represents a single account ID or to a list in which the elements are account IDs.

1. Select **Attribute** from the **Determine Notification Recipients from** menu and the following new options display:



Administrator Notifications

Determine Notification Recipients from: Attribute

Notification Recipient Attribute: Select an attribute...

Email Template: Select an email template...

Figure 7. Administrator Notifications: Attribute

   - **Notification Recipient Attribute** — Provides a list of attributes (currently defined for the view associated with the task configured by this template) used to determine recipient account IDs.
   - **Email Template** — Provides a list of email templates.

2. Select an attribute from the **Notification Recipient Attribute** menu.

   The attribute name displays in the text field adjacent to the menu.

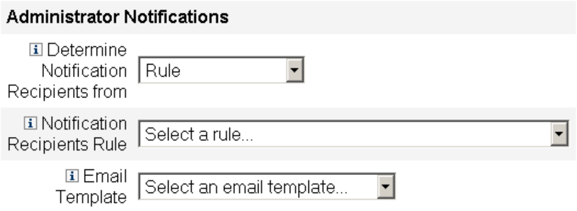
3. Select a template from the **Email Template** menu to specify a format for the administrators' notification email.

Specifying Recipients by Rule

To derive notification recipients' account IDs from a specified rule, use the following steps:

Note When evaluated, the rule must return a string that represents a single account ID or to a list in which the elements are account IDs.

1. Select **Rule** from the **Determine Notification Recipients from** menu and the following new options display in the Notification form:



Administrator Notifications

Determine Notification Recipients from: Rule

Notification Recipients Rule: Select a rule...

Email Template: Select an email template...

Figure 8. Administrator Notifications: Rule

   - **Notification Recipient Rule** — Provides a list of rules (currently defined for your system) that, when evaluated, returns the recipients' account IDs.

  - **Email Template** — Provides a list of email templates.

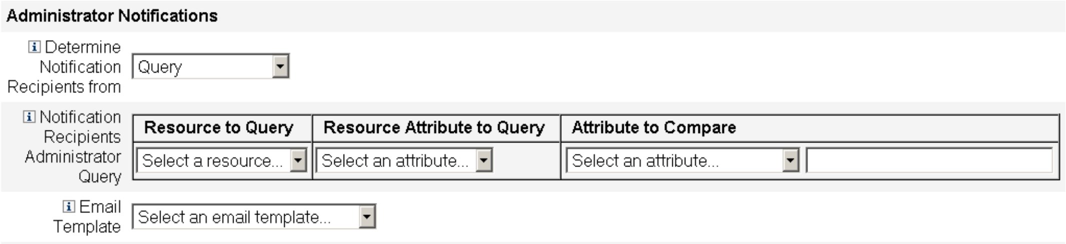
2. Select a rule from the **Notification Recipient Rule** menu.
3. Select a template from the **Email Template** menu to specify a format for the administrators' notification email.

Specifying Recipients by Query

Note Only LDAP and Active Directory resource queries are supported at this time.

To derive notification recipients' account IDs by querying a specified resource, use the following steps:

1. Select **Query** from the **Determine Notification Recipients from** menu and the following new options display in the Notification form:



Administrator Notifications

Determine Notification Recipients from: Query

Notification Recipients Administrator Query:

Resource to Query	Resource Attribute to Query	Attribute to Compare	
Select a resource...	Select an attribute...	Select an attribute...	

Email Template: Select an email template...

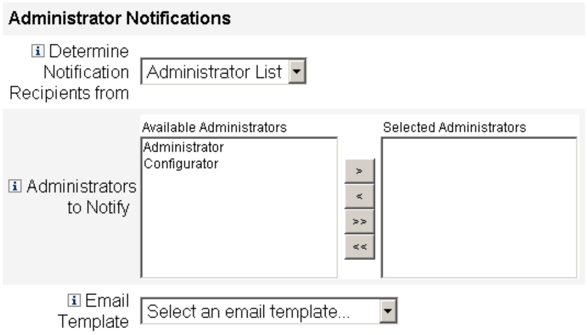
Figure 9. Administrator Notifications: Query

  - **Notification Recipient Administrator Query** — Provides a table consisting of the following menus, which you can use to construct a query:
    - **Resource to Query** — Provides a list of resources currently defined for your system.
    - **Resource Attribute to Query** — Provides a list of resource attributes currently defined for your system.
    - **Attribute to Compare** — Provides a list of attributes currently defined for your system.
  - **Email Template** — Provides a list of email templates.

2. Select a resource, resource attribute, and an attribute to compare from these menus to construct the query.
3. Select a template from the **Email Template** menu to specify a format for the administrators' notification email.

Specifying Recipients from the Administrators List

Select **Administrators List** from the **Determine Notification Recipients from** menu and the following new options display in the Notification form:



Administrator Notifications

Determine Notification Recipients from: Administrator List

Administrators to Notify

Available Administrators: Administrator, Configurator

Selected Administrators:

Email Template: Select an email template...

Figure 10. Administrator Notifications: Administrators List

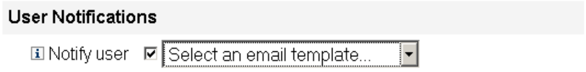
- **Administrators to Notify** — Provides a selection tool with a list of available administrators.
- **Email Template** — Provides a list of email templates.

4. Select one or more administrators in the Available Administrators list and use the > button or >> button to move the selected name(s) to the Selected Administrators list.
5. Select a template from the **Email Template** menu to specify a format for the administrators' notification email.

Configuring User Notifications

When specifying users to be notified, you must also specify the name of an email template to be used to generate the email used for notification.

To notify the user being created, updated, or deleted enable the **Notify user** checkbox and then select an email template from the menu.



User Notifications

Notify user ☑ Select an email template...

Figure 11. Specifying an Email Template

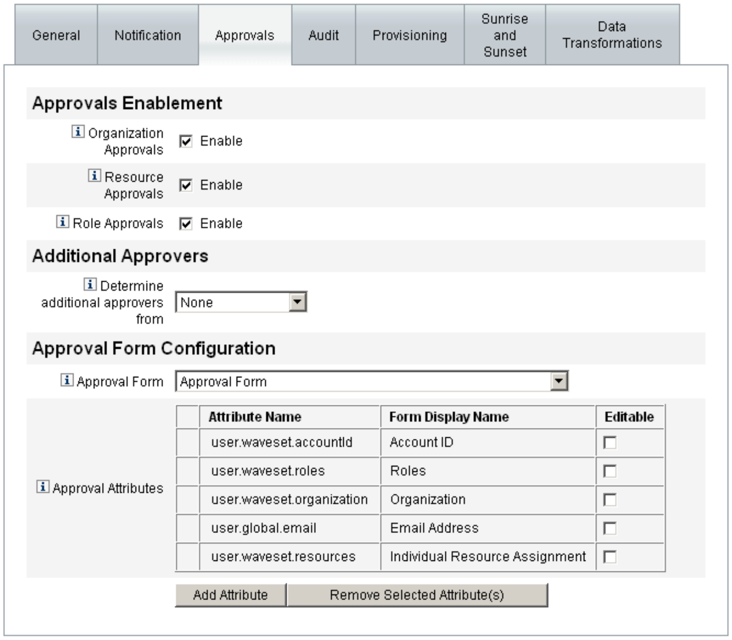
Configuring the Approvals Tab

You can use the Approvals tab to designate additional approvers and to specify attributes for the task approval form before Identity Manager executes the create, delete, or update user tasks.

Traditionally, administrators who are associated with a particular organization, resource, or role are required to approve certain tasks before execution. Identity Manager also allows you to designate *additional approvers* — additional administrators who will be required to approve the task.

Note If you configure Additional Approvers for a workflow, you are requiring approval from the traditional approvers *and* from any additional approvers specified in the template.

The following figure illustrates the initial Approvals page administrative user interface



Approvals Enablement

Organization Approvals ☑ Enable

Resource Approvals ☑ Enable

Role Approvals ☑ Enable

Additional Approvers

Determine additional approvers from None

Approval Form Configuration

Approval Form Approval Form

Approval Attributes

	Attribute Name	Form Display Name	Editable
	user.waveset.accountId	Account ID	□
	user.waveset.roles	Roles	□
	user.waveset.organization	Organization	□
	user.global.email	Email Address	□
	user.waveset.resources	Individual Resource Assignment	□

Figure 12. Approvals Tab: Create User Template

To configure approvals, use the following process:

1. Complete the Approvals Enablement section (see “Enabling Approvals” on page 13).
2. Complete the Additional Approvers section (see “Specifying Additional Approvers” on page 14).
3. Complete the Approval Form Configuration section for the Create User and Update User Templates only (see “Configuring the Approval Form” on page 22).
4. When you are finished configuring the Approvals tab, you can
   - Select a different tab to continue editing the templates.
   - Click **Save** to save your changes and return to the Configure Tasks page.
   - Click **Cancel** to discard your changes and return to the Configure Tasks page.

Enabling Approvals

Use the following **Approvals Enablement** checkboxes to require approvals before the create user, delete user, or update user tasks can proceed.

Note By default, these checkboxes are enabled for the Create User and Update User Templates, but they are *disabled* for the Delete User Template.

- **Organization Approvals** — Enable this checkbox to require approvals from any configured organizational approvers.
- **Resource Approvals** — Enable this checkbox to require approvals from any configured resource approvers.
- **Role Approvals** — Enable this checkbox to require approvals from any configured role approvers.

