Oracle® Waveset 8.1.1 Business Administrator's Guide

Part No: 821–0094
July 2010

100729@24661

Contents

Preface

This guide describes how to use the Oracle Waveset 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 Oracle Waveset (Waveset) system.

Who Should Use This Book

This *Oracle Waveset 8.1.1 Business Administrator's Guide* guide is intended for use by administrators, software developers, and IT service providers who implement an integrated identity management and web access platform using Oracle Waveset servers and software.

An understanding of the following technologies will help you apply the information discussed in this book:

- Lightweight Directory Access Protocol (LDAP)
- Java technology
- JavaServer Pages (JSP) technology
- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML)
- Extensible Markup Language (XML)

Before You Read This Book

Waveset is one component of a software infrastructure that supports enterprise applications distributed across a network or Internet environment. You should be familiar with the documentation provided for these applications, which can be accessed online at `http://docs.sun.com/coll/entsys_04q4`.

Because Oracle Waveset Directory Server is used as the data store in an Oracle Waveset deployment, you should be familiar with the documentation provided with that product. Directory Server documentation can be accessed online at `http://docs.sun.com/coll/DirectoryServer_04q2`.

How this Book is Organized

This guide is organized into the following chapters and appendices:

Chapter 1, “Waveset Overview,” describes how Oracle Waveset and the different Oracle Waveset objects help you manage administrative challenges in your dynamic working environment.

Chapter 2, “Getting Started with the Waveset User Interface,” describes how to use Waveset's graphical user interface.

Chapter 3, “User and Account Management,” describes how to create and manager users by using the Administrator interface.

Chapter 5, “Roles and Resources,” contains information to help you understand Oracle Waveset roles and resources.

Chapter 4, “Configuring Business Administration Objects,” contains information and procedures to help you set up and maintain Oracle Waveset business administration objects, such as policies, email templates, audit groups and events, and more.

Chapter 6, “Administration,” describes how to use the Administrator interface to perform different administrator-level tasks. In addition, this chapter contains information about using roles, administrative roles, and capabilities.

Chapter 7, “Data Loading and Synchronization,” describes how to use Waveset's data loading and synchronization features to keep your data current.

Chapter 8, “Reporting,” introduces Waveset report types and explains how to create and manager reports.

Chapter 9, “Task Templates,” introduces Waveset task templates and how to use them to configure workflow behaviors.

Chapter 10, “Audit Logging,” describes Waveset's auditing system.

Chapter 11, “PasswordSync,” describes how to install, configure, and use the PasswordSync feature to detect and synchronize password changes.

Chapter 12, “Security,” describes how you can use Waveset to manage system security.

Chapter 13, “Identity Auditing: Basic Concepts,” introduces identity auditing concepts and audit controls.

Chapter 14, “Auditing: Audit Policies,” describes how to create and manage audit policies by using the Audit Policy Wizard.

Chapter 15, “Auditing: Monitoring Compliance,” describes how to perform audit reviews and manage compliance with federally mandated regulations.

Chapter 16, "Data Exporter," introduces the Data Exporter feature and explains how to use this feature to write information about users, roles, and other object types to an external data warehouse.

Chapter 17, "Service Provider Administration," describes how to configure and administer the Service Provider feature.

Appendix A, "`lh` Reference," explains how to use the Waveset command line interface.

Appendix B, "Audit Log Database Schema," contains information about audit data schema values for supported database types and audit log mappings.

Appendix C, "User Interface Quick Reference," provides a quick reference indicating how to accomplish commonly performed tasks in Waveset.

Appendix D, "Capabilities Definitions," provides a quick reference describing the task-based and functional capabilities you can assign to users.

Related Books

Oracle provides additional documentation and information to help you install, use, and configure Waveset. The Oracle Waveset 8.1.1 library includes the following publications:

Primary Audience	Title	Description
All Audiences	*Oracle Waveset 8.1.1 Overview*	Provides an overview of Waveset features and functionality. Provides product architecture information and describes how Waveset integrates with other Oracle products.
	Oracle Waveset 8.1.1 Release Notes	Describes known issues, fixed issues, and late-breaking information not already provided in the Waveset documentation set.
System Administrators	*Oracle Waveset Installation*	Describes how to install Waveset and optional components such as the Oracle Waveset Gateway and PasswordSync.
	Oracle Waveset 8.1.1 Upgrade	Provides instructions on how to upgrade from an older version of Waveset to a newer version.
	Oracle Waveset 8.1.1 System Administrator's Guide	Contains information and instructions to help system administrators manage, tune, and troubleshoot their Waveset installation.
Business Administrators	*Oracle Waveset 8.1.1 Business Administrator's Guide*	Describes how to use Waveset's provisioning and auditing features. Contains information on the user interfaces, user and account management, reporting, and more.

Primary Audience	Title	Description
System Integrators	*Oracle Waveset 8.1.1 Deployment Guide*	Describes how to deploy Waveset in complex IT environments. Topics covered include working with identity attributes, data loading and synchronization, configuring user actions, applying custom branding, and so on.
	Oracle Waveset 8.1.1 Deployment Reference	Contains information on workflows, forms, views, and rules, as well as the XPRESS language.
	Oracle Waveset 8.1.1 Resources Reference	Provides information about installing, configuring, and using resource adapters.
	Oracle Waveset Service Provider 8.1.1 Deployment	Describes how to deploy Oracle Waveset Service Provider, and how views, forms, and resources differ from the standard Waveset product.
	Oracle Waveset 8.1.1 Web Services	Describes how to configure SPML support, which SPML features are supported (and why), and how to extend support in the field.

In addition, the `http://docs.sun.com` web site enables you to access Oracle technical documentation online. You can browse the archive or search for a specific book title or subject.

Documentation Updates

Corrections and updates to this and other Waveset publications are posted to the Waveset Documentation Updates website:

`http://blogs.sun.com/idmdocupdates/`

An RSS feed reader can be used to periodically check the website and notify you when updates are available. To subscribe, download a feed reader and click a link under Feeds on the right side of the page. Starting with version 8.0, separate feeds are available for each major release.

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Oracle is not responsible for the availability of third-party web sites mentioned in this document. Oracle does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Oracle will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

See the following web sites for additional resources:

- Documentation (`http://docs.sun.com`)
- Support (`http://www.oracle.com/us/support/systems/index.html`)
- Training (`http://education.oracle.com`) – Click the Sun link in the left navigation bar.

Oracle Welcomes Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of its documentation. If you find any errors or have any other suggestions for improvement, go to `http://docs.sun.com` and click Feedback. Indicate the title and part number of the documentation along with the chapter, section, and page number, if available. Please let us know if you want a reply.

Oracle Technology Network (`http://www.oracle.com/technetwork/index.html`) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the Discussion Forums (`http://forums.oracle.com`).
- Get hands-on step-by-step tutorials with Oracle By Example (`http://www.oracle.com/technology/obe/start/index.html`).
- Download Sample Code (`http://www.oracle.com/technology/sample_code/index.html`).

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`**
		`Password:`

aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

CHAPTER 1

Waveset Overview

The Waveset system allows you to manage and audit access to accounts and resources. By giving you the capabilities and tools to quickly handle periodic and daily user-provisioning and auditing tasks, Waveset 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. Today, 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.

Additionally, businesses today face strict requirements governing the security and integrity of critical business information. In an environment dictated by compliance-related legislation– such as the Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act– the overhead created by monitoring and reporting activities is substantial and costly. You must be able to respond quickly to changes in access control, as well as satisfy the data-gathering and reporting requirements that help keep your business secure.

Waveset was developed specifically to help you manage these administrative challenges in a dynamic environment. By using Waveset to distribute access management overhead and address the burden of compliance, 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 Waveset to accommodate the structure of your enterprise and answer these challenges. By mapping Waveset objects to the entities that you manage– users and resources– you significantly increase the efficiency of your operations.

In a service provider environment, Waveset extends these capabilities to managing extranet users as well.

Goals of the Waveset System

The Waveset solution enables you to accomplish the following goals:

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

  Define audit policies to manage compliance with user access privileges and manage violations through automated remediation actions and email alerts.
- Conduct periodic access reviews and define attestation review and approval procedures that automate the process of certifying user privileges.
- Monitor key information and audit and review statistics through the dashboard.

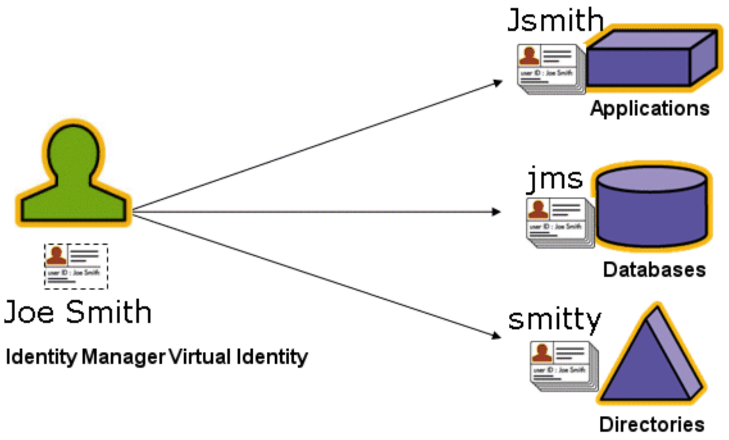
Defining User Access to Resources

Users in your extended enterprise can be anyone with a relationship to your company, including employees, customers, partners, suppliers, or acquisitions. In the Waveset 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 Waveset terms, these things are *resources*.

Because users often have one or more identities on each of the resources they access, Waveset creates a single, *virtual identity* that maps to disparate resources. This allows you to manage users as a single entity. See Figure 1–1.

FIGURE 1–1 Waveset 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 geographical divisions. Each of these departments typically requires access to different resources. In Waveset terms, this type of group is called an *organization*.

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

Within the Waveset 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.

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

Understanding User Types

Waveset provides two user types: *Waveset Users* and *Service Provider Users*, if you configure your Waveset system for a service provider implementation. These types enable you to distinguish users that might have different provisioning requirements based on their relationship with your company, for example extranet users compared with intranet users.

A typical scenario for a service provider implementation is a service provider company with internal users and external users (customers) that it wants to manage with Waveset. For information about configuring a service provider implementation, see *Oracle Waveset Service Provider 8.1.1 Deployment*.

You specify the Waveset user type when you configure a user account. For more information about service provider users, see Chapter 17, “Service Provider Administration”

Delegating Administration

To successfully distribute responsibility for user identity management, you need the right balance of flexibility and control. By granting select Waveset 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 Waveset *administrators*.

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

The Waveset workflow model also includes a method to ensure that certain actions require approval. Using workflow, Waveset administrators retain control over tasks and can track their progress. For detailed information about workflow, see Chapter 1, “Workflow,” in *Oracle Waveset 8.1.1 Deployment Reference*.

Waveset Objects

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

- “Waveset User Accounts” on page 27
- “Waveset Roles” on page 27
- “Resources and Resource Groups” on page 28
- “Organizations and Virtual Organizations” on page 29
- “Directory Junctions” on page 29
- “Waveset Capabilities” on page 30
- “Admin Roles” on page 30
- “Waveset Policies” on page 31
- “Audit Policies” on page 31
- “Object Relationships” on page 31

Note – When naming Waveset objects, do not use the following characters:

’ (apostrophe), .. (period), |(pipe), [(left bracket),] (right bracket), , (comma), : (colon), $ (dollar sign), " (double quote), \ (backslash), or = (equals sign).

The following characters should also be avoided: _ (underscore), % (percent-sign), ^ (caret), and * (asterisk).

Waveset User Accounts

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

Oracle Waveset user accounts:

- Provide users access to one or more resources, and manage user account data on those resources.
- Are assigned 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.

Administrators are users with additional privileges to manage user accounts, resources, and other Oracle Waveset system objects and tasks. Oracle Waveset administrators manage organizations, and are assigned a range of capabilities to apply to objects in each managed organization.

For more information on user accounts, see Chapter 3, “User and Account Management.” For more information on administrator accounts, see Chapter 6, “Administration.”

Waveset Roles

A role is an Oracle Waveset object that allows resource access rights to be grouped and efficiently assigned to users. Roles are organized into four role types:

- Business Roles
- IT Roles
- Applications
- Assets

Business Roles organize into groups the access rights that people who do similar tasks in an organization need to do their job duties. Typically, Business Roles represent user job functions.

IT Roles, Applications, and *Assets* organize resource entitlements (or *access rights*) into groups. To provide users with access to resources, IT Roles, Applications, and Assets are assigned to Business Roles so that users can access the resources they need to do their jobs.

IT Roles, Applications, and Assets can be *required, conditional,* or *optional.*

- **Required roles** are always assigned to the user.
- **Conditional roles** have conditions that must evaluate to true in order for the role to be assigned.
- **Optional roles** can be requested separately, and, upon approval, assigned to the user.

Because roles can be conditional or optional, users with the same general job description can have the same Business Role, but still have different access rights. This approach allows a Business Role designer to define coarse-grained access to roles in order to achieve regulatory compliance, while still allowing flexibility for the user's manager to fine-tune the user's access rights. With this approach, there is no need to define a new Business Role for each permutation of access needs in the enterprise, which is a problem known as *role explosion*.

A user can be assigned one or more roles, or no role.

Note – For more information about roles, see "Understanding and Managing Roles" on page 109.

Resources and Resource Groups

Waveset stores information about how to connect to a resource or system. Resources to which Waveset provides access include:

- Digital resources, such as the following:
  - Mainframe security managers
  - Databases
  - Directory services (such as LDAP)
  - Applications
  - Operating systems
  - ERP systems (such as SAP)
- Non-digital or `external` resources that are external to Waveset, such as the following:
  - Cell phones
  - Desktop computers
  - Laptop computers
  - Security badges

Each Waveset resource stores the following kinds of information:

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

There are two ways to assign resources to users. A resource can be assigned to a user directly (this is known as a individual or direct assignment), or a resource can be assigned to a role, which is then assigned to a user (this is a role-based or indirect assignment).

- **Individual assignment**. Individual resources are assigned directly to user accounts.
- **Role-based assignment**. One or more resources are assigned to a role (an Application, Asset, or IT Role). The Application, Asset, or IT Roles are then assigned to a Business Role. Finally, one or more Business Roles are assigned to a user account.

A related Waveset 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. Also, they simplify the process of assigning multiple resources to user accounts.

For more information about resource groups, see “Resource Groups” on page 154.

Organizations and Virtual Organizations

Organizations are Waveset containers used to enable administrative delegation. They define the scope of entities that an Waveset 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 Waveset repository. By mirroring an existing directory structure and membership through a virtual organization, Waveset 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.

For more information on organizations, see “Understanding Waveset Organizations” on page 190.

Directory Junctions

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 topmost 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.

You can make Waveset users members of, and available to, a virtual organization in the same way as an organization.

For more information on directory junctions, see "Understanding Directory Junctions and Virtual Organizations" on page 195.

Waveset Capabilities

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

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

For more information on capabilities, see "Understanding and Managing Capabilities" on page 198.

Admin Roles

Oracle Waveset 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 Oracle Waveset. Oracle Waveset rules control dynamic assignment.

For more information on admin roles, see "Understanding and Managing Admin Roles" on page 201.

Waveset Policies

Policies set limitations for Waveset users by establishing constraints for account ID, login, and password characteristics. *Identity system account policies* establish user, password, and authentication policy options and constraints. *Resource password and account ID policies* set length rules, character type rules, and allowed words and attribute values. A *dictionary policy* enables Identity Auditor to check passwords against a word database to ensure protection from simple dictionary attacks.

For more information about policies, see "What are Policies?" on page 94.

Audit Policies

Distinct from other system policies, an *audit policy* defines a policy violation for a group of users of a specific resource. Audit policies establish one or more rules by which users are evaluated for compliance violations. These rules depend on conditions based on one or more attributes defined by a resource. When the system scans a user, it uses the criteria defined in the audit policies assigned to that user to determine whether compliance violations have occurred.

For more information about audit policies, see "About Audit Policies" on page 407.

Object Relationships

The following table provides a quick overview of Waveset objects and their relationships.

TABLE 1–1 Waveset Object Relationships

Waveset Object	What Is It?	Where Does It Fit?
User account	An account on Waveset and on one or more resources. User data may be loaded into Waveset from resources. A special class of users, Waveset administrators, have extended privileges	**Role**. Generally, each user account is assigned one or more roles. **Organization**. User accounts are arranged in a hierarchy as part of an organization. Waveset administrators additionally manage organizations. **Resource**. Individual resources can be assigned to user accounts. **Capability**. Administrators are assigned capabilities for the organizations they manage.

TABLE 1–1 Waveset Object Relationships *(Continued)*

Waveset Object	What Is It?	Where Does It Fit?
Role	Business Roles organize into groups the access rights that people who do similar tasks in an organization need to do their job duties. Application, and IT Roles group resources into groups so that resources can be assigned to users by way of Business Roles. Role-based resource assignments simplify resource management in large organizations.	**Resource and resource group**. Resources and resource groups are assigned to Asset, Application, and IT Roles. **User account**. User accounts with similar characteristics are assigned to Business Roles. **Asset, Application, and IT Roles**, Asset, Application, and IT Roles are assigned to Business Roles.
Resource	Stores information about a system, application, or other resource on which accounts are managed.	**Role**. Resources are assigned to Application and IT Roles, which are in turn assigned to Business Roles. A user account loosely "inherits" resource access from its Business 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 Business Role assignments. **User account**. Resource groups can be directly assigned to user accounts.
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 Waveset organization and one or more directory organizations.

TABLE 1–1 Waveset Object Relationships *(Continued)*

Waveset Object	What Is It?	Where Does It Fit?
Directory junction	Hierarchically related set of organizations that mirrors a directory resource's actual set of hierarchical containers.	**Organization**. Each organization in a directory junction is a virtual organization.
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.
Audit policy	Sets rules by which users are evaluated for compliance violations.	**User account**. Audit policies are assigned to user accounts. **Organization**. Audit policies are assigned to organizations.

CHAPTER 2

Getting Started with the Waveset User Interface

Read this chapter to learn about the Waveset graphical user interfaces (UI) and how you can quickly begin using Waveset.

Topics covered include:

- "Waveset Administrator Interface" on page 35
- "Logging in to the Waveset Administrator Interface" on page 37
- "Waveset End-User Interface" on page 38
- "Logging in to the Waveset End-User Interface" on page 41
- "Help and Guidance" on page 41
- "The Waveset Debug Page" on page 42
- "Identity Manager IDE" on page 44
- "Where to Go from Here" on page 45

Waveset Administrator Interface

The Waveset system includes two primary graphical interfaces through which users perform tasks. These interfaces are the end-user interface and the administrator interface. The end-user interface (also called the User interface) is discussed later in this chapter on "Waveset End-User Interface" on page 38. The Administrator interface is discussed here.

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

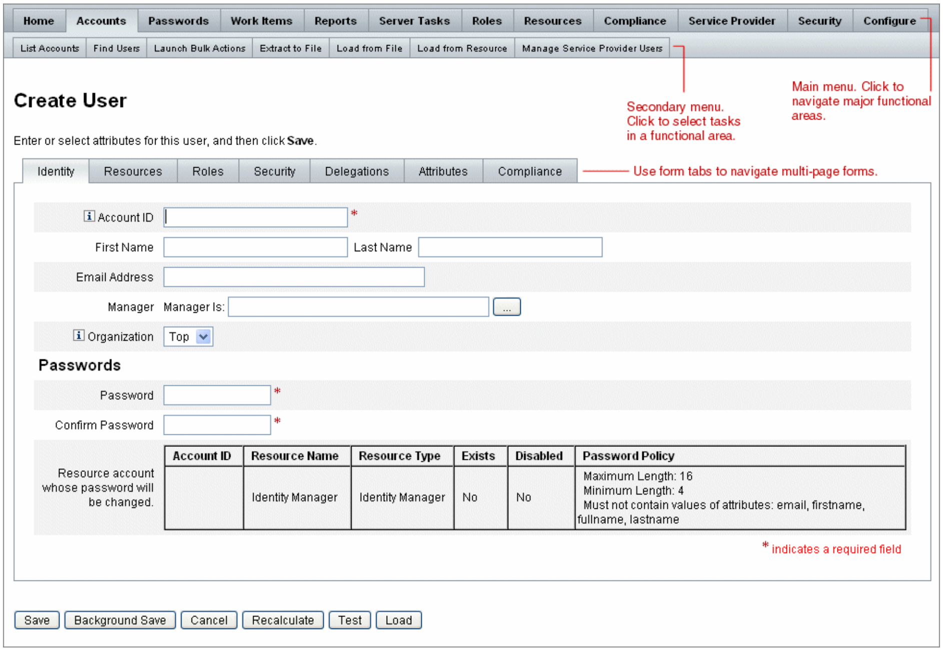
Interface organization is represented by these elements:

- **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. This is illustrated in Figure 2–1.

Note – A quick reference to performing administrative tasks in the UI is available in Appendix C, "User Interface Quick Reference."

FIGURE 2–1 Waveset Administrator Interface



Secondary menu. Click to select tasks in a functional area.

Main menu. 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.

Account ID *

First Name

Last Name

Email Address

Manager Manager Is:

Organization Top

Passwords

Password *

Confirm Password *

Resource account whose password will be changed.

Account ID	Resource Name	Resource Type	Exists	Disabled	Password Policy
	Identity Manager	Identity Manager	No	No	Maximum Length: 16 Minimum Length: 4 Must not contain values of attributes: email, firstname, fullname, lastname

* indicates a required field

Logging in to the Waveset Administrator Interface

▼ To Open the Administrator Interface

1. **Open a Web browser and type the following URL into the address bar:**

   `http://<AppServerHost>:<Port>/idm/login.jsp`

2. **Enter your user ID and password and click Log In.**

   The Administrator interface opens if your User ID has assigned capabilities and an assigned controlled organization.

Session Limits and Cookies

If cookies are enabled in the administrator's Web browser, administrators will remain logged on to the Administrator interface up to the time allotted by the configured session limit. If cookies are disabled in the browser, then certain actions will cause the system to prompt the administrator to log in again during the session.

These actions include:

- Administrator, role, and organization rename cancellation
- Organization deletion cancellation
- User login module and admin login module creation

To avoid multiple login requests, cookies should be enabled.

Forgotten User ID

Waveset allows an administrator to retrieve his or her forgotten user ID. When an administrator clicks Forgot Your User ID? from the login page, a lookup page appears and requests identity attribute information associated with the account, such as first and last name, email address, or phone number.

Waveset then constructs a query to find a single user matching the entered values. If no match is found, or multiple matches are found, then an error message appears on the Lookup User ID page.

The lookup feature is enabled by default, but you can use one of the following actions to disable this feature:

- Set `forgotUserIdMode` in `login.jsp` to a value of false.
- Edit the system configuration object and set the `disableForgotUserId` attribute to a value of true for the `admin` attribute and/or the `user` attribute.

  For instructions on editing the system configuration object, see "Editing Waveset Configuration Objects" on page 108.

Note – If you upgrade from an earlier Waveset version to version 8.1.1, the Forgot Your User ID? feature will be *disabled* by default.

To enable this feature, you must modify the following attributes in the System Configuration object ("Editing Waveset Configuration Objects" on page 108):

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

The set of user attribute names presented are configured through the system configuration attributes `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>`. The attributes that can be specified are those defined as queryable attributes in the `IDM Schema Configuration` configuration object.

If recovered, then Waveset sends email to the email address of the recovered user by using the User ID Recovery email template.

Waveset End-User Interface

The Waveset end-user interface (also known as the *Waveset user interface*) presents a limited view of the Waveset system. This view is specifically tailored to users without administrative capabilities.

Note – For instructions on how to log on to the end-user interface, see "Logging in to the Waveset End-User Interface" on page 41.

A user can perform various activities from the User interface, such as changing their password, performing self-provisioning tasks, and managing work items and delegations.

Waveset can be configured so that users can request an account by clicking a link on the end-user interface login page. For details, see "Anonymous Enrollment" on page 89.

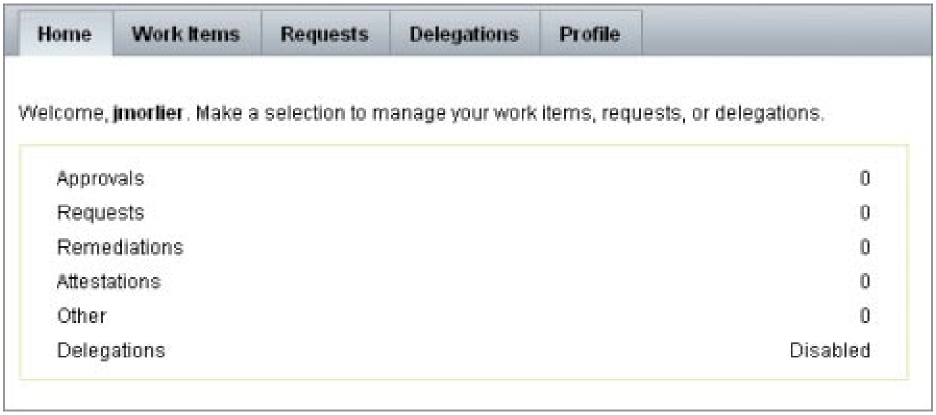
The end-user interface is organized into the following tabs:

- "Home Tab" on page 39
- "Work Items Tab" on page 39
- "Requests Tab" on page 39
- "Delegations Tab" on page 40
- "Profile Tab" on page 40

Home Tab

When a user logs in to the Waveset User interface, any pending work items and delegations for the user are displayed on the Home tab, as illustrated in the following figure.

FIGURE 2–2 User Interface (Home Tab)



Welcome, **jmorlier**. Make a selection to manage your work items, requests, or delegations.

Approvals	0
Requests	0
Remediations	0
Attestations	0
Other	0
Delegations	Disabled

The Home tab provides quick access to any pending items. Users can click an item in the list to respond to a work item request or perform other available actions.

Work Items Tab

The Work Items tab is further divided into separate Approvals, Attestations, Remediations, and Other tabs. In this area of the user interface users can approve or reject any pending work items that the user owns or has the authority to act on.

Requests Tab

The Requests tab has two subtabs: Launch Requests and View.

On the Launch Requests tab users have two choices: Update My Roles and Update My Resources.

- On the Update My Roles page, users can request from a list of available roles that may be appropriate for the user. When the end-user submits a role request, a work item is generated and an approval notification is sent to the designated approvers for that role. End-users can also request that they be removed or *deassigned* from one or more roles.

  See the Chapter 5, “Roles and Resources,” chapter for information on how to create optional roles that end-users can request access to.
- On the Update My Resources page, users can request from a list of individual resources that may be appropriate for the user. As with role-requests, resource-requests generate work items that require an approval before they can be processed.

The View subtab displays status details for requests submitted by the user. From this area users can view the process status and task results for the requests they submit.

Delegations Tab

From the Delegations tab, users can delegate work items to other Waveset users. For example, a user who is the assigned approver for one or more roles can designate that future approval work items be sent to a colleague for a certain amount of time while the user is away on vacation. Using the Delegations page, users can create and manage delegations without requiring the assistance of an administrator.

Profile Tab

End-users can manage their Waveset password and account attribute settings from the Profile tab. This tab is divided into the following four subtabs:

- **Change Password**. End-users can change their password on a selected resource or on all resources.
- **Account Attributes**. End-users can change certain attributes, such as the account email address that Waveset sends account notifications to.
- **Authentication Questions**. Used to manage authentication questions and answers for the user account.
- **Access Privileges**. Lists the user’s currently assigned role and resource assignments.

Logging in to the Waveset End-User Interface

Use the following instructions to log into the Waveset End-User Interface.

▼ To Open the End-User Interface

1. **Open a Web browser and type the following URL into the address bar:**

   `http://<AppServerHost>:<Port>/idm/user/login.jsp`

2. **Enter a user ID and password and click Log In.**

   The end-user interface opens.

Retrieving Forgotten User IDs

Waveset allows end-users to retrieve their forgotten user IDs. For more information, see "Forgotten User ID" on page 37 in the "Logging in to the Waveset Administrator Interface" on page 37 section.

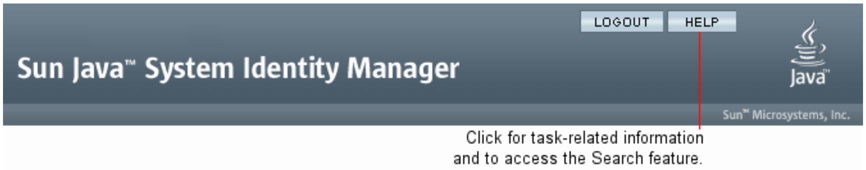
Help and Guidance

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

Waveset Help

For task-related help and information, click the Help button, which is located at the top of each Administrator and User interface page, as depicted in the following figure.

FIGURE 2–3 Help Button in the Waveset Interface


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

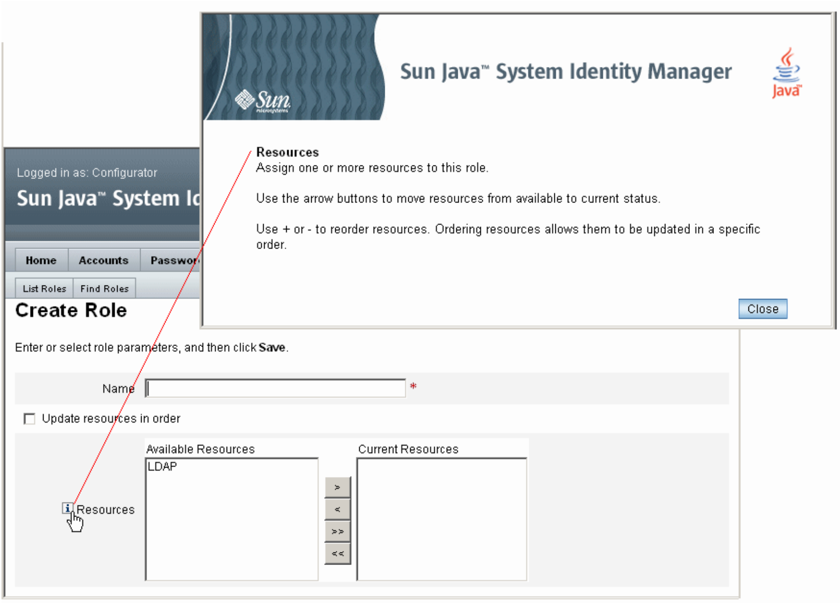
At the bottom of each Help window is a Contents link that guides you to other Help topics and the Waveset terms glossary.

Waveset Guidance

Waveset 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.

A symbol marked with the letter "i" displays next to fields with guidance. Click the symbol to open a window and display its associated information.

FIGURE 2–4 Waveset Guidance



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

Create Role

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

The Waveset Debug Page

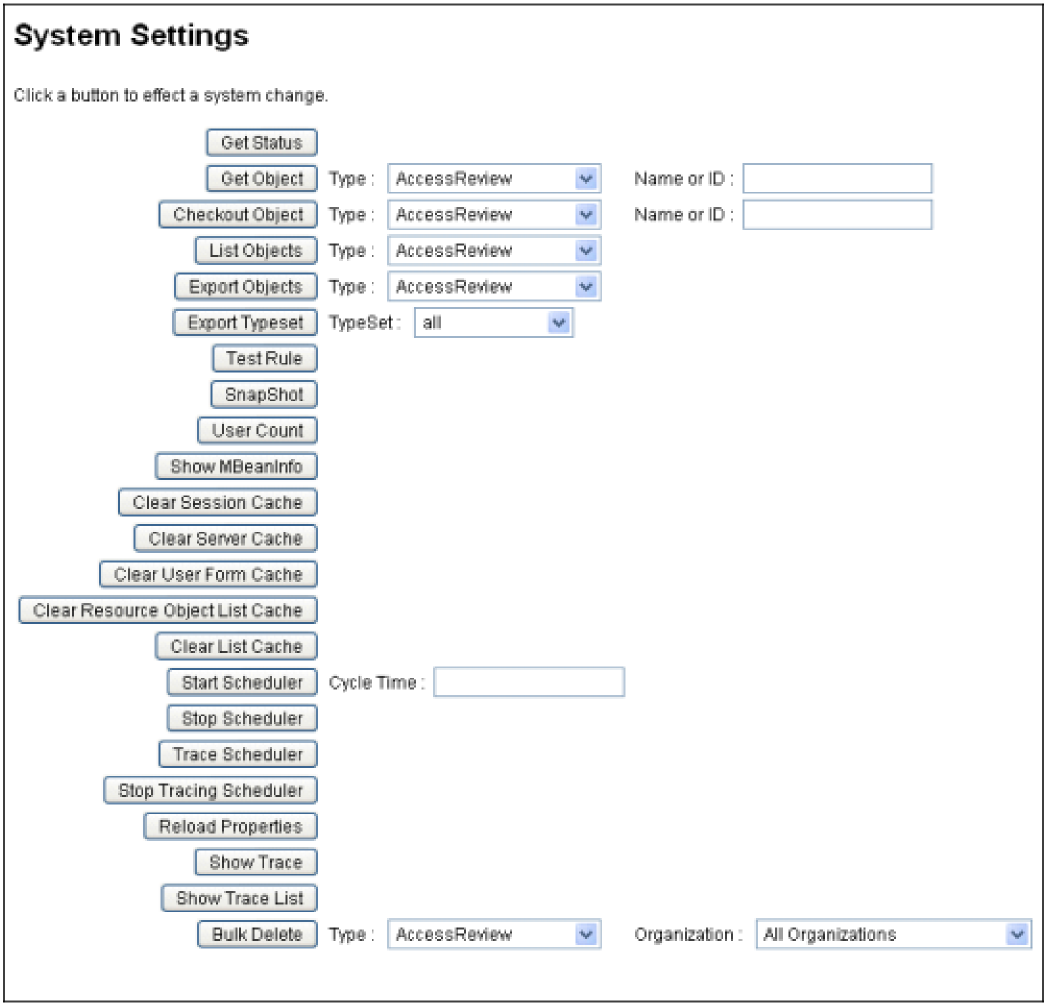
The administrator interface includes pages that are useful when you need to optimize Waveset or troubleshoot a problem. To access these pages open the Waveset Debug Page, which is also called the System Settings page.

To open the Waveset Debug Page, type the following URL into your browser. (Depending on your platform and configuration, URLs may be case-sensitive.)

```
http://<AppServerHost>:<Port>/idm/debug/session.jsp
```

Users must have the Debug capability to view `/idm/debug/` pages. For information about capabilities, see "Assigning Capabilities to Users" on page 201.

FIGURE 2–5 The Waveset Debug Page (System Settings)



System Settings

Click a button to effect a system change.

Type : AccessReview

Type : AccessReview

Type : AccessReview

Type : AccessReview

TypeSet : all

Cycle Time :

Type : AccessReview

Organization : All Organizations

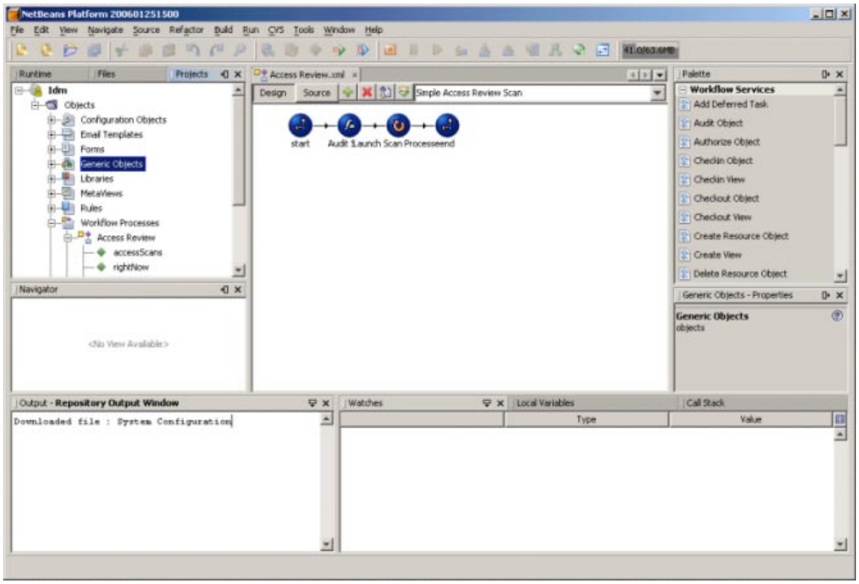
For information about troubleshooting Waveset, seeChapter 5, “Tracing and Troubleshooting,” in *Oracle Waveset 8.1.1 System Administrator's Guide*.

Identity Manager IDE

The Identity Manager Integrated Development Environment (Identity Manager IDE) provides a graphical view of Waveset forms, rules, and workflows. It is a fully integrated NetBeans plug-in that is distributed with Waveset in the Waveset distribution package.

Using the Identity Manager IDE, you create and edit forms that establish the features available on each Waveset page. You can also modify Waveset *workflows*, which define the sequence of actions followed or tasks performed when working with Waveset user accounts. Additionally, you can modify rules defined in Waveset that determine workflow behaviors.

FIGURE 2–6 Identity Manager IDE Interface



```
Downloaded file : System Configuration
```

To download the Identity Manager IDE, visit this website:

https://identitymanageride.dev.java.net/

You can also use the Business Process Editor (BPE) to make customizations, if you have it installed with earlier versions of Waveset.

Where to Go from Here

After you become familiar with Waveset interfaces and the ways that you can find information, use the following reference to guide you to the topics you want to focus on:

Chapter Topic	Description
Chapter 3, "User and Account Management"	Describes the Accounts area of the interface and provides procedures for managing user accounts.
Chapter 5, "Roles and Resources"	Describes how to work with Waveset roles and resources.
Chapter 4, "Configuring Business Administration Objects"	Describes the configuration tasks and how to set up Waveset objects.
Chapter 6, "Administration"	Explains how to create and manage Waveset administrators and organizations.
Chapter 7, "Data Loading and Synchronization"	Provides a guide to the features and tools you can use to maintain current data in Waveset.
Chapter 8, "Reporting"	Describes the reports and how to generate them.
Chapter 9, "Task Templates"	Describes the Task Templates you can use to configure certain workflow behaviors.
Chapter 10, "Audit Logging"	Describes the audit logs and how the auditing system works.
Chapter 11, "PasswordSync"	Describes how to set up the PasswordSync utility to synchronize password changes in Windows Active Directory domains with changes with Waveset.
Chapter 12, "Security"	Describes the security features and how to use them.
Chapter 13, "Identity Auditing: Basic Concepts"	Describes basic auditing concepts.
Chapter 14, "Auditing: Audit Policies"	Describes how to create audit policies.
Chapter 15, "Auditing: Monitoring Compliance"	Describes how to conduct audit reviews and implement practices that help you manage compliance with federally mandated regulations
Chapter 16, "Data Exporter"	The Data Exporter feature allows you to write information about users, roles, and other object types to an external data warehouse.
Chapter 17, "Service Provider Administration"	Describes features for managing service provider users.
Appendix A, "`lh` Reference"	Describes commands available from the Waveset command line.

Chapter Topic	Description
Appendix B, "Audit Log Database Schema"	Audit data schema values for the supported database types and audit log database mappings
Appendix C, "User Interface Quick Reference"	A quick reference to performing administrative tasks in the UI. It shows the primary 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.
Appendix D, "Capabilities Definitions"	A list of Waveset's default task-based and functional capabilities (with definitions). This appendix also lists the tabs and subtabs that may be accessed with each task-based capability.

CHAPTER 3

User and Account Management

This chapter provides information and procedures for creating and managing users from the Waveset Administrator interface.

This information is organized into the following sections:

The Accounts Area of the Interface

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

The Waveset Accounts / User List page lets you manage Waveset users. To access this area, click **Accounts** on the Administrator interface menu bar.

The accounts list shows all Waveset user accounts. Accounts are grouped into 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. When you sort by full name (the Name column), then all items in the hierarchy, at all levels, are sorted alphabetically.

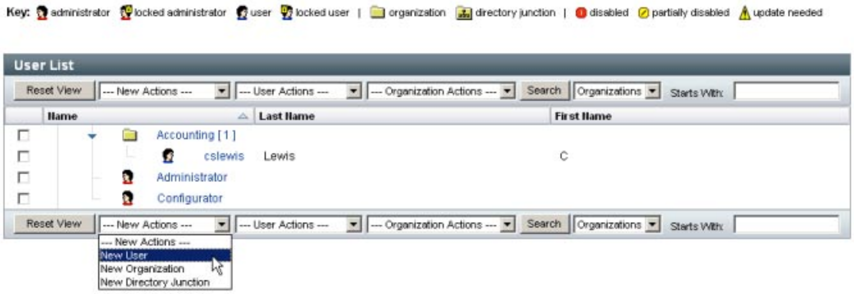
To expand the hierarchical view and see accounts in an organization, click the triangular indicator next to a folder. Collapse the view by clicking the indicator again.

Actions Lists in the Accounts Area

Use the actions lists (located at the top and bottom of the accounts area, as shown in “Actions Lists in the Accounts Area” on page 48), 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.


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		

Searching in the Accounts List Area

Use the accounts area search feature to locate users and organizations. Select Organizations or Users from the list, enter one or more characters that the user or organization name starts with in the search area, and then click **Search**. For more information about searching in the accounts area, see “Finding and Viewing User Accounts” on page 57.

User Account Status

Icons that display next to each user account indicate current, assigned account status. Table 3–1 describes what each icon represents.

TABLE 3–1 User Account Status Icon Descriptions

Indicator	Status
🔒	The user's Waveset account is locked. Note that this icon only reflects the locked state of the Waveset account, not any of the user's resource accounts. Users become locked after exceeding the maximum number of failed Waveset account login attempts as defined in the Waveset Account Policy. Only failed password or question logins to Waveset accounts are counted towards the maximum allowed. Therefore, if an Waveset login application (that is, the administrator interface, the end-user interface, and so on) does not include the Waveset Login Module in its login module group, then the Waveset failed password policy will not be considered. However, regardless of the stack of login modules configured for a given Waveset login application, failed question logins that exceed the maximum configured in the Waveset Account Policy can cause a user to become locked and this icon to be displayed. For information on how to unlock accounts see "To Unlock User Accounts" on page 71.
🔒	The administrator Waveset account is locked. Note that this icon only reflects the locked state of the Waveset account, not any of the administrator's resource accounts. For more information, see the description for the user lockout icon, above.
⛔	The account is disabled on all assigned resources and on Waveset. (When an account is enabled, no icon appears.) For information about how to enable disabled accounts, see "Disabling, Enabling, and Unlocking User Accounts" on page 69.
⊘	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 Waveset user account on one or more resources. (When an account is updated on all assigned resources, no icon appears.)

Note – In the Manager column, a manager's user name appears inside parentheses if Waveset cannot find an Waveset account that matches the name listed.

The User Pages (Create/Edit/View)

This section describes the Create User, Edit User, and View User pages that are available in the Administrator interface. Instructions on how to use these pages appear later in this chapter.

Note – This documentation describes the default set of Create User, Edit User, and View User pages that ship with Waveset. To better reflect your business processes or specific administrator capabilities, however, you should create custom user forms specifically for your environment. For more information about customizing the user form, see Chapter 2, "Waveset Forms," in *Oracle Waveset 8.1.1 Deployment Reference*.

- "Identity Tab" on page 50
- "Resources Tab" on page 51
- "Roles Tab" on page 51
- "Security Tab" on page 51
- "Delegations Tab" on page 52
- "Attributes Tab" on page 52
- "Compliance Tab" on page 52

The default Waveset user pages are organized into the following tabs or sections:

- Identity
- Assignments
- Security
- Delegations
- Attributes
- Compliance

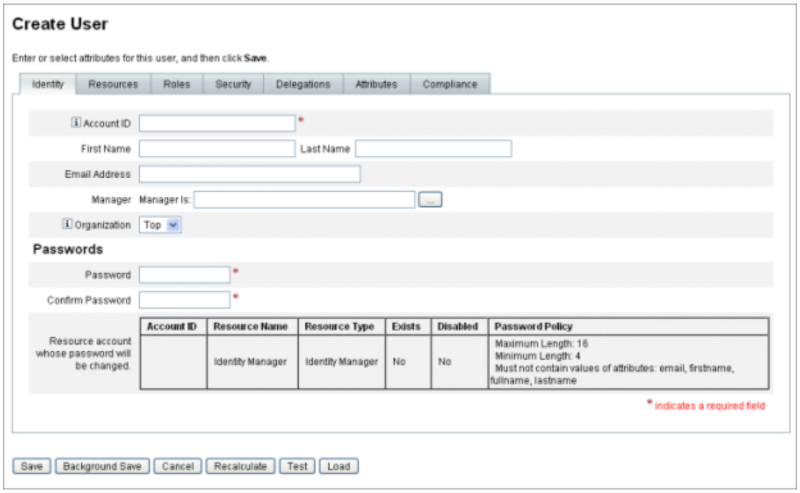
Identity Tab

The Identity area defines a user's account ID, name, contact information, manager, governing organization, and Waveset 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 "Managing Account Security and Privileges" on page 79.

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

FIGURE 3–1 Create User - Identity



Create User

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

Account ID: *

First Name: Last Name:

Email Address:

Manager: Manager Is:

Organization: Top

Passwords

Password: *

Confirm Password: *

Resource account whose password will be changed.

Account ID	Resource Name	Resource Type	Exists	Disabled	Password Policy
	Identity Manager	Identity Manager	No	No	Maximum Length: 16 Minimum Length: 4 Must not contain values of attributes: email, firstname, fullname, lastname

* indicates a required field

Resources Tab

The Resources area provides for the direct assignment of resources and resource groups to a user. Resource exclusions can also be assigned.

Directly assigned resources supplement resources that are indirectly assigned to the user through *role assignment*. Role assignment profiles a class of users. Roles define user access to resources through indirect assignment.

Roles Tab

The Roles tab is used to assign one or more roles to a user, and manage those role assignments.

See "To Assign Roles to a User" on page 132 for information about this tab.

Security Tab

In Waveset terminology, a user who is assigned extended capabilities is an Waveset *administrator*. Use the Security tab to assign a user administrator privileges.

For more information on using the Security tab to create administrators, see "Creating and Managing Administrators" on page 185.

The **Security** form consists of the following sections.

- **Admin roles**. Assigns one or more administrative roles to the user. A role is a specific pairing of capabilities and controlled organizations that facilitates assigning administrative duties to users in a coordinated way.
- **Capabilities**. Enables rights in the Waveset system. Each Waveset administrator is assigned one or more capabilities, frequently aligned with job responsibilities.

Capabilities are discussed on "Understanding and Managing Capabilities" on page 198. A list of task-based capabilities with definitions is included in Appendix D, "Capabilities Definitions," on Appendix D, "Capabilities Definitions." This appendix also lists the tabs and subtabs that may be accessed with each capability.

- **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.

Note – To have administrator capabilities, a user must be assigned at least one Admin role, or one or more capabilities AND one or more controlled organizations. For more information about Waveset administrators, see"Understanding Waveset Administration" on page 183.

- **User Form**. Specifies the user form that the administrator will use when creating and editing users. If **None** is selected, the administrator will inherit the user form assigned to his organization.
- **View User Form**. Specifies the user form that the administrator will use when viewing users. If **None** is selected, the administrator will inherit the view user form assigned to his organization.
- **Account policy**. Establishes password and authentication limits.

Delegations Tab

The Delegations tab on the Create User page lets you delegate work items to other users for a specified length of time. For more information about delegating work items, read "Delegating Work Items" on page 213.

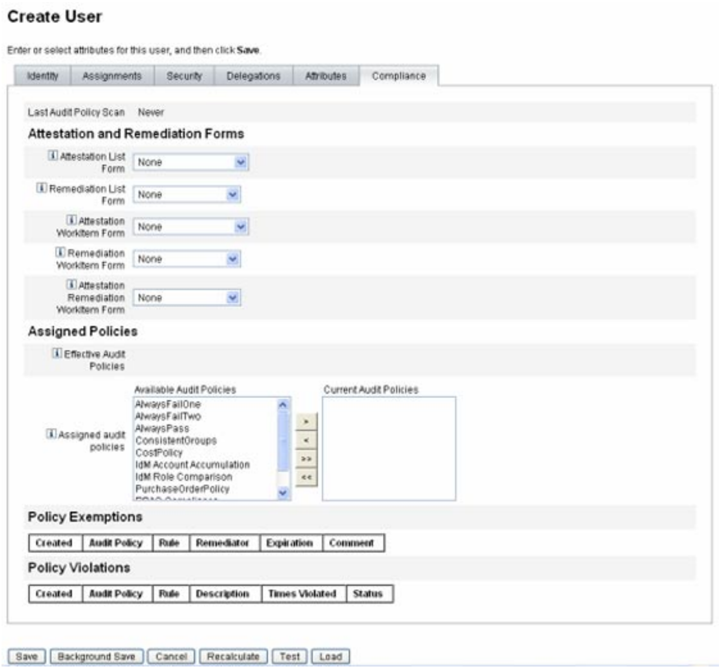
Attributes Tab

The Attributes tab on the Create User page defines account attributes associated with assigned resources. Listed attributes are categorized by assigned resource, and differ depending on which resources are assigned.

Compliance Tab

The Compliance tab:

- Lets you select the attestation and remediation forms for the user account.
- Specifies the assigned audit policies for the user account, including those in effect through the user's Organization assignment. These policy assignments can be changed only by editing the user's current organization or moving the user to another Organization.
- Indicates the current status of policy scans, violations, and exemptions (as illustrated by the following figure), if applicable for the user account. The information includes the date and time of the last audit policy scan for the selected user.



Create User

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

Last Audit Policy Scan: Never

Attestation and Remediation Forms

Attestation List Form: None

Remediation List Form: None

Attestation Workitem Form: None

Remediation Workitem Form: None

Attestation Remediation Workitem Form: None

Assigned Policies

Effective Audit Policies

Assigned audit policies

Available Audit Policies:
AlwaysFailOne
AlwaysFailTwo
AlwaysPass
ConsistentGroups
CostPolicy
IdM Account Accumulation
IdM Role Comparison
PurchaseOrderPolicy

Current Audit Policies

Policy Exemptions

Created	Audit Policy	Rule	Remediator	Expiration	Comment

Policy Violations

Created	Audit Policy	Rule	Description	Times Violated	Status

To assign audit policies, move selected policies from the **Available Audit Policies** list to the **Current Audit Policies** list.

Note – You can view compliance violations logged for a user for a specific time period, by selecting **View Compliance Violation Log** from the **User Actions** list and specifying the range of entries to view.

Creating Users and Working with User Accounts

From the Accounts/User List page in the Administrator interface, you can perform a range of actions on the following system objects:

- **Administrators & Users**. View, create, edit, move, rename, deprovision, enable, disable, update, unlock, delete, unassign, unlink, and audit.

  For more information about creating and editing administrator accounts, see “Understanding Waveset Administration” on page 183.

- **Organizations**. Create, edit, refresh, and perform user actions on members of the organization.

For more information on organizations, see "Understanding Waveset Organizations" on page 190.

- **Directory Junctions**. Create a hierarchically related set of organizations to mirror a directory resource's actual set of hierarchical containers.

  For more information about directory junctions, see "Understanding Directory Junctions and Virtual Organizations" on page 195.

Enabling Process Diagrams for Use in Waveset

Process diagrams depict the workflow that Waveset follows when it creates or otherwise acts on a user account. When enabled, process diagrams display on the results page or task summary page that is created when Waveset completes the task.

In Waveset version 8.0, process diagrams were disabled for both new and upgrade installations.

Use the following steps to enable process diagrams for use in Waveset.

1. Open the system configuration object for editing by following the procedure on "Editing Waveset Configuration Objects" on page 108.
2. Locate the following XML element.

   ```
   <Attribute name='disableProcessDiagrams'>
     <Boolean>true</Boolean>
   </Attribute>
   ```
3. Change the `true` value to `false`.
4. Click Save.
5. Restart your server (or servers) in order for the change to take effect.

   Process diagrams can also be enabled in the end-user interface, but only if they are first enabled in the Administrator interface using the steps described above. For details, see "To Enable Process Diagrams in the End-User Interface" on page 104.

Creating a User in Waveset

You can create and manage users from the Accounts tab on the Administrator interface menu bar.

1. In the Administrator interface, click Accounts.
2. To create a user in a specific organization, select the organization, then select New User from the New Actions list.

   Otherwise, to create a user account in the Top organization, select New User from the New Actions list.
3. Complete the information in the following tabs or sections.

- **Identity**. Name, organization, password, and other details. (See “Identity Tab” on page 50.)
- **Resources**. Individual resource and resource group assignments, as well as resource exclusions. (See “Resources Tab” on page 51.)
- **Roles**. Role assignments. For information on roles, see “Understanding and Managing Roles” on page 109. See “To Assign Roles to a User” on page 132 for instructions on completing the Roles tab.
- **Security**. Admin roles, controlled organizations and capabilities. Also, user form settings and account policy. (See “Security Tab” on page 51.)
- **Delegations**. Work item delegations. (See “Delegations Tab” on page 52.)
- **Attributes**. Specific attributes for assigned resources. (See “Attributes Tab” on page 52.)
- **Compliance**. Select attestation and remediation forms for the user account. The compliance area also lets you specify the assigned audit policies for the user account, including those in effect through the user’s organization assignment. Indicates the current status of policy scans, violations, and exemptions, and includes information about the user’s last audit policy scan. (See “Attributes Tab” on page 52.)

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

To better reflect your business processes or specific administrator capabilities, you should customize the user form specifically for your environment. For more information about customizing the user form, see “Customizing Forms” in *Oracle Waveset 8.1.1 Deployment Reference*.

4. When you are finished, Save the account.

   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 Waveset. A task status indicator displays on the Accounts page, the Find User Results page, and the Home page, for each save in progress.

     Status indicators, as described in the following table, help you monitor the progress of the save process.

Status Indicator	Status
↻	The save process is in progress.
⌛	The save process is suspended. Often, this means that the process is waiting for approval.

Status Indicator	Status
✓	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.

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

Note – If sunrise is configured, creating a user creates a work item that can be viewed from the Approvals tab. Approving this item overrides the sunrise date and creates the account. Rejecting the item cancels account creation. For more information about configuring sunrise, see "Configuring the Sunrise and Sunset Tab" on page 303.

Creating Multiple Resource Accounts for a User

Waveset provides the ability to assign multiple resource accounts to a single user. It does this by allowing multiple resource account types or *types of accounts* to be defined for each resource. Resource account types should be created as needed to match each functional account type on the resource. For example, AIX SuperUser or AIX BusinessAdmin.

Why Assign Multiple Accounts per User per Resource?

In some situations, an Waveset user may require more than one account on a resource. A user can have several different job functions related to the resource. For example, the user can be both a user and administrator of the resource. Best practice suggests using separate accounts for each function. That way, if one account is compromised, the access granted by the other accounts is still secure.

Configuring Types of Accounts

For a resource to support multiple accounts for a single user, the resource account types must first be defined in Waveset. To define resource account types for a resource, use the Resource Wizard. For information, see "Managing the Resources List" on page 145.

You must enable and configure resource account types before assigning them to users.

Assigning Types of Accounts

Once you have defined account types, you can assign them to a resource. Waveset treats each assignment of an account type as a separate account. As a result, each distinct assignment in a role can have different attributes set.

Similar to the single account per resource case, all assignments of a specific type create only one account, regardless of the number of assignments.

Although you can assign users to any number of different types of accounts on a resource, each user can be assigned one account of a given type on a resource. The exception to this rule is the built-in "default" type. Users can have any number of accounts of default type on a resource. It is not recommended that you do this however, as this leads to ambiguity when referencing accounts in forms and views.

Finding and Viewing User Accounts

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

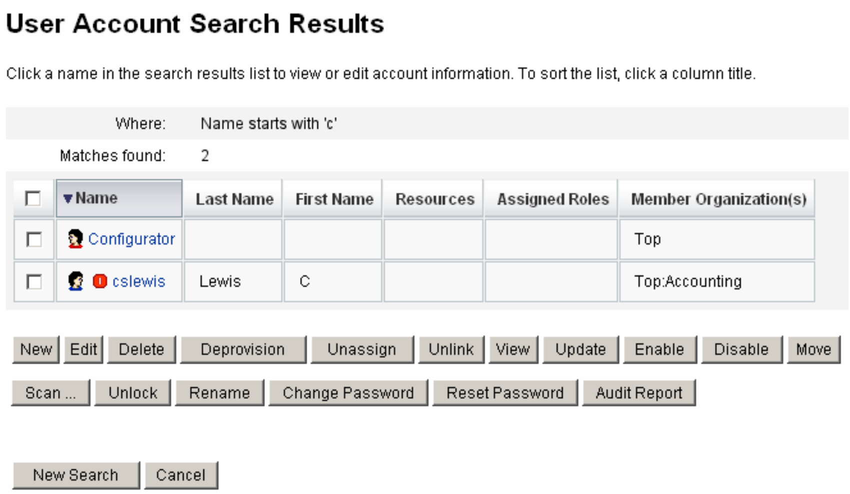
To search for accounts, select Accounts → Find Users from the menu bar. You can search for accounts by using one or more of these search types:

- **Account detail** (such as user name, email address, or last name, or first name). These choices depend on your institution's specific Waveset implementation.
- **User's manager**. The manager's user name appears in parentheses if the user name does not match an existing account in Waveset.
- **Resource account status**. Options include:
  - **Disabled**. User cannot access any Waveset or assigned resource accounts.
  - **Partially Disabled**. User cannot access one or more assigned resource accounts.
  - **Enabled**. User has access to all assigned resource accounts.
- **Assigned resource**. Options include:
  - **Role** (see "To Find Users Assigned to a Specific Role" on page 138)
  - **Organization**
  - **Organizational control**
  - **Capabilities**
  - **Admin role**
- **User account status**. Options include:
  - **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**. Use this query to search for users for whom all updates have or have not succeeded. Options include:
  - **no**. User accounts that have not been updated on any resource.
  - **some**. User accounts that require an update (identified by an exclamation point symbol).
  - **all**. User accounts that have been updated on all assigned resources (no updates are required).

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

Editing Users

The information in this section covers viewing, editing, reassigning, and renaming user accounts.

▼ To View User Accounts

Use the View User page and perform the following steps to view account information.

1. **In the Administrator interface, click Accounts in the menu.**

   The User List page opens.

2. **Select the box next to the user whose account you want to view.**

3 **In the User Actions drop-down menu, select View.**

The View User page displays a subset of the user's identity, assignments, security, delegations, attributes, and compliance information. The information on the View User page is view-only and cannot be edited.

4 **Click Cancel to return to the Accounts list.**

▼ To Edit User Accounts

Use the Edit User page and perform the following steps to edit account information.

1 **In the Administrator interface, click Accounts in the menu.**

2 **Select the box next to the user whose account you want to edit.**

3 **In the User Actions drop-down menu, select Edit.**

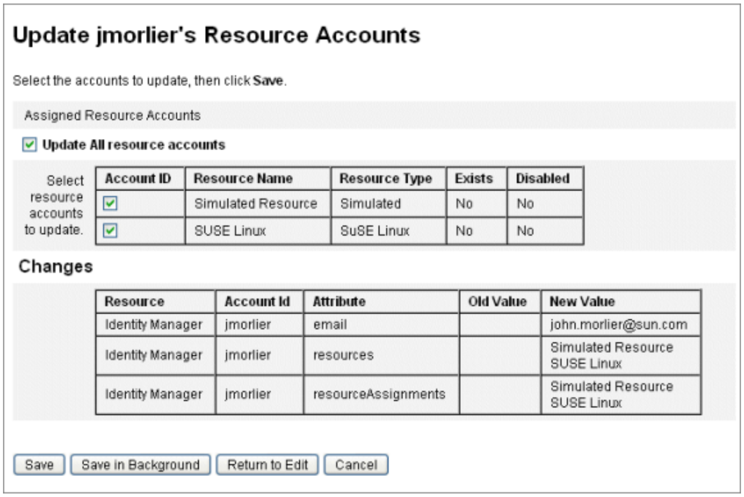
4 **Make and save your changes.**

Waveset displays the Update Resource Accounts page. This page shows resource accounts assigned to the user and the changes that will apply to the account.

5 **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.**

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

FIGURE 3–2 Edit User (Update Resource Accounts)



Update jmorlier'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
☑	Simulated Resource	Simulated	No	No
☑	SUSE Linux	SuSE Linux	No	No

Changes

Resource	Account Id	Attribute	Old Value	New Value
Identity Manager	jmorlier	email		john.morlier@sun.com
Identity Manager	jmorlier	resources		Simulated Resource SUSE Linux
Identity Manager	jmorlier	resourceAssignments		Simulated Resource SUSE Linux

Reassigning Users to Another Organization

The move action allows you to remove one or more users from one organization and reassign, or move, the users to a new organization. Use the following steps to move a user:

1. In the Administrator interface, click Accounts in the menu.

   The User List page opens.
2. Select the box next to the user (or users) to be moved.
3. In the User Actions drop-down menu, select Move.

   The Change Organization of Users task page opens.
4. Select the organization that you want to reassign the user to and click Launch.

Renaming Users

Typically, renaming an account on a resource is a complex action. Because of this, Waveset provides a separate feature to rename a user's Waveset 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.

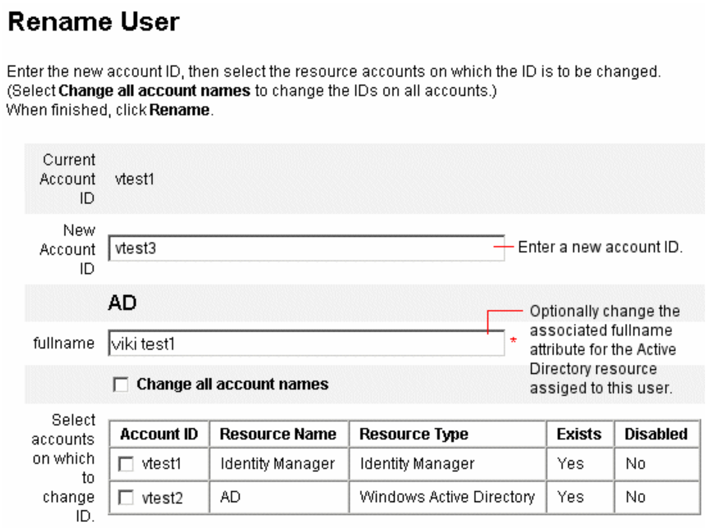
The Rename User page allows you to change the user account name, associated resource account names, and resource account attributes associated with the user's Waveset account.

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:

- Waveset 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

Enter a new account ID.

AD

fullname	viki test1 *

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

□ **Change all account names**

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

Updating Resources Associated with an Account

In an update action, Waveset 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 have the following options:

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

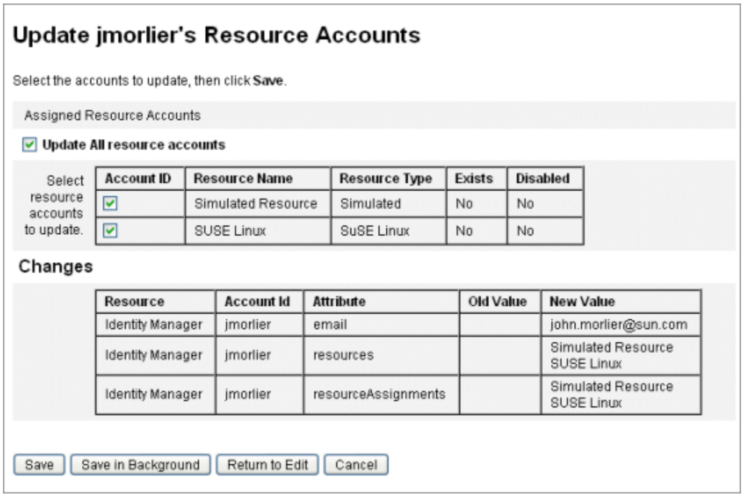
Updating Resources on a Single User Account

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.

Figure 3–3 illustrates the Update Resource Accounts page.



Update jmorlier'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
☑	Simulated Resource	Simulated	No	No
☑	SUSE Linux	SuSE Linux	No	No

Changes

Resource	Account Id	Attribute	Old Value	New Value
Identity Manager	jmorlier	email		john.morlier@sun.com
Identity Manager	jmorlier	resources		Simulated Resource SUSE Linux
Identity Manager	jmorlier	resourceAssignments		Simulated Resource SUSE Linux

FIGURE 3–3 Update Resource Accounts

Updating Resources on Multiple User Accounts

You can update two or more Waveset 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.

Deleting Waveset User Accounts

In Waveset, an Waveset user account is deleted in the same way that a remote resource account is deleted. Follow the steps for deleting a resource account, but instead of selecting a remote resource account for deletion, select the Waveset account.

Note – If a user has outstanding work items, or if a user has outstanding work items that have been delegated to another user, Waveset will not allow the user's Waveset account to be deleted. The delegated work items either need to be resolved or forwarded to another user before the user's Waveset account can be deleted.

For more information, see "Deleting Resources from User Accounts" on page 63.

Deleting Resources from User Accounts

Waveset provides several deletion operations that can be used to remove Waveset user account access from a resource:

- **Delete**. For each resource selected, Waveset deletes the user's account on the remote resource. (To delete a user from Waveset, select Waveset as the resource.)
  - Deleted resource accounts are automatically *unlinked* from the Waveset user.
  - Deleted resource accounts are not *unassigned* from the user. The resource remains assigned to the user unless the unassign action is also selected.
- **Unassign**. For each resource selected, Waveset removes the resource from the user's list of assigned resources.
  - Unassigned resource accounts are automatically *unlinked* from the Waveset user.
  - The user account on the remote resource *is not* deleted. The account remains intact unless the delete action is also selected.
- **Unlink**. For each resource selected, the user's resource account information is removed from Waveset.
  - The user's account on the remote resource remains intact unless a delete action is also selected.
  - The resource remains on the user's list of assigned resources unless an unassign action is also selected.
  - 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.

Although deprovision appears as a user-action in the User List page menus, there are actually only three Deletion actions in Waveset: delete, unassign, and unlink.

To deprovision a remote resource, use the delete and unassign actions on the resource.

▼ To Start a Delete, Unassign, or Unlink Action for a Single User Account

Use the following procedure to perform a delete operation on a single Waveset user. By working with one user account at a time, you can specify different delete, unassign, and/or unlink operations for individual resource accounts.

Note – You can use the Delete Resource Accounts page to unassign or unlink resource accounts when the Delete operation has been disabled.

---

1 **In the Administrator interface, click Accounts in the main menu.**

The User List page displays on the List Accounts tab.

2 **Select a user and click the User Actions drop-down menu.**

3 **Select any of the Deletion actions (Delete, Deprovision, Unassign, or Unlink) from the list.**

Waveset displays the Delete Resource Accounts page (Figure 3–4).

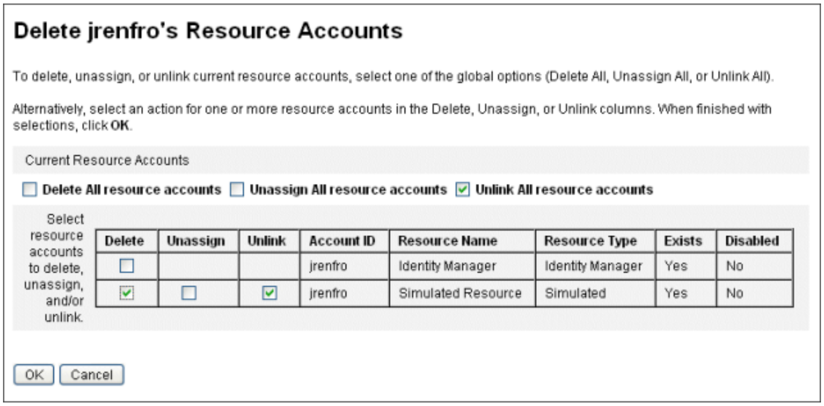
4 **Complete the form. For more information on the Delete, Unassign, and Unlink actions, see "Deleting Resources from User Accounts" on page 63.**

5 **Click OK.**

Figure 3–4 shows the Delete Resource Accounts page. In the screen capture, the user jrenfro has one active account on a remote resource (the Simulated Resource). The Delete action is selected, which means that when the form is submitted, jrenfro's account on the resource will be deleted. Because deleted accounts are automatically unlinked, the account information for this resource will be removed from Waveset. The Simulated Resource will remain assigned to jrenfro because the Unassign action is not selected.

To delete jrenfro's Waveset account, the Delete action should be selected for Waveset.

FIGURE 3–4 The Delete Resource Accounts page



Delete jrenfro'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**

Select resource accounts to delete, unassign, and/or unlink.

Delete	Unassign	Unlink	Account ID	Resource Name	Resource Type	Exists	Disabled
□			jrenfro	Identity Manager	Identity Manager	Yes	No
☑	□	☑	jrenfro	Simulated Resource	Simulated	Yes	No

To Start A Delete, Unassign, or Unlink Action for Multiple Users

You can perform a delete operation on more than one Waveset user account at a time, however, you can only perform the selected delete operation on *all* of the users' resource accounts.

Delete operations can also be performed using Waveset's Bulk Account Actions feature. See "Delete, DeleteAndUnlink, Disable, Enable, Unassign, and Unlink Commands" on page 74.

Note – You can use the Delete Resource Accounts page to unassign or unlink resource accounts when the Delete operation has been disabled.

---

1 **In the Administrator interface, click Accounts in the main menu.**

The User List page displays on the List Accounts tab.

2 **Select one or more users and click the User Actions drop-down menu.**

3 **Select any of the Deletion actions (Delete, Deprovision, Unassign, or Unlink) from the list.**

Waveset displays the Confirm Delete, Unassign, or Unlink page (Figure 3–5).

4 **Specify the action to be performed.**

The options include:

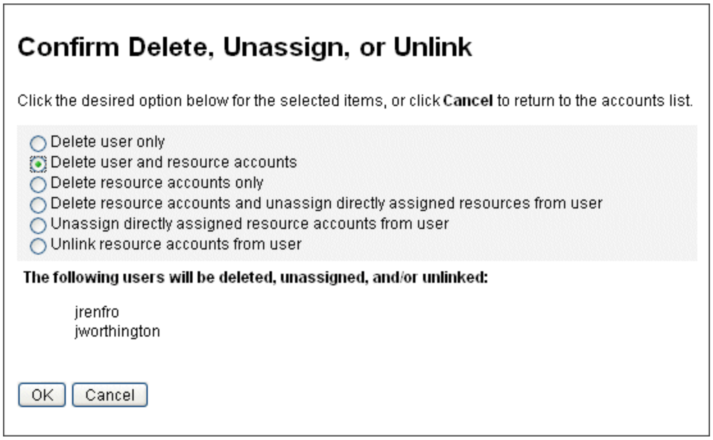
- **Delete user only**. Deletes the users' Waveset accounts. This option does not delete or unassign the users' resource accounts.
- **Delete user and resource accounts**. Deletes the users' Waveset accounts and all of the users' resource accounts.
- **Delete resource accounts only**. Deletes all of the users' resource accounts. This option does not unassign the resource accounts, nor does it delete the users' Waveset accounts.

- **Delete resource accounts and unassign directly assigned resources from user**. Deletes and unassigns all of the users' resource accounts, but does not delete the users' Waveset accounts.
- **Unassign directly assigned resource accounts from user**. Unassigns directly assigned resource accounts. This option does not delete the users' accounts on the remote resources. Resource accounts assigned through a role or resource group are not affected.
- **Unlink resource accounts from user**. The users' resource account information is removed from Waveset. The users' accounts on the remote resources are not deleted and are not unassigned. Accounts that are indirectly assigned to the users through a role or resource group may be restored when the users are updated.

5 Click OK.

Figure 3–5 shows the Confirm Delete, Unassign, or Unlink page. The top portion of the page displays the six available actions that can be carried out for multiple users. The bottom portion of the page displays the users who will be affected by the selected action.

FIGURE 3–5 The Confirm Delete, Unassign, or Unlink Page



Confirm Delete, Unassign, or Unlink

Click the desired option below for the selected items, or click **Cancel** to return to the accounts list.

○ Delete user only
● Delete user and resource accounts
○ Delete resource accounts only
○ Delete resource accounts and unassign directly assigned resources from user
○ Unassign directly assigned resource accounts from user
○ Unlink resource accounts from user

The following users will be deleted, unassigned, and/or unlinked:

jrenfro
jworthington

Changing User Passwords

All Waveset users are assigned a password. When set, the Waveset 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.

Note – For information about account password policies, as well as general information about user authentication, see "Managing Account Security and Privileges" on page 79.

▼ To Change Passwords from the User List Page

You can use the Change Password User Action from the User List page (Accounts → List Accounts) to change a user account password from the User List page. Follow these steps:

1. **In the Administrator interface, click Accounts in the main menu.**

   The User List page displays on the List Accounts tab.

2. **Select a user and click the User Actions drop-down menu.**

3. **To change the password, select Change Password.**

   The Change User Password page opens.

4. **Type the new password and click the Change Password button.**

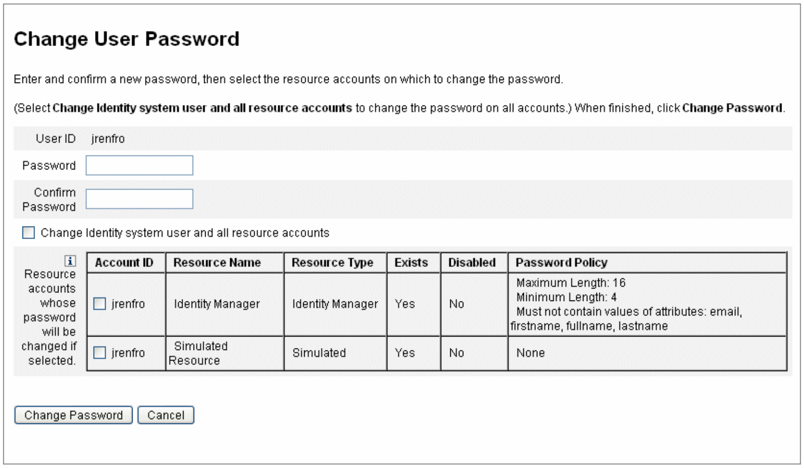
▼ To Change Passwords from the Main Menu

To change a user account password from the main menu, follow these steps:

1. **In the Administrator interface, click Passwords in the main menu.**

   The Change User Password page appears by default.

FIGURE 3–6 Change User Password



Change User Password

Enter and confirm a new password, then select the resource accounts on which to change the password.

(Select **Change Identity system user and all resource accounts** to change the password on all accounts.) When finished, click **Change Password**.

User ID jrenfro

Password

Confirm Password

□ Change Identity system user and all resource accounts

Resource accounts whose password will be changed if selected.

Account ID	Resource Name	Resource Type	Exists	Disabled	Password Policy
□ jrenfro	Identity Manager	Identity Manager	Yes	No	Maximum Length: 16 Minimum Length: 4 Must not contain values of attributes: email, firstname, fullname, lastname
□ jrenfro	Simulated Resource	Simulated	Yes	No	None

2. **Select a search term (such as account name, email address, last name, or first name), and then a search type (starts with, contains, or is).**

3 **Type one or more letters of a search term in the entry field, and then click Find. Waveset 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.**

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

Resetting User Passwords

The process for resetting Waveset 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, Waveset 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 (by direct assignment or through the user's organization) controls several reset options, including:

- How often a password can be reset before resets are disabled
- Where the new password is displayed or sent

  Depending on the Reset Notification Option selected for the role, Waveset emails the new password to the user or displays it (on the Results page) to the Waveset administrator requesting the reset.

▼ To Reset Passwords from the User List Page

The Reset Password user action is available on the User List page (Accounts > List Accounts).

To reset a password from the User List page, use the following steps.

1 **In the Administrator interface, click Accounts in the main menu. The User List page displays on the List Accounts tab.**

2 **Select a user and click the User Actions drop-down menu.**

3 **To reset the password, select Reset Password.**

The Reset User Password page opens.

4 **Click the Reset Password button.**

▼ To Expire Passwords Using the Waveset Account Policy

When you reset a user password, the password is immediately expired by default. Consequently, the first time users log in after a password reset, they must select a new password to gain access. You can use the Edit the Reset User Password form to override this default, so that the user's password will expire according to the expire password policy set in the Waveset Account Policy associated with that user.

Use the following process to override the default change-password requirement.

1. **Edit the Reset User Password Form and set the following value to `false`.**

   `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword`

2. **Use the Reset option in the Waveset Account Policy to specify when a password expires.**

   The settings include

   - **permanent**. Waveset uses the time period specified in the `passwordExpiry` policy attribute 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**. Waveset uses the time period specified in the `tempPasswordExpiry` policy attribute 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.

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

Disabling, Enabling, and Unlocking User Accounts

This section describes how to disable and enable Waveset user accounts, and describes how to help users who have become locked out of their Waveset accounts.

▼ To Disable User Accounts

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

Note that administrators can disable user accounts from the Administrator interface, but they cannot lock user accounts. Accounts can only become locked if the user exceeds the allowable number of unsuccessful login attempts defined by the Waveset account policy

Note – If an assigned resource does not have native support for account disabling, but does support password changes, then Waveset can be configured to disable user accounts on that resource by assigning new, randomly generated passwords.

Use the following steps to ensure that this functionality works correctly:

1 **Open the "Identity System Parameters" page in the Edit Resource Wizard. (See "Managing Resources" on page 151 for instructions on how to open the wizard.)**

2 **In the "Account Features Configuration" table verify that both the Password feature and the Disable feature do not have check marks in the Disable? column. (To display the Disable feature, select Show All Features.)**

If the Disable feature does have a check mark in the Disable? column, accounts in the resource cannot be disabled.

More Information

Disabling Single User Accounts

To disable a user account, select it in the User List, and then select Disable from the User Actions drop-down menu.

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

Disabling Multiple User Accounts

You can disable two or more Waveset 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.

▼ To Enable User Accounts on a Resource Through Password Resets

User account enabling reverses the disabling process.

Depending on selected notification options, Waveset also displays the 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.

Note – If an assigned resource does not have native support for account enabling, but does support password changes, then Waveset can be configured to enable user accounts on that resource through password resets.

To ensure that this functionality works correctly, do the following:

---

1 **Open the "Identity System Parameters" page in the Edit Resource Wizard. (See "Managing Resources" on page 151 for instructions on how to open the wizard.)**

2 **In the "Account Features Configuration" table, verify that both the Password feature and the Enable feature do not have check marks in the Disable? column. (To display the Enable feature, select Show All Features.)**

If the Enable feature does have a check mark in the Disable? column, accounts in the resource cannot be enabled.

More Information

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. Waveset displays the results of enabling the Waveset account and all associated resource accounts.

Enabling Multiple User Accounts

You can enable two or more Waveset 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.

To Unlock User Accounts

Users become locked out if they are unsuccessful at logging in to Waveset. To become locked out, the user has to exceed the allowable number of unsuccessful login attempts defined by the Waveset account policy.

Note – Only login attempts on an Waveset user interface are counted towards an Waveset lockout (that is, either the administrator interface, the end-user interface, the command-line interface, or the SPML API interface). Failed login attempts on resource accounts are not counted and will not cause the user to be locked out of their Waveset account.

The Waveset account policy establishes the maximum number of failed password or question login attempts that can be made.

- Users who exceed the maximum number of failed password login attempts are locked out of all Waveset application interfaces, including the Forgot My Password interface.
- Users who exceed the maximum number of failed question login attempts can authenticate to any Waveset application interface except Forgot My Password.

Failed Password Login Attempts

Users who are locked out of Waveset due to excessive failed password login attempts will not be able to log in until an administrator unlocks the account or until the lock expires.

- An administrator can unlock an account if the administrator has administrative control of the user's member organization, as well as the `Unlock User` capability.
- If a `Lock Timeout` value is set in the Waveset Account Policy, a lock placed on an account will eventually expire. The `Lock Timeout` value for failed password login attempts is set by the Account lock created by failed password-logins expires in value.

Failed Question Login Attempts

Users who are locked out of the Forgot My Password interface due to excessive failed question login attempts will not be able to log in to that interface until an administrator unlocks the account, or until the locked user (or a user with appropriate capabilities) changes or resets the user's password, or until the lock expires.

- An administrator can unlock an account if the administrator has administrative control of the user's member organization, as well as the `Unlock User` capability.
- If a `Lock Timeout` value is set in the Waveset Account Policy, a lock placed on an account will eventually expire. The `Lock Timeout` value for failed question login attempts is set by the Account lock created by failed question-logins expires in value.

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

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

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.

Bulk Account Actions

You can perform several *bulk* actions on Waveset accounts, which allow you to act on multiple accounts at the same time.

You can initiate the following Bulk actions:

- **Delete**. Deletes, unassigns, and unlinks selected resource accounts. Select the "Target the Waveset Account" option to also delete each user's Waveset 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 Waveset Account" option to also disable each user's Waveset account.
- **Enable**. Enables any selected resource accounts. Select the "Target the Waveset Account" option to enable each user's Waveset account.
- **Unassign, Unlink**. Unlinks any selected resource accounts and removes the Waveset 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 Waveset user through a role or resource group.
- **Unlink**. Removes a resource account's association (link) with the Waveset user account. Unlinking does not remove the account from the resource. If you unlink an account that has been indirectly assigned to the Waveset 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. Use the Find Users page (Accounts → Find Users) to search for users.

You can save the results of a bulk account operation to a CSV file by clicking Download CSV when the task results appear upon completion of the task.

Launching Bulk Account Actions

▼ To Launch Bulk Account Actions

1. **In the Administrator interface, click Accounts in the main menu.**

2. **Click Launch Bulk Actions in the secondary menu.**

3. **Complete the form and then click Launch.**

   Waveset launches a background task to perform the bulk actions.

   To monitor the status of the bulk actions task, click Server Tasks in the main menu, and then click All Tasks.

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 Waveset 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 Waveset user.
- **command**. Contains the action taken on the Waveset user. Valid commands are:
  - **Delete**. Deletes, unassigns, and unlinks resource accounts, the Waveset account, or both.
  - **DeleteAndUnlink**. Deletes and unlinks resource accounts.
  - **Disable**. Disables resource accounts, the Waveset account, or both.
  - **Enable**. Enables resource accounts, the Waveset account, or both.
  - **Unassign**. Unassigns and unlinks resource accounts.
  - **Unlink**. Unlinks resource accounts.
  - **Create**. Creates the Waveset account. Optionally creates resource accounts.
  - **Update**. Updates the Waveset account. Optionally creates, updates, or deletes resource accounts.
  - **CreateOrUpdate**. Performs a create action if the Waveset 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, the only additional field you need to specify is resources. Use the resources field to specify which accounts on which resources will be affected.

The resources field can have the following values:

- **all**. Process all resource accounts including the Waveset account.
- **resonly**. Process all of the resource accounts excluding the Waveset account.
- *resource_name* `[ |` *resource_name …* `]`. Process the specified resource accounts. Specify Waveset to process the Waveset account.

The 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,Waveset
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create, Update, and CreateOrUpdate Commands

If you are performing Create, Update, or CreateOrUpdate commands, 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 "User View Attributes" in *Oracle Waveset 8.1.1 Deployment Reference* for information about 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 Waveset account.
- **waveset.resources**. A list of one or more resource names to assign to the Waveset account.
- **waveset.applications**. A list of one or more role names to assign to the Waveset account.
- **waveset.organization**. The organization name in which to place the Waveset account.
- **accounts**[*resource_name*].*attribute_name*. A resource account attribute. The names of the attributes are listed in the schema for the resource.

The following example illustrates the CSV format for create and update actions:

```
command,user,waveset.resources,password.password,
password.confirmPassword,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
```

The `CreateOrUpdate` command allows you to specify a specific account-type on a resource that supports multiple account-types. So if a user has multiple accounts on a specific resource, with each account being a different account type, the following example shows how to update the `admin` account type for the `userAye` user:

```
command,user,accounts[Sim1|admin].emailAddress
CreateOrUpdate,userAye,bbye8@example.com
```

Note –

Although the `CreateOrUpdate` command allows you to set account-specific attributes for a user's accounts, be aware that the following values in the global section of the User's View will be applied to *all* specified accounts:

- `accountId`
- `email`
- `password`
- `disable`
- All extended attributes

Consequently, a `BulkOps` command of the following form *might* not do what you expect.

```
command,user,accounts[Sim1].email
CreateOrUpdate,userAye,bbye8@example.com
```

If `userAye` already has a value for `email`, that value will be applied to the email attribute on the `Sim1` resource. You have no way to override this behavior.

Fields with More Than One Value

Some fields can have multiple values. These are known as multivalued 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 as follows:

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

When updating multivalued 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, as follows:

```
|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:

- The `waveset.bulk.fields.`*field_name* 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.
- The `waveset.bulk.fieldDirectives.`*field_name* attributes are only defined for those fields for which a directive was specified. The value is the directive string.
- Set the `waveset.bulk.abort` Boolean attribute to true to abort the current action.
- Set the `waveset.bulk.abortMessage` attribute 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 Waveset 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 Waveset users that match the action fields. A confirmation rule tests an Waveset user against the action fields to determine whether the user is a match. This two-stage approach allows Waveset 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.

For more information about correlation and confirmation rules, see Chapter 3, "Data Loading and Synchronization," in *Oracle Waveset 8.1.1 Deployment Guide*.

Correlation Rules

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

- 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 in the Waveset configuration object named `IDM Schema Configuration.`

Correlating on an extended attribute requires special configuration. The extended attribute must be specified as queryable.

Use the following steps to set an extended attribute as queryable:

1. Open `IDM Schema Configuration`. You must have the IDM Schema Configuration capability to view or edit `IDM Schema Configuration`.
2. Locate the `<IDMObjectClassConfiguration name='User'>` element.
3. Locate the `<IDMObjectClassAttributeConfiguration name=' xyz '>` element, where `xyz` is the name of the attribute that you want to set as queryable.
4. Set `queryable='true'`

   In "Correlation Rules" on page 78 the `email` extended attribute is defined as queryable.

EXAMPLE 3–1 XML Excerpt That Defines the Email Extended Attribute as Queryable

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email' syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User' extends='Principal' description='User description'>
      <IDMObjectClassAttributeConfiguration name='email' queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
 </IDMSchemaConfiguration>
```

You must restart the Waveset application (or the application server) for the `IDM Schema Configuration` change to take effect.

Confirmation Rules

Inputs to any confirmation rule are as follows:

- Use `userview` for a full view of an Waveset user.
- Use `account` for a 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 for the following situations:

- 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.

Managing Account Security and Privileges

This section discusses actions you can take to provide secure access for user accounts and to manage user privileges in Waveset.

- "Setting Password Policies" on page 80
- "Setting Account Authentication Policies" on page 83
- "Assigning Administrative Privileges" on page 88

Setting Password Policies

Resource password policies establish the limitations for passwords. Strong password policies provide added security to help protect resources from unauthorized login attempts. You can edit a password policy to set or select values for a range of characteristics.

To begin working with password policies, click Security on the main menu, and then click Policies.

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

Note – For more information on policies, see "Configuring Waveset Policies" on page 93.

Creating a Policy

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

Length Rules

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

Policy Type

Choose one of the policy type buttons . If you choose the Other option, you must enter the type in the text field provided.

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

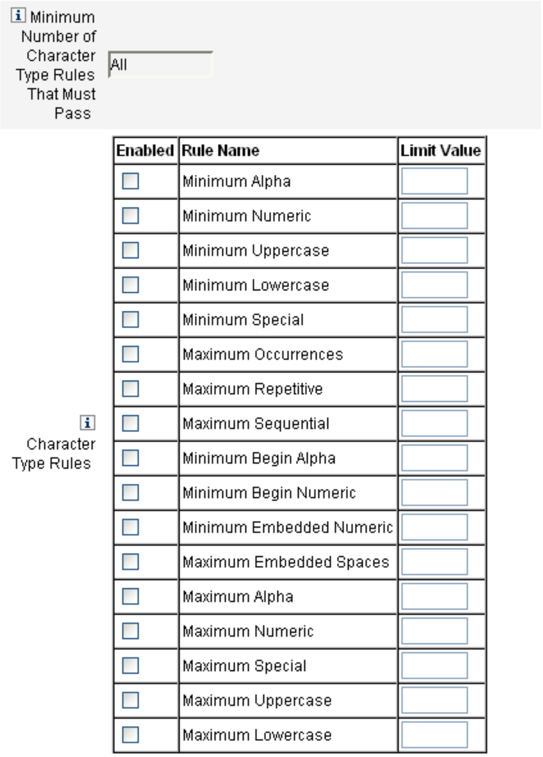
Enter a numeric limit value for each character type rule; or enter All to indicate that all characters must be of that type.

Minimum Number of Character Type Rules

You can also set the minimum number of character type rules that must pass validation, as illustrated in Figure 3–7. The minimum number that must pass is one. The maximum cannot exceed the number of character type rules that you have enabled.

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

FIGURE 3–7 Password Policy (Character Type) Rules



Minimum Number of Character Type Rules That Must Pass: All

Character Type Rules

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

Dictionary Policy Selection

You can choose to check passwords against words in a dictionary to guard against simple dictionary attacks.

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, see "What is a Dictionary Policy?" on page 96.

Password History Policy

You can prohibit the reuse 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.

You can also exclude words by configuring and implementing the dictionary policy. For more information, see "What is a Dictionary Policy?" on page 96.

Must Not Contain Attributes

You can enter one or more attributes that the password may not contain.

You can specify the following attributes:

- `accountID`
- `email`
- `firstname`
- `fullname`
- `lastname`

You can change the allowed set of "must not contain" attributes for passwords in the `UserUIConfig` configuration object. See "Must Not Contain Attributes in Policies" on page 96 for more information.

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: Waveset Parameters pages.

Setting Account Authentication Policies

You must configure user authentication, and the rules that govern authentication, as part of an Waveset account policy. Unlike password policies, Waveset account policies are assigned directly to the user or through the organization assigned to the user (on the Create and Edit User pages). The user authentication methods you establish enables users to access Waveset when they forget their user ID or passwords, or when their passwords are reset.

You can configure the following authentication methods for an Waveset account policy:

- **Authentication questions**. Require users to answer one or more account authentication questions to gain access to Waveset. The authentication question policy determines what happens when a user clicks on the Forgot Your Password? button on the login page or when accessing the Change My Answers page.
- **Login recovery**. Resets the user's password, then emails both the login and password to the user's email address.

Instructions for configuring these methods from the Waveset Administrator interface follow.

To Establish Authentication Questions for an Account Policy

1. Select Security > Policies from the main menu.
2. Choose DefaultWaveset Account Policy from the list of policies.

   Authentication selections are offered in the Secondary Authentication Policy Options area of the page. The following table describes each option.

Option	Description
All	Requires the user to answer all policy-defined and personalized questions.
Any	Waveset displays all policy-defined and personalized questions. You must specify how many questions the user must answer.

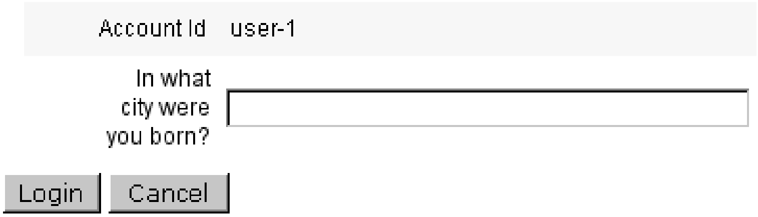
Option	Description
Next	Requires the user to answer all possible policy-defined questions the first time that user logs in. If the user clicks the Forgot Your Password? button during login, Waveset displays the first question. If the user answers incorrectly, Waveset displays the next question, and so on until the user answers an authentication question correctly and logs in, or is locked out based on the specified failure attempts limit. User-generated questions are not supported for this policy.
Random	Allows the administrator to specify how many questions the user must answer. Waveset randomly selects and displays the specified number of questions from the list of questions defined in the policy as well as those the user has defined. The user must answer all questions displayed.
Round robin	Waveset selects the next question from the list of configured questions and assigns this question to the user. The first user is assigned the first question in the list of authentication questions, and the second user is assigned the second question. This pattern continues until the number of questions is exceeded. At that point, questions are assigned to users in sequential order. For example, if there are 10 questions, the 11th and 21st users are assigned the first question. Only the selected question is displayed. If you want the user to answer a different question every time, use the Random policy and set the number of questions to 1. Users cannot define their own authentication questions. See "Using Personalized Authentication Questions" on page 85 for more information about this feature.

You can verify your authentication choices by logging in to the Waveset End User interface, clicking the Forgot Your Password? button, and answering the presented question or questions.

Note – After you set up the authentication questions, users *must* log in to the End User interface and provide initial answers to their authentication questions. If the users do not set answers the first time they log in, they cannot successfully log in without a password.

The following figure shows an example of the User Account Authentication screen.

FIGURE 3–8 User Account Authentication



Account Id user-1

In what city were you born?

Using Personalized Authentication Questions

In the Waveset account policy, you can select an option to allow users to supply their own authentication questions in the End 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.

To configure Waveset to allow user-supplied questions, perform the following steps:

1. Select the Security > Policies tabs.
2. On the Policies page, click Default Identity Manager Account Policy.
3. When the Policy page displays, scroll down to the Secondary Authentication Policy Options section.

   Complete this section as follows:

   - **For Login Interface**. Select User Interface from the menu.
   - **Maximum Number of Failed Login Attempts**. Enter the maximum number of failed attempts you want to allow.
   - **Enforce Answer Policy at Login**. Deselect this option.
   - **Authentication Questions Policy**. Select Any from the menu.
   - **Minimum Number of Questions User is Required to Answer**. Enter the minimum number of questions you want the user to answer.
   - **Answer Quality Policy**. Select None from the menu.

   Note – If you previously configured one or more Authentication Answer Quality Policies, they will be available for selection from the menu. Otherwise, the only option is None.

   - **Allow User Supplied Questions**. Select this option to allow user-supplied questions.
   - **Minimum Number of User Supplied Questions**. Enter the minimum number of questions you want the user to provide.
   - **Supplied Question Quality Policy**. Select None from the menu.

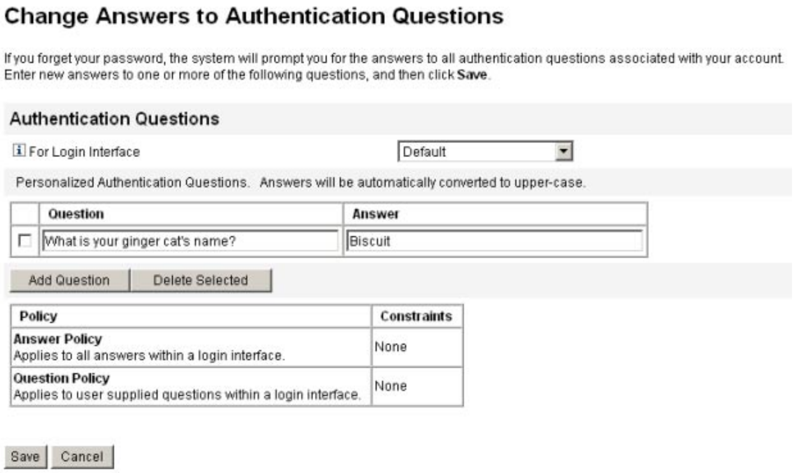
Note – If you previously configured one or more Authentication Question Quality Policies, they will be available for selection from the menu. Otherwise, the only option is None.

- **Organizations**. Select one or more organizations to which this object will be available.

4. Click Save to save your changes.

Users can add and change questions from the Change Answers to Authentication Questions page. An example of this page is shown in Figure 3–9.

FIGURE 3–9 Change Answers: Personalized Authentication Questions



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

Bypassing the Change Password Challenge after Authentication

When users successfully authenticate by answering one or more questions, by default they are challenged by the system to provide a new password. You can configure Waveset to bypass the change password challenge, however, by setting the `bypassChangePassword` system configuration property for one or more Waveset applications.

For instructions on editing the system configuration object, see "Editing Waveset Configuration Objects" on page 108.

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

EXAMPLE 3–2 Setting the Attribute to Bypass the Change Password Challenge

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

To disable this password challenge for a specific application, set it as follows.

EXAMPLE 3–3 Setting the attribute to Disable the Change Password Challenge

```
<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>
...
```

To Establish Login Recovery for an Account Policy

Configuring Login Recovery as an alternative to the security questions-based login implements a message obfuscation option that renders the same generic result message for all errors and successes. This method helps prevent account harvesting.

Note – The obfuscate messages option is enabled by default in the `loginRecovery.jsp` file. You can set this same option in the `lookupUserId.jsp` files.

Functionally, Login Recovery uses the same system as the Forgot Your User ID? method and both methods share the same configuration attributes. The main difference between these two methods is that Login Recovery also resets the user's password and then emails both the login and the password to the user's email address.

You can replace the security questions-based log-in method with the Login Recovery method by redirecting the Forgot Your Password? button or by creating a new Login Recovery button on the Log In pages. You configure either option in the System Configuration file, as follows:

- To redirect Forgot Password to Login Recovery, specify

  ```
  ui.web.user.questionLogin.forceLoginRecovery = true
  ui.web.admin.questionLogin.forceLoginRecovery = true
  ```

- To use a Login Recovery button instead of Forgot Password/Lookup, specify

  ```
  ui.web.user.disableLoginRecovery = false
  ui.web.admin.disableLoginRecovery = false
  ui.web.user.disableForgotPassword = true
  ui.web.admin.disableForgotPassword = true
  ui.web.user.disableForgotUserId = true
  ui.web.admin.disableForgotUserId = true
  ```

Assigning Administrative Privileges

You can assign Waveset administrative privileges, or capabilities, to users as follows:

- Admin Roles. Users assigned an Admin Role inherit the capabilities and controlled organizations defined by the role. By default, all Waveset user accounts are assigned the `User Admin Role` when created. For detailed information about Admin Roles and creating an Admin Role, see "Understanding and Managing Admin Roles" on page 201 in Chapter 6, "Administration."
- Capabilities. Capabilities are defined by rules. Waveset provides sets of capabilities grouped into functional capabilities that you can select from. Assigning capabilities allows for more granularity in assigning administrative privileges. For information about capabilities and creating capabilities, see"Understanding and Managing Capabilities" on page 198 in Chapter 6, "Administration."
- Controlled organizations. Controlled organizations grant administrative control privileges over specified organizations. For more information, see "Understanding Waveset Organizations" on page 190 in Chapter 6, "Administration."

For more information about Waveset Administrators and administrative duties, see Chapter 6, "Administration"

User Self-Discovery

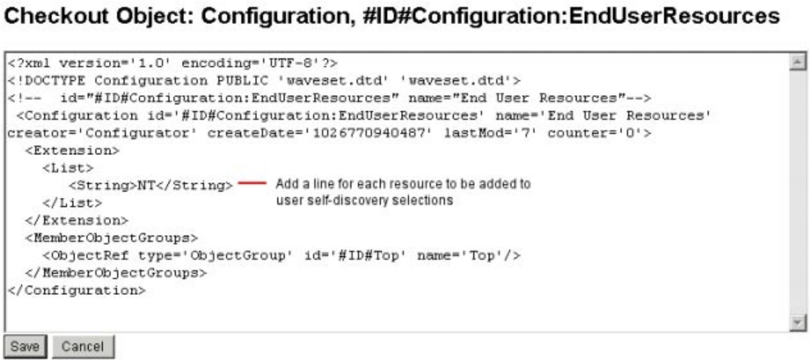
The Waveset end-user interface allows end-users to *discover* resource accounts. This means that a user with an Waveset identity can associate it with an existing, but unassociated, resource account.

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.

1. Edit the “End User Resources” configuration object.

   For instructions on editing Waveset configuration objects, see “Editing Waveset Configuration Objects” on page 108.

2. Add `<String>`*Resource*`</String>`, where *Resource* matches the name of a resource object in the repository, as illustrated in the following figure.



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

3. Click Save.

   When self-discovery is enabled, the user is presented with a new selection under the Profile menu tab on the Waveset User interface (Self Discovery). This area allows the user to select a resource from an available list, and then enter the resource account ID and password to link the account with his Waveset identity.

Note – To give end-users access to Waveset configuration objects, administrators can also use the “End User” organization. See “The End User Organization” on page 211 for details.

Anonymous Enrollment

The anonymous enrollment feature allows a user without an Waveset account to obtain one by request.

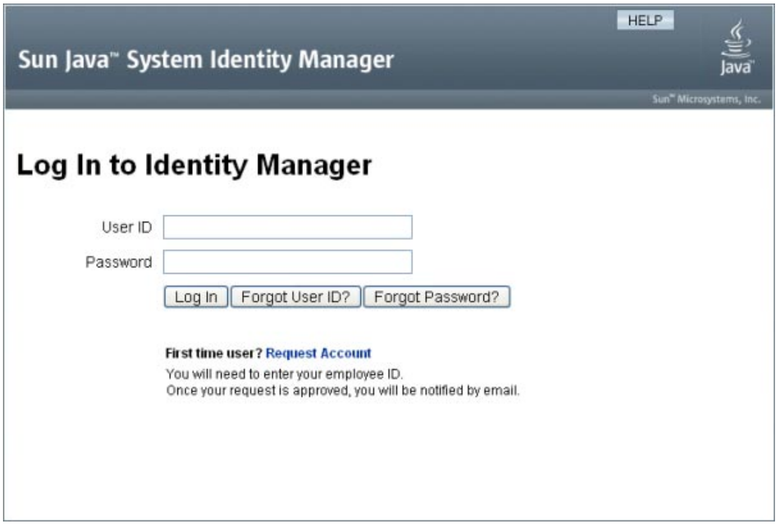
Enabling Anonymous Enrollment

By default, the anonymous enrollment feature is disabled.

To enable the anonymous enrollment feature,

1. In the Administrator interface, click Configure, and then click User Interface.
2. In the Anonymous Enrollment area, select the Enable option, and then click Save.

   When a user logs in to the User interface, the login page will display the text First time user? followed by a Request Account link.



Log In to Identity Manager

First time user? Request Account
You will need to enter your employee ID.
Once your request is approved, you will be notified by email.

Note – The text First time user? Request Account is customizable. See the *Oracle Waveset 8.1.1 Deployment Guide*for details.

Configuring Anonymous Enrollment

From the Anonymous Enrollment area on the User Interface page, you can configure the following options for the anonymous enrollment process:

- **Notification Template**. Specify the ID of an email template to use to send notifications to the user requesting an account.
- **Require Privacy Policy**. If selected, then the user must accept the privacy policy before he can request an account. This is enabled by default.

- **Enable Validation**. If selected, then the user must validate his employment before he can request an account. This is enabled by default.
- **Process Launch URL**. Enter a URL to specify which workflow will be used for the anonymous enrollment process.
- **Enable Notifications**. If selected, then a notification email will be sent to the user when his account has been created.
- **Email Domain**. Enter the name of the email domain to use to construct the user's email address.

Click Save when finished.

User Enrollment Process

When a user logs on to the User interface, that user can request an account by clicking Request Account on the login page.

Waveset displays the first of two registration pages, which requests a first name, last name, and employee ID. If the Enable Validation attribute is set to yes (the default), then this information must be validated before the user can proceed to the next page.

