HP OpenView Select Identity

For the Red Hat Enterprise Linux and
Microsoft Windows 2003 Operating Systems

Software Version: 4.0

Administrator's Guide

March 2006

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils.
- Commons-collections.
- Commons-logging.
- Commons-digester.
- Commons-httpclient.
- Element Construction Set (ecs).

- Jakarta-poi.
- Jakarta-regexp.
- Logging Services (log4j).

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge.
- iText (for JasperReports) developed by SourceForge.
- BeanShell.
- Xalan from the Apache XML Project.
- Xerces from the Apache XML Project.
- Java API for XML Processing from the Apache XML Project.
- SOAP developed by the Apache Software Foundation.
- JavaMail from SUN Reference Implementation.
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation.
- Java Cryptography Extension (JCE) from SUN Reference Implementation.
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation.
- OpenSPML Toolkit from OpenSPML.org.
- JGraph developed by JGraph.
- Hibernate from Hibernate.org.
- BouncyCastle engine for keystore management, bouncycastle.org.

Trademark Notices

UNIX® is a registered trademark of The Open Group.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Welcome to Select Identity

Studies show that the IT costs associated with maintaining a manual identity management solution are climbing. As companies grow and collaborate with greater numbers of customers and partners, manual methods require significant resources and time to meet expanding requirements.

HP OpenView Select Identity provides a new approach to identity management called Business Services Identity Management (BSIM), which is the first truly scalable solution for managing identity within and between large enterprises. The HP OpenView Select Identity BSIM solution automates the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries.

HP OpenView Select Identity addresses the challenges of identity management (IdM) in complex, extended, and federated enterprises with its BSIM solution. BSIM replaces the static role-based conceptual model of IdM with a new and more powerful model, which facilitates the creation of "dynamic roles."

Key Product Features

The OpenView Select Identity solution increases efficiency, productivity, and security for the complex or extended enterprise through the following key business features:

- **Centralized Management** – Provides a single point of control for the management of users and entitlements
- **Provisioning** – Automates the creation, update, and deletion of accounts and entitlements on information systems across the enterprise
- **Administrative Delegation** – Enables administrative rights to be distributed to multiple tiers of functional departments, customers, and partners

- **My Identity Self-Registration** – Optionally enables end users to initiate access to subscribe to services, change passwords, set password hints, and update general identity information through a simple web-based client based on your company's specific needs
- **Approval Workflow** – Automates approval processes required to grant access privileges to users
- **Password & Profile Management** – Manages and distributes password and user profile information across and between enterprise information systems
- **Audit and Reporting** – Provides standardized reporting on actions and user account activity

With HP OpenView Select Identity, provisioning and management of user accounts and privileges is no longer a barrier to realizing the efficiencies and competitive advantage of extending system access to ever greater numbers of employees, customers, and partners.

HP OpenView Select Identity provides a service-centric approach to managing identities. In any company, its employees, customers, and partners participate in a number of services or business processes that comprise the operation of the company. For example, these processes might include "order processing" or "accounts receivable." Each service may consist of a number of applications or resources that require unique access privileges depending on its participants and corporate policy. HP OpenView Select Identity incorporates these complex relationships and leverages them to automate the tasks associated with managing identities, including provisioning of accounts and privileges, approval workflows, delegation of administrative rights, enforcement of security policy, and reporting. HP OpenView Select Identity mitigates the limitations of the traditional role and rule-based identity management, enabling scalability throughout the extended enterprise while reducing deployment times and management costs.

Support

If you need to call support for help regarding HP OpenView Select Identity deployment or maintenance, please have the version and build numbers available for the representative. View the version and build numbers on the About page by navigating to **Help** → **About**.

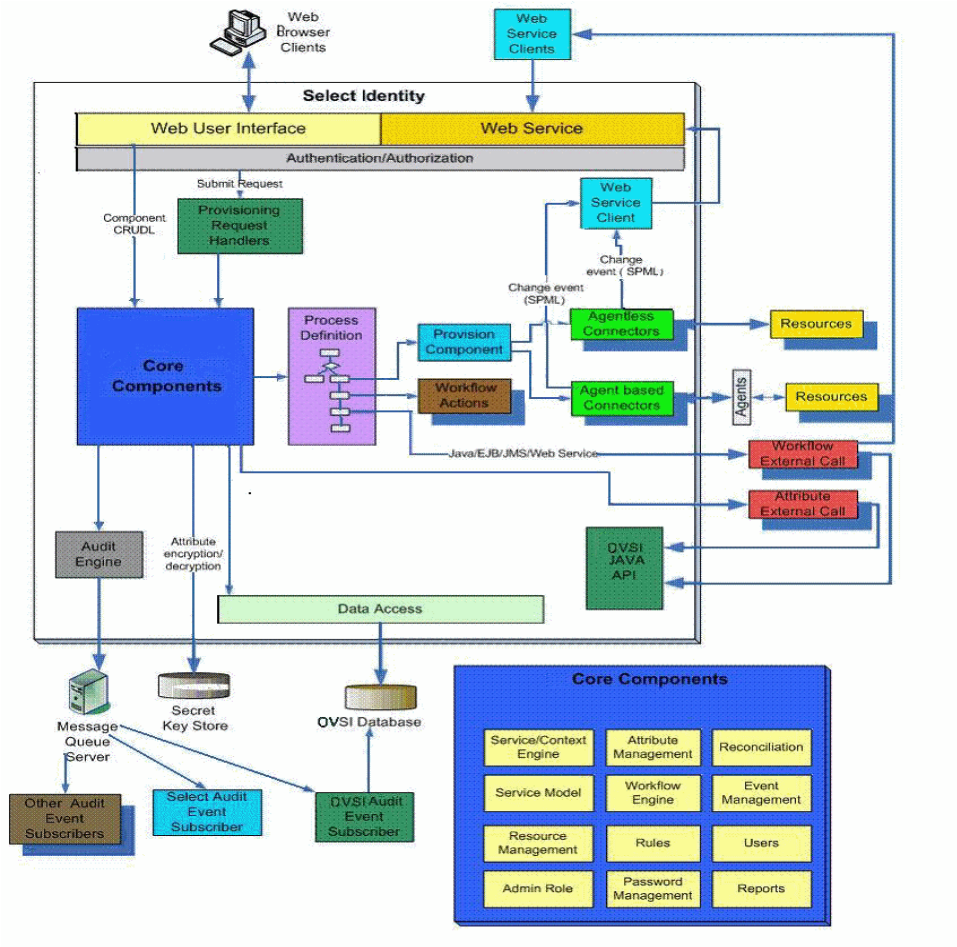
Configuring and Optimizing HP OpenView Select Identity

It is strongly recommended that you customize HP OpenView Select Identity before you start using it. Performance during tasks such as User Import and Reconciliation is impacted if Select Identity is not optimized. For more information, refer to the HP OpenView Select identity Installation Guide, which contains a section about how to configure the product after installation. Configuration tasks should be performed by a qualified system administrator.

System Architecture

HP OpenView Select Identity is an event-driven, J2EE application that enables clustering, failover, multi-phase commit, and asynchronous operation. The following illustration provides a high-level view of the Select Identity system and its components.

Figure 1 HP OpenView Select Identity Architecture



All requests to and from the system use the HTTP protocol. User accounts use one virtual ID to access back-end systems and services and are governed by HP OpenView Select Identity system functions and actions. Accounts are also governed by attributes and entitlements based on the access requirements of the company's products and services.

The Context Engine and Identity Business Process Services components of the HP OpenView Select Identity architecture are particularly useful to administrators and personnel responsible for deploying and maintaining the Select Identity system. These components contain the functions that administrators use most.

The HP OpenView Select Identity core components include the following:

- **Service / Context Engine** – Assembles the hierarchy of services and service roles. Filters groupings based on context user groups.
- **Attribute Management** – Facilitates the configuration and setup of attributes in a service, e.g., the definition, characters that make up an attribute and any constraints that apply.
- **Reconciliation** – Reports on the consistency of a user's identity data in multiple resources. Synchronizes any change that occurred on a field designated to sync in or out such as a telephone number change, by replicating it in all the applicable resources and / or the HP OpenView Select Identity database.
- **Service Mode**l – Provides an abstraction layer that allows change management of users' belonging to a service so that it is more dynamic and flexible. HP OpenView Select Identity's object model. Users and groups are not tied tightly to resources or systems, unlike other identity management products in the market.
- **Workflow Engine** – Provides a facility to create, modify, and delete the process steps used in provisioning one or more users.
- **Event Management** – Determines what workflow process or view applies to an event, e.g., add a user.
- **Resource Management** –Captures the definition and details about the resource, whether or not it is authoritative, and allows the administrator to verify connection to the resource.
- **Rules** – Allows for the creation, modification, viewing, and deletion of rules that determine how information is imported and exported throughout the reconciliation process.
- **Users** – Permits management of users in a service. This includes creation, modification, and deletions of user accounts. Users are assigned to services that are subscribed to them, and attributes that apply to these services also apply to the user account.