Specifying Additional Approvers

Use the **Determine additional approvers from** menu to specify how Identity Manager will determine additional approvers for the create user, delete user, or update user tasks. The options on this menu include:

Option	Description
None (default)	No additional approvers are required for task execution.
Attribute	Approvers' account IDs are derived from within an attribute specified in the user's view.
Rule	Approvers' account IDs are derived by evaluating a specified rule.
Query	Approvers' account IDs are derived by querying a particular resource.
Administrator List	Approvers are chosen explicitly from a list.

When you select any of these options (except **None**), additional options display in the administrative user interface. Instructions for configuring these options begin on page 14.

Use the instructions provided in the following sections to specify a method for determining additional approvers.

- From Attributes (page 15)
- From Rules (page 16)
- From a Query (page 17)
- From the Administrators List (page 18)

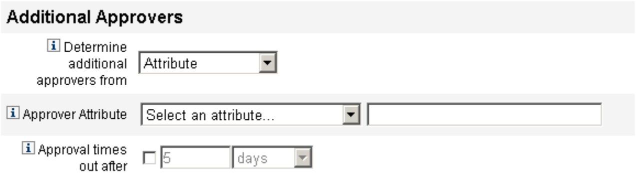
From Attributes

To determine additional approvers from an attribute,

1. Select **Attribute** from the **Determine additional approvers from** menu.

Note The attribute must resolve to a string that represents a single account ID or to a list in which the elements are account IDs.

The following new options display:



Additional Approvers

Determine additional approvers from: Attribute

Approver Attribute: Select an attribute...

Approval times out after: □ 5 days

Figure 13. Additional Approvers: Attribute

- **Approver Attribute** — Provides a list of attributes (currently defined for the view associated with the task configured by this template) used to determine approvers' account IDs.
- **Approval times out after** — Provides a method for specifying when the approval will time out.

Note The **Approval times out after** setting affects both initial approvals and escalated approvals.

2. Use the **Approver Attribute** menu to select an attribute.

   The selected attribute displays in the adjacent text field.

3. Decide whether you want the approval request to timeout after a specified period of time.
   - If you want to specify a timeout period, continue to *Configuring Approval Timeouts* on page 9-19 for instructions.
   - If you do not want to specify a timeout period, you can continue to *Configuring the Approval Form* on page 22 or save your changes and go on to configure a different tab.

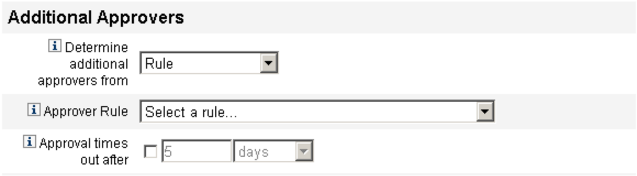
From Rules

To derive the approvers' account IDs from a specified rule, use the following steps:

1. Select **Rule** from the **Determine additional approvers from** menu.

Note When evaluated, the rule must return a string that represents a single account ID or to a list in which the elements are account IDs.

The following new options display.



Additional Approvers

Determine additional approvers from: Rule

Approver Rule: Select a rule...

Approval times out after: □ 5 days

Figure 14. Additional Approvers: Rule

- **Approver Rule** — Provides a list of rules (currently defined for your system) that, when evaluated, returns the recipients' account IDs.
- **Approval times out after** — Provides a method for specifying when the approval will time out.

Note The **Approval times out after** setting affects both initial approvals and escalated approvals.

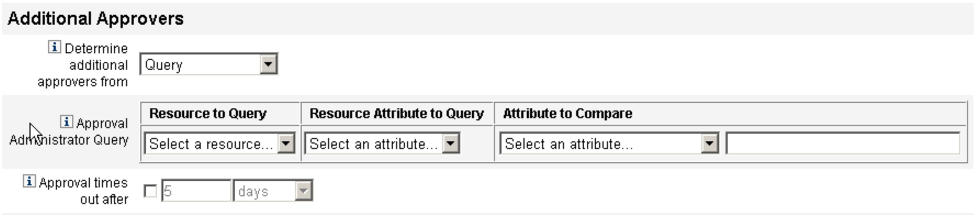
2. Select a rule from the **Approver Rule** menu.
3. Decide whether you want the approval request to timeout after a specified period of time.
   - If you want to specify a timeout period, continue to *Configuring Approval Timeouts* on page 9-19 for instructions.
   - If you do not want to specify a timeout period, you can continue to *Configuring the Approval Form* on page 22 or save your changes and go on to configure a different tab.

From a Query

Note Only LDAP and Active Directory resource queries are supported at this time.

To derive approvers account IDs by querying a specified resource, use these steps:

1. Select **Query** from the **Determine additional approvers from** menu and the following new options display:



Additional Approvers

Determine additional approvers from: Query

Approval Administrator Query:

Resource to Query	Resource Attribute to Query	Attribute to Compare	
Select a resource...	Select an attribute...	Select an attribute...	

Approval times out after: □ 5 days

Figure 15. Additional Approvers: Query

- **Approval Administrator Query** — Provides a table consisting of the following menus, which you can use to construct a query:
  - **Resource to Query** — Provides a list of resources currently defined for your system.
  - **Resource Attribute to Query** — Provides a list of resource attributes currently defined for your system.
  - **Attribute to Compare** — Provides a list of attributes currently defined for your system.
- **Approval times out after** — Provides a method for specifying when the approval will time out.

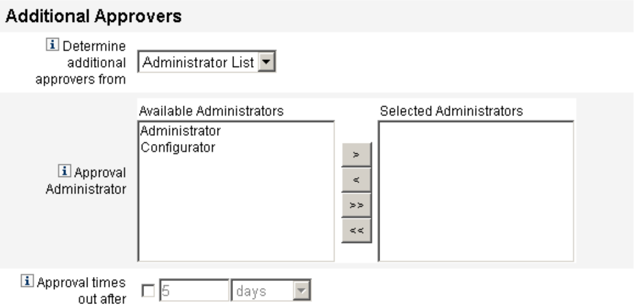
Note The **Approval times out after** setting affects both initial approvals and escalated approvals.

2. Construct a query as follows:
   a. Select a resource from the **Resource to Query** menu.
   b. Select attributes from the **Resource Attribute to Query** and **Attribute to Compare** menus.
3. Decide whether you want the approval request to timeout after a specified period of time.
   - If you want to specify a timeout period, continue to *Configuring Approval Timeouts* on page 9-19 for instructions.
   - If you do not want to specify a timeout period, you can continue to *Configuring the Approval Form* on page 22 or save your changes and go on to configure a different tab.

From the Administrators List

To explicitly choose additional approvers from the Administrators List,

1. Select **Administrators List** from the **Determine additional approvers from** menu and the following new options display:



Additional Approvers

Determine additional approvers from: Administrator List

Available Administrators: Administrator, Configurator

Selected Administrators:

Approval times out after: □ 5 days

Figure 16. Additional Approvers: Administrators List

- **Administrators to Notify** — Provides a selection tool with a list of available administrators.
- **Approval Form** — Provides a list of user forms additional approvers can use to approve or reject an approval request.
- **Approval times out after** — Provides a method for specifying when the approval will time out.

Note The **Approval times out after** setting affects both initial approvals and escalated approvals.

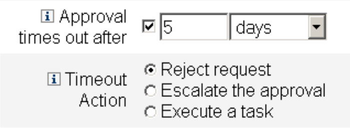
2. Select one or more administrators in the Available Administrators list and use the > button or >> button to move the selected name(s) to the Selected Administrators list.
3. Decide whether you want the approval request to timeout after a specified period of time.
   - If you want to specify a timeout period, continue to *Configuring Approval Timeouts* on page 9-19 for instructions.
   - If you do not want to specify a timeout period, you can continue to *Configuring the Approval Form* on page 22 or save your changes and go on to configure a different tab.

Configuring Approval Timeouts

To configure an approval timeouts,

1. Enable the checkbox.

   The adjacent text field and menu become active, and the **Timeout Action** buttons display, as shown in the following figure.



Approval times out after ☑ 5 days

Timeout Action ● Reject request ○ Escalate the approval ○ Execute a task

Figure 17. Approval Timeout Options

2. Use the **Approval times out after** text field and menu to specify a timeout period as follows:

   a. Select seconds, minutes, hours, or days from the menu.

   b. Enter a number in the text field to indicate how many seconds, minutes, hours, or days you want to specify for the timeout.

Note The **Approval times out after** setting affects both initial approvals and escalated approvals.

3. Enable one of the following **Timeout Action** buttons to specify what happens when the approval request times out:

   - **Reject Request** — Identity Manager automatically rejects the request if it is not approved before the specified timeout period.
   - **Escalate the approval** — Identity Manager automatically escalates the request to another approver if the request is not approved before the specified timeout period.

     When you enable this button, new options display because you must specify how Identity Manager will determine approvers for an escalated approval. Continue to *Escalating Approvals* on page 9-20 for instructions.
   - **Execute a task** — Identity Manager automatically executes an alternate task if the approval request is not approved before the specified timeout period.

     Enable this button and the **Approval Timeout Task** menu displays so you can specify a task to execute if the approval request times out. Continue to *Executing a Task* on page 9-22 for instructions.

Escalating Approvals

When you enable the Timeout Action **Escalate the approval** button, the **Determine escalation approvers from** menu displays as follows:

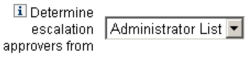

Determine escalation approvers from: Administrator List

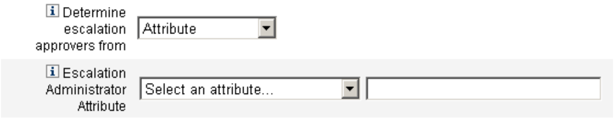
Figure 18. Determine Escalation Approvers From Menu

Select one of the following options from this menu to specify how approvers are determined for an escalated approval.