The `verifyFirstname`, `verifyLastname`, `verifyEmployeeId`, and `verifyEligibility` rules in `EndUserLibrary` validate the information for each attribute.

Note – You may need to modify one or more of these rules. In particular, you should modify the rule that verifies the employee ID to use a Web services call or Java class to verify the information.

If the Enable Validation attribute is disabled, then the initial registration page does not display. In this case, you must modify the End User Anonymous Enrollment Completion form to allow the user to enter information normally captured by the initial validation form.

From the information provided on the Registration page, Waveset generates:

- An account ID (following the convention of first initial, last initial, employee ID).
- An email address in the form:

  FirstName.LastName@EmailDomain

  Where *EmailDomain* is the domain set by the Email Domain attribute in anonymous enrollment configuration.
- The manager attribute (`idmManager`). You can set this attribute by modifying the `EndUserRuleLibrary:getIdmManager` rule. By default, the manager is set to Configurator. The administrator designated as the manager must approve the user request before his account is provisioned.

- The organization attribute. You can set this attribute by customizing the `EndUserRuleLibrary:getOrganization` rule. By default, users are assigned to the top of the organizational hierarchy ("Top").

If the information provided by the user on the Registration page validates correctly, then Waveset presents the user with the second Registration page. Here the user must enter a password and password confirmation. If the Require Privacy Policy attribute is set to yes, then the user must also select an option to accept the terms of the privacy policy.

When the user clicks Register, Waveset presents a confirmation page. If the Enable Notifications attribute is set to yes, then the page indicates the user will receive email notification when he account has been created.

The account is created after the standard Create User process (including approvals required by the `idmManager` attribute and policy settings) is complete.

◆ ◆ ◆ CHAPTER 4

Configuring Business Administration Objects

This chapter provides information and procedures for using the Administrator Interface to set up and maintain Waveset objects. For more information about Waveset objects, see "Waveset Objects" on page 26 of the Overview chapter.

Note – For information about configuring Waveset for a Service Provider implementation, see Chapter 17, "Service Provider Administration"

This chapter is organized in the following topics:

- "Configuring Waveset Policies" on page 93
- "Customizing Email Templates" on page 98
- "Configuring Audit Groups and Audit Events" on page 102
- "Remedy Integration" on page 103
- "Configuring the End-User Interface" on page 104
- "Registering Waveset" on page 105
- "Editing Waveset Configuration Objects" on page 108

Configuring Waveset Policies

Read this section for information about configuring user policies.

This section contains the following topics:

- "What are Policies?" on page 94
- "Must Not Contain Attributes in Policies" on page 96
- "What is a Dictionary Policy?" on page 96

What are Policies?

Waveset policies set limitations for Waveset users by establishing constraints for Waveset accountID, login, and password characteristics.

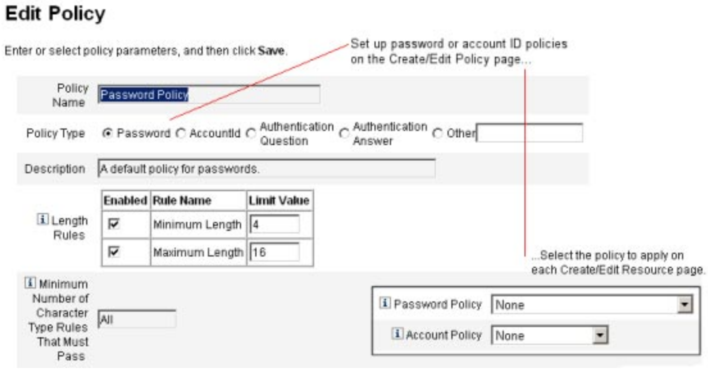
Note – Waveset also provides Audit policies that are specifically designed to audit user compliance. Audit policies are discussed in Chapter 13, "Identity Auditing: Basic Concepts"

Policies are categorized as the following types:

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

  You can set or select the following options:

  - **User Account Policy Options**. Specify how Waveset 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.
  - **Secondary Authentication Policy Options**. Determine how authentication questions are presented to the user, whether the user can provide his own authentication questions, enforce authentication at login, and establish the bank of questions that can be presented to a user.
- **Service Provider System Account Policies**. Use this policy type in a service provider implementation to establish user, password, and authentication policy options and constraints for service provider users. You assign the policies to organizations from the Create and Edit Organization pages or to users from the Create and Edit Service Provider User pages.
- **String Quality Policies**. Includes policy types such as password, accountID, and authentication. Use to set length rules, character type rules, allowed words, and attribute values. This policy type is tied to each Waveset resource and is set on each resource page. The following figure provides an example.



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

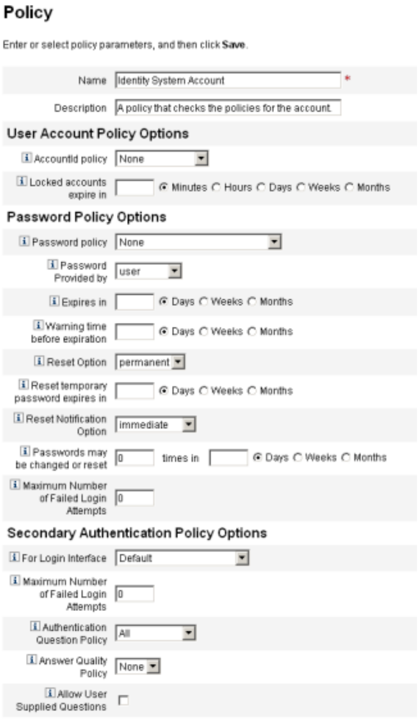
You can set the following options and rules for passwords and accountIDs:

- **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 reused. 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.

You create and edit Waveset user policies from the Policies page. To open this page, follow these steps:

1. Log in to the Administrator interface.
2. Click the Security tab, then click the Policies subtab.

   The Policies page opens as shown in the following figure.



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: □

Must Not Contain Attributes in Policies

You can change the allowed set of "must not contain" attributes in the `UserUIConfig` configuration object.

Attributes are listed in `UserUIConfig` as follows:

- `<PolicyPasswordAttributeNames>` attribute. Policy type Password
- `<PolicyAccountAttributeNames>` attribute. Policy type AccountId
- `<PolicyOtherAttributeNames>` attribute. Policy type Other

What is a Dictionary Policy?

A dictionary policy enables Waveset 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, Waveset 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.)

▼ To Configure a Dictionary Policy

To set up a dictionary policy, you must:

- Configure dictionary server support
- Load the dictionary

1 **Open the Policies page as described in "Configuring Waveset Policies" on page 93.**

2 **Click Configure Dictionary to display the Dictionary Configuration page.**

3 **Select and enter database information.**

Database information includes:

- **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. The load task may take a few minutes to complete.**

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

▼ To Implement a Dictionary Policy

Use the following steps to implement a dictionary policy:

1 **Open the Policies page as described in "Configuring Waveset Policies" on page 93.**

2 **Click the Password Policy link to edit the password policy.**

3. **On the Edit Policy page, select the Check passwords against dictionary words option.**

4. **Click Save to save your changes.**

   Once implemented, all changed and generated passwords will be checked against the dictionary.

Customizing Email Templates

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

- **Access Review Notice**. Sends notification that the access rights for a user needs to be reviewed. The system sends this notification when a violation of an access policy must be remediated or mitigated.
- **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.
- **Account Deletion Approval**. Sends notification to an approver that a user account deletion action is awaiting approval. 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.
- **Account Deletion Notification**. Sends notification that an account has been deleted.
- **Account Update Notification**. Sends notification to the specified email addresses or user accounts that an account has been updated.
- **External Resource**. Notifies an external resources provisioner that a provisioning task must be performed.
- **Password Reset**. Sends notification of an Waveset password reset. Depending on the Reset Notification Option value selected for the associated Waveset 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.

- **Policy Violation Notice**. Sends a notice that an account policy violation has occurred.
- **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.

  Note – Request resources are deprecated in favor of external resources as of the Waveset version 8.1 release. You can no longer create new connections using the Request adapter. Use the External Resource adapter instead. For more information, see "Understanding and Managing External Resources" on page 157.

- **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 Waveset policy, the system displays notification immediately (in the Web browser) to the user, emails the user, or emails the role approvers.
- **User ID Recovery**. Sends a recovered user ID to the specified email address.

▼ To Customize an Email Template

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

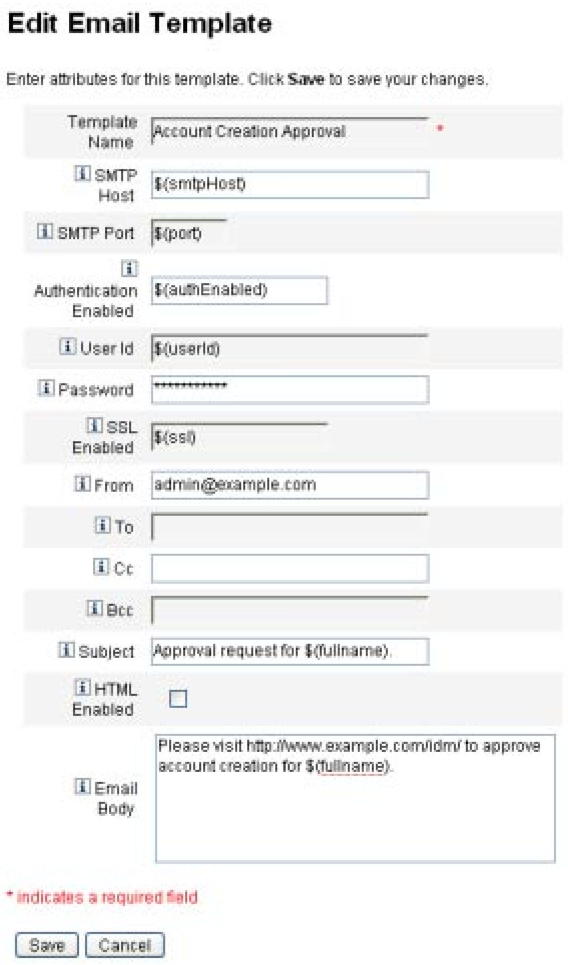
```
Please go to http://host.example.com:8080/idm/approval/approval.jsp to approve
account creation for $(fullname).
```

Use the following procedure to customize an email template using the Account Creation Approval template as an example:

1 **In the Administrator interface, click the Configure tab, then click the Email Templates subtab.**

The Email Templates page opens.

2 **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	$(smtpHost)
SMTP Port	$(port)
Authentication Enabled	$(authEnabled)
User Id	$(userId)
Password	************
SSL Enabled	$(ssl)
From	admin@example.com
To	
Cc	
Bcc	
Subject	Approval request for $(fullname).
HTML Enabled	□
Email Body	Please visit http://www.example.com/idm/ to approve account creation for $(fullname).

* indicates a required field

3 **Enter details for the template.**

You can enter the following information:

- 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 Waveset accounts that will be the recipients of the email notification.
- In the Bcc field, enter one or more email addresses or Waveset accounts that will receive blind copies of the email notification.

- In the Email Body field, customize the content to provide a pointer to your Waveset location.

4 **Click Save.**

You can also modify email templates by using the Identity Manager Integrated Development Environment (Identity Manager IDE). For information about the Identity Manager IDE, go to the following website: `https://identitymanageride.dev.java.net/`.

Note – You must register and log in to this site.

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.

.

TABLE 4–1 Email Template Variables

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

TABLE 4–1 Email Template Variables *(Continued)*

Template	Allowable Variables
Risk Analysis	`$(report)` – risk analysis report
Temporary Password Reset	`$(password)` – newly generated password `$(expiry)` – password expiration date

Configuring Audit Groups and Audit Events

Setting up audit configuration groups allows you to record and report on system events you select. Setting up audit groups also enables you to run AuditLog reports later.

▼ To Open the Audit Configuration Page

You use the Audit Configuration page to set up audit groups. To open the Audit Configuration page, follow these steps:

1 **Open the Administrator interface.**

2 **Click the Configure tab, then click the Audit subtab.**

The Audit Configuration page opens.

▼ To Configure Audit Groups

Configuring audit groups and events requires the Configure Audit administrative capability.

1 **Open the Audit Configuration page as described in the previous section.**

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

2 **Click an audit 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.**

3 **Check that the Enable auditing check box is selected. Clear the check box to disable the auditing system.**

Note – For more information about audit groups, see “Audit Configuration” on page 317 inChapter 10, “Audit Logging.”

▼ To Add Events to the Audit Configuration Group

Use the following steps to add an event to the group:

1. **Click New.**

   Waveset adds an event at the bottom of the page.

2. **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.**

3. **Click OK to add the event to the group.**

▼ To Edit Events in the Audit Configuration Group

You can edit events in the group by adding or deleting actions for an object type, as follows:

1. **Move items in the Actions column from the Available to the Selected area for that object type.**

2. **Click OK.**

Remedy Integration

You can integrate Waveset 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. (See “Managing the Resources List” on page 145.) 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, open the Administrator interface, click the Configure tab, then click Remedy Integration. You will then select the Remedy schema and resource.

Creation of Remedy tickets is configured through Waveset 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 Chapter 1, “Workflow,” in *Oracle Waveset 8.1.1 Deployment Reference*.

Configuring the End-User Interface

Administrators can configure certain aspects of the end-user interface by modifying a form in the Administrator interface.

▼ To Set Options for Displaying Information in the End-User Interface

1. **In the Administrator interface, click Configure in the main menu.**

2. **Click User Interface in the secondary menu.**

   The User Interface page opens.

3. **Complete and save the End User Dashboard portion of the form. Click Help if you need help with the form.**

   For information on completing the Anonymous Enrollment portion of the form, see "Anonymous Enrollment" on page 89.

▼ To Enable Process Diagrams in the End-User Interface

Process diagrams depict the workflow that Waveset follows when end-users launch a request or update their profile. When enabled, process diagrams display on the results page after the end-user submits a form.

Process diagrams must be enabled in the Administrator interface before they can be enabled in the end-user interface. See "Enabling Process Diagrams for Use in Waveset" on page 54 for more information.

1. **Open the User Interface configuration page by following the steps in "Configuring the End-User Interface" on page 104**

2. **Select the Enable End-User Process Diagrams option, which is located in the Result Pages section of the form.**

   If the Enable End-User Process Diagrams option is not available, then you must first enable process diagrams in the Administrator interface. See "Enabling Process Diagrams for Use in Waveset" on page 54.

3. **Click Save.**

Registering Waveset

Administrators are encouraged to register their installation of Waveset.

You must have an Oracle Online Account and password to register. If you do not have an Oracle Online Account, you can register for one by completing the form at this address:

https://reg.sun.com/register

Waveset can be registered from the console or by using the Administrator interface.

Registering from the console allows you to also create a local service tag, which can be used with Sun Service Tag software to track your inventory of Oracle systems, software, and services. The service tags client package should be installed before you create a local service tag. This package can be downloaded by clicking the Download Service Tags button at the following address:

http://inventory.sun.com/inventory

To register Waveset, you must log on with an administrator account that allows you to configure Waveset objects. This account must have the Product Registration capability. For information about capabilities, see "Assigning Capabilities to Users" on page 201.

Note – Java on your Waveset application servers must be properly configured for SSL for the product registration feature to work. All Jar files referenced in your `java.security` file (or equivalent) need to be present.

The rest of this section provides information and instructions to help you register Waveset. This information is organized into the following topics:

- "Registering Waveset from the Console" on page 105
- "To Register Waveset from the Administrator Interface" on page 107

Registering Waveset from the Console

You use the `register` command to register Waveset from the console. This section contains information about this command, including:

- "`register` Command Usage" on page 105
- "`register` Command Options" on page 106
- "To Register Waveset from the Console" on page 106

`register` Command Usage

```
register -local
register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

register Command Options

The following table describes the options you can use with the register command.

TABLE 4–2 Command Options

Option	Description
`-local`	Create a service tag on this host.
`-remote`	Register this installation of Waveset over the network directly with Oracle.
`-u <userid>`	The Waveset user ID of the Waveset administrator who is authorized to do the registration.
`-p <password>`	The Waveset password of the Waveset administrator who is authorized to do the registration.
`-prompt`	Interactively prompt for the password if missing.
`-userSOA <userid>`	The user ID of the Oracle Online Account that will be used for registration. Required if registering with the `-remote` option.
`-passSOA <password>`	The password of the Oracle Online Account that will be used for registration. Required if registering with the `-remote` option.
`-proxy <proxyHost>`	The network proxy to use for access to the Oracle online registration service. Required if registering with the `-remote` option and your network is configured to use a proxy to reach external Internet addresses.
`-port <proxyPortNumber>`	The port on the network proxy to use for access to the Oracle online registration service. Required if registering with the `-remote` option and your network is configured to use a proxy to reach external Internet addresses.
`-help | -?`	Print help for this command to the console.

▼ To Register Waveset from the Console

To register Waveset from the Console, you must create a local service tag or register with Oracle over the Internet. Use the following instructions:

1 **Start the Waveset console (command-line) interface.**

- From a Windows command line, type

  `%WSHOME%\bin\lh`

- From a UNIX command line, type

  `$WSHOME/bin/lh`

2 **Use the `register` command to register Waveset.**

Use the following syntax:

- To create a local service tag,

  `register -local`

- To register Waveset over the Internet, use the following command:

  `register -remote -u` <*userid*> **`-p`** <*password*> **`-userSOA`** <*soaUserid*> **`-passSOA`** <*soaPassword*> **`-proxy`** <*proxyHost*> **`-port`** <*proxyPortNumber*>

  where:

  - **userid** is the Waveset userID of the Waveset administrator who is authorized to do the registration.
  - **password** is the Waveset password of the Waveset administrator who is authorized to do the registration.
  - **soaUserid** is the user ID of the Oracle Online Account that will be used for registration.
  - **soaPassword** is the password of the Oracle Online Account that will be used for registration.
  - **proxyHost** is the network proxy to use for access to the Oracle online registration service. Only required if your network is configured to use a proxy to reach external Internet addresses.
  - **proxyPortNumber** is the port on the network proxy to use for access to the Oracle online registration service. Only required if your network is configured to use a proxy to reach external Internet addresses.

▼ To Register Waveset from the Administrator Interface

If you do not need to create a local service tag, register Waveset from the Administrator interface.

1. **In the Administrator interface, click Configure.**

2. **In the secondary menu, click Product Registration.**

   The Product Registration page opens.

3. **Complete the form and click Register Now. Click the i-Helps for information about individual form fields.**

Note –

- If your application server is not configured to allow outgoing SSL connections, you might see the following error message:

  ```
  Failed to register on Sun Connection server
  due to invalid Sun Online Account user/password.
  ```

  To resolve this issue, add the appropriate trusted root certificates to your application server's keystore. Consult your application server's documentation for details.
- If old versions of `xml-apis.jar` and `xercesImpl.jar` are present in your application server's classpath, you might see the following error message:

  ```
  java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
  ```

  To resolve this problem, modify the classpath so that only the most recent versions of `xml-apis.jar` and `xercesImpl.jar` are present.

Editing Waveset Configuration Objects

In the course of administering Waveset, you will occasionally be called upon to edit the Waveset system configuration object (also referred to as the System Configuration File), or other similar objects.

1. **Open the Waveset Debug Page by typing the following URL into your browser.**

   `http://<`*AppServerHost*`>:<`*Port*`>/idm/debug/session.jsp`

   The System Settings page opens.

   Note – You must have the Debug capability to view `/idm/debug/` pages.
2. **Find the List Objects button, then select Configuration from the adjacent Type drop-down list.**
3. **Click the List Objects button.**

   The List Objects of type: Configuration page opens.
4. **In the list of objects, find the object you need, then click edit.**

   For example, to edit the system configuration object, find System Configuration, then click edit.
5. **Edit the object as directed and click Save.**
6. **If directed to do so, restart your server (or servers).**

CHAPTER 5

Roles and Resources

This chapter discusses Waveset roles and resources.

The information in this chapter is organized into the following topics:

- "Understanding and Managing Roles" on page 109
- "Understanding and Managing Waveset Resources" on page 144
- "Understanding and Managing External Resources" on page 157

Understanding and Managing Roles

Read this section for information about setting up roles in Waveset. In large organizations, role-based resource assignments greatly simplify resource management.

Note – Do not confuse *roles* and *admin-roles*. Roles are used to manage end-user access to external resources. Admin-roles, on the other hand, are primarily used to manage administrator access to internal Waveset objects such as users, organizations, and capabilities.

The information in this section discusses roles. For information about admin-roles, see "Understanding and Managing Admin Roles" on page 201.

What are Roles?

A role is an Waveset object that allows resource access rights to be grouped and efficiently assigned to users.

Roles are organized into four role types:

- Business Roles
- IT Roles

- Applications
- Assets

Business Roles organize into groups the access rights that people who do similar tasks in an organization need to do their job duties. Typically, Business Roles represent user job functions. In a financial institution, for example, Business Roles might correspond to job functions like bank teller, loan officer, branch manager, clerk, accountant, or administrative assistant.

IT Roles, Applications, and *Assets* organize resource entitlements into groups. In order to provide end-users with access to resources, IT Roles, Applications, and Assets are assigned to Business Roles so that users can access the resources they need to do their jobs. IT Roles contain a specific set of Applications, Assets, and/or Resources, including specific entitlements on those assigned Resources. IT Roles can also contain other IT Roles.

Note – The concept of role types is new in Waveset version 8.0. If your organization upgraded to version 8.0 from an earlier version of Waveset, your legacy roles were imported as IT Roles. For more information, see "Managing Roles Created In Versions Prior to Version 8.0" on page 110.

IT Roles, Applications, and Assets can be *required, conditional,* or *optional.*

- A required role will always be assigned to the end-user.
- A conditional role has conditions that must evaluate to true in order for the role to be assigned.
- An optional role can be requested separately, and, upon approval, assigned to the end-user.

Required, conditional, and optional roles allow a Business Role designer to define coarse-grained access to contained roles in order to achieve regulatory compliance, while still allowing flexibility for an end-user's manager to fine-tune the end-user's access rights. Users assigned conditional or optional roles can still share the same assigned Business Role, but have different assigned access rights. With this approach, there is no need to define a new Business Role for each permutation of access requirements within an organization (a problem known as *role explosion*).

Putting Role Types to Work

The following discussion describes how to use role types effectively. For role type descriptions, see the previous section.

Managing Roles Created In Versions Prior to Version 8.0

Organizations that upgraded from an earlier version of Waveset to version 8.0 will automatically have their legacy roles converted to IT Roles. These IT Roles will remain directly assigned to users. Legacy roles will not be assigned a role owner as part of the upgrade process.

A role owner can be assigned later, however. (For information on role owners, see “Designating Role Owners and Role Approvers” on page 122.)

By default, organizations that upgrade to version 8.0 can directly assign both IT Roles and Business Roles to users (see Figure 5–2).

Organizations with legacy roles should consider creating new roles based on the guidelines outlined in the next section.

Using Role Types to Design Flexible Roles

IT Roles, Applications, and Assets are the role designer’s building blocks. These three role types are used in combination to build up user entitlements (or, *access rights*). IT Roles, Applications, and Assets are then assigned to Business Roles.

Designing Business Roles

In Waveset, a user can be assigned one or more roles, or no role. With the introduction of role types in Waveset 8.0, it is recommended that you only directly assign Business Roles to users. In fact, by default, you cannot directly assign any of the other role types to users unless your organization had a pre-8.0 version of Waveset installed and upgraded to at least version 8.0. This default restriction can be changed by modifying the role configuration object (“Configuring Role Types” on page 140).

To reduce complexity, Business Roles cannot be nested. In other words, one Business Role cannot contain another Business Role. In addition, Business Roles cannot directly contain resources and resource groups. Instead, resources and resource groups should be assigned to either an IT Role or an Application, which can then be assigned to one or more Business Roles.

Designing IT Roles

IT Roles can contain Applications, and Assets, as well as other IT Roles. IT Roles can also contain resources and resource groups.

IT Roles are intended to be created and managed either by your organization’s IT staff, or by the resource owners who understand the entitlements that are required to enable specific privileges within the resource.

Designing Applications and Assets

Applications and Assets are role types that are intended to represent commonly used business terms to describe things that end-users need in order to do their jobs. For example, an Application role could be named “Customer Support Tools” or “Intranet HR-Tool Admin.“

- Applications cannot contain roles, but they can contain resources and resource groups. Applications can also define specific entitlements that restrict access to only specific applications on contained resources.

- Assets are (typically) non-connected or non-digital resources, such as mobile phones and portable computers, that require manual provisioning. Consequently, assets cannot contain roles, resources, or resource groups.

Applications and Assets are intended to be assigned to Business Roles and IT Roles.

Note –

Role administrators should be assigned one or more of the following capabilities:

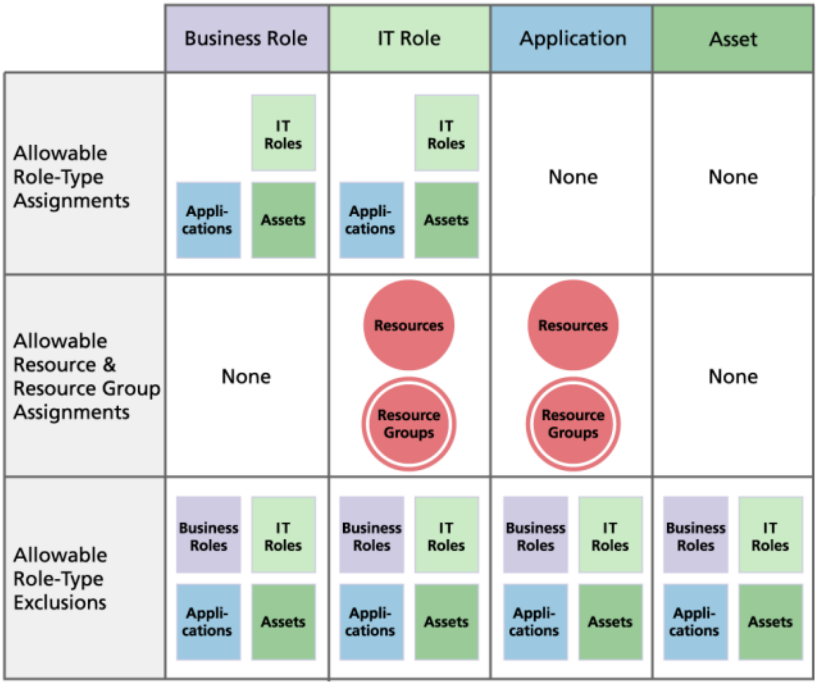
- Asset Administrator
- Application Administrator
- Business Role Administrator
- IT Role Administrator

See "Assigning Capabilities to Users" on page 201 for more information.

Role Types in Summary

The following figure shows which role-types, resources, and resource-groups can be assigned to each of the four role-types. The figure also shows that role-type exclusions can be assigned to all four role-types. (For a description of Role exclusions, see "To Assign Resources and Resource Groups" on page 117.)

FIGURE 5–1 The Business Role, IT Role, Application, and Asset Role-Types

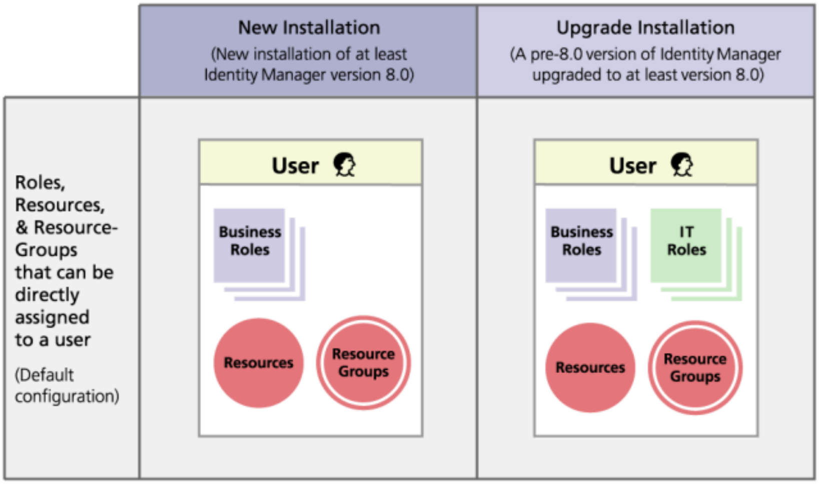


	Business Role	IT Role	Application	Asset
Allowable Role-Type Assignments	IT Roles Applications Assets	IT Roles Applications Assets	None	None
Allowable Resource & Resource Group Assignments	None	Resources Resource Groups	Resources Resource Groups	None
Allowable Role-Type Exclusions	Business Roles IT Roles Applications Assets	Business Roles IT Roles Applications Assets	Business Roles IT Roles Applications Assets	Business Roles IT Roles Applications Assets

Optional, conditional, and required contained-roles ("What are Roles?" on page 109) provide added flexibility. Flexible role definitions can reduce the total number of roles your organization needs to manage.

Figure 5–2 shows that Business Roles and IT Roles are directly assignable to users if a pre-8.0 version of Waveset is upgraded to at least version 8.0. On upgrade, legacy roles are converted to IT Roles, and, to ensure backwards compatibility, IT Roles are directly assigned to users. If Waveset was not upgraded from a pre-8.0 version, then only Business Roles are directly assignable to users.

FIGURE 5–2 Roles and resources that can be directly assigned to users.


New Installation
(New installation of at least Identity Manager version 8.0)
Upgrade Installation
(A pre-8.0 version of Identity Manager upgraded to at least version 8.0)
Roles, Resources, & Resource-Groups that can be directly assigned to a user
(Default configuration)
User
Business Roles
Resources
Resource Groups
User
Business Roles
IT Roles
Resources
Resource Groups

Creating Roles

This section describes how to create roles and the information is organized as follows:

- "To Create Roles Using the Create Role Form" on page 114
- "To Assign Resources and Resource Groups" on page 117
- "To Edit Assigned Resource Attribute Values" on page 118
- "To Assign Roles and Role Exclusions" on page 120
- "Designating Role Owners and Role Approvers" on page 122
- "Designating Notifications" on page 123
- "Initiating Change-Approval and Approval Work Items" on page 124

Note – For tips on designing roles, see "Using Role Types to Design Flexible Roles" on page 111

When you create or edit a role, Waveset 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.

▼ To Create Roles Using the Create Role Form

1. **In the Administrator interface, click Roles in the main menu.**

   The Roles page (List Roles tab) opens.

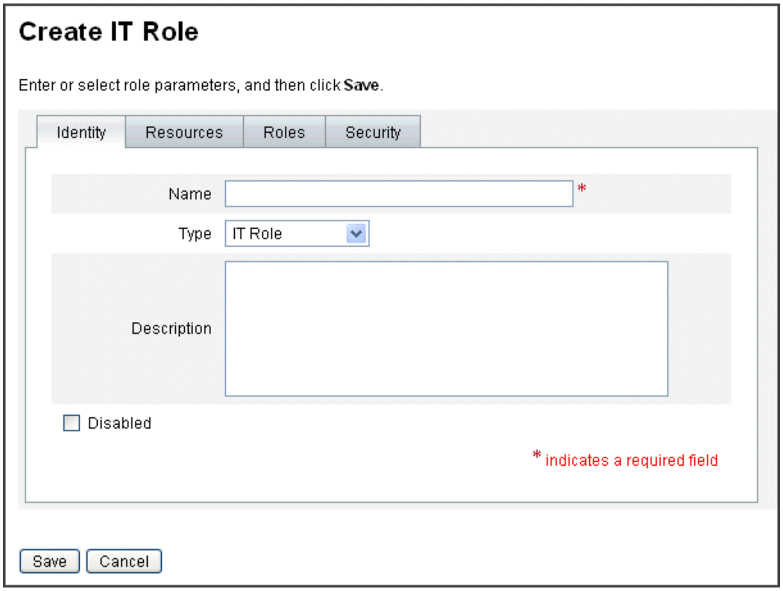
2. **Click New at the bottom of the page.**

   The Create IT Role page opens. To create another type of role, use the Type drop-down menu.

3 **Complete the form fields on the Identity tab.**

The following figure shows the Identity tab.

FIGURE 5–3 Identity Tab on the Create IT Role Page



Create IT Role

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

Name □ *

Type IT Role

Description

□ Disabled

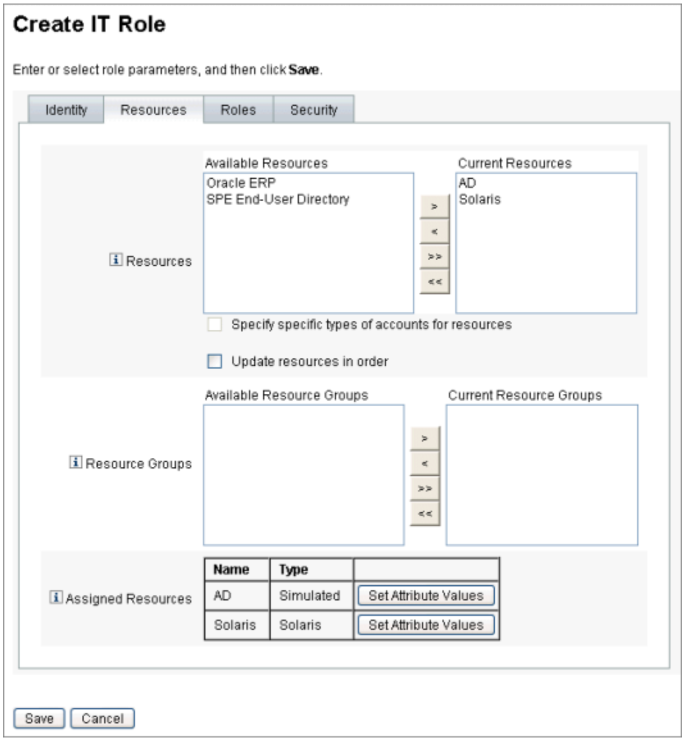
* indicates a required field

4 **Complete the form fields on the Resources tab (if applicable). For help filling out the fields on this tab, refer to online help, and also see “To Assign Resources and Resource Groups” on page 117.**

For help setting extended attributes values on roles, see “To View or Edit Resource Account Attributes” on page 153.

The following figure shows the Resources tab.

FIGURE 5–4 Resources Tab on the Create IT Role Page



Create IT Role

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

Resources

Available Resources: Oracle ERP, SPE End-User Directory

Current Resources: AD, Solaris

□ Specify specific types of accounts for resources

□ Update resources in order

Resource Groups

Available Resource Groups

Current Resource Groups

Assigned Resources

Name	Type	
AD	Simulated	Set Attribute Values
Solaris	Solaris	Set Attribute Values

5. **Complete the form fields on the Roles tab (if applicable). For help filling out the fields on this tab, refer to online help, and also see "To Assign Roles and Role Exclusions" on page 120.**

   Figure 5–6 shows the Roles tab.

6. **Complete the form fields on the Security tab. For help filling out the fields on this tab, refer to online help, and also see "Designating Role Owners and Role Approvers" on page 122 and "Designating Notifications" on page 123.**

   "Designating Role Owners and Role Approvers" on page 122 shows the Security tab.

7. **Click Save at the bottom of the page.**

8. **Enter a role name and description on the Identity tab of the Create Role form. If you are creating a new role, use the Type drop-down menu to select the role-type you are creating.**

   Figure 5–4 shows the Identity portion of the Create Role form's Identity tab. For help using this form, see online help.

▼ To Assign Resources and Resource Groups

Resources and Resource Groups can be directly assigned to IT Roles and Application roles using the Resources tab of the Create Role form. Resources are described later, in the "Understanding and Managing Waveset Resources" on page 144 section. Resource Groups are described in the "Resource Groups" on page 154section.

- Resources and Resource Groups cannot be directly assigned to Business Roles because only roles can be assigned to Business Roles.
- Resources and Resource Groups cannot be assigned to Asset roles because Asset roles are reserved for non-connected or non-digital resources that require manual provisioning.

This procedure describes how to assign resources and resource groups to a role when completing the Create Role form. See "To Create Roles Using the Create Role Form" on page 114 to get started.

1. **Click the Resources tab in the Create Role page.**

2. **To assign a resource, select it in the Available Resources column and move it to the Current Resources column by clicking the arrow buttons.**

3. **If you are assigning multiple resources, you can specify the order in which the resources are updated: Select the Update resources in order checkbox and use the + and - buttons to change the order of the resources in the Current Resources column.**

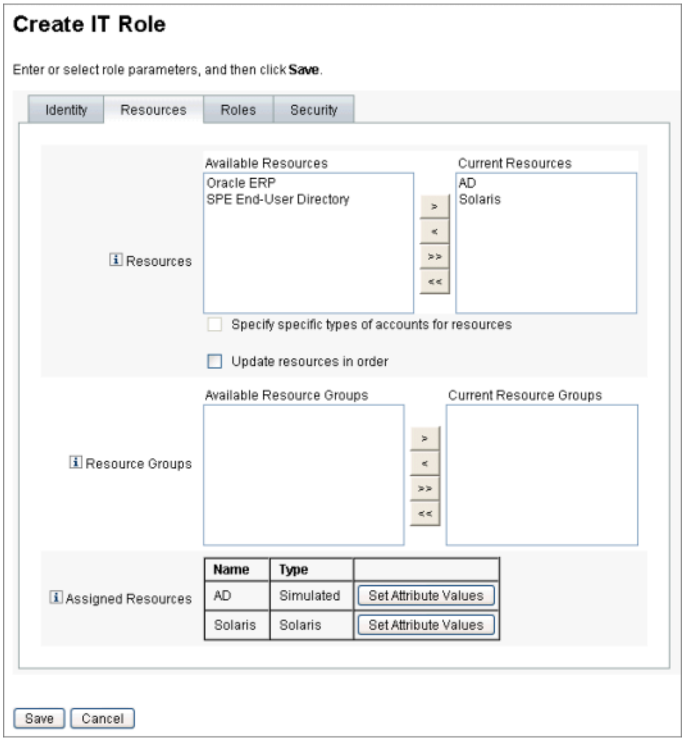
4. **To assign a resource group to this role, select it in the Available Resource Groups column and move it to the Current Resource Groups column by clicking the arrow buttons. A resource group is a collection of resources that provides another way to specify the order in which resource accounts are created and updated.**

5. **To specify account attributes for this role on a per resource basis, click Set Attribute Values in the Assigned Resources section. See "To View or Edit Resource Account Attributes" on page 153 for more information.**

6. **Click Save to save the role, or click the Identity, Roles, or Security tabs to continue with the role creation process.**

   The following figure shows the Create Role form's Resources tab.

FIGURE 5–5 The Resources section of the Create Role Tabbed Form



Create IT Role

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

Available Resources: Oracle ERP, SPE End-User Directory

Current Resources: AD, Solaris

□ Specify specific types of accounts for resources

□ Update resources in order

Available Resource Groups

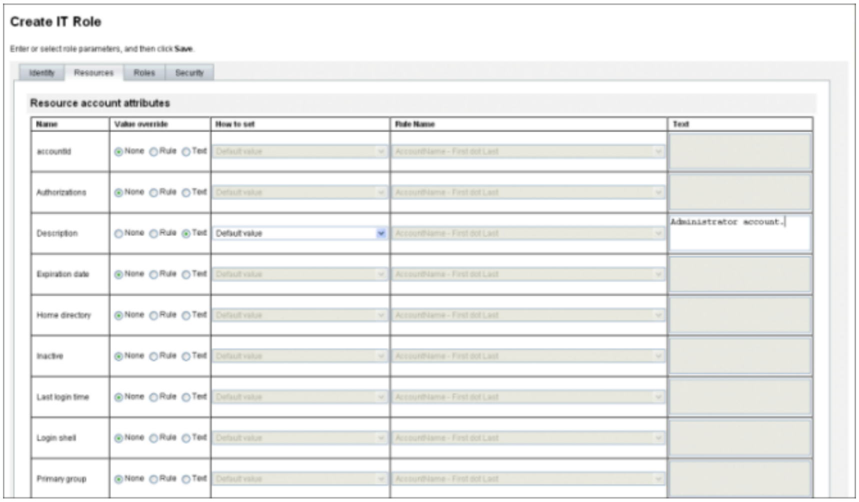
Current Resource Groups

Name	Type	
AD	Simulated	Set Attribute Values
Solaris	Solaris	Set Attribute Values

▼ To Edit Assigned Resource Attribute Values

Use the Assigned Resources table to set or modify resource attribute values on resources assigned to a role. A resource can have different attribute values defined on a role-by-role basis. Clicking the Set Attribute Values button opens the Resource Account Attributes page.

The following figure shows the Resource Account Attributes page, which is used to set extended attribute values on resources assigned to a role.



Create IT Role

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

Resource account attributes

Name	Value override	How to set	Rule Name	Text
accountId	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Authorizations	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Description	○ None ○ Rule ● Text	Default value	AccountName - First dot Last	Administrator account.
Expiration date	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Home directory	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Inactive	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Last login time	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Login shell	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	
Primary group	● None ○ Rule ○ Text	Default value	AccountName - First dot Last	

1. **From the page Resource Account Attributes page, specify new values for each attribute and determine how attribute values are set.**

   Waveset enables you to directly set values or use a rule to set values and provides a range of options for overriding existing values or merging values with existing values. For general information about resource attribute values, see "To View or Edit Resource Account Attributes" on page 153.

   Use the following options to establish values for each resource account attribute:

   - **Value override**. Choose one of the following options:
     - **None** *(Default)*. No value is established.
     - **Rule**. Uses a rule to set the value.

       If you select this option, you must select a rule name from the list.
     - **Text**. Uses specified text to set the value.

       If you select this option, you must enter the text in the adjacent Text field.
   - **How to set**. Choose one of the following options:
     - **Default value**. Makes the rule or text the default attribute value.

       The user can change or override this value.
     - **Set to value**. Sets the attribute value as specified by the rule or text.

       The value will be set and override any user changes.
     - **Merge with value**. Merges the current attribute value with the values specified by the rule or text.
     - **Merge with value, clear existing**. Removes the current attribute values and sets the value to a merger of values specified by this and other assigned roles.

  - **Remove from value**. Removes the value specified by the rule or text from the attribute value.
  - **Authoritative set to value**. Sets the attribute value as specified by the rule or text.

    The value will be set and override any user changes. If you remove the role, the new value is null, even if it previously existed on the attribute.
  - **Authoritative merge with value**. Merges the current attribute value with the values specified by the rule or text.

    Removing the role removes the value that was assigned when the role was assigned and leaves the original attribute value intact.
  - **Authoritative merge with value, clear existing**. Removes the current attribute values and sets the value to a merger of values specified by this and other assigned roles.

    Clears the attribute value specified by this role if the role is removed, even if it previously existed on the attribute.
- **Rule Name**. If you select Rule in the Value override area, select a rule from the list.
- **Text**. If you select Text in the Value override area, enter text to be added to, deleted from, or used as the attribute value.

2 **Click OK to save your changes and return to the Create or Edit Role page.**

▼ To Assign Roles and Role Exclusions

Roles can be assigned to Business Roles and IT Roles using the Roles tab of the Create Role form. Assigned roles should be added to the Contained Roles table.

- Roles cannot be assigned to Application roles and Asset roles.
- Business roles cannot be assigned to any role type.

Role exclusions can be assigned to all four role types using the Roles tab of the Create Role form. If a role with a role exclusion is assigned to a user, the excluded role cannot also be assigned to the user. Role exclusions should be added to the Role Exclusions table.

This procedure describes how to assign one or more roles to a role when completing the Create Role form. See "To Create Roles Using the Create Role Form" on page 114 to get started.

To complete the Roles tab

1 **Click the Roles tab in the Create Role page.**

2 **Click Add in the Contained Roles section.**

The tab refreshes and displays the Find Roles to Contain form.

3 **Search for the role (or roles) that you will be assigning to this role. Start first with any *required* roles. (You will add conditional and optional roles later.)**

See "To Search for Roles" on page 125 for help using the search form. Business Roles cannot be nested or assigned to other role-types.

4 **Use the checkboxes to select one or more roles to be assigned, then click Add.**

The tab refreshes and displays the Add Contained Role form.

5 **Select Required (or Conditional or Optional, as appropriate) from the Association Type drop-down menu.**

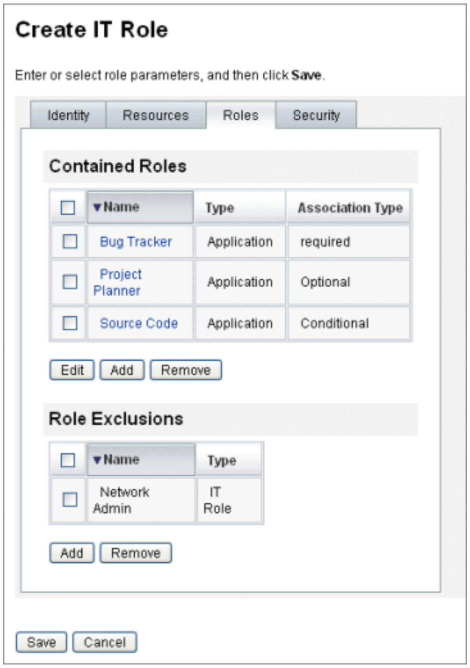
Click OK.

6 **Repeat the previous four steps to add conditional roles (if required). Repeat the previous four steps again to add optional roles (if required).**

7 **Click Save to save the role, or click the Identity, Resources, or Security tabs to continue with the role creation process.**

Figure 5–6 shows the Create Role form's Roles tab. For help using this form, see online help.

FIGURE 5–6 The Roles Portion of the Create Role Tabbed Form



Create IT Role

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

Contained Roles

□	▾Name	Type	Association Type
□	Bug Tracker	Application	required
□	Project Planner	Application	Optional
□	Source Code	Application	Conditional

Role Exclusions

□	▾Name	Type
□	Network Admin	IT Role

Designating Role Owners and Role Approvers

Roles have designated *owners* and *approvers*. Only role owners can authorize changes to the parameters that define the role, and only role approvers can authorize the assignment of the role to end-users.

Note – If you have Waveset integrated with Oracle Role Manager, you should allow Role Manager to handle all role change approvals and notifications by manually disabling Waveset's ability to perform these actions.

You must edit the `RoleConfiguration` configuration object in Waveset as follows:

- Find all instances of `changeApproval` and set the value to **`false`**.
- Find all instances of `changeNotificaiton` and set the value to **`false`**.

To be a role owner is to be the business owner responsible for the underlying resource account rights that are assigned through the role. If an administrator makes changes to a role, a role owner must approve of the changes before they can be carried out. This feature guards against an administrator changing a role without a business owner's knowledge and approval. If change approvals have been disabled in the Role configuration object, however, a role owner's approval is not required in order for changes to be carried out.

In addition to approving role changes, roles cannot be enabled, disabled, or deleted without a role owners' approval.

Owners and approvers can either be directly added to a role, or dynamically added using a role-assignment rule. In Waveset it is possible (but not recommended) to create roles without owners and approvers.

Note – Role-assignment rules have a `RoleUserRule authType`.

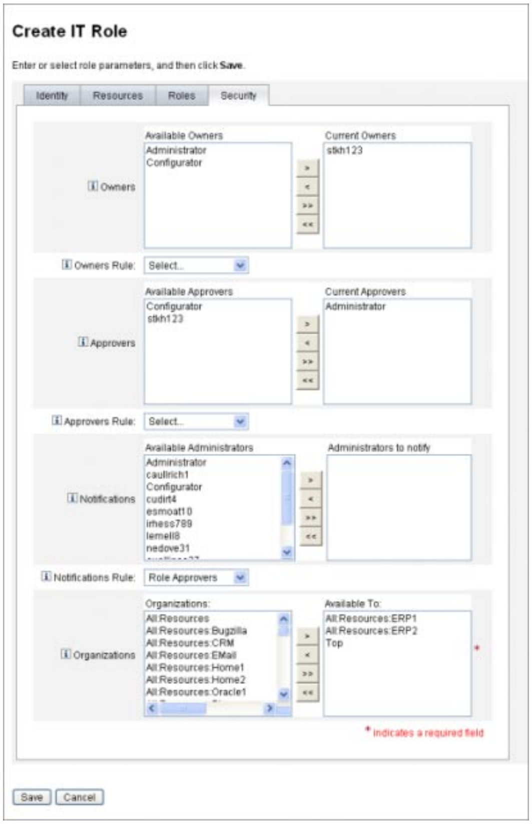
If you need to create a custom role-assignment rule, refer to the three default role-assignment rule objects and use them as an example:

- Role Approvers
- Role Notifications
- Role Owners

Owners and approvers are notified by email if a work item requires their approval. Change-approval work items and approval work items are discussed in the "Initiating Change-Approval and Approval Work Items" on page 124 section.

Owners and approvers are added to roles on the Security tab in the Create Role form.

"Designating Role Owners and Role Approvers" on page 122 shows the Create Role form's Security tab. For help using this form, see the online help.



Create IT Role

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

Owners — Available Owners: Administrator, Configurator; Current Owners: stkh123

Owners Rule: Select...

Approvers — Available Approvers: Configurator, stkh123; Current Approvers: Administrator

Approvers Rule: Select...

Notifications — Available Administrators: Administrator, caullrich1, Configurator, cudirt4, esmoat10, irhess789, lemell8, nedove31; Administrators to notify:

Notifications Rule: Role Approvers

Organizations — Organizations: All:Resources, All:Resources:Bugzilla, All:Resources:CRM, All:Resources:EMail, All:Resources:Home1, All:Resources:Home2, All:Resources:Oracle1; Available To: All:Resources:ERP1, All:Resources:ERP2, Top *

* indicates a required field

Designating Notifications

One or more administrators can be sent notifications when a role is assigned to a user.

Specifying a notification recipient is optional. You could choose to notify an administrator if you decide not to require an approval when a role is assigned to a user. Or you could designate one administrator to serve as an approver, and, another administrator to serve as a notification recipient when the approval is made.

As with owners and approvers, notifications can either be directly added to a role, or dynamically added using a role-assignment rule. Notification recipients are notified by email when a role is assigned to a user. A work item is not created, however, because an approval is not required.

Notifications are assigned to roles on the Security tab on the Create Role form. "Designating Role Owners and Role Approvers" on page 122 shows the Create Role form's Security tab.

Initiating Change-Approval and Approval Work Items

When changes are made to a role, the role owners can receive a *change-approval* email, a *change-notification* email, or no email. When a role is assigned to a user, role approvers receive role *approval* emails.

By default, role owners are sent change-approval emails whenever the roles they own are changed. This behavior is configurable, however, on a role-type by role-type basis. For example, you could choose to enable change-approvals for Business Roles and IT Roles, and enable change-notifications for Application and Asset roles.

For instructions on enabling and disabling change-approval and change-notification email, see "Configuring Role Types" on page 140.

This is how change-approvals and change-notifications work:

- If *change-approvals* are enabled, when an administrator changes a role, a work item is generated and an approval email is sent to the role owner. A role owner must approve the work item in order for the change to be made. Change-approval work items can be delegated. See "Approving User Accounts" on page 217 for more information.

  If change-approvals are disabled, no work item is generated and no change approval email is sent to the role owner.
- If *change-notifications* are enabled, when an administrator changes a role, the change is made immediately, and a notification email is sent to the role owner.

  If change-notifications are disabled, no notifications are sent to the role owner.

When a role is assigned to a user, role approvers receive role *approval* emails. Role approval emails cannot be disabled in Waveset.

For role approvals, when a user is assigned a role, a work item is generated and an approval email is sent to the role approver. A role approver must approve the work item in order for the role to be assigned to the user.

Change-approval and approval work items can be delegated. For more information on delegating work items, see "Delegating Work Items" on page 213.

Editing and Managing Roles

Most role editing and role management tasks can be performed using the Find Roles and List Roles tabs, which are located under the Roles tab in the main menu.

This section contains the following topics:

- "To Search for Roles" on page 125
- "To View Roles" on page 126
- "To Edit a Role" on page 126

- “To Clone a Role” on page 127
- “To Assign a Role to Another Role” on page 127
- “To Remove a Role Assigned to Another Role” on page 128
- “To Enable or Disable Roles” on page 129
- “To Delete a Role” on page 130
- “To Assign a Resource or a Resource Group to a Role” on page 130
- “To Remove a Resource or Resource Group Assigned to a Role” on page 131

▼ To Search for Roles

Use the Find Roles tab to search for roles that meet the search criteria you specify.

Using the Find Roles tab, you can search for roles based on a wide variety of criteria such as role owners and approvers, assigned account types, contained roles, and so on.

For information on finding users assigned to a role, see “To Find Users Assigned to a Specific Role” on page 138.

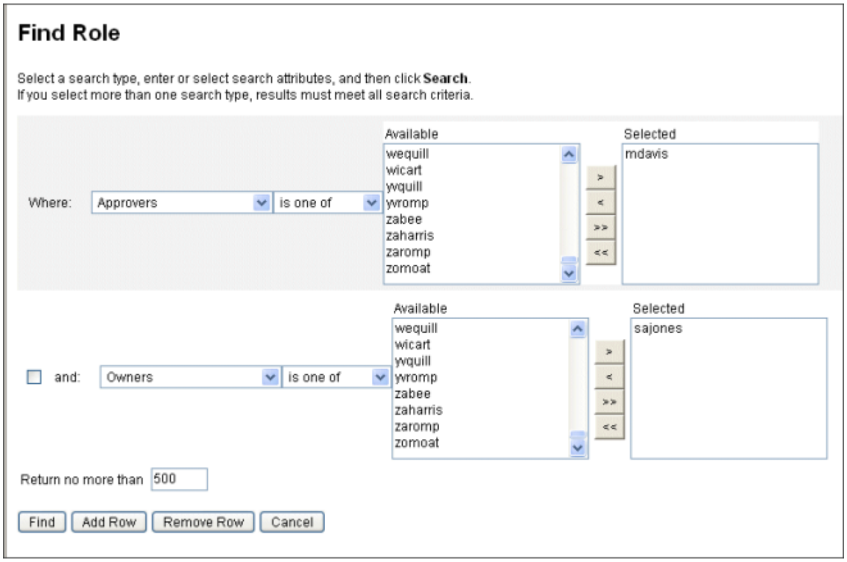
1 **In the Administrator interface, click the Roles tab.**

The List Roles tab opens.

2 **Click the Find Roles secondary tab.**

Figure 5–7 shows the Find Role tab. For help using this form, see online help.

FIGURE 5–7 The Find Role Tab



Find Role

Select a search type, enter or select search attributes, and then click **Search**.
If you select more than one search type, results must meet all search criteria.

Where: Approvers is one of

Available: wequill, wicart, ywquill, ywromp, zabee, zaharris, zaromp, zomoat

Selected: mdavis

□ and: Owners is one of

Available: wequill, wicart, ywquill, ywromp, zabee, zaharris, zaromp, zomoat

Selected: sajones

Return no more than 500

Use the drop-down menus to define the parameters of your search. Click the Add Row button to add additional parameters.

To View Roles

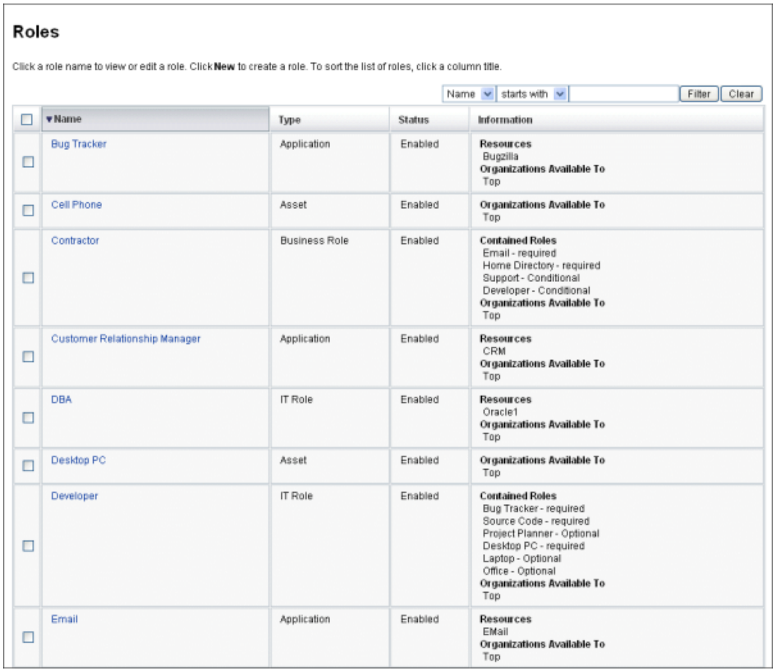
Use the List Roles tab to view roles. Use the filter fields at the top of the List Roles page to find roles by name or role type. Filtering is not case-sensitive.

- **In the Administrator interface, click the Roles tab.**

  The List Roles tab opens.

  Figure 5–8 shows the List Roles tab. For help using this form, see online help.

FIGURE 5–8 The List Roles Tab



Roles

Click a role name to view or edit a role. Click **New** to create a role. To sort the list of roles, click a column title.

□	▾Name	Type	Status	Information
□	Bug Tracker	Application	Enabled	**Resources** Bugzilla **Organizations Available To** Top
□	Cell Phone	Asset	Enabled	**Organizations Available To** Top
□	Contractor	Business Role	Enabled	**Contained Roles** Email - required Home Directory - required Support - Conditional Developer - Conditional **Organizations Available To** Top
□	Customer Relationship Manager	Application	Enabled	**Resources** CRM **Organizations Available To** Top
□	DBA	IT Role	Enabled	**Resources** Oracle1 **Organizations Available To** Top
□	Desktop PC	Asset	Enabled	**Organizations Available To** Top
□	Developer	IT Role	Enabled	**Contained Roles** Bug Tracker - required Source Code - required Project Planner - Optional Desktop PC - required Laptop - Optional Office - Optional **Organizations Available To** Top
□	Email	Application	Enabled	**Resources** EMail **Organizations Available To** Top

To Edit a Role

Search for the role you want to edit using the List Roles or Find Roles tabs. If you make changes to a role, and change approvals are set to true, a role owner must approve your changes before they can be carried out.

For information on updating users with role changes, see "To Update Roles Assigned to Users" on page 134.

1. **Search for the role you want to edit by following the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2. **Click the name of the role you want to edit.**

   The Edit Role page opens.

3. **Edit the role as needed. Refer to the steps in the "To Create Roles Using the Create Role Form" on page 114 section for help completing the Identity, Resources, Roles, and Security tabs.**

   Click Save. The Confirm Role Changes page opens.

4. **If this role is assigned to users, you can select when to update the users with role changes. See "To Update Roles Assigned to Users" on page 134 for more information.**

5. **Click Save to save your changes.**

▼ To Clone a Role

1. **Search for the role you want to edit by following the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2. **Click the name of the role you want to clone.**

   The Edit Role page opens.

3. **Enter a new name in the Name field, and then click Save.**

   The Role: Create or Rename? page opens.

4. **Click Create to make a copy of the role.**

▼ To Assign a Role to Another Role

Waveset's requirements around role assignments are described in "What are Roles?" on page 109 and "Putting Role Types to Work" on page 110. You should understand this information before assigning roles.

Waveset will change a role's role assignments if the role-owner of the parent role approves.

1. **Search for the Business Role or IT Role to which you will be assigning one or more *contained* roles. (Roles can only be assigned to Business Roles and IT Roles.) Use the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126 to search for roles.**

2. **Click the Business Role or IT Role to open it.**

   The Edit Role page opens.

3 **Click the Roles tab in the Edit Role page.**

4 **Click Add in the Contained Roles section.**

The tab refreshes and displays the Find Roles to Contain form.

5 **Search for the role (or roles) that you will be assigning to this role. Start first with any *required* roles. (You will add conditional and optional roles later.)**

See "To Search for Roles" on page 125 for help using the search form. Business Roles cannot be nested or assigned to other role-types.

6 **Use the checkboxes to select one or more roles to be assigned, then click Add.**

The tab refreshes and displays the Add Contained Role form.

7 **Select Required (or Conditional or Optional, as appropriate) from the Association Type drop-down menu.**

Click OK.

8 **Repeat the previous four steps to add conditional roles (if required). Repeat the previous four steps again to add optional roles (if required).**

9 **Click Save to open the Confirm Role Changes page.**

The Confirm Role Changes page opens.

10 **In the Update Assigned Users section select an Update Assigned Users menu option and then click Save to save your role assignments.**

See "To Update Roles Assigned to Users" on page 134 for more information.

▼ To Remove a Role Assigned to Another Role

Waveset will remove a contained role from another role if the role-owner of the parent role approves. The removed role will be removed from users when users receive role updates. (See "To Update Roles Assigned to Users" on page 134 for more information.) When the role is removed, users lose the entitlements that were bestowed by the role.

- For information about removing a role assigned to one or more users, see "To Remove One or More Roles From a User" on page 139.
- For information about disabling a role, see "To Enable or Disable Roles" on page 129.
- For information about deleting a role from Waveset, see "To Delete a Role" on page 130.

1 **Search for the Business Role or IT Role from which you want to remove a role. Use the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126 to search for roles.**

2 **Click the role to open it.**

The Edit Role page opens.

3 **Click the Roles tab in the Edit Role page.**

4 **In the Contained Roles section, select the checkbox next to the role that you want to remove, then click Remove. Select multiple checkboxes to remove multiple roles.**

The table updates to show the remaining contained roles.

5 **Click Save.**

The Confirm Role Changes page opens.

6 **In the Update Assigned Users section select an Update Assigned Users menu option. See "To Update Roles Assigned to Users" on page 134 for more information.**

7 **Click Save to finalize your changes.**

▼ To Enable or Disable Roles

Roles can be enabled and disabled on the List Roles tab. Role status is displayed in the Status column. Click the Status column header to sort the table by role status.

Disabled roles do not appear on the Roles tab in the Create/Edit user form and cannot be directly assigned to users. Roles that contain disabled roles can be assigned to users, but the disabled roles cannot be assigned.

Users who are assigned roles that are later disabled do not lose their entitlements. Role disablement only blocks *future role assignments* from occurring.

Disabling and re-enabling a role requires the permission of the role owner.

Upon enabling or disabling a role with assigned users, Waveset will prompt you to update these users. For more information, see "To Update Roles Assigned to Users" on page 134.

1 **Search for the role you want to delete by following the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2 **Click the checkboxes next to the roles that need to be enabled or disabled.**

3 **Click Enable or Disable at the bottom of the Roles table.**

The Enable Role or Disable Role confirmation page opens.

4 **Click OK to enable or disable the role.**

▼ To Delete a Role

This section describes the procedure for deleting a role from Waveset.

- For information on removing a role assigned to another role, see "To Remove a Role Assigned to Another Role" on page 128.
- For information on removing a role assigned to one or more users, see "To Remove One or More Roles From a User" on page 139.

If you delete a role that is currently assigned to a user, Waveset blocks the deletion when you try to save the role. You must unassign (or reassign) all users assigned to a role before Waveset can delete it. You also must remove the role from any other roles.

Waveset requires a role owner's approval before it will delete a role.

1 **Search for the role you want to delete by following the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2 **Select the checkbox next to each role that you want to delete.**

3 **Click Delete.**

The Delete Role confirmation page displays.

4 **Click OK to delete one or more of the roles.**

▼ To Assign a Resource or a Resource Group to a Role

Waveset's requirements around resource and resource group assignments are described in "What are Roles?" on page 109 and "Putting Role Types to Work" on page 110. You should understand this information before assigning resources to roles.

Waveset will change a role's resource and resource group assignments if the role-owner approves.

1 **Search for the IT Role or Application to which you want to add a resource or resource group. For instructions on how to search for a role, see "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2 **Click the role to open it.**

3 **Click the Resources tab in the Edit Role page.**

4 **To assign a resource, select it in the Available Resources column and move it to the Current Resources column by clicking the arrow buttons.**

5 **If you are assigning multiple resources, you can specify the order in which the resources are updated: Select the Update resources in order checkbox and use the + and - buttons to change the order of the resources in the Current Resources column.**

6 **To assign a resource group to this role, select it in the Available Resource Groups column and move it to the Current Resource Groups column by clicking the arrow buttons. A resource group is a collection of resources that provides another way to specify the order in which resource accounts are created and updated.**

7 **To specify account attributes for this role on a per resource basis, click Set Attribute Values in the Assigned Resources section. See "To View or Edit Resource Account Attributes" on page 153 for more information.**

8 **Click Save to open the Confirm Role Changes page.**

The Confirm Role Changes page opens.

9 **In the Update Assigned Users section select an Update Assigned Users menu option. See "To Update Roles Assigned to Users" on page 134 for more information.**

10 **Click Save to save your resource assignments.**

▼ To Remove a Resource or Resource Group Assigned to a Role

Waveset will remove a resource or resource group from a role if the role-owner approves. The removed resource will be removed from users when users receive role updates. (See "To Update Roles Assigned to Users" on page 134 for more information.) When the resource is removed, users lose their entitlements on that resource unless the resource is also directly assigned to the user.

1 **Search for the IT Role or Application from which you want to remove a resource or resource group. Use the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126 to search for roles.**

2 **Click the role to open it.**

The Edit Role page opens.

3 **Click the Resources tab in the Edit Role page.**

4 **To remove a resource, select it in the Current Resources column and move it to the Available Resources column by clicking the arrow buttons.**

To remove a resource group, select it in the Current Resource Groups column and move it to the Available Resource Groups column by clicking the arrow buttons.

5 **Click Save.**

The Confirm Role Changes page opens.

6 **In the Update Assigned Users section select an Update Assigned Users menu option. See "To Update Roles Assigned to Users" on page 134 for more information.**

7 **Click Save to finalize your changes.**

Managing User Role Assignments

Roles are assigned to users in the Accounts area of Waveset.

▼ To Assign Roles to a User

Use the following procedure to assign one or more roles to a user (or users).

End-users can also make role assignment requests for themselves. (Only optional roles where the parent role is already assigned to the user can be requested.) See "Requests Tab" on page 39 in the "Waveset End-User Interface" on page 38 section for information on how end-users can request available roles.

1 **In the Administrator interface, click the Accounts tab.**

The List Accounts subtab opens.

2 **To assign a role to an existing user, follow these steps:**

a. **Click the user's name in the User List.**

b. **Click the Roles tab.**

c. **Click Add to add one or more roles to the user account.**

By default, only Business Roles can be directly assigned to users. (If your installation of Waveset was upgraded from a pre-8.0 version, both Business Roles and IT Roles can be directly assigned to users.)

d. **In the table of roles, select the roles you want to assign to the user and then click OK.**

To sort the table alphabetically by Name, Type, or Description, click the column headers. Click a second time to reverse sort. To filter the list by role type, make a selection from the Current drop-down menu.

The table updates to show the selected role assignments, plus any required role assignments that are connected to the parent role assignments.

e. **Click Add to view optional role assignments that can also be assigned to the user.**

   Select the optional roles to be assigned to the user and click OK.

f. **(Optional) In the Activate On column, select the date that the role should become active. If you do not specify a date, the role assignment will become active as soon as a designated role approver approves the role assignment.**

   To make the role assignment temporary, select the date that the role should become inactive in the Deactivate On column. Role deactivation takes effect at the beginning of the selected day.

   See "To Activate and Deactivate Roles on Specific Dates" on page 133 for more information.

g. **Click Save.**

To Activate and Deactivate Roles on Specific Dates

When assigning a role to a user, you can specify an activate date and a deactivate date. Role-assignment work-item requests are created when the assignment is made. If a role assignment is not approved by the scheduled activation date, however, the role is not assigned. Role activations and deactivations take place a little after midnight (12:01 AM) on the date scheduled.

By default, only Business Roles can have activate dates and deactivate dates. All other role-types inherit the activate date and deactivate date of the Business Role that is directly assigned to the user. Waveset can be configured to allow other role types to have directly assignable activate and deactivate dates. For instructions, see "Configuring Role Types" on page 140.

▼ To Edit the Schedule for the Deferred Task Scanner

The Deferred Task Scanner scans user role assignments and activates and deactivates roles as needed. By default, the Deferred Task Scanner task runs every hour.

1 **In the Administrator interface, click Server Tasks.**

2 **Click Manage Schedule in the secondary menu.**

3 **In the Tasks Available For Scheduling section, click on the Deferred Task Scanner TaskDefinition.**

  The "Create New Deferred Task Scanner Task Schedule" page opens.

4 **Complete the form. For help, refer to the i-Helps and online help.**

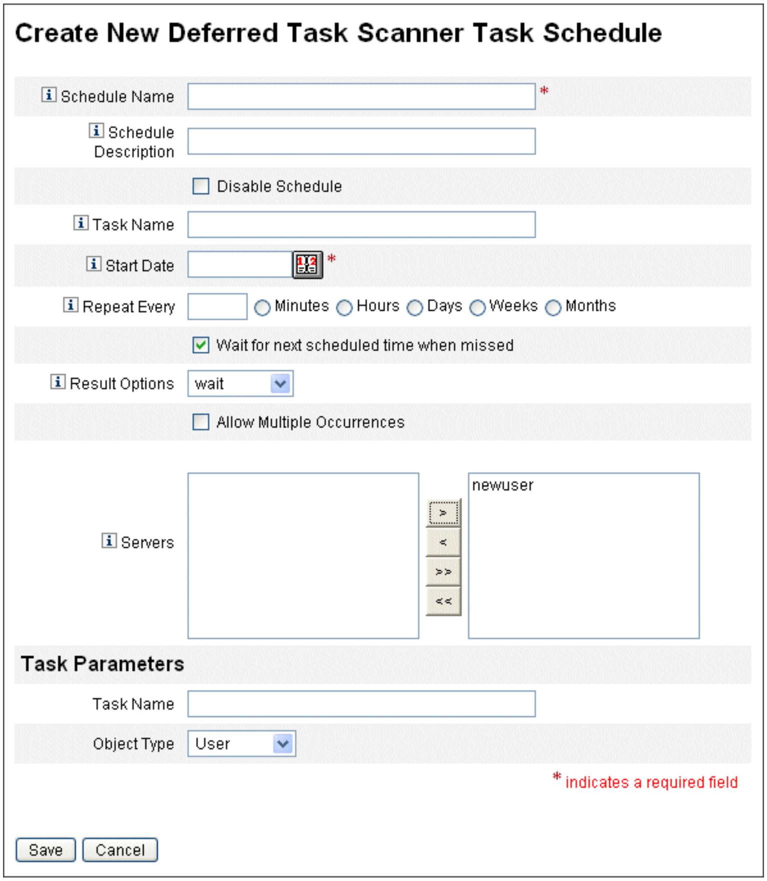
  To specify a date and time when the task should run, in Start Date use the format `mm/dd/yyyy hh:mm:ss`. For example, to schedule a task to start running at 7:00 P.M. on September 29, 2008, type `09/29/2008 19:00:00`.

In the Result Options drop-down menu, select rename. If you select wait, future instances of this task will not run until you remove the previous results. See online help for more information on the various Result Options settings.

5 **Click Save to save the task.**

Figure 5–9 shows the scheduled task form for the Deferred Task Scanner task.

FIGURE 5–9 The Deferred Task Scanner Scheduled Task Form



Create New Deferred Task Scanner Task Schedule

Schedule Name: ____ *

Schedule Description: ____

□ Disable Schedule

Task Name: ____

Start Date: ____ *

Repeat Every: ____ ○ Minutes ○ Hours ○ Days ○ Weeks ○ Months

☑ Wait for next scheduled time when missed

Result Options: wait

□ Allow Multiple Occurrences

Servers: newuser

Task Parameters

Task Name: ____

Object Type: User

* indicates a required field

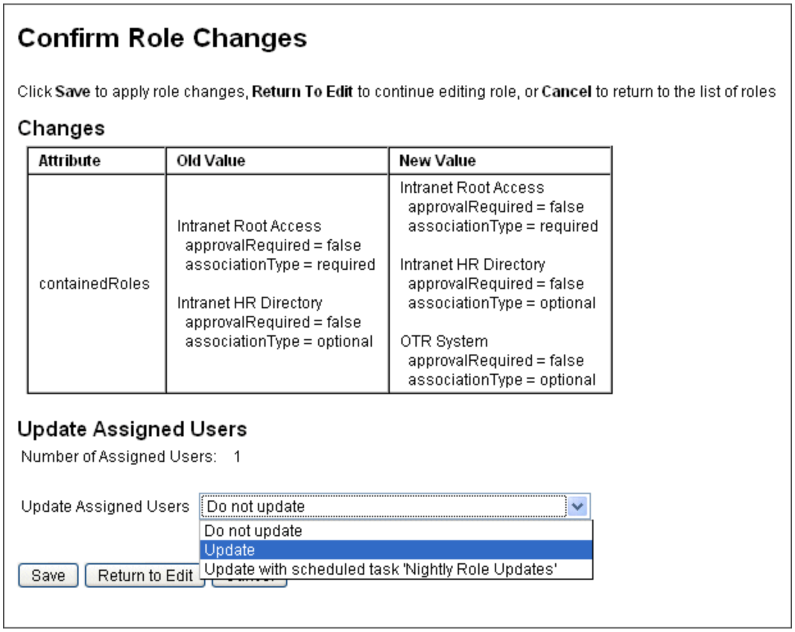
To Update Roles Assigned to Users

When editing roles assigned to users you can choose to update users with the new role changes immediately, or defer the update to run during a scheduled maintenance window.

Upon making changes to a role, the Confirm Role Changes page opens. The Confirm Roles Changes page is shown in "To Update Roles Assigned to Users" on page 134.

- The Update Assigned Users section of this page displays the number of users who currently have the role assigned.
- Use the Update Assigned Users menu to select whether to immediately update users with the new role changes (Update), to defer updating users until a later time (Do not update), or to select a custom scheduled update task.
  - Because Update updates users immediately, you should avoid choosing this option if a large number of users will be affected. Updating users can be time and resource-intensive. If many users need to be updated, it is preferable to schedule the update for off-peak hours.
  - When Do not update is selected for a role, users assigned to the role will not receive role updates until an administrator views the user's user profile or until the user is updated by the Update Role Users task. For information on scheduling the Update Role Users task, see the next section.
  - If you have created an Update Role Users task schedule, you can select it from the menu. The selected Update Role Users task will update users assigned to the role according to the schedule defined for the task. See the next section for more information.

    "To Update Roles Assigned to Users" on page 134 shows the Confirm Role Changes page. The Update Assigned Users section displays the number of users who currently have this role assigned. The Update Assigned Users drop-down menu has two default options: Do not update and Update. You can also select from a list of scheduled Update Role Users tasks. For instructions on creating scheduled Update Role Users tasks, see "To Schedule an Update Role Users Task" on page 137.



Confirm Role Changes

Click **Save** to apply role changes, **Return To Edit** to continue editing role, or **Cancel** to return to the list of roles

Changes

Attribute	Old Value	New Value

containedRoles	Intranet Root Access
	approvalRequired = false
	associationType = required
	
	Intranet HR Directory
	approvalRequired = false
	associationType = optional
		Intranet Root Access
		approvalRequired = false
		associationType = required
		
		Intranet HR Directory
		approvalRequired = false
		associationType = optional
		
		OTR System
		approvalRequired = false
		associationType = optional

Update Assigned Users

Number of Assigned Users: 1

Update Assigned Users: Do not update

▼ To Manually Update Assigned Users

You can update users assigned to roles by selecting one or more roles and clicking the Update Assigned Users button. This procedure runs an instance of the Update Role Users Task for the roles specified.

1 **Search for the role (or roles) whose assigned users should be updated by following the instructions on "To Search for Roles" on page 125 or "To View Roles" on page 126.**

2 **Select the role (or roles) using the checkboxes.**

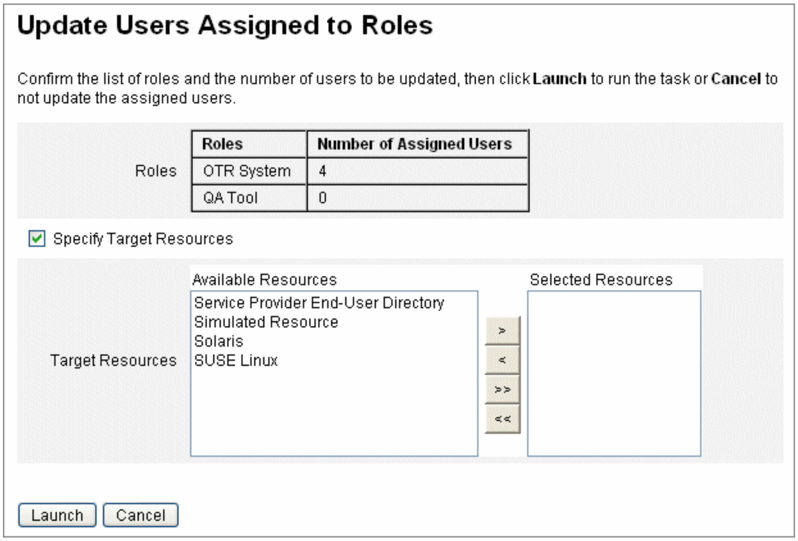
3 **Click Update Assigned Users.**

The Update Users Assigned to Roles page (Figure 5–10) displays.

4 **Click Launch to start the update.**

5 **Check the status of the Update Role Users task by clicking Server Tasks in the main menu, then click All Tasks in the secondary menu.**

FIGURE 5–10 The Update Users Assigned to Roles Page



Update Users Assigned to Roles

Confirm the list of roles and the number of users to be updated, then click **Launch** to run the task or **Cancel** to not update the assigned users.

Roles

Roles	Number of Assigned Users
OTR System	4
QA Tool	0

☑ Specify Target Resources

Target Resources

Available Resources:
Service Provider End-User Directory
Simulated Resource
Solaris
SUSE Linux

Selected Resources:

▼ To Schedule an Update Role Users Task

Note – You should schedule an Update Role Users task to run on a regular basis.

Schedule the update Role Users task to update users with outstanding role changes as follows:

1 **In the Administrator interface, click Server Tasks.**

2 **Click Manage Schedule in the secondary menu.**

3 **In the Tasks Available For Scheduling section, click on the Update Role Users TaskDefinition.**

The “Create New Update Role Users Task Schedule” page opens, or, if you are editing an existing task, the “Edit Task Schedule” page opens (Figure 5–11).

4 **Complete the form. For help, refer to the i-Helps and online help.**

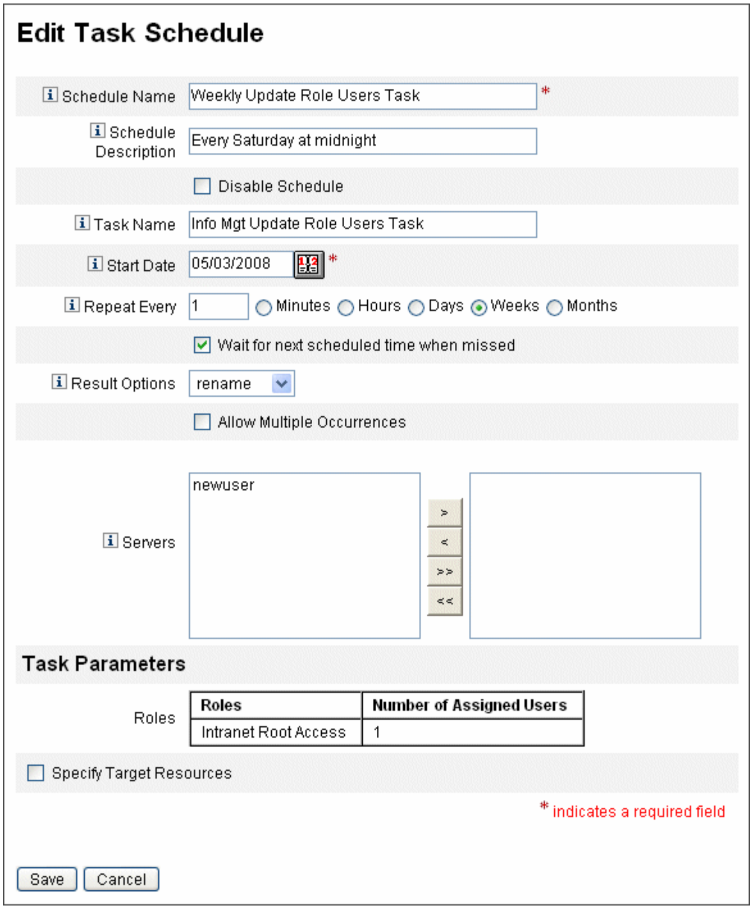
To specify a date and time when the task should run, in Start Date use the format `mm/dd/yyyy hh:mm:ss`. For example, to schedule a task to start running at 7:00 P.M. on September 29, 2008, type `09/29/2008 19:00:00`.

In the Result Options drop-down menu, select rename. If you select wait, future instances of this task will not run until you remove the previous results. See online help for more information on the various Result Options settings.

5 **Click Save to save the task.**

Figure 5–11 shows the scheduled task form for the Update Role Users task. Specific roles can be assigned to specific Update Role Users tasks (as shown in the Task Parameters section.) See "To Update Roles Assigned to Users" on page 134 for more information.

FIGURE 5–11 The Update Role Users Scheduled Task Form



Edit Task Schedule

Schedule Name: Weekly Update Role Users Task *

Schedule Description: Every Saturday at midnight

□ Disable Schedule

Task Name: Info Mgt Update Role Users Task

Start Date: 05/03/2008 *

Repeat Every: 1 ○ Minutes ○ Hours ○ Days ● Weeks ○ Months

☑ Wait for next scheduled time when missed

Result Options: rename

□ Allow Multiple Occurrences

Servers: newuser

Task Parameters

Roles

Roles	Number of Assigned Users
Intranet Root Access	1

□ Specify Target Resources

* indicates a required field

▼ To Find Users Assigned to a Specific Role

You can search for users who have a specific role assigned.

1 **In the Administrator interface, click Accounts.**

2 **Click Find Users in the secondary menu. The Find Users page opens.**

3 **Locate the search type User has [Select Role Type] role assigned.**

4 **Select the option box and use the Select Role Type drop-down menu to filter the list of available roles.**

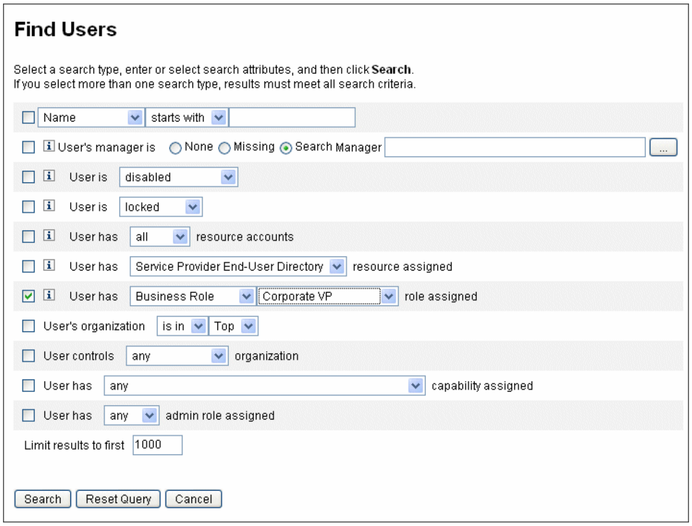
A second role menu opens.

5 **Select a role.**

6 **Clear the other search-type checkboxes, unless you want to narrow your search further.**

7 **Click Search.**

FIGURE 5–12 Searching for users assigned a role using the Find Users page



Find Users

Select a search type, enter or select search attributes, and then click **Search**.
If you select more than one search type, results must meet all search criteria.

☐ Name ▾ starts with ▾

☐ User's manager is ○ None ○ Missing ● Search Manager [...]

☐ User is disabled ▾

☐ User is locked ▾

☐ User has all ▾ resource accounts

☐ User has Service Provider End-User Directory ▾ resource assigned

☑ User has Business Role ▾ Corporate VP ▾ role assigned

☐ User's organization is in ▾ Top ▾

☐ User controls any ▾ organization

☐ User has any ▾ capability assigned

☐ User has any ▾ admin role assigned

Limit results to first 1000

To Remove One or More Roles From a User

Using the Edit User page, one or more roles can be removed from a user account. Only a directly assigned role can be removed. Indirectly assigned roles (that is, conditional and/or required *contained roles*) are removed when the parent role is removed. Another way for an indirectly assigned role to be removed from a user is if the role is removed from the parent role (see "To Remove a Role Assigned to Another Role" on page 128).

End-users can also request that assigned roles be removed from their user accounts. See "Requests Tab" on page 39 in the "Waveset End-User Interface" on page 38 section.

For information on removing a role using a scheduled deactivation date, see "To Activate and Deactivate Roles on Specific Dates" on page 133.

1 **In the Administrator interface, click the Accounts tab.**

The List Accounts subtab opens.

2 **Click the user from which you want to remove a rule (or rules).**

The Edit User page opens.

3 **Click the Roles tab.**

4 **In the table of roles, select the roles you want to remove from the user and then click OK.**

To sort the table alphabetically by Name, Type, Activate On, Deactivate On, Assigned By, or Status, click the column headers. Click a second time to reverse sort. To filter the list by role type, make a selection from the Current drop-down menu.

The table shows the parent role assignments (those roles that can be selected), plus any role assignments that are connected to the parent role assignments (those roles that cannot be selected).

5 **Click Remove.**

The table of assigned roles updates to show the remaining assigned roles.

6 **Click Save.**

The Update Resource Accounts page opens. Deselect any resource accounts that you do not want removed.

7 **Click Save to save your changes.**

Configuring Role Types

Role Type functionality can be modified by editing the Role configuration object.

▼ To Configure Role Types to be Directly Assignable to Users

By default, only certain role types can be directly assigned to users. To change these settings, use the following steps.

Note – It is a recommended best practice that you only directly assign Business Roles to users. See "Using Role Types to Design Flexible Roles" on page 111 for more information.

To change which role types can be directly assigned to users, follow these steps:

1 **Open the Role configuration object for editing using the steps in "Editing Waveset Configuration Objects" on page 108.**

2 **Locate the role object that corresponds to the role type that you want to edit.**

- To edit the IT Role, locate `Object name=’ITRole’`
- To edit the Application Role, locate `Object name=’ApplicationRole’`
- To edit the Asset Role, locate `Object name=’AssetRole’`

3 **Specify a set of instructions to update your configuration.**

Depending on how you want to update your configuration, choose one of the following:

- To modify a role type so that it can be directly assigned to a user, locate the following `userAssignment` attribute inside the role object:

```
<Attribute name=’userAssignment’>
        <Object/>
    </Attribute>
```

  And replace it with the following:

```
<Attribute name=’userAssignment’>
        <Object>
            <Attribute name=’manual’ value=’true’/>
         </Object>
    </Attribute>
```

- To modify a role type so that it cannot be directly assigned to a user, locate the `userAssignment` attribute inside the role object and delete the `manual` attribute as follows:

```
<Attribute name=’userAssignment’>
        <Object>
        </Object>
    </Attribute>
```

4 **Save the Role configuration object. You do not need to restart your application servers in order for the changes to take effect.**

▼ To Enable Role Types for Assignable Activation Dates and Deactivation Dates

By default, only Business Roles can have activate dates and deactivate dates that can be specified when roles are assigned. All other roles will inherit the activate date or deactivate date of the Business Role that is directly assigned to the user.

Note – It is a recommended best practice that you only directly assign Business Roles to users. See “Using Role Types to Design Flexible Roles” on page 111 for more information.

If you opt to allow another role type to be directly assignable to users (for example, the IT Role type), you may also want to be able to assign activate and deactivate dates for that role type.

Use the following steps to change which role types can have assignable activate dates and deactivate dates:

1. **Open the Role configuration object for editing using the steps in "Editing Waveset Configuration Objects" on page 108.**

2. **Locate the role object that corresponds to the role type that you want to edit.**

   - To edit the Business Role, locate `Object name='BusinessRole'`
   - To edit the IT Role, locate `Object name='ITRole'`
   - To edit the Application Role, locate `Object name='ApplicationRole'`
   - To edit the Asset Role, locate `Object name='AssetRole'`

3. **Specify a set of instructions to update your configuration.**

   Depending on how you want to update your configuration, choose one of the following:

   - To modify a role type so that it can have directly assignable activate dates and deactivate dates, locate the following `userAssignment` attribute inside the role object:

     ```
     <Attribute name='userAssignment'>
             <Attribute name='manual' value='true'/>
          </Attribute>
     ```

     And replace it with the following:

     ```
     <Attribute name='userAssignment'>
             <Object>
                 <Attribute name='activateDate' value='true'/>
                  <Attribute name='deactivateDate' value='true'/>
                  <Attribute name='manual' value='true'/>
             </Object>
         </Attribute>
     ```

   - To modify a role type so that it cannot have directly assignable activate dates and deactivate dates, locate the `userAssignment` attribute inside the role object and delete the `activateDate` and `deactivateDate` attributes as follows:

     ```
     <Attribute name='userAssignment'>
             <Object>
             </Object>
         </Attribute>
     ```

4. **Save the Role configuration object. You do not need to restart your application servers in order for the changes to take effect.**

▼ To Enable or Disable Change-Approval and Change-Notification Work Items

By default, change-approval work items are enabled for all role types. This means that every time a role is changed (whether it is a Business Role, an IT Role, an Application, or an Asset), if the role has an owner, the owner must approve the change in order for the change to be made.

For more information on change-approval and change-notification work items, see "Initiating Change-Approval and Approval Work Items" on page 124.

Use the following steps to enable or disable change-approval and change-notification work items for role types, follow these steps:

1 **Open the Role configuration object for editing using the steps in "Editing Waveset Configuration Objects" on page 108.**

2 **Locate the role object that corresponds to the role type that you want to edit.**

- To edit the Business Role, locate `Object name='BusinessRole'`
- To edit the IT Role, locate `Object name='ITRole'`
- To edit the Application Role, locate `Object name='ApplicationRole'`
- To edit the Asset Role, locate `Object name='AssetRole'`

3 **Locate the following attributes located in the `<Object>` element, which is located in the `<Attribute name='features'>` element:**

```
<Attribute name='changeApproval' value='true'/>
 <Attribute name='changeNotification' value='true'/>
```

4 **Set the attribute values to true or false as needed.**

5 **If necessary, repeat steps 2 - 4 to configure another role type.**

6 **Save the Role configuration object. You do not need to restart your application servers in order for the changes to take effect.**

▼ To Configure the Maximum Number of Rows that the Role List Page Can Load

The List Roles page in the Administrator interface can display a configurable maximum number of rows. The default number is 500. Use the steps in the section to change the number.

Use the following steps to change the maximum number of rows that the List Roles page can display.

1 **Open the Role configuration object for editing using the steps in "Editing Waveset Configuration Objects" on page 108.**

2 **Locate the following attribute and change the value:**

```
<Attribute name='roleListMaxRows' value='500'/>
```

3 **Save the Role configuration object. You do not need to restart your application servers in order for the changes to take effect.**

Synchronizing Waveset Roles and Resource Roles

You can synchronize Waveset 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 synchronization task, as well as existing Waveset roles that match one of the resource role names.

▼ To Synchronize an Waveset Role with a Resource Role

1. **In the Administrator interface, click Server Tasks in the main menu.**
2. **Click Run Tasks. The Available Tasks page opens.**
3. **Click the Synchronize Identity System Roles with Resource Roles task.**
4. **Complete the form. Click Help for more information.**
5. **Click Launch.**

Understanding and Managing Waveset Resources

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

What are Resources?

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

Waveset 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

The Resources Area in the Interface

Waveset displays information about existing resources on the Resources page.

To access resources, select Resources on the menu bar.

Resources in the resource list are grouped by type. Each resource type is represented by a folder icon. To 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 the following:

- 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, Waveset 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

Before you can create a new resource, you have to tell Waveset which resource types you want to be able to manage. To enable resources and create custom resources, use the Configure Managed Resources page.

▼ To Open the Configure Managed Resources Page

Use the following steps to open the Configure Managed Resources page.

1. **Log in to the Administrator interface.**

2. **Click the Resources tab.**

Use one of the following methods to open the Configure Managed Resources page:

- Locate the Resource Type Actions drop-down list and choose Configure Managed Resources.
- Click the Configure Types tab.

The Configure Managed Resources page opens.

This page has three sections:

- **Resource Connectors**. This section lists resource connector types, the connector version, and connector server.
- **Resource Adapters**. This section lists resource types that are commonly found in large enterprise environments. The version of the Waveset adapter that connects to the resource is listed in the Version column.
- **Custom Resource Adapters**. This section is used to add custom resources to the Resources list.

▼ To Enable Resource Types

You can enable a resource type from the Configure Managed Resources page by using the following steps.

1 **Open the Configure Managed Resources page if it is not already open ("Managing the Resources List" on page 145).**

2 **In the Resources section, select the box in the Managed? column for the resource type that you want to enable.**

To enable all of the listed resource types, select Manage all resources.

3 **Click Save at the bottom of the page.**

The resource is added to the Resources list.

▼ To Add a Custom Resource

You can add a custom resource from the Configure Managed Resources page by using the following steps.

1 **Open the Configure Managed Resources page if it is not already open ("Managing the Resources List" on page 145).**

2 **In the Custom Resources section, click Add Custom Resource to add a row to the table.**

3 **Enter the resource class path for the resource, or enter your custom-developed resource. For adapters provided with Waveset, see the***Oracle Waveset 8.1.1 Resources Reference* **for the full class path.**

4 **Click Save to add the resource to the Resources list.**

▼ To Create a Resource

Once a resource type is enabled, you can then create an instance of that resource in Waveset. To create a resource, use the *Resource Wizard*.

The Resource Wizard will guide you in setting up the following items:

- **Resource-specific parameters**. You can modify these values from the Waveset interface when creating a specific instance of this resource type.
- **Account attributes**. Defined in the schema map for the resource. These determine how Waveset 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.
- **Waveset parameters for the resource**. Sets up policies, establishes resource approvers, and sets up organization access to the resource.

1 **Log in to the Administrator interface.**

2 **Click the Resources tab. Verify that the List Resources subtab is selected.**

3 **Locate the Resource Type Actions drop-down list and select New Resource.**

The "New Resource" page opens.

4 **Select a resource type from the drop-down list. (If the resource type you are looking for is not listed, you need to enable it. See "Managing the Resources List" on page 145.)**

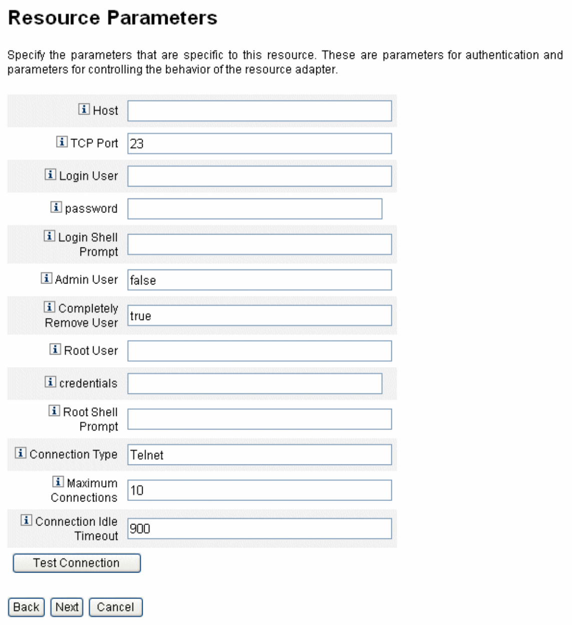
5 **Click New to display the Resource Wizard Welcome page.**

6 **Click Next to begin defining the resource.**

The Resource Wizard steps and pages display in the following 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.

  The following figure shows the Resource Parameters page for Solaris resources. The form fields on this page are different for different resources.



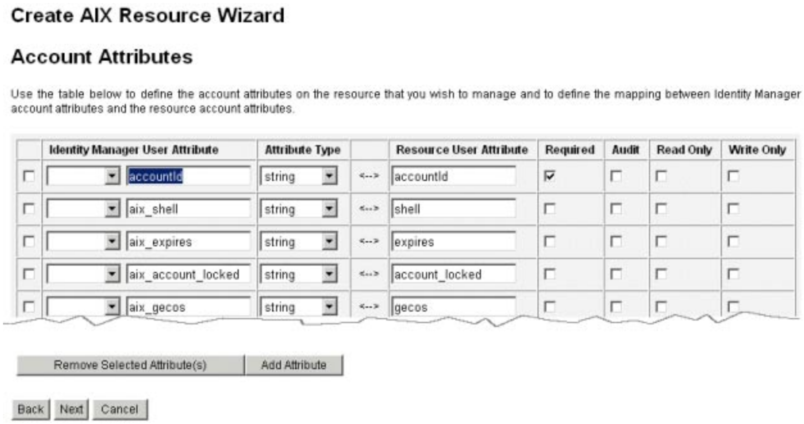
Resource Parameters

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

- **Account Attributes** *(schema map)*. Maps Waveset account attributes to resource account attributes. For more information about resource account attributes, see "To View or Edit Resource Account Attributes" on page 153.
  - To add an attribute, click Add Attribute.
  - To remove one or more attributes, select the boxes next to the attribute and click Remove Selected Attributes.

    The next figure shows the Account Attributes page in the Resource Wizard.



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	□	□	□	□

Note – If you want to export attributes to the `EXT_RESOURCEACCOUNT_ACCTATTR` table, you must check the Audit box for each attribute to be exported.

When you are finished, click Next to set up the Identity Template.

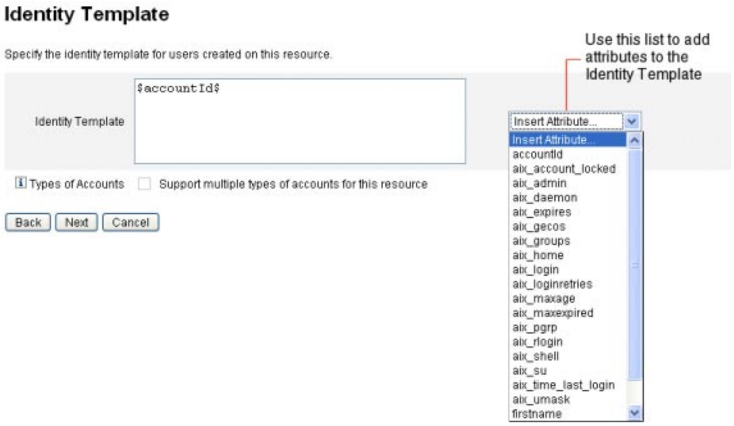
- **Identity Template**. Defines account name syntax for users. This feature is particularly important for hierarchical namespaces.
  - To add an attribute to the template, select it from the Insert Attribute list.
  - To delete an attribute, highlight it in the string and use the delete key on your keyboard. Delete the attribute name, as well as the preceding and following `$` (dollar sign) characters.
  - **Type of accounts**. Waveset provides the ability to assign multiple resource accounts to a single user. For example, a user may require an administrator-level account as well as a regular user account on a particular resource. To support multiple account types on this resource, select the Type of accounts check box.

    Note – You cannot select the Type of accounts check box if you have not created one or more Identity Generation rules identified by the subtype `IdentityRule`. Because accountIds must be distinct, different types of accounts must generate different accountIds for a given user. Identity Generation rules specify how these unique accountIds should be created.

    Sample identity rules are provided in `sample/identityRules.xml`.

    You cannot remove an account type until it is no longer referenced by other objects within Waveset. Also, you cannot rename an account type.

For more information about completing the Type of accounts form, see the Wavesetonline Help. For more information about creating multiple resource accounts for a user, see "Creating Multiple Resource Accounts for a User" on page 56.



Identity Template

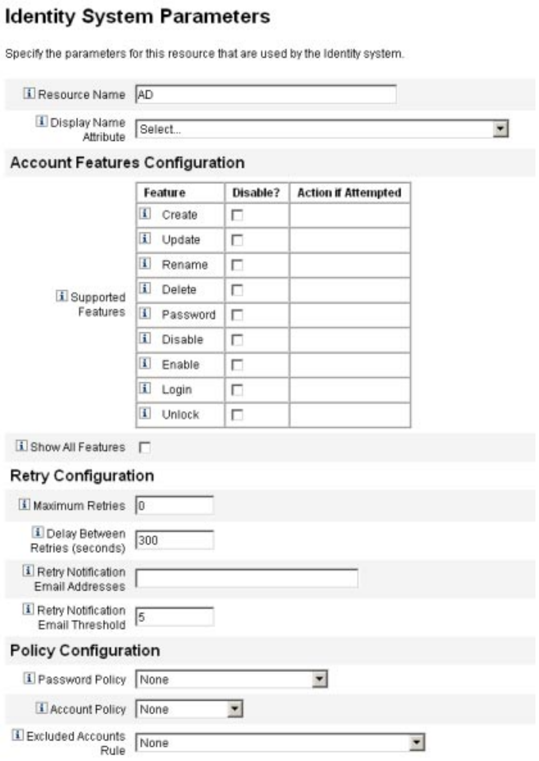
Specify the identity template for users created on this resource.

Identity Template: $accountId$

Types of Accounts □ Support multiple types of accounts for this resource

Use this list to add attributes to the Identity Template

- **Identity System Parameters**. Sets Waveset parameters for the resource, including retry and policy configuration, as shown in "To Create a Resource" on page 147.



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

7 **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

This section describes how to manage existing resources.

The topics are organized as follows:

- "To View the Resource List" on page 151
- "To Edit a Resource Using the Resource Wizard" on page 152
- "To Edit a Resource Using Resource List Commands" on page 152

▼ To View the Resource List

You can view existing resources from the Resource List.

1 **Log into the Administrator Interface.**

2 **Click Resources in the main menu.**

The Resource List is displayed on the List Resources subtab.

▼ To Edit a Resource Using the Resource Wizard

Use the Resource Wizard to edit resource parameters, account attributes, and identity system parameters. You can also specify the identity template that should be used for users created on the resource.

1 **In the Waveset Administrator Interface, click Resources in the main menu.**

The Resource List is displayed on the List Resources subtab.

2 **Select the resource you want to edit.**

3 **In the Resource Actions drop-down menu, select Resource Wizard (under Edit).**

The Resource Wizard opens in Edit mode for the selected resource.

▼ To Edit a Resource Using Resource List Commands

In addition to the Edit Resource Wizard, you can use the Resource List commands to perform a range of edit actions on a resource.

1 **Choose one or more options from the Resource List.**

These options include:

- **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.
- **Perform bulk operations on resources**. Specify a list of resources and actions to apply (from CSV-formatted input) to all resources in the list. Then launch bulk operations to initiate the bulk-operation background task.

2 **Save your changes.**

▼ To View or Edit Resource Account Attributes

Resource account attributes (or schema maps) provide an abstract method for referring to attributes on managed resources. The schema map allows you to specify how attributes will be referred to within Waveset (the left side of the schema map) and how that name is mapped to the attribute name on the actual resource (the right side of the schema map). You can then refer to the attribute name within forms or workflow definitions and effectively reference the attribute on the resource, itself.

An example of a mapping between attributes in Waveset and those for an LDAP resource is as follows:

Waveset Attribute		LDAP Resource Attribute
`firstname`	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

Any reference to the Waveset attribute, `firstname`, is actually a reference to the LDAP attribute, `givenName` when an action is taken upon that resource.

When managing multiple resources from Waveset, mapping a common Waveset account attribute to many resource attributes can greatly simplify resource management. For example, the Waveset `fullname` attribute can be mapped to the Active Directory resource attribute `displayName`. Meanwhile, on an LDAP resource, the same Waveset `fullname` attribute can be mapped to the LDAP attribute `cn`. As a result, an administrator only needs to provide a `fullname` value once. When the user is saved, the `fullname` value is then passed to the resources that have different attribute names.

By setting up a schema map on the Account Attributes page of the Resource Wizard, you can do the following:

- Define attribute names and data types for attributes coming from managed resources
- Limit resource attributes to only those that are essential for your company or organization
- Create common Waveset attribute names to use with multiple resources
- Identify required user attributes and attribute types

To view or edit resource account attributes, follow these steps:

1. **In the Administrator interface, click Resources.**

2. **Select the resource for which you want to view or edit the account attributes.**

3. **In the Resource Actions list, click Edit Resource Schema.**

   The Edit Resource Account Attributes page opens.

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

Resource Groups

Use the resources area 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 Server 2007 resource relies on an existing Windows Active Directory account. This account must exist before the Exchange account can be successfully created. By creating a resource group with (in order) a Windows Active Directory resource and an Exchange Server 2007 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.

Global Resource Policy

This section describes how to edit the Global Resource Policy and set timeout values for a resource.

▼ To Edit Policy Attributes

You can edit resource policy attributes from the Edit Global Resource Policy Attributes page.

1 **Open the Edit Global Resource Policy Attributes page and edit the attributes as needed.**

These attributes include:

- **Default Capture Timeout**. Enter a value, in milliseconds, that specifies the maximum time that the adapter should wait from the command line prompt before the adapter times out. This value applies to GenericScriptResourceAdapter or ShellScriptSourceBase adapters only. Use this setting when the results of a command or script are important and will be parsed by the adapter.

  The default value for this setting is 30000 (30 seconds).
- **Default Wait for Timeout**. Enter a value, in milliseconds, to specify the maximum time that a scripted adapter should wait between polls before checking to see if a command has characters (or results) ready. This value applies to GenericScriptResourceAdapter or ShellScriptSourceBase adapters only. Use this setting when the results of a command or script are not examined by the adapter.
- **Wait for Ignore Case**. Enter a value, in milliseconds, to specify the maximum time the adapter should wait for the command line prompt before timing out. This value applies to GenericScriptResourceAdapter or ShellScriptSourceBase adapters only. Use this setting when the case (uppercase or lowercase) is irrelevant.
- **Resource Account Password Policy**. If applicable, select a resource account password policy to apply to the selected resource. None is the default selection.
- **Excluded Resource Accounts Rule**. If applicable, select a rule that governs excluded resource accounts. None is the default selection.

2 **You must click Save to save your changes to the policy.**

▼ To Set Additional Timeout Values

You can modify the `maxWaitMilliseconds` property by editing the `Waveset.properties` file. The `maxWaitMilliseconds` property controls the frequency in which an operation's timeout will be monitored. If you do not specify this value, the system uses a default value of 50.

1 **Add the following line to the `Waveset.properties` file:**

```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

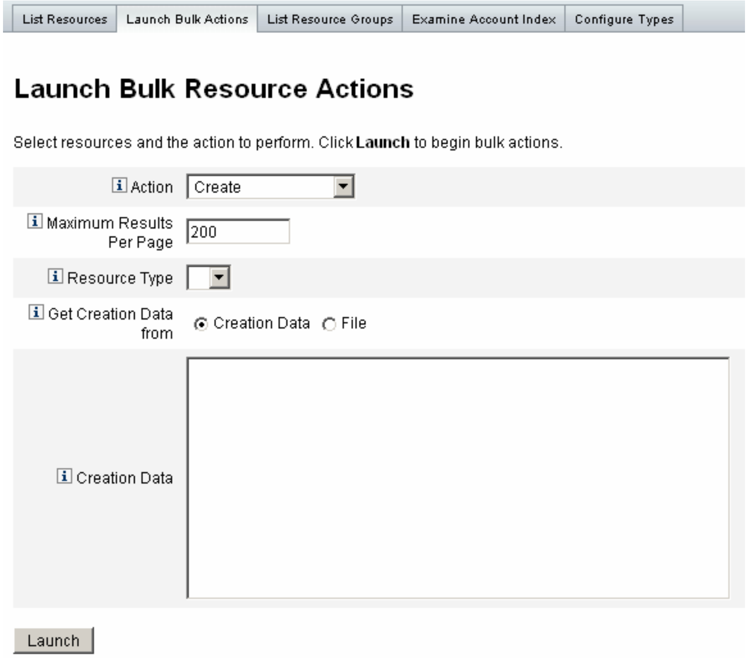
2 **Save the file.**

Bulk Resource Actions

You can perform bulk operations on resources by using a CSV-formatted file or by creating or specifying the data to apply for the operation.