- **Admin Role** – Defines a role for one or more users to administer one or more service accounts. Multiple Admin Roles may be created to handle the varied administration needs of any one company.

2 Getting Started

HP OpenView Select Identity (OVSI) automates and simplifies all identity management tasks, including provisioning of accounts and entitlements, execution of business process workflows, delegation of administrative rights, enforcement of security policy, auditing, and reporting.

Select Identity's Business Services Identity Management solution provides an organizational business model that supports best practices for business processes associated with identity management. This chapter provides an overview of the Select Identity interface and how to use Select Identity to design an identity management model for your business. Detailed procedures for each task are provided in subsequent chapters and in online help.

This chapter covers the following topics:

Signing In and Out

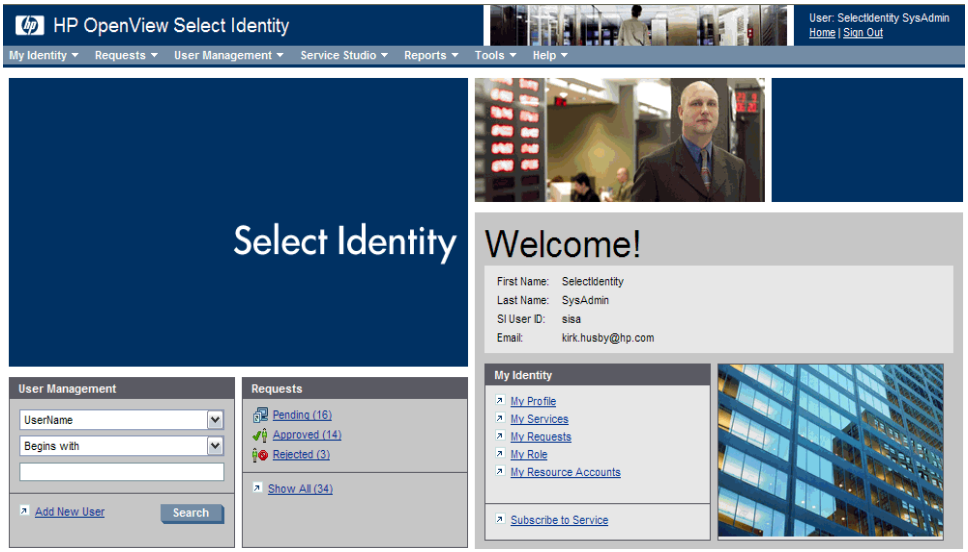
Signing In

To sign in to HP OpenView Select Identity, you must obtain the host name, port number, login ID, and password. You sign in by entering the following URL in the web browser where *app_svr_host:port* is either `WebLogic:7001` or `WebSphere:9080` (ports are default values):

http://*app_svr_host*:*port*/lmz/signin.do

The Sign In page displays.

Figure 2 Sign In Page



The following information is used by the first user who logs into HP OpenView Select Identity for the first time.

User Name = sisa

Password = abc123

Change this user name and password as quickly as possible. All users who sign in for the first time may be prompted to change their account password immediately based on your company's specific password policies.

It is highly recommended that, the first time you sign in, you create a new Select Identity administrative account that meets your company's security policy. This account belongs to the System Administrator role. See Creating and Managing Administrative Roles on page 38 for information on defining roles.

Signing Out

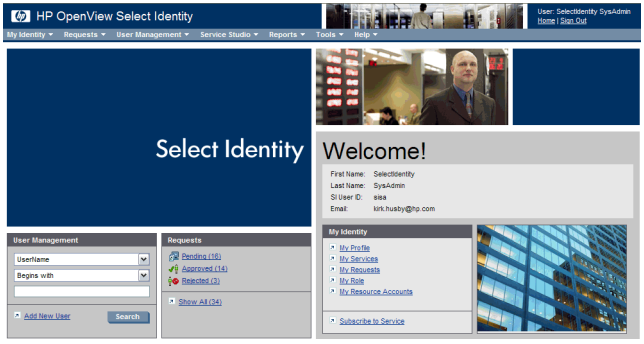
To log out of Select Identity, click on the Sign Out link in the top right corner of each page.

HP OpenView Select Identity Interface

After signing in to Select Identity, the Select Identity Home page displays (see Figure 4). The Home page displays information based on the user's profile and privileges. Panels on the page and information in the panels, as well as menus and menu items are shown or hidden according to the access privileges of the user. All users see some form of profile information under the title bar.

This section gives you a quick tour of the HP OpenView Select Identity interface based on a user that has all administrative rights. This means that all menus and possible information that a user could see displays, as shown in the following sample Home page.

Figure 3 Sample Home Page



Access all functions and actions through the panels and menus on the menu bar.

This section covers the following information:

- Home Page Panels
- Menus

Home Page Panels

This section briefly describes the contents of the following panels, with links to the associated sections in this guide:

- User Profile Information Panel
- My Identity Panel
- User Management Panel
- Requests Panel
- Service Studio Panel

User Profile Information Panel

All users can view the following information on the Home page about their account profile:

- SI User ID
- First Name
- Last Name
- Email address

My Identity Panel

The My Identity panel enables users to quickly access their available identity information, based on the privileges they are given. For details on how to set up and manage user identity tasks, see Managing My Identity on page 313. For detailed instructions on using the My Identity function for end users, see the *HP OpenView Select Identity My Identity User Guide*.

The My Identity menu contains most of the same options as the My Identity panel links. See My Identity Menu on page 13 for details.

The My Identity panel includes the following links (if the user has permission to see them all):

- **My Profile** — enables users to modify user profile information. See Modifying Profile Information on page 314.
- **My Services** — enables users to view a list of Services to which they belong. See View Services Permission on page 322.
- **My Requests** — enables administrators only to view their requests and request status. See Request Status on page 329.
- **My Role** — enables administrators only to view the roles to which they have been assigned and the permissions (entitlements) given for each role. See Administrative Roles on page 33 for details.
- **My Resource Accounts** — enables users to view the resources on which they belong. See Managing Resources on page 64.
- **Subscribe to Service** — enables users to add themselves to a Service. See Self-Subscribe Permission on page 322. This link is not in the My Identity menu.

User Management Panel

The **User Management** panel enables you to perform the following actions:

- **Search for user** — enables you to search for users using filters to refine your search. See Using Select Identity Search Features on page 17 for details.
- **Add New User** — enables you to add a new user. See Creating a User on page 278. You can also use the menu options: **User Management Menu** → **Create User**.

See User Management Menu on page 13 for User Management actions.

Requests Panel

The Requests panel enables administrators to quickly find information about their requests through the following links (see Request Status on page 329) for details:

- **Pending** — view all pending requests.

- **Approved** — view all requests that have been approved.
- **Rejected** — view all requests that have been rejected.

See Requests Menu on page 13 for Requests actions.

Service Studio Panel

The Service Studio panel provides short cut links to Service Studio functions. See

- **Resources** — navigates to the Resource List page used to add and manage resources. See Managing Resources **on page 62**.
- **Attributes** — navigates to the Attribute List page used to manage attributes. See Managing Attributes **on page 99**.
- **Notifications** — navigates to the Notification Template List page used to create and manage notification templates. See Managing Notification Templates **on page 124**.
- **Services** — navigates to the Service List page used to create and manage Services. See Service Studio on page 55.
- **External Calls** — navigates External Calls List page used to register to manage external calls. See External Calls on page 249.
- **Workflow** — navigates to the Workflow Template List page used to create and manage your business workflow templates. See Workflow Studio on page 273 for basic information about using workflows. See the *HP OpenView Select Identity Workflow Studio Guide* for procedures and complete information on how to create and modify workflow templates.

Menus

A user with complete administrative rights will see the following menus:

- My Identity Menu
- Requests Menu
- User Management Menu
- Service Studio Menu
- Reports Menu

- Tools Menu
- Help Menu

Each menu and its options is briefly described with links to the associated chapters.

My Identity Menu

The My Identity menu contains most of the options that are in the My Identity panel. See My Identity Panel on page 10 for descriptions of the following menu options:

My Profile
My Hint Questions
My Services
My Requests
My Role Permissions
My Resource Accounts

Requests Menu

The **Requests** menu enables you to perform the following actions (see Request Status on page 329):

- **Request Worklist** — enables you to specify which requests you want to view, modify, approve, or reject as well as view the status of that request.
- **Request Status** — allows you to view (based on your entitlements) the complete transaction status for account events within Select Identity based on the assigned workflow process.

User Management Menu

The User Management menu enables you to perform the following actions (see Users on page 277 for details):

- **User List** — enables you to for and manage users. You can add, modify, enable, disable, and terminate users.
- **Create User** — enables you to create (add) a new user. See Creating a User on page 278.