- **Attribute** — Determine approver account IDs from within an attribute specified in the new user’s view.

Note The attribute must resolve to a string that represents a single account ID or to a list in which the elements are account IDs.

When the **Escalation Administrator Attribute** menu displays, select an attribute from the list. The selected attribute displays in the adjacent text field.


Determine escalation approvers from: Attribute

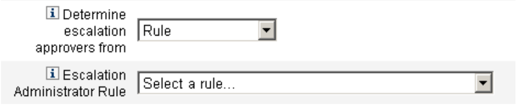
Escalation Administrator Attribute: Select an attribute...

Figure 19. Escalation Administrator Attribute Menu

- **Rule** — Determine approver account IDs by evaluating a specified rule.

Note When evaluated, the rule must return a string that represents a single account ID or to a list in which the elements are account IDs.

When the **Escalation Administrator Rule** menu displays, select a rule from the list.


Determine escalation approvers from: Rule

Escalation Administrator Rule: Select a rule...

Figure 20. Escalation Administrator Rule Menu

- **Query** — Determine approvers account IDs by querying a particular resource.

  When the **Escalation Administrator Query** menus display, build your query as follows:

  a. Select a resource from the **Resource to Query** menu.

  b. Select an attribute from the **Resource Attribute to Query** menu.

  c. Select an attribute from the **Attribute to Compare** menu.

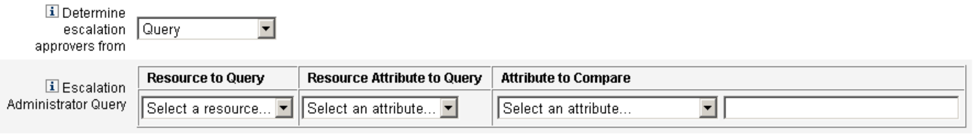

Determine escalation approvers from: Query

Figure 21. Escalation Administrator Query Menu

- **Administrator List** (default) — Choose approvers explicitly from a list.

  When the **Escalation Administrator** selection tool displays, select approver(s) as follows:

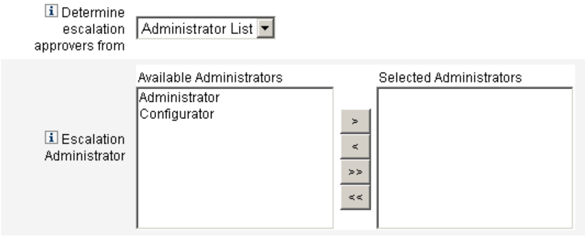

Determine escalation approvers from: Administrator List

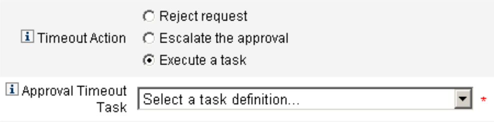
Figure 22. Escalation Administrator Selection Tool

  a. Select one or more administrator's names from the **Available Administrators** list.

  b. Use the > button or the >> button to move the name(s) to the **Selected Administrators** list.

Executing a Task

When you enable the Timeout Action **Execute a task** button, the **Approval Timeout Task** menu displays as follows:



Timeout Action
○ Reject request
○ Escalate the approval
● Execute a task

Approval Timeout Task: Select a task definition... *

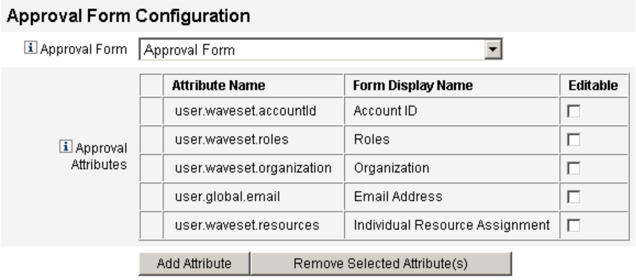
Figure 23. Approval Timeout Task Menu

Specify a task to execute if the approval request times out. For example, you might allow the requester to submit a help desk request or send a report to the Administrator.

Configuring the Approval Form

Note The Delete User Template does not contain an Approval Form Configuration section. You can configure this section for Create User and Update User Templates only.

You can use features in the Approval Form Configuration section to select an approval form, and add attributes to (or remove attributes from) the approval form.



Approval Form Configuration

Approval Form: Approval Form

Approval Attributes

	Attribute Name	Form Display Name	Editable
	user.waveset.accountId	Account ID	□
	user.waveset.roles	Roles	□
	user.waveset.organization	Organization	□
	user.global.email	Email Address	□
	user.waveset.resources	Individual Resource Assignment	□

Figure 24. Approval Form Configuration

By default, the Approval Attributes table contains the following standard attributes:

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

Note The default approval form was instrumented to allow approval attributes to display. If you are using an approval form other than the default form, you must instrument your form to display the approval attributes specified in the Approval Attributes table.

To configure an Approval form for additional approvers:

1. Select a form from the **Approval Form** menu.

   Approvers will use this form to approve or reject an approval request.

2. Enable checkboxes in the **Editable** column of the **Approval Attributes** table to allow approvers to edit the attribute value.

   For example, if you enable the `user.waveset.accountId` checkbox the approver can change the user's account ID.

Note If you modify any account-specific attribute values in the approval form, you will also override any global attribute values with the same name when the user is actually provisioned.

For example, if resource `R1` exists in your system with a `description` schema attribute, and you add `user.accounts[R1].description` attribute to the approval form as an editable attribute, any changes to the `description` attribute value in the approval form will override the value propagated from `global.description` for resource `R1` only.

3. Click the **Add Attribute** or **Remove Selected Attribute(s)** buttons to specify attributes from the new user's account data to display in the approval form.

   - To add attributes to the form, see "Adding Attributes" on page 24.
   - To remove attributes to the form, see "Removing Attributes" on page 24.

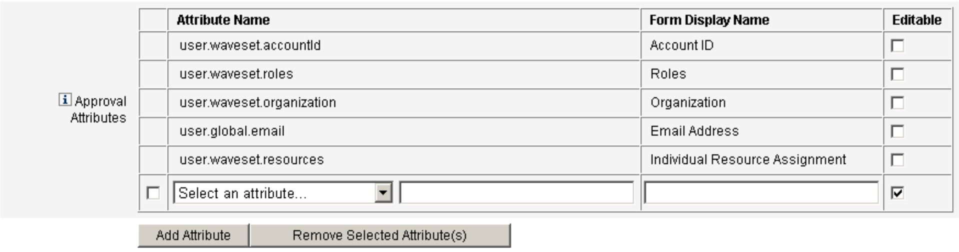
Note You cannot remove the default attributes from an approval form unless you modify the XML file.

Adding Attributes

To add attributes to the approval form

1. Click the **Add Attribute** button located under the Approval Attributes table.

   The **Attribute name** menu becomes active in the Approval Attributes table, as shown in the following figure:



Approval Attributes

	Attribute Name	Form Display Name	Editable
	user.waveset.accountId	Account ID	☐
	user.waveset.roles	Roles	☐
	user.waveset.organization	Organization	☐
	user.global.email	Email Address	☐
	user.waveset.resources	Individual Resource Assignment	☐
☐	Select an attribute...		☑

Figure 25. Adding Approval Attributes

2. Select an attribute from the menu.

   The selected attribute name displays in the adjacent text field and the attribute's default display name displays in the Form Display Name column.

   For example, if you select the `user.waveset.organization` attribute, the table will contain the following information:

   - If necessary, you can change the default attribute name or the default Form Display Name by typing a new name into the appropriate text field.
   - Enable the **Editable** checkbox if you want to allow the approver to change the attribute's value.

     For example, the approver may want to override information such as the user's email address.

3. Repeat these steps to specify additional attributes.

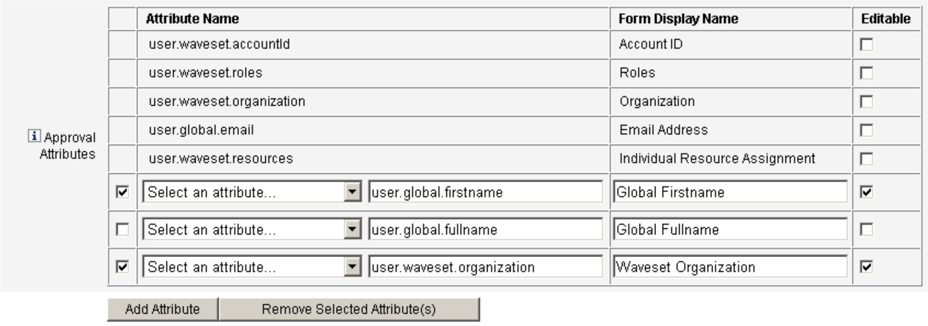
Removing Attributes

Note You cannot remove the default attributes from an approval form unless you modify the XML file.

To remove attributes from the approval form, use the following steps:

1. Enable one or more checkboxes in the leftmost column of the Approval Attributes table.
2. Click the **Remove Selected Attribute(s)** button to immediately remove the selected attributes from the Approval Attributes table.

For example, `user.global.firstname` and `user.waveset.organization` would be removed from the following table when you clicked the **Remove Selected Attribute(s)** button.