Figure 5–13 shows the launch page for bulk operations using a create action.

FIGURE 5–13 Launch Bulk Resource Actions Page



Launch Bulk Resource Actions

Select resources and the action to perform. Click **Launch** to begin bulk actions.

Action: Create

Maximum Results Per Page: 200

Resource Type:

Get Creation Data from: ● Creation Data ○ File

Creation Data:

The options available for the bulk resource operation depend on the Action you select for the operation. You can specify a single action to apply to the operation or select From Action List to specify multiple actions.

- **Actions**. To specify a single action, select one of the following options: create, clone, update, delete, change password, reset password.

  For a single action selection, you will be presented with options to specify the resource involved with the action. For a Create action, you will specify the resource type.

  If you specify From Action List, use the Get action list from area to specify either the file to use that contains the actions or the actions you specify in the Input area.

  Note – The actions you enter in the input area list or in the file must be in comma-separated value (CSV) format.

- **Maximum Results Per Page**. Use this option to specify the maximum number of bulk action results to display on each task results page. The default value is 200.

Click Launch to start the operation, which runs as a background task.

Understanding and Managing External Resources

You can also use Oracle Waveset to create, provision, and centrally manage *external resources* for your enterprise.

This section describes how to work with external resources, and the information is organized into the following topics:

- "What Are External Resources?" on page 157
- "Why Use External Resources?" on page 157
- "Configuring External Resources" on page 158
- "Creating External Resources" on page 174
- "Provisioning External Resources" on page 177
- "Unassigning and Unlinking External Resources" on page 181
- "Troubleshooting External Resources" on page 181

What Are External Resources?

An *external resource* is a unique resource type that does not directly store user account information. Rather, it is a resource that is external to the workings of Oracle Waveset. These resources can be desktop computers, laptop computers, cell phones, security badges, and so forth.

Provisioning external resources almost always requires one or more manual processes. For example, after making the initial request and getting the required approvals to provision a laptop for a new employee, you might have to submit a purchase requisition request to the company's order request system. After the order is filled, someone else might have to preconfigure the laptop with corporate applications before personally delivering that laptop to the new employee to complete the provisioning request.

Why Use External Resources?

Using Oracle Waveset to provision external resources enables you to notify one or more provisioners about pending requests, including detailed information about what is being provisioned.

For example, an external resource provisioner might be an IT manager who needs to manually order and preconfigure a laptop for a user.

Oracle Waveset also maintains information about the external resources provisioned for a given user and updates that information upon completion of the provisioning request. Oracle Waveset then makes this information available for viewing, reporting, audit compliance validation, and exporting.

Note – To configure external resources, you must have the External Resource Administrator capability. To create new external resources, you must have the Resource Administrator capability.

Configuring External Resources

This section describes the process for configuring the external resource data store and the external resources provisioner notification.

Configuring the External Resources Data Store

Oracle Waveset's external resource data store is a single data store that holds information about external resources and assignments to external resources. This data store can be a database or a directory.

- If the external resource data store is a *database*, that data store is managed by the ScriptedJdbcResourceAdapter.
- If the external resource data store is a *directory*, that data store is managed the LDAPResourceAdapter.

Note – You must have the External Resource Administrator capability to configure the external resource data store.

The external resource data store allows you to store data in whatever attribute values you want and you can store those values in one or more tables.

For example, if you are using a MySQL database, Oracle Waveset stores external resource information in the following tables:

- The `extres.accounts` table contains accountIDs and resourceIDs. Because external resource data store is a single data store, Oracle Waveset provides a unique ID key, `<accountId>@<resourceId>`, that uniquely identifies an account by its resourceID.
- The `extres.attributes` table contains a collection of name/value pair attributes. You define these attributes in the schema mapping when creating an external resource.

Sample scripts used to create the database tables are co-packaged with Oracle Waveset in the following location:

wshome`/sample/ScriptedJdbc/External`

Oracle Waveset supports multiple database types, and provides sample scripts for each type. You can modify these scripts as needed for your specific environment.

The external resource data store also supports LDAP using the LDAPResourceAdapter, which enables you to store data in existing or custom classes. A sample LDIF script is also co-packaged with Oracle Waveset in the following location:

wshome`/sample/other/externalResourcePerson.ldif`

You can modify this script as part of configuring an external resources directory data store.

▼ To Configure a Database-Type Data Store

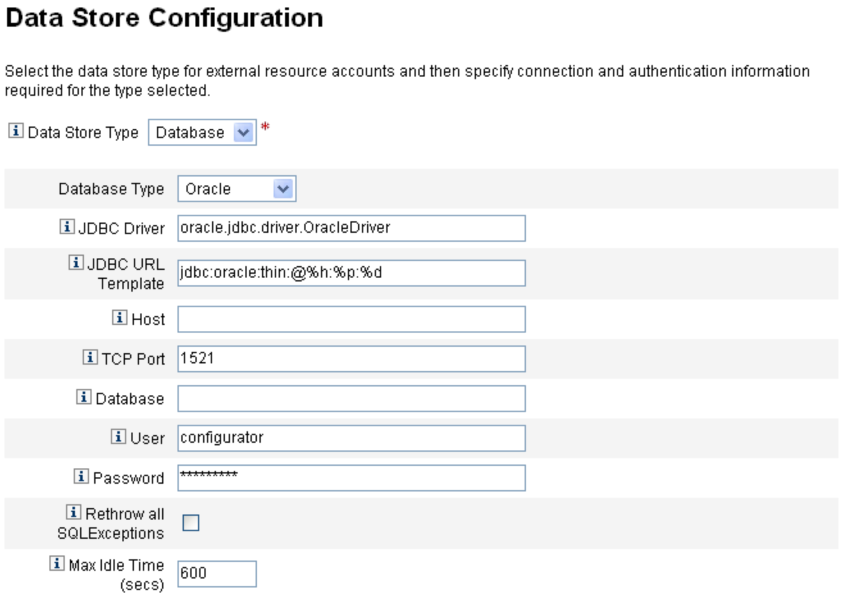
Although you can easily make changes, the external resource data store is typically configured only once. If you modify the configuration, Oracle Waveset automatically updates all existing external resources to use the newly configured data store.

Use the following steps to configure a database-type data store:

1. **Select Configure → External Resources from the menu bar in the Oracle Waveset Administrator interface.**

2. **When the Data Store Configuration page displays, choose Database from the Data Store Type menu. Additional options display.**

FIGURE 5–14 Data Store Configuration Page: Database



Data Store Configuration

Select the data store type for external resource accounts and then specify connection and authentication information required for the type selected.

Data Store Type: Database *

Database Type	Oracle
JDBC Driver	oracle.jdbc.driver.OracleDriver
JDBC URL Template	jdbc:oracle:thin:@%h:%p:%d
Host	
TCP Port	1521
Database	
User	configurator
Password	*********
Rethrow all SQLExceptions	□
Max Idle Time (secs)	600

3. **Specify the following connection and authentication information:**

Note – Oracle Waveset automatically populates the JDBC Driver, JDBC URL template, port, and Max Idle Time (secs) fields with default values. You can change these default values if necessary.

- **JDBC Driver**. Specify the JDBC Driver class name.
- **JDBC URL Template**. Specify the JDBC Driver URL template.
- **Host**. Enter the name of the host where you are running the database.
- **TCP Port**. Enter the port number where the database is listening.
- **Database**. Enter the name of the database on the database server that contains the data store table.
- **User**. Enter the ID of a database user with permissions sufficient to read, update, and delete rows from the data store table. For example, root.
- **Password**. Enter the database user's password.
- **Rethrow all SQLExceptions**. Check this box to rethrow SQL exceptions to SQL statements if the exception error codes are 0.

  If you do not enable this option, Oracle Waveset catches and suppresses these exceptions.
- **Max Idle Time**. Specify the maximum time, in seconds, that you want JDBC connections to remain unused in a pool.

  If the connection is not used before the specified time elapses, Oracle Waveset closes the connection and removes the connection from the pool.
  - Default value is 600 seconds
  - A `-1` value prevents the connection from ever expiring

4 **After successfully connecting to the data store, you must specify one or more scripts to be executed for each supported resource action. See "To Configure the Action Scripts" on page 160 for instructions.**

▼ To Configure the Action Scripts

You must specify a set of BeanShell (`bsh`) scripts that Oracle Waveset can use to track and execute the Get, Create, Update, Delete, Enable, Disable, and Test states of a given request.

Sample action scripts are available in

wshome`/sample/ScriptedJdbc/External/beanshell`

Note – You can modify these samples to create your own custom action scripts. Custom scripts are added to the Action Scripts selection tool, and they are displayed below the line in the Available and Selected lists.

Oracle Waveset provides sample scripts for the resource actions of any database types that are supported for external resources. To access these scripts, use the ResourceAction scripts provided in the following location:

wshome`/sample/ScriptedJdbc/External/beanshell`

The default database name, username, and password are all `extres`.

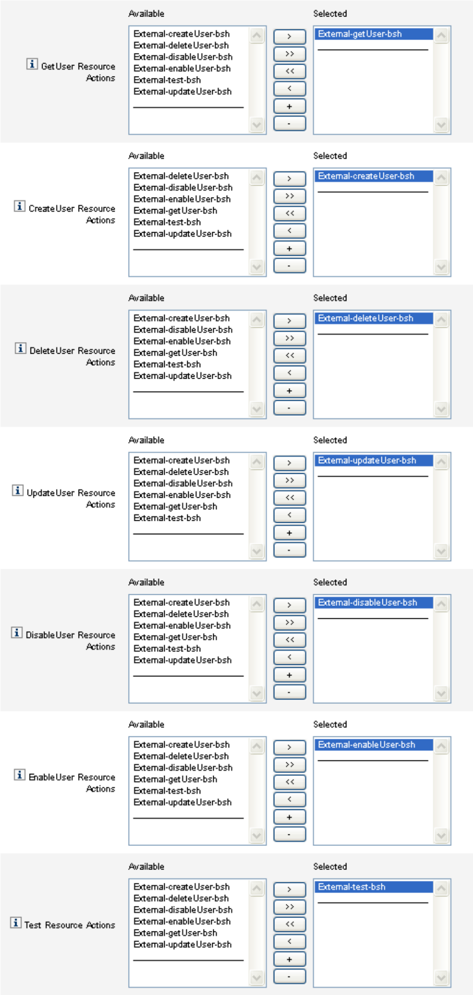
- If you choose any of the other database options or prefer using a different user name or database name, you must modify the sample database creation scripts and the ResourceAction scripts with different values.

  For example, if you choose a MySQL database, but want to change the existing database name, username, and password, you must perform the following changes: You must update the `create_external_tables.mysql` script by changing the default database name, username, and password from `extres` to `externalresources`, `externaladmin`, and `externalpassword` respectively.
- Next, you must change the ResourceAction scripts from the default `extres.accounts` and `extres.attributes` values to `externalresources.accounts` and `externalresources.attributes` respectively.

Use the following steps to configure the Action scripts:

1. **Use the Action Scripts selection tools on the Data Store Configuration page to specify one or more action scripts for each resource action. You must select at least one script per resource action.**

FIGURE 5–15 Action Scripts Area



GetUser Resource Actions
Available: External-createUser-bsh, External-deleteUser-bsh, External-disableUser-bsh, External-enableUser-bsh, External-test-bsh, External-updateUser-bsh
Selected: External-getUser-bsh

CreateUser Resource Actions
Available: External-deleteUser-bsh, External-disableUser-bsh, External-enableUser-bsh, External-getUser-bsh, External-test-bsh, External-updateUser-bsh
Selected: External-createUser-bsh

DeleteUser Resource Actions
Available: External-createUser-bsh, External-disableUser-bsh, External-enableUser-bsh, External-getUser-bsh, External-test-bsh, External-updateUser-bsh
Selected: External-deleteUser-bsh

UpdateUser Resource Actions
Available: External-createUser-bsh, External-deleteUser-bsh, External-disableUser-bsh, External-enableUser-bsh, External-getUser-bsh, External-test-bsh
Selected: External-updateUser-bsh

DisableUser Resource Actions
Available: External-createUser-bsh, External-deleteUser-bsh, External-enableUser-bsh, External-getUser-bsh, External-test-bsh, External-updateUser-bsh
Selected: External-disableUser-bsh

EnableUser Resource Actions
Available: External-createUser-bsh, External-deleteUser-bsh, External-disableUser-bsh, External-getUser-bsh, External-test-bsh, External-updateUser-bsh
Selected: External-enableUser-bsh

Test Resource Actions
Available: External-createUser-bsh, External-deleteUser-bsh, External-disableUser-bsh, External-enableUser-bsh, External-getUser-bsh, External-updateUser-bsh
Selected: External-test-bsh

You must select the default action script that matches the resource action. For example, you must use

- `External-getUser-bsh` for GetUser Resource Actions

Note – GetUser Resource Actions are used for Search operations.

- `External-createUser-bsh` for CreateUser Resource Actions
- `External-deleteUser-bsh` for DeleteUser Resource Actions

- `External-updateUser-bsh` for UpdateUser Resource Actions
- `External-disableUser-bsh` for DisableUser Resource Actions
- `External-enableUser-bsh` for EnableUser Resource Actions
- `External-test-bsh` for Test Resource Actions

Note – Test Resource Actions are used to enable full functionality for the Test Connection button.

Selecting any of the other `bsh` scripts from the sample scripts in the list will not work.

2 **Choose an Action Context Mode from the menu to specify how attribute values will be passed to the action scripts.**

- **Strings**. Passes attribute values as string values.
- **Direct**. Passes attribute values as a `com.waveset.object.AttributeValues` object.

3 **Now is a good time to test your data store connection configuration. Click the Test Connection button, located at the bottom of the page.**

A message displays to confirm that the connection is successful or to report an error with the configuration.

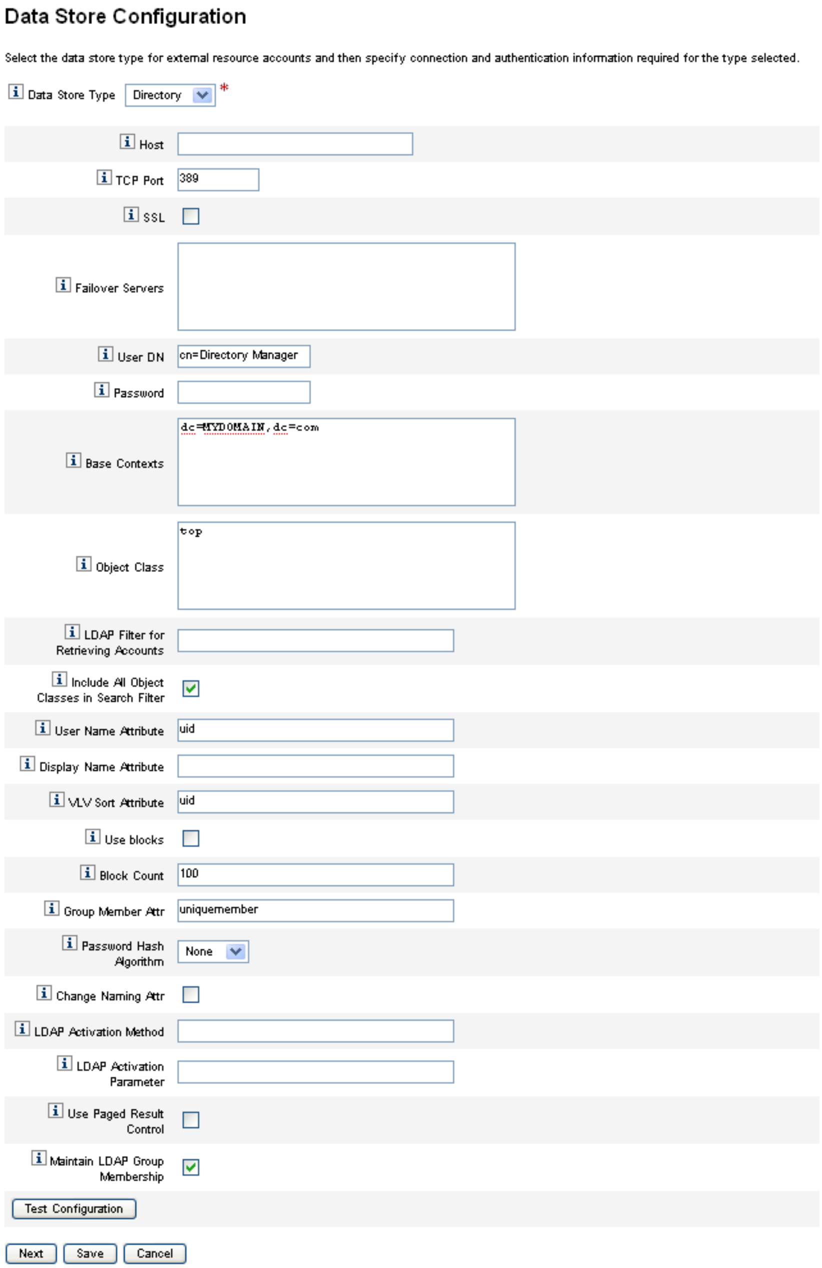
4 **When you are finished, click Next to continue to the Provisioner Notification Configuration page.**

▼ To Configure a Directory-Type Data Store

Use the following steps to configure a Directory-type data store.

1 **Choose Directory from the Data Store Type menu. Additional options display.**

FIGURE 5–16 Data Store Configuration Page: Directory



Data Store Configuration

Select the data store type for external resource accounts and then specify connection and authentication information required for the type selected.

Data Store Type: Directory *

Host	
TCP Port	389
SSL	□
Failover Servers	
User DN	cn=Directory Manager
Password	
Base Contexts	dc=MYDOMAIN,dc=com
Object Class	top
LDAP Filter for Retrieving Accounts	
Include All Object Classes in Search Filter	☑
User Name Attribute	uid
Display Name Attribute	
VLV Sort Attribute	uid
Use blocks	□
Block Count	100
Group Member Attr	uniquemember
Password Hash Algorithm	None
Change Naming Attr	□
LDAP Activation Method	
LDAP Activation Parameter	
Use Paged Result Control	□
Maintain LDAP Group Membership	☑

2 You must specify connection and authentication information for a Directory-type data store.

Configure the following options:

- **Host**. Enter the IP address or the name of the host where the LDAP server is running.
- **TCP Port**. Enter the TCP/IP port being used to communicate with the LDAP server.
  - If you are using SSL, this port is typically 636.
  - If you are using non-SSL, this port is typically 389.
- **SSL**. Check this option to connect to the LDAP server using SSL.
- **Failover Servers**. List all of the servers being used for failover if the preferred server fails. Enter this information in the following format, which follows the standard LDAP version 3 URLs described in RFC 2255:

  ```
  ldap://ldap.example.com:389/o=LdapFailover
  ```

  Only the host, port, and distinguished name (dn) portion of the URL are relevant in this setting.

  If the preferred server fails, JNDI will automatically connect to the next server in this list.
- **User DN**. Enter the dn used to authenticate to the LDAP server when making updates. (Defaults to `cn=Directory Manager`)
- **Password**. Enter the principal's password.
- **Base Contexts**. Specify one or more starting points that Oracle Waveset can use when searching the LDAP tree for users. (Defaults to `dc=MYDOMAIN,dc=com`)

  Oracle Waveset performs searches when trying to discover users from the LDAP server or when looking for groups in which users are members.
- **Object Class**. Enter one or more object classes to use when creating new user objects in the LDAP tree. (Defaults to top)

  Each entry must be on a separate line. Do not use commas or spaces to separate entries.

  Some LDAP servers require you to specify all of the object classes in a class hierarchy. For example, you might be required to specify `top`, `person`, `organizationalperson`, and `inetorgperson` instead of just using `inetorgperson`.
- **LDAP Filter for Retrieving Accounts**. Enter an LDAP filter to control which accounts are returned from the LDAP resource. If you do not specify a filter, Oracle Waveset returns all accounts that include all of the specified object classes.
- **Include All Object Classes in Search Filter**. Check this box to require all accounts to include every specified object class and to match the filter specified in the LDAP Filter for Retrieving Accounts field.

  Note – You must enable this option when no search filter is specified. If you disable this option, accounts that do not include all of the specified object classes can be loaded into Oracle Waveset by using the reconciliation or load from resource features.

After loading, the account's `objectclass` attribute is not automatically updated. If an attribute on a missing object class is exposed through the Administrator interface, then providing a value for this attribute without modifying the `objectclass` attribute will fail. To avoid this problem, override the `objectclass` value in the Reconciliation or Load from Resource form.

- **User Name Attribute**. Enter the name of the LDAP attribute that maps to the name of the Oracle Waveset user when discovering users from the directory. This name is frequently `uid` or `cn`.
- **Display Name Attribute**. Enter the resource account attribute name whose value is used when displaying this account name.
- **VLV Sort Attribute**. Enter the name of a sort attribute to use for VLV indexes on the resource.
- **Use blocks**. Check this box to retrieve and process users in blocks.

  When you are performing operations on a large number of users, processing users in blocks reduces the amount of memory used by the operation.
- **Block Count**. Enter the maximum number of users to be grouped in blocks for processing.
- **Group Member Attr**. Enter the name of the group member attribute to be updated with the user distinguished name (DN) when a user is added to the group.

  The attribute name depends on the group's object class. For example, the Sun Java System Enterprise Edition Directory Server and other LDAP servers use groups with the `groupOfUniqueNames` object class, and the `uniqueMember` attribute. Other LDAP servers use groups with the `groupOfUniqueNames` object class and the member attribute.
- **Password Hash Algorithm**. Enter an algorithm that Oracle Waveset can use to hash the password.

  Supported values include:

  - `SSHA`
  - `SHA`
  - `SMD5`
  - `MD5`

  If you specify 0 or leave this field blank, Oracle Waveset will not hash passwords and will store cleartext passwords in LDAP unless the LDAP server performs the hash. For example, Directory Server hashes passwords.
- **Change Naming Attr**. Check this box to allow modifications to change the user attribute representing the leftmost relative distinguished name (DN). Modifications frequently change naming attributes to `uid` or `cn`.
- **LDAP Activation Method**. Use this field to configure activation actions for a resource.
  - Leave this field blank if you want the resource to use password assignment for enable or disable actions.

  - Enter the `nsmanageddisabledrole` keyword, the `nsaccountlock` keyword, or the class name to use when performing an activation action for users of this resource.
- **LDAP Activation Parameter**. Enter a value, based on how you completed the LDAP Activation Method field.
  - If you specified the `nsmanageddisabledrole` keyword, you must enter a value in the following format:

    IDMAttribute`=CN=nsmanageddisabledrole,`*baseContext*
  - If you specified the `nsaccountlock` keyword, you must enter a value in the following format:

    IDMAttribute`=true`
  - If you specified a class name, you must enter a value in the following format:

    IDMAttribute

  Note – For more information about the LDAP Activation Method and the LDAP Activation Parameter, see the *Oracle Waveset 8.1.1 Resources Reference*.

- **Use Paged Result Control**. Check this box to use LDAP Paged Results Control instead of VLV Control to iterate accounts during reconciliation.

  Note – The resource must support simple paging control.

- **Maintain LDAP Group Membership**. Check this box to have the adapter maintain LDAP group memberships when renaming or deleting users.

  If you do not enable this option, the LDAP resource maintains the group memberships.

3 **Test your data store connection configuration by clicking the Test Connection button.**

A message displays to confirm that the connection is successful or to report an error with the configuration.

4 **When you are finished, click Save and then click Next to continue to the Provisioner Notification Configuration page.**

Note – You must set up valid account attributes and an identity template before you can create users on an LDAP resource.

Configuring Provisioner Notification

After configuring the data store for external resources, you must configure provisioner notifications. You can also configure requester notifications. This section describes the process for configuring notifications using email or Remedy.

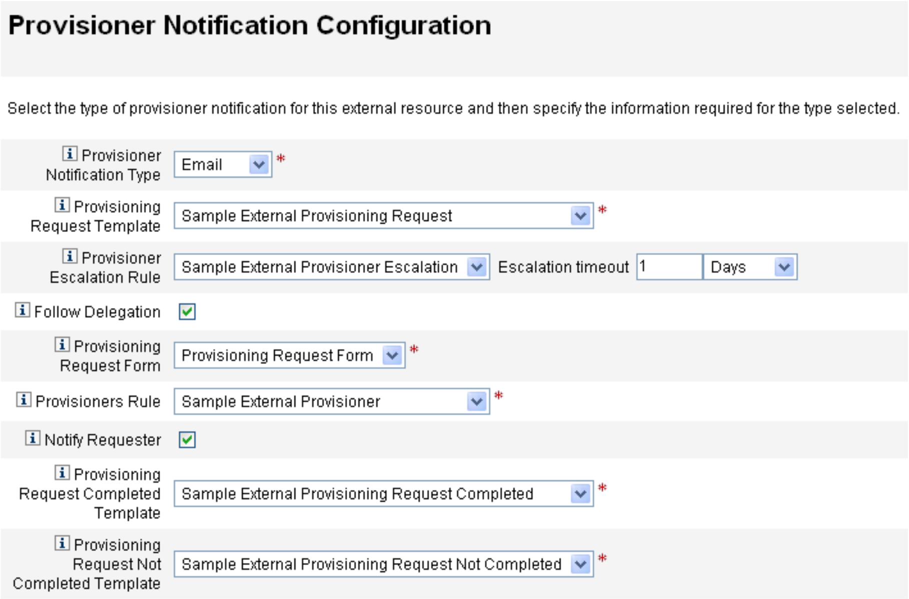
▼ To Configure Email Notification

Note – For more information about Email templates, see Configuring Task Templates.

Use the following instructions to configure and send email notifications to one or more provisioners:

1 **From the Provisioner Notification Configuration page, select Email from the Provisioner Notification Type menu. Additional options display, as shown in the following figure.**

FIGURE 5–17 Provisioner Notification Configuration Page: Email Notification Type



Provisioner Notification Configuration

Select the type of provisioner notification for this external resource and then specify the information required for the type selected.

Provisioner Notification Type	Email *
Provisioning Request Template	Sample External Provisioning Request *
Provisioner Escalation Rule	Sample External Provisioner Escalation · Escalation timeout 1 Days
Follow Delegation	☑
Provisioning Request Form	Provisioning Request Form *
Provisioners Rule	Sample External Provisioner *
Notify Requester	☑
Provisioning Request Completed Template	Sample External Provisioning Request Completed *
Provisioning Request Not Completed Template	Sample External Provisioning Request Not Completed *

2 **Configure the following options.**

- **Provisioning Request Template**. Choose Sample External Provisioning Request from the menu. You use this email template to configure the email used to notify provisioners of external resource requests.

- **Follow Delegation**. Check this box if you want Oracle Waveset to follow delegations defined for the provisioner.
- **Provisioner Escalation Rule** (*optional*). Choose a rule to determine to which provisioner a request is escalated if the current provisioner does not respond to the request before the specified timeout period.

  Note – Although there are several sample rules available on this menu, you must choose the *Sample External Provisioner Escalation* rule or use your own custom rule. The Sample External Provisioner Escalation rule uses an External Provisioner Escalation rule to determine a provisioner for escalations.

- **Escalation timeout**. Specify the maximum time to wait before escalating a provisioning request to the next provisioner.

  Note –

  - If you leave this field blank or enter a zero, the request never escalates.
  - If you specify a timeout, but do not select a Provisioner Escalation Rule, Oracle Waveset escalates the request to the Configurator when the request exceeds the specified timeout. If a Configurator does not exist, the request is classified as "not complete" once the timeout expires.

- **Provisioning Request Form**. Choose a form that external resource provisioners can use to mark a provisioning request as completed or not completed.
- **Provisioners Rule**. You must choose a rule to define the provisioner to whom provisioning requests are sent when external resources are assigned to users.

  Note –

  - You can write your own rules for this purpose. You can also define multiple provisioners. As any provisioner completes the task, that task is removed from all provisioner's queues. For more information about writing custom rules, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.
  - Although there are several sample rules available on this menu, you must choose the *Sample External Provisioner* rule or use your own custom rule. The Sample External Provisioner rule makes Configurator the provisioner.

- **Notify Requester**. Check this box to send email back to the original requester with information about what happened with the request. For example, whether the provisioning request completed or not completed, is additional information needed, and so forth.

When you enable this option, the following additional fields are displayed:

Note –

- **Provisioning Request Completed Template**. Choose the Sample External Provisioning Request Completed template to notify requestors when their requests are completed.
- **Provisioning Request Not Completed Template**. Choose the Sample External Provisioning Request Not Completed template to notify requestors when their requests are not completed.

---

3 **Click Save.**

The Configure page displays indicating that you can go on to perform another configuration task.

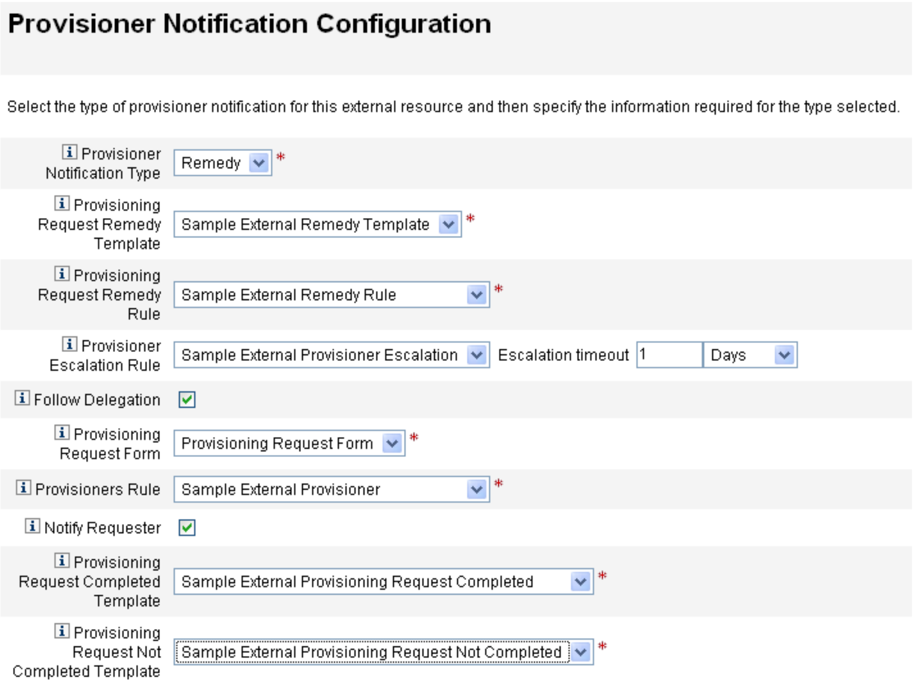
4 **Go to the Resources → List Resources tab. You are now ready to create individual external resources based on this configuration. See "To Create a Resource" on page 147 for instructions.**

▼ To Configure Remedy Notification

Use the following instructions to create and send a Remedy ticket to provisioners:

1 **Select Remedy from the Provisioner Notification Type menu. Additional options display, as shown in the following figure.**

FIGURE 5–18 Provisioner Notification Configuration Page: Remedy Notification Type



Provisioner Notification Configuration

Select the type of provisioner notification for this external resource and then specify the information required for the type selected.

Provisioner Notification Type	Remedy *
Provisioning Request Remedy Template	Sample External Remedy Template *
Provisioning Request Remedy Rule	Sample External Remedy Rule *
Provisioner Escalation Rule	Sample External Provisioner Escalation — Escalation timeout 1 Days
Follow Delegation	☑
Provisioning Request Form	Provisioning Request Form *
Provisioners Rule	Sample External Provisioner *
Notify Requester	☑
Provisioning Request Completed Template	Sample External Provisioning Request Completed *
Provisioning Request Not Completed Template	Sample External Provisioning Request Not Completed *

2 Configure the following options.

- **Provisioning Request Remedy Template**. Choose Sample External Remedy template from the menu.

  Note – Oracle Waveset provides a Sample Remedy Template that you can use or modify as needed.

  A Remedy template contains a set of fields that are used to create a Remedy ticket. Oracle Waveset also uses this template to query Remedy for ticket status, to see if a task has been completed or not completed.

- **Provisioning Request Remedy Rule**. You must choose a rule from this menu to define configuration settings for Remedy.

Note – Although there are several sample rules available on this menu, you must choose the *Sample External Remedy Rule* rule or use your own custom rule. The Sample External Remedy Rule uses a Remedy rule to determine whether the current status of a Remedy tick is completed or not completed.

A Remedy template contains a set of fields that are used to create a Remedy ticket. Oracle Waveset also uses this template to query Remedy for ticket status, to see if a task has been completed or not completed.

Oracle Waveset uses this rule to query a Remedy ticket for status information. If the ticket status is completed or not completed, Oracle Waveset marks the work item completed or not completed, respectively.

Note – You can write your own rules for this purpose. A sample rule, called Sample External Remedy Rule is provided for you to use or modify as needed. For more information about writing custom rules, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.

- **Follow Delegation**. Check this box if you want Oracle Waveset to follow delegations defined for the provisioner.
- **Provisioner Escalation Rule** (*optional*). Choose a rule to determine to which provisioner a request is escalated if the current provisioner does not respond to the request before the specified timeout period.

Note – Although there are several sample rules available on this menu, you must choose the *Sample External Provisioner Escalation* rule or use your own custom rule. The Sample External Provisioner Escalation rule uses an External Provisioner Escalation rule to determine a provisioner for escalations.

- **Escalation timeout**. Specify the maximum time to wait before escalating a provisioning request to the next provisioner.

Note –

- If you leave this field blank or enter a zero, the request never escalates.
- If you specify a timeout, but do not select a Provisioner Escalation Rule, Oracle Waveset escalates the request to the Configurator when the request exceeds the specified timeout. If a Configurator does not exist, the request is classified as "not complete" once the timeout expires.

- **Provisioning Request Form**. Choose a form that external resource provisioners can use to mark a provisioning request as completed or not completed.
- **Provisioners Rule**. Choose a rule that determines one or more provisioners for this external resource request.

Note – You can write your own rules for this purpose. You can also define multiple provisioners. As any provisioner completes the task, that task is removed from all provisioner's queues. For more information about writing custom rules, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.

  - **Sample External Provisioner**. Makes Configurator the provisioner.
  - **Sample External Provisioner Escalation**. Uses an External Provisioner Escalation rule to determine a provisioner for escalations.
  - **Sample External Remedy Rule**. Defines configurator settings for Remedy.
- **Notify Requester**. Check this box if you want to send email to the requester when their request is completed or not completed. When you enable this option, the following additional fields are displayed:
  - **Provisioning Request Completed Template**. Choose the email template to use when requests are completed.
  - **Provisioning Request Not Completed Template**. Choose the email template to use when requests are not completed.

Note – For more information about Email templates, see "Configuring the Task Templates" on page 279.

3 **Click Save.**

The Configure page displays indicating that you can go on to perform another configuration task.

4 Go to the Resources → List Resources tab. You are now ready to create individual external resources based on this configuration. See "Creating External Resources" on page 174 for instructions.

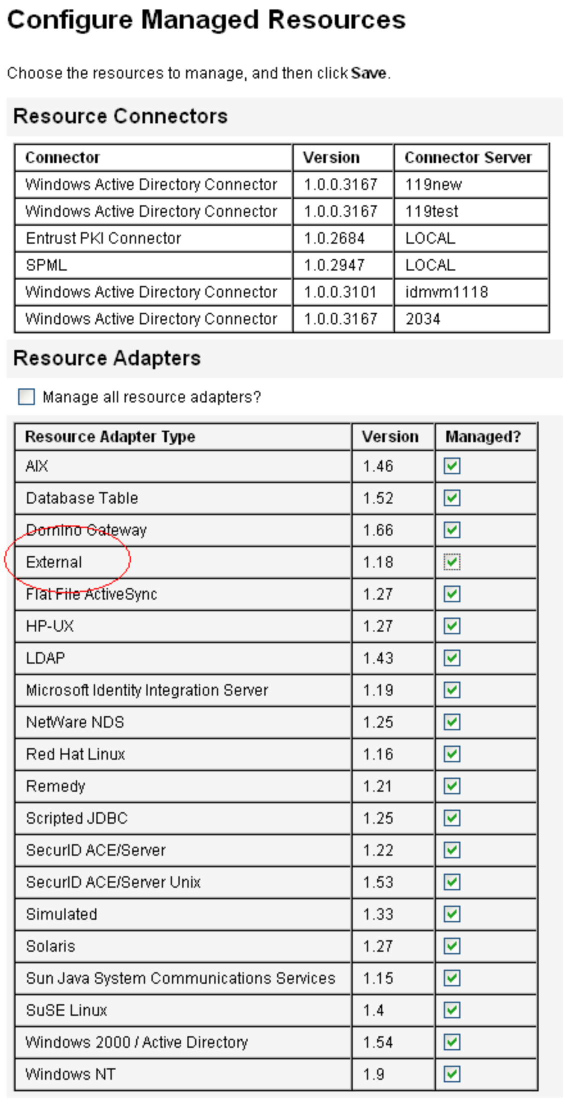
Creating External Resources

After configuring the external resource data store and provisioner notifications, you can create a new external resource.

Note – You must have the Resource Administrator capability to create new external resources.

To create a new external resource, use the following steps:

1. From the main menu bar, select the Resources tab. The List Resources tab is displayed by default.
2. Click the Configure Types tab to open the Configure Managed Resources page.



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resource Connectors

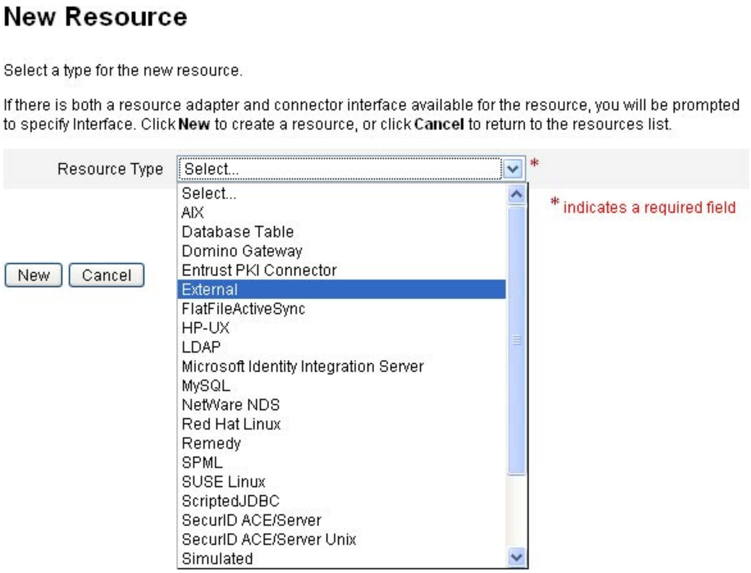
Connector	Version	Connector Server
Windows Active Directory Connector	1.0.0.3167	119new
Windows Active Directory Connector	1.0.0.3167	119test
Entrust PKI Connector	1.0.2684	LOCAL
SPML	1.0.2947	LOCAL
Windows Active Directory Connector	1.0.0.3101	idmvm1118
Windows Active Directory Connector	1.0.0.3167	2034

Resource Adapters

□ Manage all resource adapters?

Resource Adapter Type	Version	Managed?
AIX	1.46	☑
Database Table	1.52	☑
Domino Gateway	1.66	☑
External	1.18	☑
Flat File ActiveSync	1.27	☑
HP-UX	1.27	☑
LDAP	1.43	☑
Microsoft Identity Integration Server	1.19	☑
NetWare NDS	1.25	☑
Red Hat Linux	1.16	☑
Remedy	1.21	☑
Scripted JDBC	1.25	☑
SecurID ACE/Server	1.22	☑
SecurID ACE/Server Unix	1.53	☑
Simulated	1.33	☑
Solaris	1.27	☑
Sun Java System Communications Services	1.15	☑
SuSE Linux	1.4	☑
Windows 2000 / Active Directory	1.54	☑
Windows NT	1.9	☑

3. Review the Resource Adapters table to verify that the External resource type is available.
4. Return to the List Resources tab and choose New Resource from the Resource Type Actions menu.
5. When the New Resource page displays, choose External from the Resource Type menu, and click New.



New Resource

Select a type for the new resource.

If there is both a resource adapter and connector interface available for the resource, you will be prompted to specify Interface. Click **New** to create a resource, or click **Cancel** to return to the resources list.

Resource Type: Select... *

* indicates a required field

6. The Create External Resource Wizard Welcome page displays. Click Next.

   A read-only view of the Data Store Configuration page displays and shows the connection and authentication information you defined earlier.

   As mentioned previously, you generally configure this data store only once because the configuration applies to all external resources. If you want to change any of this information, you must go back to the Configure → External Resources tab.

   Note – You can click Test Configuration, located at the bottom of the page, if you want to retest the current data store configuration before you proceed.

   ---

7. Click Next to open the Provisioner Notification Configuration page, which is identical to the one you configured on the Configure → External Resources tab.
8. Review the current Provisioner Notification settings and make any necessary changes for the new resource.

   Note – If necessary, refer back to the configuration instructions in "Configuring Provisioner Notification" on page 168. Any changes made to this page will only affect this resource.

   ---

9. Click Next.

From this point, the process for creating an external resource is the same as that used to create any other resource. The Wizard takes you through several more pages:

- **Account Attributes page**. Use this page to define optional account attributes for the resource and map Identity system attributes to the new resource account attributes. For example, if you are creating an external resource called “laptop,” you might want to add attributes for model and size.

  Note – No defaults are specified for this page.

- **Identity Template page**. Use this page to define account name syntax for users created on this external resource. You can use the default identity template, `$accountId$`, or specify a different template.
- **Identity System Parameters page**. Use this page to configure identity system parameters for external resources. For example, you can disable policies, configure retries, or specify approvers.

See “To Create a Resource” on page 147 for more information about these pages and for the instructions you need to finish configuring this resource.

10. When you finish configuring the Identity System Parameters page, click Save. Now you can assign this resource to a user, just as you would any other resource.

Provisioning External Resources

This section describes the actual provisioning process, including:

- “To Assign an External Resource to a User” on page 177
- “To Respond to An External Resource Provisioning Request” on page 178

▼ To Assign an External Resource to a User

Use these steps to assign an external resource to a user:

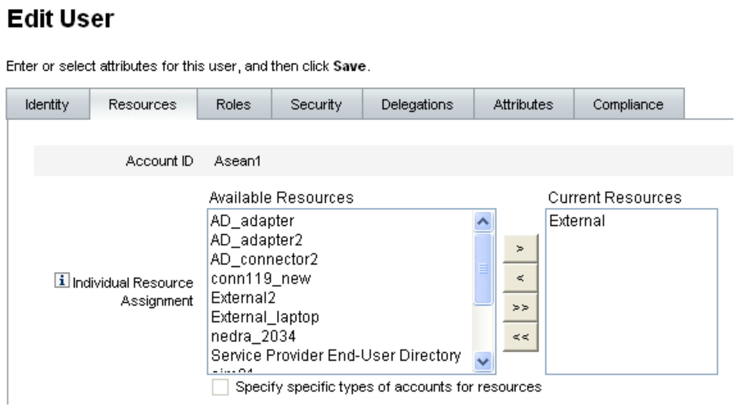
Note – To assign external resources, you must have the Resource Administrator capability.

1 **Click Accounts → List Accounts and then click the user's name from the page.**

2 **When the Edit User page displays, click the Resources tab.**

3 **Locate the External resource in the Individual Resource Assignment's Available Resources list, move it to the Current Resources list, and then click Save.**

FIGURE 5–19 Edit User Page



Edit User

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

Account ID Asean1

Individual Resource Assignment

Available Resources:
AD_adapter
AD_adapter2
AD_connector2
conn119_new
External2
External_laptop
nedra_2034
Service Provider End-User Directory

Current Resources:
External

□ Specify specific types of accounts for resources

Oracle Waveset creates a provisioning task and sends you a message indicating who owns that provisioning task. Remember that one or more provisioners were defined, using the Provisioners Rule, when the Provisioner Notification page was configured for this resource.

Oracle Waveset also notifies the provisioners by using email or a Remedy ticket that they have a request pending.

Note – As with other resources, you can define approvers and they can approve or reject a request. You must define provisioners, but they do not approve or reject requests. Instead, provisioners either complete or do not complete tasks.

---

4 **Click OK to return to the Accounts → List Accounts page. Notice that an hourglass is displayed next to the user's name, in the work item icon, to indicate the request is pending.**

▼ To Respond to An External Resource Provisioning Request

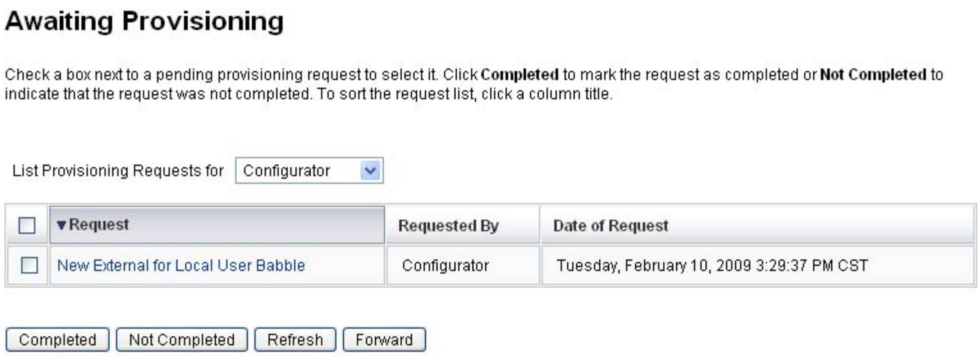
When a provisioning request is generated, the request suspends the provisioning process until one of the defined provisioners completes the manual provisioning or marks the request not complete, or the request times out. Oracle Waveset audits these provisioning responses.

As with any other work item, you can review all of your pending external resource provisioning requests from the Work Items → Provisioning Requests tab.

You respond to provisioning requests as follows:

1 **Click the Work Items > Provisioning Requests tabs to open the Awaiting Provisioning page.**

FIGURE 5–20 Awaiting Provisioning Page



Awaiting Provisioning

Check a box next to a pending provisioning request to select it. Click **Completed** to mark the request as completed or **Not Completed** to indicate that the request was not completed. To sort the request list, click a column title.

List Provisioning Requests for: Configurator

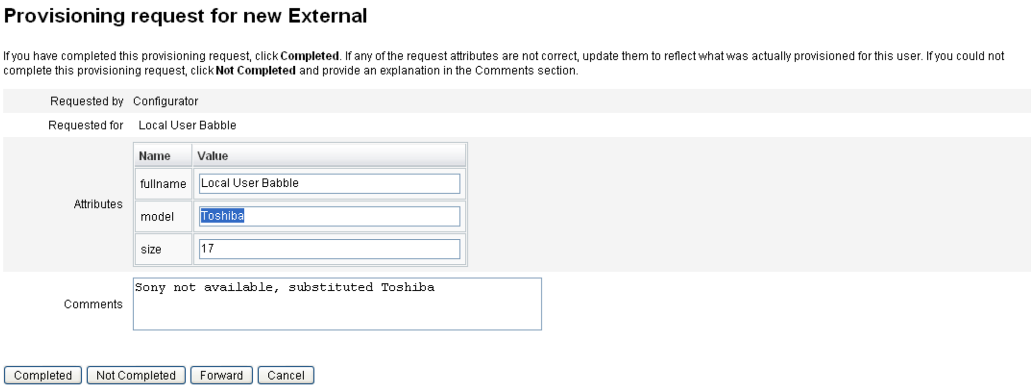
□	▾Request	Requested By	Date of Request
□	New External for Local User Babble	Configurator	Tuesday, February 10, 2009 3:29:37 PM CST

2 **Locate and select the pending provisioning request.**

3 **Optionally, you can open your provisioning request email, click a link that is defined in the Provisioning Request Template, and log in to view a page containing details about the provisioning request.**

From this page, you can update any of the requested attributes to accurately reflect what was provisioned for the user. For example, if the user requested a Sony laptop, but that model was not available, you could update the page with the model you actually provisioned.

FIGURE 5–21 Provisioning Request for a New Laptop



Provisioning request for new External

If you have completed this provisioning request, click **Completed**. If any of the request attributes are not correct, update them to reflect what was actually provisioned for this user. If you could not complete this provisioning request, click **Not Completed** and provide an explanation in the Comments section.

Requested by: Configurator

Requested for: Local User Babble

Attributes:

Name	Value
fullname	Local User Babble
model	Toshiba
size	17

Comments: Sony not available, substituted Toshiba

4 **Click one of the following buttons to process the request:**

- If you can provision the resource, click Completed.

  Oracle Waveset updates the user's external resource account attributes to show what was actually provisioned, removes the pending provisioning state flag, and completes the provisioning request work item being updated.

If configured, Oracle Waveset also notifies the requester that the provisioning request is complete by using the email template configured for that purpose.

- If you cannot provision the resource, specify a reason why, and click Not Completed.

  When you mark a request Not Completed,

  - The user is not provisioned to the external resource.
  - The external resource remains assigned to the user.
  - A yellow icon, indicating that an update is needed for the user, displays next to the user's name.

    If this user is edited, an error message displays, stating that the user cannot be found in the external resource.
  - If configured, Oracle Waveset also notifies the requester by using the email template configured for that purpose.
- If you cannot provision the resource you can also click Forward to forward the request to someone else.

When the provisioning request work item is completed or not completed, Oracle Waveset clears the user's assigned external resource pending state and no updates occur to the external resource data store.

The resource displays in the user's list of assigned resources and in the list of current resource accounts, including the user's accountId on that resource.

Note – If the assigned provisioner does not respond to a provisioning request before the specified timeout period, Oracle Waveset will cancel the associated provisioning request work item.

More Information

Escalating Provisioning Requests

- If you specified a timeout period when you configured the Provisioner Notification page, and a provisioning request exceeds the timeout period, Oracle Waveset performs one of the following actions:
  - If you specified a Provisioner Escalation Rule, Oracle Waveset uses that rule to determine the next provisioner, and then escalates the request to that provisioner.
  - If you did not select a Provisioner Escalation Rule, Oracle Waveset escalates the request to the Configurator. If a Configurator does not exist, the request is classified as ”not complete” once the timeout expires.
- If you left the Escalation timeout field blank, or entered a zero, Oracle Waveset never escalates the request.

Delegating Provisioning Requests

You can delegate external resource provisioning work items just like any other provisioning request. See "Delegating Work Items" on page 213 for more information and instructions.

Unassigning and Unlinking External Resources

You can unassign or unlink external resources from a user, from the General tab as with any other resource. See "Creating Users and Working with User Accounts" on page 53 for instructions.

Note –

- Unassigning or unlinking an external resource from a user does not create a provisioning request or a work item. When you unassign or unlink an external resource, Oracle Waveset does not deprovision or delete the resource account, so there is nothing for you to do.
- You can use the Delete Resource Accounts page to unassign or unlink resource accounts when the Delete operation has been disabled.

Troubleshooting External Resources

You cannot delete users who still have assigned external resources. You must first deprovision or delete those external resources before you can delete the users.

Oracle Waveset enables you to use the following methods for debugging and tracing external resources:

- You can trace the External Resource adapter.
  - If you are using a data store that is a database, trace the `com.waveset.adapter.ScriptedJdbcResourceAdapter` and `com.waveset.adapter.JdbcResourceAdapter` trace class names.
  - If you are using a data store that is a directory, trace the `com.waveset.adapter.LDAPResourceAdapter` trace class name.
- You can use workflow tracing to trace additional data flow and work flow, and use the NetBeans or Eclipse Identity Manager IDE plug-in to for debugging.
- Because you configure and control the data store, you can use data store inspection to ensure the correct information is in that data store.
- Oracle Waveset writes audit records for all activities that occur.

For more information about tracing and troubleshooting, see the *Oracle Waveset 8.1.1 System Administrator's Guide*.

CHAPTER 6

Administration

This chapter provides information and procedures for performing a range of administrative-level tasks in the Waveset system, such as creating and managing Waveset administrators and organizations. It also provides an understanding of how you can use roles, capabilities, and administrative roles in Waveset.

The information is grouped in the following topics:

Understanding Waveset Administration

Waveset administrators are users with extended Waveset privileges.

Waveset administrators manage:

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

Unlike users, administrators in Waveset are assigned capabilities and controlled organizations, which are defined as follows:

- **Capabilities**. A set of permissions granting access rights to Waveset users, organizations, roles, and resources.
- **Controlled organizations**. Once assigned to control an organization, the administrator can manage the objects in that organization, as well as any organizations that are descended from it in the hierarchy.

Delegated Administration

In most companies, employees who perform administrative tasks hold specific responsibilities. Consequently, the account management tasks that these administrators can perform are limited in scope.

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

Waveset can also restrict administrators to a specific tasks within a specific, defined scope.

Waveset supports the separation of responsibilities and a delegated administration model as follows:

- Assigned **capabilities** limit administrators to specific job duties
- Assigned **controlled organizations** restrict administrators to controlling only specific organizations (and the objects within those organizations)
- Filtered views of the Create User and Edit User pages prevent administrators from viewing information that is not relevant to their job duties

You can specify delegations for a user from the Create User page when you set up a new user account, or when you edit a user account.

You can also delegate work items, such as requests for approvals, from the Work Items tab. For more information on delegations, see "Delegating Work Items" on page 213 for details.

Creating and Managing Administrators

This section is organized into the following topics:

- "To Create an Administrator" on page 185
- "Filtering Administrator Views" on page 186
- "Changing Administrator Passwords" on page 187
- "Challenging Administrator Actions" on page 187
- "Changing Answers to Authentication Questions" on page 189
- "Customizing Administrator Name Display in the Administrator Interface" on page 190

▼ To Create an Administrator

To create an administrator, assign one or more capabilities to a user and designate the organizations to which the capabilities will apply.

1 **In the Administrator interface, click Accounts in the menu bar.**

The User List page opens.

2 **To give an existing user administrative privileges, click the user name (the Edit User page opens), then click the Security tab.**

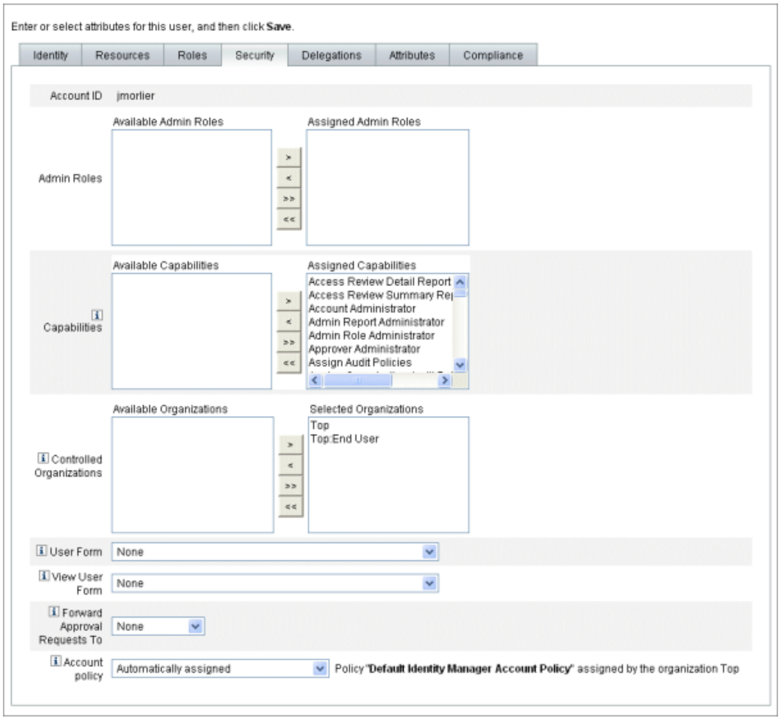
If a new user account needs to be created, see "Creating Users and Working with User Accounts" on page 53.

3 **Specify attributes to establish administrative control.**

Available attributes include:

- **Capabilities**. Select one or more capabilities that should be assigned to this administrator. This information is required. For more information, see "Understanding and Managing Capabilities" on page 198.
- **Controlled Organizations**. Select one or more organizations that should be assigned to the administrator. The administrator will control objects in the assigned organization and in any organizations beneath it in the hierarchy. This information is required. For more information, see "Understanding Waveset Organizations" on page 190.
- **User Form**. Select the user form that this administrator will use when creating and editing Waveset 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 current pending approval requests to that user. This administrator setting also can be set from the Approvals page.

- **Delegate Work Items To**. If available, use this option to specify delegations for this user account. You can specify the administrator's manager, one or more selected users, or use a delegate approvers rule.



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

Account ID jmorlier

Admin Roles
Available Admin Roles
Assigned Admin Roles

Capabilities
Available Capabilities
Assigned Capabilities
Access Review Detail Report
Access Review Summary Re
Account Administrator
Admin Report Administrator
Admin Role Administrator
Approver Administrator
Assign Audit Policies

Controlled Organizations
Available Organizations
Selected Organizations
Top
Top:End User

User Form: None

View User Form: None

Forward Approval Requests To: None

Account policy: Automatically assigned — Policy "**Default Identity Manager Account Policy**" assigned by the organization Top

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 Waveset users. Any form set at the administrator level overrides the form set here. If no form is selected for the administrator or the organization, Waveset inherits the form selected for the parent organization. If no form is set there, Waveset 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).

"Understanding and Managing Capabilities" on page 198 describes built-in Waveset 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 using these forms:

- **Change User Password form**. There are two ways to open this form:
  - Click Accounts in the menu. The User List opens. Select an administrator and then, in the User Actions list, select Change Password. The Change User Password page opens.
  - Click Passwords in the menu. The Change User Password page opens.
- **Tabbed User form**. Click Accounts in the menu. The User List opens. Select an administrator, and then, in the User Actions menu, select Edit. The "Edit User" page (Tabbed User Form) opens. On the Identity form tab, type a new password in the Password and Confirm Password fields.

An administrator can change his own password from the Passwords area. Click Passwords in the menu, then click Change My Password.

Note – The Waveset 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

Waveset can be configured to prompt administrators for a password before processing certain account changes. If authentication fails, then the account changes will be cancelled.

There are three forms that administrators can use to change user passwords. These are the Tabbed User form, the Change User Password form, and the Reset User Password form. To ensure that administrators are required to enter their password before Waveset processes user account changes, be sure to update all three forms.

▼ To Enable the Challenge Option for Tabbed User Forms

To require a password challenge on the Tabbed User form, follow these steps.

1. **In the Administrator interface, open the Waveset debug page ("The Waveset Debug Page" on page 42) by typing the following URL into your browser. (You must have the Debug capability to open this page.)**

   `http://`*<AppServerHost>*`:`*<Port>*`/idm/debug/session.jsp`

   The System Settings page (Waveset debug page) opens.

2. **Find the List Objects button, select UserForm from the drop-down menu, then click the ListObjects button.**

   The List Objects of type: UserForm page opens.

3. **Locate the copy of the Tabbed User Form that you have in production and click edit. (The Tabbed User Form distributed with Waveset is a template and should not be modified.)**

4. **Add the following code snippet inside the `<Form>` element:**

```
<Properties>
  <Property name='RequiresChallenge'>
    <List>
      <String>password</String>
      <String>email</String>
      <String>fullname</String>
    </List>
  </Property>
</Properties>
```

   The property value is a list that can contain one or more of the following user view attribute names:

   - `applications`
   - `adminRoles`
   - `assignedLhPolicy`
   - `capabilities`
   - `controlledOrganizations`
   - `email`
   - `firstname`
   - `fullname`
   - `lastname`
   - `organization`

- `password`
- `resources`
- `roles`

5 **Save your changes.**

▼ To Enable the Challenge Option for Change User Password and Reset User Password Forms

To require a password challenge on the Change User Password and Reset User Password forms, follow these steps:

1 **In the Administrator interface, open the Waveset debug page ("The Waveset Debug Page" on page 42) by typing the following URL into your browser. (You must have the Debug capability to open this page.)**

`http://<AppServerHost>:<Port>/idm/debug/session.jsp`

The System Settings page (Waveset debug page) opens.

2 **Locate the List Objects button, select UserForm from the drop-down menu, then click the ListObjects button.**

The List Objects of type: UserForm page opens.

3 **Locate the copy of the Change Password User Form that you have in production and click edit. (The Change Password User Form distributed with Waveset is a template and should not be modified.)**

4 **Locate the `<Form>` element, then go to the `<Properties>` element.**

5 **Add the following line inside the `<Properties>` element and save your changes.**

```
<Property name='RequiresChallenge' value='true'/>
```

6 **Repeat steps 3 - 5, except edit the copy of the "Reset User Password Form" that you have in production.**

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 the "Setting Account Authentication Policies" on page 83 section in Chapter 3, "User and Account Management."

Customizing Administrator Name Display in the Administrator Interface

You can display an Waveset administrator by attribute (such as `email` or `fullname`) rather than by accountId in some Waveset Administrator interface pages and areas.

For example, you can display Waveset administrators by attribute in the following areas:

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

To configure Waveset 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 the following attribute name to `UserUIconfig`:

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

Understanding Waveset Organizations

Organizations allow you to:

- Logically and securely manage user accounts and administrators
- Limit access to resources, applications, roles, and other Waveset 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 Waveset users (including administrators) are *statically assigned* to one organization. Users also can be *dynamically assigned* to additional organizations.

Waveset administrators are additionally assigned to *control* organizations.

Creating Organizations

▼ To Create an Organization

Create organizations in the Waveset Accounts area.

1 **In the Administrator interface, click Accounts in the menu bar.**

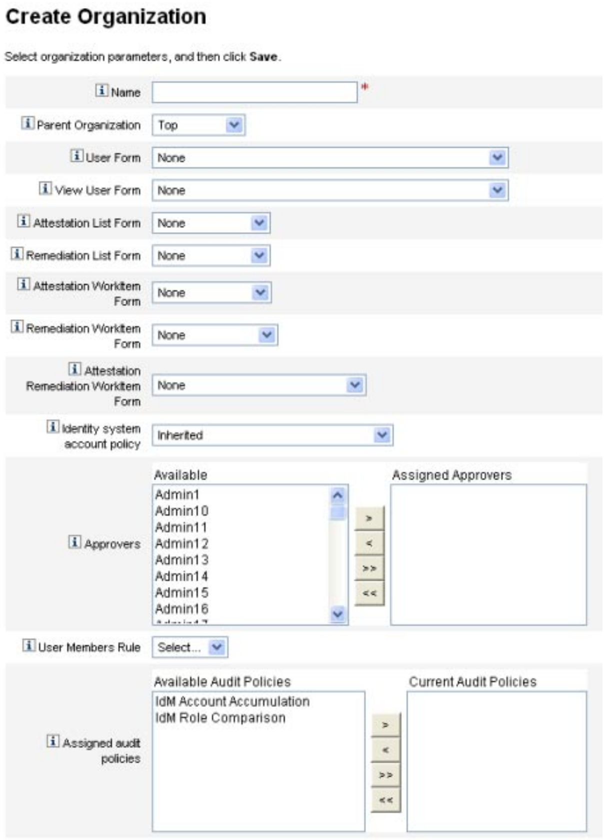
The User List page opens.

2 **In the New Actions menu, select New Organization.**

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

Figure 6–1 illustrates the Create Organization page.

FIGURE 6–1 Create Organization Page



Create Organization

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

Name	*
Parent Organization	Top
User Form	None
View User Form	None
Attestation List Form	None
Remediation List Form	None
Attestation WorkItem Form	None
Remediation WorkItem Form	None
Attestation Remediation WorkItem Form	None
Identity system account policy	Inherited
Approvers	Available: Admin1 Admin10 Admin11 Admin12 Admin13 Admin14 Admin15 Admin16 Assigned Approvers:
User Members Rule	Select...
Assigned audit policies	Available Audit Policies: IdM Account Accumulation IdM Role Comparison Current Audit Policies:

Assigning Users to Organizations

Each user is a static member of one organization, and can be a dynamic member of more than one organization.

You define organizational memberships using either of the following methods:

- **Direct (static) assignment**. Select the Identity form tab on the Create User page or Edit User page to assign users directly to an organization. A user must be directly assigned to one organization.
- **Rule-driven (dynamic) assignment**. Use a User Members Rule that is assigned to an organization to assign users to that organization. The rule, when evaluated, returns a set of member users.

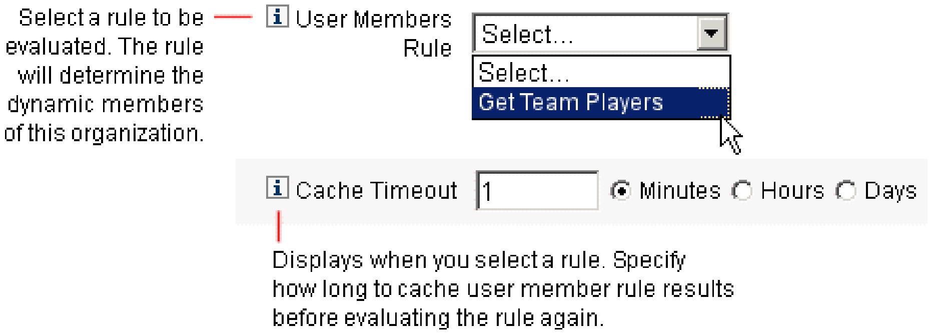
Waveset evaluates the User Members Rule when:

- 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 Members Rule
- Requesting access to a user, provided that the current administrator controls an organization with a User Members Rule

---

Note – For more information about creating and working with rules in Waveset, see Chapter 4, “Working with Rules,” in *Oracle Waveset 8.1.1 Deployment Reference*.

Select a User Members Rule from the User Members Rule menu on the Create Organization page. The following figure shows an example User Members Rule.



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

User Members Rule: Select...

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.

The following example illustrates the syntax for a sample User Members Rule used to dynamically control an organization’s user membership.

Note –

Before creating a User Members Rule, you should be aware of the following:

- For a rule to appear in the User Members Rule option box, its `authType` must be set as `authType=’UserMembersRule’`.
- The context is the currently authenticated Waveset user’s session.
- The defined variable `(defvar) Team players` gets the distinguished name (dn) for each user that is a member of the Windows Active Directory organization unit (ou) `Pro Ball Team`.

- For each user found, the append logic will concatenate the dn of each member user of the `Pro Ball Team` ou with the name of the Waveset Resource prefixed by a colon (as in `:smith-AD`).
- The results returned will be a list of dn's concatenated with the Waveset resource name in the format *dn*`:smith-AD`.

EXAMPLE 6–1 Sample User Members Rule

```
<Rule name='Get Team Players' authType='UserMembersRule'>
  <defvar name='Team 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>singleton-AD</s>
      <map>
        <s>searchContext</s>
        <s>OU=Pro Ball Team,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>:sampson-AD</s>
    </concat>
    </append>
  </dolist>
    <ref>player names</ref>
  </block>
   </defvar>
    <ref>Team players</ref>
</Rule>
```

Note – You can configure several properties in `Waveset. properties` to control the rule-driven User Members list cache, which can affect memory and performance. For information, see "Tracing Rule-Driven Members Caches" in *Oracle Waveset 8.1.1 System Administrator's Guide*.

Assigning Organization Control

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

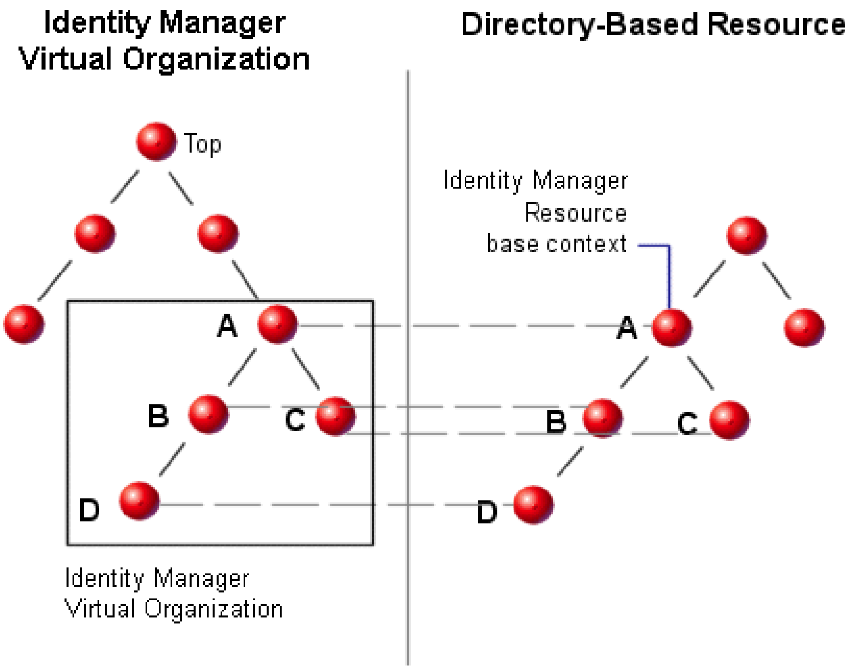
You can also assign administrative control of organizations by assigning one or more admin roles, from the Admin Roles field.

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 topmost 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. This structure is illustrated in Figure 6–2.

FIGURE 6–2 Waveset Virtual Organization


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

Directory junctions can be spliced into the existing Waveset 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 Waveset 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 Waveset objects (such as users, resource, and roles) members of, and available to, a virtual organization in the same way as an Waveset organization.

Setting Up Directory Junctions

This section describes how to set up a directory junction.

▼ To Set Up a Directory Junction

1. **In the Administrator interface, select Accounts in the menu bar.**

   The User List page opens.

2. **Select an Waveset organization in the Accounts list.**

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

3. **In the New Actions menu, select New Directory Junction.**

   Waveset opens the Create Directory Junction page.

4. **Use the options on the Create Directory Junction page to set up the virtual organization.**

   These options include:

   - **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.
   - **Waveset 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 Waveset organization only**. Deletes the Waveset directory junction only.
- **Delete the Waveset organization and the resource container**. Deletes the Waveset directory junction and the corresponding organization on the native resource.

Select an option, and then click Delete.

Understanding and Managing Capabilities

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

Not all Waveset users need capabilities assigned. Only those users who will perform one or more administrative actions through Waveset will require capabilities. 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 Waveset Administrator Interface you can access.

All Waveset administrative users can access certain areas of Waveset, 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)

Note – A list of Waveset's default task-based and functional capabilities (with definitions) is included in Appendix D, "Capabilities Definitions." This appendix also lists the tabs and subtabs that may be accessed with each task-based capability.

Capabilities Categories

Waveset 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 Waveset 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

This section describes how to create, edit, assign, and rename capabilities. These tasks are performed using the Capabilities page.

View the Capabilities Page

The Capabilities page is found under the Security tab.

▼ To Open the Capabilities Page

1. **In the Administrator interface, click Security in the top menu.**

2. **Click Capabilities in the secondary menu.**

   The Capabilities page opens and shows a list of Waveset capabilities.

Create a Capability

Use the following procedure to create a capability. To *clone* a capability, see "Save and Rename a Capability" on page 200.

▼ To Create a Capability

1. **In the Administrator interface, click Security in the top menu.**

2. **Click Capabilities in the secondary menu.**

   The Capabilities page opens and shows a list of Waveset capabilities.

3. **Click New.**

   The Create Capability page opens.

4. **Complete the form as follows:**

   a. **Name the new capability.**

   b. **In the Capabilities section, use the arrow buttons to move the capabilities that should be assigned to users into the Assigned Capabilities box.**

   c. **In the Assigners box, select one or more users that will be allowed to assign this capability to other users.**

      - If no users are selected, the only user who can assign this capability is the one that created the capability.
      - If the user who created the capability does not have the Assign User Capability capability assigned, then you must select one or more users to ensure that at least one user can assign the capability to another user.

   d. **In the Organizations box, select one or more organizations to which this capability will be available.**

e. **Click Save.**

Note – The set of users from which you can make assigner selections are those who have been assigned the Assign Capability right.

Edit a Capability

You can edit a non-protected capability.

▼ To Edit a Non-Protected Capability

1. **In the Administrator interface, click Security in the top menu.**

2. **Click Capabilities in the secondary menu.**

   The Capabilities page opens and shows a list of Waveset capabilities.

3. **Right-click the capability in the list, and then select Edit. The Edit Capability page opens.**

4. **Make your changes and click Save.**

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

Save and Rename a Capability

You can create a new capability by saving an existing capability with a new name. This process is known as *cloning* the capability.

▼ To Clone a Capability

1. **In the Administrator interface, click Security in the top menu.**

2. **Click Capabilities in the secondary menu.**

   The Capabilities page opens and shows a list of Waveset capabilities.

3. **Right-click the capability in the list, and then select Save As.**

   A dialog box opens and asks you to type a name for the new capability.

4. **Type a name and click OK.**

   You can now edit the new capability.

Assigning Capabilities to Users

Use the Create User page ("Creating Users and Working with User Accounts" on page 53) or the Edit User page ("Editing Users" on page 58) to assign capabilities to users. You can also assign capabilities to a user by assigning an administrator role, which you set up through the Security area in the interface. See "Understanding and Managing Admin Roles" on page 201 for more information.

Note – A list of Waveset's default task-based and functional capabilities (with definitions) is included in Appendix D, "Capabilities Definitions." This appendix also lists the tabs and subtabs that may be accessed with each task-based capability.

Understanding and Managing Admin Roles

Admin Roles define two things: a set of capabilities and a scope of control. (The term scope of control refers to one or more managed organizations.) Once defined, admin roles can then be assigned to one or more administrators.

Note – Do not confuse *roles* with *admin-roles*. Roles are used to manage end-users' access to external resources, whereas admin-roles are primarily used to manage Waveset administrator access to Waveset objects.

The information presented in this section is limited to admin roles. For information about roles, see "Understanding and Managing Roles" on page 109.

Multiple admin roles can be assigned to a single administrator. This enables an administrator to have one set of capabilities in one scope of control, and a different set of capabilities in another scope of control. For example, one admin role might grant the administrator the right to create and edit users for the controlled organizations specified in that admin role. A second admin role assigned to the same administrator, however, might grant only the "change users' passwords" right in a separate set of controlled organizations as defined in that admin role.

Admin roles enable the reuse of capabilities and scope-of-control pairings. Admin roles also simplify the management of administrator privileges across a large number of users. Instead of directly assigning capabilities and controlled organizations to individual users, admin roles should be used to grant administrator privileges.

The assignment of capabilities or organizations (or both) to an admin role can be either direct or dynamic (indirect).

- **Direct**. Using this method, capabilities and/or controlled organizations are explicitly assigned to the admin role. For example, an admin role might be assigned the User Report Administrator capability and the controlled organization Top.
- **Dynamic** (*indirect*). This method uses rules to assign capabilities and controlled organizations. Rules are evaluated each time an administrator assigned the admin role logs in. Once an administrator is authenticated, rules dynamically determine which set of capabilities and/or controlled organizations are assigned.

  For example, when a user logs in:

  - If his Active Directory (AD) user title is *manager*, then the capabilities rule might return Account Administrator as the capability to be assigned.
  - If his Active Directory (AD) user department is *marketing*, then the controlled organizations rule might return Marketing as the controlled organization to be assigned.

The dynamic assignment of admin roles to users can be enabled or disabled for each login interface (for example, the User interface or Administrator interface). To do this, set the following system configuration attribute to `true` or `false`:

```
security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface
```

The default for all interfaces is `false`.

For instructions on editing the system configuration object, see "Editing Waveset Configuration Objects" on page 108.

Admin Role Rules

Waveset provides sample rules that you can use to create rules for Admin Roles. These rules are available in the Waveset installation directory in `sample/adminRoleRules.xml`.

Table 6–1 provides the rule names and the `authType` you must specify for each rule.

TABLE 6–1 Admin Role Sample Rules

Rule Name	`authType`
Controlled Organizations Rule	`ControlledOrganizationsRule`
Capabilities Rule	`CapabilitiesRule`
User Is Assigned Admin Role Rule	`UserIsAssignedAdminRoleRule`

Note – For information about the sample rules provided for service provider users admin roles, see “Delegated Administration for Service Provider Users” on page 502 in Chapter Chapter 17, “Service Provider Administration.”

The User Admin Role

Waveset includes a built-in admin role, named User Admin Role. By default, it has no assigned capabilities or controlled organization assignments. It cannot be deleted. This admin role is implicitly assigned to all users (end-users and administrators) at login time, regardless of the interface they log in to (for example, user, administrator, console, or Identity Manager IDE).

Note – For information about creating an admin role for service provider users, see “Delegated Administration for Service Provider Users” on page 502 in ChapterChapter 17, “Service Provider Administration.”

You can edit the User Admin Role through the Administrator interface (select Security, 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.

There may be cases, however, where a user should have specific access to one or more objects outside of (and potentially inside of) workflows. In these cases, using rules to dynamically assign capabilities and controlled organizations allows for fine-grain authorization to those objects.

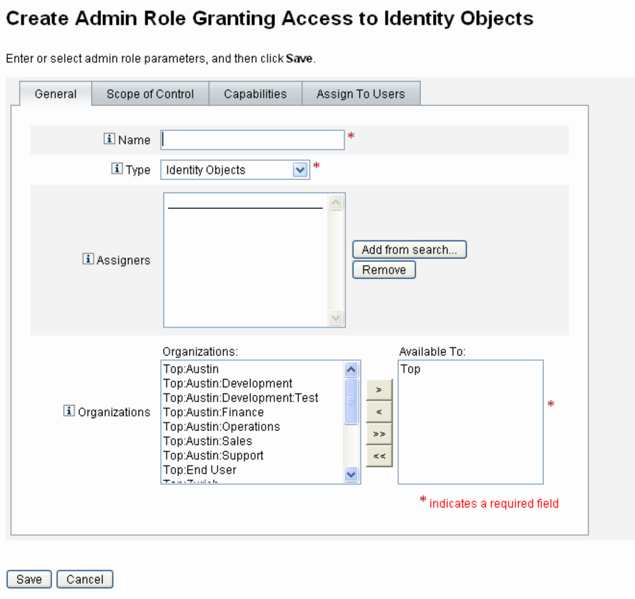
Creating and Editing Admin Roles

To create or edit an admin role, you must be assigned the Admin Role Administrator capability.

To access admin roles in the Administrator interface, click Security, and then click the Admin Roles tab. The Admin Roles list page allows you to create, edit, and delete admin roles for Waveset users and for service provider users.

To edit an existing admin role, click a name in the list. Click New to create an admin role. Waveset displays the Create Admin Role options (illustrated in Figure 6–3). The Create Admin Role view presents four tabs that you use to specify the general attributes, capabilities, and scope of the new admin role, as well as assignments of the role to users.

FIGURE 6–3 Admin Role Create Page: General Tab



Create Admin Role Granting Access to Identity Objects

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

General | Scope of Control | Capabilities | Assign To Users

Name: *

Type: Identity Objects *

Assigners:

Organizations:

Organizations:
Top:Austin
Top:Austin:Development
Top:Austin:Development:Test
Top:Austin:Finance
Top:Austin:Operations
Top:Austin:Sales
Top:Austin:Support
Top:End User

Available To:
Top *

* indicates a required field

General Tab

Use the General tab of the create admin role or edit admin role view to specify the following basic characteristics of the admin role:

- **Name**. A unique name for this admin role.

  For example, you might create the Finance Admin Role for users who will have administrative capabilities for users in the Finance department (or organization).

- **Type**. Select either Identity Objects or Service Provider Users for the type. This field is required.

  Select Identity Objects if you are creating an admin role for Waveset users (or objects). Select Service Provider Users if you are creating the admin role to grant access to service provider users.

Note – For information about creating an admin role to grant access to service provider users, see "Delegated Administration for Service Provider Users" on page 502 in Chapter Chapter 17, "Service Provider Administration."

- **Assigners**. Select or search for users that will be allowed to assign this admin role to other users. The set of users from which you can make selections includes those who have been assigned the Assign Capability right.

  If no users are selected, the only user who will be able to assign the admin role is the one that created it. If the user who created the admin role does not have the Assign User Capabilities capability assigned, then select one or more users as Assigners to ensure that at least one user can assign the admin role to another user.
- **Organizations**. Select one or more organizations to which this admin role will be available. This field is required.

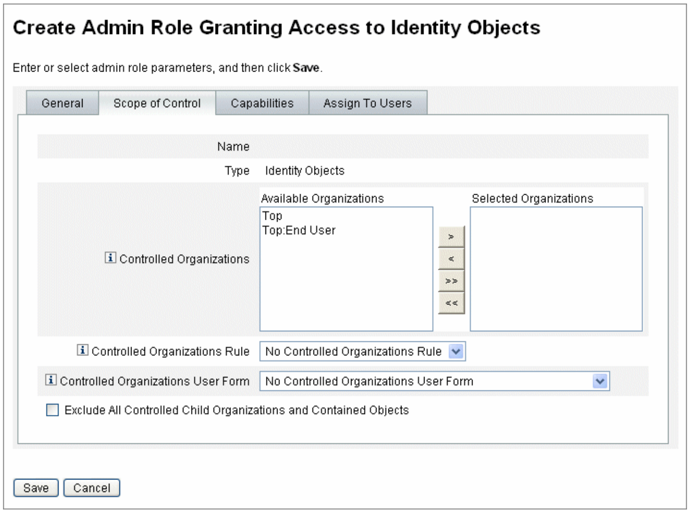
  The administrator can manage objects in the assigned organization and in any organizations below that organization in the hierarchy.

Scope of Control

Waveset allows you to control which users are within an end user's scope of control.

Use the Scope of Control tab (shown in Figure 6–4) to specify organizations that members of this organization can manage, or to specify the rule that determines the organizations to be managed by users of the admin role, and to select the user form for the admin role.

FIGURE 6–4 Create Admin Role: Scope of Control



Create Admin Role Granting Access to Identity Objects

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

Name

Type Identity Objects

Controlled Organizations Rule: No Controlled Organizations Rule

Controlled Organizations User Form: No Controlled Organizations User Form

□ Exclude All Controlled Child Organizations and Contained Objects

- **Controlled Organizations**. Select from the Available Organizations list the organizations that this admin role has the rights to manage.
- **Controlled Organizations Rule**. Select a rule that will be evaluated, at user login, to zero or more organizations to be controlled by a user assigned this admin role. The selected rule must have the `ControlledOrganizationsRule` authType. By default, no controlled organization rule is selected.

  You can use the `EndUserControlledOrganizations` rule to define whatever logic is necessary to ensure the right set of users are available for delegating, based on your organizational needs.

  If you want the scoped list of users to be the same for administrators, whether they are logged into the Administrator interface or the End User interface, you must change the `EndUserControlledOrganizations` rule.

  Modify the rule to first check whether the authenticating user is an administrator, and then configure the following:

  - If the user is not an administrator, return the set of organizations that should be controlled by an end user, such as the user’s own organization (for example, `waveset.organization`).
  - If the user is an administrator, do not return any organizations so the user only controls organizations that are assigned because that user is an administrator.

    For example:

    ```
    <Rule protectedFromDelete=’true’
          authType=’EndUserControlledOrganizationsRule’
          id=’#ID#End User Controlled Organizations’
          name=’End User Controlled Organizations’>
    ```

```
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type=’ObjectGroup’ id=’#ID#Top’ name=’Top’/>
  </MemberObjectGroups>
</Rule>
```

- If the user or administrator belongs to a dynamic organization, they are not returned in search results.

  However, you can create a rule to return users in dynamic organizations. Change the following sample rule by adding a new attribute to the Waveset user schema definition that is defined in the `Idm Schema Configuration` object, import that object, and then restart the Waveset server.

```
        <IDMAttributeConfigurations>
            ...
            <IDMAttributeConfiguration name=’region’
                                       syntax=’STRING’
                                       description=’region of the country’/>
        </IDMAttributeConfigurations>

        <IDMObjectClassConfigurations>
            ...
            <IDMObjectClassConfiguration name=’User’
                                         extends=’Principal’
                                           description=’User description’>
                ...
                <IDMObjectClassAttributeConfiguration name=’region’
                                                      queryable=’true’/>
            </IDMObjectClassConfiguration>
        </IDMObjectClassConfigurations>

Next, import the following Waveset objects:

<!-- User member rule that will include all users whose region attribute
matches the region organization display name -->

<Rule name="Region User Member Rule" authType="UserMembersRule">
  <Description>User Member Rule</Description>
  <list>
    <new class=’com.waveset.object.AttributeCondition’>
      <s>region</s>
      <s>equals</s>
      <ref>userMemberRuleOrganizationDisplayName</ref>
    </new>
  </list>
  <MemberObjectGroups>
    <ObjectRef type="ObjectGroup" id="#ID#All" name="All"/>
  </MemberObjectGroups>
</Rule>

<!-- North & South Region organizations with user member rule assigned -->

<ObjectGroup id='#ID#North Region' name='North Region'
displayName='North Region'> <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<ObjectGroup id='#ID#South Region' name='South Region'
displayName='South Region'>  <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- Organization containing all employees -->

<ObjectGroup id='#ID#Employees' name='Employees' displayName='Employees'>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- End user controlled organization rule that give each user control
of the regional organization they are a member of -->

<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'
      primaryObjectClass='Rule'>
  <switch>
    <ref>waveset.attributes.region</ref>
    <case>
      <s>North Region</s>
      <s>North Region</s>
    </case>
    <case>
      <s>South Region</s>
      <s>South Region</s>
    </case>
    <case>
      <s>East Region</s>
      <s>East Region</s>
    </case>
    <case>
      <s>West Region</s>
      <s>West Region</s>
    </case>
  </switch>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>

<!-- 4 employees (2 in North and 2 in South region) -->

<User name='emp1' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee One'/>
  <Attribute name='lastname' type='string' value='One'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp2' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Two'/>
  <Attribute name='lastname' type='string' value='Two'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp4' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Four'/>
  <Attribute name='lastname' type='string' value='Four'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp5' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Five'/>
  <Attribute name='lastname' type='string' value='Five'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>
```

Next, log in through the Waveset End User interface as emp1, who is in the North region. Select Delegations → New. Change the search → provide criteria to **Starts with**, change the value to **emp**, and choose Find. This selection should return emp2 in the list of available users.

- **Controlled Organizations User Form**. Select a user form that a user who is assigned this admin role will use when he creates or edits users who are members of this admin role's controlled organizations. By default, no Controlled Organizations User Form is selected.

  A user form assigned through an admin role overrides any user form that is inherited from the organization of which the administrator is a member. It does not override a user form that is directly assigned to the admin.

Assigning Capabilities to the Admin Role

Capabilities assigned to the admin role determine what administrative rights users assigned the admin role have. For example, this admin role might be restricted to creating users only for the controlled organizations of the admin role. In that case, you assign the Create User capability.

On the Capabilities tab, select the following options:

- **Capabilities**. These are specific capabilities (administrative rights) that the users of the admin role will have for their controlled organizations. Select one or more capabilities from the list of available capabilities and move them to the Assigned Capabilities list.
- **Capabilities Rule**. Select a rule that when evaluated at user login, will determine the list of zero or more capabilities granted to users assigned the admin role. The selected rule must have the `CapabilitiesRule` authType.

Assigning User Forms to an Admin Role

You can specify a user form to for the members of an admin role. Use the Assign To Users tab on the create admin role or edit admin role view to specify the assignments.

The administrator assigned the admin role will use this user form when creating or editing 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. This user form does not override a user form that is directly assigned to the admin.

The user form that is 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.

The End User Organization

The End User organization provides a convenient way for administrators to make certain objects, such as resource and roles, available to end-users. End-users can view and potentially assign designated objects to themselves (pending an approval process) using the end-user interface ("Logging in to the Waveset End-User Interface" on page 41).

Note – The End User organization was introduced in Waveset Version 7.1.1.

Previously, in order to grant end-users access to Waveset configuration objects, such as Roles, Resources, Tasks, and so on, administrators had to edit configuration objects and use End User Tasks, End User Resources, and End User authTypes.

Going forward, Oracle recommends using the "End User" organization to give end-users access to Waveset configuration objects.

The End User organization is implicitly controlled by all users, and enables them to view several types of objects, including tasks, rules, roles, and resources. Initially, however, the organization has no member objects.

The End User organization is a member of `Top` and cannot have child organizations. In addition, the End User organization is not displayed in the Accounts page list. When editing objects (such as Roles, AdminRoles, Resources, Policy, Tasks, and so on), however, you can make any object available to the End User organization using the Administrator user interface.

When end-users log in to the end-user interface, the following happens:

- End-users are granted control of the `EndUser` organization (`ObjectGroup`).
- Waveset evaluates the built-in End User Controlled Organization rule, which automatically gives the user control of any organization names that are returned by the rule. (This rule was added in Waveset Version 7.1.1. See the "The End User Controlled Organization Rule" on page 212section for more information.)
- End-users are granted rights to the object types specified in the `EndUser` capability.

The End User Controlled Organization Rule

The input argument to the End User Controlled Organization rule is the authenticating user's view. Waveset expects the rule to return one or more organizations that the user logging in to the End User interface will control. Waveset expects the rule to return either a string (for a single organization) or a list (for multiple organizations).

To manage these objects, users need the End User Administrator capability. Users who are assigned the End User Administrator capability can view and modify the contents of the End User Controlled Organization rule. These users can also view and modify the object types specified in the EndUser capability.

The End User Administrator capability is assigned to the Configurator user by default. Any changes made to the list or to organizations returned by the evaluation of the End User Controlled Organization rule will not be reflected dynamically for logged in users. These users must log out and then log in again to see the changes.

If the End User Controlled Organization rule returns an invalid organization (for example, an organization that does not exist in Waveset), the problem will be logged in the System Log. To correct the problem, log in to the Administrator user interface and fix the rule.

Managing Work Items

Some workflow processes generated by tasks in Waveset create action items or *work items*. These work items might be a request for approval or some other action request assigned to an Waveset account.

Waveset groups all work items in the Work Items area of the interface, enabling you to view and respond to all pending requests from one location.

Work Item Types

A work item might be one of the following types:

- **Approvals**. Requests for approvals of new accounts or changes to accounts.
- **Attestations**. Requests to review and approve user entitlements.
- **Remediations**. Requests to remediate or mitigate user account policy violations.
- **Other**. Action item request for other than one of the standard types. This might be an action request generated from a customized workflow.

To view pending work items for each work item type, click Work Items in the menu.

Note – If you are a work item owner with pending work items (or delegated work items), then your Work Items list is displayed when you log into the Waveset User interface.

Working With Work Item Requests

To respond to a work item request, click one of the work item types in the Work Items area of the interface. Select items from the list of requests and then click one of the buttons available to indicate the action you want to take. The work item options vary depending on the work item type.

For more information about responding to requests, see the following topics:

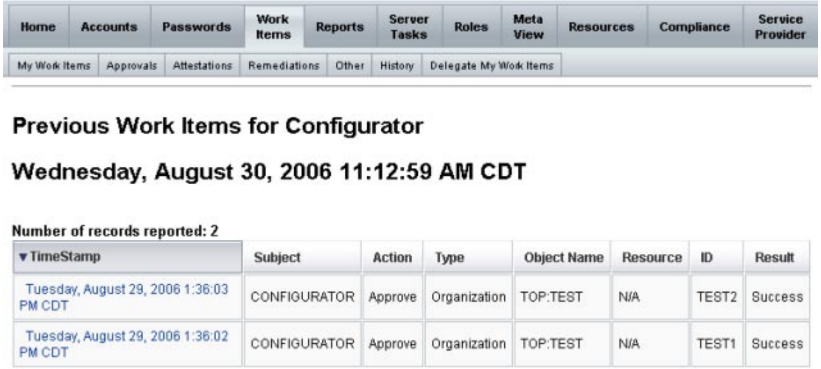
- "Approving User Accounts" on page 217
- "Managing Attestation Duties" on page 455
- "Compliance Violation Remediation and Mitigation" on page 433

Viewing Work Item History

Use the History tab in the Work Items area to view the results of previous work item actions.

Figure 6–5 displays a sample view of Work Item history.

FIGURE 6–5 Work Items History View



Previous Work Items for Configurator

Wednesday, August 30, 2006 11:12:59 AM CDT

Number of records reported: 2

▼TimeStamp	Subject	Action	Type	Object Name	Resource	ID	Result
Tuesday, August 29, 2006 1:36:03 PM CDT	CONFIGURATOR	Approve	Organization	TOP:TEST	N/A	TEST2	Success
Tuesday, August 29, 2006 1:36:02 PM CDT	CONFIGURATOR	Approve	Organization	TOP:TEST	N/A	TEST1	Success

Delegating Work Items

Work item owners can manage work loads by delegating work items to other users for a specified period of time. From the main menu, you can use the Work Items → Delegate My

Work Items page to delegate future work items (such as requests for approval) to one or more users (delegates). Users do not need approver capabilities to be delegates.

Note – The delegation feature applies only to future work items. Existing items (those listed under My Work Items must be selectively forwarded through the forwarding feature.

There are other pages from which you can delegate work items:

- In the Administrator interface, you can delegate work items from the Create User and Edit User pages ("The User Pages (Create/Edit/View)" on page 49). Click the Delegations form tab.
- In the end-user User Interface ("Waveset End-User Interface" on page 38), users can click the Delegations menu item.

Delegates can approve work items on a work item owner's behalf during the effective delegation period. Delegated work items include the name of the delegate.

Any user can create one or more delegations for their future work items. Administrators who can edit a user can also create a delegation on that user's behalf. An administrator cannot, however, delegate to someone that the user cannot delegate to. (With regards to delegations, the administrator's scope of control is the same as the user on whose behalf the delegation is being made.)

Audit Log Entries

Audit log entries list the delegator's name when delegated work items are approved or rejected. Changes to a user's delegate approver information are logged in the detailed changes section of the audit log entry when a user is created or modified.

Viewing Current Delegations

View delegations on the Current Delegations page.

▼ To View Current Delegations

1. **In the Administrator interface, click Work Items in the main menu.**
2. **Click Delegate My Work Items in the secondary menu.**

   Waveset displays the Current Delegations page, where you can view and edit delegations currently in effect.

Viewing Previous Delegations

View previous delegations on the Previous Delegations page.

▼ To view previous delegations

1 **In the Administrator interface, click Work Items in the main menu.**

2 **Click Delegate My Work Items in the secondary menu.**

The Current Delegations page opens.

3 **Click Previous.**

The Previous Delegations page opens. Previously delegated work items can be used to set up new delegations.

Creating Delegations

Create a delegation using the New Delegation page.

▼ To Create a Delegation

1 **In the Administrator interface, click Work Items in the main menu.**

2 **Click Delegate My Work Items.**

The Current Delegations page opens.

3 **Click New.**

The New Delegation page opens.

4 **Complete the form as follows:**

a. **Select a work item type from the Select Work Item Type to Delegate selection list. To delegate all of your work items, select All Work Item Types.**

If you are delegating a role-type, organization, or resource work-item, specify the specific roles, organizations, or resources that should define this delegation by using the arrows to move selections from the Available column to the Selected column.

b. **Delegate Work Items To.**

Select one of the following options:

- **Selected Users**. Select to search for users in your scope of control (by name) to be delegates. If any one of the selected delegates has also delegated his work items, then your future work item requests will be delegated to that delegate's delegates.
- **Select one or more users in the Users Selected area**. Alternatively, click Add from Search to open the search feature and search for users. Click Add to add a found user to the list. To remove a delegate from the list, select it, and then click Remove.
  - **My Manager**. Select to delegate work items to your manager (if assigned).
  - **DelegateWorkItemRule**. Select a rule that returns a list of Waveset user names to which you can delegate the selected work item type.

c. **Start Date. Select the date on which delegation of the work item should start. By default, the day selected begins at 12:01 a.m.**

d. **End Date. Select the date on which delegation of the work item should end. By default, the day selected ends at 11:59 p.m.**

Note – You can select the same start and end dates to delegate work items for a single day.

e. **Click OK to save selections and return to the list of work items awaiting approval.**

Note – After setting up delegation, any work items created during the effective delegation period are added to the delegate's list. If you end a delegation or the delegation time period expires, then the delegated work items are returned to your list. This may result in duplicate work items on your list. However, when you approve or reject one, then the duplicate will be automatically removed from your list.

Delegations to Deleted Users

Waveset works as follows when a user is deleted that owns any pending work items:

- If the pending work items were delegated and the delegator has not been deleted, the pending work items will be returned to the delegator.
- If the pending work items were not delegated, or if the pending work items were delegated and the delegator has been deleted, the delete attempt will fail until the user's pending work items have either been resolved or forwarded to another user.

Ending Delegations

End one or more delegations from the Current Delegations page.

▼ To End One or More Delegations

1. **In the Administrator interface, click Work Items in the main menu.**

2. **Click Delegate My Work Items in the secondary menu.**

   The Current Delegations page opens.

3. **Select one or more delegations to end, and then click End.**

   Waveset removes the selected delegation configurations, and returns any delegated work items of the type selected to your list of pending work items.

Approving User Accounts

When a user is added to the Waveset system, administrators who are assigned as *approvers* for new accounts must validate account creation.

Waveset supports three categories of approval:

- **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.

In addition, if change-approvals are enabled, and changes are made to a role, a change-approval work item is sent to designated role owners.

Waveset supports change-approvals by *Role Definition*. If an administrator changes a role definition, change-approval is needed from a designated role owner. A role owner must approve the work item in order for the change to be made.

Note –

- You can configure Waveset for digitally signed approvals. For instructions see “Configuring Digitally Signed Approvals and Actions” on page 219.
- Administrators who are new to Waveset sometimes confuse the concept of approvals with the similar sounding concept of attestation. While the names sound similar, approvals and attestation take place in different contexts.

  Approvals are concerned with validating new user accounts. When a user is added to Waveset, one or more approvals may be required to validate that the new account is authorized.

  Attestations are concerned with verifying that existing users have only appropriate privileges on appropriate resources. As part of a Periodic Access Review process, an Waveset user (the attestor) may be called upon to certify that another user's account details (that is, the user's assigned resources) are valid and correct. This process is known as attestation.

Setting Up Account Approvers

Setting up account approvers for organization, role, and resource approvals is optional, but recommended. For each category in which approvers are set up, at least one approval 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. You can, however, customize this process to require it.

You can customize workflows by using the Identity Manager IDE to change the flow of approvals, capture account deletions, and capture updates.

For information about the Identity Manager IDE, go to `https://identitymanager.dev.java.net`. For information about workflows, and an illustrated example of altering the approval workflow, see Chapter 1, “Workflow,” in *Oracle Waveset 8.1.1 Deployment Reference*.