Service Studio Menu

The **Service Studio** menu enables you to perform the following actions and functions:

- **Resources** — enables you to add and manage resources. See Managing Resources **on page 62**.
- **Attributes** — enables you to manage attributes. See Managing Attributes **on page 99**.
- **Notifications** — enables you to manage notifications. See Managing Notification Templates **on page 124**.
- **Services** — enables you to create and manage Services. See Service Studio on page 55.
- **External Calls** — enables you to manage external calls. See External Calls on page 249.
- **Workflow** — enables you to create your business workflow. See Workflow Studio on page 273 for basic information about using workflows. See the *HP OpenView Select Identity Workflow Studio Guide* for procedures and complete information on how to create and modify workflow templates.

Reports Menu

The **Reports** menu enables you to perform the following functions:

- **Audit Reports** — enables you to create and manage audit reports. See Audit Reports on page 461.
- **Configuration Reports** — enables you to create and manage configuration reports. See Configuration Reports on page 467.
- **Request Status** — Enables you to view information about requests that have been submitted. See Viewing Request Status on page 329.

Tools Menu

The **Tools** menu enables you to perform the following actions:

- Admin Roles
  - **Admin Role List** - enables you to add and manage administrative roles. See Modifying a Role on page 44.

- **Create Admin Role** - allows you to add a new admin role. See Creating an Administrator Role on page 39.

- User Import
  - **User Import List** - permits you to view User Import job requests. SeeUsing User Import on page 232
  - **Schedule User Import** - enables you to schedule a User Import job. See Scheduling the User Import on page 235.
  - **Service Assignment List** - allows you to schedule the assignment of users to services. See Service Assignment List Page on page 240
  - **Schedule Service Assignment** - permits you to schedule the assignment of users to services. See Scheduling a Service Assignment on page 242.
- Bulk
  - **Bulk Job List** - permits you to view and manage bulk jobs. See Viewing Bulk Jobs
  - **Schedule Bulk Move** - enables you to schedule the movement of a group of users from one context to another. Scheduling a Bulk Move User Task
  - **Bulk Task List** - allows you to view Bulk job tasks. See Viewing Job Results.
- Challenge \ Response Settings - enables you to create and manage challenge response questions used when users are given the ability to reset their own passwords through self registration. See Changing Challenge/Response Settings.
- Import \ Export Configurations
  - **Import Configuration** - enables you to import configurations from HP OpenView Select Identity instances See Importing a Configuration on page 456.
  - **Export Configuration** - allows you to export configuration from HP OpenView Select Identity instance to be imported to another. See Exporting a Configuration on page 452.
- Reconciliation
  - **Reconciliation Job Lis**t - permits you to view and manage See Scheduling Jobs on page 433

- **Reconciliation Task List** - allows you to view and modify reconciliation at the task level. See Viewing the Task Status on page 440.

- Rules
  - **Rule List** - permits you to view and manage reconciliation SPML files. See Managing Rules on page 377.
  - **Add Rule** - enables you to upload a new or modified SPML rule files. See Adding a Rule to the Rule List on page 377
- Server Management
  - **Server Instance List** - allows you to view the status of servers within a cluster when you work in a clustered server environment. See Viewing the Server Work List on page 504.

Help Menu

The Help menu provides an online help administrator's guide, Workflow Studio guide, online help, an About option for information about the HP OpenView Select Identity application, and a link to the HP Support web site.

Understanding Passwords

HP OpenView Select Identity manages and synchronizes multiple passwords used throughout an enterprise. This is typically the case as legacy systems, client-server and newer technology systems are often managed by different IT groups and require different password formats, strengths and policy. The key to managing multiple passwords in Select Identity lies in the attribute management function. An HP OpenView Select Identity admin can create as many attributes as needed to properly provision user-related data into a resource. A resource's password is simply another attribute in SI, which can be pushed to the resource during account creation and reset activities.

Select Identity ships with one password attribute – Password. This attribute cannot be removed as it is used for authentication into SI itself. It can also be used to push the same password to any number of identity stores (resources), thus synchronizing SI with the resources. However, multiple password attributes can be created, one for each resource if a customer wanted to do such. Each password attribute must have a unique text name and each will

contain a unique password policy, such as min./max characters allowed during registration, or whether the password should be auto-generated to a corporate standard.

Once a password attribute is used to provision a user, that password is tracked by HP OpenView Select Identity for the life of the user's existence in Select Identity. Subsequent password reset requests will display all password attributes for the user, thus all resource(s) using that password attribute will be synchronized. This mapping of password attribute to resource can be 1:1 or 1: many.

Multiple passwords may be established for a single user as well if single sign on is not selected. Passwords may be managed at the service and the resource level. See Resetting Passwords on page 294 to learn more about managing user's passwords

Using Select Identity Search Features

The search function enables you to search for matching values. Search functions are provided on all list pages and on other pages as necessary. Searches often provide filter options. Filter options help you narrow the criteria so that the values returned are more likely to contain a match. Filter your search by entering specific values in one or more fields. When values are entered in more than one field the values returned must match each of the values entered.

.

Search Method	Criteria
Drop Down Filter Options	Select the appropriate criteria from one or more predefined lists and enter the search text in the entry field.
Icon Filter Options	Select the appropriate icon in the top-left panel to filter the information shown in the right-panel of the page.
Conditions	Enter text in the blank text box and select a predefined condition. You can use wildcards before, in the middle, or at the end of characters. For example, you can perform a search specifying: **First Name** **Includes** ***ath*** Text may be case sensitive.

.

The Search icon displays instead of the drop-down lists when the number of items is above a configurable threshold. Refer to the *HP OpenView Select Identity Installation Guide* for information on configuring the search criteria property.

Understanding Field Types

Select Identity uses several types of fields in order to capture data in the most efficient and convenient way.

Field Type	Action Required
Entry	Type data in these fields.
Drop down Menus	Menus used to make selections based on a predefined list of possible choices.
Multi-Line Text Box	Enter the date into the field, then click the **Add** button to insert it into the multi-line text box. Repeat the process until all data is entered. Delete unwanted data by highlighting the text and clicking **Remove** or by deselecting a highlighted item Only highlighted text is applied.
Search List Box	Click the  or  icon to add data to the list. Remove unwanted data by deselecting the text or by clicking  when available. Only highlighted text is applied.
List Box	Type text in one or more fields located to the left of the list box, then click the to insert the text in the list box. Edit existing text by clicking on the  icon to move the text back to the entry fields, then make the necessary changes and click  to reinsert the text in the list box. Delete the text by highlighting the item and clicking the **Remove** button or  icon when available. Only text in the list box will be applied.

Field Type	Action Required
Check box	Click on or more check boxes to insert a check
Radio Button	Select only one button of the options show.
Calendar	Click the  icon and select the date. Delete a date by highlighting the date and pressing the **Backspace** key.

.

Some list boxes and allow you to change the order of the selected items when appropriate. Highlight the item you want to move and use the and icons to move it up or down in the list.

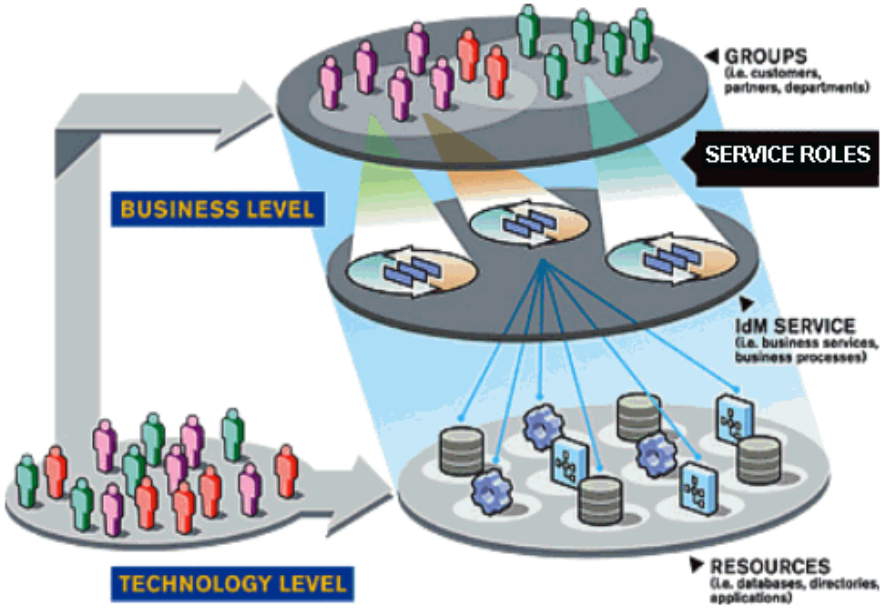
Understanding Business Services Identity Management

HP OpenView Select Identity's Business Services Identity Management (BSIM) solution provides a model for designing, implementing and managing identity management business processes. for an enterprise-level business or large organization.

To support today's companies, best practices in provisioning require identity management to focus on connecting customers to the business processes, rather than to the individual resources themselves. BSIM, HP OpenView Select Identity's ground breaking approach, does just that. Select Identity's focus on connecting customers to business services creates a host of benefits and efficiencies across the enterprise. This "business level" abstraction ensures customers have access to the systems and the rights within those systems that they need to do their jobs.