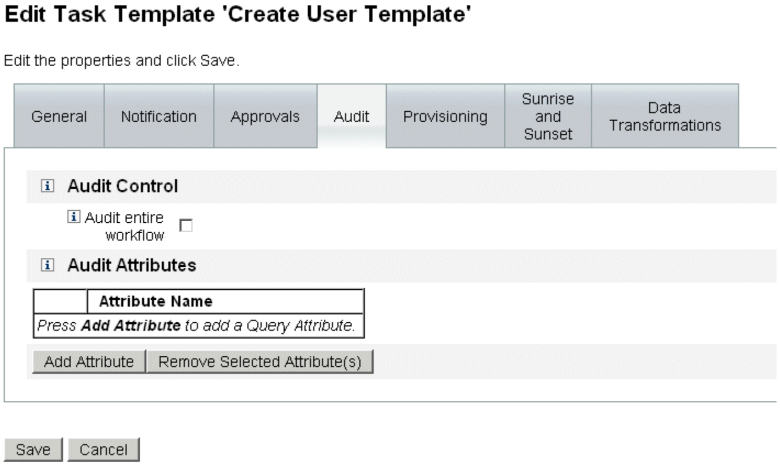
Approval Attributes

	Attribute Name		Form Display Name	Editable
	user.waveset.accountId		Account ID	□
	user.waveset.roles		Roles	□
	user.waveset.organization		Organization	□
	user.global.email		Email Address	□
	user.waveset.resources		Individual Resource Assignment	□
☑	Select an attribute...	user.global.firstname	Global Firstname	☑
□	Select an attribute...	user.global.fullname	Global Fullname	□
☑	Select an attribute...	user.waveset.organization	Waveset Organization	☑

Figure 26. Removing Approval Attributes

Configuring the Audit Tab

All of the configurable Task Templates support configuring workflows to audit certain tasks. Specifically, you can configure the Audit tab to control whether workflow events will be audited and specify which attributes will be stored for reporting purposes.



Edit Task Template 'Create User Template'

Edit the properties and click Save.

Audit Control

Audit entire workflow □

Audit Attributes

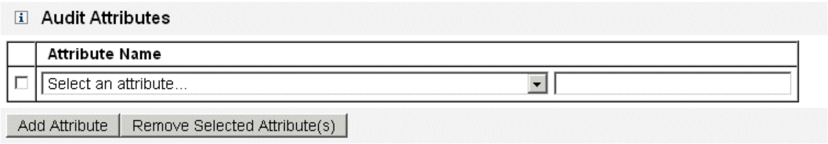
	Attribute Name
*Press **Add Attribute** to add a Query Attribute.*	

Figure 27. Audit Create User Template

To configure auditing from the User Template's Audit tab:

1. Enable the **Audit entire workflow** checkbox to activate the workflow auditing feature.
2. Click the **Add Attribute** button (located in the Audit Attributes section) to select attributes you want to record for reporting purposes.
3. When the **Select an attribute** menu displays in the Audit Attributes table, select an attribute from the list.

   The attribute name will display in the adjacent text field.

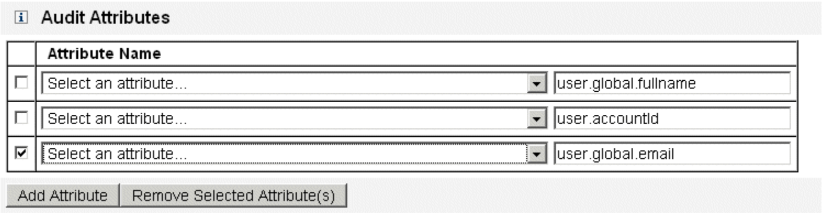


	Attribute Name	
□	Select an attribute...	

Figure 28. Adding an Attribute

To remove attributes from the Audit Attributes table,

1. Enable the checkbox adjacent to the attribute you want to remove.



	Attribute Name	
□	Select an attribute...	user.global.fullname
□	Select an attribute...	user.accountId
☑	Select an attribute...	user.global.email

Figure 29. Removing the user.global.email Attribute

2. Click the **Remove Selected Attribute(s)** button.

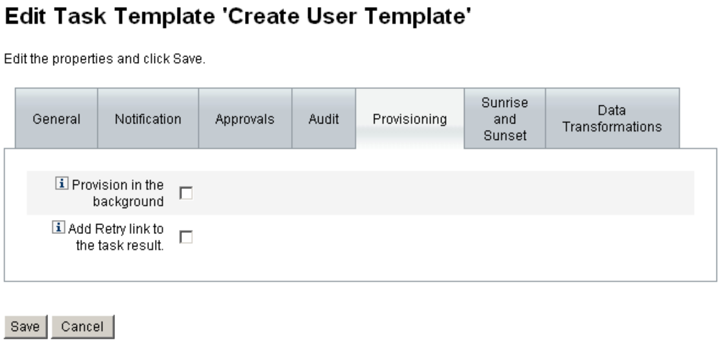
When you are finished configuring this tab, you can

- Select a different tab to continue editing the template(s).
- Click **Save** to save your changes and return to the Configure Tasks page.
- Click **Cancel** to discard your changes and return to the Configure Tasks page.

Configuring the Provisioning Tab

Note This tab is available for the Create and Update User Templates only.

You can use the Provisioning tab to configure the following options, which are related to provisioning:



Edit Task Template 'Create User Template'

Edit the properties and click Save.

Provision in the background □

Add Retry link to the task result. □

Figure 30. Provisioning Tab: Create User Template

- **Provision in the background** – Enable this checkbox to run a create, delete, or update task in the background instead of running the task synchronously.

  Provisioning in the background allows you to continue working in Identity Manager while the task executes.
- **Add Retry link to the task result** – Enable this checkbox to add a **Retry** link to the user interface when a provisioning error results from task execution. The **Retry** link allows the user to attempt the task again if it failed on the first attempt.

When you are finished configuring the Provisioning tab, you can

- Select a different tab to continue editing the template.
- Click **Save** to save your changes and return to the Configure Tasks page.
- Click **Cancel** to discard your changes and return to the Configure Tasks page.

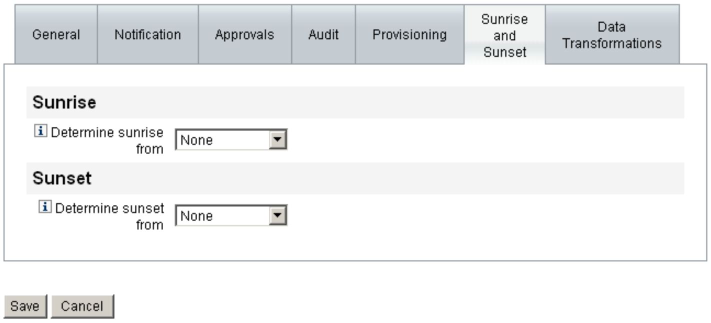
Configuring the Sunrise and Sunset Tab

Note This tab is available for the Create User Template only.

You use the Sunrise and Sunset tab to select a method for determining the time and date when

- Provisioning will take place for a new user (*sunrise*).
- Deprovisioning will take place for a new user (*sunset*).

  For example, you can specify a sunset date for a temporary worker whose contract expires after six months.



Sunrise

Determine sunrise from: None

Sunset

Determine sunset from: None

Figure 31. Sunrise and Sunset Tab: Create User Template

The rest of this section provides instructions for configuring the Sunrise and Sunset tab. The information is organized as follows:

- “Configuring Sunrises” on page 28
- “Configuring Sunsets” on page 31

Configuring Sunrises

This section provides instructions for determining the time and date provisioning will take place for a new user, and for specifying the user who will own the work item for sunrise.

To configure sunrises:

1. Select one of the following options from the **Determine sunrise from** menu to specify how Identity Manager will determine a time and date for provisioning.
   - **Specifying a Time** — Delays provisioning until a specified time in the future. Continue to page 29 for instructions.
   - **Specifying a Date** — Delays provisioning until a specified calendar date in the future. Continue to page 29 for instructions.
   - **Specifying an Attribute** — Delays provisioning until a specified date and time based on the attribute’s value in the user’s view. The attribute must contain a date/time string. When specifying an attribute to contain a date/time string, you can specify a data format to which the data is expected to conform.

     Continue to page 30 for instructions.

- **Specifying a Rule** — Delays provisioning based on a rule that, when evaluated, produces a date/time string. As when specifying an attribute, you can specify a data format to which the data is expected to conform.

  Continue to page 30 for instructions.

Note The **Determine sunrise from** menu defaults to the **None** option, which allows provisioning to take place immediately.

2. Select a user from the **Work Item Owner** menu to specify who will own the work item for sunrise.

Note Sunrise work items are available from the Approvals tab.

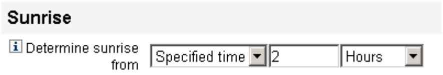
3. When you are finished configuring sunrises, you can
   - Select a different tab to continue editing the Create User Template.
   - Click **Save** to save your changes and return to the Configure Tasks page.
   - Click **Cancel** to discard your changes and return to the Configure Tasks page.

Specifying a Time

To delay provisioning until a specified time,

1. Select **Specified time** from the **Determine sunrise from** menu.
2. When a new text field and menu display to the right of the **Determine sunrise from** menu, type a number into the blank text field and select a unit of time from the menu.

   For example, if you want to provision a new user in two hours, specify the following:



Sunrise

Determine sunrise from: Specified time | 2 | Hours

Figure 32. Provisioning a New User in Two Hours

Specifying a Date

To delay provisioning until a specified calendar date,

1. Select **Specified day** from the **Determine sunrise from** menu.

   The following new menus display to the right of the **Determine sunrise from** menu.