Waveset Approvers can either approve or reject an approval request.

Administrators can view and manage pending approvals from the Work Items area of the Waveset interface. From the Work Items page, click **My Work Items** to view pending approvals. Click the **Approvals** tab to manage approvals.

Signing Approvals

To approve a work item using a digital signature, you must first set up the digital signature as described in "Configuring Digitally Signed Approvals and Actions" on page 219.

▼ To Sign an Approval

1. **From the Waveset Administrator interface, select Work Items.**
2. **Click the Approvals tab.**
3. **Select one or more approvals from the list.**
4. **Enter comments for the approval, and then click Approve.**

   Waveset prompts you and asks whether to trust the applet.
5. **Click Always.**

   Waveset displays a dated summary of the approval.
6. **Enter or click Browse to locate the keystore location. (This location is set during the signed-approval configuration, as described in Step 10m of the "To Enable Server-Side Configuration for Signed Approvals Using PKCS12" on page 222 procedure.)**
7. **Enter the keystore password (this password is set during the signed-approval configuration, as described in Step 10l of the procedure "To Enable Server-Side Configuration for Signed Approvals Using PKCS12" on page 222).**
8. **Click Sign to approve the request.**

More Information

Signing Subsequent Approvals

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

Configuring Digitally Signed Approvals and Actions

Use the following information and procedures to set up digital signing. You can digitally sign:

- Approvals (including change-approvals)
- Access review actions
- Remediations for compliance violations

The topics discussed in this section explain the server-side and client-side configuration required to add the certificate and CRL to Waveset for signed approvals.

▼ To Enable Server-Side Configuration for Signed Approvals

1. **Open the system configuration object for editing and set** `security.nonrepudiation.signedApprovals=true`

   For instructions on editing the system configuration object, see "Editing Waveset Configuration Objects" on page 108.

   If you are using PKCS11 you must also set `security.nonrepudiation.defaultKeystoreType=PKCS11`

   If you are using a custom PKCS11 Key provider, you must also set `security.nonrepudiation.defaultPKCS11KeyProvider=`*your provider name*

   Note – Please refer to the following items in the REF kit for more information on when you need to need to write a custom provider:

   ```
   com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)
   REF/transactionsigner/SamplePKCS11KeyProvider
   ```

   The REF (Resource Extension Facility) kit is provided in the `/REF` directory on your product CD or with your install image.

2. **Add your certificate authority's (CA) 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.**

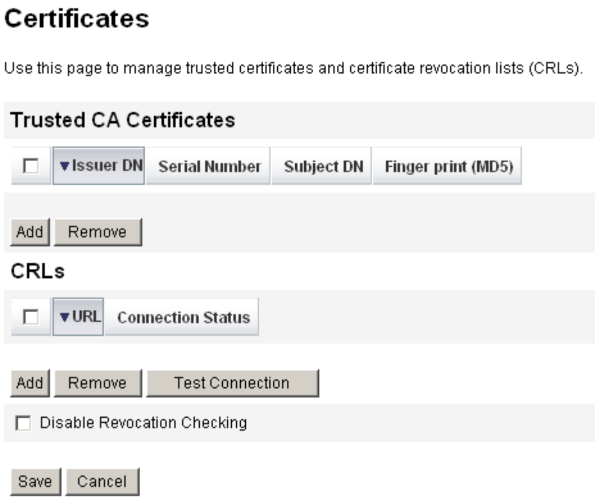
   b. **Select Retrieve the CA certificate or certificate revocation list, and then click Next.**

   c. **Download and save the CA certificate.**

3. **Add the certificate to Waveset as a trusted certificate:**

   a. **From the Administrator interface, select Security, and then select Certificates. Waveset displays the Certificates page.**

FIGURE 6–6 Certificates Page



Certificates

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

Trusted CA Certificates

CRLs

b. **In the Trusted CA Certificates area, click Add. Waveset 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.**

Note –

- 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`/ts2.jar` using jarsigner.**

Note – Refer to `http://download.oracle.com/docs/cd/E17476_01/javase/1.5.0/docs/tooldocs/windows/jarsigner.html` for more information. The `ts2.jar` file provided with Waveset 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.

▼ To Enable Server-Side Configuration for Signed Approvals Using PKCS12

The following configuration information is for signed approvals using PKCS12. 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:

Before You Begin Waveset now requires at least JRE 1.5.

1. **Using Internet Explorer, browse to `http://`*IPAddress*`/certsrv` and 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.**

Note – Note the information that you use in step 10l (password) and 10m (certificate location) of the client-side configuration. You will need this information to sign approvals.

▼ To Enable Client-Side Configuration for Signed Approvals Using PKCS11

If you are using PKCS11 for signed approvals

- **Refer to the following resources in the REF kit for configuration information:**

```
com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)
REF/transactionsigner/SamplePKCS11KeyProvider
```

The REF (Resource Extension Facility) kit is provided in the `/REF` directory on your product CD or with your install image.

Viewing the Transaction Signature

This section describes the procedure for viewing transaction signatures in an Waveset AuditLog report.

▼ To View a Transaction Signature

1 **From the Waveset 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.**

Transaction signature information can include the following:

- Issuer
- Subject
- Certificate serial number
- Message signed
- Signature
- Signature algorithm

Configuring XMLDSIG-Format Signed Approvals

Waveset allows you to add XMLDSIG-format signed approvals, including an RFC 3161-compliant digital timestamp, to the Waveset approval process. When you configure Waveset to use XMLDSIG signed approvals, no changes are visible to approvers unless they view the approval in the audit log. Only the format of the signed approval that is stored in the audit log record is changed.

As with previous signed approvals in Oracle Waveset, an applet is launched on the client machine and the approver is presented with the approval information for signing. They then choose a keystore and a key with which to sign the approval.

After the approver signs the approval, an XMLDSIG document containing the approval data is created. This document is returned to the server which validates the XMLDSIG signed document. If successful, and if RFC 3161 digital timestamps have been configured, a digital timestamp is also generated for this document. The timestamp retrieved from the timestamp authority (TSA) is checked for errors and its certificates are validated. Finally, if successful, Oracle Waveset generates an audit log record that includes the XMLDSIG-format signed approval object in the XML blob column.

Approval Data Format

The format for an XMLDSIG-format approval object is as follows:

```
<XMLSignedData signedContent="...base64 transaction text ...">
   <XMLSignature>
      <TSATimestamp>
         ...The base64 encoded PKCS7 timestamp token returned by the TSA...
      </TSATimestamp
      <Signature>
        <SignedInfo>...XMLDSIG stuff...</SignedInfo>
        <SignatureValue>...base64 signature value</SignatureValue>
        <KeyInfo>...cert info for signer</KeyInfo>
      </Signature>
   </XMLSignature>
</XMLSignedData>
```

where:

- The `base64` approval data consists of the actual approval data text that is presented to the approver in the applet, encoded in `base64` format.
- The `<TSATimestamp>` element contains the `base64` encoded PKCS7 timestamp response from the Timestamp Authority (TSA).
- The entire `<Signature>` comprises the XMLDSIG signature data.

This XMLDSIG document that is stored in the XML column of the audit log approval record.

Installation and Setup

The installation and setup requirements for using XMLDSIG signed approvals are the same as those described in "To Enable Server-Side Configuration for Signed Approvals" on page 220, with one additional step. You must sign the `xmlsec-1.4.2.jar` file in addition to signing the `ts2.jar` file.

Approval Configuration

You can use system configuration attributes to:

- Choose the `SignedData` format or the `XMLSignedData` format. Note that you can configure only one format at a time, although administrators can change this setting as needed.
- Include a digital timestamp retrieved from a configured RFC 3161 Timestamp Authority (TSA).
- Specify a URL, in HTTP only, from which to fetch this timestamp.

To edit these attributes, use the Waveset debug pages to edit the system configuration object. These attributes are all located under `security.nonrepudiation`, along with other signed approval attributes.

The XMLDSIG attributes include:

- `security.nonrepudiation.useXmlDigitalSignatures` is a boolean value that enables XMLDSIG signatures.
- `security.nonrepudiation.timestampXmlDigitalSignatures` is a boolean value that includes RFC 3161 digital timestamps in XMLDSIG signatures.
- `security.nonrepudiation.timestampServerURL` is a string value where the URL points to the HTTP-based TSA from which to fetch timestamps.

Note –

- You must first set the existing `useSignedApprovals` attribute to **`true`** for any of the preceding attributes to have an effect.
- Waveset does not support multiple signatures on one approval or signed approvals for more general provisioning requests.

CHAPTER 7

Data Loading and Synchronization

This chapter provides information and procedures for using Waveset data loading and synchronization features. You will learn how to use Waveset's data synchronization tools (discovery, reconciliation, and synchronization) to keep data current.

The information in this chapter is organized as follows:

For an in-depth explanation of how data loading and synchronization works in Waveset, see Chapter 3, "Data Loading and Synchronization," in *Oracle Waveset 8.1.1 Deployment Guide*.

Data Synchronization Tools: Which to Use?

Waveset provides several tools that can be used to import and synchronize account data. For help selecting the correct tool for a given task, refer to Table 7–1.

Note – For an in-depth explanation of how data loading and synchronization works in Waveset, see Chapter 3, "Data Loading and Synchronization," in *Oracle Waveset 8.1.1 Deployment Guide*
.

TABLE 7–1 Tasks to Use with the Data Synchronization Tools

If you want to	Choose this feature
Initially *pull* resource accounts into Waveset, without viewing before loading	Load from Resource

TABLE 7–1 Tasks to Use with the Data Synchronization Tools *(Continued)*

If you want to	Choose this feature
Initially *pull* resource accounts into Waveset, optionally viewing and editing data before loading	Extract to File, Load from File
Periodically *pull* resource accounts into Waveset, taking action on each account according to configured policy	Reconcile with Resources
Push or *pull* resource account changes into Waveset	Synchronization using Active Sync adapters (multiple resource implementations)

Account Discovery Features

Waveset 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 Waveset.
- **Load from File**. Reads accounts in a file (in CSV or XML format) and loads them into Waveset.
- **Load from Resource**. Combines the other two discovery features, extracting accounts from a resource and loading them directly into Waveset.

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

Note – The pages in this section focus on how to use Waveset's Discovery features. To learn about data loading and synchronization in depth, see Chapter 3, "Data Loading and Synchronization," in *Oracle Waveset 8.1.1 Deployment Guide*.

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 Waveset.

▼ 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. Waveset displays a File Download dialog, in which you may choose to save or view the extracted file.**

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

Load from File

Use this feature to load resource accounts, extracted from a resource through Waveset or from another file source, into Waveset. A file created by the Waveset 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 and saved in comma-separated-value (CSV) format for loading into Waveset.

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 CVS file might look like the following example file entries:

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

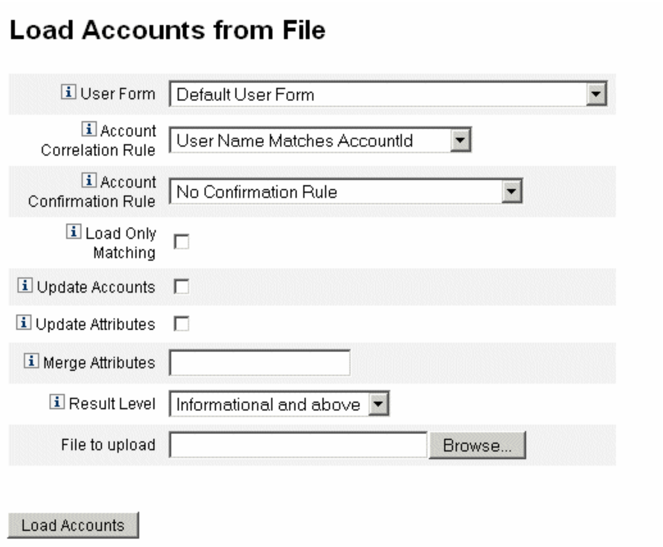
  In this example, note that Jane Doe, the second user, does not have a department. The missing value is represented by adjacent commas (,,).

▼ To Load Accounts

1 **In the Administrator interface, click Accounts in the menu, then click Load from File.**

Waveset displays the Load Accounts from File page.

FIGURE 7–1 Load From File



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	

2 **Use this page to specify the necessary account loading options.**

The options include:

- **User Form**. When load creates an Waveset 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 Waveset 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 Waveset 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 Waveset 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, Waveset 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 Waveset only those accounts that match an existing Waveset user. If you select this option, load will discard any unmatched resource account.
- **Update Attributes**. Select to replace the current Waveset 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.

3 **In the File to Upload field, specify a file to load, and then click Load Accounts.**

Note –

- 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 reuse a file name, then the task instance associated with the latest load process will overwrite any previous task instances.

  "About CSV File Format" on page 229 illustrates the fields and options available in the Load from File screen.

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 Waveset 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 Waveset according to the load options you specify.

▼ To Import Accounts

1. **In the Administrator interface, click Accounts in the menu, then click Load from Resource.**

   The “Load Accounts from Resource” page opens.

2. **Specify the load options on the “Load Accounts from Resource” page.**

   The load options for this page are the same as those on the “Load from File” page (see “Load from File” on page 229).

Account Reconciliation

Use the reconciliation feature to periodically compare resource accounts in Waveset with the accounts actually present on the resources. Reconciliation correlates account data and highlights differences.

Note – The pages in this section focus on how to perform reconciliation tasks using the Administrator interface. To learn about reconciliation in depth, see Chapter 3, “Data Loading and Synchronization,” in *Oracle Waveset 8.1.1 Deployment Guide*.

Reconciliation in a Nutshell

Because reconciliation is designed for ongoing comparison, it has the following characteristics:

- 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 Waveset reconciliation features from the Resources area. The Resources list shows when each resource was last reconciled and its current reconciliation status.

Note – Reconciliation is carried out by Waveset's reconciler component. For information about reconciler configuration settings, see .

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 Waveset) to account attributes.

Editing Reconciliation Policies

▼ To Edit a Reconciliation Policy

1. **In the Administrator interface, click Resources in the menu.**

2. **Select a resource in the Resource List.**

3. **In the Resource Actions list, select Edit Reconciliation Policy.**

   Waveset displays the Edit Reconciliation Policy page, where you can make these policy selections:

   - **Reconciliation Servers**. In a clustered environment, each server may run reconciliation. Specify which Waveset 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 Waveset 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 default policy option to inherit the indicated schedule from a higher-level policy.

  - Clear the Inherit default policy option to specify a schedule. Use the fields provided to establish a recurring schedule, or, to create a custom adjustment to the reconciliation schedule, use a Task Schedule Repetition rule. For information on creating a Task Schedule Repetition rule, see "Using Task Schedule Repetition Rules" on page 240.
- **Incremental Reconciliation Schedule**. If incremental mode reconciliation is enabled, it is performed automatically on a fixed schedule.
  - Select the Inherit default policy option to inherit the schedule from a higher-level policy.
  - Clear the Inherit default policy option to specify a schedule. Use the fields provided to establish a recurring schedule, or, to create a custom adjustment to the reconciliation schedule, use a Task Schedule Repetition rule. For information on creating a Task Schedule Repetition rule, see "Using Task Schedule Repetition Rules" on page 240.

Note – Not all resources support incremental reconciliation.

- **Attribute-level Reconciliation**. Reconciliation can be configured to detect changes made natively (that is, not made through Waveset) 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 Waveset 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 Waveset 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 Waveset 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, Waveset 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) that is 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. Situations are described below. Specify in the Response column any action reconciliation should take.
  - **CONFIRMED**. The expected account exists.

    To be marked as CONFIRMED, the following must be true:
    - Waveset expects the account to exist.
    - The account exists on the resource.
  - **COLLISION**. Two or more Waveset users are assigned the same account on a resource.
  - **DELETED**. The expected account does not exist.

    To be marked as DELETED, the following must be true:
    - Waveset expects the account to exist.
    - The account does not exist on the resource.
  - **FOUND**. The reconciliation process found a matching account on an assigned resource.

    To be marked as FOUND, the following must be true:
    - Waveset expects that the account may or may not exist. (An account may or may not exist on a resource if the resource has been assigned to the user, but has not yet been provisioned.)
    - The account exists on the resource.
  - **MISSING**. No matching account exists on a resource assigned to the user.

    To be marked as MISSING, the following must be true:
    - Waveset expects that the account may or may not exist. (An account may or may not exist on a resource if the resource has been assigned to the user, but has not yet been provisioned.)
    - The account does not exist on the resource.
  - **UNASSIGNED**. The reconciliation process found a matching account on a resource not assigned to the user.

    To be marked as UNASSIGNED, the following must be true:
    - Waveset does not expect the account to exist. (Waveset does not expect an account to exist if that resource is not assigned to the user.)
    - The account exists on the resource.
  - **UNMATCHED**. The resource account does not match any users.
  - **DISPUTED**. The resource account matches more than one user.

    Select from one of these response options (available options vary by situation):
    - **Create new Waveset 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 Waveset 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 Waveset user and Unlink resource account from Waveset user**. Adds or removes the resource account assignment to or from the user. No form processing is performed.
  - **Do nothing**. Select this option if you do not want reconciliation to perform repairs.

    You can manually repair any account situation discovered by reconciliation. In the menu click Resources → Examine Account Index. From there you can browse the recorded situation for all accounts which have been reconciled. Right-click on an account and you will see a list of valid repair options. See "Examining the Account Index" on page 239 for more information.

- **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.
- **Explain Situation**. If enabled, reconciliation will record additional information explaining how it classified account situations. By default, this option is disabled. Recording explanations will cause the reconciliation process to run longer.
- **Error Limit**. If enabled, reconciliation will automatically terminate once the specified number of errors have occurred during processing. A value of 0 indicates that there is no limit on errors. Deselect the Inherit default policy option to display the Maximum errors allowed field and enter a value.
- **Maximum Natively Removed Accounts**. This option is a safeguard that evaluates the number of missing accounts on the resource and, if a threshold is exceeded, prevents the reconciler from unlinking them.

  To enable this feature, clear the Inherit default policy checkbox and specify a percentage in the Maximum natively removed accounts allowed field. The threshold must be set to a whole percentage from 0 to 100. (0 turns this feature off.)

  If the percentage of removed accounts exceeds the threshold, reconciliation continues all processing not related to the missing accounts and completes with an error.

Click Save to save policy changes.

Starting Reconciliation

This section describes two options for starting reconciliation tasks:

- Running Reconciliation at scheduled intervals
- Immediate reconciliation

▼ To Run Reconciliation at Regular Intervals

1. **Open the Edit Reconciliation Policy page as described in "Editing Reconciliation Policies" on page 233.**

2. **Specify the reconciliation schedule parameters.**

   Reconciliation will run according to the parameters you set in the policy.

▼ To Run Reconciliation Immediately

1. **In the Administrator interface, click Resources in the menu.**

2. **Choose a resource in the Resource List.**

3. **Choose an option from the Resource Actions list.**

   The options include:

   - 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.

▼ To Cancel Reconciliation

1. **In the Administrator interface, click Resources in the menu.**

2. **Choose the resource in the Resource List for which you want to cancel reconciliation.**

3. **Locate the Resource Actions list and select Cancel Reconciliation.**

Viewing Reconciliation Status

There are two main ways to view reconciliation status. To view detailed reconciliation status, open the Reconciliation Summary Results page for a specific resource. Limited reconciliation status is also available directly in the Resource List.

▼ To View Detailed Reconciliation Status

View detailed reconciliation status using the Reconciliation Summary Results page.

1 **In the Administrator interface, click Resources in the menu.**

2 **Select the resource in the Resource List for which you want to view reconciliation status.**

3 **Locate the Resource Actions list and select View Reconciliation Status.**

The Reconciliation Summary Results page for the resource opens.

▼ To View Reconciliation Status in the Resource List

You can also view Reconciliation status from the Resource List.

1 **Open the Administrator interface.**

2 **Click Resources in the main menu.**

The **Status** column reports the following reconciliation status conditions:

- **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 status changes. (The information does not automatically refresh.)

Working with the Account Index

The Account Index records the last known state of each resource account known to Waveset. It is primarily maintained by reconciliation, but other Waveset functions will also update the Account Index, as needed.

Discovery tools do not update the Account Index.

▼ To Search the Account Index

Search the account index to view the last known state of a given resource account.

1 **In the Administrator interface, click Resources in the menu.**

2 Select the resource in the Resource List for which you want to search the account index.

3 Locate the Resource Actions list and select Search Account Index.

The Search Account Index page opens.

4 Select a search type, and then enter or select search attributes.

- **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.

5 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 Waveset user accounts and optionally reconcile them on a per-user basis.

▼ To Examine the Account Index

1 In the Administrator interface, click Resources in the menu.

2 Click Examine Account Index in the secondary menu.

The Examine Account Index page opens.

The table displays all of the resource accounts that Waveset knows about (whether or not an Waveset user owns the account). This information is grouped by resource or by Waveset 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. Waveset 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 Waveset knows about.

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. Right-click on an account and you will see a list of valid repair options. You can also view account details or choose to reconcile that one account.

Working with Users

To work with Waveset users, select the Group by user index view. In this view, Waveset users and organizations are displayed in a hierarchy similar to the Accounts List page. To see accounts currently assigned to a user in Waveset, 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 Waveset 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.

Using Task Schedule Repetition Rules

Use Task Schedule Repetition Rules to make adjustments to a reconciliation schedule. For example, if you want to push reconciliations scheduled for Saturday to the following Monday, use a Task Schedule Repetition Rule.

Task Schedule Repetition Rules can be used to adjust schedules for both full and incremental reconciliations.

For information on how to select Task Schedule Repetition rules, see "Editing Reconciliation Policies" on page 233.

How Reconciliation Run Times are Scheduled

Upon completing a reconciliation job, the reconciler component checks for its next scheduled run time.

First, the reconciler looks at the default schedule to obtain its next run time. Next, the reconciler runs all applicable Task Schedule Repetition Rules to see if schedule adjustments needs to be made. If an adjustment is needed, the rule schedule overrides the default schedule for that reconciliation.

Note – Task Schedule Repetition Rules cannot overwrite the default schedule. They can only override scheduled start times on a per-job basis.

▼ To View the Accept All Dates Sample Rule

This section describes the built-in Accept All Dates sample rule.

1. **In a text editor, open** `ReconRules.xml`**, which is located in Waveset's** `sample` **directory.**

2. **Search for the rule named** `SCHEDULING_RULE_ACCEPT_ALL_DATES`**.**

   In order for a rule to be listed in the TaskSchedule Repetition Rule drop-down menu (on the Edit Reconciliation Policy page), the rule's `subtype` attribute must be set to `SUBTYPE_TASKSCHEDULE_REPETITION_RULE`:

```
<Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
```

   As noted previously, Task Schedule Repetition rules can modify the default reconciliation schedule.

   The variable `calculatedNextDate` can either accept the next date, which is calculated in the default manner, or return a different date. As it is written in the sample rule, `calculatedNextDate` unconditionally accepts the default date, as shown in the following excerpt:

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

   To create a custom schedule, replace the rule logic in between the `<block>` elements. For example, to change the reconciliation start time to 10:00 AM on Saturdays, include the following JavaScript in between the `<block>` elements:

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

    // Test to see if this task is scheduled for a Saturday
    // (Note that 6 is used to denote Saturday in JavaScript)
    if(calculatedNextDate.getDay() == 6) {
      // If so, set the time to 10:00:00
      calculatedNextDate.setHours(10);
      calculatedNextDate.setMinutes(0);
      calculatedNextDate.setSeconds(0);
    }
    // Return the modified date
    calculatedNextDate;
  </script>
</block>
```

   In "To View the Accept All Dates Sample Rule" on page 241, `calculatedNextDate` is initially set to the default scheduled time. If the next scheduled run date is a Saturday, then the rule schedules reconciliation to start at 10:00. If the next scheduled run date is not a Saturday, "To View the Accept All Dates Sample Rule" on page 241 returns `calculatedNextDate` without making any time adjustments, and the default schedule is used.

For more information about creating custom rules for use in Waveset, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.

Active Sync Adapters

The Waveset Active Sync feature allows information that is stored in an *authoritative external resource* (such as an application or database) to synchronize with Waveset user data. Configuring synchronization for an Waveset resource enables it to *listen* or poll for changes to the authoritative resource.

You can configure how resource attribute changes are flowed into Waveset by specifying the Input Form in the resource's synchronization policy (for the appropriate target object type).

Note – The pages in this chapter focus on how to perform Active Sync tasks using the Administrator interface. To learn about Active Sync in depth, see Chapter 3, "Data Loading and Synchronization," in *Oracle Waveset 8.1.1 Deployment Guide*.

Configuring Synchronization

Waveset uses a synchronization policy to enable synchronization for resources.

▼ To Edit or Configure Synchronization

Each resource has its own synchronization policy. Use the following steps to configure or edit a synchronization policy:

1. **In the Administrator interface, click Resources in the menu.**

2. **Select the resource in the Resource List for which you want to configure synchronization.**

3. **Find the Resource Actions list and select Edit Synchronization Policy.**

   The Edit Synchronization page for the resource opens.

   Specify the following options in the Edit Synchronization Policy page to configure synchronization:

   - **Target Object Type**. Select the type of users to which the policy applies, either Waveset Users or Service Provider Users.

Note – In a Service Provider implementation you must configure a synchronization policy (with Service Provider Users specified as the object type) to enable synchronization of data for those users. For more information about service provider users, see Chapter 17, "Service Provider Administration."

- **Scheduling Settings**. Use this section to specify the start-up method and polling schedule.

  You can specify the following Startup Types:

  - **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.

    Use the Start Date and Start Time options to specify when polling begins. Specify the polling cycles by selecting an interval and entering a value for the interval (seconds, minutes, hours, days, weeks, months).

    Note – If you change the start-up method or polling schedule, you must restart the server for those changes to take effect.

    If you set a polling start date and time that is in the future, polling will begin when specified. If you set a polling start date and time that is in the past, Waveset 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. If you take this approach, each time the application server is restarted, all resources configured for active synchronization will begin polling immediately. The typical approach, is to set a start date and time.

- **Synchronization Servers**. In a clustered environment, each server can run synchronization. Select an option to specify which servers will be used to run synchronization for the resource.

  - Select Use any available server if it does not matter where synchronization runs. A server will be chosen from the set of possible servers when synchronization starts.

    - Select Use the settings in `waveset.properties` to use servers specified there to run synchronization. (This feature is deprecated.)
    - Select Use specified servers, and then select one or more available servers from the Synchronization Servers list, to select specific servers to run synchronization.
- **Resource Specific Settings**. Use this section to specify how synchronization will determine the data to be processed for the resource.
- **Common Settings**. Specify the general settings for data synchronization activities.

  These settings include:

    - **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.
    - **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.
    - **Rules** (*optional*). Select rules to use during the data synchronization process.

      You can specify the following:

        - **Process Rule**. Select this rule to specify 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.
        - **Correlation Rule**. Select 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**. Select a confirmation rule to override the confirmation rule specified in the resource's reconciliation policy.
        - **Resolve Process Rule**. Select this rule to specify the name of a Task Definition to run in case of multiple matches to a record in the data 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**. Select 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 this option is enabled (true), the adapter will attempt to create accounts that it does not find in the Waveset system. If not enabled, the adapter will run the account through the process returned by the Resolve Process Rule.
    - **Logging Settings**. Specify a value for the logging options.

The logging options consist of the following:

- **Maximum Log Archives**. If greater than zero, retain the latest `N` log files. If zero, then a single log file is reused. 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 reused 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 reused after this time period. This size criteria is evaluated independently of the age criteria specified by Maximum Active Log Age.
- **Log Level**. Specify a logging level.

  The following logging levels are available:
  - **0**. No logging
  - **1**. Error
  - **2**. Information
  - **3**. Verbose
  - **4**. Debug

4 **Click Save to save the policy settings for the resource.**

Editing Active Sync Adapters

Before editing an Active Sync adapter, stop synchronization.

▼ To Stop Synchronization

1 **Open the Edit Synchronization page. (For instructions, see “To Edit or Configure Synchronization” on page 242.)**

2 **Under Scheduling Settings, locate Startup Type and select Disabled.**

For Service Provider users deselect the Enable Synchronization option.

A warning message will appear to indicate that active synchronization is disabled.

3 **Click Save.**

Disabling synchronization for a resource will result in stopping the synchronization task when the changes are saved.

Tuning Active Sync Adapter Performance

Because synchronization is a background task, Active Sync adapter configuration can affect server performance.

Tuning Active Sync adapter performance involves these tasks:

- "Changing Polling Intervals" on page 246
- "Specifying the Host Where the Adapter Will Run" on page 246
- "Starting and Stopping" on page 247
- "Adapter Logging" on page 247

Manage Active Sync adapters through the resources list. Select an Active Sync adapter, and then access start, stop, and status refresh controls actions from the *Synchronization* section of the Resource Actions list.

Changing Polling Intervals

The polling interval determines when the Active Sync 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 Waveset 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 minute.

Specifying the Host Where the Adapter Will Run

To specify the host where the adapters will run, you must edit the `sources.hosts` property in the `SystemConfiguration` object.

Specify one of the following settings:

- Set `sources.hosts=`*hostname1,hostname2,hostname3*. This setting lists the host names of machines to run Active Sync adapters. The adapter will run on the first available host listed in this field.

  Note – The *hostname* you enter must match an entry in the Waveset list of servers. View the list of servers from the Configure tab.

- Set `sources.hosts=localhost`. With this setting, the adapter will run on the first Waveset server that attempts to start Active Sync for the resource.

Note – In a cluster you should use the first option if you need to specify a specific server.

This property setting applies only to Waveset user synchronization. Host configuration for Service Provider user synchronization is determined by the Synchronization Policy.

Active Sync 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

Active Sync adapters can be disabled, manually started, or automatically started. You must have the appropriate administrator capability to change Active Sync resources in order to start or stop Active Sync adapters. For information about administrator capabilities, see "Capabilities Categories" on page 198.

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 Logging

Adapter logs capture information about the adapter currently 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 in the Logging section of the Synchronization Policy for the appropriate user type (Waveset or Service Provider).

Delete Adapter logs only when the adapter has been stopped. In most cases, it is a good practice to make a copy of an adapter log for archive purposes before you delete the log.

CHAPTER 8

Reporting

Waveset reports on automated and manual system activities. A robust set of reporting features lets you capture and view important access information and statistics on Waveset users at any time.

In this chapter, you will learn about the Waveset report types, how to create, run, and email reports, and how to download report information.

This chapter is organized into the following topics:

Working with Reports

In Waveset, reports are considered a special task category. As a result, you work with reports in two areas of the Waveset Administrator interface:

- **Reports (Run Reports)**. Use the Run Reports area to define, run, delete, and download reports. Only administrators with sufficient capabilities can define, run, delete, and download reports. See Appendix D, "Capabilities Definitions," for more information.
- **Server Tasks**. After you define reports, go to the Scheduled Tasks area (Server Tasks → Manage Schedule) to schedule and modify report tasks. TaskDefinition objects must contain `visibility=schedule` in order to be scheduled. Use the debug pages to make this change. See "Editing Waveset Configuration Objects" on page 108 for more information.

Note – Waveset logs report creation, modification, and deletion events. Waveset logs the create and modification events with attributes, but only logs delete events for deletions.

Report Types

Reports are organized into two categories:

- **Waveset Reports**. Includes a variety of report types, including real-time, summary, audit log, system log, and usage reports.
- **Auditor Reports**. Provides information that helps you manage user compliance based on criteria defined in audit policies.

Within these two categories, reports are further divided into a variety of report types. Report types are discussed in greater detail later in this chapter. Waveset reports are discussed starting on "Waveset Reports" on page 255 and Auditor reports on "Auditor Reports" on page 263.

For instructions on how to view Waveset Reports and Auditor Reports, see "Viewing Reports" on page 251.

Running Reports

▼ To Run a Report

1. **In the Administrator interface, click Reports in the main menu.**

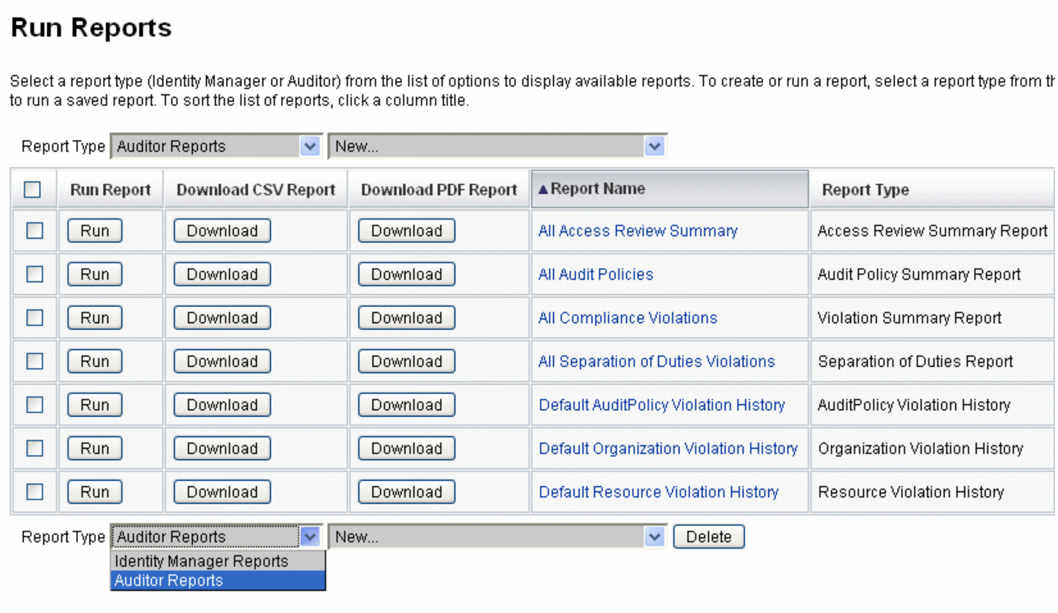
   The Run Reports page opens.

2. **To view a list of available Waveset Reports, select Waveset Reports in the Report Type drop-down menu. (This option is selected by default.)**

   To view a list of available Auditor Reports, select Auditor Reports in the Report Type drop-down menu. See "Working with Auditor Reports" on page 429 in Chapter 15, "Auditing: Monitoring Compliance," for more information.

   Figure 8–1 shows an example of the Run Reports page. Auditor Reports are selected in the Report Type drop-down menu.

FIGURE 8–1 Run Reports Selection



Run Reports

Select a report type (Identity Manager or Auditor) from the list of options to display available reports. To create or run a report, select a report type from th
to run a saved report. To sort the list of reports, click a column title.

Report Type Auditor Reports New...

□	Run Report	Download CSV Report	Download PDF Report	▲Report Name	Report Type
□	Run	Download	Download	All Access Review Summary	Access Review Summary Report
□	Run	Download	Download	All Audit Policies	Audit Policy Summary Report
□	Run	Download	Download	All Compliance Violations	Violation Summary Report
□	Run	Download	Download	All Separation of Duties Violations	Separation of Duties Report
□	Run	Download	Download	Default AuditPolicy Violation History	AuditPolicy Violation History
□	Run	Download	Download	Default Organization Violation History	Organization Violation History
□	Run	Download	Download	Default Resource Violation History	Resource Violation History

Report Type Auditor Reports New... Delete

3 **Click Run to run a report.**

Note – To allow multiple instances of the same report to run at the same time, edit the report and select the Allow Reports to Execute Concurrently option. Enabling this option allows multiple administrators to run the same report at the same time.

If two or more instances of the same report run concurrently, each report will have the administrator’s ID followed by a timestamp appended to the report name.

Viewing Reports

After running a report from the Run Reports page, you can view the output immediately or at a later time.

▼ To View a Report

1 **In the Administrator interface, click Reports in the main menu.**

The Run Reports page opens.

2 **Click the View Reports tab.**

The View Reports page opens.

3 **Click a report to view it.**

Creating Reports

This section describes how to create a new Waveset or Identity Auditor report that is not based on an existing report.

Note – To modify an existing report and save it with a new name, see "Editing and Cloning Reports" on page 252 in the next section.

▼ To Create a New Report

1 **In the Administrator interface, click Reports in the main menu.**

The Run Reports page opens.

2 **Use the Report Type drop-down menu to select a report category.**

There are two report categories:

- Waveset Reports
- Identity Auditor Reports

3 **Use the next drop-down menu to select a specific report type to create. (This menu says New at the top.)**

Waveset displays the Define a Report page, where you choose options to create the report, run it, or save it.

After entering and selecting report criteria, you can:

- Run the report without saving. Click Run to run the report. Waveset 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).

For more information on running reports, see "Running Reports" on page 250.

Editing and Cloning Reports

This section describes how to modify or clone an existing report and save it with a new name.

▼ To Edit or Clone a Report

1 **In the Administrator interface, click Reports in the main menu.**

The Run Reports page opens.

2 **Use the Report Type drop-down menu to select a report category.**

There are two report categories:

- Waveset Reports
- Auditor Reports

  The table of reports shows the existing reports in the category selected.

3 **Click a report name to edit it.**

4 **To edit a report, adjust the report parameters as needed and click Save.**

To clone a report, enter a new report name. adjust the report parameters as needed, and click Save to save it with the new name.

Sending Email 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 one of the following formats for 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).

Scheduling Reports

You can immediately run a report or schedule it to run at regular intervals by choosing one of the following selections:

- Select **Reports** → **Run Reports** to run saved reports immediately. From the list of reports, click Run. Waveset runs the report and then displays the results in summary and detailed formats.
- Select **Server Tasks** → **Manage Schedule** to schedule when report tasks are 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).

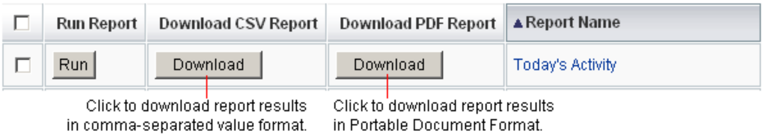
  For a report TaskDefinition to show up in this list, you must set the `visibility` attribute in the TaskDefinition object to `schedule`.

Downloading Report Data

From the Run Reports page you can download report information for use in another application, such as Acrobat Reader or StarOffice.

Open the Run Reports page and click Download in one of these columns:

- **Download CSV Report**. Downloads report output in CSV format. Once saved, you can open and work with the report in another application, such as StarOffice.
- **Download PDF Report**. Downloads report output in Portable Document Format, which can be viewed with Adobe Reader.



□	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.

Configuring Report Output

To configure report output, click Reports, and then select Configure Reports.

These selections are available on the Configure Reports page:

- **PDF Report Options**

  For reports generated in portable document format (PDF), you can make selections to determine the fonts to be used in the report, the page size, and page orientation.

  - **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 computer system 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.

  - **Page Size**. Choose the PDF page size by selecting letter (8 ½ by 11 inches) or legal (8 ½ by 14 inches) from the menu. (Default value is *letter*.)

Note – You can add other sizes to this menu by using the pdfPageSize field on the Reports Config Library form. The pdfPageSize value must be a value known to the `com.lowagie.text.Rectangle` class in the `itext` package.

  - **Orientation**. Choose the PDF page orientation by selecting portrait or landscape from the menu. (Default value is *portrait*.)
- **CSV Report Options**. Select the Character Set Name option to specify a character set to use when generating CSV reports. Not all applications that import CSV files support the default UTF-8 encoding. Select another character set as needed.
- **Tracked Event Configuration**. Select the Enable event collection option to configure reports for system monitoring and does not apply to customizing report formatting. For more information, see "Tracked Event Configuration" on page 271.

Click Save to save report configuration options.

Waveset Reports

Waveset report types can be grouped into the following report type categories:

- "AuditLog Reports" on page 255
- "Individual User AuditLog Reports" on page 256
- "Real Time Reports" on page 257
- "Summary Reports" on page 257
- "SystemLog Reports" on page 260
- "Usage Reports" on page 260
- "Workflow Reports" on page 262

AuditLog Reports

AuditLog 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, self-provisioning activities, policy violations, and service provider (extranet) users, among others.

Note – Before running audit logs, you must specify the types of Waveset events you want to capture. To do this, select Configure from the menu bar, and then select Audit. 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 "Configuring Audit Groups and Audit Events" on page 102.

▼ To Define an AuditLog Report

1. **Follow the instructions for Creating a Report on "Creating Reports" on page 252.**

   Select Waveset Reports from the first Report Type menu, and select AuditLog Report from the second menu.

   The Define a Report page opens.

2. **Complete the form and click Save.**

   Click Help if you have questions about the form.

   Once you have set and saved report parameters, run the report from the Run Reports 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.

Individual User AuditLog Reports

As with the AuditLog reports, the Individual User AuditLog report is based on events captured in the system audit log. This report, however, prompts you for a user to report on, and returns a list of activities that have been performed on that user. To maximize results, this report searches both the `AccountId` and `ObjectDesc` fields in the audit log for the matching user name.

This report can either return a fixed set of columns, or you can select a custom set of columns. Columns are defined in `reporttasks.xml` and `defaultreports.xml`. Both files can be found in the `sample` directory (located in your Waveset installation directory).

▼ To Define an Individual User AuditLog Report

1. **Follow the instructions for Creating a Report on "Creating Reports" on page 252.**

   Select Waveset Reports from the first Report Type menu, and select Individual User AuditLog Report from the second menu.

   The Define a Report page opens.

2. **Complete the form and click Save.**

   Click Help if you have questions about the form.

Real Time Reports

Real time reports poll resources directly to report real-time information.

Real time reports include:

- **Resource Group Report**. Summarizes group attributes, including user memberships.
- **Resource Status Report**. Tests the connection status of one or more specified resources by executing the `testConnection` method against each resource.
- **Resource User Report**. Lists user resource accounts and account attributes.

▼ To Define a Real-Time Report

1. **Follow the instructions for Creating a Report on "Creating Reports" on page 252.**

   Select Waveset Reports from the first Report Type menu, and select Resource Group Report, Resource Status Report, or Resource User Report from the second menu.

   The Define a Report page opens.

2. **Complete the form and click Save.**

   Click Help if you have questions about the form.

   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 the following reports available from the Waveset Reports list:

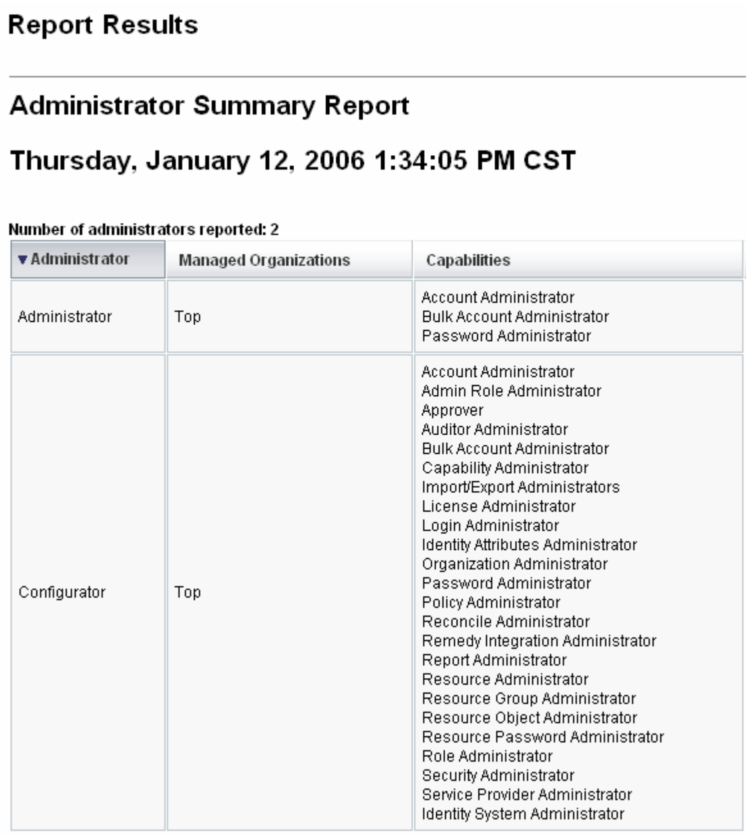
- **Account Index Report**. Report on selected resource accounts according to reconciliation situation.
- **Administrator Report**. View Waveset administrators, the organizations they manage, and assigned capabilities. When defining an administrator report, you can select administrators to include by organization.
- **Admin Role Report**. List users assigned to admin roles.
- **Role Report**. Report on all aspects of roles and associated resources.
- **Task Report**. 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 Report**. 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, assigned manager, role, organization, or resource assignment.

- **User Question Report**. 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.

Note – By default, the following reports are run on the set of organizations controlled by the logged-in administrator, unless overridden by selecting one or more organizations against which the report will be run.

- Admin Role Summary
- Administrator Summary
- Role Summary
- User Questions Summary
- User Summary

As shown in the following figure, the Administrator Report lists Waveset 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

▼ To Define a Summary Report

1 Follow the instructions for Creating a Report on "Creating Reports" on page 252.

Select one of the Summary report types (listed above) from the second menu.

The Define a Report page opens.

2 Complete the form and click Save.

Click Help if you have questions about the form.

SystemLog Reports

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 the following items:

- 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.

When running a SystemLog Report, specific Syslog entries can be retrieved by specifying the syslog ID of the target entry. For example, to view specific entries in the Recent Systems Messages report, edit the report and select the Event field. Then enter the requested syslog ID and click Run.

Note – You also can run the `lh syslog` command to extract records from the system log. For detailed command options, read "`syslog` Command" on page 525 in Appendix A, "`lh` Reference."

▼ To Define a SystemLog Report

1. **Follow the instructions for Creating a Report on "Creating Reports" on page 252.**

   Select Waveset Reports from the first Report Type menu, and select SystemLog Report from the second menu.

   The Define a Report page opens.

2. **Complete the form and click Save.**

   Click Help if you have questions about the form.

   Once you have set and saved report parameters, run the report from the Run Reports list page.

Usage Reports

Create and run usage reports to view graphical and/or tabular summaries of system events related to Waveset objects such as administrators, users, roles, or resources. You can display usage reports display data in table, bar chart, pie chart, or line chart format.

▼ To Define a Usage Report

1. **Follow the instructions for Creating a Report on “Creating Reports” on page 252.**

2. **Select Waveset Reports from the first Report Type menu, and select Usage Report from the second menu.**

   The Define a Report page opens.

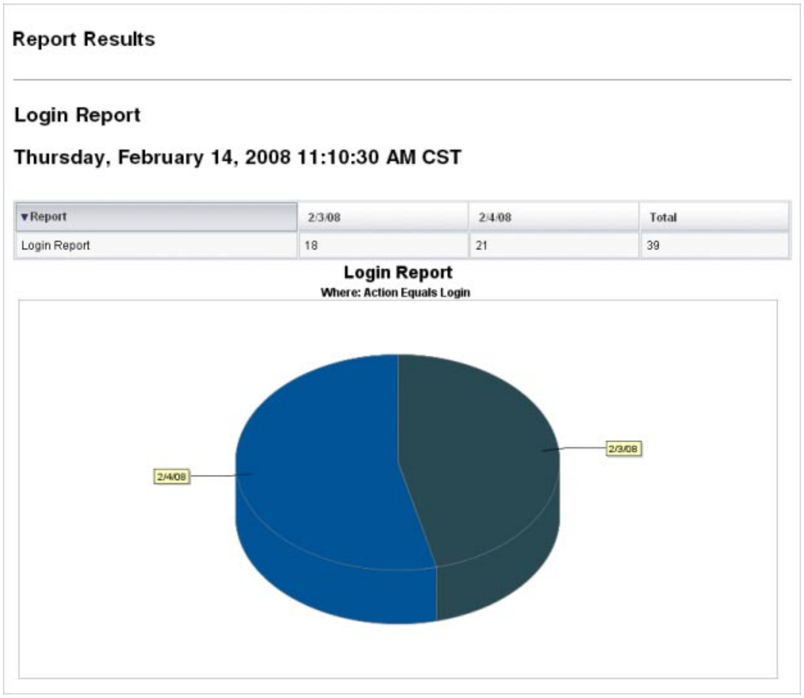
3. **Complete the form and click Save.**

   Click Help if you have questions about the form.

   Once you have set and saved report parameters, run the report from the Run Reports list page.

Example 8–1 Usage Report Chart (Generated User Accounts)

The following figure shows an example usage report. The table at the top of the report shows events comprising the report and the chart below shows the same information in graphical format.



Report Results

Login Report

Thursday, February 14, 2008 11:10:30 AM CST

▾Report	2/3/08	2/4/08	Total
Login Report	18	21	39

Login Report

Where: Action Equals Login

Workflow Reports

This report lists workflows by name and provides the following information:

- The average time the workflow took to complete
- The number of times the workflow was requested
- The number of workflow requests that were completed

In addition, clicking the workflow name opens a detailed view of the workflow, which will show each activity that was instrumented within the workflow, and its average time to complete.

Workflow Reports are especially useful for capturing performance metrics that can help establish whether Service Level Agreement (SLA) targets are being met.

Waveset must be configured to capture workflow timing metrics as a prerequisite to running Workflow Reports. See the next section for more information.

Configuring Workflows to Capture Audit Timing Events

Before you can run Workflow Reports, you must first turn on workflow auditing for each workflow type that you want to report on.

Note – Auditing workflows degrades performance. Consequently, you should only enable workflow auditing for those workflows that you plan to use with Workflow Reports.

Turn on workflow auditing as follows:

- For workflows that you can configure in the Administrator interface using task templates, select the Audit entire workflow checkbox on the Audit tab of the task template configuration form. See "Configuring the Audit Tab" on page 300 for instructions.
- For workflows that do not have task templates, refer to "Modifying Workflows to Log Timing Audit Events" on page 315.

Specifying Attributes to Store for the Workflow Report

While it is not necessary to define attributes, to get the most out of Workflow Reports it is important to store attributes that you later plan to filter your reports on.

To define the set of attributes that you want to store for each workflow type, use the Administrator interface's tabbed task template configuration form. The Audit tab contains an Audit Attributes section, which is located below the Audit entire workflow checkbox. See "Configuring the Audit Tab" on page 300 for instructions.

▼ To Define a Workflow Report

1 **Follow the instructions for creating a report on "Creating Reports" on page 252.**

Select Waveset Reports from the first Report Type menu, and select Workflow Report from the second menu.

The Define a Report page opens.

2 **Complete the form and click Save. You can define time parameters as well as add any of the attributes that you elected to audit. (See "Specifying Attributes to Store for the Workflow Report" on page 262 in the previous section.)**

To narrow your results, specify an attribute name (for example, `user.global.state`), select a condition, and enter an attribute value. You can enter as many attributes as you need.

Click Help if you have questions about the form.

Once you have set and saved report parameters, run the report from the Run Reports page. Click Run to produce a report of all results that match the saved criteria.

The report will return workflows by name, along with their average time to complete, the number of times the workflow was requested, and how many of those requests were completed.

Click the workflow name to open a detailed view of the workflow, which will show each activity that was instrumented in the workflow. Because processes can have the same named activities, the activities are scoped by process.

Auditor Reports

Auditor reports provide information that help you manage user compliance based on criteria defined in audit policies.

Waveset provides the following auditor reports:

- Access Review Coverage Reports
- Access Review Detail Reports
- Access Review Summary Reports
- Access Scan User Scope Coverage Reports
- Audit Policy Summary Reports
- Audited Attribute Reports
- Audit Policy Violation History
- User Access Reports
- Organization Violation History
- Resource Violation History
- Separation of Duties Reports
- Violation Summary Reports

To define an auditor report, follow the steps in "Creating Reports" on page 252.

For more information about auditor reports, see "Working with Auditor Reports" on page 429 in Chapter 15, "Auditing: Monitoring Compliance."

Working with Graphs

You can perform the following activities related to graphs:

- "Viewing Defined Graphs" on page 264
- "To Create a Dashboard Graph" on page 265
- "To Edit a Dashboard Graph" on page 267
- "To Delete a Defined Graph" on page 268

Viewing Defined Graphs

Waveset provides some sample graphs. Some use sample data and some do not. You are encouraged to create additional graphs that are applicable to your deployment.

You should remove the sample graphs and sample dashboards before moving a deployment into production. Some of the sample graphs that do not use sample data might appear blank if no applicable data has been collected.

▼ To View a Defined Graph

1. **In the Administrator interface, click Reports in the main menu.**

2. **Click Dashboard Graphs in the secondary menu.**

3. **Select a category of dashboard graphs from the Select Dashboard Graph Type list of options.**

   All graphs in the selected category display in the graphs list.

4. **Click a graph name.**

5. **If desired, click Pause refresh to pause the dashboard refresh. Click Resume to renew the view.**

   Note – For dashboards containing many graphs, it is sometimes helpful to pause the refresh until all of the graphs are initially loaded.

6. **If desired, click Refresh now to force an immediate refresh.**

7. **Click Done to return to the Dashboard Graphs list page.**

Note – If any of the graphs show an error message, open the system configuration object for editing ("Editing Waveset Configuration Objects" on page 108) and set `dashboard.debug=true`. Once this property is set, return to the graph that generated the error and use the Please include this text script if reporting a problem link to retrieve the graph script. This graph script should be included when reporting the problem.

To Create a Dashboard Graph

1 **In the Administrator interface, select Reports → Dashboard Graphs.**

2 **Select a dashboard graphs category from the list of Select Dashboard Graph Type options.**

All graphs in the selected category display in the graphs list.

3 **Click New to display the Create Dashboard Graph page and enter a Graph Name.**

Choose a unique, meaningful name because graphs are added to dashboards by name.

4 **Select a Registry: IDM or SAMPLE.**

The sample data selection is provided for you to familiarize yourself with the system. As sample data is not available for all tracked events, this selection is most useful for demos and when experimenting with the various graph options. Delete sample data prior to going to a production environment.

Note – The set of tracked events that use sample data differs from the events that are actually tracked.

5 **Select a Tracked Event type from the list.**

An event is a system characteristic, such as memory usage, or an aggregation of events, such as resource operations, whose historical values are tracked and displayed visually as graphs or charts.

Tracked events for the IDM registry are:

- **Provisioner Execution Counts**. Tracks how many provisioner operations occurred (by operation type).
- **Provisioner Execution Duration**. Tracks the duration of each provisioner operation (by operation type).
- **Resource Operation Count**. Tracks the number of resource operations.
- **Resource Operation Duration**. Tracks the duration of a resource operation.
- **Workflow Duration**. Tracks how long it takes to execute a workflow.
- **Workflow Execution Count**. Tracks the number of times each workflow is executed.

6 **Select a Time Scale from the list.**

This option controls how often data is aggregated (for example, one hour) and how often it is retained (for example, one month). The system stores tracked event data for progressively larger time scales to allow both a detailed, current view of the system as well as an understanding of historical trends.

7 **Select a Metric from the list.**

A metric (count or average) will be selected by default, depending on the selected tracked event. Each graph displays a single metric. The available metrics depend on the selected tracked event.

Possible metrics include:

- **Count**. The total number of times the event occurred in the time interval
- **Average**. The arithmetic mean of the event values for the time interval
- **Maximum**. The maximum event value for the time interval
- **Minimum**. The minimum event value for the time interval
- **Histogram**. The separate counts for discrete ranges of event values for the time interval

8 **Select Show count as from the list.**

The graph count is shown either as a raw total or scaled by various time scales.

9 **Select a Graph Type from the list.**

This controls how the tracked event data is displayed. The available graph types depend on the selected tracked event and can include line graphs, bar charts, and pie charts.

10 **Specify a Base Dimension (*optional*).**

Select from the following list:

- **Resource Name**. If selected, all values for the dimension are included in the graph. Deselect this option to choose individual values of the dimension to include in the graph.
- **Server Instance**. If selected, all values for the dimension are included in the graph. Deselect this option to choose individual values of the dimension to include in the graph.
- **Operation Type**. If selected, all values for the dimension are included in the graph. Deselect this option to choose individual values of the dimension to include in the graph.

  After you select the dimension, the page refreshes to display a graph.

11 **Enter text in the Graph Options field to produce a subtitle under the main title of the graph (*optional*).**

12 **Select Advanced Graph Options (*optional*).**

Use this option if you want to specify the following:

- **Grid Lines**
- **Font**
- **Color Palette**

13 **Click Save to create the graph.**

▼ To Edit a Dashboard Graph

1 **In the Administrator interface, click Reports in the main menu.**

2 **Click Dashboard Graphs in the secondary menu.**

The Dashboard Graphs page opens.

3 **From the Select Dashboard Graph Type drop-down menu, select a category.**

A table listing dashboard graphs opens.

4 **Click a graph name to edit it.**

The graph attributes you can edit vary depending on the graph selected.

One or more of the following characteristics are available for editing:

- **Graph Name**. Graphs are added to a dashboard by name.
- **Registry**. Specifies the *tracked event description* defined in the registry. The current selection includes: SAMPLE, Service Provider, and IDM.
- **Tracked Event**. A system characteristic, such as memory usage, or an aggregation of events, such as resource operations, whose historical values are tracked and displayed visually as graphs or charts.
- **Time Scale**. Controls how often data is aggregated and how often it is retained.
- **Metric**. Each graph displays a single metric. The available metrics depend on the selected tracked event. Other options may be available for the metric selected.
- **Graph type**. Controls how the tracked event data is displayed (for example, line graph or bar graph).
- **Included Dimension Values**. If selected, all values for the dimensions are included in the graph.
- **Graph Subtitle**. If desired, enter a subtitle under the main title of the graph.
- **Advanced Graph Options**. Select this if you want to set the following:
  - **Grid Lines**
  - **Font**
  - **Color Palette**

5 **Click Save.**

▼ To Delete a Defined Graph

1 **In the Administrator interface, click Reports in the main menu.**

2 **Click Dashboard Graphs in the secondary menu.**

3 **Select a category of dashboard graphs from the Select Dashboard Graph Type list of options.**

All graphs in the selected category display in the graphs list.

4 **Use the checkboxes to select the graphs to delete and then click Delete.**

Note – Graphs are deleted without warning from all dashboards that included it.

Working with Dashboards

A dashboard is a collection of related graphs that are viewed on a single page. As with graphs, Waveset provides a set of sample dashboards that administrators are encouraged to customize to their own deployment. See "To Create Dashboards" on page 269 for instructions.

▼ To View Dashboards

1 **In the Administrator interface, click Reports in the main menu.**

2 **Click View Dashboards in the secondary menu to view currently defined Dashboards.**

The Dashboards page opens.

3 **Click Display next to the dashboard you want to view**

Note – For dashboards containing many graphs, it's sometimes helpful to pause the refresh until all of the graphs are initially loaded.

Click Pause to pause dashboard refresh, or Refresh to renew the view.

The following sections provide procedures for working with dashboards:

- "To Create Dashboards" on page 269
- "Editing Dashboards" on page 269

- "Deleting Dashboards" on page 270

▼ To Create Dashboards

1. **In the Administrator interface, click Reports in the main menu.**

2. **Click View Dashboards in the secondary menu.**

3. **Click New.**

4. **Enter a name for the new dashboard.**

5. **Enter a summary describing the new dashboard.**

6. **Select a refresh rate in either seconds, minutes, or hours, from the list.**

   Note – Setting a refresh rate of less than 30 seconds can cause problems with dashboards that contain several graphs.

   ---

7. **To associate a graph style to the dashboard, select the appropriate entry from the list.**

   Note – A single graph can be used in multiple dashboards.

   ---

8. **To remove a dashboard graph, select the appropriate entry from the list and click Remove Graphs.**

9. **Click Save.**

Editing Dashboards

Use the procedure described in "To Create Dashboards" on page 269 to edit a dashboard, except instead of selecting New, select the dashboard you want to modify and edit the following attributes:

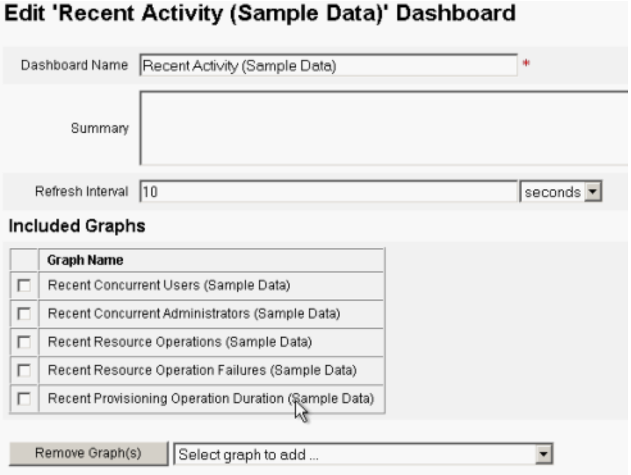
- The name for the dashboard.
- The summary describing the new dashboard.
- The refresh rate in either seconds, minutes, or hours from the list.
- Add or remove graphs associated with a dashboard.

Note – Removing a graph from a dashboard does not delete the graph. The graph is still available for use with other dashboards.

A single graph can be used in multiple dashboards.

Figure 8–2 illustrates a sample dashboard edit page.

FIGURE 8–2 Edit Dashboards



Edit 'Recent Activity (Sample Data)' Dashboard

Dashboard Name	Recent Activity (Sample Data) *
Summary	
Refresh Interval	10 seconds

Included Graphs

	Graph Name
□	Recent Concurrent Users (Sample Data)
□	Recent Concurrent Administrators (Sample Data)
□	Recent Resource Operations (Sample Data)
□	Recent Resource Operation Failures (Sample Data)
□	Recent Provisioning Operation Duration (Sample Data)

Deleting Dashboards

To delete Service Provider dashboards, from the Service Provider area click Manage Dashboards, then select the desired dashboard and click delete.

Note – The graphs included in the dashboard are not removed using this procedure. Delete graphs using the Manage Dashboard Graphs page (see "To Delete a Defined Graph" on page 268).

System Monitoring

You can set up Waveset to track events in real-time and monitor the events by viewing them in dashboard graphs. The dashboards allow you to quickly assess system resources and spot abnormalities, to understand historical performance trends (based on the time of day, the day of week, and so on), and to interactively isolate problems before looking at audit logs. They do not provide as much detail as the audit logs, but they do provide you with hints about where to look for problems in the logs.

You can create graphic dashboard displays to track automated and manual activities at a high level. Waveset provides sample *resource operations* dashboard graphs. The *resource operations* dashboard graphs enable you to quickly monitor system resources to maintain an acceptable level of service.

You can view sample data for these graphs in the Resource Operations Dashboard. For more information about using dashboards, see “Working with Dashboards” on page 268.

Statistics are collected and aggregated at various levels to present a real-time view based on your specifications.

Tracked Event Configuration

From the Tracked Event Configuration area of the Configure Reports page, you can determine if statistics collection for tracked events is currently enabled, and enable it. Click Enable event collection to enable the tracked event configuration.

Specify the following options for event collection:

- **Time Zone**. This option sets the time zone to use for recording tracked events. This primarily determines when day boundaries occur.

  Alternatively, you can set the time zone to the default time zone set on the server.
- **Time Scales to collect**. This option specifies the time intervals for which the data is aggregated (in other words, how often it is collected and persisted). For example, if a one-minute interval is selected, data is collected and persisted every minute.

The system stores tracked event data for progressively larger time scales to allow a detailed, current view of the system, as well as an understanding of historical trends.

The following time scales are available, and all of these intervals are selected by default. Clear the selections for the intervals you do not want to collect.

- 10 Second Intervals
- 1 Minute Intervals
- 1 Hour Intervals
- 1 Day Intervals

- 1 Week Intervals
- 1 Month Intervals

After configuring tracked events, use the dashboards to monitor the tracked events. Where present, use the sliders to zoom in on a section of the chart.

Risk Analysis

Waveset 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, 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 ("The Waveset Debug Page" on page 42), and modify these by using the Identity Manager IDE. See Chapter 2, "Waveset Forms," in *Oracle Waveset 8.1.1 Deployment Reference*for more information about configuring forms.

▼ To Create a Risk Analysis Report

1. **In the Administrator interface, click Reports in the main menu.**

2. **Click Run Risk Analysis in the secondary menu.**

3. **In the New drop-down menu, select a report to create.**

   A Risk Analysis Report Settings page opens.

4. **Complete the form.**

   You can limit the report to scan selected resources and, depending on the resource type, you can scan for accounts that meet these criteria:

   - Accounts that are disabled, expired, inactive, or locked
   - Accounts that have never been used
   - Accounts that do not have a fullname or password
   - Accounts that do not require a password

- Accounts with passwords that have expired or have not changed for a specified number of days

5 **Click Save.**

▼ To Schedule a Risk Analysis Report

Once defined, you can use the following steps to schedule risk analysis reports to run at specified intervals.

1 **In the Administrator interface, click Server Tasks in the main menu.**

2 **Click Manage Schedule in the secondary menu.**

The Scheduled Tasks page opens.

3 **Select a risk analysis report to schedule.**

The Create New Risk Analysis Task Schedule page opens.

4 **Enter a name and schedule information, and then optionally adjust other risk analysis selections.**

5 **Click Save to save the schedule.**

CHAPTER 9

Task Templates

Waveset's task templates enable you to use the Administrator interface to configure certain workflow behaviors as an alternative to writing customized workflows.

This chapter is organized into the following sections:

- "Enabling the Task Templates" on page 275. Describes how to make the task templates available to your system.
- "Configuring the Task Templates" on page 279. Describes how to use task templates to configure workflow behaviors.

Enabling the Task Templates

Waveset provides these task templates that 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.

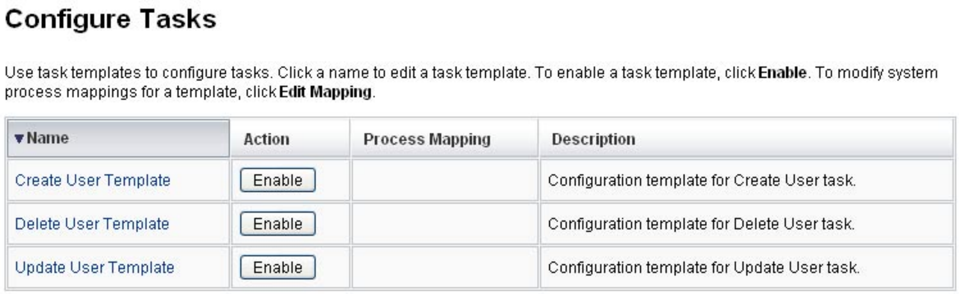
Before using the task templates, you must map the task template's processes.

▼ To Map Process Types

1 **In the Administrator interface, select Server Tasks from the menu, and then select Configure Tasks.**

Figure 9–1 illustrates the Configure Tasks page.

FIGURE 9–1 Initial Configure Tasks Page



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	Enable		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.

The Configure Tasks page contains a table with the following columns:

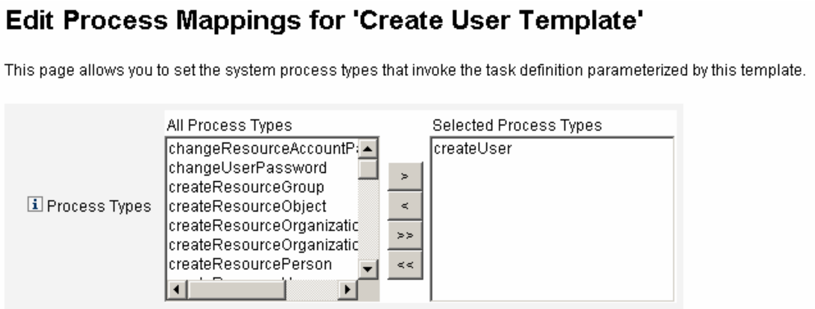
- **Name**. Provides links to the Create User, Delete User, and Update User Templates.
- **Action**. Contains one of the following buttons:
  - **Enable**. Displays if you have not enabled a template yet.
  - **Edit Mapping**. Displays after you enable a template.

    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 (Figure 9–2) displays for the Create User Template.

FIGURE 9–2 Edit Process Mappings Page



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.

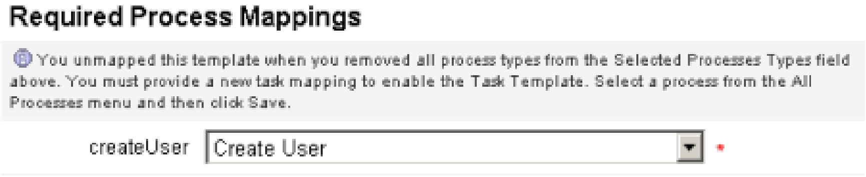
Process Types

All Process Types:
changeResourceAccountP
changeUserPassword
createResourceGroup
createResourceObject
createResourceOrganizatic
createResourceOrganizatic
createResourcePerson

Selected Process Types:
createUser

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

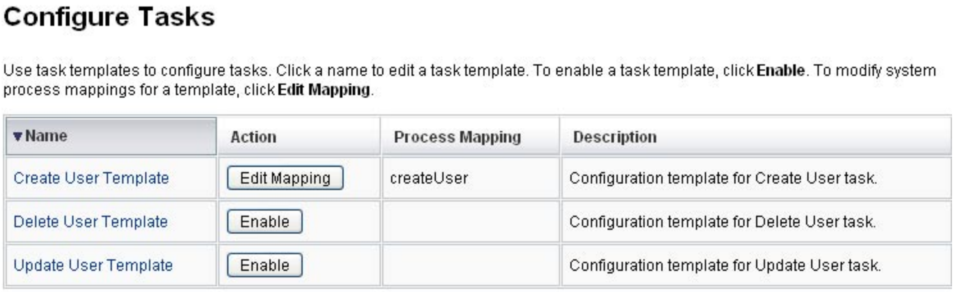
You unmapped this template when you removed all process types from the Selected Processes Types field above. You must provide a new task mapping to enable the Task Template. Select a process from the All Processes menu and then click Save.

createUser Create User *

3 **Click Save to map the selected process type and return to the Configure Tasks page.**

Note – When the Configure Tasks page re-displays, an Edit Mapping button replaces the Enable button and the process name is listed in the Process Mapping column.

FIGURE 9–3 Updated Configure Tasks Table



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	Enable		Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

4 **Repeat the mapping process for each of the remaining templates.**

More Information

Verifying Your Mappings

- You can verify the mappings by selecting Configure → Form and Process Mappings. When the Configure Form and Process Mappings page appears, 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 the Form and Process Mapping page if you type **`Template`** into the Process Name Mapped To column as shown in the table.

▼ To Configure a Task Template

After mapping the template process types ("Enabling the Task Templates" on page 275), you can configure the task templates.

1 **In the Administrator interface, click Server Tasks in the main menu, then click Configure Tasks.**

The Configure Tasks page opens.

2 **Select a link in the Name column.**

One of the following pages displays:

- **Edit Task Template 'Create User Template'**. Open to edit the template used to create a new user account.
- **Edit Task Template 'Delete User Template'**. Open to edit the template used to delete or deprovision a user's account.
- **Edit Task Template 'Update User Template'**. Open 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 or deprovisioned	Delete User Template only

Tab Name	Purpose	Template
Notification	Allows you to configure email notifications sent to administrators and users when Waveset 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 Waveset executes certain tasks.	All Templates
Audit	Allows you to enable and configure auditing for the workflow. Use this tab to configure a workflow to capture information for Workflow Reports.	All Templates
Provisioning	Allows you to run a task in the background and to allow Waveset 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
Data Transformations	Allows you to configure how user data is transformed during provisioning.	Create User and Update User Task Templates only

3 **Select one of the tabs to configure workflow features for the template.**

Instructions for configuring these tabs are provided in the following sections:

- "To Map Process Types" on page 275
- "To Configure a Task Template" on page 278

4 **When you are finished configuring the templates, click the Save button to save your changes.**

Configuring the Task Templates

This section contains information and instructions for configuring task templates. The topics include:

- "Configuring the General Tab" on page 280
- "Configuring the Notification Tab" on page 282
- "Configuring the Approvals Tab" on page 287
- "Configuring the Audit Tab" on page 300
- "Configuring the Provisioning Tab" on page 302
- "Configuring the Sunrise and Sunset Tab" on page 303
- "Configuring the Data Transformations Tab" on page 308

Configuring the General Tab

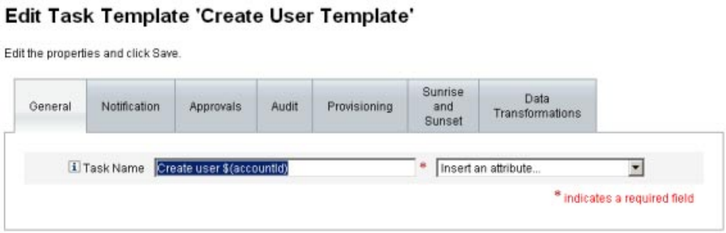
This section provides instructions for configuring the General tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.

Note – In the Administrator interface, the pages for editing the Create User Template and Update User Template are identical, so configuration instructions are provided in one section.

For the Create User or Update User Templates

When you open either the Edit Task Template Create User Template form or the Edit Task Template Update User Template form, the General tab page displays by default. This page consists of a Task Name text field and a Insert an attribute menu, as shown in Figure 9–4. For instructions on how to start the configuration process see the "Configuring the Task Templates" on page 279 section.

FIGURE 9–4 General Tab: Create User Template



Edit Task Template 'Create User Template'

Edit the properties and click Save.

Task Name: Create user $(accountId) * Insert an attribute...

* indicates a required field

Task names can contain literal text and/or attribute references that are resolved during task execution.

▼ To Change the Default Task Name

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 an attribute from the menu (*optional*).**

   Waveset 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 Waveset 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' page the General tab page displays by default. (For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.)

▼ To Specify How User Accounts Are Deleted/Deprovisioned

1 **Use the Delete Waveset Account buttons to specify whether an Waveset account can be deleted during a delete operation.**

These buttons include:

- **Never**. Select to prevent accounts from being deleted.
- **Only if user has no linked accounts after deprovisioning**. Select to allow user account deletions only if there are no linked resource accounts after deprovisioning.
- **Always**. Select 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.**

Note –

- Unassigning or unlinking an external resource from a user does not create a provisioning request or a work item. When you unassign or unlink an external resource, Oracle Waveset does not deprovision or delete the resource account, so there is nothing for you to do.
- You can use the Delete Resource Accounts page to unassign or unlink resource accounts when the Delete operation has been disabled.

These boxes include:

- **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 Waveset 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.

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).**

These boxes include:

- **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 Waveset 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.

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.

Configuring the Notification Tab

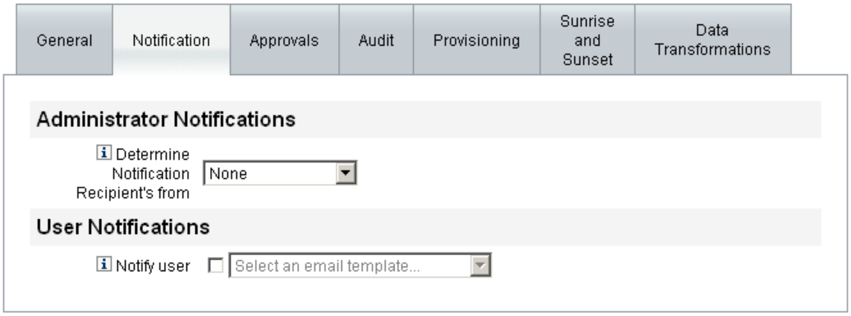
This section provides instructions for configuring the Notification tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.

All of the Task Templates support sending email notifications to administrators and users when Waveset invokes a process (usually after the process has completed). You can use the Notification tab to configure these notifications.

Note – Waveset uses email templates to deliver information and requests for action to administrators, approvers, and users. For more information about Waveset email templates, see the section titled "Customizing Email Templates" on page 98 in this guide.

Figure 9–5 shows the Notification page for the Create User Template.

FIGURE 9–5 Notification Tab: Create User Template



Administrator Notifications

Determine Notification Recipient's from: None

User Notifications

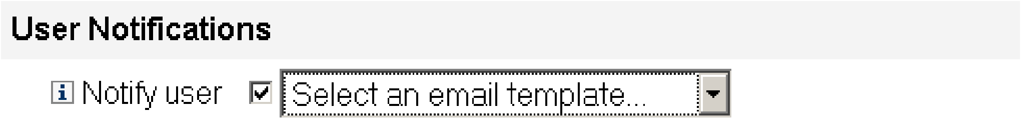
Notify user □ Select an email template...

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, as shown in Figure 9–6, and then select an email template from the list.

FIGURE 9–6 Specifying an Email Template



User Notifications

Notify user ☑ Select an email template...

Configuring Administrator Notifications

To specify how Waveset determines administrator notification recipients, select an option from the Determine Notification Recipients from menu.

The available options are:

- **None** (default). No administrators will be notified.
- **Attribute**. Select to derive notification recipients' account IDs from a specified attribute in the user view. For more information see "Specifying Administrator Notification Recipients by Attribute" on page 284.
- **Rule**. Select to derive notification recipients' account IDs by evaluating a specified rule. For more information see "Specifying Administrator Notification Recipients by Rule" on page 285.
- **Query**. Select to derive notification recipients' account IDs by formulating a query to a particular resource. For more information see "Specifying Administrator Notification Recipients by Query" on page 286.
- **Administrator List**. Select to choose notification recipients' explicitly from a list. For more information see "Specifying Administrator Notification Recipients by Attribute" on page 284.

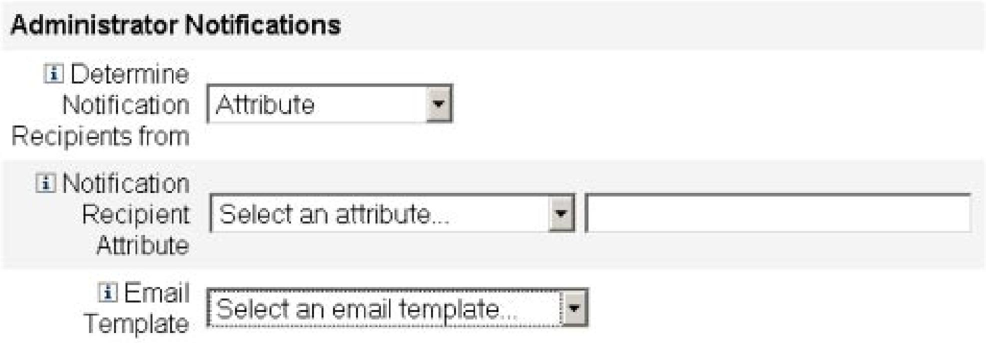
Specifying Administrator Notification Recipients by Attribute

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.

▼ To Derive Notification Recipients' Account IDs From a Specified Attribute

1 Select Attribute from the Determine Notification Recipients from menu and new options display, as shown in the following figure.

FIGURE 9–7 Administrator Notifications: Attribute



Administrator Notifications

Determine Notification Recipients from: Attribute

Notification Recipient Attribute: Select an attribute...

Email Template: Select an email template...

These options include:

- **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.**

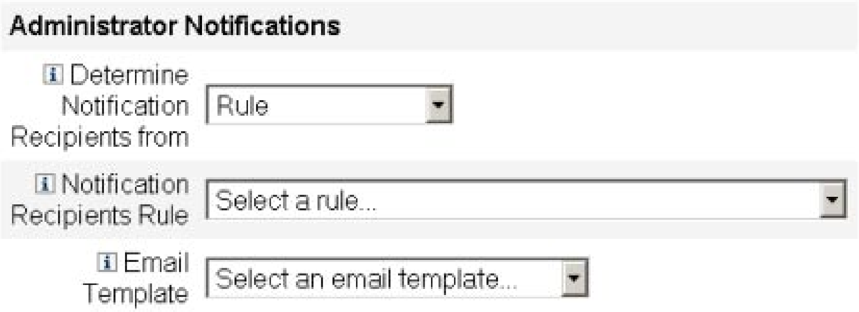
Specifying Administrator Notification Recipients by Rule

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.

▼ To Derive Notification Recipients' Account IDs From a Specified Rule

1 **Select Rule from the Determine Notification Recipients from menu and the following new options display in the Notification form.**

FIGURE 9–8 Administrator Notifications: Rule



Administrator Notifications

Determine Notification Recipients from: Rule

Notification Recipients Rule: Select a rule...

Email Template: Select an email template...

- **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 Administrator Notification 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

1 **Select Query from the Determine Notification Recipients from menu and new options display in the Notification form, as shown in Figure 9–9.**

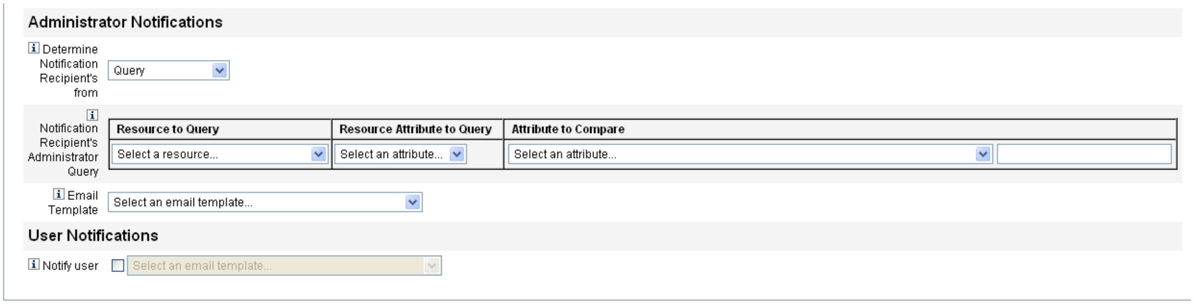


FIGURE 9–9 Administrator Notifications: Query

Administrator Notifications

Determine Notification Recipient's from: Query

Notification Recipient's 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...

User Notifications

Notify user □ Select an email template...

The Notification Recipient Administrator Query table consists 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.

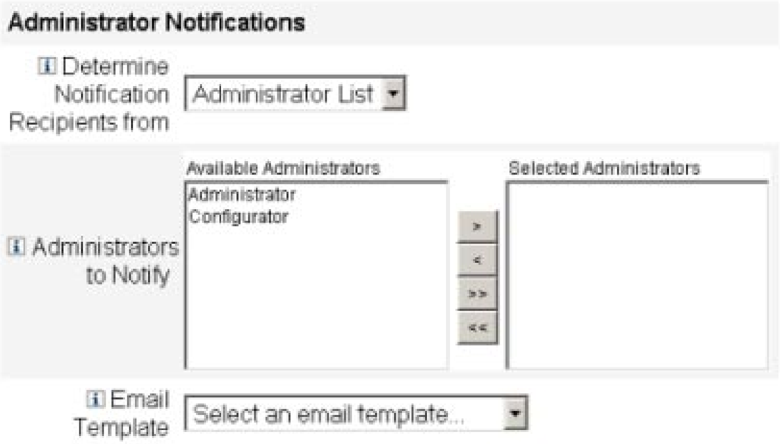
2 **Select a resource, a resource attribute, and an attribute to compare from these menus to construct the query.**

3 **Select a template from the Email Template menu to specify a format for the administrators' notification email.**

▼ To Specify Administrator Notification Recipients From the Administrator List

1. **Select Administrator List from the Determine Notification Recipients from menu and new options display in the Notification form, as shown in the following figure.**

   FIGURE 9–10 Administrator Notifications: Administrators List

   Administrator Notifications

   Determine Notification Recipients from: Administrator List

   Administrators to Notify:

   Available Administrators: Administrator, Configurator

   Selected Administrators:

   Email Template: Select an email template...

   These options include:

   - **Administrators to Notify**. Provides a selection tool with a list of available administrators.
   - **Email Template**. Provides a list of email templates.

2. **Select one or more administrators in the Available Administrators list and move them to the Selected Administrators list.**

3. **Select a template from the Email Template menu to specify a format for the administrators' notification email.**

Configuring the Approvals Tab

This section provides instructions for configuring the Approvals tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see the "Configuring the Task Templates" on page 279 section.

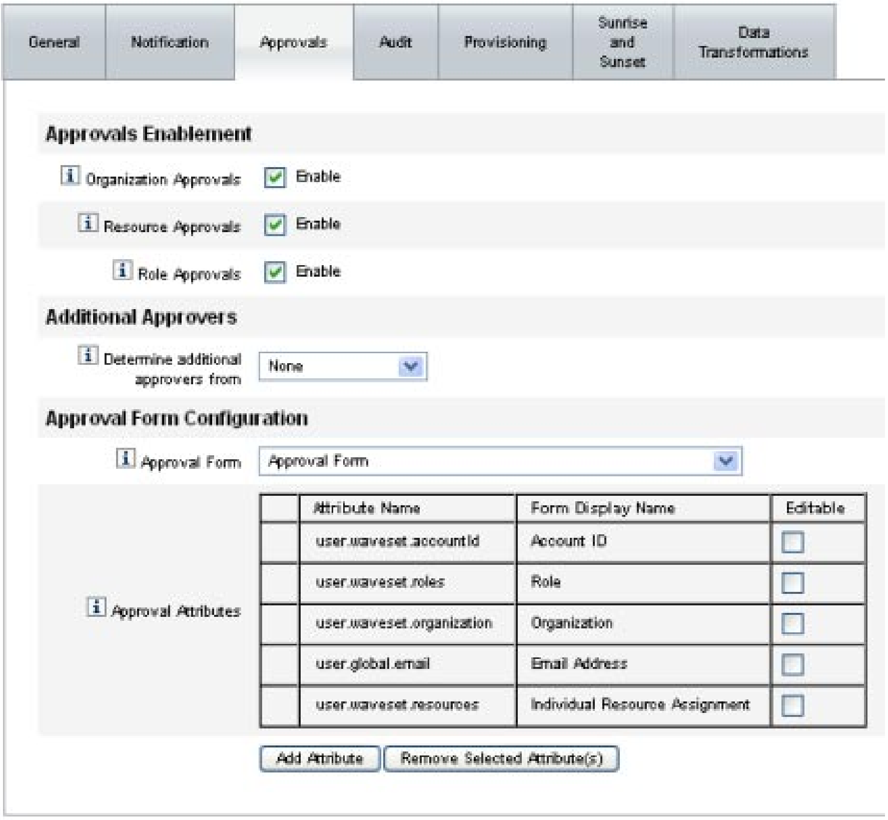
You can use the Approvals tab to designate additional approvers and to specify attributes for the task approval form before Waveset executes the create, delete, or update user tasks.

Traditionally, administrators who are associated with a particular organization, resource, or role are required to approve certain tasks before execution. Waveset 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.

Figure 9–11 illustrates the initial Approvals page Administrator user interface.

FIGURE 9–11 Approvals Tab: Create User Template



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	Role	□
	user.waveset.organization	Organization	□
	user.global.email	Email Address	□
	user.waveset.resources	Individual Resource Assignment	□

▼ To Configure Approvals

1. **Complete the Approvals Enablement section (see “Enabling Approvals (Approvals Tab, Approvals Enablement Section)” on page 289).**

2. **Complete the Additional Approvers section (see “Specifying Additional Approvers (Approvals Tab, Additional Approvers Section)” on page 289).**

3. **Complete the Approval Form Configuration section for the Create User and Update User Templates only (see “Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)” on page 297).**

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 (Approvals Tab, Approvals Enablement Section)

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 (Approvals Tab, Additional Approvers Section)

Use the Determine additional approvers from menu to specify how Waveset will determine additional approvers for the create user, delete user, or update user tasks.

The options on this menu are listed in Table 9–1.

TABLE 9–1 Determine Additional Approvers From Menu Options

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 Administrator user interface.

Use the instructions provided in the following sections to specify a method for determining additional approvers.

▼ To Determine Additional Approvers From an Attribute

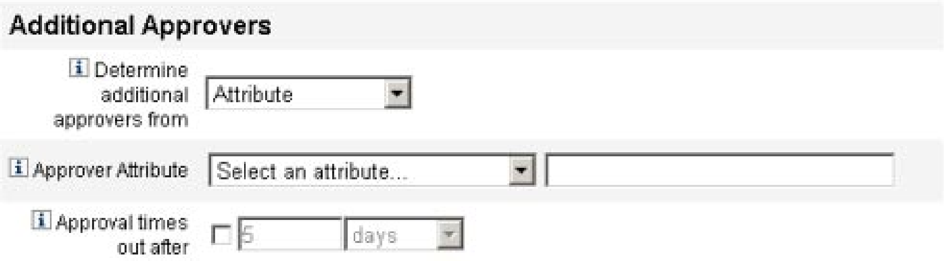
Use the following steps to determine additional approvers from an attribute.

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.

New options display, as shown in the following figure.

FIGURE 9–12 Additional Approvers: Attribute



Additional Approvers

Determine additional approvers from: Attribute

Approver Attribute: Select an attribute...

Approval times out after: □ 5 days

- **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.

  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 “To Configure Approval Timeouts” on page 294 for instructions.
- If you do not want to specify a timeout period, you can continue to “Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)” on page 297 or save your changes and go on to configure a different tab.

▼ To Determine Additional Approvers from a Rule

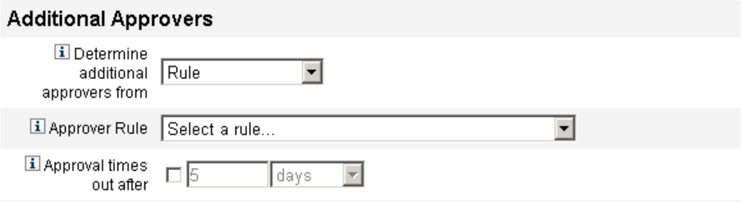
Use the following steps to derive the approver's accountIDs from a specified rule.

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.

New options display, as shown in the following figure.

FIGURE 9–13 Additional Approvers: Rule



Additional Approvers

Determine additional approvers from: Rule

Approver Rule: Select a rule...

Approval times out after: □ 5 days

- **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.

  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 "To Configure Approval Timeouts" on page 294 for instructions.
- If you do not want to specify a timeout period, you can continue to "Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)" on page 297 or save your changes and go on to configure a different tab.

▼ To Determine Additional Approvers From a Query

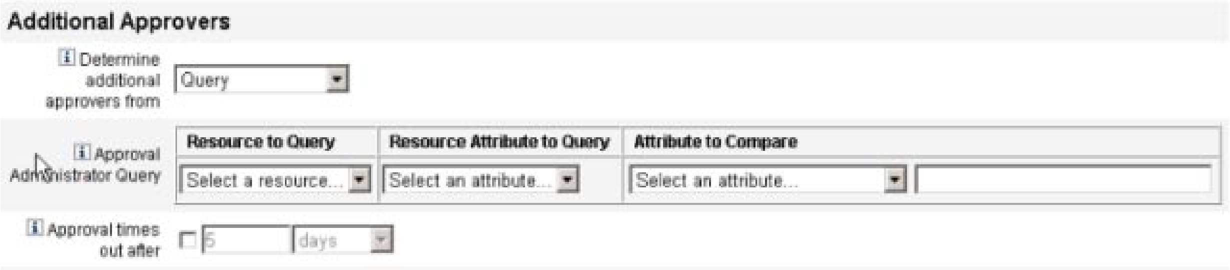
Use the following steps to derive approvers accountIDs by querying a specified resource.

Note – Only LDAP and Active Directory resource queries are supported at this time.

---

1 **Select Query from the Determine Additional Approvers from menu and new options display, as shown in the following figure.**

FIGURE 9–14 Additional Approvers: Query



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

- **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.**

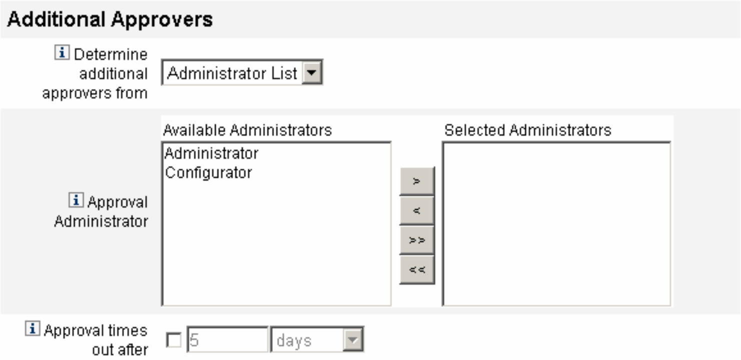
- If you want to specify a timeout period, continue to "To Configure Approval Timeouts" on page 294 for instructions.
- If you do not want to specify a timeout period, you can continue to "Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)" on page 297 or save your changes and go on to configure a different tab.

▼ To Determine Additional Approvers From the Administrator List

Use the following steps to explicitly choose additional approvers from the administrators list.

1 **Select Administrator List from the Determine Additional Approvers from menu and new options display, as shown in the following figure.**

FIGURE 9–15 Additional Approvers: Administrators List



Additional Approvers

Determine additional approvers from: Administrator List

Approval Administrator

Available Administrators: Administrator, Configurator

Selected Administrators:

Approval times out after: ☐ 5 days

- **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.

The **Approval times out after**. Affects both initial approvals and escalated approvals.

2 **Select one or more administrators in the Available Administrators list and move the selected names 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 "To Configure Approval Timeouts" on page 294 for instructions.
- If you do not want to specify a timeout period, you can continue to "Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)" on page 297.

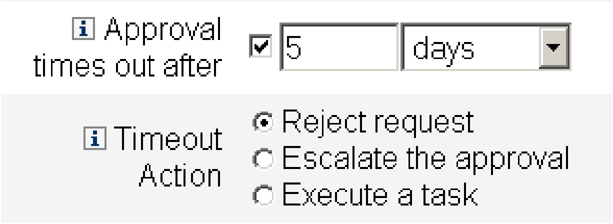
To Configure Approval Timeouts

Use the following steps to configure approval timeouts in the Approval times out after section.

1 **Select the Approval times out after checkbox.**

The adjacent text field and menu become active, and the Timeout Action options display, as shown in the following figure.

FIGURE 9–16 Approval Timeout Options



Approval times out after ☑ 5 days

Timeout Action ● Reject request ○ Escalate the approval ○ Execute a task

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 **Use the Timeout Action buttons to specify what happens when the approval request times out.**

Click one of the following:

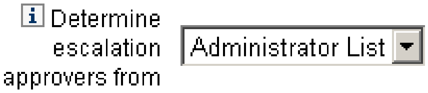
- **Reject Request**. Waveset automatically rejects the request if it is not approved before the specified timeout period.
- **Escalate the approval**. Waveset automatically escalates the request to another approver if the request is not approved before the specified timeout period.

  When you enable this button, new options display because you must specify how Waveset will determine approvers for an escalated approval. Continue to "To Configure the Determine Escalation Approvers From Section" on page 295 for instructions.
- **Execute a task**. Waveset 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 "To Configure the Approval Timeout Task Section" on page 297 for instructions.

▼ To Configure the Determine Escalation Approvers From Section

When you select Escalate the approval in the Timeout Action section ("To Configure Approval Timeouts" on page 294), the Determine escalation approvers from menu displays, as shown in the following figure.



Determine escalation approvers from: Administrator List

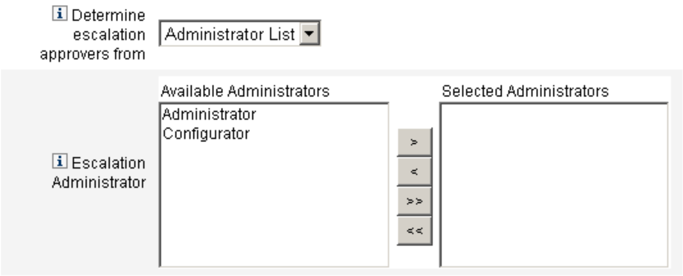
● **Choose an option from this menu to specify how approvers are determined for an escalated approval.**

The options include:

- **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 you select this option, the Escalation Administrator Attribute menu displays. Select an attribute from the list and the selected attribute displays in the adjacent text field, as shown in the following figure.



Determine escalation approvers from: Administrator List

Escalation Administrator

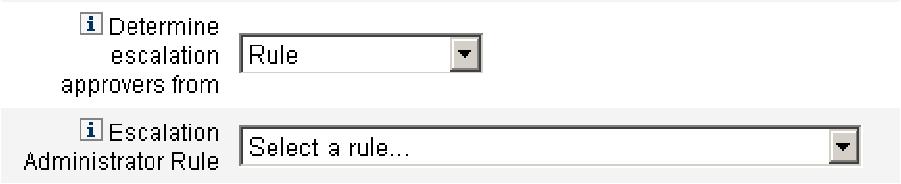
Available Administrators: Administrator, Configurator

Selected Administrators

- **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 you select this option, the Escalation Administrator Rule menu displays, as shown. Select a rule from the list.



Determine escalation approvers from: Rule

Escalation Administrator Rule: Select a rule...

- **Query**. Determine approvers account IDs by querying a particular resource.

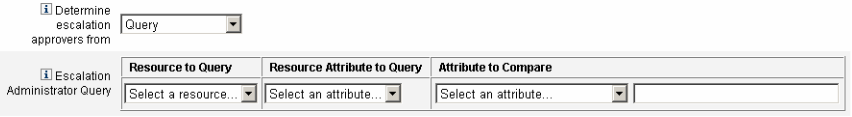
  The Escalation Administrator Query menus display as shown in the following figure.

  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.



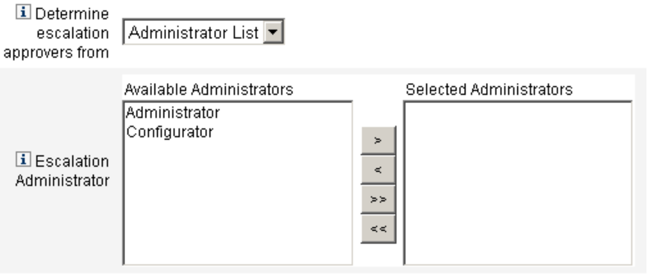
Determine escalation approvers from: Query

Escalation Administrator Query

Resource to Query	Resource Attribute to Query	Attribute to Compare
Select a resource...	Select an attribute...	Select an attribute...

- **Administrator List** (*default*). Choose approvers explicitly from a list.

The Escalation Administrator selection tool displays as shown in the following figure.



Determine escalation approvers from: Administrator List

Escalation Administrator

Available Administrators	Selected Administrators
Administrator Configurator	

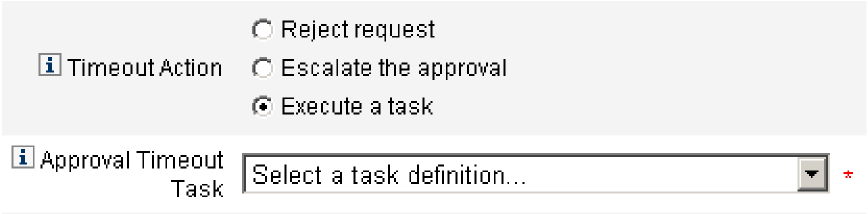
Select approvers as follows:

a. Select one or more administrator names from the Available Administrators list.

b. Move the selected names to the Selected Administrators list.

To Configure the Approval Timeout Task Section

When you select the Execute a task option in the Timeout Action section ("To Configure Approval Timeouts" on page 294), the Approval Timeout Task menu displays as shown in the following figure.



Timeout Action
○ Reject request
○ Escalate the approval
● Execute a task

Approval Timeout Task: Select a task definition... *

- **Choose a task definition to execute if the approval request times out.**

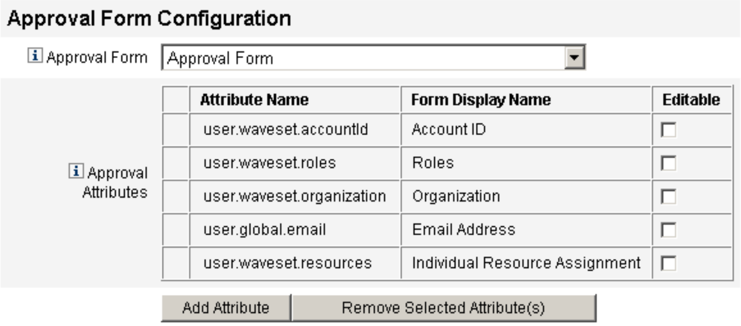
  For example, you might allow the requester to submit a help desk request or send a report to the Administrator.

Configuring the Approval Form (Approvals Tab, Approval Form Configuration Section)

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.

FIGURE 9–17 Approval Form Configuration



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	□

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 Attributes* buttons to specify attributes from the new user's account data to display in the approval form.**

- To add attributes to the form, see "To Add Attributes to the Approval Form" on page 299.
- To remove attributes from the form, see "To Remove Attributes From the Approval Form" on page 300.

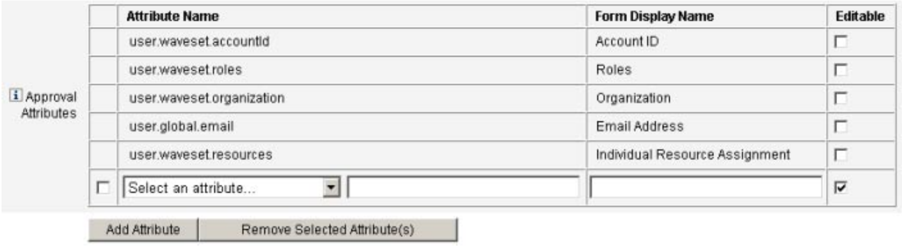
You cannot remove the default attributes from an approval form unless you modify the XML file.

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.

FIGURE 9–18 Adding Approval Attributes



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...			☑

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, you can:

- Change the default attribute name or the default Form Display Name if necessary by typing a new name into the appropriate text field.
- Enable the Editable checkbox to allow the approver to change the attribute's value.

  For example, the approver might want to override information such as the user's email address.

3 **Repeat these steps to specify additional attributes.**

▼ To Remove Attributes From the Approval Form

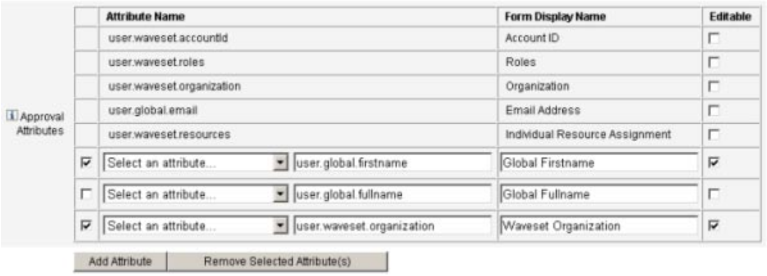
1 **Enable one or more checkboxes in the leftmost column of the Approval Attributes table.**

2 **Click the Remove Selected Attributes 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 Attributes button.

Note – You cannot remove the default attributes from an approval form unless you modify the XML file.

FIGURE 9–19 Removing Approval Attributes



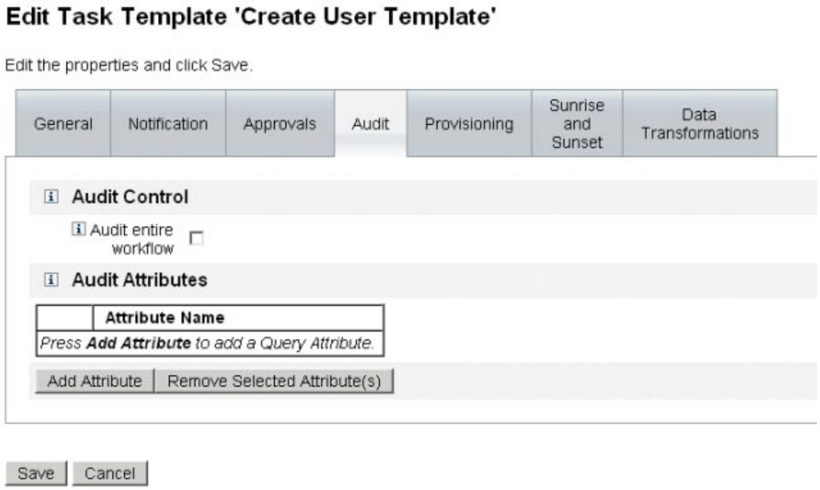
	Attribute Name		Form Display Name	Editable
	user.waveset.accountId		Account ID	☐
	user.waveset.roles		Roles	☐
	user.waveset.organization		Organization	☐
	user.global.email		Email Address	☐
	user.waveset.resources		Individual Resource Assignment	☐
☑	Select an attribute...	user.global.firstname	Global Firstname	☑
☐	Select an attribute...	user.global.fullname	Global Fullname	☐
☑	Select an attribute...	user.waveset.organization	Waveset Organization	☑

Configuring the Audit Tab

This section provides instructions for configuring the Audit tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.

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.

FIGURE 9–20 Audit Create User Template



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.*	

To Configure Auditing

1. **Select the Audit entire workflow checkbox to activate the workflow auditing feature.**

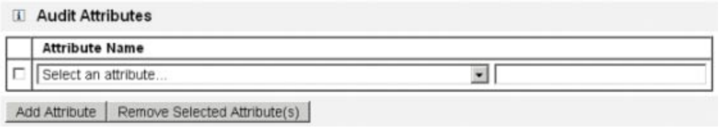
   For information about workflow auditing, see "Creating Audit Events From Workflows" on page 312. Note that auditing workflows degrades performance.

2. **Click the Add Attribute button located in the Audit Attributes section to select the attributes you want to audit for reporting purposes.**

3. **When the Select an attribute menu displays in the Audit Attributes table, select an attribute from the list.**

   The selected attribute name displays in the adjacent text field.

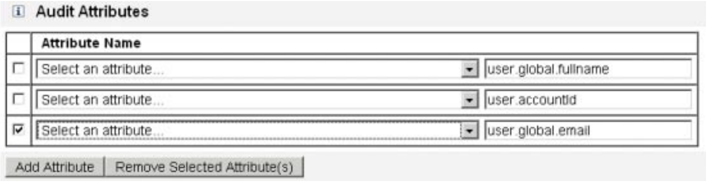
FIGURE 9–21 Adding an Attribute



To Remove Attributes

1 **Enable the checkbox adjacent to the attribute you want to remove.**

FIGURE 9–22 Removing the `user.global.email` Attribute



□ Select an attribute... user.global.fullname

□ Select an attribute... user.accountId

☑ Select an attribute... user.global.email

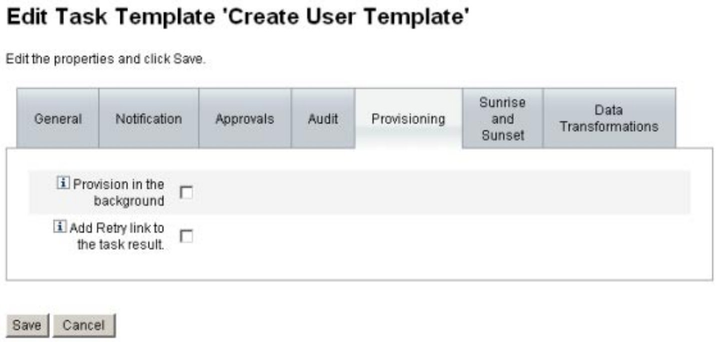
2 **Click the Remove Selected Attributes button.**

Configuring the Provisioning Tab

This section provides instructions for configuring the Provisioning tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see “Configuring the Task Templates” on page 279.

Note – This tab is available for the Create and Update User Templates only.

FIGURE 9–23 Provisioning Tab: Create User Template



Edit Task Template 'Create User Template'

Edit the properties and click Save.

Provision in the background □

Add Retry link to the task result. □

You can use the Provisioning tab to configure the following options, which are related to provisioning:

- **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 Waveset 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.

Configuring the Sunrise and Sunset Tab

This section provides instructions for configuring the Sunrise and Sunset tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.

Note – This tab is available for the Create User task template only.

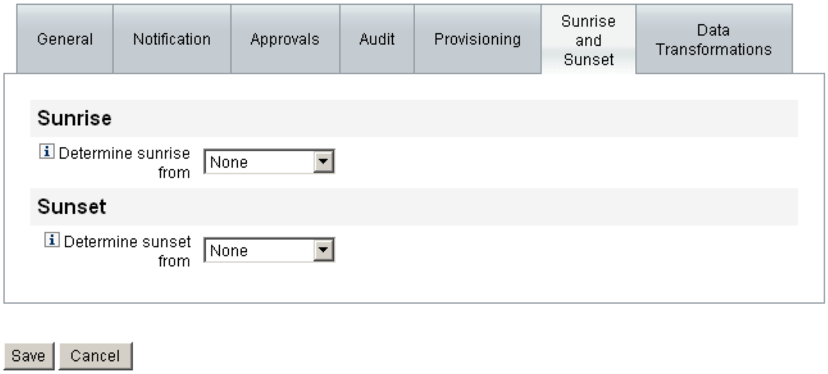
You use the Sunrise and Sunset tab to select a method for determining the time and date when the following actions will occur.

- 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.

Figure 9–24 illustrates the settings on the Sunrise and Sunset tab.

FIGURE 9–24 Sunrise and Sunset Tab: Create User Template



Sunrise

Determine sunrise from: None

Sunset

Determine sunset from: None

The topics that follow provide instructions for configuring the Sunrise and Sunset tab.

Configuring Sunrises

Configure the sunrise settings to specify the time and date when provisioning will take place for a new user, and to specify the user who will own the work item for sunrise.

1. Select one of the following options from the Determine sunrise from menu to specify how Waveset determines a time and date for provisioning.
   - **Specifying a Time**. Delays provisioning until a specified time in the future. Continue to “To Delay Provisioning Until a Specified Time” on page 305 for instructions.
   - **Specifying a Date**. Delays provisioning until a specified calendar date in the future. Continue to “To Delay Provisioning Until a Specified Calendar Date” on page 305 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 “To Determine Provisioning Date and Time by Specifying an Attribute” on page 306 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 “To Determine Provisioning Date and Time by Evaluating a Rule” on page 307 for instructions.

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.

▼ To Delay Provisioning Until a Specified Time

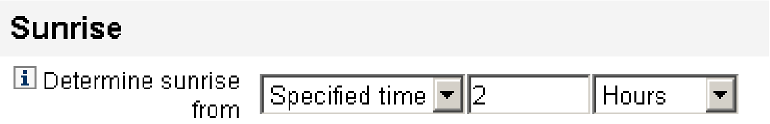
This section provides instructions to help you delay provisioning until a specific time.

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, to provision a new user in two hours, specify information shown in the following figure.

FIGURE 9–25 Provisioning a New User in Two Hours



Sunrise

Determine sunrise from: Specified time | 2 | Hours

▼ To Delay Provisioning Until a Specified Calendar Date

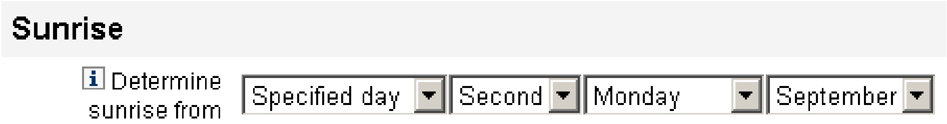
This section provides instructions to help you delay provisioning until a specific date.

1 **Select Specified day from the Determine sunrise from menu.**

2 **Use the menu options that appear to specify which week in the month, which day of the week, and which month the provisioning should occur.**

For example, to provision a new user on the second Monday in September, specify the following information.

FIGURE 9–26 Provisioning a New User by Date



Sunrise

Determine sunrise from: Specified day | Second | Monday | September

To Determine Provisioning Date and Time by Specifying an Attribute

This section provides instructions to help you determine a provisioning date and time based on attribute values in the users account data.

1 **Select Attribute from the Determine sunrise from menu.**

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).

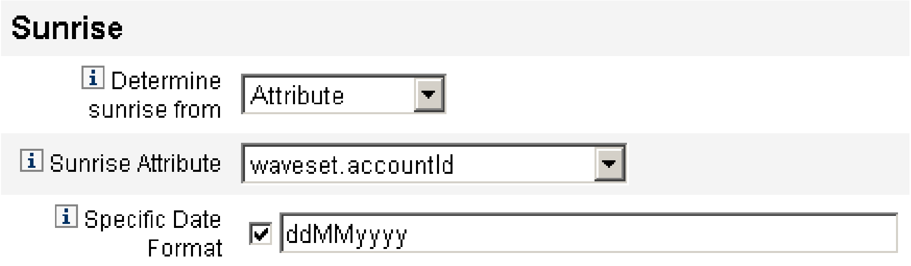
If you do not enable the Specific Date Format checkbox, date strings must conform to a format that is acceptable to the `FormUtil` method's `convertDateToString`. Consult the product documentation for a complete list of supported date formats.

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 information shown in the following figure.

FIGURE 9–27 Provisioning a New User by Attribute



Sunrise

Determine sunrise from: Attribute

Sunrise Attribute: waveset.accountId

Specific Date Format: ☑ ddMMyyyy

▼ To Determine Provisioning Date and Time by Evaluating a Rule

This section provides instructions to help you determine the provisioning date and time by evaluating a specific rule.

1 **Select Rule from the Determine sunrise from menu.**

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).

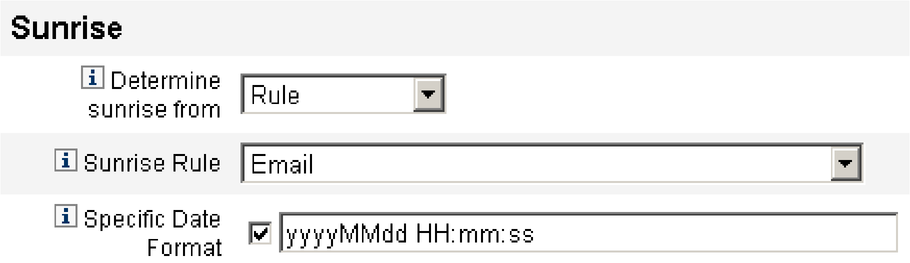
If you do not enable the Specific Date Format checkbox, date strings must conform to a format that is acceptable to the `FormUtil` method's `convertDateToString`. Consult the product documentation for a complete list of supported date formats.

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 information shown in the following figure.

FIGURE 9–28 Provisioning a New User by Using a Rule



Sunrise

Determine sunrise from: Rule

Sunrise Rule: Email

Specific Date Format: ☑ yyyyMMdd HH:mm:ss

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, perform the following steps.

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. See "To Delay Provisioning Until a Specified Time" on page 305for instructions.
- **Specified date**. Delays deprovisioning until a specified calendar date in the future. See "To Delay Provisioning Until a Specified Calendar Date" on page 305 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 "To Determine Provisioning Date and Time by Specifying an Attribute" on page 306 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.

  See "To Determine Provisioning Date and Time by Evaluating a Rule" on page 307 for instructions.

2. Use the Sunset Task menu to specify a task to deprovision the user on the specified date and time.

Configuring the Data Transformations Tab

This section provides instructions for configuring the Data Transformations tab, which is available as part of the task template configuration process. For instructions on how to start the configuration process see "Configuring the Task Templates" on page 279.

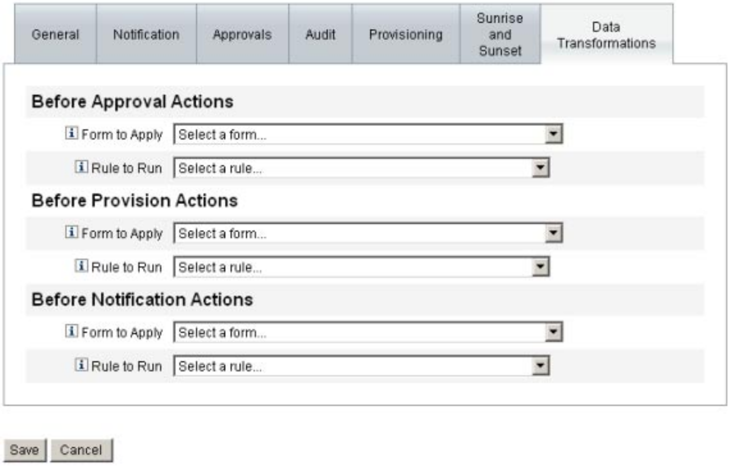
Note – This tab is available for the Create and Update User Templates only.

If you want to alter user account data as the workflow executes, you can use the Data Transformations tab to specify how Waveset 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.

FIGURE 9–29 Data Transformations Tab: Create User Template



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...

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.

CHAPTER 10

Audit Logging

This chapter describes how the auditing system records events.

The information is organized into the following topics:

Audit Logging Overview

The purpose of Waveset auditing is to record who did what to which Waveset objects, and when did they do it.

Audit events are handled by one or more publishers. By default, Waveset records audit events in the repository using the repository publisher. Filtering, with the help of audit groups, allows the administrator to select a subset of audit events for recording. Each publisher can be assigned one or more audit groups that are enabled initially.

Note – For information about monitoring and managing user violations, see Chapter 13, "Identity Auditing: Basic Concepts"

What Does Waveset Audit?

Most default auditing is carried out by internal Waveset components. There are, however, interfaces that allow events to be generated from workflows or from Java code.

The default Waveset audit instrumentation focuses on four main areas:

- **Provisioner**. An internal component known as the provisioner may generate audit events.
- **View Handlers**. In the view architecture, the view handler generates audit records. A view handler should always audit when objects are created or modified.
- **Session**. The session methods (such as `checkinObject`, `createObject`, `runTask`, `login`, and `logout`) create an audit record after completing an auditable operation. Most of the instrumentation is pushed into the view handlers.
- **Workflow**. By default, only the approval workflows are instrumented to generate audit records. These generate an audit event when requests are approved or rejected. The workflow feature's interface to the audit logger is through the `com.waveset.session.WorkflowServices` application. See the next section for more information.

Creating Audit Events From Workflows

By default, only the approval workflows are instrumented to generate audit records. This section describes how to use the `com.waveset.session.WorkflowServices` application to generate extra audit events from any workflow process.

Additional audit events may be required if you need to report on custom workflows. See "Modifying Workflows to Log Standard Audit Events" on page 313 for information on adding audit events to workflows.

Special audit events can also be added to workflows in support of Workflow Reports ("Workflow Reports" on page 262). Workflow Reports report the amount of time it takes for workflows to complete. Special audit events are required to store the data necessary for time computations. See "Modifying Workflows to Log Timing Audit Events" on page 315 for information on adding timing audit events to workflows.

The `com.waveset.session.WorkflowServices` Application

The `com.waveset.session.WorkflowServices` application generates audit events from any workflow process. Table 10–1 describes the arguments that are available for this application.

TABLE 10–1 Arguments for com.waveset.session.WorkflowServices

Argument	Type	Description
op	String	Operation for WorkflowServices. Must be set to audit or auditWorkflow. Use audit for standard workflow auditing. Use auditWorkflow to store timing audit events required for time computations. Required.
type	String	Name of the object type that is being audited. Auditable object types are listed in Table B–5. Required to log standard audit events.
action	String	Name of the action performed. Auditable actions are listed in Table B–6. Required.
status	String	Name of the status for the specified action. Status is listed in Table B–7 (in the Results column). Required to log standard audit events.
name	String	Name of the object being affected by the specified action. Required to log standard audit events.
resource	String	(*Optional*) Name of the resource where the object being changed resides.
accountId	String	(*Optional*) Account ID that is being modified. This should be a native resource account name.
error	String	(*Optional*) Localized error string to accompany any failures.
reason	String	(*Optional*) Name of the ReasonDenied object, which maps to an internationalized message describing the causes of common failures.
attributes	Map	(*Optional*) Map of attribute names and values that were added or modified.
parameters	Map	(*Optional*) Maps up to five additional names or values that are relevant to an event.
organizations	List	(*Optional*) List of organization names or IDs where this event will be placed. This is used for organizational scoping of the audit log. If not present, the handler will attempt to resolve the organization based on the type and name. If the organization cannot be resolved, the event is placed in Top (the highest level of the organizations hierarchy).
originalAttributes	Map	(*Optional*) Map of old attribute values. The names should match the ones listed in the attributes argument. The values will be any previous value you want to save in your audit log.

Modifying Workflows to Log Standard Audit Events

To create a standard audit event in a workflow, add the following <Activity> element to the workflow:

```
<Activity name='createEvent'>
```

Next, nested in the `<Activity>` element, include an `<Action>` element that references the `com.waveset.session.WorkflowServices` application:

```
<Action class='com.waveset.session.WorkflowServices'>
```

Nested in the `<Action>` element, include the required and optional `<Argument>` elements. See Table 10–1 for a list of the arguments.

To log standard audit events, the op argument must be set to `audit`.

Following are two examples that show the minimum code required to create a standard audit event.

The first example illustrates a simple workflow activity and shows the generation of an event that will log a resource deletion activity named `ADSIResource1`, performed by `ResourceAdministrator`.

EXAMPLE 10–1 Simple Workflow Activity

```
<Activity name='createEvent'> <Action class='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='Resource'/>
<Argument name='action' value='Delete'/> <Argument name='status' value='Success'/>
<Argument name='subject' value='ResourceAdministrator'/>
<Argument name='name' value='ADSIResource1'/> </Action> <Transition to='end'/> </Activity>
```

The second example illustrate how you can add specific attributes to a workflow that tracks the changes applied by each user in an approval process to a granular level. This addition typically will follow a `ManualAction` that solicits input from a user.

`ACTUAL_APPROVER` is set in the form and in the workflow (if approving from the approvals table) based on the person who actually performed the approval. `APPROVER` identifies the person to whom it was assigned.

EXAMPLE 10–2 Attributes Added to Track Changes in an Approval Process

```
<Action name='Audit the Approval' application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='User'/>
<Argument name='name' value='$(CUSTOM_DESCRIPTION)'/> <Argument name='action' value='approve'/>
<Argument name='accountId' value='$(accountId)'/> <Argument name='status' value='success'/>
<Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
<Argument name='loginApplication' value='$(loginApplication)'/>
<Argument name='attributes'> <map>
<s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
<s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
<s>location</s><ref>user.accounts[Lighthouse].location</ref>
<s>team</s><ref>user.waveset.organization</ref> <s>agency</s>
<ref>user.accounts[Lighthouse].agency</ref> </map> </Argument>
<Argument name='originalAttributes'> <map> <s>fullname</s> <s>User's previous fullname</s>
<s>jobTitle</s> <s>User's previous job title</s> <s>location</s> <s>User's previous location</s>
```

EXAMPLE 10–2 Attributes Added to Track Changes in an Approval Process *(Continued)*

```
<s>team</s> <s>User’s previous team</s> <s>agency</s> <s>User’s previous agency</s> </map>
</Argument> <Argument name=’attributes’> <map> <s>firstname</s> <s>Joe</s> <s>lastname</s>
<s>New</s> </map> </Argument> <Argument name=’subject’> <or> <ref>ACTUAL_APPROVER</ref>
<ref>APPROVER</ref> </or>
</Argument> <Argument name=’approver’ value=’$(APPROVER)’/> </Action>
```

Modifying Workflows to Log Timing Audit Events

Workflows can be modified to log timing events in support of Workflow Reports (“Workflow Reports” on page 262). Standard audit events only log that an event occurred; Timing audit events log when an event started and stopped, making it possible to perform time computations. In addition to timing event data, most of the information logged by standard audit events is also stored. See “What Information Do Timing Audit Events Store?” on page 316 for more information.

Note – To log timing audit events, you must first activate workflow auditing for each workflow type that you plan to audit.

- For workflows that you can configure in the Administrator interface using task templates, first enable the task template that corresponds to the workflow that you want to audit. See “Enabling the Task Templates” on page 275 for instructions.

  Next, turn on workflow auditing by selecting the Audit entire workflow checkbox. See “Configuring the Audit Tab” on page 300 for instructions.
- For workflows that do not have task templates, instead define a variable named `auditWorkflow` and set its value to `true`.

Note that auditing workflows degrades performance.

The Example 10–3 example shows the code required to create timing audit events. To log timing audit events, the `op` argument must be set to `auditWorkflow`.

The `action` argument is also required and must be set to one of the following values:

- `StartWorkflow`
- `EndWorkflow`
- `StartProcess`
- `EndProcess`
- `StartActivity`
- `EndActivity`

Additional action arguments may be defined in `auditconfig.xml`.

Examples: Starting and Stopping Audit Events in a Workflow

Example 10–3 illustrates enabling timing audit events in a workflow. To instrument a workflow, auditWorkflow events should be added at the beginning and end of workflows, processes, and activities.

The auditWorkflow operation is defined in com.waveset.session.WorkflowServices. See "The com.waveset.session.WorkflowServices Application" on page 312 for more information.

EXAMPLE 10–3 Starting Timing Audit Events in a Workflow

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/>
<Argument name='action' value='StartWorkflow'/>
</Action>
```

To stop logging timing audit events in a workflow, add the code in Example 10–4 to a pre-end activity near the conclusion of the workflow. Note that, when instrumenting a workflow or process, you are not permitted to put anything in an end activity. You must create a pre-end activity that performs the final auditWorkflow event, and then unconditionally transition to the end event.

EXAMPLE 10–4 Stopping Timing Audit Events in a Workflow

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/> <Argument name='action' value='EndWorkflow'/>
</Action>
```

What Information Do Timing Audit Events Store?

By default, timing audit events log most of the information stored by regular audit events, including the following attributes:

Attribute	Description
WORKFLOW	Name of the workflow being executed
PROCESS	Name of the current process being executed
INSTANCEID	Unique instance ID of the workflow being executed
ACTIVITY	Activity in which the event is being logged
MATCH	Unique identifier within a workflow instance

The above attributes are stored in the logattr table and they come from auditableAttributesList. Waveset also checks whether the workflowAuditAttrConds attribute is defined.

It is possible to call some activities several times within a single instance of a process or a workflow. To match the audit events for a particular activity instance, Waveset stores a unique identifier within a workflow instance in the `logattr` table.

To store additional attributes in the `logattr` table for a workflow, you must define a `workflowAuditAttrConds` list, which is assumed to be a list of `GenericObjects`. If you define an `attrName` attribute within the `workflowAuditAttrConds` list, Waveset pulls `attrName` out of the object within the code, first using `attrName` as the key, and then storing the `attrName` value. All keys and values are stored as uppercase values.

Audit Configuration

Audit configuration is composed of one or more publishers and several predefined groups.

An audit group defines a subset of all audit events based on object types, actions, and action results. Each publisher is assigned one or more audit groups. By default, the repository publisher is assigned to all audit groups.

An audit publisher delivers audit events to a particular audit destination. The default repository publisher writes audit records into the repository. Each audit publisher may have implementation specific options. Audit publishers may have a text formatter assigned. (Text formatters provide textual representation of audit events.)

The Audit Configuration (`#ID#Configuration:AuditConfiguration`) object is defined in the `sample/auditconfig.xml` file. This configuration object has an extension that is a generic object.

At the top level, this configuration object has the following attributes:

- "The `filterConfiguration` Attribute" on page 317
- "The `extendedTypes` Attribute" on page 323
- "The `extendedActions` Attribute" on page 324
- "The `extendedResults` Attribute" on page 325
- "The `publishers` Attribute" on page 325

The `filterConfiguration` Attribute

The `filterConfiguration` attribute lists event groups, which are used to enable one or more events to pass through the event filter. Each group listed in the `filterConfiguration` attribute contains the attributes listed in Table 10–2.

TABLE 10–2 `filterConfiguration` Attributes

Attribute	Type	Description
`groupName`	String	Event group name
`displayName`	String	Message catalog key representing the group name
`enabled`	String	Boolean flag indicating whether the entire group is enabled or disabled. This attribute is an optimization for the filtering object.
`enabledEvents`	List	List of generic objects that describe which events a group enables. An event must be listed to enable its logging. Each object listed must have these attributes: ■ `objectType` (String)– `objectType` Name. ■ `actions` (List)– List of one or more actions. ■ `results` (List)– List of one or more results.

Example 10–5 illustrates the default Resource Management group.

EXAMPLE 10–5 Default Resource Management Group

```
<Object name=’Resource Management’> <Attribute name=’enabled’ value=’true’/>
<Attribute name=’displayName’ value=’UI_RESOURCE_MGMT_GROUP_DISPLAYNAME’/>
<Attribute name=’enabledEvents’> <List> <Object> <Attribute name=’objectType’ value=’Resource’/>
<Attribute name=’actions’ value=’ALL’/> <Attribute name=’results’ value=’ALL’/> </Object> <Object>
<Attribute name=’objectType’ value=’ResourceObject’/> <Attribute name=’actions’ value=’ALL’/>
<Attribute name=’results’ value=’ALL’/> </Object> </List> </Attribute> </Object>
```

Waveset provides default audit event groups. These groups, and the events they enable, are described in the following sections:

- “Account Management” on page 319
- “Logins/Logoffs Group” on page 319
- “Report Modifications” on page 319
- “Password Management” on page 320
- “Resource Management” on page 320
- “Role Management” on page 320
- “Security Management” on page 320
- “Task Management” on page 321
- “Changes Outside Identity System” on page 321
- “Configuration Management” on page 321
- “Service Provider” on page 322
- “Event Management” on page 322
- “Compliance Management” on page 322

You can configure each group from the Audit Configuration page of the Waveset Administrator interface (Configure > Audit). See “Configuring Audit Groups and Audit Events” on page 102 for instructions.

The Audit Configuration page allows you to configure successful or failed events for each group. The interface does not support adding or modifying enabled events for groups, but you can do this by using the Waveset debug pages (see "The Waveset Debug Page" on page 42).

The default event groups and the events they enable are described in the following sections.

Note – Setting the *Actions* value to **`All`** does not specify a default set of actions for the object type. Rather, the `All` value means that there are no actions specified for the object type, and that Waveset can audit any action for the object type.

Account Management

This group is enabled by default.

TABLE 10–3 Default Account Management Event Groups

Type	Actions
`EncryptionKey`	All Actions
`Identity System Account`	All Actions
`Resource Account`	Approve, Create, Delete, Disable, Enable, Modify, Pending Create, Pending Delete, Pending Disable, Pending Enable, Pending Rename, Pending Update, Reject, Rename, Unlock
`Provisioning Request`	Completed, Not Completed
`Workflow Case`	End Activity, End Process, End Workflow, Start Activity, Start Process, Start Workflow
`User`	Approve, Create, Delete, Deprovision, Disable, Enable, Modify, Reject, Rename

Logins/Logoffs Group

This group is enabled by default.

TABLE 10–4 Default Waveset Logins/Logoffs Event Groups

Type	Actions
`User`	Credentials Expired, Lock, Login, Logout, Unlock, Username Recovery

Report Modifications

This group is enabled by default.

TABLE 10–5 Default Waveset Report Modifications Event Groups

Type	Actions
`TaskTemplate`	Create, Delete, Disable, Enable, Modify

Password Management

This group is enabled by default.

TABLE 10–6 Default Password Management Event Groups and Events

Type	Actions
Resource Account	Change Password, Reset Password

Resource Management

This group is enabled by default.

TABLE 10–7 Default Resource Management Event Groups and Events

Type	Actions
`Resource`	All Actions
`ResourceForm`	All Actions
`ResourceObject`	All Actions
`Workflow Case`	End Activity, End Process, End Workflow, Start Activity, Start Process, Start Workflow
`ResourceAction`	All Actions
`AttrParse`	All Actions

Role Management

This group is disabled by default.

TABLE 10–8 Default Role Management Event Groups and Events

Type	Actions
`Role`	All Actions

Security Management

This group is enabled by default.

TABLE 10–9 Default Security Management Event Groups and Events

Type	Actions
`Capability`	All Actions
`EncryptionKey`	All Actions
`Organization`	All Actions
`Admin Role`	All Actions

Task Management

This group is disabled by default.

TABLE 10–10 Task Management Event Groups and Events

Type	Actions
`ProvisioningTask`	All Actions
`TaskDefinition`	All Actions
`TaskInstance`	All Actions
`TaskSchedule`	All Actions
`TaskResult`	All Actions

Changes Outside Identity System

This group is disabled by default.

TABLE 10–11 Changes Outside Waveset Event Groups and Events

Type	Actions
`ResourceAccount`	`NativeChange`

Configuration Management

This group is enabled by default.

TABLE 10–12 Default Configuration Management Event Groups

Type	Actions
`Configuration`	All Actions
`Data Exporter`	All Actions

TABLE 10–12 Default Configuration Management Event Groups *(Continued)*

Type	Actions
`Database Connection`	All Actions
`EmailTemplate`	All Actions
`Log`	All Actions
`LoginConfig`	All Actions
`Policy`	All Actions
`Rule`	All Actions
`UserForm`	All Actions
`XmlData`	Import

Service Provider

This group is enabled by default.

TABLE 10–13 Service Provider Event Groups and Events

Type	Actions
`Directory User`	Challenge Response, Create, Delete, Modify, Post-Operation Callout, Pre-Operation Callout, Update Authentication Answers, Username Recovery

Event Management

This group is enabled by default.

TABLE 10–14 Default Event Management Event Groups

Type	Actions
`Email`	Notify
`TestNotification`	Notify

Compliance Management

This group is enabled by default.

TABLE 10–15 Default Compliance Management Group Events

Type	Actions
`Audit Policy`	All Actions

TABLE 10–15 Default Compliance Management Group Events *(Continued)*

Type	Actions
AccessScan	All Actions
ComplianceViolation	All Actions
Data Exporter	All Actions
UserEntitlement	Attestor Approved, Attestor Rejected, Remediation Requested, Rescan Requested, Terminate
Access Review Workflow	All Actions
Remediation Workflow	All Actions

The extendedTypes Attribute

Each new Type that you add to the com.waveset.object.Type class can be audited. A new Type must be assigned a unique two-character database key, which is stored in the database. All new Types are added to the various audit reporting interfaces. Each new Type to be logged to the database without being filtered must be added to an audit event groups enabledEvents attribute (as described with the enabledEvents attribute).

There may be situations in which you want to audit something that does not have an associated com.waveset.object.Type, or where you want to represent an existing type with more granularity.

For example, the WSUser object stores all of the user's account information in the repository. Instead of marking each event as a USER type, the auditing process splits the WSUser object into two different audit types (Resource Account and Waveset Account). Splitting the object in this way makes it easier to find specific account information in the audit log.

Add extended audit types by adding to the extendedObjects attribute. Each extended object must have the attributes listed in the following table.

TABLE 10–16 Extended Object Attributes

Argument	Type	Description
name	String	The name of the type, which is used when constructing AuditEvents and during event filtering.
displayName	String	A message catalog key that represents the name of the type.
logDbKey	String	Two-character database key to use when storing this object in the Log table. See "Audit Log Database Mappings" on page 534 for reserved values.

TABLE 10–16 Extended Object Attributes *(Continued)*

Argument	Type	Description
`supportedActions`	List	Actions supported by the object type. This attribute will be used when creating audit queries from the user interface. If this value is null, all actions will be displayed as possible values to be queried for this object type.
`mapsToType`	String	(Optional) The name of the `com.waveset.object.Type` that maps to this type, if applicable. This attribute is used when attempting to resolve an object organizational membership if not already specified on the event.
`organizationalMembership`	List	(Optional) A default list of organization IDs where events of this type should be placed, if they do not already have assigned organizational membership.

All customer-specific keys should start with the # symbol to prevent duplicate keys when new internal keys are added.

Example 10–6 illustrates the extended-type Waveset Account.

EXAMPLE 10–6 Extended Type Waveset Account

```
<Object name='LighthouseAccount'> <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
<Attribute name='logDbKey' value='LA'/> <Attribute name='mapsToType' value='User'/>
<Attribute name='supportedActions'> <List> <String>Disable</String> <String>Enable</String>
<String>Create</String> <String>Modify</String> <String>Delete</String> <String>Rename</String>
</List> </Attribute> </Object>
```

The `extendedActions` Attribute

Audit actions typically map to `com.waveset.security.Right` objects. When adding new Right objects, you must specify a unique two-character `logDbKey`, which will be stored in the database. You may encounter situations where there is no right to correspond to a particular action that must be audited. You can extend actions by adding them to the list of objects in the `extendedActions` attribute.

Each `extendedActions` object must include the attributes listed in Table 10–17.

TABLE 10–17 `extendedAction` Attributes

Attribute	Type	Description
`name`	String	The name of the action, which is used when constructing AuditEvents and during event filtering.
`displayName`	String	A message catalog key that represents the name of the action.

TABLE 10–17 `extendedAction` Attributes *(Continued)*

Attribute	Type	Description
`logDbKey`	String	Two-character database key to use when storing this action in the Log table. See "Audit Log Database Mappings" on page 534 for reserved values.

All customer-specific keys should start with the # symbol to prevent duplicate keys when new internal keys are added.

Table 10–17 illustrates adding an action for Logout.

EXAMPLE 10–7 Adding an Action for Logout

```
<Object name='Logout'> <Attribute name='displayName' value='LG_LOGOUT'/>
<Attribute name='logDbKey' value='LO'/> </Object>
```

The `extendedResults` Attribute

In addition to extending audit types and actions, you can add results. By default, there are two results: *Success* and *Failure*. You can extend results by adding them to the list of objects in the `extendedResults` attribute.

Each `extendedResults` object must include the attributes described in Table 10–18.

TABLE 10–18 `extendedResults` Attributes

Attribute	Type	Description
`name`	String	The name of the result, which is used when setting the status on AuditEvents and during event filtering.
`displayName`	String	A message catalog key that represents the name of a result.
`logDbKey`	String	One-character database key to use when storing this result in the Log table. See the section titled Database Keys for reserved values.

All customer-specific keys should use the range 0–9 to prevent duplicate keys when new internal keys are added.

The `publishers` Attribute

Each item in the `publishers` list is a generic object. Each `publishers` object has the following attributes.

TABLE 10–19 publishers Attributes

Attribute	Type	Description
class	String	The name of the publisher class.
displayName	String	A message catalog key that represents the name of the publisher.
description	String	A description of the publisher.
filters	List	A list of audit groups assigned to this publisher.
formatter	String	The name of the text formatter (if any).
options	List	A list of publisher options. These options are publisher specific; each item in the list is a map representation of PublisherOption. See sample/auditconfig.xml for examples.

Database Schema

There are two tables in the Waveset repository that are used to store audit data:

- waveset.log– Stores most of the event details.
- waveset.logattr– Stores the IDs of the organizations to which each event belongs.

These tables are discussed first in this section.

When audit log data exceeds the column length limits specified for the above tables, Waveset truncates the data to fit. Audit log truncation is discussed on "Audit Log Truncation" on page 329.

A few columns in the audit log have configurable column length limits. To find out about these columns and learn how to change their length limits, see "Audit Log Configuration" on page 329.

The waveset.log Table

This section describes the various column names and data types found in the waveset.log table. The data types are taken from the Oracle database definition and vary slightly from database to database. For a list of data schema values for all supported databases, see Appendix B, "Audit Log Database Schema"

A few of the column values are stored as keys in the database for space optimization. For key definitions, see the section titled "Audit Log Database Mappings" on page 534.

- objectType CHAR(2) – A two-character key that represents the object type that is being audited.

- action CHAR(2) – A two-character key that represents the action that was performed.
- actionStatus CHAR(1) – A one-character key that represents the result of the action that was performed.
- reason CHAR(2) – A two-character database key to describe a ReasonDenied object if there was a failure. ReasonDenied is a class that wraps a message catalog entry and is used for common failures such as invalid credentials and insufficient privileges.
- actionDateTimeVARCHAR(21) – The date and time in which the above action took place. This value is stored in GMT time.
- objectName VARCHAR(128) – The name of the object that was acted on during an operation.
- resourceName VARCHAR(128) – The resource name that was used during an operation, if applicable. Some events do not reference resources; however, in many situations it gives greater detail to log the resource where an operation has performed.
- accountName VARCHAR(255) – The account ID being acted on, if applicable.
- server VARCHAR(128) – The server where the action was performed (automatically assigned by the event logger).
- message VARCHAR(255*)or CLOB – Any localized messages associated with an action including things like error messages. The text is stored localized so it will not be internationalized. The column length limit for this column is configurable. The default data type is VARCHAR and the default size limit is 255. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.
- interface VARCHAR(50) – The Waveset interface (such as the Administrator, User, IVR, or SOAP interface) from which the operation was performed.
- acctAttrChanges VARCHAR(4000) to CLOB – Stores the account attributes that have changed during a create and update. The attributes changes field is always populated during a create or update for a resource account or Waveset account object. All of the attributes changed during an action are stored in this field as a string. The data is in NAME=VALUE NAME2=VALUE2 format. This field can be queried by executing "contains" SQL statements against the name or value.

  The following code example illustrates a value in the acctAttrChanges column.

  ```
  COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH DESCRIPTION"
  FAX NUMBER="5122222222" HOME ADDRESS="12282 MOCKINGBIRD LANE" HOME CITY="AUSTIN"
  HOME PHONE="5122495555" HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
  MOBILE PHONE="5125551212" WORK PHONE="5126855555" EMAIL="someone@somecompany.COM"
  EXPIREPASSWORD="TRUE" FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
  ```

Note – If your Waveset installation uses an Oracle repository, and you notice truncation errors in the audit log, you can convert the `accountAttrChanges` field in the audit log table from `VARCHAR(4000)` to `CLOB`. Waveset provides a sample DDL script in the `/web/sample` directory that converts `log.acctAttrChanges` from `VARCHAR(4000)` to `CLOB`. The `convert_log_acctAttrChangesCHAR2CLOB.oracle.sql` script preserves existing data and allows more than 4000 characters in the `accountAttrChanges` field.

This conversion is optional and should only be performed if you notice truncation errors. Also, be sure to back up the affected tables before running the conversion script.

After running the conversion script, stop and restart your web application server. When you run a new report, it should display correctly.

- `acctAttr01label-acctAttr05label` `VARCHAR(50)` – These five additional `NAME` slots are columns that can promote up to five attribute names to be stored in their own column instead of in the big blob. You can promote an attribute from the Resource Schema Configuration page using the "`audit?`" setting, and the attribute will be available for data mining.
- `acctAttr01value-acctAttr05value` `VARCHAR(128)` – Five additional `VALUE` slots that can promote up to five attribute values to be stored in a separate column instead of in the blob column.
- `parm01label-parm05label` `VARCHAR(50)` – Five slots used to store parameters associated with an event. Examples of these are Client IP and Session ID names.
- `parm01value-parm05value` `VARCHAR(128*)`or `CLOB` – Five slots used to store parameters associated with an event. Examples of these are Client IP and Session ID values. The column length limit for these columns is configurable. The default data type is `VARCHAR` and the default size limit is 128. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.
- `id` `VARCHAR(50)` – Unique ID assigned to each record by the repository referenced in the `waveset.logattr` table.
- `name` `VARCHAR(128)` – Generated name assigned to each record.
- `xml` `BLOB` – Used internally by Waveset.

The `waveset.logattr` Table

The `waveset.logattr` table is used to store IDs of the organizational membership for each event, which is used to scope the audit log by organization.

- `id` `VARCHAR(50)` – ID of the `waveset.log` record.
- `attrname` `VARCHAR(50)` – Currently, always `MEMBEROBJECTGROUPS`.
- `attrval` `VARCHAR(255)` – ID of the `MemberObject` group where the event belongs.

Audit Log Truncation

When one or more columns of audit log data exceed the specified column length limits, the column data is truncated to fit. Specifically, the data is truncated to the specified limit, less three characters. An ellipsis (...) is then appended to the column data to indicate truncation has occurred.

In addition, the `NAME` column of that audit record is prepended with the string `#TRUNCATED#` to facilitate querying of truncated records.

Note – Waveset assumes UTF–8 encoding when it computes where to truncate messages. If your configuration uses encoding other than UTF–8, there is a chance that truncated data may still exceed the actual column size in your database. If this happens, the truncated message does not appear in the audit log and an error is written in the system log.

Audit Log Configuration

Certain columns in the Audit Log can be configured to store large amounts of data in the repository.

Resizing Column Length Limits

Several columns in the audit log have configurable column length limits. These columns are:

- The `message` column
- The `parmNNvalue` columns (where `NN` = `01`, `02`, `03`, `04`, or `05`)
- The `xml` column

Note – For audit log column descriptions see “Database Schema” on page 326.

Column length limits can be changed by editing the `RepositoryConfiguration` object. For instructions on editing the `RepositoryConfiguration` object, see “Editing Waveset Configuration Objects” on page 108.

- To change the column length limit for the `message` column, modify the `maxLogMessageLength` value.
- To change the column length limit for the `parmNNvalue` column, modify the `maxLogParmValueLength` value. The same limit value applies to all five columns. (Individual column length values cannot be defined.)
- To change the column length limit for the `xml` column, modify the `maxLogXmlLength` value.

A server restart is required in order for the new values to take effect.

The column length limit settings in the `RepositoryConfiguration` object determine the maximum amount of data that can be stored in a column. If the data to be stored exceeds these settings, Waveset truncates the data. See "Audit Log Truncation" on page 329 for more information.

If you increase a column length setting in the `RepositoryConfiguration` object, also verify that the column size setting in your database is at least as large as the size configured in the `RepositoryConfiguration` object.

Removing Records from the Audit Log

The audit log should be truncated periodically to keep it from growing too large. Use the AuditLog Maintenance Task to schedule a task that removes old records from the audit log.

1. **In the Administrator interface, click Server Tasks → Manage Schedule.**
2. **In the Tasks Available for Scheduling section, click the AuditLog Maintenance Task**.

   The Create New AuditLog Maintenance Task Task Schedule page displays.
3. **Complete the form and click Save.**

Using Custom Audit Publishers

Waveset can submit audit events to custom audit publishers.

The following custom publishers are provided:

- **Console**. Prints audit events to the standard output or standard error.
- **File**. Writes audit events to a flat file.
- **JDBC**. Records audit events in a JDBC datastore.
- **JMS**. Records audit events in a JMS queue or topic.
- **JMX**. Publishes audit events so that a JMX (Java Management Extensions) client can monitor Waveset audit log activity.
- **Scripted**. Allows for custom scripts to store audit events.

If you want to create your own publisher, see "Developing Custom Audit Publishers" on page 338.

The information in this section includes the following topics:

- "To Enable Custom Audit Publishers" on page 331
- "The Console, File, JDBC, & Scripted Publisher Types" on page 331

- "The JMS Publisher Type" on page 331
- "The JMX Publisher Type" on page 333

▼ To Enable Custom Audit Publishers

Custom audit publishers are enabled from the Audit Configuration page.

1. **In the Administrator interface, click Configure in the main menu, then click Audit in the secondary menu.**

   The Audit Configuration page opens.

2. **Select the Use custom publisher option at the bottom of the page.**

   A table opens listing the currently configured audit publishers.

3. **To configure a new audit publisher, select the custom publisher type from the New Publisher drop-down menu.**

   Complete the Configure New Audit Publisher form. Click OK.

4. **Important! Click Save to save the new audit publisher!**

The Console, File, JDBC, & Scripted Publisher Types

To enable the Console, File, JDBC, or Scripted audit publishers, follow the steps in "To Enable Custom Audit Publishers" on page 331. Select the appropriate publisher type from the New Publisher drop-down menu.

Complete the Configure New Audit Publisher form. If you have questions about the form, refer to the i-Helps and online Help.

- The Console audit publisher prints audit events to either standard out or to standard error.
- The File audit publisher writes audit events to a flat file.
- The JDBC audit publisher records audit events in a JDBC datastore.
- The Scripted audit publisher allows custom scripts written in JavaScript or BeanShell to store audit events.

The JMS Publisher Type

The JMS audit log custom publisher makes it possible to publish audit event records to a JMS (Java Message Service) queue or topic.

Why Use JMS?

Publishing to JMS provides additional flexibility for correlation in environments that have multiple Waveset servers. In addition, JMS can be used in situations where there are restrictions on using the File audit log publisher, for example in Windows environments where the log may not be accessible to a client reporting tool while the server is running.

JMS offers several benefits for environments with multiple servers:

- The JMS message store centralizes (and simplifies) message storage and retrieval.
- The JMS architecture does not place restrictions on how many clients can access the service.
- The JMS protocol is easy to send through firewalls and other network infrastructure.

Point-to-Point or Publish-and-Subscribe?

Java Message System provides two models for messaging: the point-to-point or queuing model, and the publish and subscribe or topic model. Waveset supports both models.

In the point-to-point model, a producer posts messages to a particular queue and a consumer reads messages from the queue. Here, the producer knows the destination of the message and posts the message directly to the consumer's queue.

The point-to-point model has the following characteristics:

- Only one consumer will get the message.
- The producer does not have to be running at the time the receiver consumes the message, nor does the receiver need to be running at the time the message is sent.
- Every message successfully processed is acknowledged by the receiver.

The publish and subscribe model, on the other hand, supports publishing messages to a particular message topic. Zero or more subscribers may register interest in receiving messages on a particular message topic. In this model, neither the publisher nor the subscriber know about each other. A good metaphor for this model is the anonymous bulletin board.

The publish and subscribe model has the following characteristics:

- Multiple consumers can receive messages.
- A timing dependency exists between publishers and subscribers. The publisher has to create a subscription before clients can subscribe. Once subscribed, subscribers have to remain continuously active to receive messages, unless a durable subscription has been established. In the case of a durable subscription, messages published while the subscriber is not connected will be redistributed when the subscriber reconnects.

Note – For more information about JMS, see `http://www.oracle.com/goto/glassfish`.

Configuring the JMS Publisher Type

The JMS publisher formats audit events into JMS TextMessages. These TextMessages are then sent to either a queue or a topic, depending on the configuration. Text messages can be formatted as XML or Universal Logging Format (ULF), depending on configuration.

To enable the JMS publisher type, follow the steps in “To Enable Custom Audit Publishers” on page 331 and select JMS from the New Publisher drop-down menu.

To configure the JMS publisher type, complete the Configure New Audit Publisher form. If you have questions about the form, refer to the i-Helps and online Help.

The JMX Publisher Type

The JMX audit log publisher publishes audit events so that a JMX (Java Management Extensions) client can monitor Waveset audit log activity.

What is JMX?

Java Management Extensions (JMX) is a Java technology that allows for managing and/or monitoring applications, system objects, devices, and service oriented networks. The managed/monitored entity is represented by objects called MBeans (for Managed Bean).

Waveset’s JMX Publisher Implementation

Waveset’s JMX audit log publisher monitors the audit log for events. When an event is detected, the JMX publisher wraps the audit event record with an MBean, and also updates a temporary history (which is kept in memory). For each event, a separate small notification is sent to the JMX client. If the event is of interest, the JMX client can query the MBean wrapping the audit event for additional information.

Note – See the `com.waveset.object.AuditEvent` Javadoc for information about audit event records. The Javadoc is available in the REF kit, which is discussed in “Developing Custom Audit Publishers” on page 338.

To retrieve information from the correct MBean, a history sequence number is required. This number is included in the event notification.

Each event notification includes the following information:

- **Type**. A string describing the type of event. The string follows the format `AuditEvent.<ObjectType>.<Action>` where `ObjectType` and `Action` are returned from `com.waveset.AuditEvent`. For example, if an unlock event is sent, the type would be `AuditEvent.LighthouseAccount.Unlock`.
- **SequenceNumber**. The history buffer key used to query information from the MBean.

▼ To Configure the JMX Publisher Type

1. **To enable the JMX publisher type, follow the steps in "To Enable Custom Audit Publishers" on page 331 and select JMX from the New Publisher drop-down menu.**

2. **To configure the JMX publisher type, complete the Configure New Audit Publisher form. If you have questions about the form, refer to the i-Helps and online Help.**

   - **Publisher Name**. Type a unique name for the JMX audit event publisher.
   - **History Limit**. Change the default value as needed to specify the number of event items that the publish should retain in memory. (Default is 100.)

3. **Click Test to verify that the Publisher Name is acceptable.**

4. **Click OK. The Configure New Audit Publisher form closes.**

5. **Important! Click Save.**

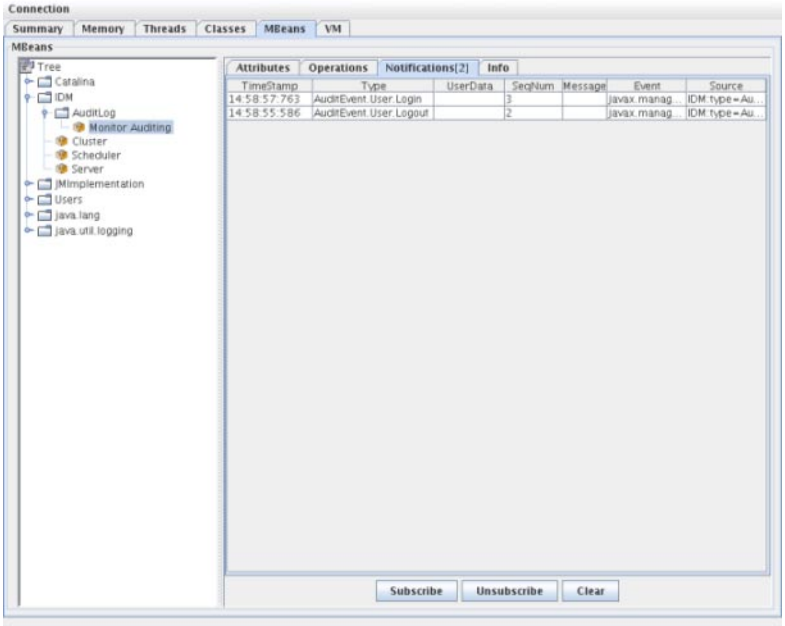
Viewing Audit Events with a JMX Client

Use a JMX client to view the JMX publisher. JConsole, which is included in the JDK 1.5, was used to create the following screen captures.

If using JConsole, choose attach to process to view the `IDM:type=AuditLog` MBean. For information on configuring JConsole for use as a JMX client, see "Viewing JMX Data" in *Oracle Waveset 8.1.1 System Administrator's Guide*.

In JConsole, click the Notifications tab to view audit events. Note the sequence number in the notification. A sequence number is required when querying the MBean for additional information.

FIGURE 10–1 Viewing JMX Audit Event Notifications in JConsole

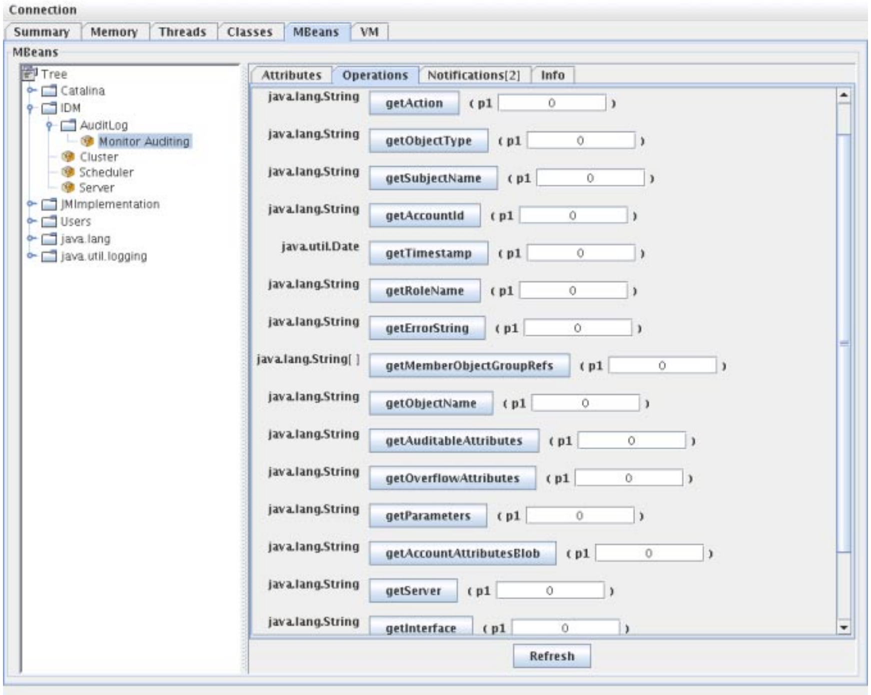


TimeStamp	Type	UserData	SeqNum	Message	Event	Source
14:58:57:763	AuditEvent.User.Login		3		javax.manag...	IDM:type=Au...
14:58:55:586	AuditEvent.User.Logout		2		javax.manag...	IDM:type=Au...

Querying the MBean for Additional Information

In JConsole, click the Operations tab. Use the sequence number in the notification to query the MBean for event details. Each of the operations are prefixed with 'get' and the only parameter is the 'sequence' number.

FIGURE 10–2 Querying the MBean for Additional Information in JConsole



java.lang.String getAction (p1 0)
java.lang.String getObjectType (p1 0)
java.lang.String getSubjectName (p1 0)
java.lang.String getAccountId (p1 0)
java.util.Date getTimestamp (p1 0)
java.lang.String getRoleName (p1 0)
java.lang.String getErrorString (p1 0)
java.lang.String[ ] getMemberObjectGroupRefs (p1 0)
java.lang.String getObjectName (p1 0)
java.lang.String getAuditableAttributes (p1 0)
java.lang.String getOverflowAttributes (p1 0)
java.lang.String getParameters (p1 0)
java.lang.String getAccountAttributesBlob (p1 0)
java.lang.String getServer (p1 0)
java.lang.String getInterface (p1 0)

The MBean is virtually a one-to-one mapping to the `com.waveset.object.AuditEvent` class. Table 10–20 provides a description for each attribute/operation that the MBean provides.

TABLE 10–20 MBeanInfo Attribute/Operation Descriptions

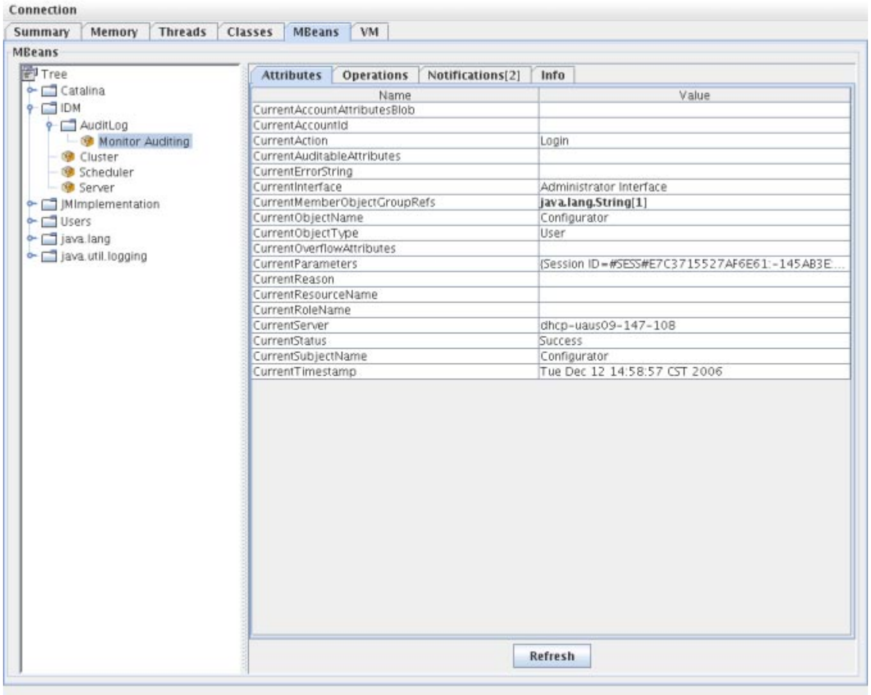
Attribute / Operation	Description
`AccountAttributesBlob`	The list of changed attributes
`AccountId`	AccountId associated with the event
`Action`	Action taken during the event
`AuditableAttributes`	The Auditable attributes
`ErrorString`	Any error string
`Interface`	The Audit interface
`MemberObjectGroupRefs`	The member object group references
`ObjectName`	The object name
`ObjectType`	The object type

TABLE 10–20 MBeanInfo Attribute/Operation Descriptions *(Continued)*

Attribute / Operation	Description
`OverflowAttributes`	All the overflow attributes
`Parameters`	All the parameters
`Reason`	The reason for the event
`ResourceName`	Resource associated with the event
`RoleName`	Role associated with the event
`SubjectName`	User or service associated with the event
`Server`	Name of the server from which the event fired
`Status`	Status of the audit event
`Timestamp`	Date/Time of the audit event

In JConsole, click the Attributes tab. Attributes are prefixed with `Current` to indicate that the attribute contains the most recent audit event sent to the system.

FIGURE 10–3 Viewing MBean Attributes in JConsole



Name	Value
CurrentAccountAttributesBlob	
CurrentAccountId	
CurrentAction	Login
CurrentAuditableAttributes	
CurrentErrorString	
CurrentInterface	Administrator Interface
CurrentMemberObjectGroupRefs	**java.lang.String[1]**
CurrentObjectName	Configurator
CurrentObjectType	User
CurrentOverflowAttributes	
CurrentParameters	{Session ID=#SESS#E7C3715527AF6E61:-145AB3E...
CurrentReason	
CurrentResourceName	
CurrentRoleName	
CurrentServer	dhcp-uaus09-147-108
CurrentStatus	Success
CurrentSubjectName	Configurator
CurrentTimestamp	Tue Dec 12 14:58:57 CST 2006

Developing Custom Audit Publishers

This section documents how to create a new custom audit publisher in Java.

The Console, File, and JDBC custom publishers that are provided with Waveset implement the `AuditLogPublisher` interface. The source code of these publishers can be found in the REF kit. The documentation of the interfaces is also available in the REF kit, in Javadoc format. (Refer to the Javadoc for interface details.)

Note – The REF (Resource Extension Facility) kit is provided in the `/REF` directory on your product CD or with your install image.

Developers are encouraged to extend the `AbstractAuditLogPublisher` class. This class parses the configuration and ensures that all required options have been provided to the publisher. (See the example publishers in the REF kit.)

Publishers must have a `no-arg` constructor.

Publisher Lifecycle

The following steps describe the lifecycle of a publisher:

1. The Object is instantiated.
2. The Formatter (if any) is set using the `setFormatter()` method.
3. Options are provided using the `configure(`*Map*`)` method.
4. Events are published using the `publish(`*Map, LoggingErrorHandler*`)` method.
5. Publisher is terminated using the `shutdown()` method.

Steps 1-3 are executed when Waveset starts up and whenever the audit configuration is updated. Step 4 will not occur if no audit event is generated before shutdown is called.

The `configure(`*Map*`)` is only called once on the same publisher object. (A publisher does not have to prepare for on-the-fly configuration changes). After the audit configuration is updated, the current publishers are first shut down and new publishers are created.

The `configure()` method in Step 3 may throw a `WavesetException`. In this case, the publisher will be ignored and no other calls will be made to the publisher.

Publisher Configuration

Publishers can have zero or more options. The `getConfigurationOptions()` method returns the list of options the publisher supports. The options are encapsulated using the `PublisherOption` class (see Javadoc for details of this class). The audit configuration viewer invokes this method when it builds the configuration interface for the publisher.

Waveset configures the publisher using the `configure(`*Map*`)` method at server startup and after audit configuration changes.

Developing Formatters

The REF kit includes the source code for the following formatters:

- `XmlFormatter`. Formats audit events as XML strings.
- `UlfFormatter`. Formats audit events according to the Universal Logging Format (ULF). The Oracle Application Server uses this format.

Formatters must implement the `AuditRecordFormatter` interface. In addition, formatters must have a `no-arg` constructor. Refer to the Javadoc included in the REF kit for details.

Registering Publishers/Formatters

The audit attribute of `#ID#Configuration:SystemConfiguration` object lists all the registered publishers and formatters. Only these publishers and formatters are available in the audit configuration user interface.

CHAPTER 11

PasswordSync

PasswordSync detects user password changes initiated on Windows domains and forwards those changes to Waveset. Waveset then synchronizes password changes with the other resources defined in Waveset.

This chapter is organized as follows:

What is PasswordSync?

The PasswordSync feature keeps user password changes made on Windows Active Directory domains synchronized with other resources defined in Waveset. PasswordSync must be installed on each domain controller in the domains that will be synchronized with Waveset. PasswordSync must be installed separately from Waveset.

PasswordSync consists of a DLL (`lhpwic.dll`) that resides on each domain controller. This DLL receives password update notifications from Windows, encrypts them, and sends them over HTTPS to the PasswordSync servlet. The PasswordSync servlet is located on the application server running Waveset.

Note – Using HTTPS is preferred, but HTTP is also supported.

The PasswordSync servlet translates the notification into a format Waveset can understand. The servlet then sends the password change (still encrypted) to Waveset using one of the following methods:

- **Direct method**. The servlet communicates the password change directly to Waveset using native Waveset classes. (See "What is PasswordSync?" on page 341.)

  The direct connection method is only recommended for smaller, less complex environments that only require message delivery to one system, and that do not require guaranteed message delivery. (If direct message delivery fails for some reason, the message will be lost. Back up delivery is not possible.)
- **JMS method**. The servlet sends the password information to Waveset using JMS (Java Message Service). With JMS, the servlet submits password changes to the JMS Message Queue. Separately, Waveset's JMS Listener Resource Adapter checks the Queue for new messages. If a password change message is found waiting on the Queue, the JMS Listener Adapter takes the message off the Queue and imports it into Waveset. (See Figure 11–2.)

  The JMS method is recommended for more complex environments that have a high volume requirement, need messages delivered to multiple systems, and require guaranteed message delivery. The JMS Message Queue can be made highly available. As long as a message gets into the queue, if message delivery to Waveset should fail, the queue will keep the change until the message can be delivered to Oracle Waveset.

  You must install and configure JMS separately.

Figure 11–1 diagrams a direct connection. In this configuration the PasswordSync servlet sends update messages directly to Waveset.

FIGURE 11–1 PasswordSync Logical Diagram (Direct Connection)

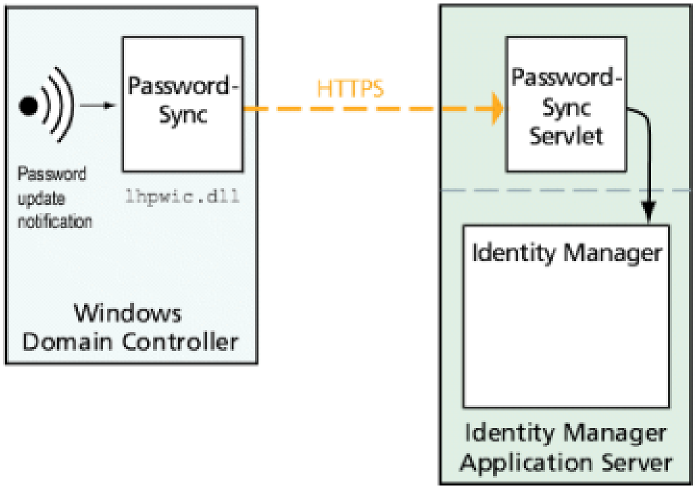
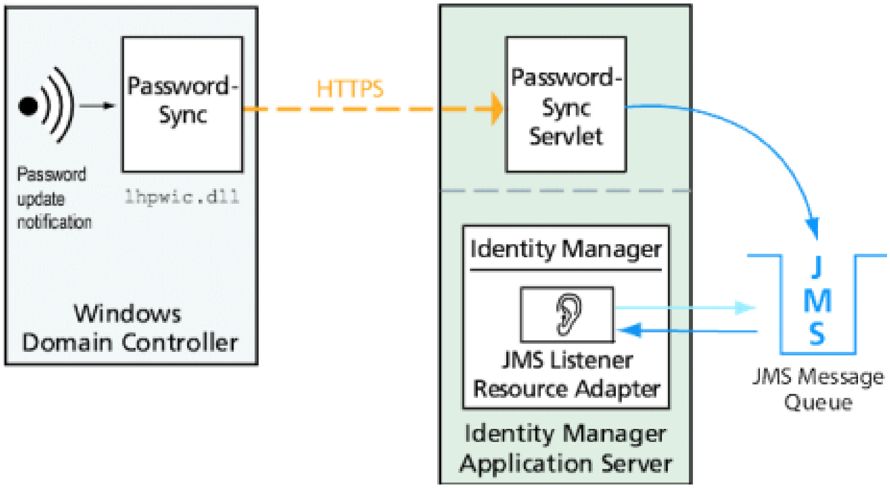

Password update notification
Password-Sync
lhpwic.dll
Windows Domain Controller
HTTPS
Password-Sync Servlet
Identity Manager
Identity Manager Application Server

Figure 11–2 diagrams a JMS connection. In this configuration the PasswordSync servlet sends update messages to the JMS Message Queue. Waveset's JMS Listener Resource Adapter periodically checks the Queue (indicated by the light blue arrow in the diagram) for new messages. The Queue responds by sending the messages to Waveset (indicated by the dark blue arrow).

FIGURE 11–2 PasswordSync Logical Diagram (JMS Connection).

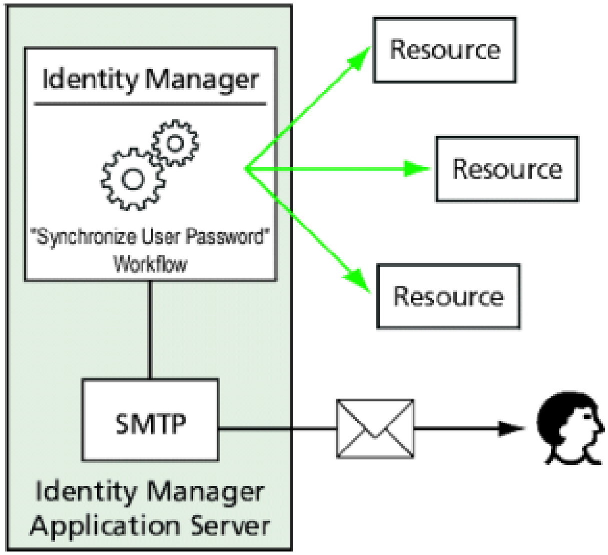

Password update notification
Password-Sync
lhpwic.dll
Windows Domain Controller
HTTPS
Password-Sync Servlet
Identity Manager
JMS Listener Resource Adapter
Identity Manager Application Server
J
M
S
JMS Message Queue

When Waveset receives a password change notification, it decrypts it and processes the change 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 – Windows only sends out an update notification if a password change is successful. If a password change request does not meet the domain's password policy, Windows will reject it and no synchronization data will be sent to Waveset.

Figure 11–3 shows Waveset initiating a workflow and sending email to the user after receiving a password update notification.

FIGURE 11–3 PasswordSync Triggers a Workflow


Identity Manager
"Synchronize User Password" Workflow
Resource
Resource
Resource
SMTP
Identity Manager Application Server

Note – PasswordSync discards all account change notifications for account names that end in a $ (dollar sign). Account names that end in a $ are assumed to be Windows computer accounts. Any user account names that end in a dollar sign will not be forwarded to Waveset.

Before You Install

The PasswordSync feature can be set up only on Windows 2008, Windows 2008 R2, Windows 2003, and Windows 2000 domain controllers. (Support for Windows NT domain controllers was discontinued in version 8.0 of Waveset.) You must install PasswordSync on each primary and backup domain controller in the domains that will be synchronized with Waveset. Configuring PasswordSync for HTTPS is highly recommended.

Note –

- PasswordSync does not support the Windows Server `CORE` install type as a configuration option because Windows Server 2008 and Windows Server 2008 R2 do not support the required .NET runtime for the `CORE` install type.
- Versions of PasswordSync that are older than version 7.1.1 should be updated to at least version 7.1.1 on all domain controllers.

  Support for the rpcrouter2 servlet has been deprecated in version 8.0, and will be removed in a future release. PasswordSync versions 7.1.1 and newer support the new protocol.

If using JMS, PasswordSync requires connectivity with a JMS server. See the JMS Listener resource adapter section in the *Oracle Waveset 8.1.1 Resources Reference*for more information about the requirements for the JMS system.

In addition, PasswordSync requires you to

- Install at least Microsoft .NET 2.0 on each domain controller.
- Remove any previous versions of PasswordSync.

These requirements are discussed in more detail in the following sections.

Install Microsoft .NET 2.0

To use PasswordSync, you must install at least the Microsoft .NET 2.0 Framework. This Framework is installed by default on Windows 2008 domain controllers. If you are using a Windows 2000 or 2003 domain controller, you can download the toolkit from the Microsoft Download Center at:

`http://www.microsoft.com/downloads`

Note –

- Enter `.NET Framework Redistributable` in the Keywords search field to quickly locate the Framework toolkit.
- The toolkit installs the .NET Framework.

Configure PasswordSync for SSL

Although sensitive data is encrypted before being sent to the Waveset server, Oracle recommends configuring PasswordSync to use a secure SSL connection (that is, an HTTPS connection).

For information on how to install imported SSL certificates, see this Microsoft Knowledge Base How-To article:

`http://support.microsoft.com/kb/816794`

Once you have installed PasswordSync, you can test that your SSL connection is properly configured by specifying an HTTPS URL in the PasswordSync Configuration dialog. See "Testing Your Configuration" on page 371 for instructions.

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 and Configuring PasswordSync on Windows

This section contains information and instructions for installing and configuring PasswordSync.

This information is organized as follows:

- "To Install the PasswordSync Configuration Application" on page 347
- "To Configure PasswordSync" on page 348
- "Installing PasswordSync Silently" on page 356

▼ To Install the PasswordSync Configuration Application

The following procedure describes how to install the PasswordSync configuration application.

Note – You must install PasswordSync on each domain controller in the domains that will be synchronized with Waveset.

Be sure to uninstall any previously installed versions of PasswordSync before continuing.

---

1 **From the Waveset installation media,**

- If you are installing to a 32-bit version of Windows, double-click `pwsync\IdmPwSync_x86.msi`.
- If you are installing to a 64-bit version of Windows, double-click `pwsync\IdmPwSync_x64.msi`.

The installation wizard opens and the Welcome window displays with 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 window.**

3 **Click either Typical or Complete to install the full PasswordSync package, or click Custom to control which parts of the package are installed. Click Next to continue.**

4 **When the Ready to Install window displays, click Install to install the product.**

5 **A final window displays. Enable the Launch Configuration Application box so that you can begin configuring Password Sync, and then click Finish to complete the installation process.**

Instructions for configuring PasswordSync are provided in Chapter 11, "PasswordSync."

Note – A dialog displays, 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 you must restart the domain controller before implementing PasswordSync.

"Installing and Configuring PasswordSync on Windows" on page 346 describes the files that are installed on each domain controller.

Installed Component	Description
`%$INSTALL_DIR$%\configure.exe`	PasswordSync configuration program
`%$INSTALL_DIR$%\configure.exe.manifest`	Data file for the configuration program
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	DLL that handles PasswordSync messages
`%SYSTEMROOT%\SYSTEM32\lhpwic.dll`	Password Notification DLL that implements the Windows `PasswordChangeNotify()` function

▼ To Configure 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.

1 **Start the PasswordSync configuration application (if it is not already running).**

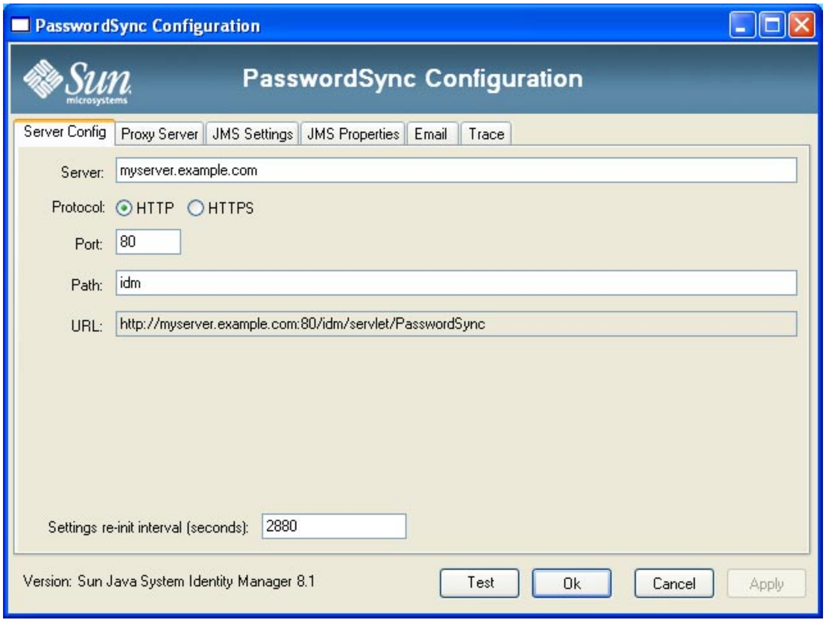
By default, the configuration application is installed at Program Files → Waveset PasswordSync → Configuration.

Note – If you do not plan to use JMS, launch the configuration application from a command line, being sure to include the `-direct` flag as follows:

```
C:\InstallDir\Configure.exe -direct
```

The PasswordSync Configuration wizard dialog is displayed (see Figure 11–4).

FIGURE 11–4 PasswordSync Configuration Wizard



Server: myserver.example.com

Protocol: ● HTTP ○ HTTPS

Port: 80

Path: idm

URL: http://myserver.example.com:80/idm/servlet/PasswordSync

Settings re-init interval (seconds): 2880

Version: Sun Java System Identity Manager 8.1

2 **Edit the fields on this dialog as necessary.**

These fields include:

- **Server** must be replaced with the fully-qualified host name or IP address where Waveset is installed.
- **Protocol** indicate whether to make secure connections to Waveset.

  PasswordSync supports the configuration of certificate check behavior for HTTPS connections. When you enable HTTPS, the following options display:

  - **Allow revoked certificates**. This setting maps to the `securityIgnoreCertRevoke` registry value on the connection. By default, PasswordSync does not ignore revocation issues and the `securityIgnoreCertRevoke` registry value is set to 0.

    If you want PasswordSync to ignore revoked certificate messages, check this box (or set the `SECURITY_FLAG_IGNORE_REVOCATION` registry value to 1).

  - **Allow invalid certificates**. This setting affects the `SECURITY_FLAG_IGNORE_CERT_CN_INVALID`, `SECURITY_FLAG_IGNORE_CERT_DATE_INVALID`, and `SECURITY_FLAG_IGNORE_UNKNOWN_CA` options on the connection. By default, PasswordSync does not allow invalid certificates and the registry values are set to 0.

Checking this box, or setting the `securityAllowInvalidCert` registry value to 1, allows PasswordSync to use certificates that do not pass a number of safety checks. Enabling this option is *not recommended* for a production environment.

Note – These settings are not displayed for the HTTP protocol type, nor do they affect HTTP settings.

- **Port** specify an available port for the server. For HTTP, the default port is 80. For HTTPS, the default port is 443.
- **Path** specify the path to Waveset on the application server.
- **URL** is generated by concatenating the other fields together. The value cannot be edited within the URL field.
- **Settings re-init interval (seconds)** specify how often the PasswordSync `dll` should reread configuration settings from the registry. The default value is 2880 seconds or 8 hours.

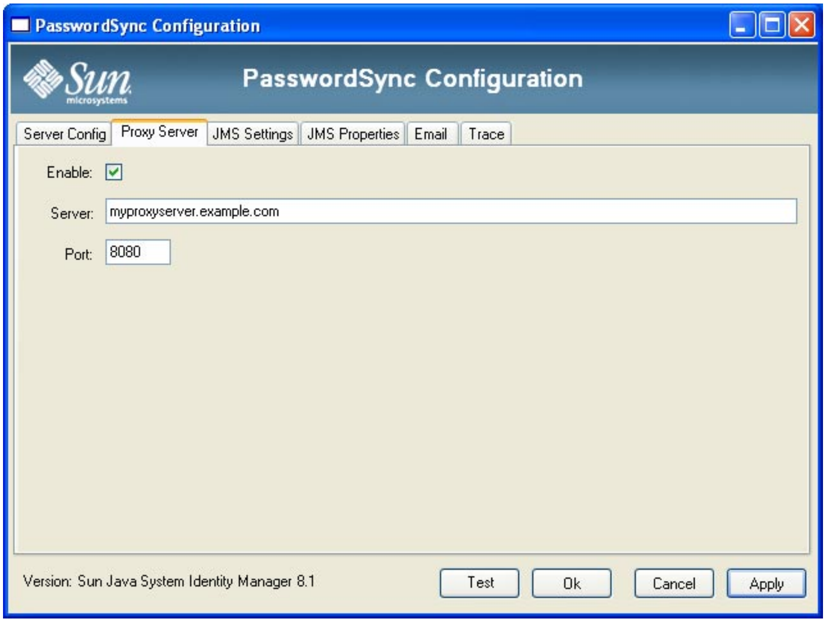
  Note – This PasswordSync Configuration wizard displays the value in seconds, but the registry value is actually stored in milliseconds.

  The PasswordSync `dll` reads the configuration settings from the registry while the `dll` is active. This interval value is stored in the `reinitIntervalMilli` registry value.

  Passwords cannot be synchronized while the settings are being updated, which can cause a small delay in processing a password change. Normally this delay is less than a second. PasswordSync processes any password changes received during an update directly after the update has completed. Also, PasswordSync does not process setting updates while a password synchronization is in progress. The update will be rescheduled and performed at a later time.

3 Click Next to display the Proxy Server Configuration page (Figure 11–5) and edit the fields as needed.

FIGURE 11–5 PasswordSync Wizard Proxy Server Dialog



Enable: ☑

Server: myproxyserver.example.com

Port: 8080

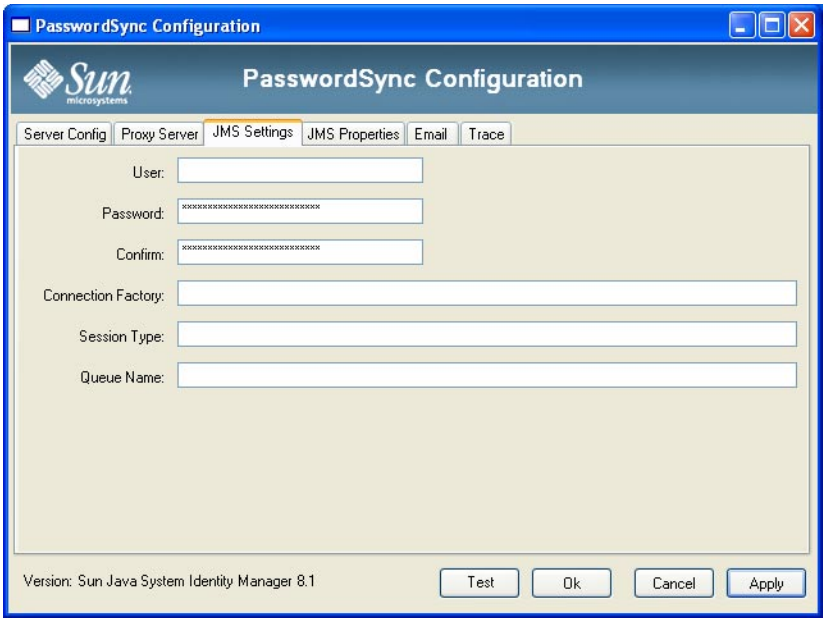
Version: Sun Java System Identity Manager 8.1

These fields include:

- **Enable**. Select if a proxy server is required.
- **Server**. You must enter 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.)

4 **Click Next.**

FIGURE 11–6 PasswordSync Wizard JMS Settings Dialog

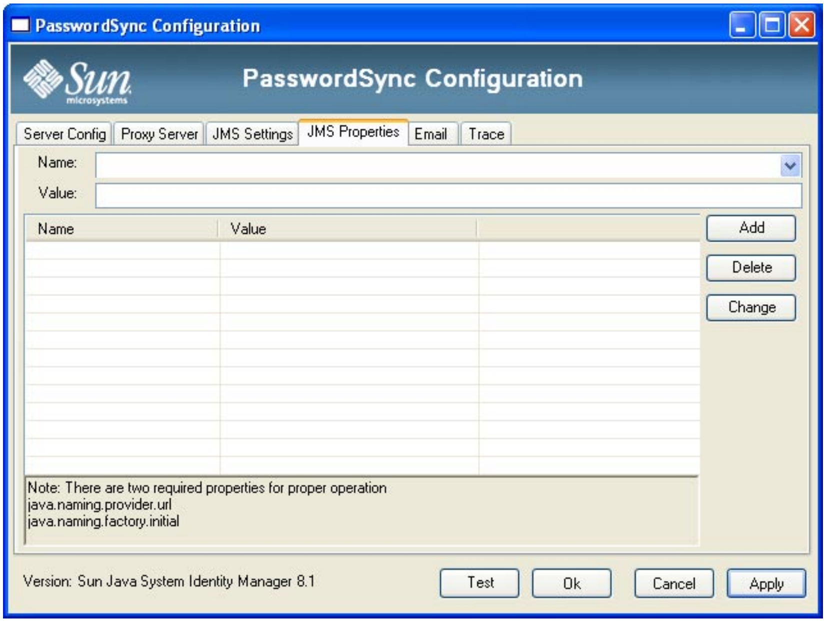


When the JMS Settings dialog (Figure 11–6) appears, perform one of the following actions:

- Edit the following fields, as needed:
  - **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 to 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 Lookup Name for the password synchronization events.
- If you do not plan to use JMS and you launched the configuration wizard with the `-direct` flag, click Next to display the User dialog. Skip to step Figure 11–7.

5 Click Next to display the JMS Properties dialog (Figure 11–7).

FIGURE 11–7 PasswordSync Wizard JMS Properties Dialog



Note: There are two required properties for proper operation
java.naming.provider.url
java.naming.factory.initial

Version: Sun Java System Identity Manager 8.1

The JMS Properties dialog allows you to define the set of properties that are used to build the initial JNDI context. You must define the following name/value pairs:

- `java.naming.provider.url` — Specify the URL of the machine running the JNDI service.
- `java.naming.factory.initial` — Specify 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.

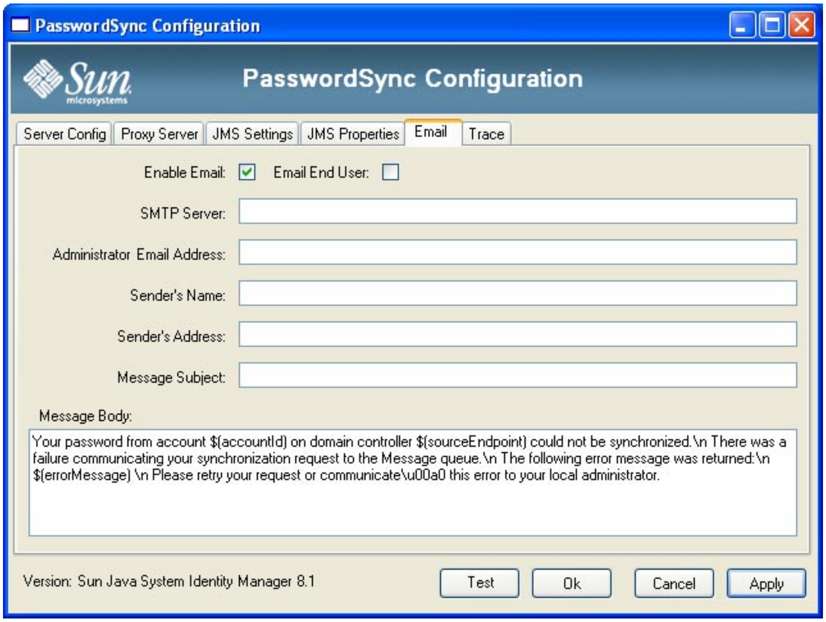
6 **If you do not plan to use JMS and you launched the configuration wizard with the `-direct` flag, configure the User tab. Otherwise, skip this step and go to the next step.**

To configure the User tab, edit the fields as necessary.

- **Account ID**. Specify the user name that will be used to connect to Waveset.
- **Password**. Specify the password that will be used to connect to Waveset.

7 **Click Next to display the Email dialog (Figure 11–8) and edit the fields as necessary.**

FIGURE 11–8 PasswordSync Wizard Email Dialog



Enable Email: ☑ Email End User: □

SMTP Server:

Administrator Email Address:

Sender's Name:

Sender's Address:

Message Subject:

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 message was returned:\n $(errorMessage) \n Please retry your request or communicate\u00a0 this error to your local administrator.

Version: Sun Java System Identity Manager 8.1

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 Waveset, use the following options on the Email dialog to set up the notification and configure the email.

- **Enable Email**. Select to enable this feature.
- **Email End User**. Select if the user is to receive notifications. Otherwise, only the administrator will be notified.
- **SMTP Server**. Enter the fully qualified name or IP address of the SMTP server to be used when sending failure notifications.
- **Administrator Email Address**. Enter the email address where you want to send the notifications.
- **Sender's Name**. Enter the sender's "friendly name."
- **Sender's Address**. Enter the sender's email address.
- **Message Subject**. Enter the subject line for all notifications.
- **Message Body**. Enter the text for the notification.

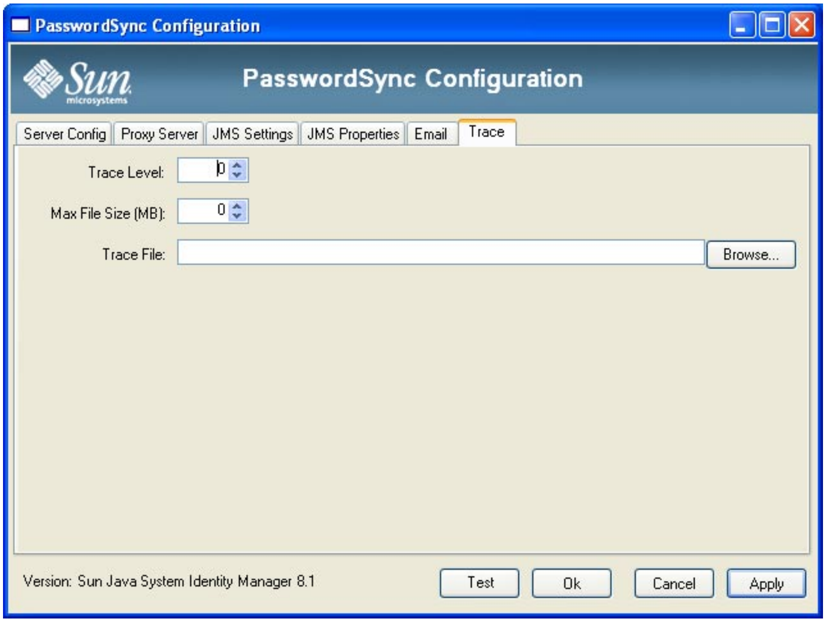
  The message body might contain the following variables:

  - `$(accountId)` — The accountId of the user attempting to change password.
  - `$(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.

8 Click the Trace tab Figure 11–9.

FIGURE 11–9 Trace Tab



Trace Level: 0

Max File Size (MB): 0

Trace File:

Version: Sun Java System Identity Manager 8.1

Set the following fields.

- **Trace Level**.
- **Max File Size (MB)**.
- **Trace File**.

9 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, type the following command from the command line:

C:\InstallDir\\`Configure.exe -wizard`

To test your PasswordSync configuration, see "Testing Your Configuration" on page 371.

Installing PasswordSync Silently

You can configure the PasswordSync installer for silent installation. To use this feature, you must first record configuration parameters to a file while installing PasswordSync. Future installations will reference the file and replay the configuration settings.

Note – To use the silent installation procedure, you must install the complete product on each server that will use PasswordSync. Recording and replaying the configuration settings relies on the configuration application to be installed on the system, which can be accomplished by adding `ADDLOCAL=”Configuration”` to the command. See the example noted at the end of “To Install PasswordSync Silently” on page 357

The silent installation process utilizes a Windows utility called`msiexec` that installs `.msi` files from the command line.

Type `msiexec /?` at a command prompt to view usage information for this utility.

Documentation is also available on Microsoft's website. For example, for documentation on using `msiexec` on Windows Server 2003, see `http://technet.microsoft.com/en-us/library/cc759262(WS.10).aspx`.

To Capture Installation Parameters to a Configuration File

Follow these instructions to install PasswordSync using the installation wizard. The configuration utility captures configuration parameters and writes them to an XML file.

Before You Begin Remove older versions of PasswordSync before installing.

1. **Go to the directory with the PasswordSync installation (`.msi`) file.**

   See “To Install the PasswordSync Configuration Application” on page 347 for information.

2. **Type the following at a command prompt. Arguments and values are case sensitive.**

   `msiexec /i` *pwSyncInstallFile* `CONFIGARGS="-writexml` *fullPathToFile*`"`

   where:

   - **pwSyncInstallFile** is the PasswordSync installation file. (Either `IdmPwSync_86.msi` or `IdmPwSync_x64.msi`).
   - **fullPathToFile** specifies where to write the XML file.

   For example:

   ```
   msiexec /i IdmPwSync_x86.msi CONFIGARGS="-writexml c:\tmp\myconfig.xml"
   ```

3. **Install the product.**

To Install PasswordSync Silently

Before You Begin

- You should have created an installation configuration XML file. See "To Capture Installation Parameters to a Configuration File" on page 356 for instructions.
- Remove older versions of PasswordSync before installing.

1 **Copy your installation configuration XML file to a location where it can be read by the installer.**

2 **Type the following at a command prompt. Arguments and values are case sensitive.**

```
msiexec /i pwSyncInstallFile ADDLOCAL="installFeature" CONFIGARGS="-readxml fullPathToFile"
 INSTALLDIR="installDir" /q
```

where:

- **pwSyncInstallFile** is the PasswordSync installation file. (Either `IdmPwSync_86.msi` or `IdmPwSync_x64.msi`).
- **installFeature** specifies which PasswordSync features to install. Choose one of the following:
  - `MainProgram` — Only install the interceptor `.dll` file
  - `Configuration` — Only install the configuration application
  - `ALL` — Install the complete product

  If nothing is specified, `MainProgram` is used by default if the `/q` option is supplied.
- **fullPathToFile** specifies the path to the configuration XML file.
- **installDir** specifies the full path to a custom installation directory. Optional.
- **/q** specifies a non-GUI install that automatically reboots the server when finished. If not included, the installation wizard will display but the configuration will run with the predefined settings. *Optional.*

Example:

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-readxml c:\tmp\myconfig.xml"

msiexec /i IdmPwSync_x86.msi ADDLOCAL="Configuration"
CONFIGARGS="-readxml c:\tmp\myconfig.xml" /q

msiexec /i IdmPwSync_x64.msi ADDLOCAL="ALL"
CONFIGARGS="-readxml c:\tmp\myconfig.xml"
INSTALLDIR="C:\Program Files\Sun Microsystems\MyCustomInstallDirectory" /q
```

Deploying PasswordSync on the Application Server

Once PasswordSync is installed on your Windows domain controllers, you must take additional steps on the application server running Waveset.

You do not need to install the PasswordSync servlet on the application server. It is automatically installed when you installed Waveset.

To finish deploying PasswordSync, however, you do need to perform the following actions in Waveset:

- Add and configure the JMS Listener Adapter (if using JMS)
- Implement the "Synchronize User Password" Workflow
- Set up notifications

Adding and Configuring a JMS Listener Adapter

If the PasswordSync servlet is using JMS to send messages to Waveset, you need to add Waveset's JMS Listener resource adapter. The JMS Listener resource adapter periodically checks the JMS Message Queue for messages placed there by the PasswordSync servlet. If the Queue contains a new message, it sends it to Waveset for processing.

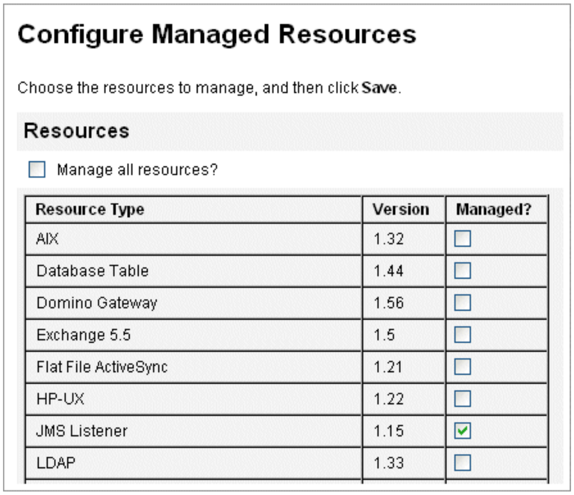
▼ To Add the JMS Listener Resource Adapter

1. **Log on to the Waveset Administrator Interface ("Waveset Administrator Interface" on page 35).**

2. **Select Resources → Configure Types from the main menu.**

   The Configure Managed Resources page opens as shown in Figure 11–10.

FIGURE 11–10 The Configure Managed Resources Page.



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resources

□ Manage all resources?

Resource Type	Version	Managed?
AIX	1.32	□
Database Table	1.44	□
Domino Gateway	1.56	□
Exchange 5.5	1.5	□
Flat File ActiveSync	1.21	□
HP-UX	1.22	□
JMS Listener	1.15	☑
LDAP	1.33	□

3 **Verify that the JMS Listener checkbox in the Managed? column is selected as shown in Figure 11–10.**

If the box is not selected, select it and click Save.

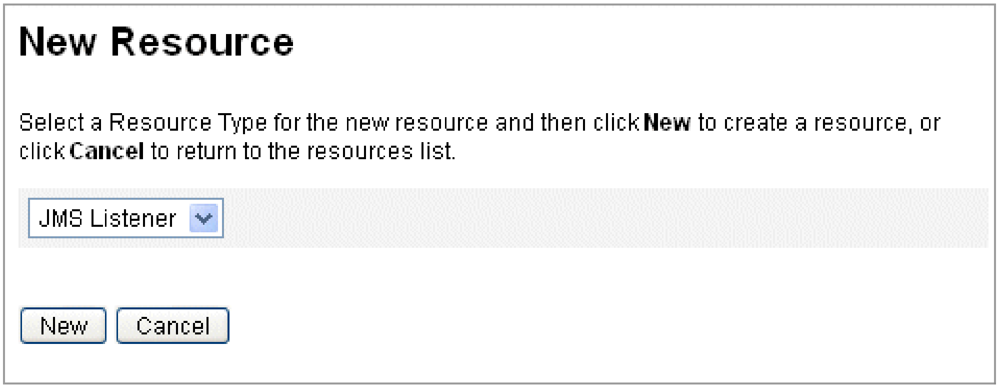
4 **Click List Resources in the secondary menu.**

5 **Locate the Resource Type Actions drop-down menu and select New Resource.**

The New Resource page is displayed.

6 **To add the JMS Listener Adapter, select JMS Listener from the drop-down menu (as shown in Figure 11–11) and click New.**

FIGURE 11–11 The New Resource Wizard



New Resource

Select a Resource Type for the new resource and then click **New** to create a resource, or click **Cancel** to return to the resources list.

JMS Listener

7. **Configure the following settings on the Resource Parameters page, and then click Next.**

- **Destination Type**. Specify the This value is typically set to Queue. (Topics are not usually relevant because there is one subscriber and potentially multiple publishers.)
- **Initial context JNDI properties**. Define the set of properties that are used to build the initial JNDI context.

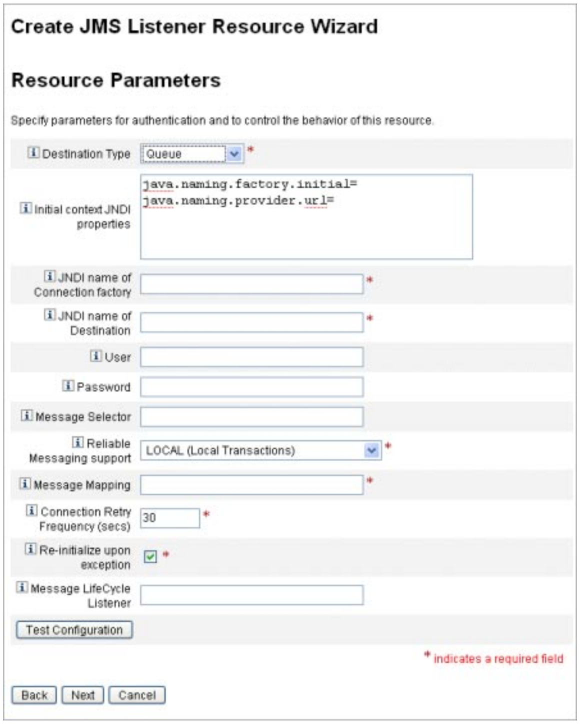
  You must define the following name/value pairs:

  - `java.naming.factory.initial`. Specify the classname (including the package) of the Initial Context Factory for the JNDI Service Provider.
  - `java.naming.provider.url`. Specify the URL of the machine running the JNDI service.

    You might have to define additional properties. The list of properties and values should match those specified on the JMS settings page on the JMS server. For example, to provide the credentials and bind method, you might need to specify the following sample properties:

    - `java.naming.security.principal` — Bind DN (for example, cn=Directory manager)
    - `java.naming.security.authentication` — Bind method (for example, simple)
    - `java.naming.security.credentials` — Password
- **JNDI name of Connection factory**. Enter the name of a connection factory, as defined on the JMS server.
- **JNDI name of Destination**. Enter the name of a destination, as defined on the JMS server.
- **User** and **Password**. Enter 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.



Create JMS Listener Resource Wizard

Resource Parameters

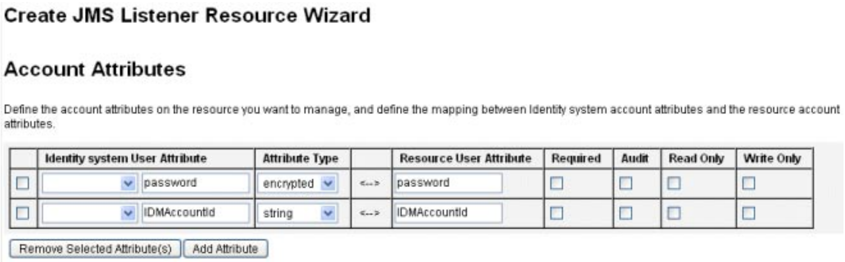
Specify parameters for authentication and to control the behavior of this resource.

Destination Type	Queue *
Initial context JNDI properties	java.naming.factory.initial= java.naming.provider.url=
JNDI name of Connection factory	*
JNDI name of Destination	*
User	
Password	
Message Selector	
Reliable Messaging support	LOCAL (Local Transactions) *
Message Mapping	*
Connection Retry Frequency (secs)	30 *
Re-initialize upon exception	☑ *
Message LifeCycle Listener	

8 **On the Account Attributes wizard page (Figure 11–12), click Add Attribute and map the following attributes, which are made available to the JMS Listener Adapter by `PasswordSyncMessageMapper`.**

- `IDMAccountId` — This attribute is resolved by the `PasswordSyncMessageMapper`, based on the `resourceAccountId` and `resourceAccountGUID` attributes passed in the JMS message.
- `password` — The encrypted password forwarded in the JMS message.

FIGURE 11–12 The Account Attributes Page of the Create JMS Listener Resource Wizard



Create JMS Listener Resource Wizard

Account Attributes

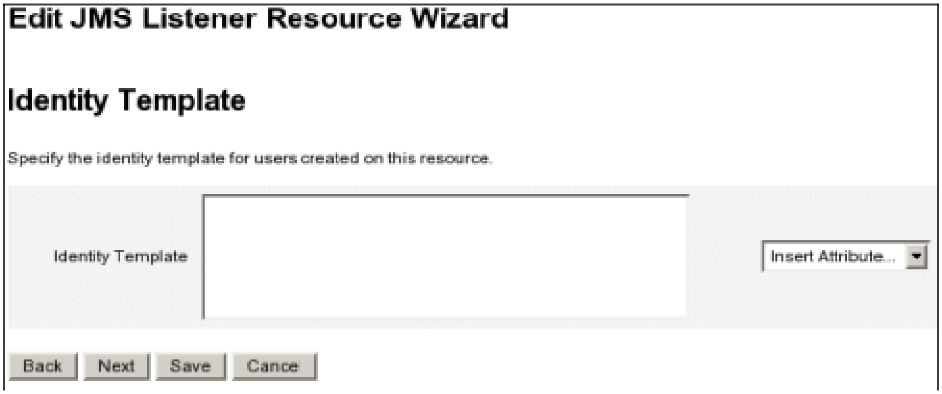
Define the account attributes on the resource you want to manage, and define the mapping between Identity system account attributes and the resource account attributes.

	Identity system User Attribute	Attribute Type		Resource User Attribute	Required	Audit	Read Only	Write Only
□	password	encrypted	<-->	password	□	□	□	□
□	IDMAccountId	string	<-->	IDMAccountId	□	□	□	□

9 **Click Next.**

The Identity Template wizard page opens as shown in Figure 11–13. Note that the attributes you added in the previous step are available in the Attribute Mappings section of the Resource Wizard (Figure 11–13).

FIGURE 11–13 JMS Listener Resource Wizard Attribute Mappings



Edit JMS Listener Resource Wizard

Identity Template

Specify the identity template for users created on this resource.

Identity Template

10 **Click Next and configure the options on Identity System Parameters page as needed.**

See *Oracle Waveset 8.1.1 Resources Reference*for more information about setting up the JMS Listener resource adapter.

Implementing the Synchronize User Password Workflow

When Waveset receives a password change notification, it starts the Synchronize User Password workflow. The default Synchronize User Password workflow checks out the ChangeUserPassword viewer, and then checks it back in again. Next, the workflow processes all of the resources accounts (except the Windows resource that sent the initial password change notification). Finally, Waveset sends the user email indicating 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 when you configure the JMS Listener for synchronization (see "Configuring Active Sync" on page 369).

If you want to modify the workflow, copy the `$WSHOME/sample/wfpwsync.xml` file and make your modifications. Then, import the modified workflow into Waveset.

Some of the modifications you might want to make to the default workflow include:

- Which entities are notified when a password is changed.
- What happens if an Waveset account cannot be found.
- How resources are selected in the workflow.
- Whether to allow password changes from Waveset.

For detailed information about using workflows, see Chapter 1, "Workflow," in *Oracle Waveset 8.1.1 Deployment Reference*.

Setting Up Notifications

Waveset provides two email templates that can inform users whether a password change was successful across all resources.

These templates are:

- Password Synchronization Notice
- Password Synchronization Failure Notice

Both templates should be updated to provide company-specific information about what users should do if they need further assistance. For more information see "Customizing Email Templates" on page 98 in Chapter 4, "Configuring Business Administration Objects."

Configuring PasswordSync with an Oracle JMS Server

Waveset can use Java Message Service (JMS) to receive password change notifications from the PasswordSync servlet. In addition to guaranteed delivery, JMS can deliver messages to multiple systems.

Note – See the *Oracle Waveset 8.1.1 Resources Reference* for more information about this adapter.

Using a sample scenario, this section provides instructions for configuring PasswordSync with an Oracle JMS server.