Select Identity's BSIM solution provides a business level model for managing customers' access to resources. This approach groups elements independently into manageable units called Services and Context user groups that correspond to existing business structures. Within Select Identity, a Context user group defines how groups of users access Services through well-defined and understood Service Roles, as shown in the following figure.

Figure 4 Business Services Identity Management Model



Select Identity's recommended approach takes the guesswork out of designing a Business Services Identity Management Solution. It gives you the framework for crafting the best approach, and saves you time and effort.

Workflow for Designing and Building Your Business Model

HP OpenView Select Identity allows you the flexibility to use set up features that determine how Select Identity can best meet your company's need. Begin by building a model of your business by considering how each of the functions listed below should be set up.

The basic steps for designing and building your business identity management model are shown below:.

Step 1	Gather business requirements and design the conceptual solution
Step 2	Define your workflow and provision models
Step 3	Determine the environment suitable for Select Identity and complete the installation taking care to read through the *HP OpenView Select Identity Install Guide* manual and set the user defined Tru.Access properties correctly to meet your business needs.
Step 4	Define and set up user Roles based on your business model.
Step 5	Deploy the connectors used to maintain your resources
Step 6	Set up application and data store resources and the resource attribute fields you plan to provision with HP OpenView Select Identity. Determine the reconciliation policies used to provision those resources and attributes.
Step7	Create the Notification Templates used in the approval processes defined in Workflow Studio.
Step 8	Create work flow in Workflow Studio used to manage the approval process.
Step 9	Build services and define context user groups and service roles. Create the forms your users will use when accessing HP OpenView Select Identity
Step 10	Write and register any external calls required to support your workflows.
Step 10	Set challenge / response questions if your company will allow users to maintain their own passwords through My Identity self registration.

Step 11	Create and load Reconciliation Rules.
Step 13	Create the SMPL files used to define import parameters and load them into User Import. Use User Import to add users to your solution
Step 14	Use User Management to maintain the imported user accounts.
Step 15	Set up My Identity Self Registration if your company uses these features.

Understanding Deployment

HP OpenView Select Identity automates and simplifies all identity management tasks, including provisioning of accounts and entitlements, execution of business process workflows, delegation of administrative rights, enforcement of security policy, auditing, and reporting.

After installing Select Identity, begin the deployment process. Select Identity creates a logical identity for each user, which links the user to the respective resources, resource IDs, and enterprise systems such as LDAP and web single sign-on services. Select Identity's use of the enterprise/relationship model and the logical identity approach enables you to manage users in a simple, efficient, cost-effective, and secure manner.

Deployment Concepts

This section provides an overview of the tasks necessary to deploy HP OpenView Select Identity in your enterprise. Detailed procedures for each task are provided in subsequent chapters and in online help.

You can deploy Select Identity in several ways. This guide provides a comprehensive view of all deployment tasks in a logical order that you can follow or adapt to fit your business needs. As with any enterprise-class software deployment, you may want to review your business requirements and security policies before performing any of the following tasks. Having all of your system information organized and available expedites this process.

Connectors

HP OpenView Select Identity uses J2EE connectors to interface with system resources that contain identity profile information. You may have received a set of connectors with your initial Select Identity purchase, or you may have used the Connector APIs to create your own. Connector management defines the communication criteria by which HP OpenView Select Identity reconciles identity information with your system resources. Each resource type in your environment requires a matching connector. For example, if your identity information resides in LDAP, Windows, and UNIX systems, you must deploy a connector for each system type.

Each Connector provided by HP comes with a guide designed to help you install and maintain your connector interface. Deploying and managing system connectors is performed through the Connectors function and includes the add, modify and delete functions.

For more information, see Managing Connectors on page 59.

Resources

Resources represent the applications, databases, and directories that HP OpenView Select Identity provisions. This application views resources as user data stores in which accounts and entitlements can be created, modified, and deleted. Typical resources in your environment might be Windows Server Systems or UNIX. After you deploy connectors for each resource type, you can add the resources on which your products and services rely.

Select Identity maps virtual user IDs to the IDs contained in the data stores of your systems. The end result is that no matter how many back-end user data stores reside in your environment, Select Identity creates a single, unified view of a user that spans all of the resources that contain information about the user. For example, you may offer a service to your customers that relies on a database or web single sign-on service. After you add these resources in the system, the end user accessing the service has one logical HP OpenView Select Identity ID, which maps to the user accounts on both the database system and the web single sign-on system.

With connectors deployed, you simply provide the addresses of the machines in your environment and HP OpenView Select Identity creates the bridge to each data store. HP OpenView Select Identity then uses administrative authority to access each user data repository in each resource as each service requires based on parameters set up by your company.

Adding and managing system resources is performed through the Resources function and includes the add, modify, view, copy, and delete functions.

For more information, see Defining Service Roles on page 169.

Attributes

HP OpenView Select Identity uses attributes and their values to map user data to the correct resources and entitlements. Attributes are also used within Select Identity to enable account and service management. Create any number of attributes to reflect user profile data, physical location, or other business management criteria.

Each connector installs a mapping file for resource attributes. This file provides a means by which HP OpenView Select Identity attributes are mapped to each resource or data store. Use the Attributes function in Service Studio to add, modify, view and delete attributes.

For more information, see Using Attributes to Facilitate User Searches on page 102.

External Calls

When accounts are added to HP OpenView Select Identity, they are verified through a series of attributes and workflow approval steps, which you define. Depending on your environment, one of those steps may require a call to a third-party application or system. External calls allow you to create these calls to validate account attributes or lookup approvers. An external call invokes a user-defined function in order to interface with an external system and update user profile information based on the data returned by the system.

For more information, see the *HP OpenView Select Identity External Call Guide*.

After you create external calls required by your business, register each call through the External Calls function. Calls that are not registered cannot be seen by HP OpenView Select Identity. Use the External Call function to view, modify, and delete registered external calls.

For more information, see Deploying an External Call on page 261.

Notifications

The Notifications section of the client enables you to define the content of email notices that are sent to users when a system event occurs. By creating these policies, you define the messages that the Select Identity system sends to users and administrators. These messages are useful at different stages in a workflow process.

Notices are sent to a user when an event occurs, such as account approval, rejection, or modification. Email can also be sent when an account password or hint is reset.

Creating and managing notification policies is performed through the Notifications function and includes the following actions:

- Add, delete, and modify notification policies
- Copy notification policies
- View notification policies

For more information, see Notification Variables on page 124.

Workflow Studio

Workflow is the process by which user requests for Service access are approved and provisioned by Select Identity. These provisioning events include the addition and removal of accounts and can require any number of approval steps. Each step, defined in a workflow template, can include a call to individuals or external systems for validation and approval. Steps within a workflow process can also send notifications to systems and individuals. Workflow templates also enable you to track the progress of a system event through the Request Status pages. See Request Status on page 329 for more information.

Creating workflow templates is performed through the Workflow Studio function. For overview information, see Workflow Studio on page 273. All conceptual and procedural information for Workflow Studio is in the *HP OpenView Select Identity Workflow Studio Guide*.

Challenge Response

While password characteristics are defined with attributes, you can define challenge and response hints for users who forget their passwords. Accounts can also be locked after a number of failed attempts.

See What is Challenge/Response? on page 307 for more information.

Service

A Select Identity Service encapsulates all of the resources, entitlements, workflows, policies, and other identity management elements related to a single business service. For example, you may have a Service, such as Customer Support, that includes all of the identity management components related to your help desk, including CRM and Internet support portal systems. The Services function enables you to add, view, modify, and delete the Services that are accessed by your customers and business partners. Services are made available to your customers and partners by setting Service Roles and Context.

Creating and managing Services, Service Roles, and Context is performed through the Services function within Service Studio and includes the following actions:

- Create, modify, copy, and delete Services
- Set Service attribute values and properties
- Create, modify, and delete Service Form views
- Create, modify, and delete Service Roles
- Create, modify, and delete Context

For more information, see Service Studio on page 55.

Context

Context functionality enables you to define logical groupings for users based on identity profile attributes and values. For example, you can create Contexts for England, India, and China that are dependent on the “country” attribute (an attribute that you defined in Attribute Management). When users register for a Service, the value for the country attribute determines the Context in which a user is managed.

Service Roles

A large part of Service creation involves establishing Service Roles within Context user groups. These are the roles you want to assign to employees, customers, and partners. The Service Roles you create define how companies, organizations, or divisions access your Services. Service Roles create a secure context in which partners and users of your Services see only what is relevant to them based on customized forms you design.

Setting Service Roles enables you to assign workflow templates and notification policies. You can also define attributes that are fixed for users. Management of Service Roles is hierarchical, which creates a secure way for Services to be shared across different companies or locations.

Administrative Roles

After you define Services, you can establish the administrative roles that are relevant for each. Administrative roles determine the functions and actions that Select Identity administrators can perform within the system. Administrators may be assigned to administer one or more services. Administrators may be grated permission to administration all functions with in HP OpenView Select Identity or a subset functions specific to the skills and responsibilities assigned to that administrate. See Granting Permissions to the New Admin Role on page 41.