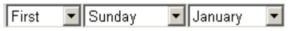
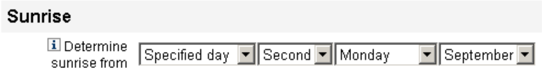


Figure 33. New Menus

2. Use these new menus to specify which week, which day of the week, and which month the provisioning should occur.

   For example, if you want to provision a new user on the second Monday in September, specify the following:



Sunrise

Determine sunrise from: Specified day | Second | Monday | September

Figure 34. Provisioning a New User by Date

Specifying an Attribute

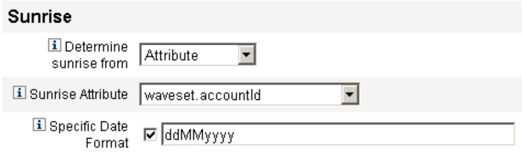
To determine the provisioning date and time based on the value of an attribute in the users account data,

1. Select **Attribute** from the **Determine sunrise from** menu and the following options become active:
   - **Sunrise Attribute** menu – Provides a list of attributes currently defined for the view associated with the task configured by this template.
   - **Specific Date Format** checkbox and menu – Enables you to specify a date format string for the attribute value (if necessary).

Note If you do not enable the **Specific Date Format** checkbox, date strings must conform to a format that is acceptable to the `FormUtil` method's `convertDateToString`. Consult the product documentation for a complete list of supported date formats.

2. Select an attribute from the **Sunrise Attribute** menu.
3. If necessary, enable the **Specific Date Format** checkbox and when the **Specific Date Format** field becomes active, enter a date format string.

   For example, to provision a new user based on their `waveset.accountId` attribute value using a day, month, and year format specify the following:



Sunrise

Determine sunrise from: Attribute

Sunrise Attribute: waveset.accountId

Specific Date Format: ☑ ddMMyyyy

Figure 35. Provisioning a New User by Attribute

Specifying a Rule

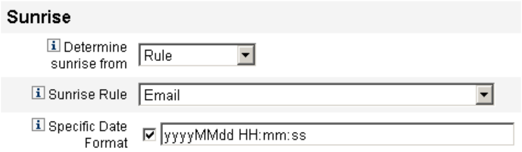
To determine the provisioning date and time by evaluating a specified rule,

1. Select **Rule** from the **Determine sunrise from** menu and the following options become active:
   - **Sunrise Rule** menu – Provides a list of rules currently defined for your system.
   - **Specific Date Format** checkbox and menu – Enables you to specify a date format string for the rule's returned value (if necessary).

Note If you do not enable the **Specific Date Format** checkbox, date strings must conform to a format that is acceptable to the `FormUtil` method's `convertDateToString`. Consult the product documentation for a complete list of supported date formats.

2. Select a rule from the **Sunrise Rule** menu.
3. If necessary, enable the **Specific Date Format** checkbox and when the **Specific Date Format** field becomes active, enter a date format string.

   For example, to provision a new user based on the Email rule using a year, month, day, hours, minutes, and seconds format specify the following:



Sunrise

Determine sunrise from: Rule

Sunrise Rule: Email

Specific Date Format: ☑ yyyyMMdd HH:mm:ss

Figure 36. Provisioning a New User by Rule

Configuring Sunsets

The options and procedures for configuring sunsets (deprovisioning) are essentially the same as those provided for sunrises (provisioning) in the Configuring Sunrises section.

The only difference is that the Sunset section also provides a **Sunset Task** menu because you must specify a task to deprovision the user on the specified date and time.

To configure a sunset,

1. Use the **Determine sunset from** menu to specify the method for determining when deprovisioning will take place:

Note The **Determine sunset from** menu defaults to the **None** option, which allows deprovisioning to take place immediately.

   - **Specified time** – Delays deprovisioning until a specified time in the future. Review "Specifying a Time" on page 29 for instructions.

- **Specified date** – Delays deprovisioning until a specified calendar date in the future. Review “Specifying a Date” on page 29 for instructions.
- **Attribute** – Delays deprovisioning until a specified date and time based on the attribute’s value in the users’ account data. The attribute must contain a date/time string. When specifying an attribute to contain a date/time string, you can specify a date format to which the data is expected to conform.

  Review “Specifying an Attribute” on page 30 for instructions.
- **Rule** – Delays deprovisioning based on a rule that, when evaluated, produces a date/time string. As when specifying an attribute, you can specify a date format to which the data is expected to conform.

  Review “Specifying a Rule” on page 30 for instructions.

2. Use the **Sunset Task** menu to specify a task to deprovision the user on the specified date and time.
3. When you are finished configuring this tab, you can
   - Select a different tab to continue editing the template.
   - Click **Save** to save your changes and return to the Configure Tasks page.
   - Click **Cancel** to discard your changes and return to the Configure Tasks page.

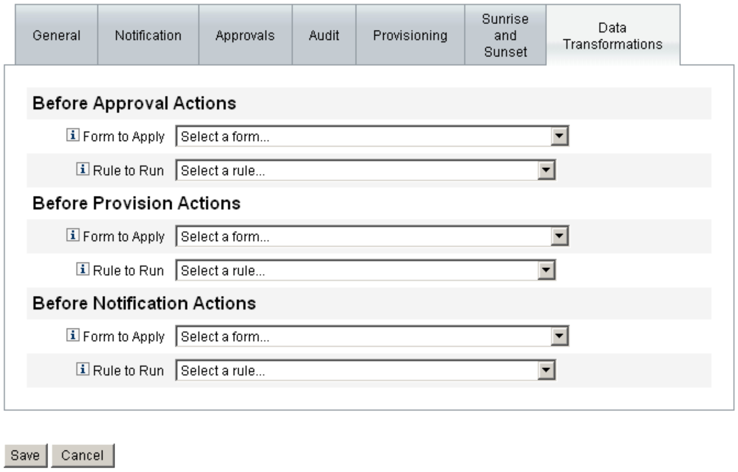
Configuring the Data Transformations Tab

Note This tab is available for the Create and Update User Templates only.

If you want to alter user account data as the workflow executes, you can use the Data Transformations tab to specify how Identity Manager will transform the data during provisioning.

For example, if you want forms or rules to generate email addresses that conform to company policy or if you want to generate sunrise or sunset dates.

When you select the Data Transformations tab, the following page displays:



Before Approval Actions

Form to Apply: Select a form...

Rule to Run: Select a rule...

Before Provision Actions

Form to Apply: Select a form...

Rule to Run: Select a rule...

Before Notification Actions

Form to Apply: Select a form...

Rule to Run: Select a rule...

Figure 37. Data Transformations Tab: Create User Template

This page consists of the following sections:

- **Before Approval Actions** – Configure the options in this section if you want to transform user account data before sending approval requests to specified approvers.
- **Before Provision Actions** – Configure the options in this section if you want to transform user account data before a provisioning action.
- **Before Notification Actions** – Configure the options in this section if you want to transform user account data before notifications are sent to specified recipients.

You can configure the following options in each section:

- **Form to Apply** menus – Provide a list of the forms currently configured for your system. Use these menus to specify forms that will be used to transform data from the users accounts.
- **Rule to Run** menus – Provide a list of the rules currently configured for your system. Use these menus to specify rules that will be used to transform data from the users accounts.

When you are finished configuring this tab, you can

- Select a different tab to continue editing the template.
- Click **Save** to save your changes and return to the Configure Tasks page.
- Click **Cancel** to discard your changes and return to the Configure Tasks page.

10 PasswordSync

This chapter describes the Sun Java™ System Identity Manager PasswordSync feature, which enables Windows clients changing passwords in their Windows Active Directory and Windows NT domains to synchronize the changes with Identity Manager.

What is PasswordSync?

The PasswordSync feature keeps user password changes made on Windows Active Directory and Windows NT domains synchronized with other resources defined in Identity Manager. PasswordSync must be installed on each domain controller in the domains that will be synchronized with Identity Manager. PasswordSync must be installed separately from Identity Manager.

When PasswordSync has been installed on a domain controller, the controller communicates with a servlet that acts as a proxy for a Java Messaging Service (JMS) client. The servlet in turn communicates with a JMS-enabled message queue. A JMS Listener resource adapter removes messages from the queue and processes the password changes using a workflow task. The password is updated on all of the user’s assigned resources, and an SMTP server sends an email to the user, notifying the user of the status of the password change.

Note A password change must pass the native password policy for the change request to be forwarded to the Identity Manager server for synchronization. If the proposed password change does not meet the native password policy, the ADSI displays an error dialog, and no synchronization data is sent to Identity Manager.

Before You Install PasswordSync

The PasswordSync feature can be set up only on Windows 2000, Windows 2003, and Windows NT domain controllers. You must install PasswordSync on each domain controller in the domains that will be synchronized with Identity Manager.

PasswordSync requires connectivity with a JMS server. See the documentation for the JMS Listener resource adapter in the *Identity Manager Resources Reference* for information about the requirements for the JMS system.

In addition, PasswordSync requires that

- Microsoft .NET 1.1 or later must be installed on each domain controller
- Any previous versions of PasswordSync must be removed

These requirements are discussed in detail in the following sections.

Install Microsoft .NET 1.1

To use PasswordSync, you must install the Microsoft .NET 1.1 (or later) Framework. This Framework is installed by default if you are using a Windows 2003 domain controller. If you are using a Windows 2000 or Windows NT domain controller, you can download the toolkit from the Microsoft Download Center at:

http://www.microsoft.com/downloads

Notes

- Microsoft .NET 1.1 Framework requires Internet Explorer 5.01 or later. Internet Explorer 5.0 (bundled with Windows 2000 SP4) is not sufficient.
- Enter **`NET Framework 1.1 Redistributable`** in the **Keywords** search field to quickly locate the framework toolkit.
- The toolkit installs the .NET 1.1 framework.