The information is organized as follows:

- "Sample Scenario" on page 364
- "Creating and Storing Administered Objects" on page 364
- "Configuring the JMS Listener Adapter for this Scenario" on page 369
- "Configuring Active Sync" on page 369

Sample Scenario

A typical (simple) use case for configuring PasswordSync with a JMS server is to enable users to change their passwords on Windows, have Waveset pick up the new password, and then update the user accounts with the new passwords on an Oracle Directory Server.

The following environment was configured for this scenario:

- Windows Server 2003 Enterprise Edition– Active Directory
- Sun Java System Identity Manager 6.0 2005Q4M3
- MySQL running on SUSE Linux 10.0
- Tomcat 5.0.28 running on SUSE Linux 10.0
- Sun Java System Message Queue 3.6 SP3 2005Q4 running on SUSE Linux 10.0
- Sun Java System Directory Server 5.2 SP4 running on SUSE Linux 10.0
- Java 1.5 (Java 5.0)

The following files were copied to the Tomcat `common/lib` directory to enable JMS and JNDI:

- `jms.jar` (from Message Queue)
- `fscontext.jar` (from Message Queue)
- `imq.jar` (from Message Queue)
- `jndi.jar` (from Java JDK)

Creating and Storing Administered Objects

This section provides instructions for creating and storing the following administered objects, which are required for the sample scenario to work successfully:

- Connection factory objects
- Destination objects

You can store administered objects in an LDAP directory or in a file. If you are using a file, all instances of the file must be the same.

For instructions, see

- "Storing Administered Objects in an LDAP Directory" on page 365
- "Storing Administered Objects in a File" on page 367

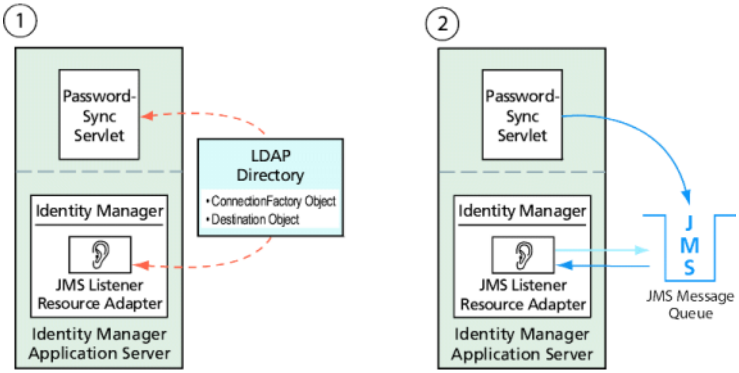
Note –

- The instructions in this section assume you have installed Message Queue. (The necessary tools are located in the `bin/` directory of your Message Queue installation.)
- You can use the Message Queue administrative GUI (`imqadmin`) or the command-line tool (`imqobjmgr`) to create these administered objects. The following instructions use the command-line tool.

Storing Administered Objects in an LDAP Directory

PasswordSync and the JMS Listener can be configured to use administered objects stored in an LDAP directory. Figure 11–14 illustrates the process. Both the PasswordSync Servlet and the JMS Listener adapter must retrieve connection factory and destination settings from the LDAP Directory in order to send and receive messages.

FIGURE 11–14 Retrieving Connection Factory and Destination Objects from the LDAP Directory


1
Password-Sync Servlet
LDAP Directory
•ConnectionFactory Object
•Destination Object
Identity Manager
JMS Listener Resource Adapter
Identity Manager Application Server
2
Password-Sync Servlet
Identity Manager
JMS Listener Resource Adapter
Identity Manager Application Server
J
M
S
JMS Message Queue

Using the Message Queue Command-Line Tool

This section explains how to use the Message Queue command-line tool (`imqobjmgr`) to store administered objects in an LDAP directory.

Storing Connection Factory Objects

Open the Message Queue command-line tool (`imqobjmgr`) and type the commands in "Storing Connection Factory Objects" on page 366 to store the connection factory objects.

EXAMPLE 11–1 Storing Connection Factory Objects

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf -o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements] ...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name: cn=mytestFactory The object’s read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url
ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication
simple java.naming.security.credentials netscape
java.naming.security.principal
cn=directory manager Object successfully added.
```

In "Storing Connection Factory Objects" on page 366 `imqAddressList` defines the JMS server/broker hostname (`gwenig.coopsrc.com`), port (`7676`), and the access method (`jms`).

Storing Destination Objects

In the Message Queue command-line tool (`imqobjmgr`), type the commands in "Storing Destination Objects" on page 366 to store the destination objects.

EXAMPLE 11–2 Storing Destination Objects

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q -o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description]
A Description for the Destination Object imqDestinationName [Destination Name]
mytestDestination Using the following lookup name: cn=mytestDestination
The object’s read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
```

EXAMPLE 11–2 Storing Destination Objects *(Continued)*

```
java.naming.security.principal cn=directory manager Object successfully added.
```

You can check the newly created object with an `ldapsearch` or an LDAP browser.

This concludes the section on Storing Administered Objects on an LDAP Server. Skip the next section, which describes how to store Administered Objects in a file, and go to the section on "Configuring the JMS Listener Adapter for this Scenario" on page 369.

Storing Administered Objects in a File

PasswordSync and the JMS Listener can be configured to use administered objects stored in a file. If you are not storing administered objects on an LDAP server ("Storing Administered Objects in an LDAP Directory" on page 365), follow the instructions in this section.

Storing Connection Factory Objects

Open the Message Queue command-line tool (`imqobjmgr`) and type the commands in "Storing Connection Factory Objects" on page 367 to store connection factory objects and specify a lookup name.

EXAMPLE 11–3 Storing Connection Factory Objects and Specifying Lookup Names

```
#> ./imqobjmgr add -l "mytestFactory" -j
"java.naming.factory.initial= com.sun.jndi.fscontext.RefFSContextFactory"
 -j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
 "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
"imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
```

EXAMPLE 11–3 Storing Connection Factory Objects and Specifying Lookup Names *(Continued)*

```
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

Creating the Destination on the Broker

By default, the Message Queue broker allows auto-creation of the queue destination (see `config.properties`, where the default value for `imq.autocreate.queue` is `true`).

If the queue destination is not created automatically, you must create the destination object on the broker using the command shown in "Creating the Destination on the Broker" on page 368 (where *myTestQueue* is the destination).

EXAMPLE 11–4 Creating a Destination Object on the Broker

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue On the broker specified by:
-------------------------
Host Primary Port
------------------------- localhost 7676
Successfully created the destination.
```

You can store administered objects in a directory or in a file:

- **In a directory:** Using a directory is a centralized way of storing the Connection Factory and the Destination objects.

  When you use a directory, these administered objects are stored as directory entries.

  Note – If the Waveset PasswordSync servlet and the Waveset server are not on the same machine, then each of them must be able to access the `.bindings` file. You can repeat the administered object creation twice (on each machine) or you can copy the `.bindings` file to the proper location on each machine.

- **In a file:** If the Waveset PasswordSync servlet and Waveset server are both running on the same server (or if you do not have a directory available), you can store the administrative objects in a file.

  When you use a file, both administered objects are stored in a single file (called `.bindings` on both Windows and UNIX), under the directory you specified for the java.naming.provider.url (for example, `file:///c:/temp` on Windows or `file:///tmp` on UNIX).

Configuring the JMS Listener Adapter for this Scenario

Configure the JMS listener adapter on the application server. Follow the instructions in the section "Adding and Configuring a JMS Listener Adapter" on page 358.

Configuring Active Sync

Next, configure the JMS Listener for synchronization. Active Sync is required if you are using JMS, but it is not used for direct connections.

▼ To Configure the JMS Listener for Synchronization

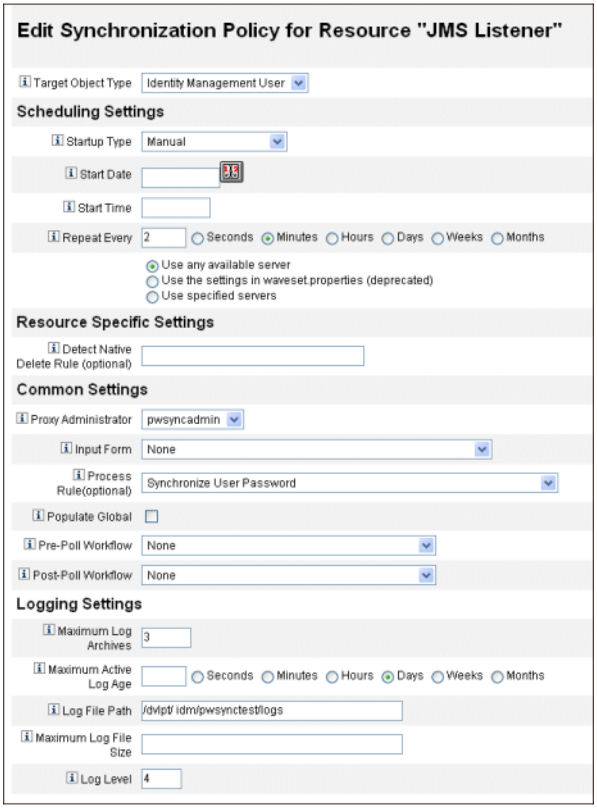
1. **In the Administrator interface, click Resources in the menu.**

2. **In the Resource List, select the JMS Listener checkbox.**

3. **In the Resource Actions list, select Edit Synchronization Policy.**

   The Edit Synchronization page for the JMS Listener resource opens (Figure 11–15).

FIGURE 11–15 Configuring Active Sync for the JMS Listener



Edit Synchronization Policy for Resource "JMS Listener"

Target Object Type	Identity Management User

Scheduling Settings

Startup Type	Manual
Start Date	
Start Time	
Repeat Every	2 ○ Seconds ● Minutes ○ Hours ○ Days ○ Weeks ○ Months
	● Use any available server ○ Use the settings in waveset.properties (deprecated) ○ Use specified servers

Resource Specific Settings

Detect Native Delete Rule (optional)	

Common Settings

Proxy Administrator	pwsyncadmin
Input Form	None
Process Rule(optional)	Synchronize User Password
Populate Global	□
Pre-Poll Workflow	None
Post-Poll Workflow	None

Logging Settings

Maximum Log Archives	3
Maximum Active Log Age	○ Seconds ○ Minutes ○ Hours ● Days ○ Weeks ○ Months
Log File Path	/dvlpt/ idm/pwsynctest/logs
Maximum Log File Size	
Log Level	4

4 **Under Common Settings, locate Proxy Administrator and select `pwsyncadmin`. (This administrator is associated with an empty form.)**

5 **Under Common Settings, locate Process Rule and select Synchronize User Password from the list. The default Synchronize User Password workflow takes each request that comes in from the JMS Listener adapter, checks out the ChangeUserPassword viewer, and then checks the ChangeUserPassword viewer back in.**

6 **In the Log File Path box, specify a path to a directory where the active and archived log files should be created.**

7 **For debugging purposes, set the Log Level to 4 to generate a verbose log.**

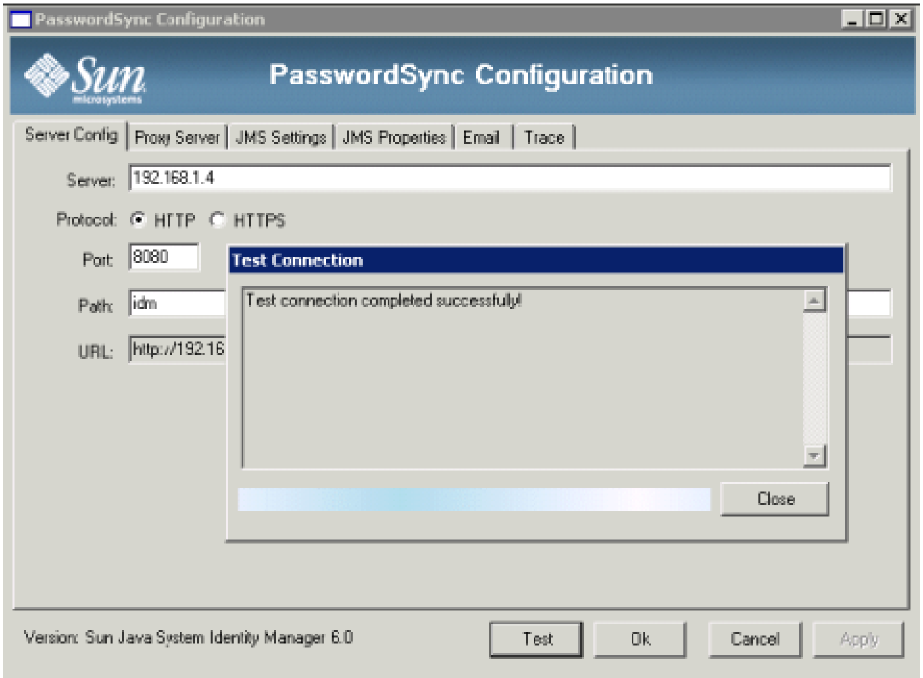
8 **Click Save.**

Testing Your Configuration

You can use the Windows PasswordSync Configuration application to debug the Windows side of your configuration.

1. **Start the PasswordSync configuration application, if it is not already running.**

   By default, the configuration application is installed at Program Files → Waveset PasswordSync → Configuration.
2. **When the PasswordSync Configuration dialog displays, click the Test button.**
3. **If using JMS, the Test Connection dialog displays, with a message stating whether the test connection completed successfully.**



Server: 192.168.1.4

Protocol: ● HTTP ○ HTTPS

Port: 8080

Path: idm

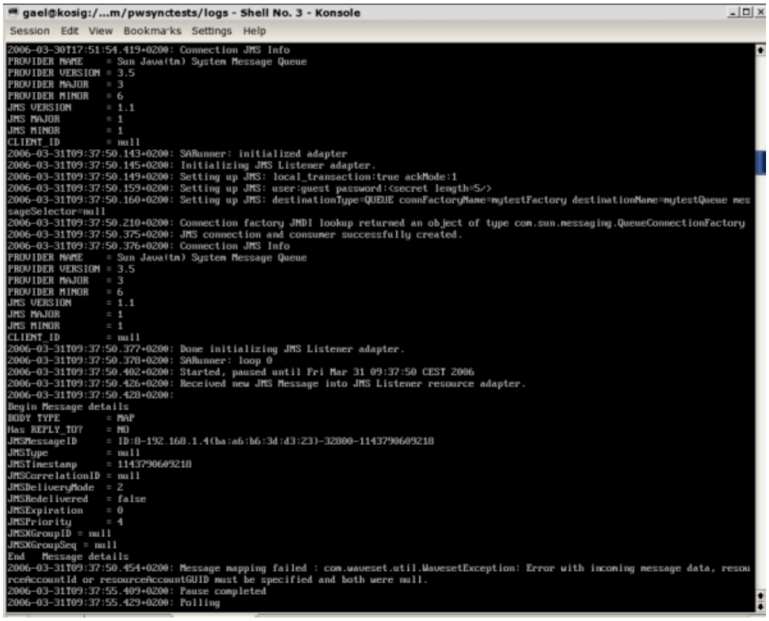
URL: http://192.16

Test connection completed successfully!

Version: Sun Java System Identity Manager 6.0

4. Click Close to close the Test Connection dialog.
5. Click OK to close the PasswordSync Configuration dialog.

   The JMS Listener adapter then runs in debug mode, and generates debug information in a file, similar to the one in the following figure.



```
2006-03-30T17:51:54.419+0200: Connection JMS Info
PROVIDER NAME     = Sun Java(tm) System Message Queue
PROVIDER VERSION = 3.5
PROVIDER MAJOR   = 3
PROVIDER MINOR   = 6
JMS VERSION      = 1.1
JMS MAJOR        = 1
JMS MINOR        = 1
CLIENT_ID        = null
2006-03-31T09:37:50.143+0200: SARunner: initialized adapter
2006-03-31T09:37:50.145+0200: Initializing JMS Listener adapter.
2006-03-31T09:37:50.149+0200: Setting up JMS: local_transaction:true ackMode:1
2006-03-31T09:37:50.159+0200: Setting up JMS: user:guest password:<secret length=5/>
2006-03-31T09:37:50.160+0200: Setting up JMS: destinationType=QUEUE connFactoryName=mytestFactory destinationName=mytestQueue mes
sageSelector=null
2006-03-31T09:37:50.210+0200: Connection factory JNDI lookup returned an object of type com.sun.messaging.QueueConnectionFactory
2006-03-31T09:37:50.375+0200: JMS connection and consumer successfully created.
2006-03-31T09:37:50.376+0200: Connection JMS Info
PROVIDER NAME     = Sun Java(tm) System Message Queue
PROVIDER VERSION = 3.5
PROVIDER MAJOR   = 3
PROVIDER MINOR   = 6
JMS VERSION      = 1.1
JMS MAJOR        = 1
JMS MINOR        = 1
CLIENT_ID        = null
2006-03-31T09:37:50.377+0200: Done initializing JMS Listener adapter.
2006-03-31T09:37:50.378+0200: SARunner: loop 0
2006-03-31T09:37:50.402+0200: Started, paused until Fri Mar 31 09:37:50 CEST 2006
2006-03-31T09:37:50.426+0200: Received new JMS Message into JMS Listener resource adapter.
2006-03-31T09:37:50.428+0200:
Begin Message details
BODY TYPE        = MAP
Has REPLY_TO?    = NO
JMSMessageID     = ID:8-192.168.1.4(ba:a6:b6:3d:d3:23)-32800-1143790609218
JMSType          = null
JMSTimestamp     = 1143790609218
JMSCorrelationID = null
JMSDeliveryMode  = 2
JMSRedelivered   = false
JMSExpiration    = 0
JMSPriority      = 4
JMSXGroupID = null
JMSXGroupSeq = null
End   Message details
2006-03-31T09:37:50.454+0200: Message mapping failed : com.waveset.util.WavesetException: Error with incoming message data, resou
rceAccountId or resourceAccountGUID must be specified and both were null.
2006-03-31T09:37:55.409+0200: Pause completed
2006-03-31T09:37:55.429+0200: Polling
```

Debugging PasswordSync on Windows

PasswordSync writes all failures to the Windows Event Viewer. (For help using Event Viewer, see Windows Help.) The source name for error log entries is *PasswordSync*.

See the *Oracle Waveset 8.1.1 System Administrator's Guide* for information on troubleshooting PasswordSync on Windows.

Uninstalling PasswordSync on Windows

To uninstall the PasswordSync application, go to the Windows Control Panel and select Add or Remove Programs. Then select Waveset PasswordSync and click Remove.

Note – PasswordSync can also be uninstalled (or reinstalled) by loading the Waveset installation media and clicking on the `pwsync\IdmPwSync.msi` icon.

You must restart your system to complete the process.

Frequently Asked Questions about PasswordSync

This section answers some frequently asked questions about PasswordSync.

Question: Can PasswordSync be implemented without a Java Messaging Service?

Answer: Yes, but doing so eliminates the advantages of using a JMS to track password change events.

To implement PasswordSync without a JMS, launch the configuration application with the following flag:

```
Configure.exe -direct
```

When the `-direct` flag is specified, the configuration application displays the User tab.

If you implement PasswordSync without a JMS, you do not need to create a JMS Listener adapter. Therefore, you should omit the procedures listed in "Deploying PasswordSync on the Application Server" on page 358. If you want to set up notifications, you may need to alter the Change User Password workflow.

Note – If you subsequently run the configuration application without specifying the `-direct` flag, PasswordSync will require a JMS to be configured. Relaunch the application with the `-direct` flag to bypass the JMS again.

Question: Can PasswordSync be used in conjunction with other Windows password filters that are used to enforce custom password policies?

Answer: 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 Waveset 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 Waveset password policies. When policies are checked on the Waveset 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 Waveset.

Note – The password intercept DLL does not enforce any password policies.

Question: Can the PasswordSync servlet be installed on a different application server than Waveset?

Answer: Yes. The PasswordSync servlet requires the `spml.jar` and `idmcommon.jar` `jar` files, in addition to any `jar` files required by the JMS application.

Question: Does the PasswordSync service send passwords over to the `lh` server in clear text?

Answer: Although best practice is to run PasswordSync over SSL, all sensitive data is encrypted before being sent to the Waveset server.

For information, see "Configure PasswordSync for SSL" on page 346.

Question: Why do some password changes result in `com.waveset.exception.ItemNotLocked`?

Answer: 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 Waveset.

If you configure the `passwordSyncThreshold` workflow variable correctly, Waveset 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.

CHAPTER 12

Security

This chapter provides information about Waveset security features, and details steps you can take to further reduce security risks.

Review the following topics to learn more about managing system security with Waveset.

Security Features

Waveset helps reduce security risks by providing the following features:

- **Instant disabling of account access**. Waveset lets you disable organizations or individual access rights with a single action.
- **Login session limitations**. You can set limitations on concurrent login sessions.
- **Active risk analysis**. Waveset 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 Chapter 8, "Reporting," for more information about reporting features.)

- **Granular Administrative-privilege controls**. You can grant and manage administrative control in Waveset by assigning a single Capability to a user or a range of administrative duties defined through Admin Roles.
- **Server key encryption**. Waveset 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.

Limiting Concurrent Login Sessions

By default, an Waveset user can have concurrent login sessions. You can limit concurrent sessions, however, to one per login application by opening the system configuration object for modification ("Editing Waveset Configuration Objects" on page 108) and editing the value of the `security.authn.singleLoginSessionPerApp` configuration attribute. This attribute is an object that contains one attribute for each login application name (for example, the Administrator Interface, User Interface, or Identity Manager IDE). Changing the value of this attribute to `true` enforces a single login session for each user.

If enforced, then a user can log in to more than one session; however, only the last logged-in session remains active and valid. If the user performs an action on an invalid session, then he is automatically forced off the session and the session terminates.

Managing Passwords

Waveset 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
- **Password policies**

  Use rules to define password parameters

Pass-Through Authentication

Use pass-through authentication to grant user and administrator access through one or more different passwords.

Waveset manages authentication through the implementation of:

- *Login applications* (a collection of login module groups)
- *Login module groups* (an ordered set of login modules)
- *Login modules* (set 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 Waveset. 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 Waveset 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 login module groups. 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, Waveset 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 HTTP 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.

EXAMPLE 12–1 Location-Based Login Constraint Rule

```
<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 Security → Login to access the Login page.

The login application list shows:

- Each Waveset login application (interface) defined
- The login module groups that comprise the login application
- The Waveset 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 Waveset Session Limits

From the Modify Login Application page, you can set a timeout value (limits) for each Waveset login session. Select hours, minutes, and seconds, and then click Save. The limits you establish display in the login application list.

You can set session timeouts for each Waveset login application. When a user logs in to an Waveset application, then the currently configured session timeout value is used to compute the future date and time when the user's session will time out due to inactivity. This computed date is then stored with the user's Waveset session so that it is available to be checked each time a request is made.

If a login administrator changes a login application session timeout value, then that value will be in effect for all future logins. Existing sessions will time out based on the value in effect when the user logged in.

Values set for HTTP timeout affect all Waveset applications and take precedence over the login application session timeout value.

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, the user is redirected to an alternate page that states 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 deselect the option. As a safeguard, you cannot disable administrator login.

Editing Login Module Groups

The login module group list shows:

- Each login module group
- The individual login modules that make up a login module group
- Whether a login module group contains constraint rules

From the Login Module Groups page you can create, edit, and delete login module groups. Select a login module group 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 Waveset by using an LDAP cn or email address (when Waveset is configured for pass-through to LDAP).

  For example, if you specify the following and the user attempts to log in as `gwilson`, then the LDAP resource will first attempt to find an LDAP user where `cn=gwilson`.

  `cn`

  `mail`

  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 to map the login information provided by the user to an Waveset user. This rule is used to search for an Waveset user by using the logic specified in the rule. The rule must return a list of one or more `AttributeConditions` that will be used to search for an Waveset user that matches. The rule you select must have the `LoginCorrelationRule` authType. For a description of the steps Waveset takes to map an authenticated user ID to an Waveset user, see Example 12–2.
- **New user name rule**. Select a new user name rule to be used when automatically creating new Waveset users as part of login.

Click Save to save a login module. Once it is saved, you can position the module relative to all other modules in the login module group.

Caution – If Waveset 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 Waveset 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 Waveset 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 are eventually locked, even though the user's login through Waveset continues to succeed.

Example 12–2 contains pseudocode that describes the steps Waveset takes to map authenticated user IDs to Waveset users.

EXAMPLE 12–2 Login Module Processing Logic

```
if an existing IDM user’s ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user’s ID

   try to find an IDM user that has a linked resource whose resource
   name matches the resource accountID returned by successful authentication

     if found, then we have found the right IDM user

     otherwise if there is a LoginCorrelationRule associated with the
     configured login module

         evaluate it to see if it maps the login credentials to a single
         IDM user

         otherwise login fails

     otherwise login fails
```

In Example 12–2, the system will try to find a matching Waveset user using the user’s linked resources (resource information). If the resource information approach fails, however, and a loginCorrelationRule is configured, the system will try to find a matching user using the loginCorrelationRule.

Configuring Authentication for Common Resources

If you have multiple resources that are logically the same (for example, multiple Active Directory domain servers that share a trust relationship), or if you have multiple resources that all reside on the same physical host, then you can specify that these resources are *common resources*.

You should declare common resources so that Waveset knows that it should only try and authenticate to a group of resources one time. Otherwise, if a user types a wrong password, Waveset will try the same password against each resource. This can lead to the user's account being locked out due to multiple login failures, even though the user only typed the wrong password one time.

With common resources, a user can authenticate to one common resource, and Waveset will automatically try and map the user to the remaining resources in the common resources group. For example, an Waveset user account may be linked to a resource account for resource AD-1. The login module group, however, 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, Waveset can also map the user to AD-1 by finding the same user accountId on resource AD-1.

Caution – All resources listed in a common resources group must also be included in the Login Module definition. If a complete list of common resources does not also appear in the Login Module definition, then the common resources functionality will not work correctly.

Common resources can be defined in the System Configuration object ("Editing Waveset Configuration Objects" on page 108) using the following format.

EXAMPLE 12–3 Configuring Authentication for Common Resources

```
<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 Waveset.

Configuration Prerequisites

To support X509 certificate-based authentication in Waveset, 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 enabled for client authentication.

▼ To Verify that the Client Certificate's Client Authentication Option is Selected

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 Waveset

▼ To Configure 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 Waveset X509 Certificate Login Module from the Assign Login Module list. Waveset displays the Modify Login Module page.**
6. **Set the login success requirement.**

   The following values are acceptable:

   - **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 Waveset 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 `Waveset user account.` A sample new user name rule is included in `idm/sample/rules,` named `NewUserNameRules.xml.`

Creating and Importing a Login Correlation Rule

A Login Correlation Rule is used by the Waveset X509 Certificate Login Module to determine how to map the certificate data to the appropriate Waveset user. Waveset includes a built-in correlation rule, named Correlate via X509 Certificate subjectDN.

You can also add your own correlation rules. Refer to `LoginCorrelationRules.xml`, which is located in the `idm/sample/rules` directory, as an example.

Each correlation rule must follow these guidelines:

- Its `authType` attribute must be set to `LoginCorrelationRule`
- It is expected to return an instance of a list of `AttributeConditions` to be used by the login module to find the associated Waveset user. For example, the login correlation rule might return an `AttributeCondition` that searches for the associated Waveset user by email address.

Arguments passed to login correlation rules are:

- Standard X509 certificate fields (such as subjectDN, issuerDN, and valid dates)
- Critical and noncritical 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 correlation rule, using the passed-in arguments, returns a list of one or more AttributeConditions. These are used by the Waveset X509 Certificate Login Module to find the associated Waveset 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 Waveset. 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 using 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

Report any problems authenticating using X509 certificates as error messages on the login form.

For more complete diagnostics, enable trace on the Waveset 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 a Client Certificate Attribute Name in an HTTP Request

1. **Enable trace for `SessionFactory` to see the complete list of HTTP attributes and determine the name of the X509 Certificate.**

2. **Use the Waveset debug facility ("The Waveset Debug Page" on page 42) to edit the `LoginConfig` object.**

3. **Change the name of the `<AuthnProperty>` in the `<LoginConfigEntry>` for the Waveset X509 Certificate Login Module to the correct name.**

4. **Save, and then retry.**

   You may also need to remove, and then re-add the Waveset 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 Waveset Server and Gateway.

The following sections provide more information about how cryptography is used and managed in the Waveset 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 Waveset product, including the ciphers used to protect each type of data.

TABLE 12–1 Cryptographically-Protected Data Types

Data Type	RSAMD5	NIST Triple DES168-Bit Key (DESede/ECB/NoPadding)	PKCS#5 Password-Based Crypto56-Bit Key (PBEwithMD5andDES)
Server encryption keys		default	configuration option
Gateway encryption keys		default	configuration option1
Policy dictionary words	yes		
User passwords		yes	
User password history		yes	
User answers		yes	

TABLE 12–1 Cryptographically-Protected Data Types *(Continued)*

Data Type	RSAMD5	NIST Triple DES168-Bit Key (DESede/ECB/NoPadding)	PKCS#5 Password-Based Crypto56-Bit Key (PBEwithMD5andDES)
Resource passwords		yes	
Resource password history	yes		
All payload between server and gateways		yes	

Frequently Asked Questions about Server Encryption Keys

Read the following sections for answers to frequently asked questions about server encryption key source, location, maintenance, and use.

Question: Where do server encryption keys come from?

Answer: 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.

Question: Where are server encryption keys maintained?

Answer: Server encryption keys are objects maintained in the repository. There can be many data encryption keys in any given repository.

Question: How does the server know which key to use for decryption and re-encryption of encrypted data?

Answer: 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, Waveset 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.

Question: How do I update server encryption keys?

Answer: Waveset 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" on page 391 in this chapter for more information about how to use this task.

Question: What happens to existing encrypted data if the "current" server key is changed?

Answer: 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.

To avoid 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.

Question: What happens when you import encrypted data for which an encryption key is not available?

Answer: If you import an object that contains encrypted data, but that data was encrypted with a key that is not in the repository into which it is being imported, then the data will be imported, but not decrypted.

Question: How are server keys protected?

Answer: If the server is not configured to use password-based encryption (PBE) - PKCS#5 encryption (set in the System Configuration object using 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 Waveset 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. Waveset 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 Oracle and IBM.

Question: Can I export the server keys for safe external storage?

Answer: 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 preprocessing 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.

Question: What data is encrypted between the server and gateway?

Answer: 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.

Frequently Asked Questions about Gateway Keys

Read the following sections for answers to frequently asked questions about gateway source, storage, distribution, and protection.

Question: Where do the gateway keys come from to encrypt or decrypt data?

Answer: Each time an Waveset 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.

Question: How are gateway keys distributed to the gateways?

Answer: 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 encrypts test data with the gateway key and sends it to the gateway. The gateway then attempts 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 then generates the server-gateway unique session key, encrypts it with the gateway key and sends it to the gateway. Upon receipt, the gateway decrypts the session key and retains it for use during the life of the server-to-gateway session. If the server cannot successfully decrypt the test data and gateway unique data, the server encrypts the gateway key using the default key and sends it to the gateway. The gateway decrypts the gateway key using its compiled in default key and stores the gateway key in its registry. The server then encrypts the server-gateway unique session key with the gateway key and sends it to the gateway for use during 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 a key exists, the gateway will use that key. If there is no key, the gateway uses the default key. Once the gateway has a key set in the registry, the gateway no longer allows sessions to be established using the default key, which prevents someone from setting up a rogue server and establishing a connection to a gateway.

Question: Can I update the gateway keys used to encrypt or decrypt the server-to-gateway payload?

Answer: Waveset 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 ("Editing Waveset Configuration Objects" on page 108).

Question: Where are the gateway keys stored on the server, on the gateway?

Answer: 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.

Question: How are gateway keys protected?

Answer: 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 "Frequently Asked Questions about Server Encryption Keys" on page 387 for more information.

Question: Can I export the gateway key for safe external storage?

Answer: The gateway key can be exported using the Manage Server Encryption task, just as with server keys. See "Frequently Asked Questions about Server Encryption Keys" on page 387 for more information.

Question: How are server and gateway keys destroyed?

Answer: 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 Waveset server encryption feature allows you to create new 3DES server encryption keys and encrypt these keys by using 3DES, PKCS#5, or AES (Advanced Encryption Standard) encryption. Only users with Security Administrator capabilities can run the Manage Server Encryption task, which is configured from the Manage Server Encryption page.

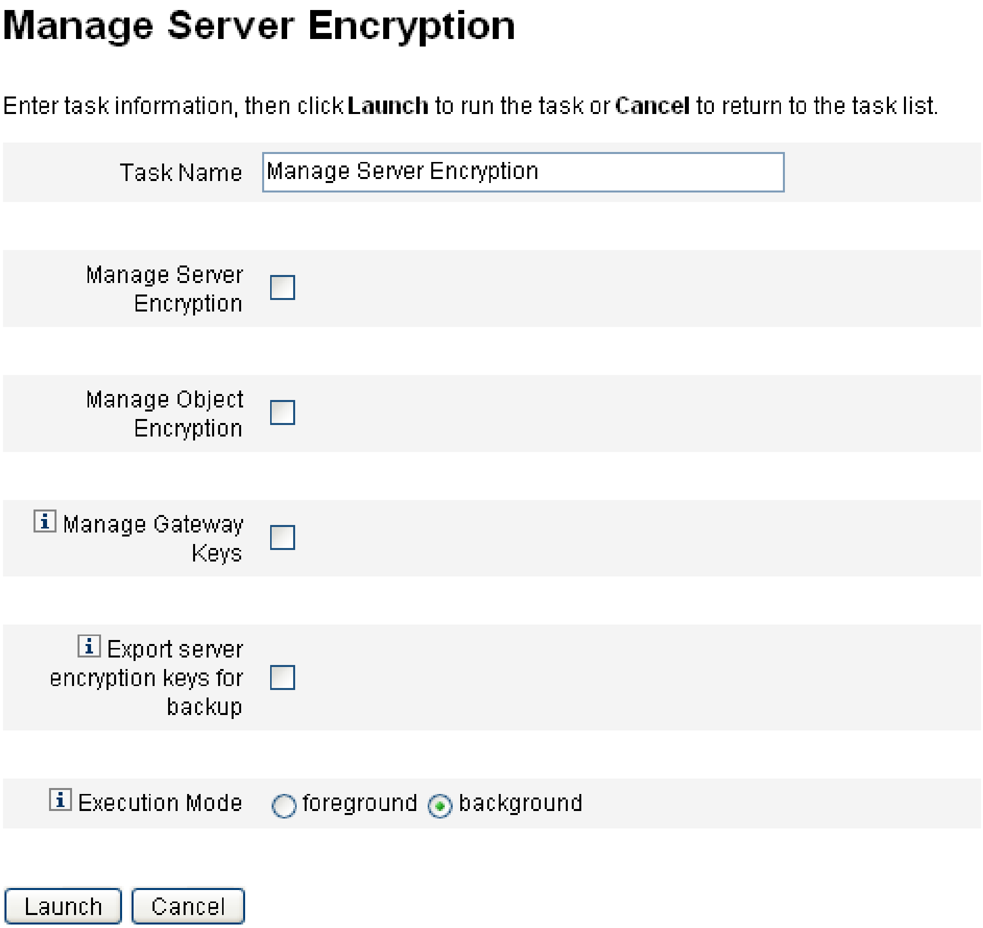
▼ To Access the Manage Server Encryption Page

To open the Manage Server Encryption page,

1. **Select Server Tasks > Run Tasks from the menu bar.**

2. **When the Available Tasks page displays, click Manage Server Encryption to open the Manage Server Encryption page.**

FIGURE 12–1 Manage Server Encryption Page



Manage Server Encryption

Enter task information, then click **Launch** to run the task or **Cancel** to return to the task list.

Task Name	Manage Server Encryption
Manage Server Encryption	□
Manage Object Encryption	□
Manage Gateway Keys	□
Export server encryption keys for backup	□
Execution Mode	○ foreground ● background

▼ To Configure Server Encryption

Use this page to configure server and object encryption, gateway keys, back-up options, and execution mode.

1 Enter a Task Name.

This field defaults to *Manage Server Encryption*. You can enter a different task name if you do not want to use the default setting.

2 Choose one or more of the following options.

- **Manage Server Encryption**. Choose this option to configure server encryption.

The following additional options display:

- **Encryption of server encryption keys**. You must specify a method for encrypting server encryption keys. Encryption types can include Triple DES, PKCS#5 (DES), or PKCS#5 (AES)

  Note –

  - Only those encryption types that are instantiable on your system are displayed on this page. For example, if your system does not support PKCS#5 (AES), only Triple DES and PKCS#5 (DES) are displayed.
  - PKCS#5 (AES) requires that you download and configure the *Unlimited Strength Jurisdiction Policy Files* for the JVM running Oracle Waveset. Refer to your Java vendor's documentation for details.

    Also, PKCS#5 (AES) requires that you install and configure the `Bouncy Castle JCE provider jar` file as a JCE provider for the JVM running Oracle Waveset. This `jar` file is packaged in the Oracle Waveset install image and can be found in the *wshome*`/WEB-INF/lib` directory. Two `jar` files are provided; `bcprov-jdk15-137.jar` and `bcprov-jdk16-137.jar` for use with corresponding versions of Java. Refer to your Java vendor's documentation and the Bouncy Castle documentation for more details.

- **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.
- **Generate new secure random PBE password**. Select this option to generate a new password, based on a server-specific secret, each time the server is started. If you do not select this option, or if your server is not configured to use password-based encryption, then Waveset will use the default key to encrypt the server keys.

- **Manage Object Encryption**. Choose this option to specify which object types should be re-encrypted and which encryption method to use.
  - **Encryption of object types**. Choose one of the displayed encryption types, which can include Triple DES (default), AES 256–bit key, AES, 192–bit key, or AES 128–bit key.

Note – AES using 192– or 256–bit keys requires that you download and configure the *Unlimited Strength Jurisdiction Policy Files* for the JVM running Oracle Waveset. Refer to your Java vendor's documentation for more details.

Only those encryption types that are instantiable on your system will be displayed on this page. For example, if your system does not support AES 192– or 256–bit keys using the *Unlimited Strength Jurisdiction Policy Files*, only Triple DES and AES 128–bit key options are displayed.

  - **Select object types to re-encrypt with current server encryption key**. Choose one or more Waveset object types listed in the table.

- **Manage Gateway Keys**. Choose this option to specify gateway encryption.

  The following options display:

  - **Select gateway key option**. Choose one of the following options:
    - **Generate a new key and synchronize all gateways**. Choose this option when initially enabling a secure gateway environment. This option generates a new gateway key and communicates that key 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.
  - **Gateway key type**. Choose one of the displayed key types, which can include Triple DES, AES 256–bit key, AES, 192–bit key, or AES 128–bit key.

  Note – AES using 192– or 256–bit keys requires that you download and configure the “Unlimited Strength Jurisdiction Policy Files” for the JVM running Oracle Waveset. Refer to your Java vendor's documentation for more details.

  Only those encryption types that are instantiable on your system will be displayed on this page. For example, if your system does not support AES 192– or 256–bit keys using the “Unlimited Strength Jurisdiction Policy Files”, only Triple DES and AES 128–bit key options are displayed.

- **Export server encryption keys for backup**. Choose this option to export existing server encryption keys to an XML-formatted file. When you select this option, Waveset displays an additional field for you to specify a path and file name to export the keys.

Note – Select this option if you are using PKCS#5 encryption and chose to generate and set a new server encryption key. In addition, you should store the exported keys on removable media and in a secure location (not on a network).

3 **Choose the Execution Mode.**

You can run this task in the foreground or background (default setting).

Note – If you choose to re-encrypt one or more object types with a newly generated key, that task can take some time and is best run in the background.

4 **When you are finished configuring the options on this page, click Launch.**

Using Authorization Types to Secure Objects

You typically use permissions specified in an `AdminGroup` capability to grant access to an Waveset `objectType` such as a Configuration, Rule, or `TaskDefinition`. However, granting access to all objects of an Waveset `objectType` within one or more controlled organizations is sometimes still too broad.

Using authorization types (`AuthType`) allows you to further scope or restrict this access to a subset of objects for a given Waveset `objectType`. For example, you might not want to give your users access to all rules within their scope of control when populating rules to select from in a user form.

To define a new authorization type, edit the `AuthorizationTypes` configuration object in the Waveset repository and add a new `<AuthType>` element.

This element requires two properties:

- The name of the new authorization type
- The existing authorization type or `objectType` the new element extends or scopes

For example, if you want to add a new Rule authorization type, called `Marketing Rule`, that extends `Rule`, you would define the following:

```
<AuthType name=’Marketing Rule’ extends=’Rule’/>
```

Next, to enable the authorization type to be used, you must reference that authorization type in two places.

- Within a custom `AdminGroup` capability that grants one or more rights to the new authorization type
- Within the objects that should be of this type

Following are examples of both references. The first example shows an AdminGroup capability definition granting access to Marketing Rules.

EXAMPLE 12–4 AdminGroup Capability Definition

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

The next example shows a Rule definition that enables users to access the object because they have been granted access to Rule or Marketing Rule.

EXAMPLE 12–5 Rule Definition

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

Note – Any user granted rights to a parent authorization type, or to a static type that an authorization type extends, will have the same rights on all child authorization types. So, using the preceding example, any user granted rights to Rule will also have the same rights to Marketing Rule. The converse, however, is not true.

Security Practices

As an Waveset administrator, you can further reduce security risks to your protected accounts and data by following these recommendations, at setup time and after.

At Setup

To reduce security risks during setup:

- Access Waveset through a secure Web server using HTTPS.
- Reset the passwords for the default Waveset 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 Waveset Index Repository.
- Turn on auditing to track activities in the Waveset application.
- Edit the permissions on files in the Waveset directory.
- Customize workflows to insert approvals or other checkpoints.
- Develop a recovery procedure to describe how to recover your Waveset environment in the event of emergency.

During Use

To reduce security risks during use:

- Periodically change the passwords for the default Waveset administrator accounts (Administrator and Configurator).
- Log out of Waveset when not actively using the system.
- Set or know the default timeout period for an Waveset session. Session timeout values may differ, as they can be set independently for each login application.

If your application server is Servlet 2.2-compliant, the Waveset 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>
```

CHAPTER 13

Identity Auditing: Basic Concepts

This chapter introduces you to the concepts behind identity auditing and audit controls. Audit controls can be used to monitor and manage auditing and compliance across enterprise information systems and applications.

In this chapter, you will learn about the following concepts and tasks:

- "About Identity Auditing" on page 399
- "Goals of Identity Auditing" on page 400
- "Understanding Identity Auditing" on page 401
- "Working with Identity Auditing in the Administrator Interface" on page 403
- "Enabling Audit Logging" on page 405

About Identity Auditing

Waveset defines *auditing* as the systematic capture, analysis, and response to identity data across an enterprise to ensure compliance with internal and external policies and regulations.

Compliance with accounting and data privacy legislation is not a simple task. Waveset's auditing features offer a flexible approach, allowing you to implement a compliance solution that works for your enterprise.

In most environments, different groups are involved with compliance: internal and external auditing teams (for whom auditing is the primary focus); and non-auditing staff (who may see auditing as a distraction). IT often is involved with compliance as well, helping transition internal auditing team requirements to a chosen solution's implementation. The key to successfully implementing an auditing solution is in accurately capturing the knowledge, controls, and processes of non-auditing staff, and then automating the application of that information.

Goals of Identity Auditing

Identity auditing improves audit performance as follows:

- *Identity auditing automatically detects compliance violations and facilitates swift remediation through immediate notification*

  Waveset audit policy features let you define *rules* (that is, criteria) for violations. Once defined, the system scans for conditions that violate established policies, such as unauthorized access changes or erroneous access privileges. Upon detection, the system notifies the appropriate persons according to a defined escalation chain. User-invoked tasks, or workflows that are automatically invoked by policy violations, can then remediate (correct) the violation.
- *Provides key information, on-demand, about the effectiveness of internal audit controls*

  The Auditor Reports provide summary status information about violations and exceptions for quick analysis of risk status. The Reports tab also provides graphical reports of violations. You can view violations by resource, organization, or policy, customizing each chart according to the report characteristics you define.
- *Automates certification reviews of identity controls to reduce operational risk*

  Workflow capabilities enable automated notification of policy and access violations to selected reviewers.
- *Prepares comprehensive reports that detail user activity and meet regulatory requirements*

  The Reports area lets you define detailed reports and charts that provide information on access history and privileges, and other policy violations. The system keeps a secure and comprehensive identity audit trail that can be mined, through reporting capabilities, for access data and user profile updates.
- *Streamlines the process of periodic reviews to maintain security and regulatory compliance*

  Periodic access reviews can be conducted to collect user entitlement records and determine which entitlements require review. The process then notifies designated attestors of pending requests for review and updates the status or pending requests when attestor actions on the requests are completed.
- *Identifies potential conflict-of-interest capabilities for user accounts*

  Waveset provides a Separation of Duties report that identifies users with specific capabilities or privileges that could be a potential conflict of interest.

Understanding Identity Auditing

Waveset provides a feature for auditing user account privileges and access rights, and a separate feature for maintaining and certifying compliance. These features are policy-based compliance and periodic access reviews.

Policy-Based Compliance

Waveset employs an audit policy system that allows administrators to maintain compliance of company-established requirements for all user accounts.

You can use audit policies to ensure compliance in two different and complementary ways: continuous compliance and periodic compliance.

These two techniques are particularly complementary in an environment in which provisioning operations may be performed outside of Waveset. When an account can be changed by a process that does not execute or honor existing audit policies, periodic compliance is necessary.

Continuous Compliance

Continuous compliance means that an audit policy is applied to all provisioning operations, such that an account cannot be modified in a way that does not comply with current policy.

You enable continuous compliance by assigning an audit policy to an organization, a user, or both. Any provisioning operations performed on a user will cause the user-assigned policies to be evaluated. Any resulting policy failure will interrupt the provisioning operation.

An *organization-based* policy set is defined hierarchically. There is only one organization policy set in effect for any user. The applied policy set is the one assigned to the lowest-level organization. For example:

Organization	Directly Assigned Policy Set	Effective Policy
Austin	Policies A1, A2	Policies A1, A2
Marketing		Policies A1, A2
Development	Policies B, C2	Policies B, C2
Support		Policies B, C2
Test	Policies D, E5	Policies D, E5
Finance		Policies A1, A2
Houston		<none>

Periodic Compliance

Periodic compliance means that Waveset evaluates policy on-demand. Any noncompliant conditions are captured as compliance violations.

When executing periodic compliance scans, you can select which policies to use in the scan. The scan process blends directly-assigned policies (user-assigned and organization-assigned policies) and an arbitrary set of selected policies.

Waveset users with Auditor Administrator capabilities can create audit policies and monitor compliance with those policies through periodic execution of policy scans and reviews of policy violations. Violations can be managed through remediation and mitigation procedures.

For more information about the Auditor Administrator capabilities, see "Understanding and Managing Capabilities" on page 198 in Chapter 6, "Administration."

Waveset auditing allows for regular scans of users. These scans execute audit policies to detect deviations from established account limits. When a violation is detected, remediation activities are initiated. The rules may be standard audit policy rules provided by Waveset, or customized, user-defined rules.

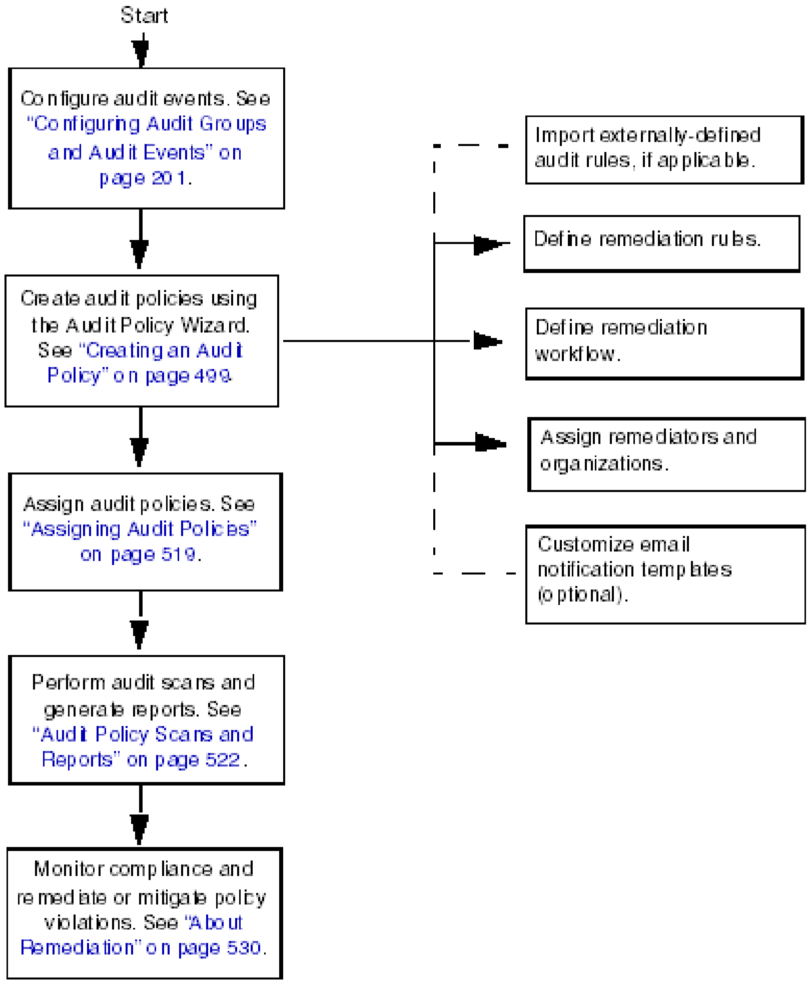
Logical Task Flow for Policy-Based Compliance

Figure 13–1 shows a logical task flow for establishing policy-based audit controls.

Periodic Access Reviews

Waveset provides for periodic access reviews that enable managers and other responsible parties to review and verify user access privileges on an ad-hoc or periodic basis. For more information about this feature, see "Periodic Access Reviews and Attestation" on page 442.

FIGURE 13–1 A Logical Task Flow for Establishing Policy-based Compliance


Start
Configure audit events. See "Configuring Audit Groups and Audit Events" on page 201.
Create audit policies using the Audit Policy Wizard. See "Creating an Audit Policy" on page 499.
Assign audit policies. See "Assigning Audit Policies" on page 519.
Perform audit scans and generate reports. See "Audit Policy Scans and Reports" on page 522.
Monitor compliance and remediate or mitigate policy violations. See "About Remediation" on page 530.
Import externally-defined audit rules, if applicable.
Define remediation rules.
Define remediation workflow.
Assign remediators and organizations.
Customize email notification templates (optional).

Working with Identity Auditing in the Administrator Interface

This section describes how to access Identity Auditing features in the Administrator Interface. Email notification templates used in identity auditing are also discussed.

Using the Compliance Section of the Interface

To create and manage audit policies, use the Compliance section of the Waveset Administrator interface.

▼ To Use the Compliance section to Create and Manage Audit Policies

1. **Log in to the Administrator interface (“Logging in to the Waveset End-User Interface” on page 41).**

2. **Click Compliance in the menu bar.**

   The following subtabs (or menu items) are available in the Compliance section:

   - Manage Policies
   - Manage Access Scans
   - Access Reviews

Manage Policies

The Manage Policies page lists the policies that you have permission to view and edit. You can also manage access scans from this area.

From the Manage Policies page, you can work with audit policies to accomplish these tasks:

- Create an audit policy
- Select a policy to view or edit
- Delete a policy

Detailed information about these tasks follows in the section “A Sample Audit Policy Scenario” on page 409.

Manage Access Scans

Use the Manage Access Scans tab to create, modify, and delete access scans. Here you can define scans that you want to run or schedule for periodic access reviews. For more information about this feature, see “Periodic Access Reviews and Attestation” on page 442.

Access Reviews

The Access Reviews tab enables you to launch, terminate, delete, and monitor the progress of your access reviews. It displays a summary report of the scan results with information links that enable you to access more detailed information about the review status and pending activities.

For more information about this feature, see “Managing Access Reviews” on page 451.

Identity Auditing Tasks Interface Reference

To look up how to perform other identity auditing tasks in the Administrator interface, see Table B–8. This quick reference tells you where to go to start a variety of auditing tasks.

Email Templates

Identity Auditing uses email-based notification for a number of operations. For each of these notifications, an email template object is used. The email template allows the headers and body of email messages to be customized.

TABLE 13–1 Identity Auditing Email Templates

Template Name	Purpose
Access Review Remediation Notice	Sent to remediators by an access review when user entitlements are initially created in a remediating state.
Bulk Attestation Notice	Sent to attestors by an access review when they have pending attestations.
Policy Violation Notice	Sent to remediators by an audit policy scan when violations occur.
Access Scan Begin Notice	Sent to an access scan owner when an access review starts a scan.
Access Scan End Notice	Sent to an access scan owner when an access scan completes.

Enabling Audit Logging

Before you can begin managing compliance and access reviews, the Waveset audit logging system must be enabled and configured to collect audit events. By default, the auditing system is enabled. An Waveset administrator with the Configure Audit capability can configure auditing.

Waveset provides the Compliance Management audit configuration group.

Use the following steps to view or modify events stored by the Compliance Management group.

1. **Log in to the Administrator interface** (“Logging in to the Waveset End-User Interface” on page 41).
2. **Select Configure from the menu bar, and then click Audit**.
3. **On the Audit Configuration page, select the Compliance Management audit group name**.

Note –

- For more information about setting up audit configuration groups, see “Configuring Audit Groups and Audit Events” on page 102.
- For information about how the audit system records events, see Chapter 10, “Audit Logging.”

CHAPTER 14

Auditing: Audit Policies

This chapter describes an audit policy and contains instructions for creating, editing, deleting, and assigning audit policies using the Audit Policy Wizard.

About Audit Policies

An *audit policy* defines the account limits for users of one or more resources. Audit scans evaluate the criteria defined in audit policies to determine whether violations have occurred in your organization.

Audit policies consist of the following components:

- **Audit Policy rules** that define conditions that constitute a policy violation. The audit policy can restrict which resources are available to the rule.
- **Remediation workflows** (optionally) that launch remediation tasks that process policy rule violations when they occur.
- **Designated administrators or remediators** who are authorized to view and respond to policy violations. Remediators can be individual users or groups of users.

Defining Audit Policy Rules

One audit policy can contain hundreds of rules that reference a wide range of resources. These rules define potential conflicts on an attribute basis within an audit policy. In Waveset, you can define rules that check only a single attribute on a single resource or that check multiple attributes on multiple resources. During evaluation, the rule has access to user account data from one or more resources.

You can use Waveset's Audit Policy Wizard to create simple rules. If you need to create more powerful rules, you can use the Identity Manager IDE or an XML editor.

When defining rules for an audit policy, remember the following:

- Rules can contain functions written in the XPRESS, XML Object, or JavaScript languages.
- Rules must be of subType `SUBTYPE_AUDIT_POLICY_RULE`.
- Rules must be of authType `AuditPolicyRule`.

Note – Rules generated by the Audit Policy Wizard are automatically assigned the appropriate subType and authType.

Rules created using the Audit Policy Wizard return a `true` or `false` value. Any policy rule that returns a `true`value results in a policy violation.

However, if you use the Identity Manager IDE, you can create rules that skip a user during an audit scan or an access review. An audit policy rule that returns a value of `ignore` stops rule processing for that user and skips to the next target user.

For more information about creating audit policy rules, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.

Addressing Policy Violations with Remediation Workflows

After creating rules to define policy violations, you select the workflow to launch when Waveset detects a violation during an audit scan. Waveset provides the default Standard Remediation workflow, which provides default remediation processing for audit policy scans. Among other actions, this default remediation workflow generates notification email to each designated Level 1 remediator (and subsequent levels of remediators, if necessary).

Note – Unlike Waveset workflow processes, you must assign the `AuthType=AuditorAdminTask` and the `SUBTYPE_REMEDIATION_WORKFLOW` subtype to remediation workflows. If you are importing a workflow for use in audit scans, you must manually add this attribute. See "(Optional) Import Separation of Duty Rules into Waveset" on page 411 for more information.

Designating Remediators

If you assign a remediation workflow, you must designate at least one remediator. You can designate up to three levels of remediators for an audit policy. For more information about remediation, see “Compliance Violation Remediation and Mitigation” on page 433.

Note – You must assign a remediation workflow before you can assign remediators.

A Sample Audit Policy Scenario

Suppose you are responsible for accounts payable and receivable, and you must implement procedures to prevent a potentially risky aggregation of responsibilities for employees working in the accounting department. This policy must ensure that personnel with responsibility for accounts payable do not also have responsibility for accounts receivable.

The audit policy must contain:

- A set of rules, each specifying a condition that constitutes a policy violation.
- A workflow that launches remediation tasks.
- A group of designated administrators, or remediators, with permission to view and respond to policy violations created by the preceding rules.

After the rules identify policy violations (in this scenario, users with too much authority), the associated workflow can launch specific remediation-related tasks, including automatically notifying select remediators.

Level 1 remediators are the first remediators contacted when an audit scan identifies a policy violation. When the escalation period identified in this area is exceeded, Waveset notifies the remediators at the next level (if more than one level is specified for the audit policy).

The “Creating an Audit Policy” on page 409 section describes how to use the Audit Policy Wizard to create an audit policy.

Creating an Audit Policy

To create an Audit Policy, use the Audit Policy Wizard.

▼ To Open the Audit Policy Wizard

The Audit Policy Wizard guides you through the process of creating an audit policy. Use the following steps to access the wizard:

1 **Log in to the Administrator interface ("Logging in to the Waveset End-User Interface" on page 41).**

2 **Click the Compliance tab.**

The Manage Policies subtab or menu opens.

3 **To create a new audit policy, click New.**

Creating an Audit Policy: Overview

Using the wizard, you will perform the following tasks to create an audit policy:

- Select or create the rules you want to use to define policy limits
- Assign approvers and establish escalation limitations
- Assign a remediation workflow

After completing the task presented in each wizard screen, click Next to move to the next step.

Before You Begin

Plan carefully before creating an audit policy! Before you begin, verify that you have completed these tasks:

- Identify the rules you will use to create the policy in the Audit Policy Wizard. The rules you choose are determined by the type of policy you are creating and the specific limitations you want to define. See "To Identify the Rules You Need" on page 410 in the next section for more information.
- Import any remediation workflow or rule that you want to include in the new policy. See "(Optional) Import Separation of Duty Rules into Waveset" on page 411for more information.
- Ensure that you have the required capabilities to create audit policies. See the required capabilities in "Understanding and Managing Capabilities" on page 198 in Chapter 6, "Administration."

▼ To Identify the Rules You Need

The constraints you specify in the policy are implemented in a set of rules that you create or import. When using the Audit Policy Wizard to create a rule, perform the following steps:

1 **Identify the specific resource you are working with.**

2 **Select an account attribute from the list of attributes that are valid for the resource.**

3 **Select a condition to impose on the attribute.**

4 **Enter a value for comparison.**

For information on creating audit policy rules outside of the Audit Policy Wizard, see Chapter 4, “Working with Rules,” in *Oracle Waveset 8.1.1 Deployment Reference*.

(Optional) Import Separation of Duty Rules into Waveset

The Audit Policy Wizard cannot create Separation of Duty rules. You must construct these rules outside of Waveset and import the rules by using the Import Exchange File option on the Configure tab.

(Optional) Import a Workflow into Waveset

▼ To Import an External Workflow

To use a remediation workflow that is not currently available from Waveset, import the external workflow. You can create custom workflows using an XML editor or the Identity Manager IDE.

1 **Set** `authType=’AuditorAdminTask’ and add subtype=’SUBTYPE_REMEDIATION_WORKFLOW’`**. You can use the Identity Manager IDE or your XML editor of choice to set these configuration objects.**

2 **Import the workflow by using the Import Exchange File option.**

a. **Log in to the Administrator interface (“Logging in to the Waveset End-User Interface” on page 41).**

b. **Click the Configure tab, then click the Import Exchange File subtab or menu.**

The Import Exchange File page opens.

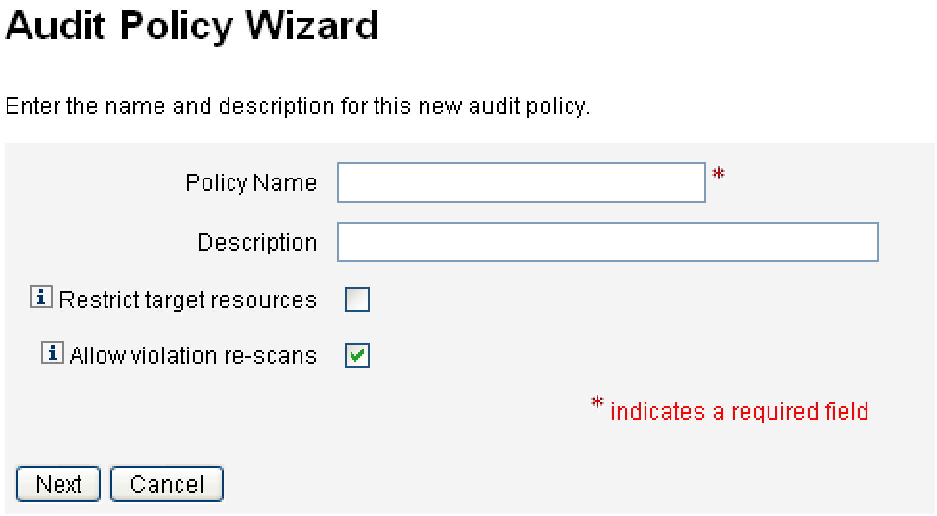
c. **Browse to the workflow file to upload, then click Import.**

After you have successfully imported the workflow, it appears in the Audit Policy Wizard (“Creating an Audit Policy” on page 409) Remediation Workflow list of options.

Name and Describe the Audit Policy

Enter the name of the new policy and a brief description in the Audit Policy Wizard (shown in Figure 14–1).

FIGURE 14–1 Audit Policy Wizard: Enter Name and Description Screen



Audit Policy Wizard

Enter the name and description for this new audit policy.

Policy Name *

Description

Restrict target resources □

Allow violation re-scans ☑

* indicates a required field

Note – Audit policy names cannot contain these characters: ' (apostrophe), . (period), | (pipe), [(left bracket),] (right bracket), , (comma), : (colon), $ (dollar sign), " (double quote), \ (backslash), or = (equals sign).

You should also avoid using the following characters: _ (underscore), % (percent-sign), ^ (caret), and * (asterisk).

If you want only selected resources to be accessed when executing the scan, select the Restrict target resources option.

If you want a remediation of a violation to result in an immediate rescan of the user, then select the Allow violation re-scans option.

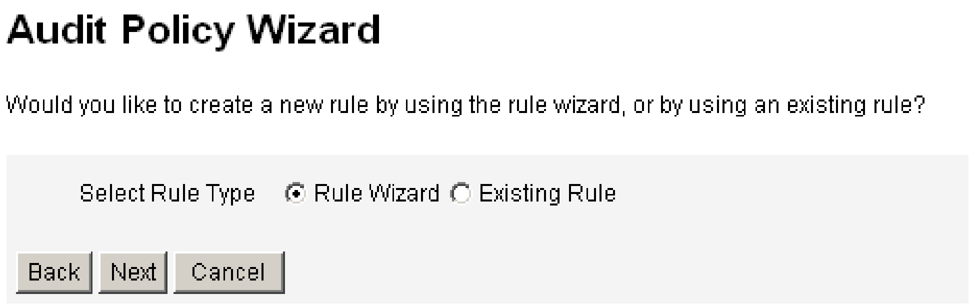
Note – If the audit policy does not restrict resources, then all resources for which a user has accounts will be accessed during the scan. If the rules only use a few resources, then it is more efficient to restrict the policy to those resources.

Click Next to proceed to the next page.

▼ To Select a Rule Type

Use this page to start the process of defining or including rules in your policy. (The bulk of your work while creating a policy is defining and creating rules.)

As shown in the following figure, you can choose to create your own rule by using the Waveset Rule wizard, or you can incorporate an existing rule. The Rule Wizard only allows one resource to be used in a rule. Imported rules can reference as many resources as needed.



Audit Policy Wizard

Would you like to create a new rule by using the rule wizard, or by using an existing rule?

Select Rule Type ● Rule Wizard ○ Existing Rule

1 **Decide whether you want to create a new rule or use an existing rule.**

Choose one of the following options:

- To create a new rule, choose the Rule Wizard option (default setting).
- To incorporate an existing rule you created using the Identity Manager IDE, choose the Existing Rule option.

2 **Click Next.**

3 **Based on your selection in step 1, continue to one of the following sections:**

- If you selected Rule Wizard, go to the "To Use the Rule Wizard to Create a New Rule" on page 414section and follow the instructions provided.
- If you selected Existing Rule, go to the "To Select an Existing Rule" on page 413section and follow the instructions provided.

To Select an Existing Rule

To include an existing rule in the new policy, select Existing Rule on the Select Rule Type Screen and click Next. Then, select an existing audit policy rule from the Select Existing Rule drop-down menu.

Note – If you cannot see the name of a rule that you have previously imported into Waveset, confirm that you added the attributes described in "Defining Audit Policy Rules" on page 407 to the rule.

Click Next.

Skip to the section "Adding Rules" on page 417.

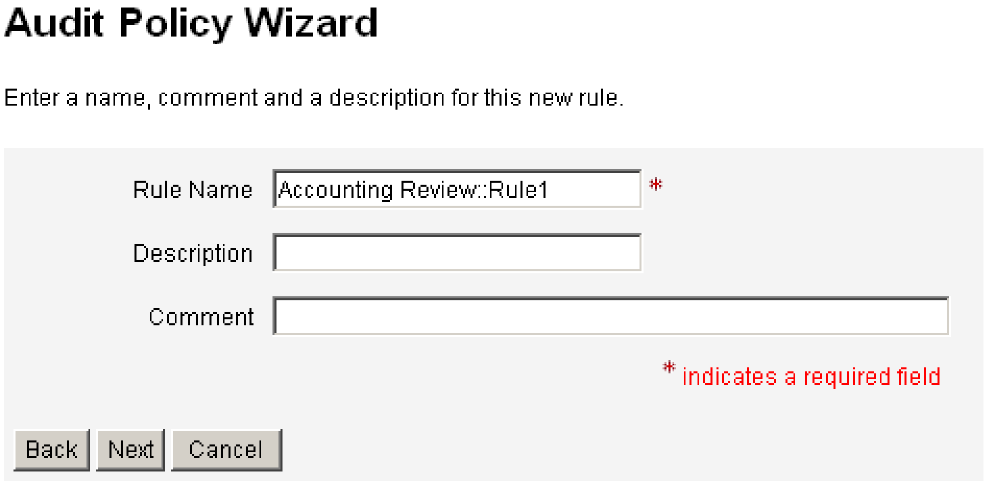
To Use the Rule Wizard to Create a New Rule

If you choose to create a rule by using the Rule Wizard selection in the Audit Policy Wizard, proceed by entering information on the pages discussed in the following sections.

To Name and Describe the New Rule

Optionally name and describe the new rule. Use this page to enter descriptive text that appears next to the rule name whenever Waveset displays the rule. Enter a concise and clear description that is meaningful in describing the rule. This description is displayed within Waveset in the Review Policy Violations page.

FIGURE 14–2 Audit Policy Wizard: Enter the Rule Description Screen



Audit Policy Wizard

Enter a name, comment and a description for this new rule.

Rule Name: Accounting Review::Rule1 *

Description:

Comment:

* indicates a required field

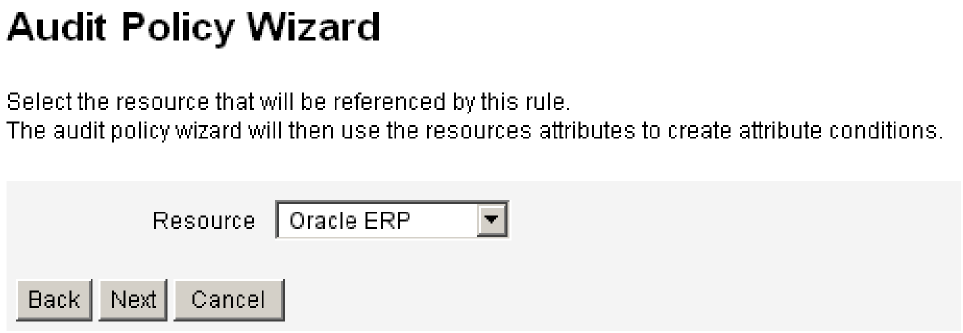
For example, if you are creating a rule that will identify users who have both an Oracle ERP responsibilityKey attribute value of `Payable User` and a `Receivable User` attribute value, you could enter the following text in the Description field: **`Identifies users with both Payable User and Receivable User responsibilities`**.

Use the Comments field to provide any additional information about the rule.

Select the Resource Referenced by the Rule

Use this page to select the resource that the rule will reference. Each rule variable must correspond to an attribute on this resource. All resources that you have view access to will appear in this options list. In this example, Oracle ERP is selected.

FIGURE 14–3 Audit Policy Wizard: Select Resource Screen



Audit Policy Wizard

Select the resource that will be referenced by this rule.
The audit policy wizard will then use the resources attributes to create attribute conditions.

Resource: Oracle ERP

Note – Most, but not all, attributes of each available resource adapter are supported. For information on the specific attributes that are available, see *Oracle Waveset 8.1.1 Resources Reference*.

Click Next to move to the next page.

Create the Rule Expression

Use this screen to enter the rule expression for your new rule. This example creates a rule in which a user with an Oracle ERP `responsibilityKey` attribute value of `Payable User` cannot also have a `Receivable User` attribute value.

▼ To Create a Rule Expression

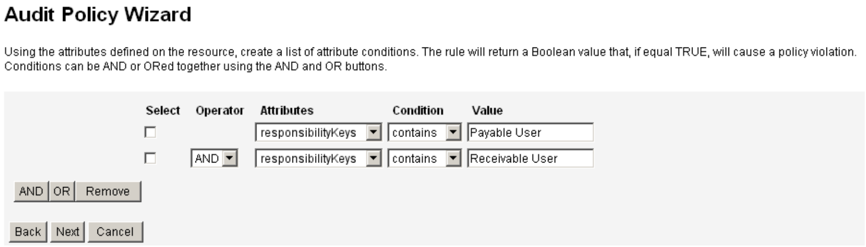
1 **Select a user attribute from the list of available attributes. This attribute will directly correspond to a rule variable.**

2 **Select a logical condition from the list. Valid conditions include = (equal to), != (not equal to), < (less than), <= (less than or equal to), > (greater than), >= (greater than or equal to), is true, is null, is not null, is empty, and contains. For the purpose of this example, you could select** `contains` **from the list of possible attribute conditions.**

3. **Enter a value for the expression. For example, if you enter `Payable user`, you are specifying an Oracle ERP user with the value of `Payable user` in the `responsibilityKeys` attribute.**

4. **(Optional) Click the `AND` or `OR` operators to add another line and create another expression.**

FIGURE 14–4 Audit Policy Wizard: Select Rule Expression Screen



Audit Policy Wizard

Using the attributes defined on the resource, create a list of attribute conditions. The rule will return a Boolean value that, if equal TRUE, will cause a policy violation. Conditions can be AND or ORed together using the AND and OR buttons.

Select	Operator	Attributes	Condition	Value
□		responsibilityKeys	contains	Payable User
□	AND	responsibilityKeys	contains	Receivable User

This rule returns a Boolean value. If both statements are true, then the policy rule returns a value of TRUE, which causes a policy violation.

Note – Waveset does not support the control of rule nesting. In addition, using the Audit Policy Wizard to create policies with different Boolean operators between the rules can produce unpredictable results because the order of evaluation is unspecified.

For complex Rule expressions, create the rules using an XML editor instead of using the Audit Policy Wizard. Using an XML editor allows you to negate where necessary to only use a single Boolean operator between rules.

The following code example shows the XML for the rule you have created in this screen:

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name=’resource’ value=’Oracle ERP’>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type=’ObjectGroup’ id=’#ID#Top’ name=’Top’/>
    </MemberObjectGroups>
</Rule>
```

To remove an expression from the rule, select the attribute condition and then click Remove.

Click Next to continue in the Audit Policy Wizard. You will have the opportunity to add more rules, either by adding existing rules, or by again using the wizard.

Adding Rules

You can create additional rules by importing existing rules or by using the wizard. (See “To Select a Rule Type” on page 412for more information.)

Click the `AND` or `OR` operators to continue adding rules as necessary. To remove a rule, select it and then click Remove.

Policy violations occur only if the Boolean expression of *all* rules evaluates to true. By grouping rules with AND/OR operators, it is possible for the policy to evaluate to true, even though all rules do not. Waveset creates violations only for rules that evaluate to true, and only if the policy expression evaluates to true.

Note – Waveset does not support the control of rule nesting. In addition, using the Audit Policy Wizard to create policies with different Boolean operators between the rules can produce unpredictable results because the order of evaluation is unspecified.

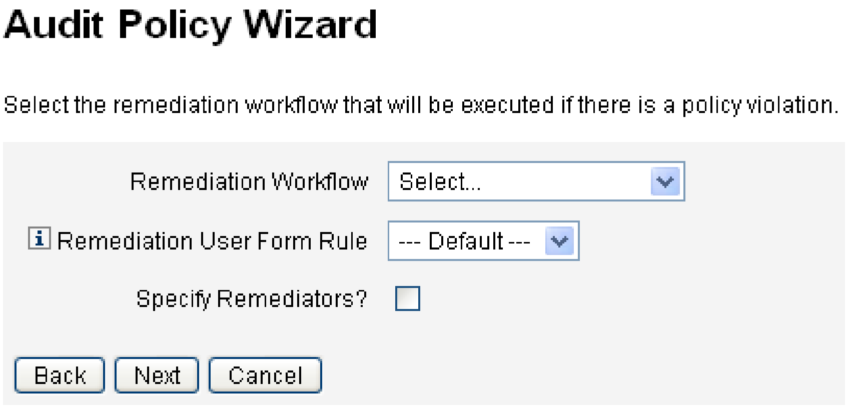
For complex Rule expressions, create the rules using an XML editor instead of using the Audit Policy Wizard. Using an XML editor allows you to negate where necessary to only use a single Boolean operator between rules.

Select a Remediation Workflow

Use this screen to select a Remediation workflow to associate with this policy. The workflow assigned here determines the actions taken within Waveset when an audit policy violation is detected.

Note – One workflow is started for each failed audit policy. Each workflow will contain one or more work items for each compliance violation created by the policy scan for the specific policy.

FIGURE 14–5 Audit Policy Wizard: Select Remediation Workflow Screen



Audit Policy Wizard

Select the remediation workflow that will be executed if there is a policy violation.

Remediation Workflow: Select...

Remediation User Form Rule: --- Default ---

Specify Remediators? □

Note – For information about importing a workflow that you have created by using an XML editor or the Identity Manager IDE, see "(Optional) Import Separation of Duty Rules into Waveset" on page 411.

Use the Remediation User Form Rule drop-down menu to select a rule that will calculate the user form that should be applied when editing a user through a remediation. By default, a remediator that edits a user in response to a remediation work item will use the user form assigned to the remediator. If an audit policy specifies a remediation user form, then this form is used instead. This allows a very specific form to be used when an audit policy indicates a corresponding, specific problem.

To specify remediators to be associated with this remediation workflow, select the Specify Remediators? check box. If you select this option, then clicking Next will display the "Assign Remediators" page. If you do not select this option, then the wizard will next display the "Audit Policy Wizard Assign Organizations" screen.

Select Remediators and Timeouts for Remediations

If you specify remediators, the remediators assigned to this audit policy will be notified when a violation of this policy is detected. Also, the default workflow assigns a remediation work item to them. Any Waveset user can be a remediator.

You might choose to assign at least one Level 1 remediator, or designated user. Level 1 remediators are contacted first through email launched by the remediation workflow when a policy violation is detected. If the designated escalation timeout period is reached before a Level

1 remediator responds, Waveset next contacts the Level 2 remediators that you specify here. Waveset contacts Level 3 remediators only if neither Level 1 nor Level 2 remediators respond before the escalation time period lapses.

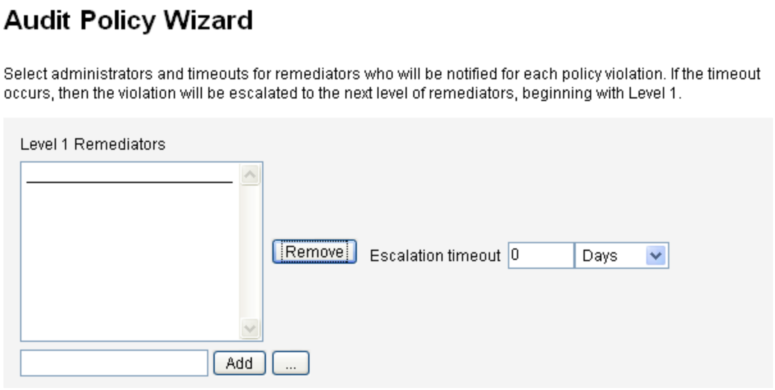
Note – If you specify an escalation timeout value for the highest-level remediator selected, then the work item is removed from the list when the escalation times out. By default, an escalation timeout is set to a value of 0. In this case, the work item does not expire and remains in the remediator's list.

Assigning Remediators is optional. If you select this option, then click Next to proceed to the next screen after specifying the settings.

To add users to the available list of remediators, enter a user ID and then click Add. Alternatively, click **...** (More) to search for a user ID. Enter one or more characters in the Starts With field, and then click Find. After selecting a user from the search list, click Add to add it to the list of remediators. Click Dismiss to close the search area.

To remove a user ID from the list of remediators, select it in the list, and then click Remove.

FIGURE 14–6 Audit Policy Wizard: Select Level 1 Remediator Area



Audit Policy Wizard

Select administrators and timeouts for remediators who will be notified for each policy violation. If the timeout occurs, then the violation will be escalated to the next level of remediators, beginning with Level 1.

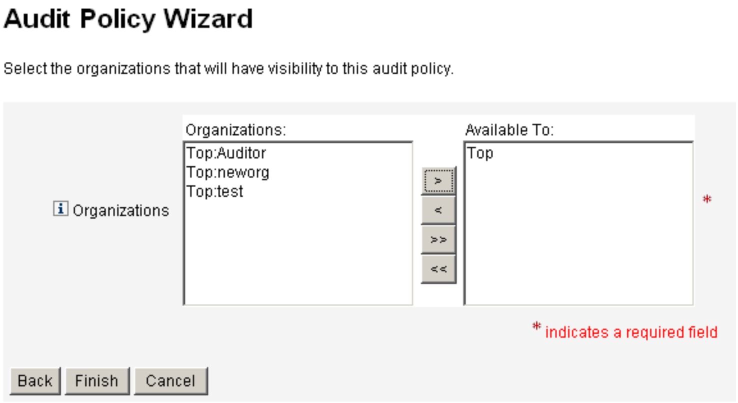
Level 1 Remediators

Escalation timeout 0 Days

Select Organizations that Can Access this Policy

Use this screen, illustrated in Figure 14–7, to select the organizations that can view and edit this policy.

FIGURE 14–7 Audit Policy Wizard: Assign Organizations Visibility Screen



Audit Policy Wizard

Select the organizations that will have visibility to this audit policy.

Organizations

Organizations:
Top:Auditor
Top:neworg
Top:test

Available To:
Top

* indicates a required field

After making organization selections, click Finish to create the audit policy and return to the Manage Policies page. The newly created policy is now visible in this list.

After creating an audit policy, you can perform various actions on the policy, such as editing or deleting it. Read the remaining sections in this chapter for more information.

Editing an Audit Policy

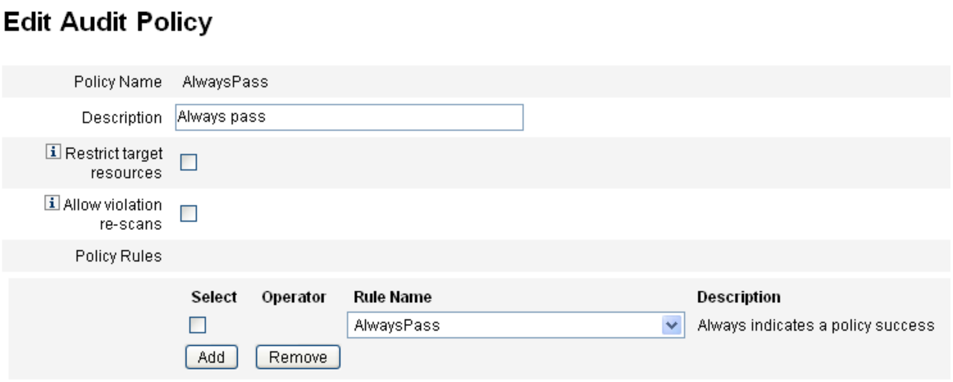
Common editing tasks on audit policies include:

- Adding or deleting rules
- Changing the targeted resources
- Adjusting the list of organizations that have access to the policy
- Changing the escalation timeout associated with each level of remediation
- Changing the remediation workflow associated with the policy

The Edit Policy Page

Click a policy name in the Audit Policy name column to open the Edit Audit Policy page. This page categorizes audit policy information in these areas:

- Identification and Rules area
- Remediators and Escalation timeout area
- Workflow and Organizations Area



Edit Audit Policy

Policy Name	AlwaysPass
Description	Always pass
Restrict target resources	□
Allow violation re-scans	□
Policy Rules	

Select	Operator	Rule Name	Description
□		AlwaysPass	Always indicates a policy success

Use this area of the page to:

- Edit the policy description
- Add or delete a rule

Note – You cannot use this product to directly edit an existing rule. Use the Identity Manager IDE or an XML editor to edit the rule, and then import it into Waveset. You can then remove the previous version, and add the newly revised version.

Edit Audit Policy Description

Edit the audit policy description by selecting the text in the Description field and then entering new text.

Edit Options

Optionally select or deselect the Restrict target resources or Allow violation re-scans options.

Delete a Rule from the Policy

To delete a rule from the policy, click the Select button that precedes the rule name, and then click Remove.

Add a Rule to the Policy

Click Add to append a new field that you can use to select a rule to add.

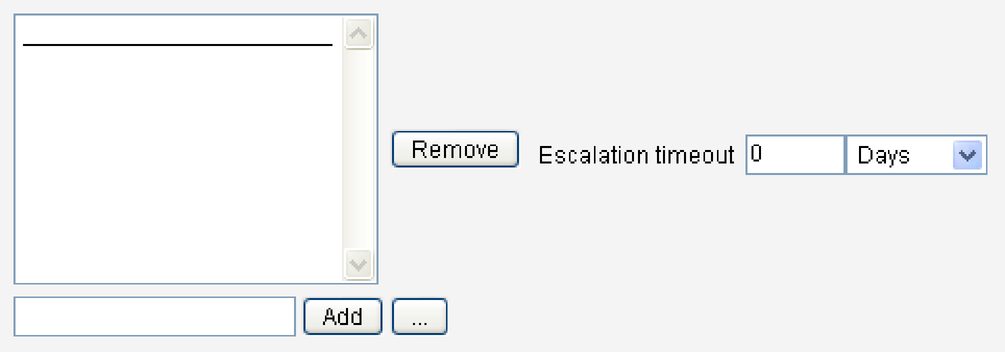
Change a Rule used by the Policy

In the Rule Name column, select another rule from the selection list.

Remediators Area

Figure 14–8 shows a portion of the Remediators area, where you assign Level 1, Level 2, and Level 3 remediators for a policy.

FIGURE 14–8 Edit Audit Policy Page: Assign Remediators



Use this area of the page to:

- Remove or assign remediators to a policy
- Adjust escalation timeouts

Remove or Assign Remediators

Select a remediator for one or more remediation levels by entering a user ID and then clicking Add. To search for a user ID, click **...** (More). You must select at least one remediator.

To remove a remediator, select a user ID in the list, and then click Remove.

Adjust Escalation Timeouts

Select the timeout value, then enter the new value. By default, no timeout value is set

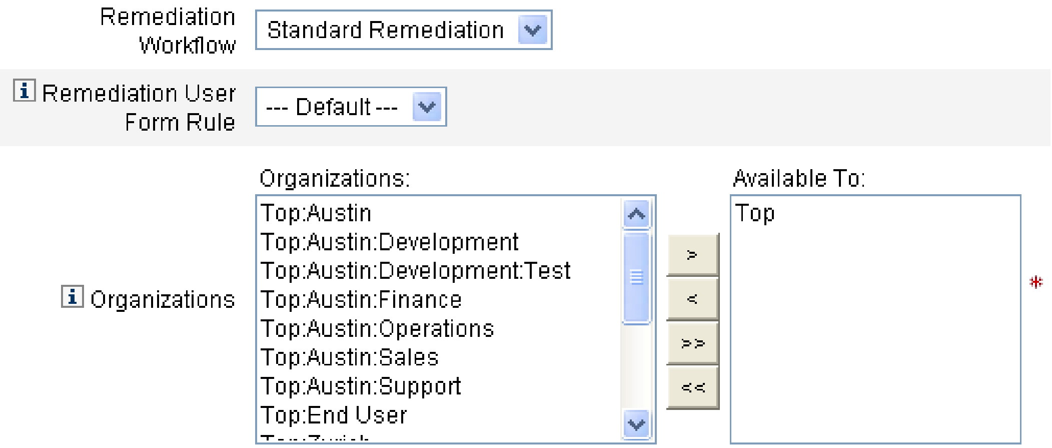
---

Note – If you specify an escalation timeout value for the highest-level remediator selected, then the work item is removed from the list when the escalation times out.

Remediation Workflow and Organizations Area

Figure 14–9 shows the area in which you specify the remediation workflow and organizations for an audit policy.

FIGURE 14–9 Edit Audit Policy Page: Remediation Workflow and Organizations



Remediation Workflow: Standard Remediation

Remediation User Form Rule: --- Default ---

Organizations

Organizations:
Top:Austin
Top:Austin:Development
Top:Austin:Development:Test
Top:Austin:Finance
Top:Austin:Operations
Top:Austin:Sales
Top:Austin:Support
Top:End User

Available To:
Top

Use this area of the page to:

- Change the remediation workflow that is launched when a policy violation occurs
- Select a remediation user form rule
- Adjust the organizations that have access to this policy

Change the Remediation Workflow

To change the workflow assigned to a policy, you can select an alternative workflow from the list of options. By default, no workflow is assigned to an audit policy.

Note – If no workflow is assigned to the Audit Policy, the violations will not be assigned to any remediators.

Select a remediation workflow from the list, and then click Save.

Select Remediation User Form Rule

Optionally select a rule to calculate the user form applied when editing a user through a remediation.

Assign or Remove Visibility to Organizations

Adjust the organizations to which this audit policy will be available, and then click Save.

Sample Policies

Waveset provides these sample policies, accessible from the Audit Policies list:

- IDM Role Comparison Policy
- IDM Account Accumulation Policy

IDM Role Comparison Policy

This sample policy allows you to compare a user's current access to the access specified by Waveset roles. The policy ensures that all resource attributes specified by roles are set for the user.

This policy fails if:

- The user is missing any resource attributes specified by roles
- The user's resource attributes differ from those specified by roles

IDM Account Accumulation Policy

This sample policy verifies that all accounts held by the user are referenced by at least one role also held by that user.

This policy fails if the user has accounts on any resources that are not explicitly referenced by a role assigned to the user.

Deleting an Audit Policy

When an audit policy is deleted from Waveset, all violations that reference the policy are also deleted.

Policies can be deleted from the Compliance area of the interface, when you click Manage Policies to view policies. To delete an audit policy, select the policy name in the policy view, and then click Delete.

Troubleshooting Audit Policies

Problems with your audit policy typically are best addressed through policy rule debugging.

To debug a rule, add the following trace elements to the rule code.

```
<block trace='true'>
<and>
    <contains>
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
        <s>Smith</s>
    </contains>
</and>
</block>
```

- If you cannot see your workflow in the Waveset interface, confirm that
  - You have added the `subtype=’SUBTYPE_REMEDIATION_WORKFLOW’` attribute to your workflow. Workflows without this subtype are not visible in the Waveset Administrator interface.
  - You have the capability for authType `AuditorAdminTask`.
  - You control the organization containing the workflow.
- If you imported rules, but do not see them in the Audit Policy Wizard, confirm that
  - Each rule is of `subtype=”SUBTYPE_AUDIT_POLICY_RULE’` or `subtype=”SUBTYPE_AUDIT_POLICY_SOD_RULE’`.
  - You have the capability for authType `AuditPolicyRule`.
  - You control the organization containing the workflow.

Assigning Audit Policies

To assign an audit policy to an organization, the user must have (at least) the Assign Organization Audit Policies capability. To assign an audit policy to a user, the user must have the Assign User Audit Policies capability. A user with the Assign Audit Policies capability has both of these capabilities.

To assign organization-level policy, select the Organization on the Accounts tab, and then select the policies in the Assigned audit policies list.

▼ To Assign a User-Level Policy

1. **Click the user in the Accounts area.**

2. **Select Compliance in the user form.**

3. **Select policies in the Assigned audit policies list.**

Note – Audit policies that are directly assigned to a user (assigned through a user account or an organization assignment) are always reevaluated when a violation for that user is remediated.

Resolving Auditor Capabilities Limitations

By default, capabilities needed to perform auditing tasks are contained in the Top organization (object group). As a result, only those administrators who control Top can assign these capabilities to other administrators.

You can resolve this limitation by adding the capabilities to another organization. Waveset provides two utilities, located in the `sample/scripts` directory, to assist with this task.