Select Identity provides basic roles that reflect the functions and actions that are performed within the system. You can use the roles as defined, edit these roles, or create your own to better reflect your business needs.

Creating and managing administrative roles is performed through the Administrative Roles function, which includes add, view, modify copy, and delete Admin roles

For more information, see Administrative Roles on page 33.

Roles are assigned through a user's association with an administrative Service. See Service Studio on page 55 for more information.

User Import

The User Import function enables you to add multiple users to one or more Services. User Import is helpful for new installations. Use this process to add user accounts directly from the resources that are defined to support a Service. This process relies on the use of a data file to upload information to the Select Identity system.

See User Import on page 223 for complete information about this process.

Bulk

You can upload several user accounts to multiple Services simultaneously. This enables you to populate your system without having to add hundreds or thousands of individual user accounts. Use Bulk upload for accounts that do not already exist in a resource or in the Select Identity system. Accounts are added to both the Services that you select and the resources that support it.

You can also use this function to move a group of users from one Service context to another.

See Bulk Add or Move on page 341 for complete information about this process.

Users

Users are added to the system by Select Identity administrators or through the registration process defined for a Service. The workflow template and Service Role that you have assigned to each context determines how this process takes place.

Creating and managing user accounts is performed through the Users function in the client and includes the following actions:

- Add, and modify user accounts
- View Service membership
- Add Service access to an existing user

- Enable and disable Service membership
- Enable and disable all Services
- Delete Service membership
- Terminate user accounts
- Manage user account expiration dates
- Reset account passwords
- View user account attributes
- Move user to another Service context

For more information, see Users on page 277.

Request Status

When user accounts are added to the system, you can view status and approval-process details by using the Request Status function. Request Status enables you to view color-coded workflow steps that are executed, not executed, or are waiting approval. HP OpenView Select Identity provides a default report template for displaying workflow information.

Request Status includes the following actions:

- View pending, approved, and rejected requests
- Modify pending requests
- Approve or reject pending request
- View request status
- View approval status

For more information, see Request Status on page 329.

Configuration and Audit Reporting

All account management processes can be viewed through audit and configuration reports. You can generate audit reports to monitor regular account interaction. Configuration reports display current information related to the setup of the Select Identity system.

For more information, see Chapter 17, Audit and Configuration Reports.

Rules

Reconciliation rules are XML files executed by OpenView Select Identity when a new user is added or updated from an Authoritative resource through the Reconciliation function. Rules provide a flexible mechanism for handling exception cases when assigning entitlements and monitoring authoritative sources. In addition, rules can be used when moving a user from one context to The XML files are created and then uploaded using the Rules functionality which includes add, modify, view, and delete.

For more information, see Rules on page page 365.

Reconciliation

You can synchronize HP OpenView Select Identity account data with other system resources and attributes. For more information, see Account Reconciliation on page 401.

Configurations

HP OpenView Select Identity enables you to configure your system in any environment, then import or export its key components, such as services, attributes, templates, and accounts. This enables you to easily move from a test to a production environment.

Managing system configurations is performed through the Configurations function and includes the following actions:

- Importing configurations
- Exporting configurations

My Identity Self Registration

HP OpenView Select Identity offers several self service functions provided through the My Identity self registration menu. Your company's set up determines what if any functions may be managed by your users. Using self registration functionality reduces the number of routine tasks that must be performed by system administrators on a regular basis.

User management of accounts includes the following possible actions:

- Changing passwords and password hints
- Delegating Admin Roles, if an administrator
- Viewing account profile
- Requesting accesses to additional resources
- Requesting accesses to additional service accounts
- Viewing the status of change requests made against your own account

For more information, see Managing My Identity on page 313.

3 Administrative Roles

Create administrator roles to govern the actions each administrator can perform within the HP OpenView Select Identity system. There are predefined roles already set up for your convenience. View and modify the existing roles to meet your own company's needs. If your environment requires more granular roles, create your own.

Administrative roles are made available to users through Services designed specifically for management. When you create a Service, you have the option to define it as an Admin Service. You can then add one or more users to this Admin Service to assign administrative roles to your users in charge of system administration. See Creating Services on page 142 for information about creating a Service.

HP OpenView Select Identity provides great flexibility so that you can set up your identity management structure the way that best serves your business. This system provides n-tier or any number of levels of delegation of management tasks. Your organization can delegate any range of management permissions to internal users, customers, and partners as needed. Administrators have access to only those services assigned to the administrative function.

Services are a combination of resource applications and data structures that communicate through one connector interface. Giving administrators permission to administrate applications through services allows one administrator to administrate multiple applications and data stores provisioned by each assigned service. For example, one administrator might administrate customer access to your purchasing and billing systems while another administers access to internal support applications.

Administrators may delegate their roles to other users as well. This feature gives you the flexibility to make sure administrative functions are covered whether or not the designated administrator is available. Delegation prevents you from having to create and assign a new role each time an administrator goes on leave, takes vacation, or is gone for any other reason. See Delegating an Admin Role on page 49.

This chapter covers the following topics:

- Administrative Functions and Actions
- Creating and Managing Administrative Roles

Administrative Functions and Actions

You may want to familiarize yourself with HP OpenView Select Identity administrative functions and actions before creating Admin Roles. Roles and actions are designed to represent all of the management functions within Select Identity and are named accordingly. Each grouping of actions is represented by a management link in the client application.

This section covers the following:

- Understanding Functions and Actions
- Reviewing Default Roles

Understanding Functions and Actions

Use roles to grant an HP OpenView Select Identity Administrator permission to perform a group of actions performed within each management functional area in the client application. The actions assigned to each administrator help form a view of the system. Management functions may be assigned to more than one administrator, but each administrator must have at least one function.

The following are all of the actions available to administrators organized by function.

Functions	Actions
Request Status	Permits the user to view and modify requests.
Request Worklist	Allows the user to view, then approve or reject requests in a pending status.
Reports	Determines the specific reports users are allowed to access. Users given access to a report get permission to add, view, modify, run, schedule and delete the report. Partial access cannot be given.
Connectors	Gives the user authority to manage connectors for the services assigned to the administrator. Admins may view, deploy, modify, or delete according to the permissions granted.
Resources	Provides the administrator with the authority to manage resources for applications and data stores within assigned services. Admins may view, deploy, modify, delete, and / or copy resources. Additionally administrators may view attribute fields. and / or modify attribute field mapping based on permissions given.
Services	Determines the authority an admin has to manage assigned services. Admins may be given permission to create, modify, and / or delete service forms, service roles, and / or Context user groups. Admins may also be given permission to reconcile services and set service attribute properties for assigned services.
Notifications	Allows the admin to view, add, copy, and / or delete notification templates for assigned services.
External Calls	Gives the user the right to manage external calls by viewing, adding, modifying, and or deleting calls used by assigned services.

Functions	Actions
Workflow Studio	Determines the admin's permission to add, copy, view, modify, and / or delete workflow diagrams that govern how resources are provisioned.
Attributes	Provides permission to add, view, modify, map and / or delete attribute fields throughout the system.
Admin Roles	Allows the administrator to manage admin roles by viewing, adding, copying, modifying, and or deleting roles.
Challenge/ Response	Permits the admin to modify challenge / response questions and settings for assigned services.
User Import	Gives the admin the authority to import users from external resources into HP OpenView Select Identity for assigned services. Admins may schedule user import jobs, import user lists, schedule service assignment, and / or view services assigned based on the permissions given.
Reconciliation	Determines the admin's access to create and manage reconciliation jobs used to provision users on assigned services. Permission may be granted to add, view, modify, and / or delete reconciliation jobs. Admins may also be given permission to view the tasks of any job being processed for services assigned.
Bulk	Gives the user permission to manage attribute changes from HP OpenView Select Identity to external resources. Permission may be granted to add, view, modify, and / or delete bulk jobs. Admins may also be given permission to view the task of any job being processed for services assigned.

Functions	Actions
Configurations	Allows the user the permission to import and export XML files used to move configurations from one instance of HP OpenView Select Identity to another. Admins may also export XML configuration files, make changes, then import the files back into the same instance.
Rules	Gives the admin the right to upload, view, modify, and delete XML and SPML files used to govern reconciliation.
Server Management	Allows the user to view the status of servers used by HP OpenView Select Identity for provisioning purposes.
Users	Allows the user to add, view, modify, disable, enable, delete, and /or transfer user accounts, service memberships and user authorities within the proper user group Context and assigned services. Admins may also receive permission to view resources assigned to users, reset passwords, move user accounts and / or terminate users within assigned services.

Reviewing Default Roles

HP OpenView Select Identity offers default roles for your use. Use the existing roles “as-is” or modify one or more to better match your business requirements.

End User
All users added to HP OpenView Select Identity are granted this role automatically. Additionally, users added through User Import are granted this role each time a user first logs in. Each user receives a default set of permissions. You can change the permissions granted to End Users by default by modifying this role. See Modifying a Role on page 45.

An end user is simply a user of HP OpenView Select Identity services. Accounts with this user role have only the entitlements granted through registration of a Service. Users granted the End User role gain access to the

My Identity self service menu which may be customized to meet your organization's specific needs. See Administrative Roles on page 33 for more information.