Uninstall Previous Versions of PasswordSync

You *must* remove any previously installed instances of PasswordSync before installing a later version.

- If the previously installed version of PasswordSync supports the `IdmPwSync.msi` installer, you can use the standard Windows Add/Remove Programs utility to remove the program.
- If the previously installed version of PasswordSync *does not* support the `IdmPwSync.msi` installer, use the InstallAnywhere uninstaller to remove the program.

Installing PasswordSync

This procedure describes how to install provides instructions for installing, configuring, and uninstalling the PasswordSync configuration application.

Note You must install PasswordSync on each domain controller in the domains that will be synchronized with Identity Manager.

1. From the Identity Manager installation media, click on the `pwsync\IdmPwSync.msi` icon. The Welcome window is displayed

   The installation wizard provides the following navigational buttons:

   - **Cancel**: Click to exit the wizard at any time without saving any of your changes.
   - **Back**: Click to return to a previous dialog box.
   - **Next**: Click to progress to the next dialog box.
2. Read the information provided on the Welcome screen, and then click Next to display the Choose Setup Type PasswordSync Configuration window. PasswordSync Setup
3. Click either **Typical** or **Complete** to install the full PasswordSync package, or **Custom** to control which parts of the package are installed.
4. Click **Install** to install the product. The following window is displayed when PasswordSync has been installed successfully.
5. Click **Finish** to complete the installation process. Make sure **Launch Configuration Application** is selected so that you can begin configuring Password Sync. See *Configuring PasswordSync* for details about this process.

Note A dialog stating that you must restart the system for the changes to take effect. It is not necessary to restart until after you have configured PasswordSync, but the domain controller must be restarted before implementing PasswordSync.

The following table identifies the files that are installed on each domain controller.

Installed Component	**Description**
`%$INSTALL_DIR$%\configure.exe`	The PasswordSync configuration program.
`%$INSTALL_DIR$%\configure.exe.manifest`	Data file for the configuration program.
`%$INSTALL_DIR$%\DotNetWrapper.dll`	DLL that handles .NET SOAP communication

Installed Component	Description
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	DLL that handles PasswordSync messages.
`%SYSTEMROOT%\SYSTEM32\lhpwic.dll`	Password Notification DLL This DLL implements the Windows `PasswordChangeNotify()` function.

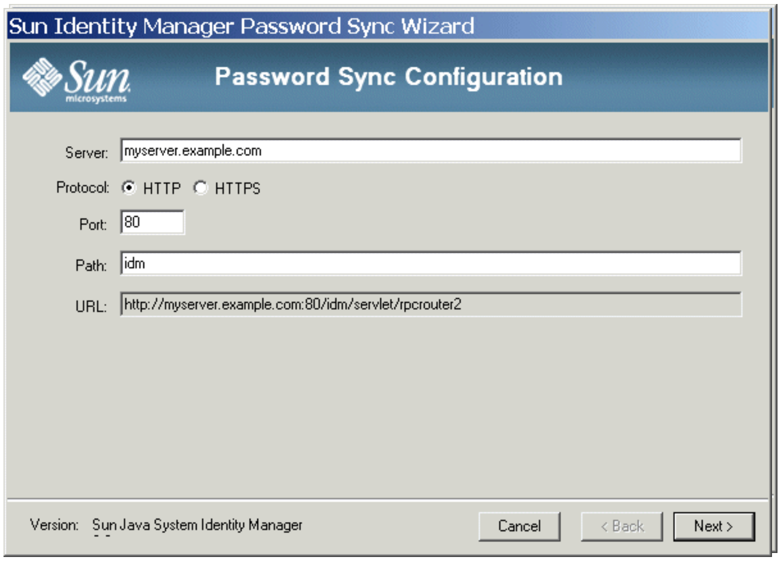
Configuring PasswordSync

If you run the configuration application from the installer, the application displays the configuration screens as a wizard. After you have completed the wizard, each subsequent time you run the PasswordSync configuration application, you can navigate between screens by selecting a tab.

Use the following steps to configure PasswordSync.

1. Start the PasswordSync configuration application, if it is not already running. By default, the configuration application is installed at Program Files —> Sun Java System Identity Manager PasswordSync —> Configuration.

   The following dialog appears.


Sun Identity Manager Password Sync Wizard
Sun microsystems
Password Sync Configuration
Cancel
< Back
Next >

Server: myserver.example.com

Protocol: ● HTTP ○ HTTPS

Port: 80

Path: idm

URL: http://myserver.example.com:80/idm/servlet/rpcrouter2

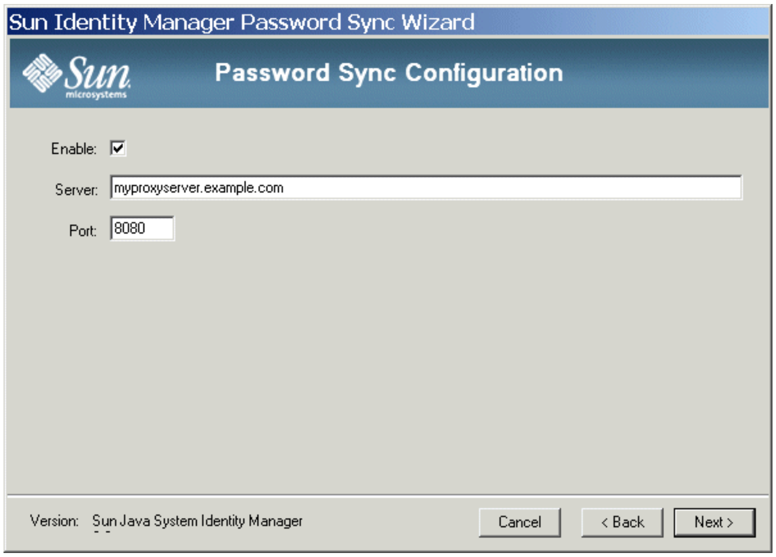
Version: Sun Java System Identity Manager

Figure 1. Server Configuration Dialog

Edit the fields as necessary.

- **Server** must be replaced with the fully-qualified host name or IP address where application server where Identity Manager is installed.
- **Protocol** indicates whether to make secure connections to Identity Manager. If HTTP is selected, the default port is 80. If HTTPS is selected, the default port is 443.
- **Path** specifies the path to Identity Manager on the application server.
- **URL** is generated by concatenating the other fields together. The value cannot be edited within the URL field.

2. Click **Next** to display the proxy server configuration page.



Sun Identity Manager Password Sync Wizard

Password Sync Configuration

Enable: ☑

Server: myproxyserver.example.com

Port: 8080

Version: Sun Java System Identity Manager

Figure 2. Proxy Server Dialog

Edit the fields as necessary.

- Click **Enable** if a proxy server is required.
- **Server** must be replaced with the fully-qualified host name or IP address of the proxy server.
- **Port**: Specify an available port number for the server.
  (The default proxy port is 8080 and the default HTTPS port is 443.)

3. Click **Next** to display the JMS Settings dialog.

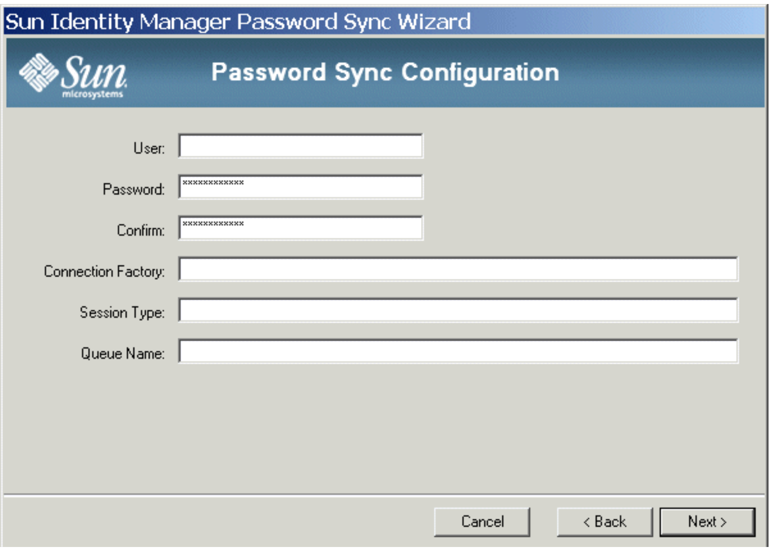
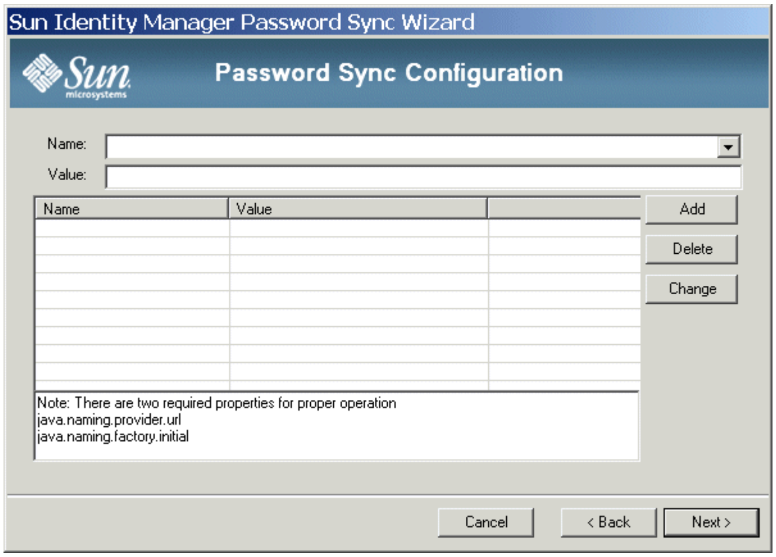


Figure 3. JMS Settings Dialog

Edit the fields as necessary.