▼ To Add Capabilities

To add the capabilities needed to perform auditing tasks to an organization other than Top, follow these steps:

1. **Run the following command to list all capabilities (AdminGroups) and their associated organizations (object groups):**

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
   ```

   This command captures the output to a comma-separated value (CSV) file.

2. **Edit the CSV file to adjust the capabilities organizational locations as desired.**

3. **Run this command to update Waveset.**

   ```
   beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
   ```

CHAPTER 15

Auditing: Monitoring Compliance

This chapter describes how to conduct audit reviews and implement practices that help you manage compliance with federally mandated regulations.

In this chapter, you will learn about the following concepts and tasks:

- "Audit Policy Scans and Reports" on page 427
- "Compliance Violation Remediation and Mitigation" on page 433
- "Periodic Access Reviews and Attestation" on page 442
- "Access Review Remediation" on page 460

Audit Policy Scans and Reports

This section provides information about audit policy scans, and provides procedures for running and managing audit scans.

Scanning Users and Organizations

A scan runs selected audit policies on individual users or organizations. You might want to scan a user or organization for a specific violation or execute policies not assigned to the user or organization. Launch scans from the Accounts area of the interface.

Note – You can also launch or schedule an audit policy scan from the Server Tasks tab.

▼ To Scan a User Account or Organization

1. **In the Administrator interface, select Accounts from the main menu.**

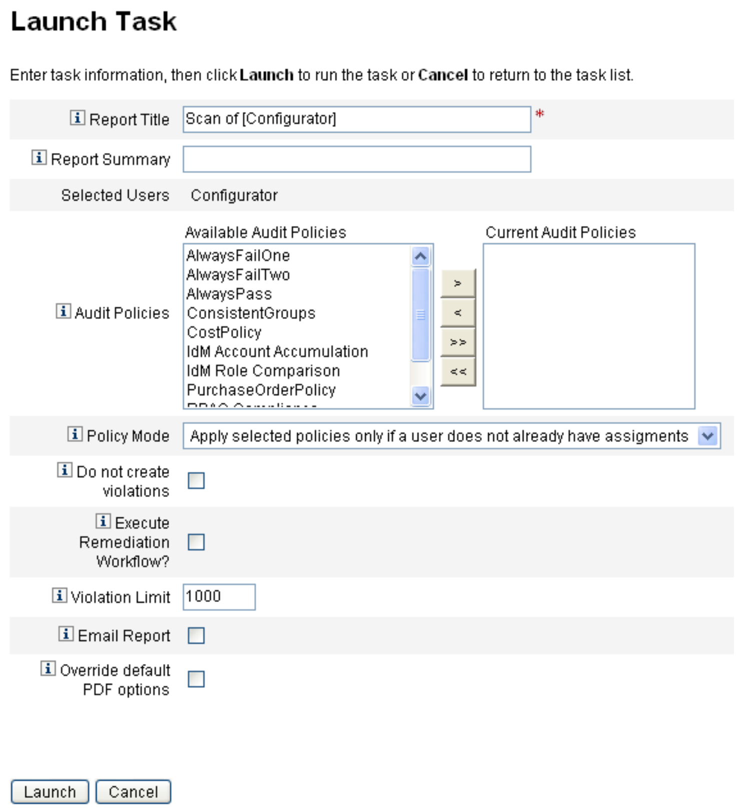
2. **In the Accounts list, perform one of these actions:**

   a. **Select one or more users, and then select Scan from the User Actions options list.**

   b. **Select one or more organizations and then select Scan from the Organization Actions options list.**

   The Launch Task dialog displays. Figure 15–1 is an example of the Launch Task page for an audit policy user scan.

FIGURE 15–1 Launch Task Dialog



Launch Task

Enter task information, then click **Launch** to run the task or **Cancel** to return to the task list.

Report Title: Scan of [Configurator] *

Report Summary:

Selected Users: Configurator

Audit Policies: Available Audit Policies / Current Audit Policies

Policy Mode: Apply selected policies only if a user does not already have assigments

Do not create violations: □

Execute Remediation Workflow?: □

Violation Limit: 1000

Email Report: □

Override default PDF options: □

3. **Enter a title for the scan in the Report Title field.** (*required*)

4 **Specify the remaining options.**

These options include:

- **Report Summary**: Enter a description for the scan.
- **Add Policies**: Select one or more audit policies to run. You must specify at least one policy.
- **Policy Mode**: Select a policy mode, which determines how the selected policies interact with users who already have policy assignments. Assignments can come directly from the user or from the organization to which the user is assigned.
- **Do not create violations**: Enable this box if you want audit policies evaluated and violations reported, but do not want compliance violations to be created or updated, and do not want remediation workflows to be executed. Task results from the scan do show which violations would have been created, making this option useful when testing audit policies.
- **Execute Remediation Workflow?**: Enable this box to run the remediation workflow assigned in the audit policy. If the audit policy does not define a remediation workflow, no remediation workflow will run.
- **Violation Limit**: Edit this box to set the maximum number of compliance violations that can be emitted by the scan before it aborts. This value is a safeguard to limit risk when running an audit policy that may be overly aggressive in its checks. An empty value means no limit is set.
- **Email Report**: Enable this box to specify recipients for the report. You might also have Waveset attach a file containing a report in CSV (comma-separated values) format.
- **Override default PDF options**: Enable this box to override the default PDF options.

5 **Click Launch to begin the scan.**

To view the reports resulting from an audit scan, view the Auditor Reports.

Working with Auditor Reports

Waveset provides a number of Auditor Reports. The following table describes these reports.

TABLE 15–1 Auditor Reports Descriptions

Auditor Report Type	Description
Access Review Coverage	Shows the overlap or differences among the users that are implied by the selected access reviews. Because most access reviews have a user scope that is specified by a query or some membership operation, the exact set of users is expected to change over time. This report can show the overlap, differences, or both, between users specified by two different access reviews (to see if the reviews are going to be efficient in operation); between entitlements generated by two different access reviews (so you can see if the coverage changes over time); or between users and entitlements (so you can see if the entitlements were generated for all users scoped by the review.
Access Review Detail	Shows the current status of all user entitlement records. This report can be filtered by a user's organization, Access Review and Access Review Instance, state of an entitlement record, and attestor.
Access Review Summary	Provides summary information about all access reviews. It summarizes the status of users scanned, policies scanned, and attestation activities for each access review scan listed.
Access Scan User Scope Coverage	Compares selected scans to determine which users are included in the scan scope. It shows the overlap (users included in all scans) or difference (users not included in all scans, but included in more than one). This report is useful when trying to organize multiple access scans to cover the same or different users, depending on the needs of the scan.
Audit Policy Summary	Summarizes the key elements of all audit policies, including the rules, remediators, and workflow for each policy.
Audited Attribute	Shows all audit records indicating a change of a specified resource account attribute. This report mines the audit data for any auditable attributes that have been stored. It will mine the data based on any extended attributes, which can be specified from WorkflowServices or resource attributes marked as auditable. For information on configuring this report, see "Configuring the Audited Attribute Report" on page 432.
Audit Policy Violation History	Graphical view of all compliance violations per policy that were created during a specified period of time. This report can be filtered by policy, and grouped by day, week, month, or quarter.
User Access	Shows the audit record and user attributes for a specified user.
Organization Violation History	Graphical view of all compliance violations per resource, that were created during a specific period of time. Can be filtered by organization, and grouped by day, week, month, or Quarter.
Resource Violation History	Graphical view of all compliance violations per resource that were created during the specified time range.

TABLE 15–1 Auditor Reports Descriptions *(Continued)*

Auditor Report Type	Description
Separation of Duties	Shows separation of duties violations arranged in a conflicts table. Using a Web-based interface, you can access additional information by clicking the links. This report can be filtered by organization, and grouped by day, week, month, or quarter.
Violation Summary	Shows all current compliance violations. This report can be filtered by remediator, resource, rule, user, or policy

The reports are available from the Reports tab in the Waveset interface.

Note – The `RULE_EVAL_COUNT` value equals the number of rules that were evaluated during a policy scan. This value is sometimes included in reports.

Waveset calculates the `RULE_EVAL_COUNT` value as follows:

```
# of users scanned x (# of rules in policy + 1)
```

The +1 is included in the calculation because Waveset also counts the *policy rule*, which is the rule that actually decides if a policy is violated. The policy rule inspects the audit rule results, and performs the boolean logic to come up with a policy result.

For example, if you have Policy A with three rules and Policy B with two rules, and you scanned ten users, the `RULE_EVAL_COUNT` value equals 70 because

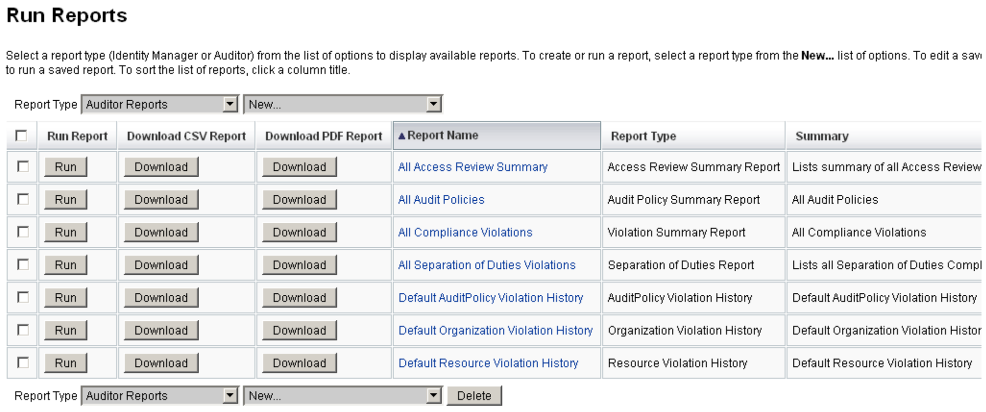
```
10 users x (3 + 1 + 2 + 1 rules)
```

Creating an Auditor Report

To run a report, you must first create the report template. You can specify various criteria for the report, including specifying email recipients to receive the report results. After a report template has been created and saved, it is available from the Run Reports page.

The following figure shows an example of the Run Reports page with a list of defined Auditor Reports.

FIGURE 15–2 Run Reports Page Selections



Run Reports

Select a report type (Identity Manager or Auditor) from the list of options to display available reports. To create or run a report, select a report type from the **New...** list of options. To edit a sav
to run a saved report. To sort the list of reports, click a column title.

Report Type Auditor Reports New...

□	Run Report	Download CSV Report	Download PDF Report	▲Report Name	Report Type	Summary
□	Run	Download	Download	All Access Review Summary	Access Review Summary Report	Lists summary of all Access Review
□	Run	Download	Download	All Audit Policies	Audit Policy Summary Report	All Audit Policies
□	Run	Download	Download	All Compliance Violations	Violation Summary Report	All Compliance Violations
□	Run	Download	Download	All Separation of Duties Violations	Separation of Duties Report	Lists all Separation of Duties Compl
□	Run	Download	Download	Default AuditPolicy Violation History	AuditPolicy Violation History	Default AuditPolicy Violation History
□	Run	Download	Download	Default Organization Violation History	Organization Violation History	Default Organization Violation Histor
□	Run	Download	Download	Default Resource Violation History	Resource Violation History	Default Resource Violation History

Report Type Auditor Reports New... Delete

To Create an Auditor Report

1. **In the Administrator interface, click Reports in the main menu.**

   The Run Reports page opens.

2. **Select Auditor Reports for the report type.**

3. **In the New list of reports, select a report.**

   The Define a Report page appears. The fields and layout of the report dialog varies for each type of report. Refer to Waveset Help for information about specifying the report criteria.

   After entering and selecting report criteria, you can:

   - Run the report without saving.

     Click Run to start running the report. Waveset 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. After it is saved, you can run the report from the Run Reports page (the list of reports). After running a report from the Run Reports page, you can view the output immediately or at a later time from the View Reports tab.

   For information about scheduling a report, see "Scheduling Reports" on page 253.

Configuring the Audited Attribute Report

The Audited Attribute Report (see Table 15–1) can report attribute-level changes to Waveset users and accounts. Standard audit logging, however, does not generate enough audit log data to support a full query expression.

Standard audit logging *does* write the changed attributes to the acctAttrChanges field in the audit log, but the changed attributes are written in a way that the report query can only match records based on the changed attribute's name. The report query cannot accurately match the attribute's value.

You can configure this report to match records containing changes to the attribute lastname, by specifying the following parameters:

```
Attribute Name = 'acctAttrChanges'
Condition = 'contains'
Value = 'lastname'
```

Note – Using Condition='contains' is necessary because of the way data is stored in the acctAttrChanges field. This field is not multi-valued. Essentially, it is a data structure that contains the before/after values of all changed attributes in the form attrname=value. Consequently, the preceding settings allow the report query to match any instances of lastname=*xxx*.

It is also possible to capture only those audit records that have a specific attribute with a specific value. To do this, follow the procedure in the "Configuring the Audit Tab" on page 300 section. Select the Audit entire workflow checkbox, click the Add Attribute button to select the attributes you want to record for reporting purposes, and click Save.

Next, enable the task template configuration (if it is not already enabled). To do this, follow the procedure in the "Enabling the Task Templates" on page 275 section. Do not change the default value in the Selected Process Types list, just click Save.

The workflow can now provide audit records that are suitable for matching both the attribute name and the value. Although turning on this level of auditing provides much more information, be aware that there is a significant performance cost and your workflows will run slower.

Compliance Violation Remediation and Mitigation

This section describes how to use Waveset Remediation to protect your critical assets.

The following topics discuss elements of the Waveset Remediation process:

- "About Remediation" on page 434
- "Remediation Email Template" on page 436
- "Working with the Remediations Page" on page 436
- "Viewing Policy Violations" on page 436
- "Prioritizing Policy Violations" on page 438
- "Mitigating Policy Violations" on page 439

About Remediation

When Waveset detects an unresolved (not mitigated) audit policy compliance violation, it creates a remediation request, which must be addressed by a *remediator* A remediator is a designated user who is allowed to evaluate and respond to audit policy violations.

Remediator Escalation

Waveset allows you to define three levels of remediator escalation. Remediation requests are initially sent to Level 1 remediators. If a Level 1 remediator does not act on a remediation request before the timeout period expires, Waveset escalates the violation to the Level 2 remediators and begins a new timeout period. If a Level 2 remediator does not respond before the timeout period expires, then the request is escalated once again to the Level 3 remediator.

To perform remediation, you must designate at least one remediator for your enterprise. Specifying more than one remediator for each level is optional, but recommended. Multiple remediators help ensure workflow is not delayed or halted.

These authorization options are for work items of authType `RemediationWorkItem`.

- The remediation work item owner
- A direct or indirect manager of the remediation work item owner
- An administrator who controls an organization in which the remediation work item owner belongs

By default, the behavior for authorization checks is one of the following:

- Owner is the user attempting the action
- Owner is in an organization controlled by the user attempting the action
- Owner is a subordinate of the user attempting the action

The second and third checks are independently configurable by modifying these options:

- **controlOrg**. Valid values are true or false.
- **subordinate**. Valid values are true or false.
- **lastLevel**. The last subordinate level to include in the result; -1 means all levels. The integer value for lastLevel defaults to -1, meaning direct and indirect subordinates.

These options can be added or modified in the following:

```
UserForm: Remediation List
```

Remediation Workflow Process

Waveset provides the Standard Remediation Workflow to provide remediation processing for Audit Policy scans.

The Standard Remediation Workflow generates a remediation request (a review-type work item) containing information about the compliance violation and sends an email notification to each Level 1 remediator named in the audit policy. When a remediator mitigates the violation, the workflow changes the state of, and assigns an expiration to, the existing compliance violation object.

A compliance violation is uniquely identified by the combination of the user, policy name, and rule name. When an audit policy evaluates to true, a new compliance violation is created for each user/policy/rule combination, if an existing violation for this combination does not already exist. If a violation does exist for the combination, and the violation is in a mitigated state, then the workflow process takes no action. If the existing violation is not mitigated, then its recurrent count is incremented.

For more information about remediation workflows, see "About Audit Policies" on page 407.

Remediation Responses

By default, three response options are given to each remediator:

- **Remediate**. A remediator indicates that something has been done to fix the problem on the resource.

  When a compliance violation is modified, Waveset creates an audit event to log the remediation. In addition, Waveset stores the name of the remediator and any comments provided.

  Note – After remediation, a violation is not deleted until the next audit scan. If an audit policy is configured to allow re-scans, then the user will be re-scanned as soon as the violation is remediated.

- **Mitigate**. A remediator allows the violation and gives the user an exemption from the violation for a certain amount of time.

  If the violation is deliberate (for example, there is a business case for belonging to two groups), you can mitigate the violation for an extended period of time. You can also mitigate the violation for a short period of time (for example, in cases where the resource's system administrator is on vacation and you do not know how to fix the problem).

  Waveset stores the name of the remediator that mitigated the violation along with the expiration date assigned to the exemption and any comments provided.

Note – When Waveset detects an expired exemption, it returns the violation from the mitigated state to a pending state.

- **Forward**. A remediator reassigns the responsibility for resolving the violation to another individual.

As an example of remediation, suppose your enterprise establishes a rule in which a user cannot be responsible for both Accounts Payable and Accounts Receivable, and you receive notice that a user is violating this rule.

- If the user is a supervisor who has responsibility for both roles until the company hires a second person for that position, you might mitigate the violation and issue an exemption for up to six months.
- If the user is violating the rule, you might ask your Oracle ERP Administrator to correct the conflict, and then remediate the violation when the problem is fixed for that resource. Alternatively, you might forward the remediation request to the Oracle ERP Administrator.

Remediation Email Template

Waveset provides a Policy Violation Notice email template (available by selecting the Configuration tab, then the Email Templates subtab. You can configure this template to notify remediators of pending violations. For more information, see "Customizing Email Templates" on page 98 in Chapter 4, "Configuring Business Administration Objects."

Working with the Remediations Page

Select Work Items → Remediations to access the Remediations page.

You can use this page to:

- View pending violations
- Prioritize policy violations
- Mitigate one or more policy violations
- Remediate one or more policy violations
- Forward one or more violations
- Edit users from a remediation work item

Viewing Policy Violations

You can use the Remediations page to view details about violations before taking action on them.

Depending on your capabilities or place in the Waveset capabilities hierarchy, you may be able to view and take action on violations for other remediators.

The following topics are related to viewing violations:

- "Viewing Pending Requests" on page 437
- "Viewing Completed Requests" on page 437
- "Updating the Table" on page 438

Viewing Pending Requests

Pending requests assigned to you are, by default, displayed in the Remediation table.

You can use the List Remediations for option to view pending remediation requests for a different remediator:

- Select My Direct Reports to view pending requests for users in your organization who report directly to you.
- Select Search Users to enter or locate one or more users whose pending requests you want to view. Enter a user ID, and then click Apply to view pending requests for that user. Alternatively, click **...** (More) to search for a user. After locating and selecting a user, click Dismiss to close the Search area.

The resulting table provides the following information about each request:

- **Remediator**. Name of the assigned remediator. This column displays only when you view remediation requests for other remediators.
- **User**. User for whom the request is made.
- **Audit Policy/Request**. Action requested of the remediator.
- **Audit Rule/Description**. Remediation comments for the request.
- **Violation State**. Current state of the violation.
- **Severity**. Severity assigned to the request (None, Low, Medium, High, or Critical).
- **Priority**. Priority assigned to the request (None, Low, Medium, High, or Urgent).
- **Date of Request**: Date and time the remediation request was issued.

Note – Each user can choose a custom form that displays remediation data relevant to that particular remediator. To assign a custom form, select the Compliance tab on the user form.

Viewing Completed Requests

To view your completed remediation requests, click the My Work Items tab, and then click the History tab. A list of previously remediated work items displays.

The resulting table (which is generated by an `AuditLog` report) provides the following information about each remediation request:

- **Timestamp**. Date and time the request was remediated
- **Subject**. Name of the remediator who processed the request
- **Action**. Whether the remediator mitigated or remediated the request
- **Type**. `ComplianceViolation` or `User Entitlement`
- **Object Name**. Name of the audit policy that was violated
- **Resource**. Provides the remediator's account ID (or may indicate N/A)
- **ID**. Account ID related to the policy violation
- **Result**. Always indicates `Success`

Clicking a timestamp in the table opens an Audit Events Details page.

The Audit Events Details page provides information about the completed request, including information about the remediation or mitigation, event parameters (if applicable), and auditable attributes.

Updating the Table

To update the information provided in the Remediations table, click Refresh. The Remediation page updates the table with any new remediation requests.

Prioritizing Policy Violations

You can prioritize policy violations by assigning them a priority, severity, or both. Prioritize violations from the Remediations page.

▼ To Edit the Priority or Severity for Violations

1. **Select one or more violations in the list.**
2. **Click Prioritize.**

   The Prioritize Policy Violations page appears.
3. **Optionally set a severity for the violation. Selections are None, Low, Medium, High, or Critical.**
4. **Optionally set a priority for the violation. Selections are None, Low, Medium, High, or Urgent.**
5. **Click OK when you have finished making selections. Waveset returns to the list of remediations.**

Note – Severity and priority values can be set only on remediations of type CV (Compliance Violation).

Mitigating Policy Violations

You can mitigate policy violations from the Remediations page.

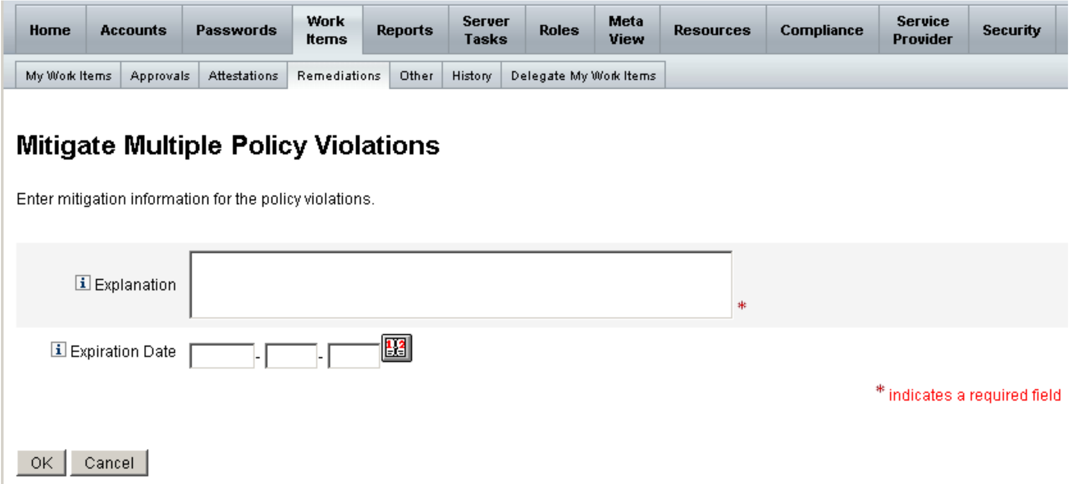
To mitigate pending policy violations from the Remediations page:

1. Select rows in the table to specify which requests to mitigate.
   - Enable one or more individual options to specify requests to be mitigated.
   - Enable the option in the table header to mitigate all requests listed in the table.

   Waveset allows you to enter only one set of comments to describe a mitigation action. You may not want to perform a bulk mitigation unless the violations are related and a single comment will suffice.

   You can mitigate only those requests that include compliance violations. Other remediation requests cannot be mitigated.
2. Click Mitigate.

   The Mitigate Policy Violation page (or Mitigate Multiple Policy Violations page) appears.



Mitigate Multiple Policy Violations

Enter mitigation information for the policy violations.

Explanation *

Expiration Date - -

* indicates a required field

3. Enter comments about the mitigation into the Explanation field. (*required*)

Your comments provide an audit trail for this action, so be sure to enter complete and meaningful information. For example, explain why you are mitigating the policy violation, the date, and why you chose the exemption period.

4. Provide an expiration date for the exemption by typing the date (in the format **`YYYY-MM-DD`**) directly into the Expiration Date field, or by clicking the date button and selecting a date from the calendar.

   Note – If you do not provide a date, the exemption is valid indefinitely.

   ---

5. Click OK to save your changes and return to the Remediations page.

Remediating Policy Violations

▼ To Remediate One or More Policy Violations

1 **Use the check boxes in the table to specify which requests to remediate.**

- Enable one or more individual check boxes in the table to specify requests to remediate.
- Enable the check box in the table header to remediate all requests listed in the table.

  If selecting more than one request, keep in mind that Waveset allows you to enter only one set of comments to describe a remediation action. You may not want to perform a bulk remediation unless the violations are related and a single comment will suffice.

2 **Click Remediate.**

3 **The Remediate Policy Violation page (or Remediate Multiple Policy Violations page) displays.**

4 **Enter your comments about the remediation into the Comments field.**

5 **Click OK to save your changes and return to the Remediations page.**

Note – Audit policies that are directly assigned to a user (who is assigned through a user account or an organization assignment) are always re-evaluated when a violation for that user is remediated.

Forwarding Remediation Requests

You can forward one or more remediation requests to another remediator.

▼ To Forward Remediation Requests

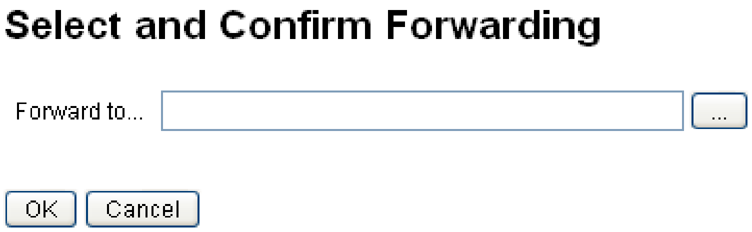
1 Use the check boxes in the table to specify which requests to forward.

- Enable the check box in the table header to forward all requests listed in the table.
- Enable individual check boxes in the table to forward one or more requests.

2 Click Forward.

The Select and Confirm Forwarding page appears.

FIGURE 15–3 Select and Confirm Forwarding Page



Select and Confirm Forwarding

Forward to... [ ] [...]

[OK] [Cancel]

3 Enter a remediator name in the Forward to field, and then click OK. Alternatively, you can click . . . (More) to search for a remediator name. Select a name from the search list, and then click Set to enter that name in the Forward to field. Click Dismiss to close the search area.

When the Remediations page reappears, the new remediator's name displays in the Remediator column of the table.

Editing a User from a Remediation Work Item

From a remediation work item, you can (with appropriate user editing capabilities) edit a user to remediate problems (as described in the associated entitlement history).

To edit a user, perform the following steps:

1. Click Edit User from the Review Remediation Request page.

   The displayed Edit User page shows:

   - Entitlement history associated with the user, for this work item
   - Attributes for the user

     The options that appear here are the same as on the Edit User form available from the Accounts area.
2. After making changes to the user, click Save.

Note – Saving user edits causes the Update User workflow to run. Because this workflow may have approvals, it is possible that the changes to the user accounts are not in effect for a period of time after the save. If the audit policy allows re-scans, and the Update User workflow has not completed, then the subsequent policy scan may detect the same violation.

Periodic Access Reviews and Attestation

Waveset provides a process for conducting access reviews that enable managers or other responsible parties to review and verify user access privileges. This process helps to identify and manage user privilege accumulation over time, and helps to maintain compliance with Sarbanes-Oxley, GLBA, and other federally regulated mandates.

Access reviews can be performed as needed or scheduled to occur periodically. such as every calendar quarter, enabling you to conduct periodic access reviews to maintain the correct level of user privileges. An access review can optionally include audit policy scans.

About Periodic Access Reviews

Periodic access review is the periodic process of attesting that a set of employees has the appropriate privileges on the appropriate resources at a specific point in time.

A periodic access review involves the following activities:

- **Access review scans**. Scans that perform rule-based evaluations of *user entitlements* to determine if attestation is needed.
- **Attestation**. Process of responding to attestation requests by approving or rejecting user entitlements.

A *user entitlement* is a detailed record of a user's accounts on a specific set of resources.

Access Review Scans

To initiate a periodic access review, you must first define at least one access scan.

The access scan defines who will be scanned, which resources will be included in the scan, any optional audit policies to be evaluated during the scan, and rules to determine which entitlement records will be manually attested, and by whom.

Access Review Workflow Process

In general, the Waveset access review workflow:

- Constructs a list of users, gets account information for each user, and evaluates optional audit policies
- Creates user entitlement records
- Determines if attestation is required for each user entitlement record
- Assigns work items to each attestor
- Waits for all attestors to approve, or for the first rejection
- Escalates to the next attestor, if no response to a request is received within a specified timeout period
- Updates user entitlement records with resolutions

See "Access Review Remediation" on page 460 for a description of the remediation capabilities.

Required Administrator Capabilities

To conduct a periodic access review and manage the review processes, a user must have the Auditor Periodic Access Review Administrator capability. A user with Auditor Access Scan Administrator capability can create and manage access scans.

To assign these capabilities, edit the user account and modify the security attributes. For more information about these and other capabilities, see "Understanding and Managing Capabilities" on page 198 in Chapter 6, "Administration."

Attestation Process

Attestation is the certification process performed by one or more designated attestors to confirm a user entitlement as it exists on a specific date. During an access review, the attestor (or attestors) receives notice of the access review attestation requests through email notification. An attestor must be an Waveset user, but is not required to be an Waveset administrator.

Attestation Workflow

Waveset uses an attestation workflow that is launched when an access scan identifies entitlement records requiring review. The access scan makes this determination based on the rules defined in the access scan.

A rule evaluated by the access scan determines if the user entitlement record needs to be manually attested, or if it can be automatically approved or rejected. If the user entitlement record needs to be manually attested, then the access scan uses a second rule to determine who the appropriate attestors are.

Each user entitlement record to be manually attested is assigned to a workflow, with one work item per attestor. Notification to the attestor of these work items can be sent using a ScanNotification workflow that bundles the items into one notification, per attestor, per scan. Unless the ScanNotification workflow is selected, notification will be per user entitlement. This means an attestor could receive multiple notifications per scan, and possibly a large number depending on the number of users scanned.

Attestation Security Access

These authorization options are for work items of authType `AttestationWorkItem`:

- The Work Item owner
- A direct or indirect manager of the Work Item owner
- An administrator who controls an organization in which the Work Item owner belongs
- Users who have been validated through authentication checks

By default, the behavior for authorization checks is *one* of the following:

- Owner is User attempting the action
- Owner is in Organization controlled by user attempting the action
- Owner is a subordinate of user attempting the action

The second and third checks are independently configurable by modifying these form properties:

- `controlOrg` — Valid values are true or false
- `subordinate` — Valid values are true or false
- `lastLevel` — Last subordinate level to include in the result; `-1` means all levels

The integer value for `lastLevel` defaults to `-1`, meaning direct and indirect subordinates.

You can add or modify these options in the following:

`UserForm: AccessApprovalList.`

Note – If you set security on attestations to organization-controlled, then the Auditor Attestor capability is also required to modify another user's attestations.

Delegated Attestation

By default, the access scan workflow respects delegations, for work items of type Access Review Attestation and Access Review Remediation, created by users for attestation work items and notifications. The access scan administrator may deselect the Follow Delegation option to ignore delegation settings. If an attestor has delegated all work items to another user but the

Follow Delegation option is not set for an access review scan, then the attestor, *not* the user to which delegations have been assigned, will receive attestation request notifications and work items.

Planning for a Periodic Access Review

An access review can be a labor- and time-intensive process for any business enterprise. The Waveset periodic access review process helps minimize the cost and time involved by automating many parts of the process. However, some of the processes still are time-consuming. For example, the process of fetching user account data from a number of locations for thousands of users can take a considerable amount of time. The act of manually attesting records can be time-consuming as well. Proper planning improves the efficiency of the process and greatly reduces the effort involved.

Planning for a periodic access review involves the following considerations:

- Scan times can vary greatly depending on the number of users and the resources involved.

  A single periodic access review for a large organization can take one or more days for scanning, as well as one or more weeks for manual attestation to complete.

  For example, for an organization with 50,000 users and ten resources, an access scan might take approximately one day to complete, based on the following calculation:

  1 sec/resource * 50K users * 10 resources / 5 concurrent threads = 28 hours

  If resources are spread across geographies, network latencies can add to the process time.
- Using multiple Waveset servers for parallel processing can speed up the access review process.

  Running parallel scans is most effective when the resources are not common across the scans. When defining an access review, create multiple scans and restrict resources to a specific set of resources, using different resources for each scan. Then when you launch the task, select multiple scans and schedule them to run immediately.
- Customizing the Attestation workflow and rules gives you greater control and can provide greater efficiency:

  For example, customize the Attestor rule to spread attestation duties across multiple attestors. The attestation process assigns work items and sends out notifications accordingly.
- Using Attestor Escalation Rules helps improve response time for attestation requests.

  Set the Default Escalation Attestor rule, or use a customized rule, to set up an escalation chain of attestors. Also specify escalation timeout values.
- Understand how to use the Review Determination Rules to save time by automatically determining which entitlement records need to be manually reviewed.
- Bundle notification of attestation requests for a scan by specifying a scan-level Notification Workflow.

Tuning Scan Tasks

During the scan process, multiple threads access the user's view, potentially accessing resources on which the user has accounts. After the view is accessed, multiple audit policies and rules are evaluated, which may result in the creation of compliance violations.

To prevent two threads from updating the same user view at the same time, the process establishes an in-memory lock on the user name. If this lock cannot be established in (by default) 5 seconds, then an error is written to the scan task and the user is skipped, thus providing protection for concurrent scans that are processing the same set of users.

You can edit the values of several "tunable parameters" that are provided as task arguments to the scan task:

- `clearUserLocks` (Boolean). If true, then all current user locks are freed before the scan starts.
- `userLock` (integer). Time (in milliseconds) to wait when trying to lock a user. The default value is 5 seconds. A negative value disables locking for that scan.
- `scanDelay` (integer). Time (in milliseconds) to sleep between dispatching scan threads. The default value is 0 (no delay). If you provide a value for this argument, then the scan is slower, but the system is more responsive to other operations.
- `maxThreads` (integer). Number of concurrent threads used to process a scan. The default value is 5. If resources are very slow to respond, increasing this number may increase scan throughput.

To change the values of these parameters, edit the corresponding Task Definition form. For more information, see Chapter 2, "Waveset Forms," in *Oracle Waveset 8.1.1 Deployment Reference*.

Creating an Access Scan

To define an access review scan, perform the following steps:

1. Select Compliance → Manage Access Scans.
2. Click New to display the Create New Access Scan page.
3. Assign a name to the access scan and add a description that is meaningful in identifying the scan (*optional*).

Note – Access scan names must not contain these characters:

apostrophe (`'`), period (`.`), pipe (`|`), left bracket (`[`), right bracket (`]`), comma (`,`), colon (`:`), dollar sign (`$`), double quote (`"`), backslash (`\`), or equals sign (`=`)

Also, avoid using these characters: underscore (`_`), percent-sign (`%`), caret (`^`), and asterisk (`*`).

---

4. Enable the Dynamic entitlements option to give attestors additional options.

   These options include:

   - A pending attestation can be immediately re-scanned to refresh the entitlement data and reevaluate the need for attestation.
   - A pending attestation can be routed to another user for remediation. Following remediation, the entitlement data is refreshed and reevaluated to determine the need for attestation.
5. Specify the User Scope Type (*Required*).

   Choose from the following options:

   - **According to attribute condition rule**. Scan users according to a selected User Scope Rule.

     Waveset provides these default rules:

     - All Administrators

       Note – You can add user scoping rules by using the Identity Manager IDE. For information about the Identity Manager IDE, go to `https://identitymanageride.dev.java.net/`.

     - All My Reports
     - All Non-Administrators
     - My Direct Reports
     - Users without a Manager
   - **Assigned to resources**. Scan all users that have an account on one or more selected resources. When you choose this option, the page displays the User Scope Resources, which lets you specify resources.
   - **According to a specific role**. Scan all members who have at least one role, or who have all the roles, that you specify.

- **Members of Organizations**. Choose this option to scan all members of one or more selected organizations.
- **Reports to managers**. Scan all users reporting to selected managers. Manager hierarchy is determined by the Waveset attribute of the user's Lighthouse account.

  If the user scope is *organization* or *manager*, then the Recursive Scope option is available. This option allows for user selection to occur recursively through the chain of controlled members.

6. If you also want to scan audit policies to detect violations during the access review scan, select the audit policies to apply to this scan by moving your selections from Available Audit Policies to the Current Audit Policies list.

   Adding audit policies to an access scan results in the same behavior as performing an audit scan over the same set of users. However, in addition, any violations detected by the audit policies are stored in the user entitlement record. This information can make automatic approval or rejection easier, because the rule can use the presence or absence of violations in the user entitlement record as part of its logic.
7. If you scanned audit policies in the preceding step, you can use the Policy mode option to specify how the access scan determines which audit policies to execute for a given user. A user can have policies assigned both at the user level and/or at the organization level. The default access scan behavior is to apply the policies specified for the access scan only if the user does not already have any assigned policies.
   a. Apply select policies and ignore other assignments
   b. Apply selected policies only if user does not already have assignments
   c. Apply selected policies in addition to user assignments
8. (*Optional*) Use the Specify the Review Process Owner option to specify an owner of the access review task being defined. If a Review Process Owner is specified, then an attestor who encounters a potential conflict in responding to an attestation request can *abstain* in lieu of approving or rejecting a user entitlement and the attestation request is forwarded to the Review Process Owner. Click the selection (ellipsis) box to search the user accounts and make your selection.
9. Select the Follow delegation option to enable delegation for the access scan. The access scan will only honor delegation settings if this option is checked. Follow Delegation is enabled by default.
10. Select the Restrict target resources option to restrict scanning to targeted resources.

    This setting has a direct bearing on the efficiency of the access scan. If target resources are not restricted, each user entitlement record will include account information for every resource the user is linked to. This means that during the scan every assigned resource is queried for each user. By using this option to specify a subset of the resources, you can greatly reduce the processing time required for Waveset to create user entitlement records.
11. Generally, do not enable the Execute Violation Remediation option except for advanced cases.

When enabled and a violation is detected for any of the assigned audit policies, Waveset executes the respective audit policy's remediation workflow.

12. Select the Access Approval Workflow and specify the default Standard Attestation workflow or select a customized workflow if available.

    This workflow is used to present the user entitlement record for review to the appropriate attestors (as determined by the attestor rule). The default Standard Attestation Workflow creates one work item for each attestor. If the access scan specifies escalation, this workflow is responsible for escalating work items that have been dormant too long. If no workflow is specified, the user attestation will remain in the pending state indefinitely.

    Note – For more information about the Identity Auditor rules mentioned in this step and the following steps, see Chapter 4, "Working with Rules," in *Oracle Waveset 8.1.1 Deployment Reference*.

    ---

13. Use the Attestor Rule option to specify the Default Attestor rule or to select a customized attestor rule if available.

    The attestor rule is given the user entitlement record as input, and returns a list of attestor names. If Follow Delegation is selected, the access scan transforms the list of names to the appropriate users following the delegation information configured by each user in the original list of names. If an Waveset user's delegation results in a routing cycle, then the delegation information is discarded, and the work item is delivered to the initial attestor. The `Default Attestor` rule indicates that the attestor should be the manager (idmManager) of the user that the entitlement record represents, or the Configurator account if that user's `idmManager` is null. If attestation needs to involve resource owners as well as managers, you must use a custom rule.

14. Use the Attestor Escalation Rule option to specify the Default Escalation Attestor rule, or select a customized rule if available. You can also specify the Escalation Timeout value for the rule. The default escalation timeout value is 0 days.

    This rule specifies the escalation chain for a work item that has passed the Escalation Timeout period. The Default Escalation Attestor rule escalates to the assigned attestor's manager (`idmManager`), or to Configurator if the attestor's `idmManager` value is null.

    You can specify the Escalation Timeout value in minutes, hours, or days.

    The book contains additional information about the Attestor Escalation Rule.

15. Specify a Review Determination Rule. (*Required*)

Select one of the following rules to specify how the scan process will determine the disposition of an entitlement record:

- **Reject Changed Users**. Automatically rejects a user entitlement record if it is different than the last user entitlement from the same access scan definition and the last user entitlement was approved. Otherwise, forces manual attestation and approves all user entitlements that are unchanged from the previously approved user entitlement. By default, only the "accounts" portion of the user view is compared for this rule.
- **Review Changed Users**. Forces manual attestation for any user entitlement record if it is different than the last user entitlement from the same access scan definition and the last user entitlement was approved. Approves all user entitlements that are unchanged from the previously approved user entitlement. By default, only the "accounts" portion of the user view is compared for this rule.
- **Review Everyone**. Forces manual attestation for all user entitlement records.

The Reject Changed Users and Review Changed Users rules compare the user entitlement to the last instance of the same access scan in which the entitlement record was approved.

You can change this behavior by copying and modifying the rules to restrict comparison to any selected part of the user view.

This rule can return the following values:

- **-1**. No attestation required
- **0**. Automatically rejects the attestation
- **1**. Manual attestation required
- **2**. Automatically approves the attestation
- **3**. Automatically remediates the attestation (auto-remediation)

  The book contains additional information about the Review Determination Rule.

16. Select a Remediator Rule to determine who should remediate a specific user's entitlement in the event of Auto-Remediation. The rule can examine the user's current user entitlement and violations, and must return a list of users that should remediate. If no rule is specified, then no remediation will take place. A common use for this rule would be if the entitlement has compliance violations.
17. Select a Remediation User Form Rule that determines an appropriate form for attestation remediators when editing users. Remediators can set their own form, which overrides this one. This form rule would be set if the scan collects very specific data that matches a custom form.
18. Select one of the following Notification Workflow options to specify the notification behavior for each work item.
    - **None** (*Default*). This selection results in an attestor getting an email notification for each individual user entitlement that he must attest.

- **ScanNotification**. This selection bundles attestation requests into a single notification. The notification indicates how many attestation requests were assigned to the recipient.

  If there is a Review Process Owner specified in the access scan, the ScanNotification Workflow will also send a notification to the review process owner when the scan begins, and when it ends. See "Creating an Access Scan" on page 446.

  The ScanNotification workflow uses the following email templates:

  - Access Scan Begin Notice
  - Access Scan End Notice
  - Bulk Attestation Notice

    You can customize the ScanNotification Workflow.

19. Use the Violation limit option to specify the maximum number of compliance violations that can be emitted by this scan before the scan aborts. The default limit is 1000. An empty value field is equal to no limit.

    Although typically during an audit scan or access scan the number of policy violations is small compared to the number of users, setting this value could provide protection from the impact of a defective policy that increases the number of violations significantly. For example, consider the following scenario:

    If an access scan involves 50,000 users and generates two to three violations per user, the cost of remediation for each compliance violation can have a detrimental effect on the Waveset system.

20. Select the Organizations to which this access scan object is available. (*Required*).
21. Click Save to save the scan definition.

Deleting an Access Scan

You can delete one or more access scans. To delete an access scan, from the Compliance tab select Manage Access Scans, select the name of the scan, and then click Delete.

Managing Access Reviews

After defining an access scan, you can use or schedule it as part of an access review. After initiating an access review, several options are available to manage the review process.

Read the following sections for more information about:

- "Launching an Access Review" on page 452
- "Scheduling Access Review Tasks" on page 452
- "Managing Access Review Progress" on page 453
- "Modifying Scan Attributes" on page 454

- “Canceling an Access Review” on page 454
- “Deleting an Access Review” on page 455

Launching an Access Review

To launch an access review from the Administrator interface, use one of these methods:

- Click Launch Review from the Compliance → Access Reviews page.
- Select the Access Review task in the Server Tasks → Run Tasks page.

On the displayed Launch Task page, specify a name for the access review. Select the scans from the Available Access Scans list and move them to the Selected list.

If you select more than one scan, you can choose one of the following launch options:

- **immediately**. This option starts running the scan immediately upon clicking the Launch button. If you select this option for multiple scans in the launch task, then the scans will run in parallel.
- **after waiting**. This option allows you to specify a period of time to wait before launching the scan, relative to the launch of the access review task.

Note – You can initiate more than one scan during an access review session. However, consider that each scan may involve a large number of users, and therefore the scan process can take many hours to complete. Best practice dictates that you manage your scans accordingly. For example, you might launch one scan to run immediately and schedule other scans at staggered intervals.

Click Launch to start the access review process.

Note – The name you assign to an access review is important. Access reviews that run on a periodic basis with the same name can be compared by some reports.

When you launch an access review, the workflow process diagram is displayed, showing the steps in the process.

Scheduling Access Review Tasks

An access review task can be scheduled from the Server Tasks area. For example to set up access reviews on a periodic basis, select Manage Schedule and then define the schedule. You might schedule the task to occur every month or every quarter.

To define the schedule, select the Access Review task on the Schedule Tasks page and then complete the information on the Create task schedule page.

Click Save to save the scheduled task.

Note – Waveset keeps the results from access review tasks for one week, by default. If you choose to schedule a review more often than once a week, set the Results Options to delete. If Results Options are not set to delete, the new review will not run because the previous task results still exist.

Managing Access Review Progress

Use the Access Reviews tab to monitor the progress of an access review. Access this feature through the Compliance tab.

From the Access Reviews tab you can review a summary of all active and previously processed access reviews. The following information is provided for each access review listed:

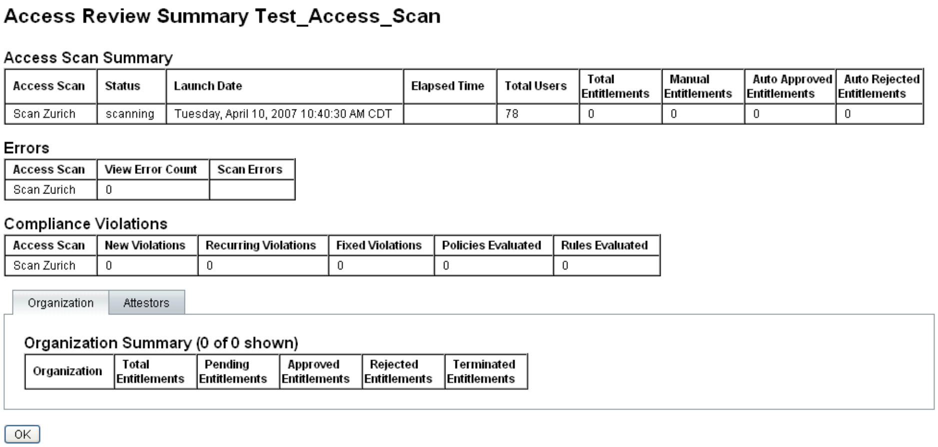
- **Status**. Current status of the review process: initializing, terminating, terminated, number of scans in progress, number of scans scheduled, awaiting attestations, or completed.
- **Launch Date**. The date (timestamp) the access review task started.
- **Total Users**. Total number of users to be scanned.
- **Entitlements details**. Additional columns in the table provide entitlement totals by status. These include details for pending, approved, rejected, terminated, and remediated entitlements, as well as total entitlements.

  The Remediated column indicates the number of entitlements currently in the REMEDIATING state. After an entitlement is remediated, it goes to the PENDING state; therefore, at the conclusion of an access review, the value of this column is zero.

To view more detailed information about the review, select it to open a summary report.

Figure 15–4 shows a sample Access Review Summary report.

FIGURE 15–4 Access Review Summary Report Page



Access Review Summary Test_Access_Scan

Access Scan Summary

Access Scan	Status	Launch Date	Elapsed Time	Total Users	Total Entitlements	Manual Entitlements	Auto Approved Entitlements	Auto Rejected Entitlements
Scan Zurich	scanning	Tuesday, April 10, 2007 10:40:30 AM CDT		78	0	0	0	0

Errors

Access Scan	View Error Count	Scan Errors
Scan Zurich	0	

Compliance Violations

Access Scan	New Violations	Recurring Violations	Fixed Violations	Policies Evaluated	Rules Evaluated
Scan Zurich	0	0	0	0	0

Organization Summary (0 of 0 shown)

Organization	Total Entitlements	Pending Entitlements	Approved Entitlements	Rejected Entitlements	Terminated Entitlements

Click the Organization or Attestors form tab to view scan information categorized by those objects.

You can also review and download this information in a report by running the Access Review Summary Report.

Modifying Scan Attributes

After setting up an access scan, you can edit the scan to specify new options, such as specifying target resources to scan or specifying audit policies to scan for violations while the access scan is running.

To edit a scan definition, select it from the list of Access Scans, and then modify the attributes on the Edit Access Review Scan page.

You must click Save to save any changes to the scan definition.

Note – Changing the scope of an access scan might change the information in newly-acquired user entitlement records, as it can affect the Review Determination Rule if that rule compares user entitlements to older user entitlement records.

Canceling an Access Review

From the Access Reviews page, click Terminate to stop a selected review in progress.

Terminating a review causes these actions to occur:

- Any scheduled scans are unscheduled
- Any active scans are halted

- All pending workflows and work items are deleted
- All pending attestations are marked canceled
- Any attestations that users completed are left unchanged

Deleting an Access Review

From the Access Reviews page, click Delete to delete a selected review.

You can delete an access review if the status of the task is *terminated* or *completed*. An access review task in progress cannot be deleted unless it is first terminated.

Deleting an access review deletes all user entitlement records that were generated by the review. The delete action is recorded in the audit log.

To delete an access review, click Delete from the Access Reviews page.

Note – Canceling and deleting an access review may result in updates to a large number of Waveset objects and tasks, and can take several minutes to complete. You can check the progress of the operation by viewing the task results in Sever Tasks → All Tasks.

Managing Attestation Duties

You can manage attestation requests from the Waveset Administrator or User interface. This section provides information about responding to attestation requests and the duties involved in attestation.

Access Review Notification

During a scan, Waveset sends notification to Attestors when attestation requests require their approval. If attestor responsibilities have been delegated, the requests are sent to the delegate. If multiple attestors are defined, each attestor receives an email notification.

Requests appear as Attestation work items in the Waveset interface. Pending attestation work items are displayed when the assigned attestor logs in to Waveset.

Viewing Pending Attestation Requests

View attestation work items from the Work Items area of the interface. Selecting the Attestation tab in the Work Items area lists all the entitlement records requiring approval. From the Attestations page, you can also list entitlement records for all of your direct reports and for specified users for which you have direct or indirect control.

Acting on Entitlement Records

Attestation work items contain the user entitlement records requiring review. Entitlement records provide information about user access privileges, assigned resources, and policy violations.

The following are possible responses to an attestation request:

- **Approve**. Attests that the entitlement is appropriate as of the date recorded in the entitlement record.
- **Reject**. The entitlement record indicates possible discrepancies that cannot be currently validated or remediated.
- **Rescan**. Requests a rescan to re-evaluate the user entitlement.
- **Forward**. Enables you to specify another recipient for review.
- **Abstain**. Attestation for this record is not appropriate, and a more appropriate attestor is not known. The attestation work item is forwarded to the Review Process Owner. This option is available only if a Review Process Owner has been defined in the Access Review task.

If an attestor does not respond to a request by taking one of these actions before the specified escalation timeout period, notice is sent to the next attestor in the escalation chain. The notification process continues until a response is logged.

Attestation status can be monitored from the Compliance → Access Reviews tab.

Closed-Loop Remediation

You can avoid rejecting user entitlements by:

- Marking an entitlement as needing to be fixed by requesting a fix from another user (Request Remediation). In this case, a new remediation work item is created and assigned to one or more specified remediators.

  The new remediator can then choose to edit the user, either by using Waveset or independently, and then mark the work item as remediated when satisfied. At that point, the user entitlement is rescanned and evaluated again.
- Requesting a reevaluation of the entitlement (Rescan). In this case, the user entitlement is rescanned and evaluated again. The original attestation work item is closed. A new attestation work item is created if the entitlement still requires attestation according to the rules defined in the access scan.

Requesting Remediation

If defined by the access scan, you can route a pending attestation to another user for remediation.

Note – The Dynamic Entitlements option on the Create or Edit Access Scan pages enables this feature.

▼ To Request Remediation From Another User

1. **Select one or more entitlements from the list of attestations, and then click Request Remediation.**

   The Select and Confirm to Request Remediation page appears.

2. **Enter a user name, and then click Add to add the user to the Forward to field. Alternatively, click ... (More) to search for a user. Select the user in the search list, and then click Add to add the user to the Forward to list. Click Dismiss to close the Search area.**

3. **Enter comments in the Comments field, and then click Proceed.**

   Waveset returns to the list of attestations.

Note – Details of the remediation request appear in the History area of the individual user entitlement.

Rescanning Attestations

If defined by the access scan, you can rescan and reevaluate a pending attestation.

Note – The Dynamic Entitlements option on the Create or Edit Access Scan pages enables this feature.

▼ To Rescan A Pending Attestation

1. **Select one or more entitlements from the list of attestations, and then click Rescan.**

   The Rescan User Entitlements page appears.

2. **Enter comments about the rescan action in the Comments area, and then click Proceed.**

Forwarding Attestation Work Items

You can forward one or more attestation work items to another user.

▼ To Forward Attestations

1. **Select one or more work items in the attestation list, and then click Forward.**

   The Select and Confirm Forwarding page appears.

2. **Enter a user name in the Forward to field. Alternatively, click ... (More) to search for a user name.**

3. **Enter comments about the forwarding action in the Comments field.**

4. **Click Proceed.**

   Waveset returns to the list of attestations.

Note – Details of the forwarding action appear in the History area of the individual user entitlement.

Digitally Signing Access Review Actions

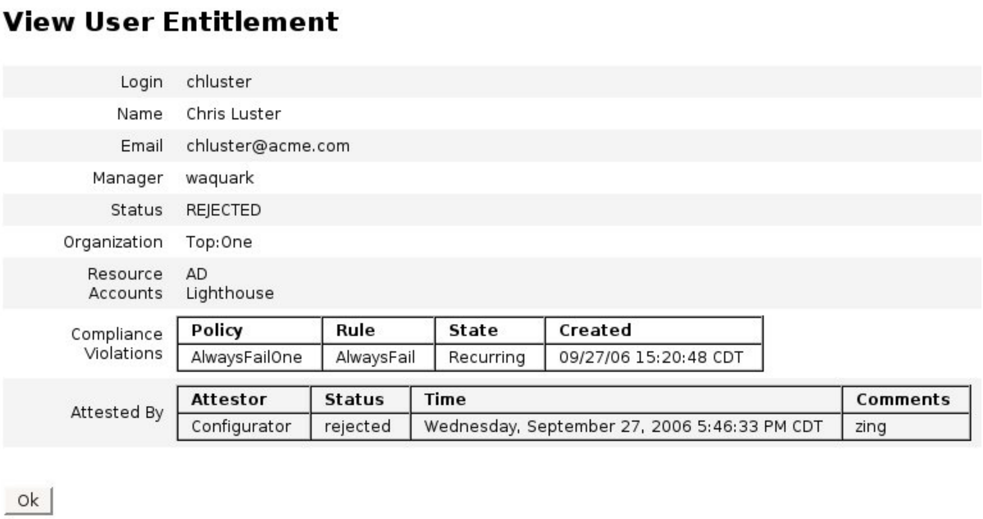
You can set up digital signing to handle access review actions. For information about configuring digital signatures, see "Signing Approvals" on page 219. The topics discussed there explain the server-side and client-side configuration required to add the certificate and CRL to Waveset for signed approvals.

Access Review Reports

Waveset provides the following reports that you can use to evaluate the results of an access review:

- **Access Review Coverage Report**. Provides a list of users with user entitlement overlaps, differences, or both in table format, depending on how the report is defined. This report might also contain additional columns that show which access reviews contain overlaps and/or differences.
- **Access Review Detail Report**. This report provides the following information, in table format:
  - **Name**. Name of user entitlement record
  - **Status**. Current status of the review process: initializing, terminating, terminated, number of scans in progress, number of scans scheduled, awaiting attestation, or completed
  - **Attestor**. Waveset users assigned as the attestor for the record
  - **Scan Date**. Timestamp recorded for when the scan occurred
  - **Disposition Date**. Date (timestamp) when entitlement record was attested
  - **Organization**. Organization of user in the entitlement records

- **Manager**. Manager of a scanned user
- **Resources**. Resources the user has accounts on that were captured in this user entitlement
- **Violations**. Number of violations detected during the review
- Click a name in the report to open the user entitlement record. “Access Review Reports” on page 458 shows a sample of the information provided in the user entitlement record view.



View User Entitlement

Login	chluster
Name	Chris Luster
Email	chluster@acme.com
Manager	waquark
Status	REJECTED
Organization	Top:One
Resource Accounts	AD Lighthouse

Compliance Violations

Policy	Rule	State	Created
AlwaysFailOne	AlwaysFail	Recurring	09/27/06 15:20:48 CDT

Attested By

Attestor	Status	Time	Comments
Configurator	rejected	Wednesday, September 27, 2006 5:46:33 PM CDT	zing

- **Access Review Summary Report**.

  This report, also discussed in “Managing Access Review Progress” on page 453 and illustrated in Figure 15–4, shows the following summary information about the access scans you select for the report:

  - **Review Name**. Name of the access scan
  - **Date**. Timestamp for when the review was launched
  - **User Count**. Number of users scanned for the review
  - **Entitlement Count**. Number of entitlement records generated
  - **Approved**. Number of entitlement records approved
  - **Rejected**. Number of entitlement records rejected
  - **Pending**. Number of entitlement records still pending
  - **Canceled**. Number of entitlement records canceled

These reports are available for download, in Portable Document Format (PDF) or comma-separated value (CSV) format, from the Run Reports page.

Access Review Remediation

Compliance violation remediation and mitigation, and access review remediation, are managed from the Remediations area of the Work Items tab. However, there are differences between the two remediation types. This section describes the unique behavior of access review remediation, and how it differs from the remediation tasks and information described in "Compliance Violation Remediation and Mitigation" on page 433.

About Access Review Remediation

When an attestor requests that a user entitlement be remediated, the Standard Attestation workflow creates a remediation request, which must be addressed by a remediator (a designated user who is allowed to evaluate and respond to remediation requests).

The problem can only be remediated; it cannot be mitigated. Attestation cannot continue until the problem is resolved.

When remediations result from an access review, then the Access Review dashboard tracks all attestors and remediators involved with the review.

Access Review Remediation Request Escalation

Access Review remediation requests are not escalated beyond the initial remediator.

The Remediation Workflow Process

The logic of access review remediation is defined in the Standard Attestation workflow.

When an attestor requests remediation of a user entitlement, the Standard Attestation workflow:

- Generates a remediation request (of type `accessReviewRemediation)` that contains information about the user entitlement requiring remediation.
- Sends an email to the requested remediator.

The new remediator can then choose to edit the user, either by using Waveset or independently, and then mark the work item as remediated when satisfied. At that point, the user entitlement is rescanned and evaluated again.

Access Review Remediation Responses

By default, three response options are given to the access review remediator:

- **Remediate**. A remediator indicates that something has been done to fix the problem.

  The user entitlement is then rescanned and evaluated again. If the user entitlement is again marked as requiring attestation, then the original attestor will see the user entitlement show again in his Attestations work item list.

  Details of the remediation request action appear in the History area of the individual user entitlement.
- **Forward**. A remediator reassigns the responsibility for resolving the remediation request to another individual.

  Details of the forwarding action appear in the History area of the individual user entitlement.
- **Edit User**. A remediator chooses to directly edit the user to remediate the problem.

  This button is shown only if the remediator has permission to modify users. After making changes to the user and clicking Save, the remediator is taken to the Remediation confirmation page to supply a comment describing the change made to the user.

  The user entitlement is then rescanned and evaluated again. If the user entitlement is again marked as requiring attestation, then the original attestor will see the user entitlement show again in his Attestations work item list.

  Details of the edit appear as a remediation request action in the History area of the individual user entitlement.

The Remediations Page

The Type column is shown as UE (user entitlement) for all remediation work items that are access review remediation work items.

Unsupported Access Review Remediation Actions

The prioritization and mitigation features are not supported for access review remediations.

CHAPTER 16

Data Exporter

The Data Exporter feature allows you to write information about users, roles, and other object types to an external data warehouse.

Read this chapter for information and procedures to help you set up and maintain Data Exporter. For full details about planning and implementing Data Exporter, see Chapter 5, "Data Exporter," in *Oracle Waveset 8.1.1 Deployment Guide*.

This chapter is organized as follows:

What is Data Exporter?

Waveset contains and processes data relevant to managing identities across distributed systems and applications. To improve overall performance, Waveset does not retain all of the data it generates during normal provisioning and other daily activities. For example, Waveset by default does not persist the intermediate status workflow activities and task instances. If it is necessary to capture all or some of the data that Waveset normally discards, you can enable the Data Exporter feature.

When Data Exporter is enabled, Waveset stores each detected change to a specified object (data type) as a record in a table in the repository. These events are queued until a task writes them to an external data warehouse. (You can configure how frequently each type of data is exported.) The exported data can be further processed or used as a basis for queries and transformations with commercial transformation, reporting, and analysis tools.

Exporting data to a data warehouse has a negative impact on the Waveset server's performance, and this feature should not be enabled unless there is a business need for the exported data.

Waveset also allows you to create and execute forensic queries. A forensic query searches the data warehouse to identify User or Role objects that meet the criteria you specify. See "Configuring Forensic Queries" on page 475 for more information.

Planning to Implement Data Exporter

Because Data Exporter is disabled by default, it must be configured to become operational. Configuration of Data Exporter requires several decisions to be made before configuration can begin.

- Which data types will be exported?
- Which techniques will be used to capture data for each data type?
- How often will data be exported for each type?
- What will be in the exported schema for each type?
- Will a custom Warehouse Interface Code (WIC) factory class be required?

When Data Exporter is enabled, the default configuration exports all attributes of all data types. This may cause an unnecessary processing burden on Waveset and the warehouse by consuming warehouse storage that will never be used. Data warehousing tends to be conservative and capture data when there is a chance the data might be used later. You do not have to export all the data that can be exported. You can configure which data types to export and restrict some events from being export.

Once these decisions above have been made, use the following steps to implement Data Exporter:

▼ To Implement Data Exporter

1. **(Optional) Customize the export schema for selected types and regenerate the warehouse DDL. Refer to the "Customizing Data Exporter" in *Oracle Waveset 8.1.1 Deployment Guide* for more information.**

2. **Create a user account on the warehouse RDBMS and load the warehouse DDL on that system. Refer to the "Customizing Data Exporter" in *Oracle Waveset 8.1.1 Deployment Guide*for more information.**

3. **Configure Data Exporter, as described in "Configuring Data Exporter" on page 465.**

4. **Test Data Exporter to ensure it was configured correctly. See "Testing Data Exporter" on page 474 for more information.**

5 **(Optional) Create forensic queries that can search data written to the data warehouse. See "Configuring Forensic Queries" on page 475 for more information.**

6 **Maintain Data Exporter using JMX and monitoring the log files. See "Maintaining Data Exporter" on page 479 for more information.**

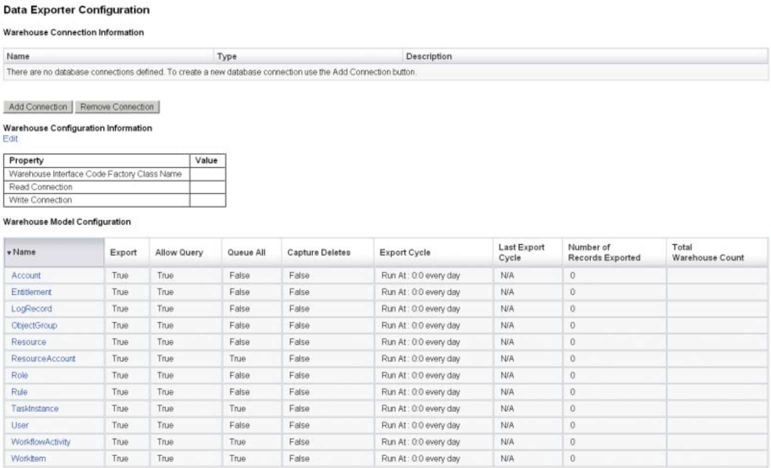
Configuring Data Exporter

The Data Exporter configuration page allows you to define what types of data to retain, specify which attributes to export, and schedule when to export the data. Each data type can be configured independently.

▼ To Configure Data Exporter

1 **In the Administrator interface, click Configure in the main menu. Then click the Warehouse secondary tab. The Data Exporter Configuration page opens.**

FIGURE 16–1 Data Exporter Configuration



Data Exporter Configuration

Warehouse Connection Information

Name	Type	Description
There are no database connections defined. To create a new database connection use the Add Connection button.		

Warehouse Configuration Information

Property	Value
Warehouse Interface Code Factory Class Name	
Read Connection	
Write Connection	

Warehouse Model Configuration

Name	Export	Allow Query	Queue All	Capture Deletes	Export Cycle	Last Export Cycle	Number of Records Exported	Total Warehouse Count
Account	True	True	False	False	Run At : 0:0 every day	N/A	0	
Entitlement	True	True	False	False	Run At : 0:0 every day	N/A	0	
LogRecord	True	True	False	False	Run At : 0:0 every day	N/A	0	
ObjectGroup	True	True	False	False	Run At : 0:0 every day	N/A	0	
Resource	True	True	False	False	Run At : 0:0 every day	N/A	0	
ResourceAccount	True	True	True	False	Run At : 0:0 every day	N/A	0	
Role	True	True	False	False	Run At : 0:0 every day	N/A	0	
Rule	True	True	False	False	Run At : 0:0 every day	N/A	0	
TaskInstance	True	True	True	False	Run At : 0:0 every day	N/A	0	
User	True	True	False	False	Run At : 0:0 every day	N/A	0	
WorkflowActivity	True	True	True	False	Run At : 0:0 every day	N/A	0	
WorkItem	True	True	True	False	Run At : 0:0 every day	N/A	0	

2 **To define read and write connections, click the Add Connection button. The Edit Database Connection page opens.**

Complete the fields on this page and click Save to return to the Data Exporter Configuration page. See "Defining Read and Write Connections" on page 466 for more information.

3 **To assign the WIC class and database connections, click the Edit link that is in the Warehouse Configuration Information section. The Data Exporter Warehouse Configuration page opens.**

Complete the fields on this page and click Save to return to the Data Exporter Configuration page. See “Defining the Warehouse Configuration Information” on page 468 for more information.

4 **Click on a data type link in the Warehouse Model Configuration table. The Data Exporter Type Configuration page opens.**

Complete the Export, Attributes, and Schedule tabs on this page and click Save to return to the Data Exporter Configuration page. See “Configuring Warehouse Models” on page 469 for more information.

Repeat this step for every data type.

5 **To configure which workflow to run before and after each data type is exported, click the Edit link in the Exporter Automation section. The Data Exporter Automation Configuration opens.**

Complete the fields on this page and click save to return to the Data Exporter Configuration page. See for more information.

6 **To configure the export task daemon, click the Edit link that is in the Warehouse Task Configuration section. The Data Exporter Warehouse Configuration page opens.**

Complete the fields on this page and click Save to return to the Data Exporter Configuration page. See “Configuring the Warehouse Task” on page 472 for more information.

Note – Exporting is fully operational once these steps have been completed. When exporting is enabled, data records will start queuing for export. If you do not enable the export task, the queue tables will fill up, and queuing will be suspended. It is generally more efficient to export smaller batches (more frequently) than larger ones, but exporting is subject to the write availability of the warehouse itself, which may be constrained for other reasons.

---

7 **Optionally set the maximum queue size. See “Modifying the Configuration Object” on page 474 for more information.**

Defining Read and Write Connections

Waveset uses a write connection during the export cycles. It uses the read connection to indicate how many records are currently in the warehouse (during warehouse configuration) and to service the forensic query interface.

Warehouse connections can be defined as an application server DataSource, as a JDBC connection, or as a reference to a database resource. If a JDBC connection or database resource is defined, data exporting uses a small number of connections extensively during write operations and then closes all of the connections. Data Exporter only uses the read connection during warehouse configuration and during forensic query execution, and it will close those connections as soon as the operation completes.

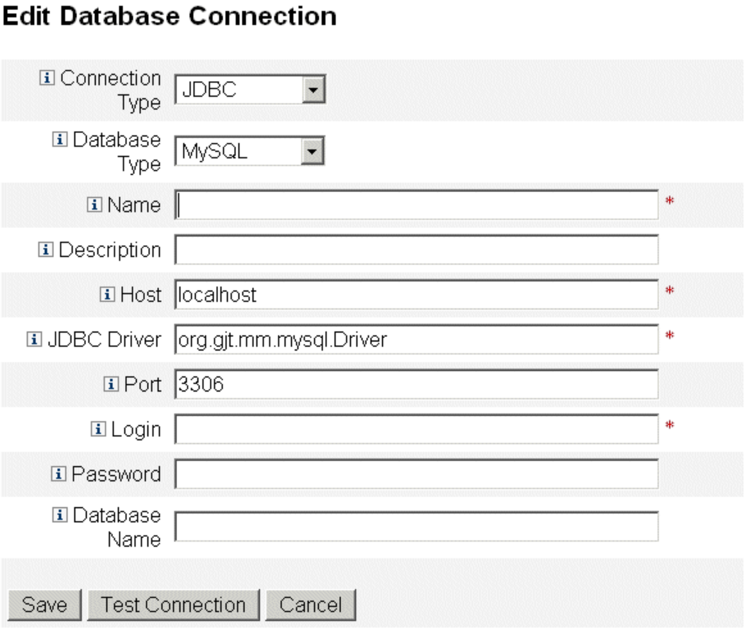
Exporter uses the same schema for write and read connections, and you can use the same connection information for both. However, if you have separate connections, the deployment can write to a set of warehouse staging tables, transform those tables into the real warehouse, and then transform the warehouse tables to a data mart that Waveset will read from.

You can edit the Data Export Configuration form to prevent Waveset from reading from the warehouse. This form contains the `includeWarehouseCount` property, which causes Waveset to query the warehouse and display the number of records of each data type. To disable this feature, copy the Data Export Configuration Form, change the value of the `includeWarehouseCount` property to `true`, and import your customized form.

▼ To Define Read and Write Connections

1 **From the Data Exporter Configuration page, click the Add Connection button.**

FIGURE 16–2 Data Exporter Configuration



Edit Database Connection

Connection Type	JDBC	
Database Type	MySQL	
Name		*
Description		
Host	localhost	*
JDBC Driver	org.gjt.mm.mysql.Driver	*
Port	3306	
Login		*
Password		
Database Name		

2 **Specify how Waveset will establish read or write connections to the data warehouse by selecting an option from the Connection Type drop-down menu.**

- **JDBC**. Connects to a database using the Java Database Connectivity (JDBC) application programming interface. Connection pooling is provided by the Warehouse Interface Code.
- **Resource**. Uses the connection information defined in a resource. Connection pooling is provided by the Warehouse Interface Code.
- **Data Source**. Uses the underlying application server for connection management and pooling. This type of connection requests connections from the application server.

  The fields that are displayed on the page vary, depending on which option you selected from the **Connection Type** drop-down menu. Refer to the online help for detailed information about configuring the database connection.

3 **Click Save to save your configuration changes and return to the Data Exporter Configuration page.**

Repeat this procedure if you will use separate read and write connections.

Defining the Warehouse Configuration Information

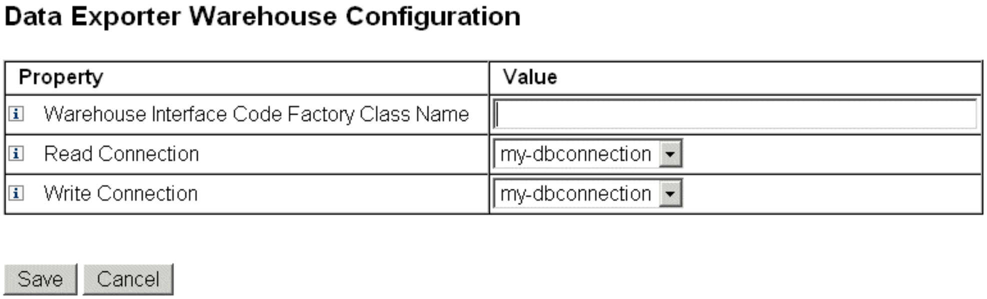
To configure the warehouse, you must select a read connection, a write connection, and specify a Warehouse Interface Code factory class. The WIC factory class provides the interface between Waveset and the warehouse. Waveset provides a default implementation of the code, but you may build your own. See Chapter 5, “Data Exporter,” in *Oracle Waveset 8.1.1 Deployment Guide* for information about creating custom factory classes.

The `jar` file containing the factory class and any supporting `jar` files must be present in the `$WSHOME/exporter` directory on the Waveset server that executes the export task and on any server that configures the Data Exporter. Only one Waveset server can export data at any given time.

▼ To Define Warehouse Configuration Information

1 **From the Data Exporter Configuration page, click the Edit link that is in the Warehouse Configuration Information section.**

FIGURE 16–3 Data Exporter Configuration



Data Exporter Warehouse Configuration

Property	Value
Warehouse Interface Code Factory Class Name	
Read Connection	my-dbconnection
Write Connection	my-dbconnection

2 **Specify a value in the Warehouse Interface Code Factory Class Name field. If your integrator has not created a custom class, enter the value** `com.sun.idm.warehouse.base.Factory`**.**

3 **Specify the connections by selecting an option from both the Read Connection and Write Connection drop-down menus.**

4 **Click Save to save your configuration changes and return to the Data Exporter Configuration page.**

Configuring Warehouse Models

Each exportable data type has a set of options that are used to control if, how and when the type is exported. Exporting data increases the load on the Waveset servers, so exporting should only be enabled for data types that are of business interest.

The following table describes each of the data types that can be exported.

TABLE 16–1 Supported Data Types

Data Type	Description
`Account`	A record containing the linkage between a User and a ResourceAccount
`AdminGroup`	A group of Waveset permissions available on all ObjectGroups
`AdminRole`	The permissions assigned to one or more ObjectGroups
AuditPolicy	A collection of rules evaluated against an Waveset object to determine compliance to a business policy.
`ComplianceViolation`	A record containing a user's non-compliance with an AuditPolicy
`Entitlement`	A record containing the list of attestations for a specific User
`LogRecord`	A record containing a single audit record

TABLE 16–1 Supported Data Types (Continued)

Data Type	Description
`ObjectGroup`	A security container that is modeled as an organization
`Resource`	A system/application on which accounts are provisioned
`ResourceAccount`	A set of attributes that comprise an account on a specific Resource
`Role`	A logical container for access
`Rule`	A block of logic that can be executed by Waveset
`TaskInstance`	A record indicating an executing or completed process
`User`	A logical user that includes zero or more accounts.
`WorkflowActivity`	A single activity of an Waveset workflow
`WorkItem`	A manual action from an Waveset workflow

▼ To Configure Warehouse Models

1. **From the Data Exporter Configuration page, click on a data type link.**

2. **In the Export tab, specify whether to export the data type. If you do not want to export this data type, deselect the Export check box and click Save. Otherwise, select the remaining options on this Export tab as needed.**

   - **Allow Query**. Controls whether the model can be queried.
   - **Queue All**. Captures all changes to objects of this type. Checking this option may add significant processing costs to the Exporter. Use this option sparingly.
   - **Capture Deletes**. Records all deleted objects of this type. Checking this option may add significant processing costs to the Exporter. Use this option sparingly.

3. **The Attributes tab allows you to select which attributes may be specified as part of a forensic query, and which attributes can be displayed in the query results. You cannot delete the default attributes from the Administrator interface. See Chapter 1, "Working with Attributes," in *Oracle Waveset 8.1.1 Deployment Guide* for information about changing the default attributes.**

   New attribute names have the following characteristics:

   - `attrName` — The attribute is a top-level and scalar.
   - `attrName[]` — The attribute is a list-valued top-level attribute, and the elements in the list are scalar.
   - `attrName['`*key*`']` — The attribute contains a map value, and the value of the map with the specified key is desired.

- `attrName[].`*name2* — The attribute is a list-valued top-level attribute, where the elements in the list are structures. *name2* is the attribute in the structure to be accessed.

Note – If you want to export attributes to the `EXT_RESOURCEACCOUNT_ACCTATTR` table, you must check the Audit box for each attribute to be exported.

---

4 **Specify how often to export the information associated with the data type on the Schedule tab. Cycles are relative to midnight on the server. A cycle of every 20 minutes would occur on the hour, then 20 minutes and 40 minutes past the hour. If an export attempt takes longer than a scheduled cycle, the next cycle will be skipped. For example, if a cycle is defined as 20 minutes and starts at midnight, and it takes 25 minutes to complete the export, the next export will start at 12:40. The export originally scheduled for 12:20 will not occur.**

Configuring Exporter Automation

Waveset allows you to specify workflows that executes before and after exporting data.

The Cycle Start workflow could be used to prevent an export if an event occurs that warrants a cancellation. For example, if an application that reads or writes to the staging tables needs exclusive access to the tables at the same time an export is scheduled to occur, the export should be cancelled. The workflow should return a value of 1 to cancel the export. Waveset creates an audit record that indicates the export was skipped and provides the error results. If the workflow returns 0 and no errors occur, the data type will be exported.

The Cycle Complete workflow runs after all the records have been exported. This workflow usually triggers another application to process the exported data. After this workflow completes, the Exporter checks for another data type to export.

Sample workflows are provided in the `$WSHOME/sample/web/exporter.xml` file. The `subtype` for a Exporter workflow is `DATA_EXPORT_AUTOMATION` and the `authType` is `WarehouseConfig`.

▼ To Configure Exporter Automation

1 **From the Data Exporter Configuration page, click the Edit link that is in the Exporter Automation section.**

2 **Optionally select a workflow to run before an export from the Cycle Start Workflow drop-down menu.**

3 **Optionally select a workflow to run after an export from the Cycle Start Workflow drop-down menu.**

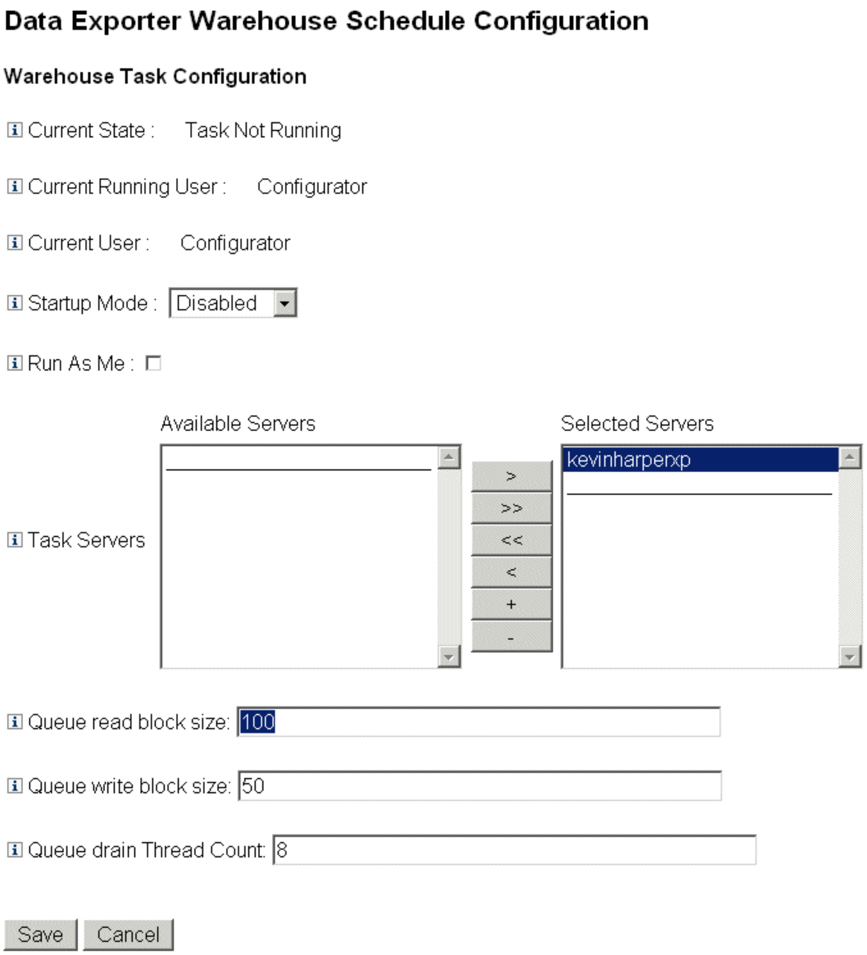
Configuring the Warehouse Task

It is not required to run the export task on a dedicated server, but you should consider it if you expect to export a large amount of data. The export task is efficient at transferring data from Waveset to the warehouse, and will consume as much CPU as possible during the export operation. If you do not use a dedicated server, you should restrict the server from handling interactive traffic, because the response time will degrade dramatically during a large export.

▼ To Configure the Warehouse Configuration Information

1. **From the Data Exporter Configuration page, click the Edit link that is in the Warehouse Task Configuration section.**

FIGURE 16–4 Data Warehouse Schedule Configuration



Data Exporter Warehouse Schedule Configuration

Warehouse Task Configuration

Current State : Task Not Running

Current Running User : Configurator

Current User : Configurator

Startup Mode : Disabled

Run As Me : □

Task Servers

Available Servers

Selected Servers: kevinharperxp

Queue read block size: 100

Queue write block size: 50

Queue drain Thread Count: 8

2 Select an option from the Startup Mode drop-down menu to determine whether the warehouse task starts automatically when Waveset starts. Selecting Disabled means the task must be started manually.

3 Check the Run As Me check box to cause the Exporter task to run under the your administrative account.

4 Select the servers that the task can run on. You may specify multiple servers, but only one warehouse task can run at any given time. If the server executing the task is stopped, the scheduler automatically restarts the task on another server from the list (if available).

5 **Specify the number of records read from the queue into a memory buffer before writing in the Queue read block size field. The default value for this field is good for most exports. Increase this value if the Waveset repository server is slow compared to the warehouse server.**

6 **Specify the number of records written to the warehouse in a single transaction in the Queue write block size field.**

7 **Specify the number of Waveset threads to use for reading queued records in the Queue drain Thread Count field. Increase this number if the queue table has a large number of records of different types. Decrease this number if the queue table has few data types.**

8 **Click Save to save your configuration changes and return to the Data Exporter Configuration page.**

Modifying the Configuration Object

When Data Exporter is configured and operational, any data types that are configured to be queued will be captured in the internal queue table. By default this table does not have an upper bound, but one can be configured by editing the `Data Warehouse Configuration` Configuration object. This object has a nested object named `warehouseConfig`. Add the following line to the `warehouseConfig` object:

```
<Attribute name=’maxQueueSize’ value=’YourValue’/>
```

The value of `maxQueueSize` can be any positive integer that is less than 2^{31}. Data Exporter disables queuing when that limit is reached. Data that is generated cannot be exported until the queue is drained.

Normal Waveset operation can generate multiple thousands of changed records per hour, so the queued table can grow very quickly. Since the queue table is in the Waveset repository, this growth will consume tablespace in the RDBMS, with the potential to exhaust the tablespace. Placing a cap on the queue may be necessary if you have a limited amount of tablespace.

Use the Data Queue JMX Mbean to monitor the size of the queue table. See “Monitoring Data Exporter” on page 479 for more information.

Testing Data Exporter

After Data Exporter is correctly configured, it behaves as a background process, sending data to the warehouse at the configured intervals. To run the Exporter on demand, use the Data Warehouse Exporter Launcher task.

▼ To Start the Data Warehouse Exporter Launcher

1. **Disable the Warehouse Task. See “Configuring the Warehouse Task” on page 472 for more information.**
2. **Click Server Tasks in the main menu. Then click the Run Tasks secondary tab. The Available Tasks page opens.**
3. **Click the Data Warehouse Exporter Launcher link. The Launch Task page opens.**
4. **Select the Debug options check box to display additional options.**
5. **Select the Ignore Initial LastMods check box to cause the Exporter to ignore the “last polled” timestamp it uses to determine which records in the Waveset repository have already been exported. When this option is selected, all records in the Waveset repository of the selected types will be exported.**
6. **Choose which types of data to export from the Export Once list. If you do not choose any types in the Export Once list, the export task runs as a daemon and exports based on the schedule previously defined. If you select one or more data types, Waveset exports these types immediately, and the export task exits.**
7. **Set the values for the other fields on the page as needed.**
8. **Click Launch to begin the task.**

Configuring Forensic Queries

Forensic queries allow Waveset to read data that has been stored in the data warehouse. They can identify users or roles based on current or historical values of the user, role, or related data types. A forensic query is similar to a Find User or Find Role report, but it differs in that the matching criteria can be evaluated against historical data, and because it allows you to search attributes that are of data types other than the user or role being queried.

The purpose of the forensic query is to take action on the results using Waveset. The forensic query is not a general-purpose reporting tool.

A forensic query can ask questions similar to the following:

- Who had access to system X between time A and B, and who approved of that access?
- How many provisioning requests have been processed in the last 48 hours, and how long did each request take?

The results of a forensic query cannot be saved. General reporting on the warehouse data should be accomplished using commercial reporting tools.

Creating a Query

A forensic query can search for either User or Role objects. The query can be very complex, allowing the author to select one or more attribute conditions on related data types. User forensic queries can search attributes with the data types of User, Account, ResourceAccount, Role, and Entitlement, and WorkItem. Role forensic queries can search attributes with data types of Role, User, and Work Item.

Within a single data type, all attribute conditions are logically ANDed, so that all conditions must be met for a match to occur. By default, matches are ANDed across data types, but if you select the Use OR check box, the matches across data types are logically ORed.

The warehouse may contain multiple records for a single User or Role object, and a single query could return multiple matches for the same user or role. To help differentiate these matches, each data type can be constrained with a date range, such that only records from within the specified date range are considered matches. Each related data type may be constrained with a date range, so it is possible to issue a query of the form:

```
find all Users with Resource Account on ERP1 between May and July 2005
who were attested by Fred Jones between June and August 2005
```

The date range is from midnight to midnight. For example, the range May 3, 2007 to May 5, 2007 is 48 hours. It would not include any records from May 5, 2007.

The operands (values to be compared to) for each attribute condition must be specified as part of the query definition. The schema restricts some attributes to have a limited set of potential values, while other attributes have no restrictions. For example, most date fields must be entered in `YYYY-MM-DD HH:mm:ss` format.

Note – Due to the potentially large volume of data in the warehouse, and the complexity of the query, it may take a long time for the query to produce results. If you navigate away from the query page while a forensic query is running. you will not be able to see the results of the query.

▼ To Create A Forensic Query

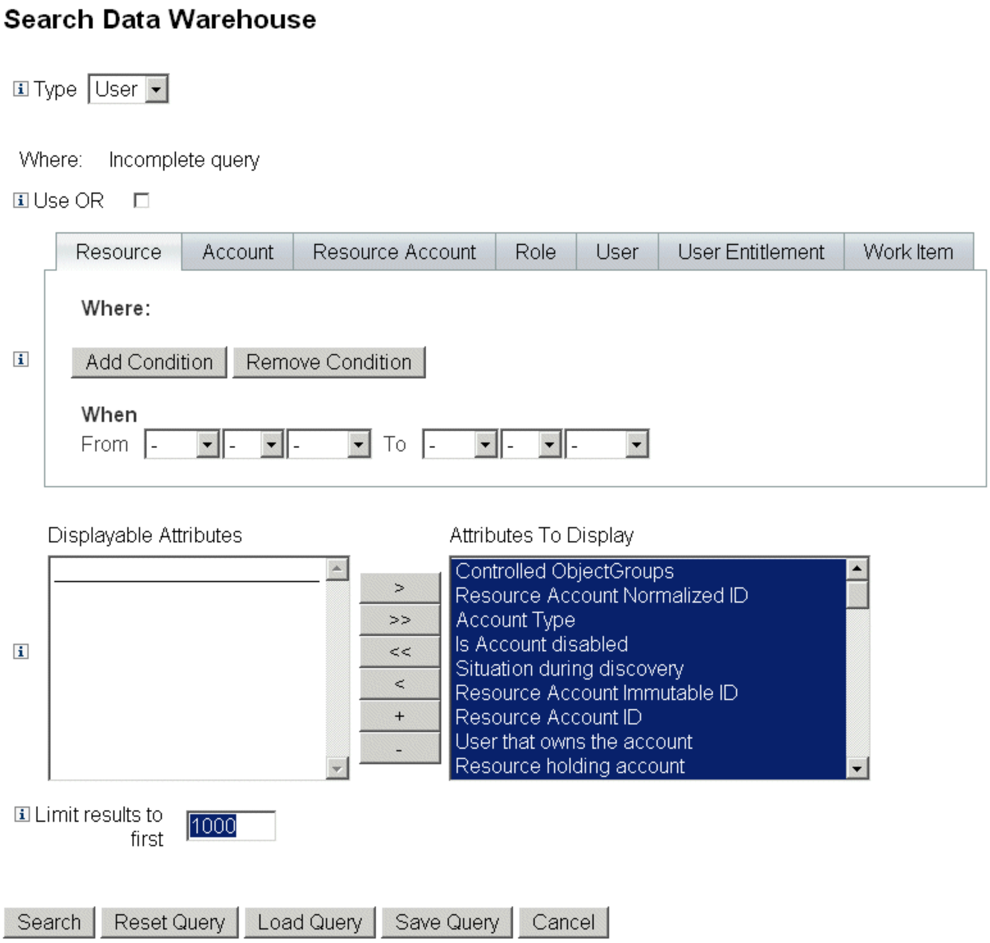
1 **In the Administrator interface, click Compliance in the main menu.**

The Audit Policies page (Manage Policies tab) opens.

2 **Click the Forensic Query secondary tab.**

The Search Data Warehouse page opens.

FIGURE 16–5 Search Data Warehouse



Search Data Warehouse

Type: User

Where: Incomplete query

Use OR □

When From - - - To - - -

Attributes To Display:

- Controlled ObjectGroups
- Resource Account Normalized ID
- Account Type
- Is Account disabled
- Situation during discovery
- Resource Account Immutable ID
- Resource Account ID
- User that owns the account
- Resource holding account

Limit results to first: 1000

3 **Select whether to search user or role records from the Type drop-down menu.**

4 **Select the Use OR check box to cause Waveset to logically OR the results of each data type queried. By default, the system performs a logical AND on the results.**

5 **Select a tab that represents a data type that will be in the forensic query.**

a. **Click Add Condition. A set of drop-down menus displays.**

b. **Select an operand (condition to check for) from the left drop-down menu and the type of comparison to make in the right drop. Then enter a string or integer to search for. The list of possible operands is defined in the external schema. Refer to the online help for a description of each operand.**

c. **Optionally, select a range of dates to narrow the scope of the query.**

   Add more conditions as necessary to the currently-selected data type. Repeat this step for all data types that will be part of the forensic query definition.

6 **Pick the attributes in the available attributes that you would like to display in the results of the forensic query.**

7 **Specify the a value in the Limit results to first field. When using conditions from multiple data types, the limit will be applied to the subquery for each type, and the final result is the intersection of all subqueries. As a result, the final result may exclude some records because of the limit on a subquery.**

8 **Click Search to run the forensic query immediately or Save Query to reuse the query. See "Saving a Forensic Query" on page 478 for information about reusing your forensic queries.**

Saving a Forensic Query

After you have configured a query (and optionally executed it to ensure that it produces the desired results), you can save the query for later execution.

▼ To Save a Forensic Query

1 **From the Search Data Warehouse page, click Save Query. The Save Forensic Query page opens.**

2 **Specify a name and description for query.**

3 **Select the Save condition values check box to save the values of the conditions (strings and integers) you entered on the Search Data Warehouse page. If you do not select this check box, then the saved forensic query serves as a template, and you must enter values each time you run the query.**

4 **Anyone can execute any saved query, but by default only the query author can modify the query. To allow other users to modify your query, select the Allow others to alter this query check box.**

5 **Because the query returns User or Role objects, you can choose which attributes of the objects to display in the results. If you want to display attributes that are not included in the Attributes to Display list, you can go to Data Exporter Configuration page and add new displayable attributes to the User or Role type.**

Loading a Query

You can load any query that has been saved by any user, but you can only alter queries that you have created, or that other people have marked as modifiable by anyone.

▼ To Load a Forensic Query

1 **From the Search Data Warehouse page, click Load Query. The Load Forensic Query page opens. The Query Summary column displays Incomplete Query if the query has been saved as a template.**

2 **Select the check box to the left of the query and click Load Query.**

Maintaining Data Exporter

This section describes how to track the status of Data Exporter. This information is organized into the following topics:

- "Monitoring Data Exporter" on page 479
- "Monitoring Logging" on page 480

Monitoring Data Exporter

After the Exporter has been configured and is operational, you may choose to monitor it to ensure its continuous operation. The Exporter has several JMX beans that are useful for determining how the Exporter is behaving. The JMX beans include statistics on the average read/write rates for the Exporter, the current/maximum size of the internal memory queue, and the size of the persistent queue. The Exporter also produces audit records during export, one record for each cycle of each data type. The audit record includes how many records of the type were exported, and how long the export took.

Data Exporter provides the following JMX management beans that monitor the Exporter.

TABLE 16–2 JMX Management Beans

Bean Name	Description
DataExporter	Contains the number of currently queued exports and the upper limit for the queue.
DataQueue	Contains the number of currently cached queued exports and the rate of arrival to the cache.
ExporterTask	Contains the number of export reads (from Waveset), writes (to the warehouse), rates (records/second) for reading, writing, and number of errors.

Data Exporter can be configured to queue export records to a queuing table during normal Waveset operation. Because the queue needs to potentially scale to a large number of records and survive a server restart, the queue is backed by a table in the Waveset repository. Since writes to the repository would typically slow down normal Waveset operations, the queue uses a small memory cache to buffer records in memory until they can be persisted in the repository.

The DataQueue MBean attributes can be plotted to show the largest number of records queued in memory (on a single Waveset server). On a balanced system, the number of records in the memory cache should be small and trend quickly to zero. If you observe this number get large (in the thousands) or not return to zero within a few seconds, you should investigate the write performance of the repository.

The ExportTask MBean contains two error counts, one for read and one for write. These counts should be zero, but there are a number of reasons that errors might occur, especially during write. The most common write error will result from the exported data not fitting within the warehouse table columns - typically a string overflow. Some exported String data is unbounded, where the export table columns must have some upper limit.

Monitoring Logging

Waveset has two sets of objects that grow without bounds: the audit log and the system log. Data Exporter addresses some of the maintenance problems associated with the log tables.

Audit Logs

Waveset writes immutable audit records to the audit log to serve as a historical audit trail of the operations it performs. Waveset uses these records in certain reports, and the data from the records may be displayed in the administrator interface. However, because the audit log grows without bounds and it grows at a modest rate, the deployer must determine when to truncate the audit log. Before Data Exporter, if you wanted to preserve the records prior to truncation, you were forced to dump the tables from the repository. If Data Exporter is enabled and configured to export log records, then the old records are preserved in the warehouse, and Waveset may truncate the audit tables as needed.

System Logs

System logs have the same immutable property that the audit logs have, but system logs are not typically generated as frequently. Data Exporter does not export system logs. To truncate the system log and preserve old records, you must dump the tables in the repository.

CHAPTER 17

Service Provider Administration

This chapter provides information that you need to know to administer the Service Provider functionality in Oracle Waveset. To use this information, an understanding of Lightweight Directory Access Protocol (LDAP) directories and federation management is helpful. For a broader discussion of an Oracle Waveset Service Provider (Service Provider) implementation, see the *Oracle Waveset Service Provider 8.1.1 Deployment*.

This chapter contains the following topics:

Overview of Service Provider Features

In a service provider environment, you need the ability to manage user provisioning for all end-users, which includes extranet as well as intranet users. The Service Provider features enable company administrators to categorize identity accounts into two distinct types: Waveset users and Service Provider users. Service Provider users in Waveset are user accounts that have been configured as the Service Provider User type.

The Waveset user-provisioning and auditing capabilities extend to service provider implementations by providing the following features:

Enhanced End-User Pages

Enhanced end-user pages that are customizable for a Service Provider implementation are provided.

Password and Account ID Policy

You can define account ID and password policies for Service Provider users and resource accounts, as with other Waveset users.

Policy checking code is activated for Service Provider users with the Service ProviderSystem Account Policy, which has been added to the main Policies table.

Waveset and Service Provider Synchronization

Synchronization for Waveset and Service Provider accounts can be configured to run on any Waveset server, or restricted to selected servers.

Service Provider Synchronization, like Waveset synchronization, can be easily stopped and started from the Resource Actions options on the Resources page. See "Start and Stop Synchronization" on page 519.

The Input Forms for Waveset user synchronization and Service Provider user synchronization differ. See "End-User Interface" on page 515.

Access Manager Integration

You can use Access Manager 7 2005Q4 for authentication on Service Provider end-user pages. If integration with Access Manager is configured, Access Manager ensures that only authenticated users can access the end-user pages.

Service Provider requires the user name for auditing purposes. Update the `AMAgent.properties` file to add the user's ID to the HTTP headers, for example:

```
com.sun.identity.agents.config.response.attribute.mapping[uid] = HEADER_speuid
```

The end-user-page authentication filter puts the HTTP header value into the HTTP session where the rest of the code expects it to be.

Initial Configuration

To configure the Service Provider features, use the following procedures to edit Waveset configuration objects to the directory server:

- Edit Main Configuration
- Edit User Search Configuration

Note –

Before continuing, ensure that you have:

- Defined your LDAP resource. A sample resource named Service Provider End-User Directory is imported by default. You can configure multiple resources if user and configuration information is to be stored in different directories.
- The schema must include mapping for an XML object.

  If desired, configure your Service Provider Account Policy.
- The Base context configured for the directory resource only applies to the users stored in the directory.

Edit Main Configuration

▼ To Edit Configuration Objects for a Service Provider Implementation

1. **In the Administrator interface, click Service Provider in the menu.**

2. **Click Edit Main Configuration.**

   The Service ProviderConfiguration page opens.

3. **Complete the Service Provider Configuration form.**

   Use the instructions provided in the following sections:

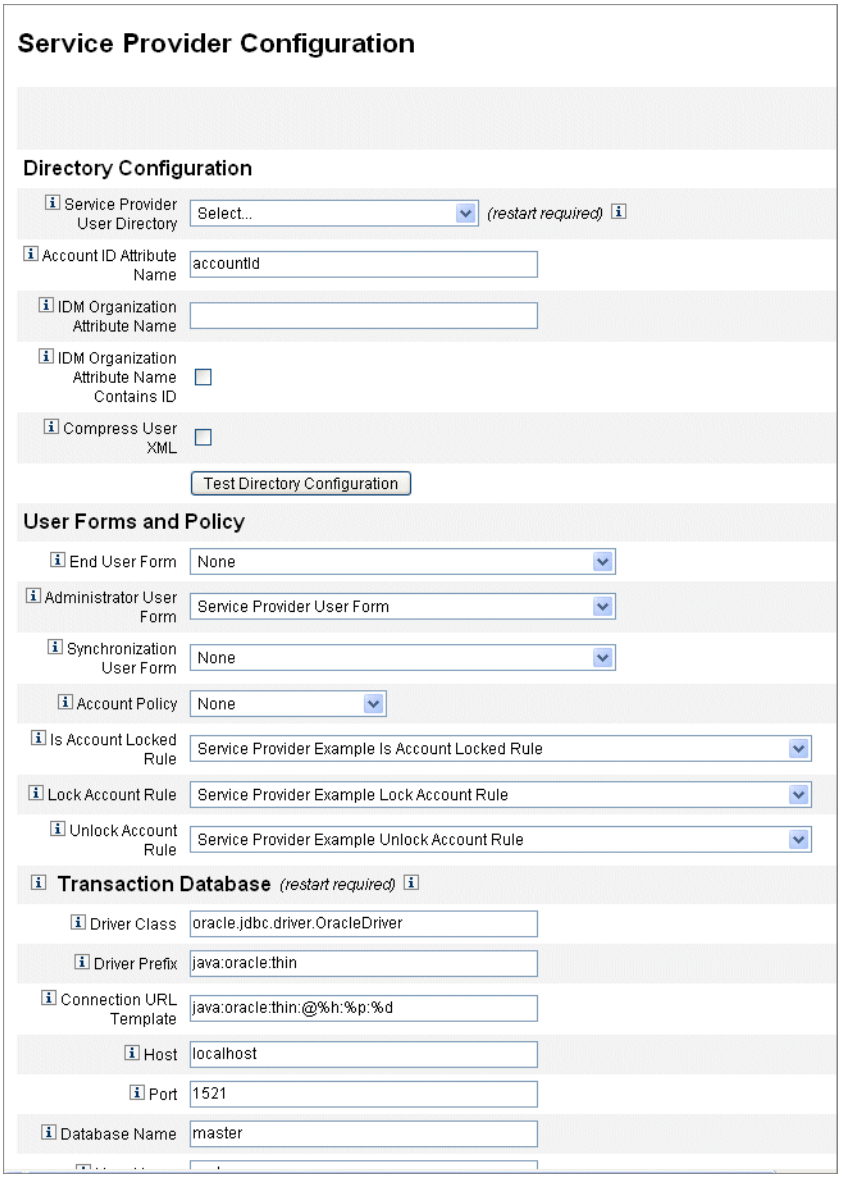
   - “Directory Configuration” on page 485
   - “User Forms and Policy” on page 487
   - “Transaction Database” on page 488
   - “Configuring Tracked Event Configurations” on page 490
   - “Synchronization Account Indexes” on page 491
   - “Callout Configuration” on page 492

Directory Configuration

In the Directory Configuration section, provide information to configure the LDAP Directory and specify Waveset attributes for service provider users.

Figure 17–1 shows this area of the Service Provider Configuration page, as well as the User Forms and Policy area discussed in the next section.

FIGURE 17–1 Service Provider Configuration (Directory, User Forms and Policy)



Service Provider Configuration

Directory Configuration

Service Provider User Directory	Select... (restart required)
Account ID Attribute Name	accountId
IDM Organization Attribute Name	
IDM Organization Attribute Name Contains ID	□
Compress User XML	□

User Forms and Policy

End User Form	None
Administrator User Form	Service Provider User Form
Synchronization User Form	None
Account Policy	None
Is Account Locked Rule	Service Provider Example Is Account Locked Rule
Lock Account Rule	Service Provider Example Lock Account Rule
Unlock Account Rule	Service Provider Example Unlock Account Rule

Transaction Database (restart required)

Driver Class	oracle.jdbc.driver.OracleDriver
Driver Prefix	java:oracle:thin
Connection URL Template	java:oracle:thin:@%h:%p:%d
Host	localhost
Port	1521
Database Name	master

▼ To Complete the Directory Configuration Form

1 **Select the Service Provider End-User Directory from the list.**

Select the LDAP directory resource where all Service Provider user data is stored.

2 **Enter the Account ID Attribute Name.**

This is the name of the LDAP account attribute that contains a unique short identifier for the account. This is considered the name of the user for authentication and account access through the API. The attribute name must be defined in the schema map.

3 **Specify an IDM Organization Attribute Name.**

This option specifies the name of the LDAP account attribute that contains the name or ID of an organization within Waveset to which the LDAP account belongs. It is used for delegated administration of LDAP accounts. The attribute name must exist in the LDAP resource schema map and is the Waveset system attribute name (the name on the left side of the schema map).

Note – Specify the Waveset Organization Attribute Name (and IDM Organization Attribute Name Contains ID, if needed) if you want to enable delegated administration through organization authorization.

4 **If you choose to select IDM Organization Attribute Name Contains ID, enable this option.**

Select this option if the LDAP resource attribute, that refers to the Waveset organization to which the LDAP account belongs, contains the ID of the Waveset organization, and not the name.

5 **If you choose to select Compress User XML, enable this option.**

Select this option if you choose to compress user XML stored in the directory.

6 **Click Test Directory Configuration to verify your entries for the configuration.**

Note – You may test your Directory, Transaction, and Audit Configurations as appropriate to your needs. To fully test all three, click all three tests configuration buttons.

User Forms and Policy

In the User Forms and Policy area, shown in Figure 17–1 above, specify the forms and policies to use for service provider user administration.

▼ To Specify Forms And Policies for Service Provider User Administration

1. **Select the End User Form from the list.**

   This form is used everywhere except for the Delegated Administrator pages and during synchronization. If None is selected, no default user form is used.

2. **Select the Administrator User Form from the list.**

   This is the default user form that is used in Administrator contexts. This includes the Service Provider Accounts edit pages. If None is selected, no default user form is used.

   Note – If you do not choose an Administrator User Form, then administrators will not be able to create or edit Service Provider users from Waveset.

   ---

3. **Select a Synchronization User Form from the list.**

   The Synchronization User Form is the default form used if no form is specified for a resource running Service Provider synchronization. If an input form is specified on a resource's synchronization policy, that form will be used instead. Resources usually require different synchronization input forms. In this case, you should set the synchronization user form on each resource instead of selecting a form from the list.

4. **Select an Account Policy from the list.**

   The choices include any Identity Account Policy defined through Configure > Policies.

5. **Select an Is Account Locked Rule from the list.**

   Select a rule to be run against the Service Provider User view that can determine if an account is locked.

6. **Select a Lock Account Rule.**

   Select a rule to be run against the Service Provider User view that can set attributes in the view that cause the account to be locked.

7. **Select a Unlock Account Rule.**

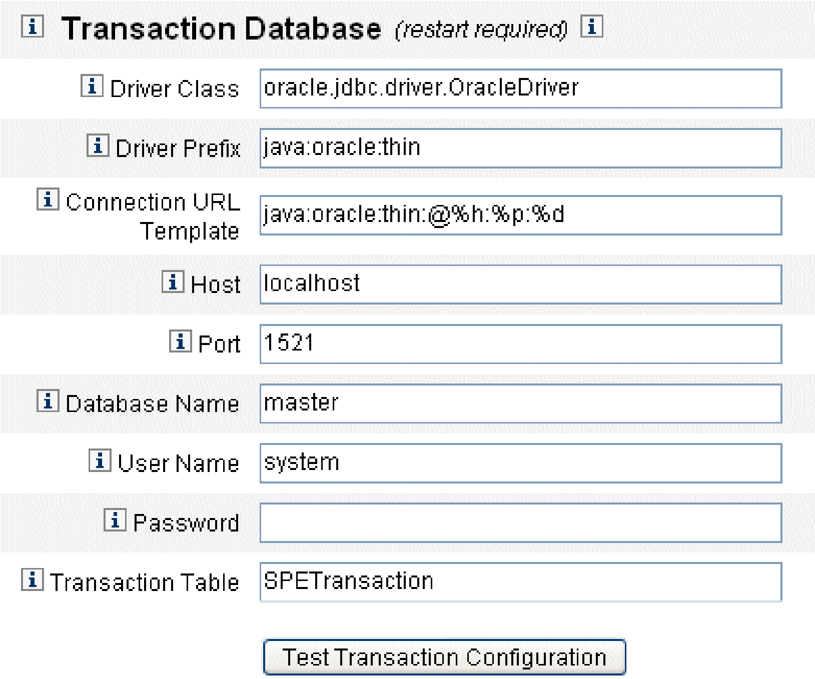
   Select a rule to be run against the Service Provider User view that can set attributes in the view that cause the account to be unlocked.

Transaction Database

Use this section of the Service Provider Configuration page, shown in Figure 17–2, to configure a transaction database. These options are required only when using the JDBC Transaction Persistent Store. Changing any of these values requires that you restart the server to apply them.

The database table for transactions must be set up according to the schema shown in the `create_spe_tables` DDL scripts (located in the `sample` directory of your Waveset installation). The appropriate script may have to be customized for the target environment.

FIGURE 17–2 Service Provider Configuration (Transaction Database)



Transaction Database *(restart required)*

Driver Class	oracle.jdbc.driver.OracleDriver
Driver Prefix	java:oracle:thin
Connection URL Template	java:oracle:thin:@%h:%p:%d
Host	localhost
Port	1521
Database Name	master
User Name	system
Password	
Transaction Table	SPETransaction

To Configure a Transaction Database

1 **Enter the database information.**

Complete the following fields:

- **Driver Class**. Specify the JDBC Driver class name.
- **Driver Prefix**. This field is optional. If specified, the JDBC DriverManager is queried before registering a new driver.
- **Connection URL Template**. This field is optional. If specified, the JDBC DriverManager is queried before registering a new driver.
- **Host**. Enter the name of the host where the database is running.
- **Port**. Enter the port number the database server is listening on.

- **Database Name**. Enter the name of the database to use.
- **User Name**. Enter the ID of a database user with permission to read, update, and delete rows from the transaction and audit tables in the selected database.
- **Password**. Enter the database user password.
- **Transaction Table**. Enter the name of the table in the selected database to use for storing pending transactions.

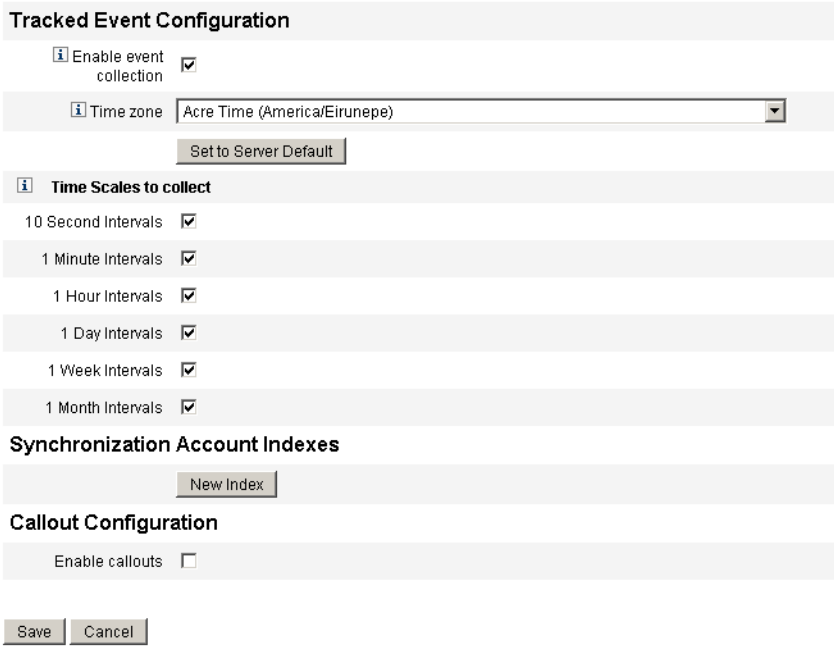
2 **If appropriate, click Test Transaction Configuration to verify your entries.**

Continue to the next section of the Service Provider Configuration page to configure tracked events.

Configuring Tracked Event Configurations

When event collection is enabled, it allows you to track statistics in real time thereby helping to maintain expected or agreed-upon levels of service. Event collection is enabled by default, as shown in Figure 17–3. Clearing the Enable event collection check box disables collection.

FIGURE 17–3 Service Provider Configuration (Tracked Events, Account Indexes, and Callout Configuration)



Tracked Event Configuration

Enable event collection ☑

Time zone Acre Time (America/Eirunepe)

Time Scales to collect

10 Second Intervals ☑

1 Minute Intervals ☑

1 Hour Intervals ☑

1 Day Intervals ☑

1 Week Intervals ☑

1 Month Intervals ☑

Synchronization Account Indexes

Callout Configuration

Enable callouts □

▼ To Specify a Time Zone and Collection Intervals for Service Provider Tracked Events

1 **Select the Time zone from the list.**

Select the time zone to use when recording tracked events, or select Set to Server Default to use the time zone set on the server.

2 **Select the Time Scales to collect options.**

Collection is aggregated over the following time intervals: every 10 seconds, every minute, every hour, daily, weekly, and monthly. Disable any of the intervals for which you do not want collection to occur.

Synchronization Account Indexes

When synchronizing resources in a Service Provider implementation, it may be necessary to define Account Indexes to properly correlate events sent by the resource to users in the Service Provider directory.

By default, resource events are required to contain a value for the attribute accountId which matches the accountId attribute in the directory. In some resources, accountId is not consistently sent. For example, delete events from Active Directory contain only the Active Directory generated account GUID.

Resources that do not include the accountId attribute must include a value for either of the following attributes.

- **guid**. This attribute typically contains a system generated unique identifier.
- **identity**. This attribute is normally the same as accountId for all resources except LDAP resources, where identity contains the full DN of the object.

If you need to correlate using either guid or identity you must define an account index for those attributes. An index is simply the selection of one or more directory user attributes that may be used to store resource specific identities. Once the identities are stored in the directory, they can be used in search filters to correlate synchronization events.

To define account indexes, first determine which resources will be used for synchronization, and which of those require an index. Then edit the Resource definition for the Service Provider directory and add attributes in the schema map for the GUID or identity attributes for each of the Active Sync resources. For example, if you were synchronizing from Active Directory, you might define an attribute named AD-GUID mapped to an unused directory attribute such as manager.

▼ To Define Index Attributes for a Resource

After defining all of the index attributes in the Service Provider resource, perform the following steps:

1 **In the Synchronization Account Indexes area of the configuration page, click the New Index button.**

The form expands to contain a resource selection field, followed by two attribute selection fields. The attribute selection fields remain empty until a resource is selected

2 **Select a Resource from the list.**

The attributes fields now contain values defined in the schema map for the selected resource.

3 **Select the appropriate index attribute for either the Guid Attribute or the Full Identity Attribute.**

It is not usually necessary to set both. If both are set, the software first attempts to correlate using the GUID, then the full identity.

4 **You may click New Index again to define index attributes for other resources.**

5 **To delete an index, click the Delete button to the right of the Resource selection field.**

Deleting an index only removes the index from the configuration, it does not modify all of the existing directory users that may currently have values stored in the index attributes.

Note – Deleting an index only removes the index from the configuration, it does not modify all of the existing directory users that may currently have values stored in the index attributes.

Callout Configuration

Select this option in the Callout Configuration section to enable callouts. When callouts are enabled, the callout mappings appear enabling you to select pre-operational and post-operational options for each transaction type listed.

By default, the pre- and post-operation options are set to None.

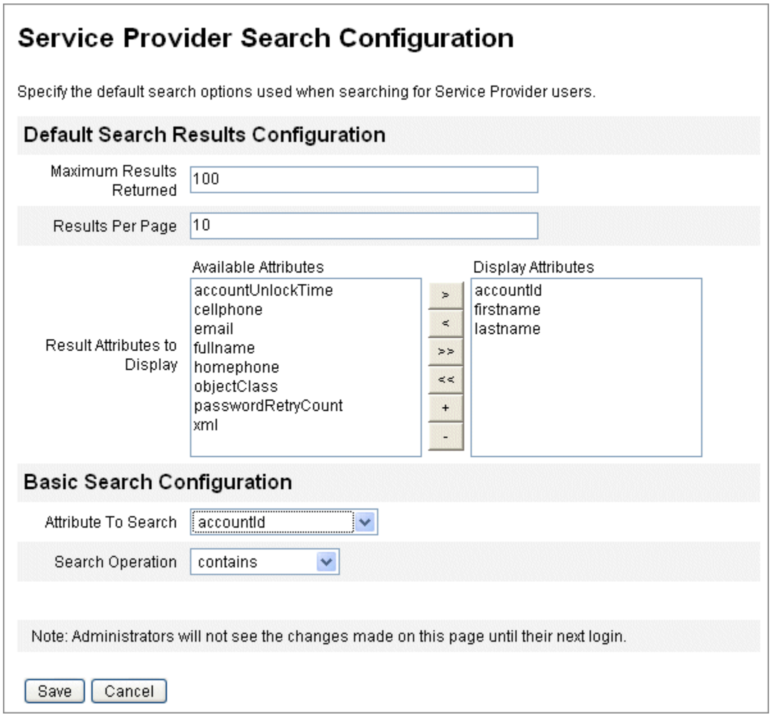
If you specify post-operation callouts, use the Wait for post-operation callout option to specify that the transaction must wait for the post-operation callout processing to complete before finishing. This ensures that any dependent transaction is executed only after the post-operation callout has successfully completed.

Note – After completing your selections for all sections on the Service Provider Configuration page, click Save to complete the configuration.

Edit User Search Configuration

Use this page, shown in Figure 17–4, to configure the default search settings for searches made by delegated administrators on the Manage Service Provider Users page. These defaults apply to all users of the Manage Service Provider Users page, but they can be overridden on a per-session basis.

FIGURE 17–4 Search Configuration



Service Provider Search Configuration

Specify the default search options used when searching for Service Provider users.

Default Search Results Configuration

Maximum Results Returned: 100

Results Per Page: 10

Result Attributes to Display

Available Attributes: accountUnlockTime, cellphone, email, fullname, homephone, objectClass, passwordRetryCount, xml

Display Attributes: accountId, firstname, lastname

Basic Search Configuration

Attribute To Search: accountId

Search Operation: contains

Note: Administrators will not see the changes made on this page until their next login.

▼ To Configure Default Search Settings for Searching Service Provider Users

1. **Click Service Provider from the menu bar.**

2. **Click Edit User Search Configuration.**

3. **Enter a number for Maximum Results Returned (default 100).**

4. **Enter a number for Results Per Page (default 10).**

5 **Select the Available Attributes next to Result Attributes to Display using the arrow keys.**

6 **Select the Attribute to search from the list.**

7 **Select the Search Operation from the list.**

8 **Click Save.**

Note – Changes made to the search configuration do not take effect until you log off and log back on.

These configuration objects are not available if the Service Provider Directory has not been configured.

Transaction Management

A transaction encapsulates a single provisioning operation, for example creating a new user or assigning new resources. To ensure that these transactions complete when resources are unavailable, they are written to the Transaction Persistent Store.

The following topics in this section contain procedures for managing service provider transactions:

- "Setting Default Transaction Execution Options" on page 494
- "Setting Transaction Persistent Store" on page 497
- "Set Advanced Transaction Processing Settings" on page 498
- "Monitoring Transactions" on page 500

Setting Default Transaction Execution Options

These options control how transactions are executed, including synchronous/asynchronous processing and when they are persisted to the Transaction Persistent Store. They can be overridden in the IDMXUser view or through the form used to process it. For more information, see *Oracle Waveset Service Provider 8.1.1 Deployment*.

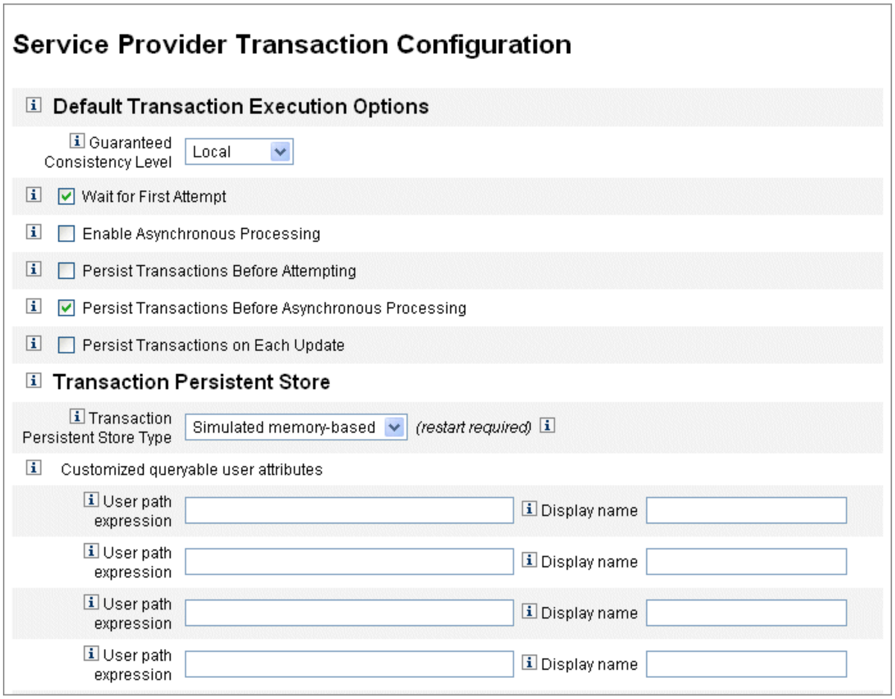
▼ To Configure Service Provider Transactions

1 **Click Service Provider → Edit Transaction Configuration.**

The Service Provider Transaction Configuration page appears.

Figure 17–5 shows the Default Transaction Execution options area.

FIGURE 17–5 Transaction Configuration



Service Provider Transaction Configuration

Default Transaction Execution Options

Guaranteed Consistency Level: Local

☑ Wait for First Attempt

□ Enable Asynchronous Processing

□ Persist Transactions Before Attempting

☑ Persist Transactions Before Asynchronous Processing

□ Persist Transactions on Each Update

Transaction Persistent Store

Transaction Persistent Store Type: Simulated memory-based *(restart required)*

Customized queryable user attributes

User path expression		Display name	
User path expression		Display name	
User path expression		Display name	
User path expression		Display name	

2 **Select the appropriate Guaranteed Consistency Level options to specify the level of transaction consistency for user updates.**

These options include:

- **None**. No guaranteed ordering of resource updates for a user.
- **Local**. Resource updates for a user being processed by the same server are guaranteed to be ordered.
- **Complete**. All resource updates for a user are guaranteed to be in order, across all servers. This option requires all transactions to be persisted before attempting the transaction or before asynchronous processing.

3 **Enable the Default Transaction Execution options as needed.**

These options include:

- **Wait for First Attempt**. Dictates how control returns to the caller when an IDMXUser view object is checked in. If the option is enabled, the check-in operation is blocked until the provisioning transaction has completed a single attempt. If asynchronous processing is disabled, then the transaction either succeeds or fails when control is returned. If asynchronous processing is enabled, then the transaction continues to be retried in the background. If the option is disabled, the check-in operation returns control to the caller before attempting the provisioning transaction. Consider enabling this option.
- **Enable Asynchronous Processing**. This option controls whether processing of provisioning transactions continues after the check-in call returns.

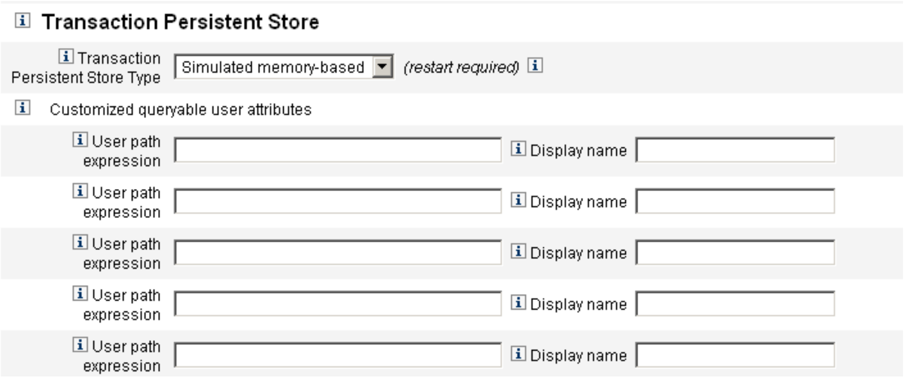
  Enabling asynchronous processing allows the system to retry transactions. It also improves throughput by allowing the worker threads configured in "Set Advanced Transaction Processing Settings" on page 498 to run asynchronously. If you select this option, configure the retry intervals and attempts for the resources being provisioned to or updated using the synchronization input form.

  When you select Enable Asynchronous Processing, enter a Retry Timeout value. This is an upper bound expressed in milliseconds of how long the server retries a failed provisioning transaction. This setting complements the retry settings on the individual resources, including the Service Provider user LDAP directory. For example, if this limit is reached before the resource retry limits are reached, the transaction is aborted. If the value is negative, then the number of retries is only limited by the settings of the individual resources.
- **Persist Transactions Before Attempting**. If enabled, provisioning transactions are written to the Transaction Persistent Store before they are attempted. Enabling this option might incur unnecessary overhead because most provisioning transactions succeed on the first attempt. Consider disabling this option unless the Wait for First Attempt option is disabled. This option is not available if Complete consistency level is selected.
- **Persist Transactions Before Asynchronous Processing**(*default selection*). If enabled, provisioning transactions are written to the Transaction Persistent Store before they are processed asynchronously. If the Wait for First Attempt option is enabled, then transactions that need to be retried are persisted before control is returned to the caller. If the Wait for First Attempt option is disabled, then transactions are always persisted before they are attempted. It is recommended to enable this option. This option is not available if Complete consistency level is selected.
- **Persist Transactions on Each Update**. If enabled, provisioning transactions are persisted after each retry attempt. This can aid in isolating problems because the Transaction Persistent Store, which is searchable from the Search Transaction page, is always up-to-date.

Setting Transaction Persistent Store

The options on the Service Provider Transaction Configuration page apply to the Transaction Persistent Store. The type of store can be configured as well as additional queryable attributes to expose in the store, as shown in the following figure.

FIGURE 17–6 Configuring Service Provider Transaction Persistent Store



Transaction Persistent Store

Transaction Persistent Store Type: Simulated memory-based (restart required)

Customized queryable user attributes

User path expression | Display name

User path expression | Display name

User path expression | Display name

User path expression | Display name

User path expression | Display name

▼ To Set Options on the Service Provider Transaction Configuration Page

1 **Select the desired Transaction Persistent Store Type from the list.**

If the Database option is selected, then the RDBMS configured on the main Service Provider configuration page is used for persisting provisioning transactions. This guarantees transactions that must be retried are not lost when a server is restarted. Selecting this option requires configuring the RDBMS on the main Service Provider configuration page. If the Simulated memory-based option is selected, then transactions that require retry are only stored in memory and are lost when the server restarts. Enable the Database option for production environments.

Note – Memory-based transaction persistent store is not suitable for use in clustered environments.

When Transaction Persistent Store Type is changed, you must restart all running Waveset instances for the change to take effect.

---

2 **If desired, enter Customized queryable user attributes.**

Select additional attributes of the IDMXUser object to expose in transaction summaries. These attributes are queryable from the search transaction page and appear in search results.

These attributes include:

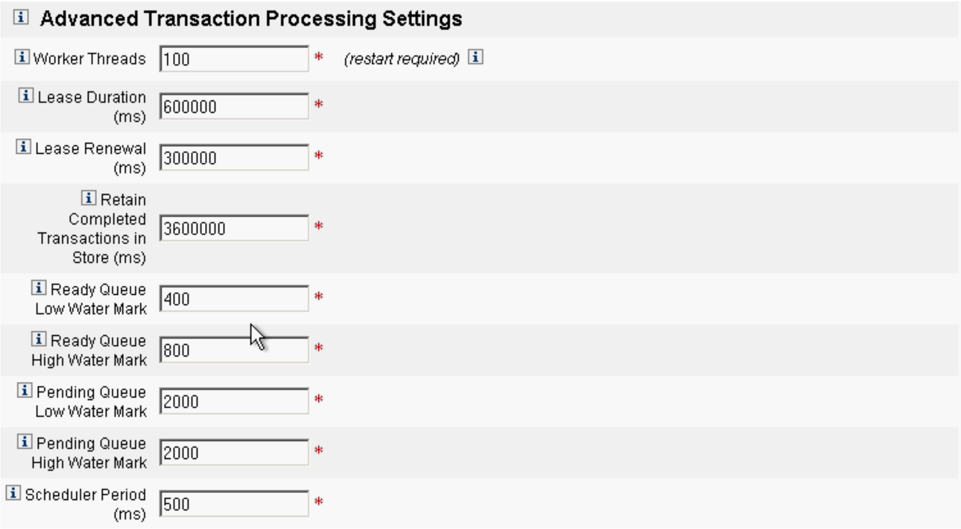
- **User path expression**. Enter a path expression into the IDMXUser object.
- **Display name**. Choose a display name corresponding to the path expression. This display name is shown on the transaction search page.

Set Advanced Transaction Processing Settings

These advanced options control the inner-workings of the transaction manager. Do not change the provided defaults unless performance analysis indicates they are not optimal. All entries are required.

Figure 17–5 illustrates the Advanced Transaction Processing Settings area on the Edit Transaction Configuration page.

FIGURE 17–7 Advanced Transaction Processing Settings



Advanced Transaction Processing Settings

Worker Threads	100 *	*(restart required)*
Lease Duration (ms)	600000 *	
Lease Renewal (ms)	300000 *	
Retain Completed Transactions in Store (ms)	3600000 *	
Ready Queue Low Water Mark	400 *	
Ready Queue High Water Mark	800 *	
Pending Queue Low Water Mark	2000 *	
Pending Queue High Water Mark	2000 *	
Scheduler Period (ms)	500 *	

▼ To Specify Advanced Transaction Processing Settings

1 Enter the desired number of Worker Threads (default 100).

This is the number of threads used to process transactions. This value limits the number of transactions that are processed concurrently. These threads are statically allocated at startup.

Note – When the Worker Threads setting is changed, you must restart all running Waveset instances for the change to take effect.

2 **Enter the desired Lease Duration (ms) (default 600000).**

This controls how long a server locks a transaction that it is retrying. The lease is renewed as needed. However, if the server does not shutdown cleanly, then another server is not able to lock the transaction until the original server's lease expires. The value should be at least one minute. Setting the value smaller can impact the load on the Transaction Persistent Store.

3 **Enter the Lease Renewal (ms) time (default 300000).**

This controls when the lease of a locked transaction is renewed. It is renewed when there are this many milliseconds remaining on the lease.

4 **Enter the time to Retain Completed Transactions in Store (ms) (default 360000).**

How many milliseconds to wait before removing completed transactions from the Transaction Persistent Store. Unless transactions are configured to be immediately persisted, the Transaction Persistent Store does not contain all completed transactions.

5 **Enter the Ready Queue Low Water Mark (default 400).**

When the transaction scheduler's queue of ready-to-run transactions falls below this limit, it refills the queue with any available ready-to-run transactions up to the high water limit.

6 **Enter the Ready Queue High Water Mark (default 800).**

When the transaction scheduler's queue of ready-to-run transactions falls below the low water mark, it refills the queue with any available ready-to-run transactions up to this limit.

7 **Enter the Pending Queue Low Water Mark (default 2000).**

The transaction scheduler's pending queue holds failed transactions that are pending a retry. If the size of the queue exceeds the high water mark, then all transactions beyond the low water mark, are flushed to the Transaction Persistent Store.

8 **Enter the Pending Queue High Water Mark (default 2000).**

The transaction scheduler's pending queue holds failed transactions that are pending a retry. If the size of the queue exceeds the high water mark, then all transactions beyond the low water mark, are flushed to the Transaction Persistent Store.

9 **Enter the Scheduler Period (ms) (default 500).**

This is how often the transaction scheduler should run. When it runs, the transaction scheduler moves ready-to-run transactions from the pending queue to the ready queue, and performs other periodic duties such as persisting transactions to the Transaction Persistent Store.

10 **Click Save to accept the settings.**

Monitoring Transactions

Service Provider transactions are written to the Transaction Persistent Store. You can search for transactions in the Transaction Persistent Store to view the transaction status.

Note – Using the Edit Transaction Configuration page (see Transaction Management), the administrator can control when transactions are persisted. For instance, they can be persisted immediately, even before they are attempted for the first time.

The Transactions Search page allows you to specify search conditions that enable you to filter the transactions to view based on specific criteria related to the transaction event, such as user, type, status, transaction ID, current state and success or failure of the transaction. This includes transactions that are still being retried, as well as transactions that have already completed. Transactions that have not completed can be cancelled preventing any further attempts.

▼ To Search Transactions

1 **In the Administrator interface, click Server Tasks → Service Provider Transactions.**

The Service Provider Transaction Search page opens, allowing you to specify search conditions.

Note – The search returns only transactions that match *all* of the conditions selected below. This is similar to the Accounts → Find Users page.

---

2 **Configure your search.**

Choose one or more of the following options:

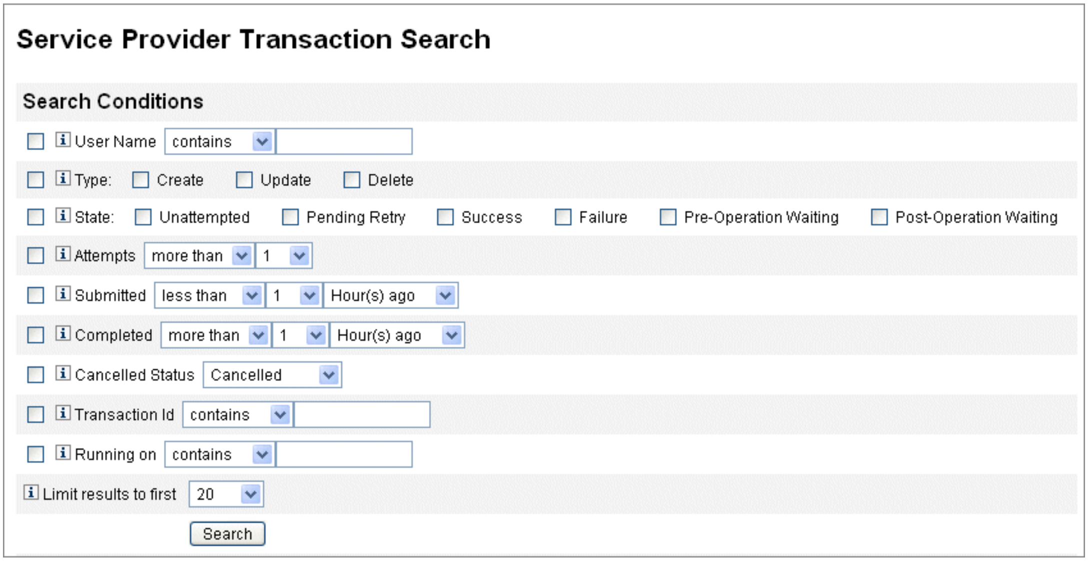
- **User Name**. Allows you to search for transactions that apply only to users with the accountId that you enter.

  Note – If you have configured any Customized queryable user attributes on the Service Provider Transaction Configuration page, then they appear here. For example, you could choose to search based on Last Name or Full Name if these were configured as customized queryable user attributes.

- **Type**. Allows you to search for transactions of the selected type or types.
- **State**. Allows you to search for transactions in the following selected state or states:
  - **Unattempted** transactions have not yet been attempted.

  - **Pending retry** transactions have been attempted one or more times, have had one or more errors, and are scheduled to be retried up to the retry limits configured for the individual resources.
  - **Success** transactions have completed successfully.
  - **Failure** transactions have completed with one or more failures.
- **Attempts**. Allows you to search for transactions based on how many times they have been attempted. Failed transactions are retried up to the retry limits configured for the individual resources
- **Submitted**. Allows you to search for transactions based on when they were initially submitted in increments of hours, minutes, or days.
- **Completed**. Allows you to search for transactions based on when they were completed in increments of hours, minutes, or days.
- **Cancelled Status**. Allows you to search for transactions based on whether or not they have already been cancelled.
- **Transaction ID**. Allows you to search for transactions based on their unique id. Use this option to find a transaction based on the id value you enter, which appears in all audit log records.
- **Running On**. Allows you to search for transactions based on the Service Provider server where they are running. The server's identifier is based on its machine name unless it has been overridden in the `Waveset.properties` file.
- **Limit the search to results to first number of entries selected from the list**. Only results up to the specified limit are returned. No indication is made if additional results are available.

FIGURE 17–8 Search Transactions



Service Provider Transaction Search

Search Conditions

□ User Name contains

□ Type: □ Create □ Update □ Delete

□ State: □ Unattempted □ Pending Retry □ Success □ Failure □ Pre-Operation Waiting □ Post-Operation Waiting

□ Attempts more than 1

□ Submitted less than 1 Hour(s) ago

□ Completed more than 1 Hour(s) ago

□ Cancelled Status Cancelled

□ Transaction Id contains

□ Running on contains

Limit results to first 20

3 **Click Search.**

The search results are displayed.

4 **You can click Download All Matched Transactions at the bottom of the results page to save the results to an XML formatted file.**

Note – To cancel transactions returned in the search results, select the transaction in the results table and click Cancel Selected. You cannot cancel transactions that have completed or have already been cancelled.

Delegated Administration for Service Provider Users

Delegated administration for Service Provider users is enabled through the use of Waveset *admin roles*, or through the organization-based authorization model.

Delegation Through Organization Authorization

Waveset provides delegation of administrative duties through the organization-based authorization model, by default.

Keep the following in mind when creating delegated administrators in an organization-based authorization model:

- Service provider administrators are Waveset users with specific capabilities and controlled organizations.
- The values of the users' organization attributes can either be the name of the Waveset organization or the object ID. This depends on the setting of the Waveset Organization Attribute Name Contains ID field in the Waveset Main Configuration screen.
- You can create an Waveset hierarchy and place organizations in that hierarchy in the way you want to delegate the administration of those organizations. Use specific identification for the organizations instead of the organizations' simple names.
- Service Provider users have their organization taken from user attributes in the directory server.
  - You must set attributes in the schema map for the directory server resource.
  - The comparison of attributes is by *exact match* to an administrator's controlled organization list. The value stored in the directory must match the organizations name, not the entire hierarchy. If an administrator controls `Top:orgA:sub1`, then `sub1` must be the value stored in the organization attribute for the Service Provider user.
  - If the attribute is not set or does not correspond to an Waveset organization, the Service Provider user is treated as a member of the Top organization. This requires that the Service Provider administrators have Service Provider user capabilities in `Top` to manage these users.

  Attribute settings determine the scope for searches by Service Provider administrators.
- To create a delegated administrator account, you first create an Waveset administrator and then add Service Provider administrator capabilities. There are capabilities specific to Service Provider tasks which can be assigned to the user (on the Security Tab of the Edit User page). The controlled organizations specify which Service Provider users the administrator can modify. Any resources available to Service Provider users are available to all Waveset administrators.

Note – For more information about Waveset delegated administration, see "Delegated Administration" on page 184 in Chapter 6, "Administration"

Delegation Through Admin Role Assignment

For granting fine-grain capabilities and scope of control on Service Provider users, use a Service Provider User Admin Role. The Admin Roles can be configured to be dynamically assigned to one or more Waveset or Service Provider Users at login time.

Rules can be defined and assigned to Admin Roles that specify the capabilities (such as `Service Provider Create User`) granted to users assigned the admin role.

To use Admin Role delegation for service provider users, you must enable it in the Waveset system configuration object ("Editing Waveset Configuration Objects" on page 108).

If delegation through Admin Role assignment is enabled, then the IDM Organization Attribute Name in the Service Provider Configuration is not required.

Enabling Service Provider Admin Role Delegation

To enable service provider admin role delegation (Service Provider delegated administration), open the system configuration object for modification ("Editing Waveset Configuration Objects" on page 108) and set the following property to `true`:

`security.authz.external.`*app name*`.`*object type*

where *app name* is the Waveset application (such as Administrator Interface) and *object type* is `Service Provider Users`

This property can be enabled per Waveset application (for example, for the Administrator Interface or User Interface) and per object type. Currently, the only supported object type is `Service Provider Users`. The default value is `false`.

For example, to enable Service Provider Delegated Administration for Waveset administrators, set the following attribute in the System Configuration configuration object to "true":

```
security.authz.external.Administrator Interface.Service Provider Users
```

If Service Provider Delegated Administration is disabled (set to false) for a given Waveset or Service Provider application, the organization-based authorization model is used.

When Service Provider Delegated Administration is enabled, tracked events capture information about the number and duration of authorization rules executed. These statistics are available in the dashboard.

Configuring a Service Provider User Admin Role

To configure a Service Provider User Admin Role, create an admin role and specify the scope of control, capabilities, and to whom it should be assigned.

Note – Before creating a Service Provider User Admin Role, define the search context, search filter, after search filter, capabilities, and user assignment rules for the admin role.

To use the following rules, you must specify the rule's `authType`:

- SPEUsersSearchContextRule
- SPEUsersSearchFilterRule
- SPEUsersAfterSearchFilterRule
- CapabilitiesOnSPEUserRule

- UserIsAssignedAdminRoleRule
- SPEUserIsAssignedAdminRoleRule

Waveset provides sample rules that you can use to create these rules for Service Provider User Admin Roles. These rules are available in `sample/adminRoleRules.xml` in the Waveset installation directory.

For more information about creating these rules for your environment, see *Oracle Waveset Service Provider 8.1.1 Deployment*.

▼ To Configure a Service Provider User Admin Role

1. **In the Administrator interface, click Security on the menu, then click Admin Roles.**

   The Admin Roles page opens.

2. **Click New.**

   The Create Admin Role page opens.

3. **Specify a name for the admin role and select Service Provider Users for the type.**

4. **Specify the Scope of Control, Capabilities, and Assign To Users options, as described in the following sections.**

Specifying the Scope of Control

The scope of control for the service provider user admin role specifies which service provider users a given Waveset administrator, Waveset end user, or Oracle Waveset service provider end user is allowed to see. It is enforced when a request is made to list Service Provider Users in the directory.

You can specify one or more of the following settings for the Service Provider User Admin Role scope of control:

- **User search context**. Specify whether a rule or text string is to be used to begin a search.

  If None is specified, the default search context will be the base context specified in the Oracle Waveset Resource configured as the Service Provider User directory.

- **User search filter**. Specify whether a rule or a text string that is to be applied for the search filter.

  The text string specified or returned by the selected rule should be an LDAP-compliant search filter string that represents the set of users, within the search context, that will be controlled by users assigned this Admin Role. The specified filter will be combined with the user specified search filter to ensure that users returned from the search do not include any users that users assigned this AdminRole are not authorized to list.

- **After user search filter rule**. Select a rule that will be applied after the User search filter is applied.

  This rule is run after the initial LDAP search is performed against the Service Provider User directory and evaluates the results to determine which distinguished names (dn) the requesting user is allowed to access.

  This type of rule can be used when you need to determine if a user should be in the requesting user's scope of control using non-LDAP user attributes (for example, group membership), or when the filter decision needs to be made using a repository other than the Service Provider User directory (for example, an Oracle database or RACF).

Specifying Capabilities

Capabilities for the Service Provider User Admin Role specify which capabilities and rights the requesting user has on the Service Provider User for which access is being requested. It is enforced when a request is made to view, create, modify, or delete a Service Provider User.

On the Capabilities tab, select the Capabilities Rule to apply for this admin role.

Assigning Admin Roles To Users

Service Provider User Admin Roles can be dynamically assigned to service provider users by specifying a rule that will be evaluated at login time to determine whether to assign the authenticating user the Admin Role.

Click the Assign To Users tab, and select the rule to apply for the assignment.

Note – Dynamic assignment of Admin Roles to users must be enabled for each login interface (for example, the User interface and the Administrator interface) by setting the following System Configuration object ("Editing Waveset Configuration Objects" on page 108) to `true`:

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*logininterface*

The default for all interfaces is `false`.

Delegating Service Provider User Admin Roles

By default, Service Provider Users can assign (or *delegate*) Service Provider User Admin Roles assigned to them to other Service Provider Users in their scope of control.

In fact, any Waveset User with capabilities to edit Service Provider Users can assign the Service Provider User Admin Roles assigned to them to the service provider users in their scope of control.

A Service Provider User Admin Role can also include a list of *Assigners* who can assign the Admin Role regardless of scope of control. These direct assignments can ensure that at least one known user account can assign the Admin Role.

Administering Service Provider Users

This section describes procedures and information for administering Service Provider users through Waveset.

This section contains the following topics:

- "User Organizations" on page 507
- "Create Users and Accounts" on page 507
- "Search Service Provider Users" on page 510
- "End-User Interface" on page 515

User Organizations

With Service Provider, the value of an attribute on the user determines to which organization the user is assigned. This is specified by the Waveset Organization Attribute Name field in the Service Provider Main configuration (see "Initial Configuration" on page 485). However, the names of those organizations must match the value of a user attribute assigned in the directory server.

If the Waveset Organization Attribute Name is defined, then a multi-select list of available organizations appears on the Create User and Edit User pages. The short organization names are displayed by default. You can modify the Service Provider User Form to display the full organization path.

You may pick which attribute becomes the organization name attribute. The organization name attribute is then used in the Service Provider user administration pages to constrain which administrators can search for and manage that user.

Note – There are now account ID and password policies for Service Provider and resource accounts.

The Service Provider System Account Policy is available from the main Policies table.

Create Users and Accounts

All service provider users must have an account in the Service Provider directory. If a user has accounts on other resources, then links to these accounts are stored in the user's directory entry, so information about these accounts is available when the user is viewed.

Note – A sample Service Provider User Form for creating and editing users is provided. Customize this form to meet the requirements for managing users in your Service Provider environment. For more information, see Chapter 2, “Waveset Forms,” in *Oracle Waveset 8.1.1 Deployment Reference*.

▼ To Create a Service Provider Account

1. **In the Administrator interface, click Accounts on the menu bar.**

2. **Click the Manage Service Provider Users tab.**

3. **Click Create User.**

   Note – When using the default Service Provider User Form the actual fields that are displayed depend on the attributes configured in the Account Attributes table (Schema map) of the Service Provider directory resource. Also, when you assign resources to the user (such as a delegated administrator), you should see new sections added to the display where you can specify values for the attributes for those resources. You may also customize the fields.

4. **Specify attribute values for these resources as required.**

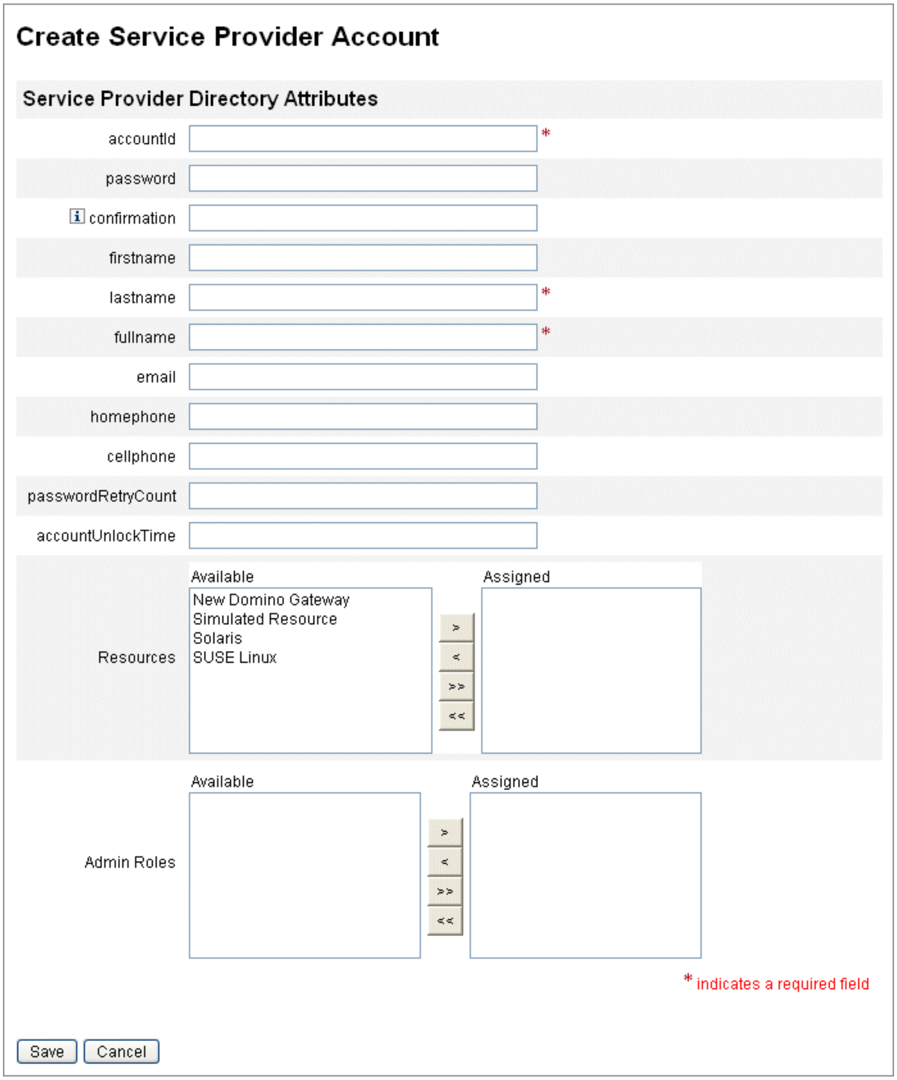
   These attribute values include:

   - **accountid** (*required*)
   - **password**
   - **confirmation** (password confirmation)
   - **firstname** (*required*)
   - **lastname** (*required*)
   - **fullname**
   - **email**
   - **home phone**
   - **cell phone**
   - **password retry count**
   - **account unlock time**

5. **Assign any desired Resources from the Available listing by using the arrow keys.**

6. **The Account Status displays whether the account is locked or unlocked. Click this option to lock or unlock the account.**

FIGURE 17–9 Create Service Provider Users and Accounts



Note – This form automatically populates values for the resource account attributes based on the attributes defined for the directory account (at the top). For example, if the resource defines `firstName`, then the product populates it with the `firstName` value from the directory account. However, after this initial population, modifications to these attributes are not propagated to the resource accounts. If desired, customize the provided sample Service Provider User Form.

7 **Click Save to create the user account.**

Search Service Provider Users

Service Provider includes a configurable search capability to aid in administering user accounts. Only the users within your scope, (as defined by your organization, and perhaps other factors) are returned in a search.

To perform a basic search of service provider users, from the Accounts area in the Waveset interface, click Manage Service Provider Users, then enter the search value and click Search.

The following topics discuss the Service Provider search features:

- "Advanced Search" on page 510
- "Search Results" on page 511
- "Link Accounts" on page 512
- "Delete, Unassign, or Unlink Accounts" on page 513
- "Set Search Options" on page 514

Advanced Search

Use the following instructions to perform an Advanced Search of Service Provider users.

▼ To Perform an Advanced Search of Service Provider Users

1 **From the Service Provider Users Search page, click Advanced.**

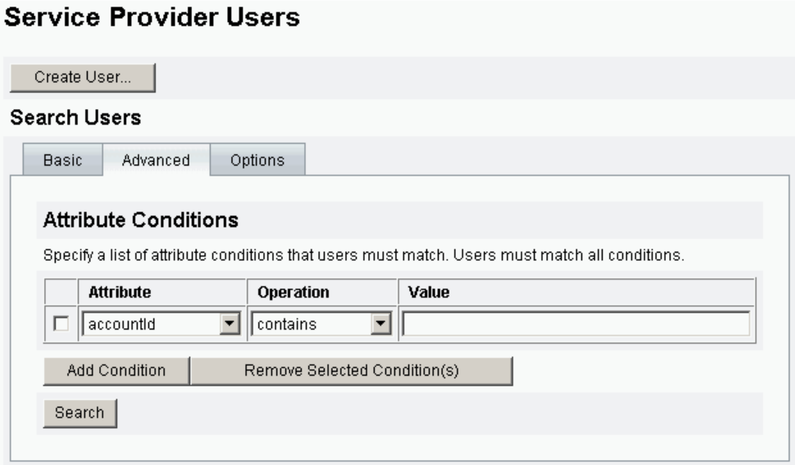
2 **Choose the desired Attribute from the list.**

3 **Choose the desired Operation from the list.**

You are specifying a set of conditions in order to filter the users returned from the search and that the users returned must meet all of the specified conditions.

4 **Enter the desired search value, and then click Search.**

FIGURE 17–10 Search Users



Service Provider Users

Search Users

Attribute Conditions

Specify a list of attribute conditions that users must match. Users must match all conditions.

	Attribute	Operation	Value
□	accountId	contains	

You can add or remove Attribute Conditions, using the following options:

- Click Add Condition and specify the new attribute.
- Select the item and click Remove Selected Conditions.

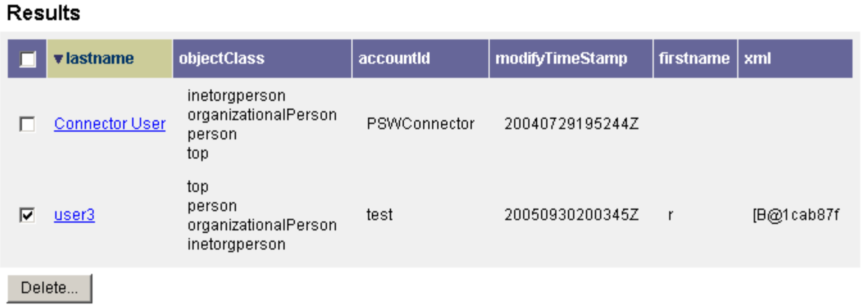
Search Results

Service Provider search results are displayed in a table, as depicted in Figure 17–11. The results can be sorted by any attribute by clicking on the column header for that attribute. The results displayed depend on the attributes you selected.

The arrow buttons navigate to the first, previous, next, and last pages of results. You can jump to a specific page by entering the number in the text box and pressing Enter.

To edit a user, click the user name in the table.

FIGURE 17–11 Example of Search Results



Results

☐	▾lastname	objectClass	accountId	modifyTimeStamp	firstname	xml
☐	Connector User	inetorgperson organizationalPerson person top	PSWConnector	20040729195244Z		
☑	user3	top person organizationalPerson inetorgperson	test	20050930200345Z	r	[B@1cab87f

The search results page enables you to delete users or unlink resource accounts, by selecting one or more users and clicking the Delete button. This action brings up a delete user page and presents additional options (see "Delete, Unassign, or Unlink Accounts" on page 513)

Link Accounts

Service Provider may be installed in environments in which users have accounts on multiple resources. The account linking feature of Service Provider enables you to assign existing resource accounts to Service Provider users in an incremental fashion. The account linking process is controlled by the Service Provider linking policy, which defines a link correlation rule, a link confirmation rule, and a link verification option.

▼ To Link User Accounts

1. **In the Administrator interface, click Resources in the menu bar.**

2. **Select the desired resource.**

3. **Select Edit Service Provider Linking Policy from the Resources Action menu.**

4. **Select a link correlation rule. This rule searches for accounts on the resource that the user may own.**

5. **Select a link confirmation rule. This rule eliminates any resource accounts from the list of potential accounts that the link correlation rule selects.**

   Note – If the link correlation rule selects no more than one account, then the link confirmation rule is not required.

   ---

6. **Select Link verification required to link the target resource account to the Service Provider user.**

Delete, Unassign, or Unlink Accounts

▼ To Delete, Unassign, or Unlink User Accounts

1. **Click Accounts from the menu bar.**

2. **Click Manage Service Provider Users.**

3. **Perform a basic or advance search.**

4. **Select the desired user or users.**

5. **Click the Delete button.**

6. **Select one of the optional global options.**

   These options include:

   - **Delete All resource accounts**

     Note – Deleting a resource deletes the account, but the resource assignment still exists. A subsequent update of the user recreates the account. Delete always implies an unlink of the resource account.

   - **Unassign All resource accounts**

     Note – Unassigning a resource removes that resource assignment. Unassign implies an unlink of the resource account. The resource account is not deleted when the resource is unassigned.

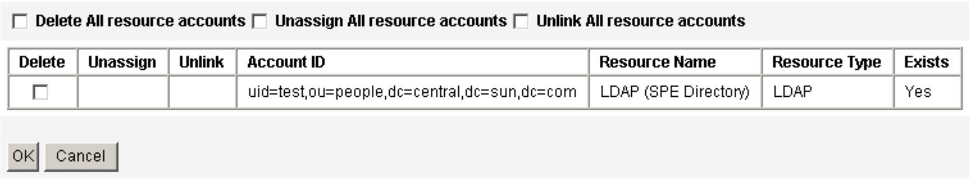
   - **Unlink All resource accounts**

     Note – Unlinking removes the link between a user and the resource account, but this does not delete the account. The resource assignment is not removed either, so a subsequent update to the user re-links the account or creates a new account on the resource.

7. **Alternatively, select an action for one or more resource accounts in the Delete, Unassign, or Unlink columns.**

8. **After selecting the desired user accounts, click OK.**

FIGURE 17–12 Delete, Unassign, or Unlink Accounts



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

Delete	Unassign	Unlink	Account ID	Resource Name	Resource Type	Exists
□			uid=test,ou=people,dc=central,dc=sun,dc=com	LDAP (SPE Directory)	LDAP	Yes

Set Search Options

To Set Search Options for Service Provider Users

1 **In the Administrator interface, click Accounts in the menu bar.**

2 **Click Service Provider.**

3 **Click Options.**

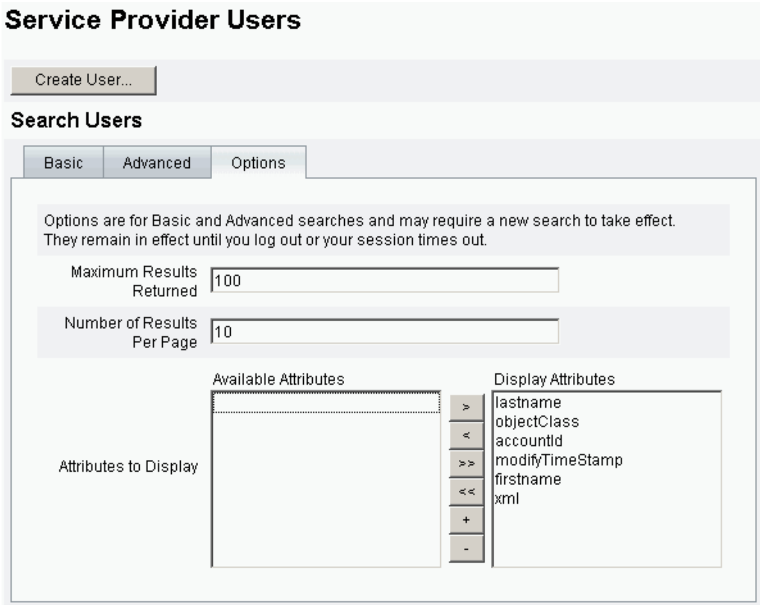
Note – These options are only valid for the current login session. The options effect how the search results are displayed, that they effect both the basic and advanced search results, and that some settings only take effect on new searches.

4 **Enter the Maximum Results Returned.**

5 **Enter the Number of Results Per Page.**

6 **Choose the desired Display Attribute from the Available Attributes using the arrow keys.**

FIGURE 17–13 Set Search Options for Service Provider Users



Options are for Basic and Advanced searches and may require a new search to take effect. They remain in effect until you log out or your session times out.

Maximum Results Returned: 100

Number of Results Per Page: 10

Attributes to Display

Available Attributes

Display Attributes:
lastname
objectClass
accountId
modifyTimeStamp
firstname
xml

End-User Interface

The bundled sample end-user pages provide examples for registration and self-service typical in xSP environments. The samples are extensible and can be customized. You may change the look and feel, modify navigation rules between pages, or display locale-specific messages for your deployment. For further information about customizing end-user pages see *Oracle Waveset Service Provider 8.1.1 Deployment*.

In addition to auditing self-service and registration events, notification to the affected user can be sent using email templates. Examples of using account ID and password policies, as well as account lockout, are also provided. Application developers can also leverage Waveset forms. The modular authentication service implemented as a servlet filter can be extended or replaced if necessary. This allows integration with access management systems like the Oracle Access Manager.

Sample End-User Pages

The bundled sample end-user pages allow the user to register and maintain basic user information through a series of easy-to-navigate screens and receive email notification of their actions.

The example pages include the following features:

- Login (and logout) including authentication using challenge questions
- Registration and enrollment
- Password changing
- User name changing
- Challenge questions changing
- Notification address changing
- User name forgotten handling
- Password forgotten handling
- Email notification
- Auditing

Note – Waveset uses a validation table for registration. Only users in that table are allowed to register. For example, when user Betty Childs registers, an entry for Betty Childs with email address bchilds@example.com, is found in the validation table and registration is accepted.

These pages are easy to customize for your deployment.

You can easily customize these pages for your deployment as follows:

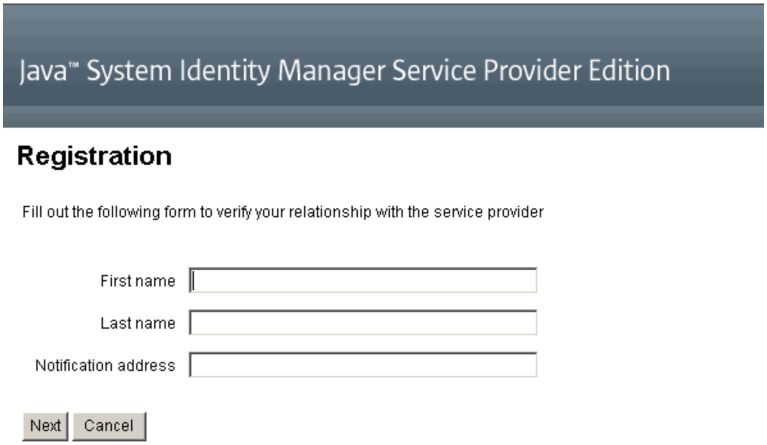
- Change the branding
- Modify the configuration options (for example, the number of failed login attempts)
- Add or remove pages

For more information on customizing the pages see *Oracle Waveset Service Provider 8.1.1 Deployment*.

New User Registration

New users are asked to register. During registration users can set their login, challenge questions, and notification information.

FIGURE 17–14 Registration Page



Registration

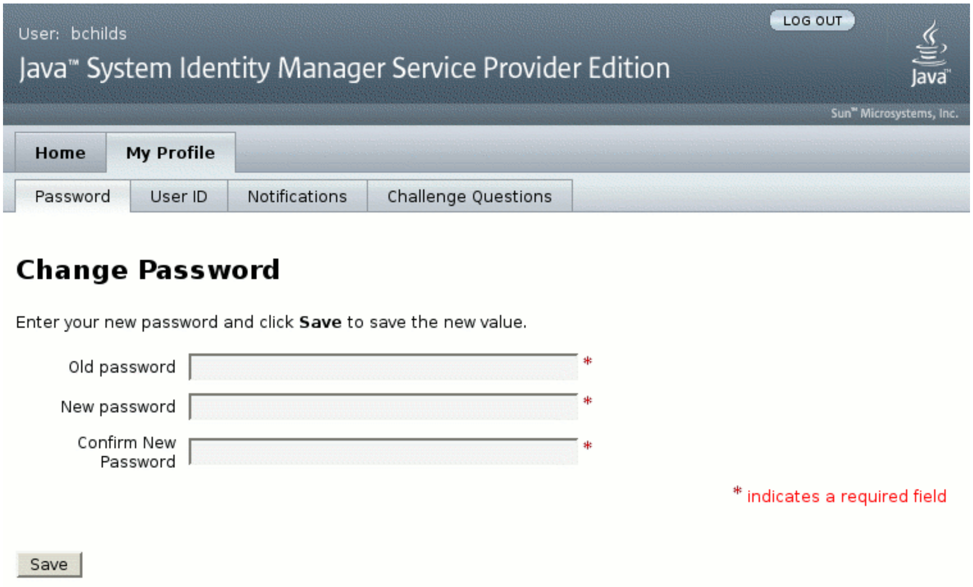
Fill out the following form to verify your relationship with the service provider

First name
Last name
Notification address

Home and Profile Screens

Figure 17–15 shows the end user home tab and Profile page. A user may change their login ID and password, manage notification, and create challenge questions.

FIGURE 17–15 My Profile Page



Change Password

Enter your new password and click **Save** to save the new value.

Old password *
New password *
Confirm New Password *

* indicates a required field

Service Provider User Synchronization

Synchronization for Service Provider users is enabled through the Synchronization Policy. To synchronize changes to attributes on resources with Waveset for service provider users, you must configure Service Provider Synchronization.

The following topics explain how to enable synchronization in a service provider implementation:

- "Configure Synchronization" on page 518
- "Monitor Synchronization" on page 519
- "Start and Stop Synchronization" on page 519
- "Migrate Users" on page 519

Note – Service Provider synchronization is configured from the list of resources in the Resources area of Waveset.

Configure Synchronization

To configure Service Provider synchronization, you edit the Synchronization Policy for resources as described in "To Edit or Configure Synchronization" on page 242.

When editing the Synchronization Policy, the following options must be specified to enable the synchronization processes for service provider users.

- Select Service Provider User as the Target Object Type.
- In the Scheduling Settings section, select Enable Synchronization.

Follow the instructions in "To Edit or Configure Synchronization" on page 242 to specify other options as appropriate for your environment. The default synchronization interval for Service Provider synchronization tasks defaults to 1 minute.

Note – The confirmation rule and form must use the IDMXUser view and not the Waveset input user view (see *Oracle Waveset Service Provider 8.1.1 Deployment* for more information).

This is required because confirmation rules access a user view for each user identified in the correlation rule, impacting synchronization performance.

Click Save to save the policy definition. If synchronization is not disabled in the policy, it will be scheduled as specified. If disable synchronization is specified, the synchronization service is stopped, if currently running. If enabled, synchronization will be started when the Waveset server is restarted, or when Start for Service Provider is selected under the Synchronization Resource Action.

Monitor Synchronization

Waveset provides the following methods for monitoring Service Provider synchronization.

- View the synchronization status in the description field on the Resource list.
- Use the JMX interface to monitor synchronization metrics.

Start and Stop Synchronization

Service Provider synchronization is enabled by default when you configure Waveset for a service provider implementation.

▼ To Disable Service Provider Active Sync

1 **In the Administrator interface, click Resources on the menu.**

The List Resources page opens.

2 **In the Service Provider area, select the resource and click Edit Synchronization Policy to edit the policy.**

3 **Clear the Enable Synchronization check box.**

4 **Click Save.**

When the policy is saved synchronization stops.

To stop synchronization without disabling it, select Stop for Service Provider from the Synchronization resource action.

Note – If you stop synchronization by using the resource action, without disabling synchronization, it will be started again when any Waveset server is started.

Migrate Users

The Service Provider functionality contains an example user migration task and associated scripts. This task migrates existing Waveset users to the Service Provider User directory. This section describes how to use the example migration task. You are encouraged to modify this example for use in your situation.

▼ To Migrate Existing Waveset Users

1. **In the Administrator interface, click Server Tasks on the menu.**

   The Find Tasks page opens.

2. **Click Run Tasks in the secondary menu.**

3. **Click SPE Migration.**

4. **Enter a unique Task Name.**

5. **Select a Resource from the list.**

   This is a resource in Waveset that represents the Service Provider directory server. Links to this resource found in Waveset users are not migrated.

6. **Enter an Identity Attribute.**

   This is the Waveset user attribute that contains the short unique identity for the directory user.

7. **Select an Identity Rule from the list.**

   This is an optional rule that may calculate the name of the directory user from attributes of the Waveset user. The Identity rule can calculate a simple name (typically UID) which is then processed through the identity template of the Resource to form the directory server distinguished Name (DN.) The rule may also return a full specified DN which avoids the id template.

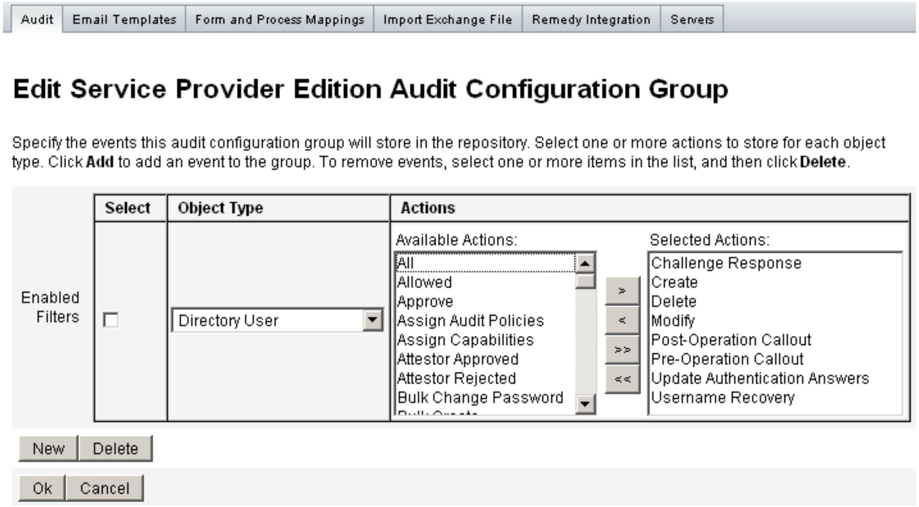
8. **Click Launch to start the background migration task.**

Configuring Service Provider Audit Events

In a Service Provider implementation, Waveset's audit logging system audits events related to extranet user activities. Waveset provides the Service Provider audit configuration group (enabled by default) that specifies the audit events logged for Service Provider users. See Figure 17–16.

For more information about audit logging, and modifying events in the Service Provider audit configuration group, see Chapter 10, "Audit Logging"

FIGURE 17–16 Edit Service Provider Audit Configuration Group Page



Edit Service Provider Edition Audit Configuration Group

Specify the events this audit configuration group will store in the repository. Select one or more actions to store for each object type. Click **Add** to add an event to the group. To remove events, select one or more items in the list, and then click **Delete**.

	Select	Object Type	Actions	
Enabled Filters	□	Directory User	Available Actions: All Allowed Approve Assign Audit Policies Assign Capabilities Attestor Approved Attestor Rejected Bulk Change Password	Selected Actions: Challenge Response Create Delete Modify Post-Operation Callout Pre-Operation Callout Update Authentication Answers Username Recovery

APPENDIX A

lh Reference

This appendix provides information to help you use the Waveset command-line interface and execute Waveset commands.

This information includes the following topics:

- "lh Command Syntax" on page 523
- "lh Command Examples" on page 525
- "syslog Command" on page 525

lh Command Syntax

Use the following syntax to invoke the Waveset command-line interface and execute Waveset commands:

```
lh { $class | $command } [ $arg [$arg... ] ]
```

where:

- class must be a fully qualified class name, such as com.waveset.session.WavesetConsole.
- command must be one of the following commands:
  - assessment can be used during upgrades. Supports subcommands that report on all modified objects and report on all installed version of Waveset. See the *Oracle Waveset 8.1.1 Upgrade* guide for details.
  - config starts the Business Process Editor.
  - console starts the Waveset console.
  - genReports generates a set of random data that can be used to demonstrate Waveset report functionality.
  - import imports an Waveset object. Specify the -s option for strict mode. When strict mode is enabled, reference checking during import is less forgiving.

- js invokes a JavaScript program.
- javascript also invokes a JavaScript program.
- msgtool generates a custom message catalog based off of WPMessages.properties. This catalog can be manipulated to make custom changes to text or languages.
- script executes JavaScript or BeanShell.
- setRepo sets the Waveset index repository.
- setup starts the Waveset setup process, which allows you to set the license key, define the Waveset index repository, and import configuration files.
- spml launches the SPML browser.
- syslog [options] extracts records from the system log. See "syslog Command" on page 525 for details.
- waveset an alias for the console command. See console, above.
- xmlparse validates XML for Waveset objects.
- xpress [options] *Filename* evaluates an expression. Valid option is -trace (enables trace output).

Usage Notes

When working with lh commands, you must be aware of the following notes:

- To view the command usage help, type lh without any arguments.
- When setting the path environment variables for the lh command,
  - Set JAVA_HOME location 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 Oracle (without the JDK), a typical directory location is C:\Program Files\Java\jre1.5.0_14 (or similar). This directory contains the bin directory with the Java executable. In this case, set JAVA_HOME to C:\Program Files\Java\jre1.5.0_14.

    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 C:\java\jdk1.5.0_14\jre.
  - Set the WSHOME variable to the Waveset installation directory, as follows:

    ```
    set WSHOME=<path_to_oracle_waveset_directory>
    ```

    For example, to set the variable to the default installation directory, type:

    ```
    set WSHOME=C:\Program Files\tomcat\webapps\idm
    ```

Note – The WSHOME variable value must *not* contain the following characters:

- Quotation marks (" ")

  Do not use quotation marks, even if the path to the application deployment directory contains spaces.
- A backslash at the end of the path (\)

On UNIX systems, you must also export the path variables by typing:

```
export WSHOME
export JAVA_HOME
```

- To run the command in 64-bit mode, uncomment the FLAGS="$FLAGS -d64" line in the lh script.
- To start the Waveset command-line interface
  - On Windows, type the following at a command line:

    ```
    %WSHOME%\bin\lh
    ```
  - On UNIX, type the following at a command line:

    ```
    $WSHOME/bin/lh
    ```

lh Command Examples

- lh com.waveset.session.WavesetConsole
- lh console
- lh console– u $user– p *PathtoPassword*.txt
- lh setup -U *Administrator* -P *PathtoPassword*.txt
- lh setRepo– c -A *Administrator* -C *PathtoPassword*.txt
- lh setRepo– t *LocalFiles*– f $WSHOME

syslog Command

This section provides information about the syslog command, including:

- "syslog Command Usage" on page 525
- "syslog Command Options" on page 526

syslog Command Usage

Use the following syntax to invoke the syslog command:

```
syslog [options]
```

`syslog` Command Options

Use the following options to include or exclude information.

TABLE A–1 `syslog` Command Options

Option	Description
`-d` *Number*	Shows records for the previous *Number* days (default=1).
`-E`	Shows only records with error severity level or above.
`-F`	Shows only records with fatal severity level.
`-i` *LogID*	Shows only records with a specified syslog ID. Syslog IDs are displayed on some error messages and reference a specific System Log entry.
`-W`	Shows only records with warning severity level or above (default).
`-X`	Includes reported cause of error, if available.

APPENDIX B

Audit Log Database Schema

This appendix provides information about audit data schema values for the supported database types and audit log database mappings.

- "Oracle Database Type" on page 527
- "DB2 Database Type" on page 529
- "MySQL Database Type" on page 531
- "SQL Server Database Type" on page 532
- "Audit Log Database Mappings" on page 534

Oracle Database Type

Table B–4 lists the data schema values for the Oracle database type.

TABLE B–1 Data Schema Values for the Oracle Database Type

Database Column	Value
`id`	`VARCHAR(50) NOT NULL`
`name`	`VARCHAR(128) NOT NULL`
`repomod`	`TIMESTAMP`
`resourceName`	`VARCHAR(128)`
`accountName`	`VARCHAR(50)`
`objectType`	`CHAR(2)`
`objectName`	`VARCHAR(128)`
`action`	`CHAR(2)`
`actionDateTime`	`CHAR(21)`

TABLE B–1 Data Schema Values for the Oracle Database Type *(Continued)*

Database Column	Value
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) or CLOB (See note[1] at end of table.)
acctAttrChanges	VARCHAR(4000) or CLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) or CLOB (See note[1] at end of table.)
sequence	CHAR(19)

TABLE B–1 Data Schema Values for the Oracle Database Type *(Continued)*

Database Column	Value
xmlSize	NUMBER(19,0)
xml	BLOB

Note – The column length limit for these columns is configurable. The default data type is VARCHAR and the default size limit is noted in parentheses. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.

DB2 Database Type

Table B–2 lists the data schema values for the DB2 database type.

TABLE B–2 Data Schema Values for the DB2 Database Type

Database Column	Value
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) or CLOB (See note[1] at end of table.)
acctAttrChanges	CLOB(16M)

TABLE B–2 Data Schema Values for the DB2 Database Type *(Continued)*

Database Column	Value
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) or CLOB (See note[1] at end of table.)
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

Note – The column length limit for these columns is configurable. The default data type is VARCHAR and the default size limit is noted in parentheses. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.

MySQL Database Type

Table B–3 lists the data schema values for the MySQL database type.

TABLE B–3 Data Schema Values for the MySQL Database Type

Database Column	Value
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) or CLOB (See note[1] at end of table.)
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)

TABLE B–3 Data Schema Values for the MySQL Database Type *(Continued)*

Database Column	Value
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) or CLOB (See note[1] at end of table.)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) or CLOB (See note[1] at end of table.)
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

Note – The column length limit for these columns is configurable. The default data type is VARCHAR and the default size limit is noted in parentheses. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.

SQL Server Database Type

Table B–4 lists the data schema values for the SQL Server database type.

TABLE B–4 Data Schema Values for the SQL Server Database Type

Database Column	Value
id	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP

TABLE B–4 Data Schema Values for the SQL Server Database Type *(Continued)*

Database Column	Value
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) or CLOB (See note[1] at end of table.)
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) or CLOB (See note[1] at end of table.)
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) or CLOB (See note[1] at end of table.)
parm03label	NVARCHAR(50)

TABLE B–4 Data Schema Values for the SQL Server Database Type *(Continued)*

Database Column	Value
parm03value	NVARCHAR(128) or CLOB (See note[1] at end of table.)
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) or CLOB (See note[1] at end of table.)
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) or CLOB (See note[1] at end of table.)
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

Note – The column length limit for these columns is configurable. The default data type is VARCHAR and the default size limit is noted in parentheses. See "Audit Log Configuration" on page 329 for information on how to adjust the size limit.

Audit Log Database Mappings

Table B–5 contains the mappings between stored audit log database keys and the display string to which they map in the audit report output. Waveset stores items that are used as constants as short database keys to save space in the repository. The product interface does not display these mappings. Instead, you see them only when examining the output of a dump of the audit report results.

Table B–6 contains the auditable action database keys, Table B–7 contains the action status keys, and Table B–8 contains the reason codes that are stored in the database as keys.

TABLE B–5 Object Key-Type Database Keys

Type Name	English Text	DbKey
AccessReview	AccessReview	AV
AccessReviewWorkflow*	Access Review Workflow	AW
AccessScan	AccessScan	AS
Account	Account	AN
AdminGroup	Capability	AG
Administrator	Administrator	AD

TABLE B–5 Object Key-Type Database Keys *(Continued)*

Type Name	English Text	DbKey
AdminRole	Admin Role	AR
Application	Resource Group	AP
AttributeDefinition	AttributeDefinition	AF
AttrParse	AttrParse	AT
AuditConfig	AuditConfig	AC
AuditPolicy	AuditPolicy	CP
BeanPod	Bean Pod	BP
ComplianceViolation	ComplianceViolation	CV
Configuration	Configuration	CN
DataExporter	Data Exporter	DE
Discovery	Discovery	DS
Email*	Email	EM
EmailTemplate	EmailTemplate	ET
EncryptionKey	EncryptionKey	KY
Event	Event	EV
Extract	Extract	ER
ExtractTask	ExtractTask	EX
IDMXUser*	Directory User	UX
LighthouseAccount*	Identity System Account	LA
LoadConfig	LoadConfig	LD
LoadTask	LoadTask	LT
Log	Log	LG
LoginApp	LoginApp	LP
LoginConfig	LoginConfig	LC
LoginModGroup	LoginModGroup	LF
MetaView	Meta View	MV
ObjectGroup	Organization	OG
Policy	Policy	PO

TABLE B–5 Object Key-Type Database Keys *(Continued)*

Type Name	English Text	DbKey
ProvisioningTask	ProvisioningTask	PT
RemediationWorkflow*	Remediation Workflow	RW
RemedyConfig	RemedyConfig	RC
Resource	Resource	RS
ResourceAccount*	Resource Account	RA
ResourceAction	ResourceAction	RN
ResourceForm	ResourceForm	RF
ResourceObject	ResourceObject	RE
RiskReportTask	RiskReportTask	RR
Role	Role	RL
Rule	Rule	RU
SnapShot	SnapShot	SS
ServerObject	ServerObject	SV
SysLog	SysLog	SL
System	System	SY
TaskDefinition	TaskDefinition	TD
TaskInstance	TaskInstance	TI
TaskResult	TaskResult	TR
TaskResultPage	ResultPage	TP
TaskSchedule	TaskSchedule	TS
TaskTemplate	TaskTemplate	TT
TestNotification*	Test Notification	TN
User	User	US
UserEntitlement	UserEntitlement	UE
UserForm	UserForm	UF
WorkflowCase*	Workflow Case	WC
WorkItem	WorkItem	WI
XmlData	XmlData	XD

[1]

TABLE B–6 Action Database Keys

Action Name	English Text	DbKey
Allowed*	Allowed	AL
Approve	Approve	AP
Assign Audit Policies	Assign Audit Policies	AA
Assign Capabilities	Assign Capabilities	AC
AttestorApproved*	Attestor Approved	TA
AttestorRejected*	Attestor Rejected	AR
AttestorRemediate*	Remediation Requested	AF
AttestorRescan*	Rescan Requested	AN
Bulk Change Password	Bulk Change Password	BW
Bulk Create	Bulk Create	BC
Bulk Delete	Bulk Delete	BD
Bulk Deprovision	Bulk Deprovision	BP
Bulk Disable	Bulk Disable	BF
Bulk Enable	Bulk Enable	BE
Bulk Modify	Bulk Modify	BM
Bulk Reset Password	Bulk Reset Password	BR
Bulk Unassign	Bulk Unassign	BU
Bulk Unlink	Bulk Unlink	BL
Bypass Verify	Bypass Verify	BV
CancelReconcile*	Cancel Reconcile	CR
challengeResponse*	Challenge Response	CD
Change Password	Change Password	CP
Connect	Connect	CN
Control Active Sync	Control Active Sync	CA

[1] * Extended Types

TABLE B–6 Action Database Keys (Continued)

Action Name	English Text	DbKey
Create	Create	CT
CredentialsExpired*	Credentials Expired	CE
Debug	Debug	DB
Delegate	Delegate	DG
Delete	Delete	DL
Deprovision	Deprovision	DP
Disable	Disable	DS
Disconnect	Disconnect	DC
Enable	Enable	EN
End Activity	End Activity	EA
End Process	End Process	PE
End Workflow	End Workflow	EW
Execute	Execute	LN
Expired*	Expired	EX
Export	Export	EP
Fixed*	Fixed	FX
Import	Import	IM
List	List	LI
Lock	Lock	LK
Login	Login	LG
Logout*	Logout	LO
Mitigated*	Mitigated	VM
Modify	Modify	MO
Modify Active Sync	Modify Active Sync	MA
NativeChange*	Native Change	NC
Notify*	Notify	NO
PostOperation*	Post-Operation Callout	PT
PreOperation*	Pre-Operation Callout	PP

TABLE B–6 Action Database Keys *(Continued)*

Action Name	English Text	DbKey
Prioritize*	Prioritize	PR
Provision	Provision	PV
Recurring*	Recurring	RC
Reject	Reject	RJ
Remediated*	Remediated	VR
Rename	Rename	RE
RequestReconcile*	Request Reconcile	RR
ResetPassword	ResetPassword	RP
Run Debugger	Run Debugger	RD
ScanBegin*	Scan Begin	SB
ScanEnd*	Scan End	SE
StartActivity*	Start Activity	SA
StartProcess*	Start Process	SP
StartWorkflow*	Start Workflow	SW
Terminate*	Terminate	TR
Unassign	Unassign	UA
Unlink	Unlink	UN
Unlock	Unlock	UL
updateAuthenticationAnswers*	Update Authentication Answers	AQ
usernameRecovery*	Username Recovery	UR
View	View	VW
View Only	View Only	VO

[2]

[2] * Extended Actions

TABLE B–7 Action Status Database Keys

Result	DbKey
`Success`	`S`
`Failure`	`F`

TABLE B–8 Reasons Stored as Keys

Reason Name	English Text	DbKey
`PolicyViolation`	Violation of policy {0}: {1}	`PV`
`InvalidCredentials`	Invalid Credentials	`CR`
`InsufficientPrivileges`	Insufficient Privileges	`IP`
`DatabaseAccessFailed`	Database Access Failed	`DA`
`AccountDisabled`	Account Disabled	`DI`

◆ ◆ ◆ APPENDIX C

User Interface Quick Reference

Table C–1 is a quick reference to commonly performed Waveset tasks. This table shows the primary Waveset interface location where you can go to begin each task, with alternate locations or methods (if available) that you can use to perform the same task.

Waveset Interface Task Reference

TABLE C–1 Task Reference

To Perform This Task	Go To	Or To
Manage Waveset Users:		
Create and edit users	Accounts tab, List Accounts selection	Accounts tab, Find Users selection (User Account Search Results page)
Approve user account creation	Work Items tab, Approvals tab	
Set up user authentication (policies)	Security 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) Waveset 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

TABLE C–1 Task Reference *(Continued)*

To Perform This Task	Go To	Or To
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)
Manage Waveset Administrators:		
Set up delegated administration (through organizations)	Accounts tab, List Accounts selection, Create User page	
Assign capabilities	Accounts tab, List Accounts selection, Create or Edit User page Security tab	
Assign capabilities (through admin roles)	Accounts tab, List Accounts selection, Create or Edit User page Security tab	
Set up approvers (to validate account creation)	Accounts tab, List Accounts selection, Create Organization page	
	Roles tab, Create Roles page	
Configure Waveset:		
Create and manage resources (Resource Wizard)	Resources tab	
Manage resource groups	Resources tab, List Resource Groups selection	
Create and manage roles	Roles tab	
Find roles	Roles tab, Find Roles selection	
Edit capabilities	Security tab, Capabilities selection	
Create and edit admin roles	Security 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	Security tab, Policies selection	

TABLE C–1 Task Reference *(Continued)*

To Perform This Task	Go To	Or To
Load and Synchronize Accounts and Data:		
Import data files (such as XML-format forms)	Configure tab, Import Exchange File selection	
Load resource accounts	Accounts tab, Load from Resource selection	
Load accounts from file	Accounts tab, Load from File selection	
Compare Waveset users with resource accounts	Resources tab, Reconcile with Resources selection	
Audit and Manage Compliance:		
Disable or enable auditing	Configure tab, Audit selection	
Set up audit events to capture	Configure tab, Audit selection	
Define audit policies (create, edit, delete)	Compliance tab, Manage Policies selection	
Assign audit policies	Accounts tab, Compliance selection	
Define remediators and assign remediation workflows for an audit policy	Compliance tab, Manage Policies tab	
Respond to policy violation remediation requests	My Work Items tab, Remediations selection	
Mitigate policy violations	Work Items tab, Remediations tab	
Review remediated policy violations	Work Items tab, Remediations tab	
Generate audit policy reports	Reports tab, Run Report tab	
Perform an audit scan on one or more users or organizations	Accounts tab, select Scan from the User Actions or Organization Actions list	
Set up Periodic Access Reviews	Compliance tab, Manage Access Scans selection	
Monitor Periodic Access Reviews	Compliance tab, Access Reviews selection	

TABLE C–1 Task Reference *(Continued)*

To Perform This Task	Go To	Or To
View Audit reports	Reports tab, Auditor Report type selection	
Edit administrator audit capabilities	Security tab, Capabilities tab	
Set up email templates for audit notification	Configure tab, Email Templates tab	
Import data files/rules (such as XML-format forms)	Configure tab, Import Exchange File tab	
Define an access review scan	Compliance tab, Manage Scans tab	
Run an access review	Compliance tab, Access Reviews tab	
Terminate an access review	Compliance tab, Access Reviews tab	
Schedule an access review	Server Tasks tab, Manage Schedule tab	
Set up periodic access reviews	Compliance tab, Manage Access Scans tab	
Monitor access review status	Compliance tab, Access Reviews tab	
Configure attestors	Compliance tab, Manage Access Scans tab	
Perform Attestor duties (review and certify user entitlements)	Work Items tab, My Work Items tab, Attestation tab	
Risk Analysis and Reporting:		
Run and manage reports	Reports tab, Run Reports selection to create, run, and download reports; View Reports to view report results.	
Define and run risk analysis reports	Reports tab, Risk Analysis selection	
View graphical reports	Reports tab, View Dashboards selection	
Review separation-of-duties report	Reports tab, Run Report tab	
Manage Waveset Tasks:		

TABLE C–1 Task Reference *(Continued)*

To Perform This Task	Go To	Or To
Run a defined task (or process)	Server Tasks tab, Run Tasks selection	
Schedule a task	Server Tasks tab, Manage Schedule selection	
View Task results	Server Tasks tab, Find Tasks, or All Tasks selection	
Suspend or terminate a task	Server Tasks tab, All Tasks selection	
Manage Service Provider Users:		
Manage Service Provider Users	Accounts tab, Manage Service Provider Users selection	
Manage Service Provider Transactions	Server Tasks tab, Service Provider Transactions selection	
Configure Service Provider features	Service Provider tab, Edit Main Configuration selection	
Configure Transaction defaults	Service Provider tab, Edit Transaction Configuration selection	
Create or edit Service Provider policies	Security tab, Policies selection	

APPENDIX D

Capabilities Definitions

This appendix provides definitions for the different capabilities used in Waveset.

The information is organized into the following sections:

- "Task-Based Capabilities Definitions" on page 547
- "Functional Capabilities Definitions" on page 565

For general information about capabilities, see "Understanding and Managing Capabilities" on page 198.

Note – All capabilities grant the user or administrator access to the Passwords → Change My Password and Change My Answers tabs.

Task-Based Capabilities Definitions

This section describes each of the task-based capabilities that can be assigned to users. It also lists the tabs and subtabs that can be accessed with each capability. Capabilities are listed in alphabetical order by name.

Note – This table does not include information about default tabs and subtabs that are available to all users, such as the Change My Password tab.

TABLE D–1 Waveset Task-Based Capabilities Definitions

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Access Review Detail Report Administrator	Create, edit, delete, and execute Access Review Detail Reports, Access Review Coverage Reports, and Access Scan User Scope Coverage Reports	Reports → Run Reports tab and View Reports tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Access Review Summary Report Administrator	Create, edit, delete, and execute Access Review Summary Reports	Reports → Run Reports tab and View Reports tab
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, and Load from Resource tabs Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Admin Report Administrator	Create, edit, delete, and run Administrator reports and Admin role reports.	Reports → Run Reports tab and View Reports tab (Administrator and Admin Role reports only)
Admin Role Administrator	Create, edit, and delete admin roles.	Security → Admin Roles tab
Application Administrator	Create, edit, and delete Application roles.	Server Tasks → Find Tasks, All Tasks, Run Tasks tabs (synchronize roles) Roles → List Roles tab and Find Roles tab
Asset Administrator	Create, edit, and delete Asset roles.	Server Tasks → Find Tasks, All Tasks, Run Tasks tabs (synchronize roles) Roles → List Roles tab and Find Roles tab
Assign Audit Policies Administrator	Assign audit policies to user accounts and organizations. Edit the User Audit Policy from the User Actions list and edit the Organization Audit Policy from the Organization Actions list.	Accounts → List Accounts tab and Find Users tab.
Assign Organization Audit Policies Administrator	Assign audit policies to organizations only. Edit the Organization Audit Policy from the Organization Actions list.	Accounts → List Accounts tab
Assign User Audit Policies Administrator	Assign audit policies to users only. Edit the User Audit Policy from the User Actions list	Accounts → List Accounts tab and Find Users tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Assign User Capabilities	Change user capabilities assignments (assign and unassign). Must be assigned with another user administrator capability (for example, Create User or Enable User).	Accounts → List Accounts (edit only) and Find Users tabs.
Audit Policy Administrator	Create, modify, and delete audit policies.	Compliance → Manage Policies tab
Audit Policy Scan Report Administrator	Run or schedule audit policy scan tasks.	Server Tasks → Find Tasks, All Tasks, Run Tasks, and Manage Schedule tabs
Audit Report Administrator	Create, modify, delete, and execute audit reports. Access to AuditLog, Historical User Changes, Individual User AuditLog, and Usage reports only.	Reports → Run Reports tab and View Reports tab.
AuditLog Report Administrator	Create, modify, delete, and execute the AuditLog Report.	Reports → Run Reports tab
Audited Attribute Report Administrator	Create, modify, delete, and execute the Audited Attribute Report.	Reports → Run Reports tab and View Reports tab
Auditor Access Scan Administrator	Create, edit, and delete Periodic Access Review scans	Compliance → Manage Access Scans tab
Auditor Administrator	Set up, manage, and monitor audit policies, audit scans, and user compliance.	Accounts → List Accounts tab and Find Users tab Server Tasks → Find Tasks, All Tasks, Run Tasks, and Manage Schedule tabs Reports → Run Reports tab and View Reports tab Compliance → Manage Policies, Manage Access Scans, and Access Reviews tabs
Auditor Attestor	Required to attest other users' attestations while organization security is enabled.	Default Passwords and Work Items tabs only
Auditor Periodic Access Review Administrator	Manage Periodic Access Reviews (PAR), manage access scans, manage attestations, manage PAR reports.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Compliance → Manage Access Scans tab and Access Review tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Auditor Remediator	Remediate, mitigate, and forward audit policy violations.	Default Passwords and Work Items tabs only
Auditor Report Administrator	Create, modify, delete, and execute any of the Auditor Reports.	Server Tasks → Find Tasks, All Tasks, Run Tasks, and Manage Schedule tabs Reports → all actions on auditor reports
Auditor View User	View compliance information associated with user.	Accounts → List Accounts tab and Find Users tab
Audit Policy Violation History Administrator	Create. modify, delete, and execute the Audit Policy Violation History report.	Reports → Run Reports tab
Bulk Account Administrator	Perform regular and bulk operations on users, including assigning capabilities.	Accounts → List Accounts, Find Users, Launch Bulk Actions, Extract to File, Load from File, and Load from Resource tabs Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Bulk Change Account Administrator	Perform regular and bulk operations except delete on existing users, including assigning capabilities. Cannot create or delete users.	Accounts → List Accounts, Find Users, and Launch Bulk Actions tabs. Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Bulk Change Resource Password Administrator	Change the password for the specified resource connection account on the specified resources.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Resources → List Resources tab and Launch Bulk Actions tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Bulk Change User Account Administrator	Perform regular and bulk operations except delete on existing users. Cannot create, delete, or assign capabilities to users.	Accounts → List Accounts, Find Users, and Launch Bulk Actions tabs. Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Create Users	Assign resources and initiate user create requests (on individual users and by using bulk operations).	Accounts → List Accounts (Create only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Delete Users	Delete Waveset user accounts; deprovision, unassign, and unlink resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts, Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Delete IDM Users	Delete existing Waveset user accounts (on individual users and by using bulk operations).	Accounts → List Accounts (Delete only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Deprovision User	Delete and unlink existing resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts (Deprovision only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and 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, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Enable User	Enable existing users and resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts (Enable only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tab Roles → List Roles tab and Find Roles tab
Bulk Reset Resource Password Administrator	Reset the password for the specified resource connection account on the specified resources.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab and Launch Bulk Actions tab
Bulk Unassign User	Unassign and unlink existing resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts (Unassign only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Bulk Unlink User	Unlink existing resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts (Unlink only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Bulk Update Users	Edit, move, and update existing users and resource accounts (on individual users and by using bulk operations).	Accounts → List Accounts (edit, move, and update actions only), Find Users, and Launch Bulk Actions tabs Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Bulk User Account Administrator	Perform all regular and bulk operations on users.	Accounts → List Accounts, Find Users, Launch Bulk Actions, Extract to File, Load from File, and Load from Resource tabs Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Business Role Administrator	Create, edit, and delete Business Roles.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs (synchronize roles) Roles → List Roles tab and Find Roles tab
Capability Administrator	Create, modify, and delete capabilities.	Security → Capabilities tab
Change Account Administrator	Perform all operations except delete on existing users, including assigning capabilities. Does not include bulk operations Create admin and user reports, run and edit admin reports, run AuditLog reports in scope. Cannot run admin or user reports on out-of-scope organizations. Cannot delete users.	Accounts → List Accounts tab and Find Users tab Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Change Resource Active Sync Administrator	Change Active Sync resource parameters.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Change Password Administrator	Change user and resource account passwords. Access to Export Password Scan task only (from Run Tasks tab)	Accounts → List Accounts tab and Find Users tab Passwords → Change User Password Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs. Roles → List Roles tab and Find Roles tab
Change Password Administrator (Verification Required)	Change user and resource account passwords following successful validation of the user's authentication question answers. Access to Export Password Scan task only (from Run Tasks tab)	Accounts → List Accounts tab and Find Users tab Passwords → Change User Password tab (verification required before action) Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Change Resource Password Administrator	Change resource administrator account passwords. Change resource passwords only (from Manage Connection → Change Password in the actions menu)	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab.
Change User Account Administrator	Perform all operations on existing users except deletes and bulk operations. Also cannot create, delete, or assign capabilities to users.	Accounts → List Accounts tab and Find Users tab Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Configure Audit	Configure the events and configuration groups audited in the system.	Configure → Audit tab
Configure Certificates	Configure trusted certificates and CRLs.	Security → Certificates tab
Control Active Sync Resource Administrator	Control Active Sync resource state (such as start, stop, and refresh)	Resources → List Resources tab For Active Sync resources: Active Sync actions menu

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Create User	Assign resources and initiate user create requests. Does not include bulk operations	Accounts → List Accounts (Create only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run tasks tabs Roles → List Roles tab and Find Roles tab
Data Warehouse Administrator	Configure Data Exporter and run the Data Warehouse Exporter Launcher task.	Reports → Dashboard Graphs tab and View Dashboards tab Resources → List Resources tab Configure → Warehouse tab
Data Warehouse Query	Configure and run forensic queries	Reports → Dashboard Graphs tab and View Dashboards tab Resources → List Resources tab Compliance → Forensic Query
Debug	Access and execute operations from the Waveset debug pages. **Note –** The Waveset debug pages cannot be accessed from the menu. To access the debug pages, type the following URL into your browser: `http://`*<AppServerHost>*`:`*<Port>*`/idm/debug`	All default tabs
Delete User	Delete Waveset user accounts; deprovision, unassign, and unlink resource accounts. Does not include bulk operations.	Accounts → List Accounts (Delete only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Delete IDM User	Delete Waveset user accounts. Does not include bulk operations.	Accounts → List Accounts (Delete only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Deprovision User	Delete and unlink existing resource accounts. Does not include bulk operations.	Accounts → List Accounts (Deprovision only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Disable User	Disable existing users and resource accounts. Does not include bulk operations	Accounts → List Accounts (Disable only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Enable User	Enable existing users and resource accounts. Does not include bulk operations	Accounts → List Accounts (Enable only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
End User Administrator	View and modify the rights to object types specified in the End User capability and the End User Controlled Organizations rule.	All default tabs
External Resource Administrator	View and configure external resources only. Cannot create new resources.	Configure → External Resources tab
Configure Identity Manager Schema	View and configure the effective schema for Users or Roles using the Waveset configuration object `IDM Schema Configuration`.	All default tabs
Import User	Import users from defined resources.	Accounts → List Accounts, Find Users, Extract to File, Load from File, and Load from Resource tabs Roles → List Roles tab and Find Roles tab
Import/Export Administrator	Import and export all types of objects.	Configure → Import Exchange File tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
IT Role Administrator	Create, edit, and delete IT Roles.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs (synchronize roles) Roles → List Roles tab and Find Roles tab
Login Administrator	Edit the set of login modules for a given login interface.	Security → Login tab
Organization Administrator	Create and edit organizations and directory junctions. Delete organizations only.	Accounts → List Accounts tab
Organization Approver	Approve requests for new organizations.	Default Passwords and Work Items tabs only
Organization Violation History Administrator	Create, edit, delete, and execute the Organization Violation History reports only.	Reports → Run Reports tab
Password Administrator	List, change, and reset user and resource account passwords.	Accounts → List Accounts tab and Find Users tabs Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Password Administrator (Verification Required)	List, change, and reset user and resource account passwords only. Successful validation of the user's authentication question answers required before action succeeds.	Accounts → List Accounts tab and Find Users tab Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Policy Administrator	Create, edit, and delete Policies.	Security → Policies tab
Policy Summary Report Report Administrator	Create, edit, delete, and execute the Policy Summary Reports.	Reports → Run Report tab and View Reports tab
Register Identity Manager Product Component	Register an installation of Waveset with Oracle or create a local service tag.	Configure → Product Registration tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Reconcile Administrator	Edit reconciliation policies and control reconciliation tasks.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs (View reconcile task). Resources → List Resources tab and Examine Account Index tab
Reconcile Report Administrator	Create, edit, delete, and run reconciliation reports.	Reports → Run Reports tab (Account Index report only) and View Reports tab
Reconcile Request Administrator	Manage reconciliation requests.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab (list and reconciliation features only) and View Reports tab
Remedy Integration Administrator	Edit Remedy integration configuration (view tasks, run role synchronization).	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Configure → Remedy Integration tab
Rename User	Rename existing users and resource accounts (list all accounts in scope, rename users).	Accounts → List Accounts tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Report Administrator	Configure audit settings and run all report types (view tasks, run role synchronization).	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Reports → Run Reports, View Reports, Run Risk Analysis, and View Risk Analysis tabs Roles → List Roles tab and Find Roles tab Configure → Audit tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Reset Password Administrator	Reset user and resource account passwords.	Accounts → List Accounts tab and Find Users tab (Reset Password only) Passwords → Reset User Password Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs (No tasks are available to users with this capability) Roles → List Roles tab and Find Roles tab
Reset Password Administrator (Verification Required)	Reset user and resource account passwords. Successful validation of the user's authentication question answers is required before action succeeds.	Accounts → List Accounts tab and Find Users tab Passwords → Reset User Password Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs (No tasks are available to users with this capability) Roles → List Roles tab and Find Roles tab
Reset Resource Password Administrator	Reset resource administrator account passwords (from Manage Connection → Reset Password in the actions menu).	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab
Resource Administrator	Create, edit, and delete resources. Resource User Report and Resource Group Report return an error on out-of-scope resources. Edit global policies, parameters, and resource groups. Cannot manage connections or resource objects	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources, List Resource Groups, and Examine Account Index tabs Configure → Connector Servers
Resource Approver	Approve resource assignments	All default Passwords and Work Items tabs
Resource Group Administrator	Create, edit, and delete resource groups.	Resources → List Resource Groups tab
Resource Object Administrator	View, create, modify, and delete resource objects.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Resource Password Administrator	Change and reset resource proxy account passwords.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Resources → List Resources tab (Change resource password only from Manage Connection → Change Password in the actions menu)
Resource Report Administrator	Create, edit, delete, and run resource reports.	Reports → Run Reports tab and View Reports tab
Resource Violation History Administrator	Create, edit, delete, and execute Resource Violation History reports.	Reports → Run Reports
Risk Analysis Administrator	Create, edit, delete, and run risk analysis.	Reports → Risk Analysis tab and View Risk Analysis tab
Role Administrator	Create, edit, synchronize, and delete roles.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Role Approver	Approve role assignments	All default Passwords and Work Items tabs
Role Report Administrator	Create, edit, delete, and run resource reports.	Reports → Run Reports tab and View Reports tab Roles → List Roles tab
Run Access Review Detail Report	Run the Access Review Detail Report	Reports → Run Reports tab and View Reports tab
Run Access Review Summary Report	Run the Access Review Summary Report	Reports → Run Reports tab and View Reports tab
Run Admin Report	Run administrator reports.	Reports → Run Reports tab and View Reports tab
Run Audit Policy Scan Report	Run the Audit Policy Scan Report.	Server Tasks → All Tasks, Find Tasks, and Run Tasks only
Run Audit Report	Run Audit, AuditLog, Historical User Changes, Individual User AuditLog, and Usage reports only.	Reports → Run Reports tab and View Reports tab
Run Audited Attribute Report	Execute and view the Audited Attribute Report.	Reports → Run Reports tab and View Reports tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Run Auditor Report	Run all reports of the type, AuditLog Report.	Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Reports → Run Reports tab and View Reports tab
Run AuditLog Report	Execute and view the AuditLog, Today's Activity and Weekly Activity reports.	Reports → Run Reports
Run Audit Policy Violation History	Execute and view the Organization Violation History report and Today's Activity and Weekly Activity report.	Reports → Run Reports
Run Policy Summary Report	Execute and view the Policy Summary Report.	Reports → Run Reports tab and View Reports tab
Run Organization Violation History	Execute the Organization Violation History report.	Reports → Run Reports tab
Run Reconcile Report	Execute and view Account Index reports.	Reports → Run Reports tab and View Reports tab
Run Resource Report	Execute and view Resource User and Resource Group reports.	Reports → Run Reports tab and View Reports tab
Run Resource Violation History	Execute Resource Violation History reports.	Reports → Run Reports tab
Run Risk Analysis	Execute and view risk analyses.	Reports → Run Risk Analysis tab and View Risk Analysis tab
Run Role Report	Execute and view role reports.	Reports → Run Reports tab and View Reports tab Roles → List Roles tab
Run Separation of Duties Report	Execute and view Separation of Duties Reports.	Reports → Run Reports tab and View Reports tab
Run Task Report	Execute and view task reports.	Reports → Run Reports tab and View Reports tab
Run User Access Report	Execute and view Detailed User Reports and User Access reports.	Reports → Run Reports tab and View Reports tab
Run User Report	Execute and view user reports.	Reports → Run Reports tab and View Reports tab
Run Violation Summary Report	Execute the Violation Summary report.	Reports → Run Reports tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Security Administrator	Create users with capabilities; enable and disable users, list and control resource objects, and manage encryption keys, manage log-in and audit configurations, and manage policies.	Accounts → List Accounts (some actions) tab and Find Users tab (audit report) Passwords → Change user Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, Run Tasks, and Configure Tasks tabs Reports → Run Reports, View Reports, Dashboard Graphs, View Dashboards, and Configure Reports Resources → List Resources Configure → Audit tab and Warehouse tabs Security → Certificates, Login, and Policies tabs Service Provider → Edit User Search Configuration
Separation of Duties Report Administrator	Create, edit, execute, view, and delete Separation of Duties Reports.	Reports → Run Reports tab and View Reports tab
Service Provider Admin Role Administrator	Manage Service Provider Admin Roles and the associated rules.	Security → Admin Roles tab
Service Provider Administrator	Create, edit, and manage service provider users and transactions; configure the transaction database and tracked events.	Accounts → Manage Service Provider Users tab Server Tasks → Service Provider Transactions tab Reports → Dashboard Graphs tab Reports → View Dashboards tab Service Provider → Edit Main Configuration, Edit Transaction Configuration, and Edit User Search Configuration tabs
Service Provider Create User	Create user accounts for service provider (extranet) users.	Accounts → Manage Service Provider Users tab
Service Provider Delete User	Delete a service provider user account.	Accounts → Manage Service Provider Users tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Service Provider Update User	Update a service provider user account.	Accounts → Manage Service Provider Users tab
Service Provider User Administrator	Manage service provider (extranet) users.	Accounts → Manage Service Provider Users
Service Provider View User	View service provider (extranet) user account information.	Accounts → Manage Service Provider Users tab
Task Report Administrator	Create, edit, delete, execute and view task reports.	Reports → Run Reports tab and View Reports tab
Unassign User	Unassign and unlink existing resource accounts. Does not include bulk operations.	Accounts → List Accounts (Unassign only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Unlink User	Unlink existing resource accounts. Does not include bulk operations.	Accounts → List Accounts (Unlink only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
Unlock User	Unlock existing user's resource accounts that support unlock. Does not include bulk operations.	Accounts → List Accounts (Unlock only) tab and Find Users tab Server Tasks → Find Tasks, All Tasks, Run Tasks tabs Roles → List Roles tab and Find Roles tab
Update User	Edit existing users and initiate user update requests. Manage existing server tasks.	Accounts → List Accounts tab and Find Users tab Server Tasks → Find Tasks, All Tasks, Run Tasks tabs Roles → List Roles tab and Find Roles tab
User Access Report Administrator	Create, edit, delete, execute, and view User Access Reports.	Reports → Run Reports tab and View Reports tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
User Account Administrator	All operations on users, except cannot assign user capabilities.	Accounts → List Accounts, Find Users, Extract to File, Load from File, and Load from Resource tabs. Passwords → Change User Password tab and Reset User Password tab Server Tasks → Find Tasks, All Tasks, and Run Tasks tabs Roles → List Roles tab and Find Roles tab
User Report Administrator	Create, edit, delete, execute and view user reports.	Reports → Run Reports tab and View Reports tab
View Application	List Application type roles and view Application type role information. No change actions allowed.	Roles → List Roles tab and Find Roles tab
View Asset	List Asset type roles and view Asset type role information. No change actions allowed.	Roles → List Roles tab and Find Roles tab
View Business Role	List Business roles and view Business role information. No change actions allowed.	Roles → List Roles tab and Find Roles tab
View IT Role	List IT roles and view IT role information. No change actions allowed.	Roles → List Roles tab and Find Roles tab
View Role	List all role types and view all role information. No change actions allowed.	Roles → List Roles tab and Find Roles tab
View User	View individual user details. No change actions allowed.	Accounts → List Accounts tab and Find Users tab
Violation Summary Report Administrator	Create, edit, delete, and execute Violation Summary reports.	Reports → Run Reports tab

TABLE D–1 Waveset Task-Based Capabilities Definitions *(Continued)*

Capability	Allows the Administrator/User to	Can Access These Tabs and Subtabs
Identity System Administrator	Perform system-wide tasks, such as editing system configuration objects, synchronizing roles, editing source adapter templates, and running reports.	Server Tasks → Find Tasks, All Tasks, Run Tasks, Manage Schedule, and Configure Tasks tabs Reports → Run Reports, View Reports, Dashboard Graphs, View Dashboards, and Configure Reports tabs Resources → List Resources Configure → Audit, Warehouse, Email Templates, Form and Process Mappings, Servers, User Interface, and Product Registration tabs Compliance → Access Reviews Security → Certificates

Functional Capabilities Definitions

Functional capabilities consist of task-based capabilities, as well as other functional capabilities.

- **Account Administrator**
  - Approver Administrator
    - Organization Approver
    - Resource Approver
    - Role Approver
  - Assign User Capabilities
  - SPML Access
  - 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**
- **Auditor Administrator**
  - Assign Audit Policies
    - Assign Organization Audit Policies
    - Assign User Audit Policies
  - Audit Policy Administrator

    Auditor View User
  - Auditor Periodic Access Review Administrator

    Auditor Access Scan Administrator
  - Auditor Report Administrator
  - Password Administrator
  - User Account Administrator
  - Assign User Capabilities
- **Auditor Report Administrator**
  - Access Review Detail Report Administrator

    Run Access Review Detail Report
  - Access Review Summary Report Administrator

    Run Access Review Summary Report
  - Audit Policy Scan Report Administrator

    Run Audit Policy Scan Report
  - Audited Attribute Report Administrator

    Run Audited Attribute Report
  - Audit Policy Violation History Administrator

    Run Audit Policy Violation History Report
  - Organization Violation History Administrator

    Run Organization Violation History Report
  - Policy Summary Report Administrator
  - Resource Violation History Administrator

    Run Resource Violation History Report
  - Run Auditor Report
  - Separation of Duties Report Administrator

    Run Separation of Duties Report
  - User Access Report Administrator

    Run User Access Report
  - Violation Summary Report Administrator
- **Auditor View User**

  View User
- **Bulk Account Administrator**
  - Approver Administrator
  - 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 Administrator
  - 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

- **Bulk Resource Administrator**
  - Change Active Sync Resource Administrator
  - Control Active Sync Resource Administrator
  - Resource Group Administrator
- **Bulk Resource Password Administrator**
  - Bulk Change Resource Password Administrator
  - Bulk Reset Resource Password Administrator
- **Capability Administrator**
- **Change Account Administrator**
  - Approver Administrator
  - Assign User Capabilities
  - Change User Account Administrator
    - Password Administrator
      - Change Password Administrator
      - Reset Password Administrator
    - Disable User
    - Enable User
    - Rename User
    - Unlock User
    - Update User
    - View User
- **Configure Certificates**
- **Data Warehouse Administrator**
- **Data Warehouse Query**
- **Debug**
- **End User Administrator**
- **IDM Schema Configuration**
- **Import/Export Administrator**
- **License Administrator**
- **Login Administrator**
- **Meta View Administrator**
- **Organization Administrator**
- **Password Administrator (Verification Required)**

  - Change Password Administrator (Verification Required)
  - Reset Password Administrator (Verification Required)
- **Policy Administrator**
- **Product Administrator**
- **Reconcile Administrator**

  Reconcile Request Administrator
- **Remedy Integration Administrator**
- **Report Administrator**
  - Admin Report Administrator

    Run Admin Report
  - Audit Report Administrator

    Run Audit Report
  - Auditor Report Administrator
    - Access Review Detail Report Administrator

      Run Access Review Detail Report
    - Access Review Summary Report Administrator

      Run Access Review Summary Report
    - Audit Policy Scan Report Administrator

      Run Audit Policy Scan Report
    - Audited Attribute Report Administrator

      Run Audited Attribute Report
    - AuditLog Report Administrator

      Run AuditLog Report
    - Audit Policy Violation History Administrator

      Run Audit Policy Violation History
    - Organization Violation History Administrator

      Run Organization Violation History
    - Policy Summary Report Administrator

      Run Policy Summary Report
    - Reconcile Report Administrator

      Run Reconcile Report
    - Resource Violation History Administrator

      Run Resource Violation History
    - Run Auditor Report

-
  -
    -
      - Run Access Review Detail Report
      - Run Access Review Summary Report
      - Run Audit Policy Scan Report
      - Run Audited Attribute Report
      - Run AuditLog Report
      - Run Audit Policy Violation History
      - Run Organization Violation History
      - Run Policy Summary Report
      - Run Resource Violation History
      - Run Separation of Duties Report
      - Run User Access Report
      - Run Violation Summary Report
    - Separation of Duties Report Administrator

      Run Separation of Duties Report
    - User Access Report Administrator

      Run User Access Report
    - Violation Summary Report Administrator

      Run Violation Summary Report
  - 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
  - Configure Audit
- **Resource Administrator**
  - Change Active Sync Resource Administrator
  - Control Active Sync Resource Administrator
  - Resource Group Administrator
- **Resource Object Administrator**
- **Resource Password Administrator**

  - Change Resource Password Administrator
  - Reset Resource Password Administrator
- **Role Administrator**
  - Application Administrator
  - Asset Administrator
  - Business Role Administrator
  - IT Role Administrator
- **Security Administrator**
- **Service Provider Administrator**
  - Service Provider User Administrator
  - Service Provider Create User
  - Service Provider Delete User
  - Service Provider Update User
  - Service Provider View User
- **Service Provider Admin Role Administrator**
- **Waveset Administrator**

Glossary

access review An audited process that enables managers or other responsible parties to review and certify user access privileges. User entitlement records can be automatically approved or rejected, or, they can be manually attested. Also see *attestation*.

account attribute Account attributes provide a way for Waveset administrators to create a standard set of names that map to attributes on managed resources. For example, an Waveset attribute named *fullname* might map to the *displayName* attribute on Active Directory resources, and the *cn* attribute on LDAP resources. Any changes to the user's *fullname* attribute in Waveset, is then passed to the user's *displayName* and *cn* attributes on the user's remote resource accounts.

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

administrator Person who configures Waveset or is responsible for operational tasks, such as creating users and managing access to resources.

administrator interface User interface used by administrators to configure and manage Waveset.

Application (Role) One of the four role types in Waveset, the Application role-type is a collection of resources, and/or resource groups, and/or specific applications on resources, that users need in order to do their jobs. Application roles cannot be assigned directly to users, but can be assigned to IT Roles and Business Roles.

approval The process of granting or denying a user access request to a role, a resource, or an organization. An Waveset administrator with permission to view and respond to an approval work item is called an *approver*.

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

Asset (Role) One of the four role types in Waveset, the Asset role-type is (typically) reserved for non-connected and/or non-digital resources that require manual provisioning, such as mobile phones and portable computers. Asset roles cannot be assigned directly to users, but can be assigned to IT Roles and Business Roles.

attest An action performed by an attestor during an access review to confirm that a user entitlement is appropriate.

attestation The process of certifying that a specific user has the appropriate privileges on the appropriate resources at a specific point in time. An Waveset user with permission to view and respond to an attestation work item is called an *attestor*. Waveset rules determine whether a user entitlement record needs to be manually attested, or if it can be automatically approved or rejected.

attestation task

A logical collection of user entitlement reviews requiring attestation. User entitlements are grouped into a single attestation task if they are assigned to the same attestor and produced from the same access review instance.

attestor

User who accepts responsibility for certifying (*attesting*) that a user entitlement is appropriate. An attestor has extended privileges in Waveset that are necessary to manage user entitlements requiring attestation.

business process editor (BPE)

Graphical view of Waveset forms, rules, and workflow provided with Waveset versions prior to 7.0. The BPE has been replaced by the Identity Manager IDE in the current versions of Waveset. See Glossary.

Business Role

One of the four role types in Waveset, Business Roles are used to organize into groups the access rights that people who do similar tasks in an organization need. The Business Role role-type is made up of one or more Asset roles, Application roles, and/or IT Roles. Business Roles are meant to be directly assigned to users.

capability

A group of access rights for user accounts that governs actions performed in Waveset; a low-level access control within Waveset.

delegation

The process of temporarily assigning future work items to one or more other users for a specified period of time.

directory junction

Hierarchically related set of organizations that mirrors a directory resource's actual set of hierarchical containers. Each organization in a directory junction is a *virtual organization*.

entitlement

See *user entitlement*

escalation timeout

A time range specified for a work item request in which the assigned work item owner has to respond before the Waveset process sends it to the next assigned responder.

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 Manager IDE

The Identity Manager Integrated Development Environment (Identity Manager IDE) is an application that enables you to view, customize, and debug Oracle Waveset objects in your deployment. The Identity Manager IDE is available as a NetBeans plug-in.

identity template

Defines the user's resource account name.

IT Role

One of the four role types in Oracle Waveset, the IT Role role-type is a collection of roles (Assets, Applications, and/or other nested IT Roles), as well as resources, and/or resource groups. In some configurations, IT Roles can be directly assigned to users, but usually IT Roles are assigned to Business Roles, which are assigned to users.

organization

Oracle Waveset 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 Oracle Waveset administrative purposes.

periodic access review

An access review that is performed at periodic intervals, for example, every calendar quarter.

policy Establishes limitations for Oracle Waveset accounts.

Oracle Waveset 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.

reconciliation An Oracle Waveset feature that periodically compares resource accounts in Oracle Waveset with accounts that reside on the resources themselves. Reconciliation correlates account data and highlights differences.

remediation The process of correcting compliance violations discovered by Oracle Waveset's auditing feature. Oracle Waveset audits data across the enterprise to ensure compliance with internal and external policies and regulations. An administrator with permission to view and respond to policy violations is called a *remediator*.

remediator An Waveset user specified as the assigned remediator for an audit policy.

When Waveset detects a compliance violation that requires remediation, it creates a remediation work item and sends the work item to the remediator's work item list.

resource In Oracle Waveset, a resource stores information about how to connect to a remote resource or system on which accounts are created. Remote resources to which Oracle Waveset provides access include mainframe security managers, databases, directory services, applications, operating systems, ERP systems, messaging platforms, and more.

resource adapter Oracle Waveset component that provides a link between the Oracle Waveset engine and the resource.

This component enables Oracle Waveset 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 Oracle Waveset 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 Oracle Waveset tool that steps through the resource creation and modification process, including setup and configuration of resource parameters, account attributes, identity template, and Oracle Waveset parameters.

role A role is an Oracle Waveset object that allows resource access rights to be grouped and efficiently assigned to users. Roles are organized into four role types: Business Roles, IT Roles, Application Roles, and Assets. IT Roles, Applications, and Assets organize resource entitlements into groups. These three groups are then assigned to Business Roles so that users can access the resources they need to do their jobs.

rule Object in the Oracle Waveset 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 Oracle Waveset account attributes for a resource.

Oracle Waveset account attributes create a common link to multiple resources and are referenced by forms.

service provider users Extranet users, or customers of a service provider that are distinguished separately from the service provider company's personnel or intranet users.

user Person who holds an Oracle Waveset system account. Users can hold a range of capabilities in Oracle Waveset. Those with extended capabilities are Oracle Waveset *administrators*.

user account Account created using Oracle Waveset.

Can refer to either an Oracle Waveset account, or an account on a remote resource managed by Oracle Waveset. 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 entitlement In Oracle Waveset, an auditable access privilege granted to a user on a resource or system that enforces access restrictions.

user interface In Oracle Waveset, the user interface allows users without administrative capabilities to perform a range of self-service tasks such as changing passwords, setting answers to authentication questions, and managing delegated assignments. Also known as the *end-user interface*

virtual organization Organization defined within a directory junction. *See* directory junction.

work items an action request generated by an Waveset workflow, form, or procedure. Approvals, change-approvals, attestations, and remediations are four kinds of work item.

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

Index