Approver
An Approver often called the Workflow Approver, performs account provisioning actions. The system automatically grants this role to users assigned any approval task. A user with this role can approve user account additions, modifications, or deletions for those users within the Approver's Context user group.

System Administrator
Often called the Concero Sys Admin this administrator has the most powerful administrative role including: Admin Role, Connector, Resource, Workflow, Service, Notification, User, External Call, and Attribute management actions. You cannot delete this role.

Creating and Managing Administrative Roles

The Admin Roles function enables you to create, modify, and manage the roles that define each administrator's permission to access to the HP OpenView Select Identity system.

This section covers the following:

- Adding an Administrator Role
- Modifying a Role
- Copying a Role
- Deleting Admin Roles
- Viewing Admin Roles

Adding an Administrator Role

You can add any number of roles to meet your management needs. Roles are later assigned to users through Administrator Services. Save time when creating a new admin role that is very similar to an existing role by copying and modifying the matching role instead. See Copying a Role on page 48.

Complete the following tasks to add an administrator role:

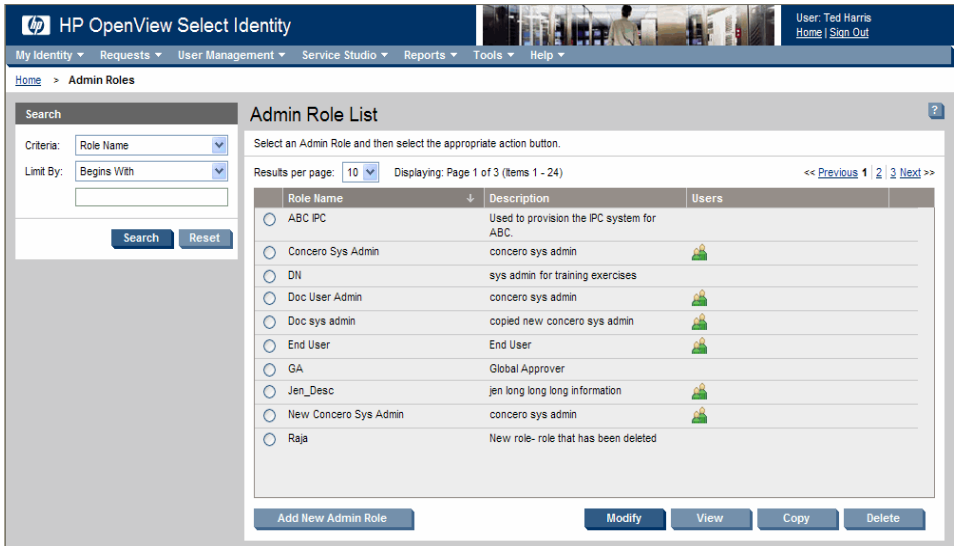
- Creating an Administrator Role
- Granting Permissions to the New Admin Role

Creating an Administrator Role

Perform the following steps to create a new administrator role:

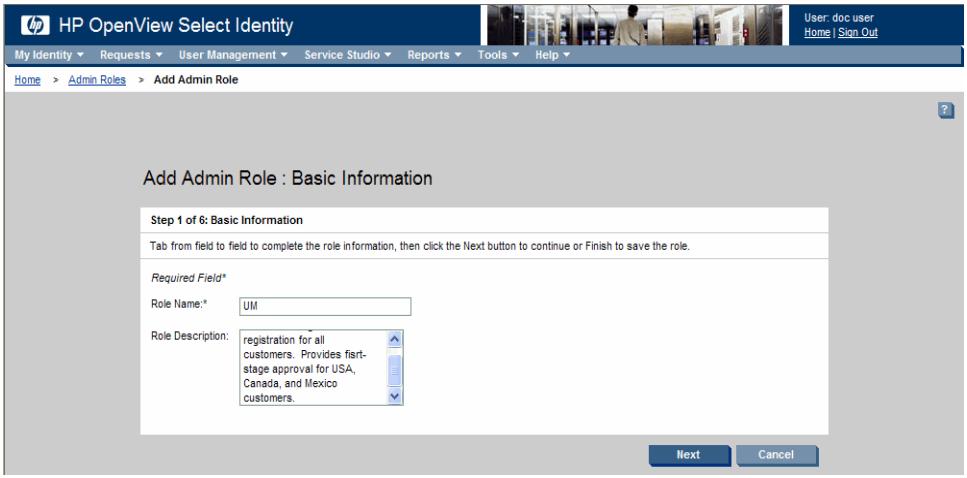
1 Select the **Tools -> Admin Roles -> Create Admin Role** menu options.
The **Admin Role List** page opens.

Figure 5 Admin Role List Page



2 Click **Add Admin Role**.
The **Add Admin Role: Basic Information** page opens.

Figure 6 Add Admin Role: Basic Information

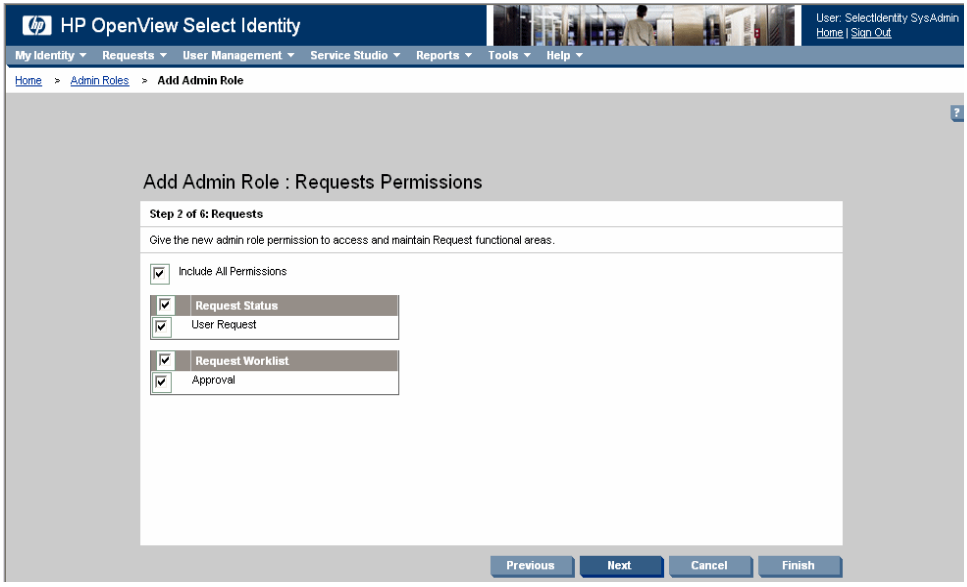


3 Enter a name for this role in the **Role Name** field.

4 Enter a brief description for the role in the **Role Description** field.

5 Click **Next**.
The **Add Admin Role: Requests Permissions** page opens.

Figure 7 Add New Admin Role: Request Permissions Page



Granting Permissions to the New Admin Role

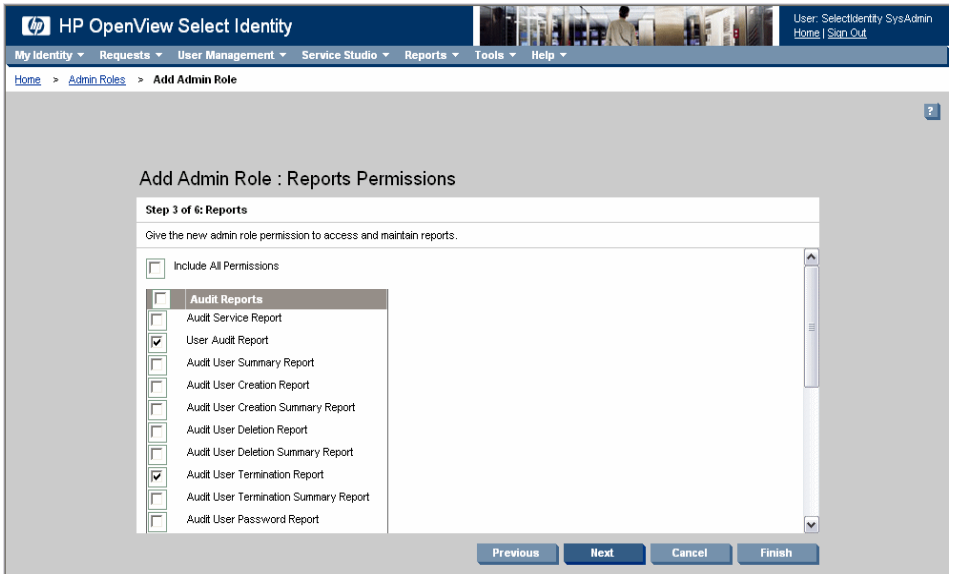
Take great care to review your permission selections to be sure you are granting the right authority to this new role. Complete the steps below to grant permissions to the newly created Admn Role:

If the role will be granted all or most of the available permissions on the page, then click the **Include All Permissions** check box.