- **User** specifies the JMS user name that places new messages on the queue.
- **Password** and **Confirm** specify the password for the JMS user.
- **Connection Factory** specifies the name of the JMS connection factory that should be used. This factory must already exist on the JMS system.
- In most cases, **Session Type** should be set to LOCAL, which indicates that a local session transaction will be used. The session will be committed after each message is received. Other possible values include AUTO, CLIENT, and DUPS_OK.
- **Queue Name** specifies the destination for the password synchronization events.

4. Click **Next** to display the JMS Properties dialog.



Note: There are two required properties for proper operation
java.naming.provider.url
java.naming.factory.initial

Figure 4. JMS Properties Dialog

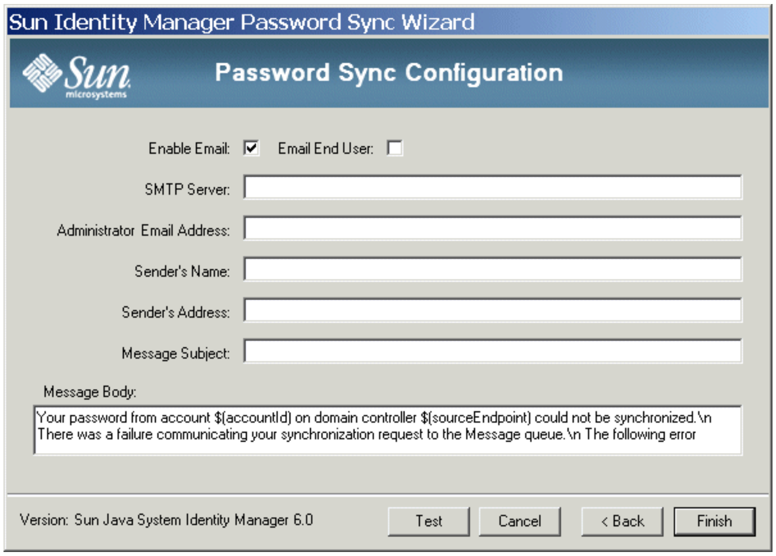
The JMS Properties dialog allows you to define the set of properties that are used to build the initial JNDI context. The following name/value pairs must be defined:

- `java.naming.provider.url` — The value must be set to the URI of the machine running the JNDI service.
- `java.naming.factory.initial` — The value must be set to the classname (including the package) of the Initial Context Factory for the JNDI Service Provider.

The **Name** pull-down menu contains a list of classes from the `java.naming` package. Select a class or type in a class name, then enter its corresponding value in the Value field.

5. Click **Next** to display the Email dialog.

   The Email dialog enables you to configure whether to send an email notification when a user's password change does not synchronize successfully due to a communication error or other error outside of Identity Manager.



Enable Email: ☑ Email End User: □

Message Body:

Your password from account $(accountId) on domain controller $(sourceEndpoint) could not be synchronized.\n There was a failure communicating your synchronization request to the Message queue.\n The following error

Version: Sun Java System Identity Manager 6.0

Figure 5. Email Dialog

Edit the fields as necessary.

- Select **Enable Email** to enable this feature. Select **Email End User** if the user is to receive notifications. Otherwise, only the administrator will be notified.
- **SMTP Server** is the fully qualified name or IP address of the SMTP server to be used when sending failure notifications.
- **Administrator Email Address** is the email address used to send notifications.
- **Sender's Name** is the "friendly name" of the sender.
- **Sender's Address** is the email address of the sender.
- **Message Subject** specifies the subject line of all notifications
- **Message Body** specifies the text of the notification.

  The message body may contain the following variables:

  - `$(accountId)` — The accountId of the user attempting to change password.
  - `$(sourceEndpoint)` — The host name of the domain controller where the password notifier is installed, to help locate troubled machines.
  - `$(errorMessage)` — The error message that describes the error that has occurred.

6. Click **Finish** to save your changes.

If you run the configuration application again, a set of tabs is displayed, instead of a wizard. If you want to display the application as a wizard, enter the following command from the command line:

```
C:\InstallDir\Configure.exe -wizard
```

Debugging PasswordSync

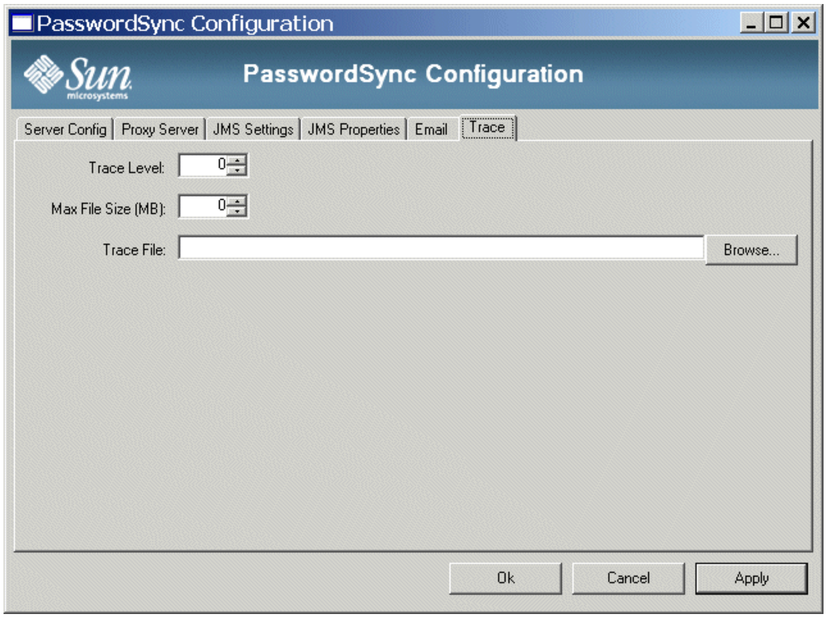
This section provides details about finding information needed to diagnose problems encountered with PasswordSync. about using the configuration tool to enable tracing. It also lists registry keys that might be needed to debug PasswordSync or enable features that cannot be implemented from the configuration tool

Error Logs

PasswordSync writes all failures to the Windows Event Viewer. The source name for error log entries is PasswordSync.

Trace Logs

When the configuration tool is run for the first time, the wizard does not include a panel for configuring tracing. However, the **Trace** tab is displayed all subsequent times the tool is launched.



Trace Level: 0

Max File Size (MB): 0

Trace File:

Figure 6. Trace Dialog

The **Trace Level** field specifies the level of detail PasswordSync will provide when it writes to the trace log. A value of 0 indicates that tracing is turned off, while a value of 4 provides the most detail.

When the trace file exceeds the size specified in the **Max File Size (MB)** field, PasswordSync moves the file to the basename with `.bk` appended. For example, if your trace file is set to `C:\logs\pwicsvc.log`, and your trace level is set to 100 MB, when the trace file exceeds 100 MB, PasswordSync renames the file `C:\logs\pwicsvc.log.bk`, and writes the new data to a new `C:\logs\pwicsvc.log` file.

Registry Keys

The registry keys listed in the following table may be edited using the Windows Registry Editor. The keys are located in the `HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\PasswordSync` key. Other keys are present in this location, but they may be edited with the configuration tool.

Key Name	Type	Description
allowInvalidCerts	REG_DWORD	If set to 1, sets the following flags on the .NET client: • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID As a result, the client will tolerate certificates that have expired or have an invalid CN or hostname. It only applies when SSL is being used. This setting is useful when debugging in test environments where most of the certificates are produced from invalid certificate authorities (CAs). The default is 0.
clientConnectionFlags	REG_DWORD	Optional connection flags that will be passed on to the .NET SOAP client. The default is 0.
clientSecurityFlags	REG_DWORD	Optional security flags that can be passed to the .NET SOAP client. The default is 0.
installdir	REG_SZ	The directory where the PasswordSync application was installed.
soapClientTimeout	REG_DWORD	Timeout, in milliseconds, for a SOAP client to communicate to the Identity Manager server before failure.

Uninstalling PasswordSync

To uninstall the PasswordSync application, go to the Windows Control Panel and select **Add or Remove Programs**. Then select Sun Java System Identity Manager PasswordSync and click **Remove**.

Note PasswordSync can also be uninstalled (or reinstalled) by loading the Identity Manager installation media and clicking on the `pwsync\IdmPwSync.msi` icon.

You must restart your system to complete the process.

.Deploying PasswordSync

To deploy PasswordSync, you must perform the following actions in Identity Manager:

- Configure a JMS Listener Adapter
- Implement the Synchronize User Password Workflow
- Set Up Notifications

Configuring a JMS Listener Adapter

Once messages are being placed on a queue indirectly by the domain controllers, a resource adapter must be configured to accept those messages. You must create a JMS Listener resource adapter and configure it to communicate to the queue. See *Identity Manager Resources Reference* for more information about setting up this adapter.

The following resource parameters must be configured:

Destination Type — This value will typically be set to Queue. Topics are not usually relevant because there is one subscriber and potentially multiple publishers.

Initial context JNDI properties — This text box defines the set of properties that are used to build the initial JNDI context. The following name/value pairs must be defined:

- `java.naming.provider.url` — The value must be set to the URI of the machine running the JNDI service.
- `java.naming.factory.initial` — The value must be set to the classname (including the package) of the Initial Context Factory for the JNDI Service Provider.

It may be necessary to define additional properties. The list of properties and values should match those specified on the JMS settings page of the configuration application.

JNDI Name of Connection factory — The name of a connection factory, as defined on the JMS server.

User and **Password** — The account name and password of the administrator that requests new events from the queue.

Reliable Messaging Support — Select LOCAL (Local Transactions). The other options are not applicable for password synchronization.

Message Mapping — Enter `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`. This class transforms messages from the JMS server into a format that can be used by the Synchronize User Password workflow.

Implementing the Synchronize User Password Workflow

The default Synchronize User Password workflow takes each request that comes in from the JMS Listener adapter and checks out, then back in the ChangeUserPassword viewer. After the checkin has completed, the workflow iterates over all the resources accounts and selects all of the resources, except the source resource. Identity Manager notifies the user by email whether the password change was successful on all resources.

If you want to use the default implementation of the Synchronize User Password workflow, assign it as the process rule for the JMS Listener adapter instance. Process rules may be assigned in the Active Sync wizard for the adapter.

If you want to modify the default Synchronize User Password workflow, copy the `$WSHOME/sample/wfpwsync.xml` file and make your modifications. Then import the modified workflow into Identity Manager.

Some possible modifications that you might want to make to the default workflow include:

- Which entities are notified when a password is changed.
- What happens if an Identity Manager account cannot be found.
- How resources are selected in the workflow.
- Whether to allow password changes from Identity Manager

For detailed information about using workflows, see *Identity Manager Workflows, Forms, and Views*.

Setting Up Notifications

Identity Manager provides the Password Synchronization Notice and Password Synchronization Failure Notice email templates. These templates inform users whether an attempt to change passwords across multiple resources was successful.

Both templates should be updated to provide company-specific information about what users should do if they need further assistance. See *Understanding Email Templates* in the chapter titled *Configuration* for more information.

Frequently Asked Questions about PasswordSync

Can PasswordSync be used in conjunction with other Windows password filters that are used to enforce custom password policies?

Yes, you can use PasswordSync in conjunction with other _WINDOWS_ password filters. It must, however, be the last password filter listed in the Notification Package registry value.

You must use this Registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification
Packages (value of type REG_MULTI_SZ)
```

By default, the installer places the Identity Manager password intercept at the end of the list, but if you installed the custom password filter after the installation, you will be required to move `lhpwic` to the end of the Notification Packages list.

You can use PasswordSync in conjunction with other Identity Manager password policies. When policies are checked on the Identity Manager server side, all resource password policies must pass in order for the password synchronization to be pushed out to other resources. Consequently, you should make the Windows native password policy as restrictive as the most restrictive password policy defined in Identity Manager.

Note The password intercept DLL does not enforce any password policies.

Can the PasswordSync servlet be installed on a different application server than Identity Manager?

Yes. The PasswordSync servlet requires the `spml.jar` and `idmcommon.jar` JAR files, in addition to any JAR files required by the JMS application.

Does the PasswordSync service send passwords over to the lh server in clear text?

Although we recommend running PasswordSync over SSL, all sensitive data is encrypted before being sent to the Identity Manager server.

Sometimes password changes result in com.waveset.exception.ItemNotLocked?

If you enable PasswordSync, a password change (even one initiated from the user interface), will result in a password change on the resource, which causes the resource to contact Identity Manager.

If you configure thepasswordSyncThreshold workflow variable correctly, Identity Manager examines the user object and decides that it has already handled the password change. However, if the user or the administrator makes another password change for the same user, at the same time, the user object could be locked.

A lh Reference

Usage

```
lh { $class | $command } [ $arg [$arg… ] ]
```

Notes

- To display command usage help, type `lh` (do not supply any arguments).
- When using the `lh` command, you should set `JAVA_HOME` to the JRE directory that contains a `bin` directory with the Java executable. This location differs depending on your installation.

  If you have a standard JRE from Sun (without the JDK), a typical directory location is `C:\Program Files\Java\j2re1.4.1_01`. This directory contains the `bin` directory with the Java executable. In this case, set `JAVA_HOME` to `C:\Program Files\Java\j2re1.4.1_01`.

  A full JDK installation has more than one Java executable. In this case, set `JAVA_HOME` to the embedded `jre` directory, which contains the correct `bin/java.exe` file. For a typical installation, set `JAVA_HOME` to `D:\java\jdk1.3.1_02.jre`.

class

Must be a fully qualified class name, such as `com.waveset.session.WavesetConsole`.

commands

Must be one of the following commands:

- `config` – Starts the Business Process Editor.
- `console` – Starts the Identity Manager console.
- `js` – Invokes a JavaScript program.
- `license [options] {status | set {parameters }}` – Sets the Identity Manager license key.
- `setRepo` – Sets the Identity Manager index repository.

- `setup` – Starts the Identity Manager setup process, which allows you to set the license key, define the Identity Manager index repository, and import configuration files.
- `syslog [options]` – Extracts records from the system log.
- `xpress [options]` *Filename* — Evaluates an expression. Valid option is `-trace` (enables trace output).

Examples

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console -u$user -p$password`
- `lh setup -U`*Administrator* `-P`*Password*
- `lh setRepo -c -A`*Administrator* `-C`*Password*
- `lh setRepo -t`*LocalFiles* `-f$WSHOME`

license command

Usage

```
license [options] { status | set {parameters} }
```

Options

`-U` *username* (if Configurator account renamed)

`-P` *password* (if Configurator password changed)

Parameters for the `set` option must be in the form `-f` *File*.

Examples

- `lh license status`
- `lh license set -f` *File*

syslog command

Usage

```
syslog [options]
```

Options

`-d` *Number* – Shows records for the previous *Number* days (default=1)

`-F` – Shows only records with fatal severity level

`-E` – Shows only records with error severity level or above

`-W` – Shows only records with warning severity level or above (default)

`-X` – Includes reported cause of error, if available

B Advanced Search for Online Documentation

You can use advanced syntax to create complex queries when searching the Identity Manager online documentation. These are:

- Wildcard characters — Allow you to specify spelling patterns, rather than complete words.
- Query operators — Specify how query elements are to be combined or modified.

Note You can use wildcard characters and query operators in the same search.

Wildcard Characters

Wildcards are special characters that represent other characters, or groups of characters, in a search.

Identity Manager online documentation search supports these wildcard characters.

Wildcard Character	What it does
Question mark (?)	Matches any single character. For example, searching for t?p matches the words tap, tip, and top. Searching for ball???? matches the words ballpark, ballroom, and ballyhoo, but does not find ballet or balloon, because these do not contain exactly four letters after “ball.”
Asterisk (*)	Matches any group of characters. For example, searching for comp* finds matches to any word starting with the letters comp, such as computer, company, or comptroller.

Query Operators

Query operators allow you to combine, modify, or exclude elements of a search. You can type query operators in upper, lower, or mixed case. Generally, query operators begin and end with angle brackets, such as <CONTAINS>.

Note Basic Boolean operators (AND, OR, and NOT), and special character operators (such as <, =, and !=) do not require brackets.

Rules of Precedence

When you use more than one type of operator in a query, then rules of precedence and parentheses determine the scope of operators. The AND operator takes precendence over the OR operator. For example, the query:

```
resource AND adapter OR attribute
```

is equal to:

```
(resource AND adapter) OR attribute
```

If you want the search feature to interpret “adapter” and “attribute” as alternative terms to be found with “resource”, then you must use parentheses, as in:

```
resource AND (adapter OR attribute)
```

Default Operators

When you type a sequence of query terms or elements without specifying an operator, the standard, default operator <AND> is used to combine query elements.

If a query consists of single words without an explicit unary term operator (such as <EXACT>, <MORPH>, or <EXPAND>), then they are assumed to be governed by the default term operator <MORPH>.

The following table lists the query operators that are most commonly used for online documentation search.

Operator	Description	Example
<AND> or AND	Adds mandatory criteria to the search.	Searching for “apples AND oranges” returns matches that include “apples “and “oranges” in any order. It ignores documents containing only one word.
<CASE>	Case-matches the following term or terms. Note: Identity Manager automatically assumes that upper case or capitalized query terms should be matched as case-sensitive, so <CASE> is not necessary. Lower case terms are treated as case-insensitive, so you must use <CASE> with these to match only lower case.	Searching for “<CASE> bill” finds matches to “bill” but not to “Bill”.
<EXACT>	Finds documents containing the exact word specified.	Searching for “<EXACT> soft” finds documents containing the word “soft,” but does not find documents containing “softest” or “softer”.
<MORPH>	Finds documents that are morphological variations of the specified word, including plurals, past tenses, and complex forms involving prefixes, suffixes, and compound words. Will also use knowlege from a lexicon to correctly handle irregular forms.	Searching for “<MORPH> surf” finds documents containing inferable variants of the word “surf”, such as “surfs”, “surfed”, and “surfing”, as well as those involving prefixes (“resurf”) and compounds (“surfboard”).

Operator	Description	Example
<NEAR>	Finds documents in which the specified words are within 1000 words of each other. The closer the words, the higher the document appears in the search results.	Searching for “resource <NEAR> configuration” finds documents containing both words, with no more than 1000 words between.
<NEAR/n>	Finds documents in which words are within n words of each other. Note: The value of ***n*** must be between 1 and 1024.	Searching for “buy <NEAR/3> sell” finds documents containing “buy low and sell high” because there are no more than three words between “buy” and “sell.”
<NOT> or NOT	Finds documents that do not contain a specific word or phrase.	Searching for “surf <AND> <NOT> channel” finds documents containing “surf” but not “channel.”

Index