1 Review the list of available permissions and select the applicable options.

2 Click **Next**.
Opens the **Add Admin Role: Reports Permissions** page.

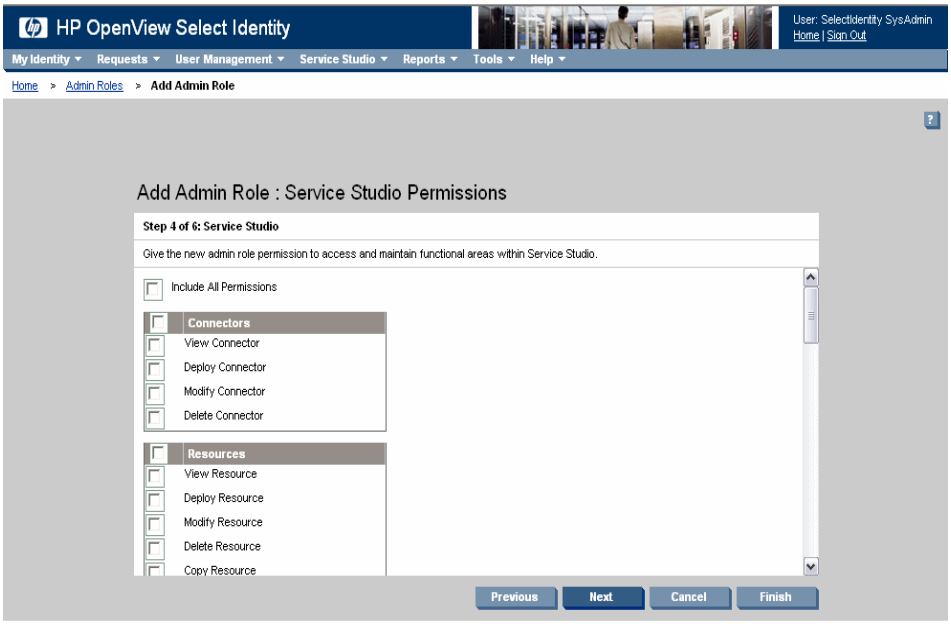
Figure 8 Add Admin Role: Reports Permissions Page



3 Review the list of available reports and select the reports this role should use.

4 Click **Next**.
The **Add New Admin Role: Service Studio Permissions** page opens.

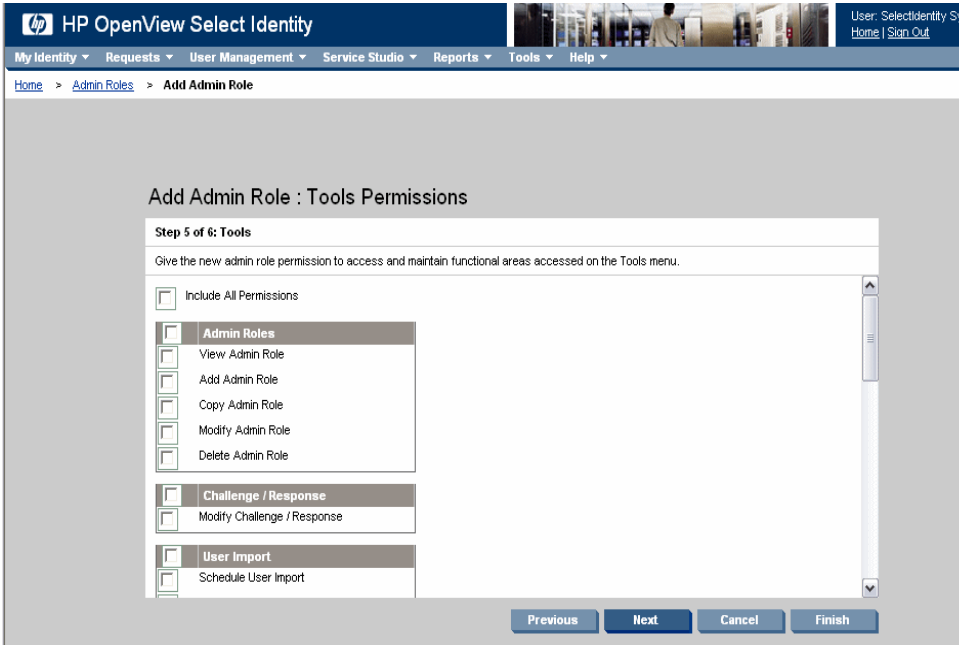
Figure 9 Add New Admin Role: Service Studio Permissions Page



5 Review the list of available Service Studio permissions and select the applicable options.

6 Click **Next**.
The **Add Admin Role: Tools Permissions** page opens.

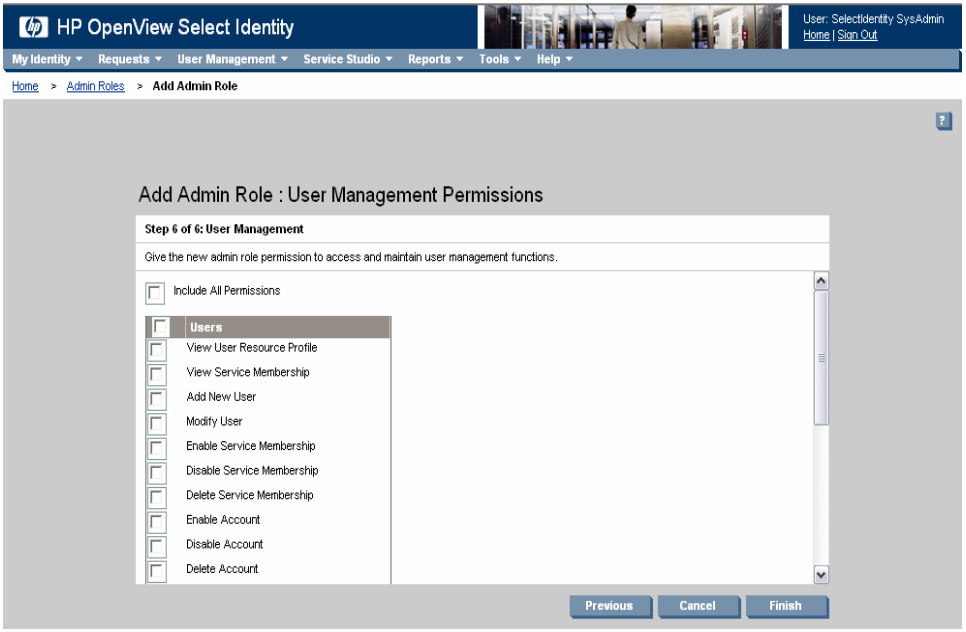
Figure 10 Add New Admin Role: Tools Permissions Page



7 Review the list of available administrative tools and select the applicable options.

8 Click on the **Next** button.
The **Add New Admin Role: User Management Permissions** page opens.

Figure 11 Add New Admin Role: User Management Permissions Page



9 Review the list of available user management tasks and select the applicable options.

> Do not select the Transfer Accounts permission. This functionality will be available for future use, but is not available now.

10 Click **Finish**.
Returns to the **Admin Role List** with your new administrative role displayed.

> Notice that only roles with users assigned have the user icon in the **Users** column.

Modifying a Role

Change the authority granted to an admin by modifying the permissions granted to the admin role. Complete the following tasks to modify an administrative role:

- Modifying a Role

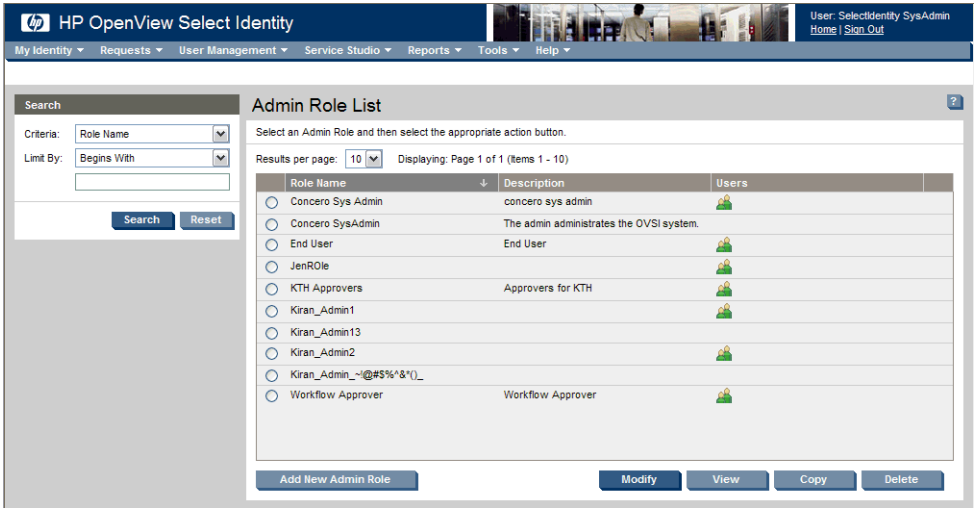
- Modifying Permissions Granted to a Role

Modifying a Role

Perform the following steps to modify an admin role:

1 Select the **Tools > Admin Roles > Admin Role List** menu options.
The **Admin Role List** page opens.

Figure 12 Admin Role List Page

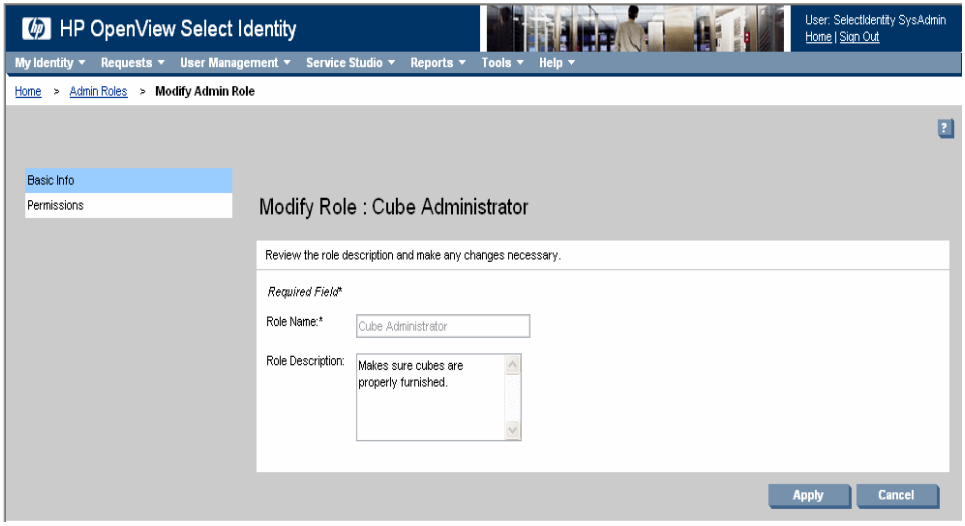


2 Select the role you want to modify.

> You can also search for the administrator role by using the **Filter** search panel. See Using Select Identity Search Features on page 17 to learn more.

3 Click **Modify.**
Opens the **Modify Admin Role: Role Name** page.

Figure 13 Modify Admin Role: Role Name Page



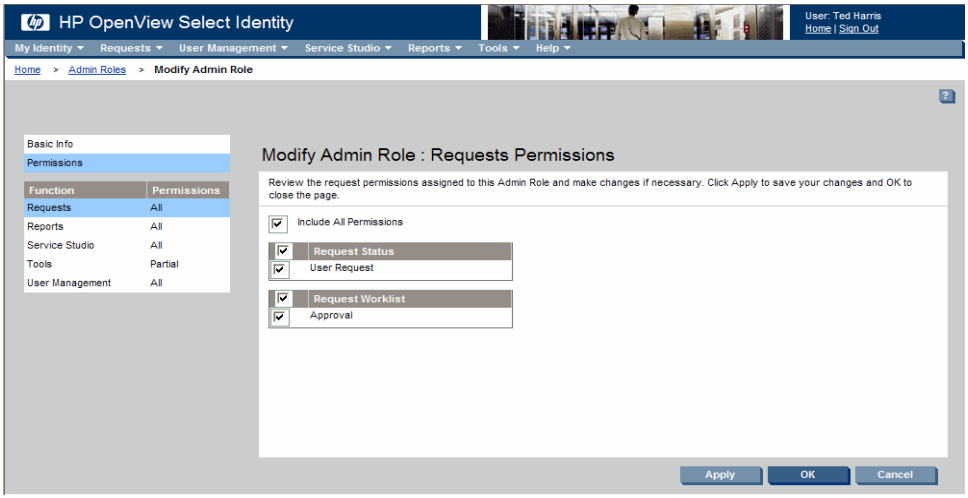
4 Review the **Role Description** field and make any changes necessary.

5 Click **Apply**.
Saves your changes.

Modifying Permissions Granted to a Role

1 Click the **Permissions** link in the left panel.

Figure 14 Modifying Admin Role: Requests Permissions Page



2 Review the functions listed in the left panel and click the function you want to modify.
Opens the selected permissions list.

> Do not select the Transfer Accounts permission from the User Management permissions list. This functionality will be available for future use, but is not available now.

3 Review the list of available permissions, then select or deselect any option you want to modify.

4 Click **Apply**.
Saves your changes.

5 Repeat the procedure until all necessary permissions have been changed in each functional category.

6 Click **OK**.
Returns to the **Admin Role List**.

Copying a Role

If you have permission to do so, you can create new admin roles by copying and modifying existing roles. You must have permission to both create and modify a role before you can complete the copy procedure. Use this method to save time when you have to create one or more admin roles that are nearly the same.

Complete the following procedures to copy an Admin Role:

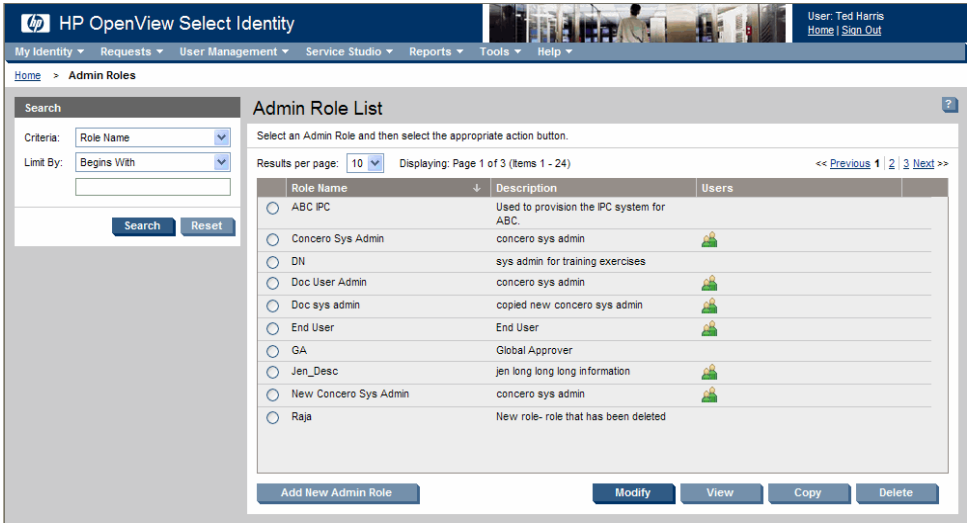
- Copying the Admin Role
- Modifying Permissions Granted to a Role

Copying the Admin Role

Perform the following steps to copy an administrative role:

1 Select the **Tools -> Admin Roles -> Admin Role List** menu options.
The **Admin Role List** page opens.

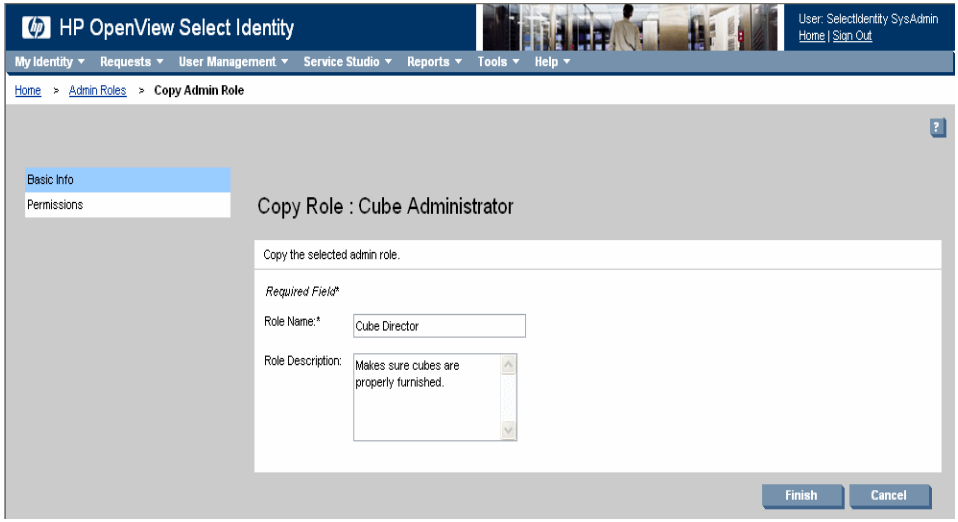
Figure 15 Admin Role List



2 Select the role you want to copy.

3 Click **Copy.**
The **Copy Admin Role: Role Name** page opens.

Figure 16 Copy Admin Role: Role Name



4 Click the **Role Name** field and change the name.

5 Review the **Role Description** and make any changes necessary.

6 Save any changes.

Be aware that modifying permissions from a copy operation is not permitted. Access to view permissions is available; however attempts to change permissions from this screen fail.

Delegating an Admin Role

Delegation of Admin Roles is optional. Administrators delegate their roles using the My Identity self service tools when the HP OpenView Select Identity system has been set up to provide this privilege See *HP OpenView Select Identity My Identity Guide* for more information.

Deleting Admin Roles

With the exception of the Concero Sys Admin Role, Workflow Approver, and End User, every administrator role created can be deleted. Review the services administered by the admin role prior to deleting any role. Remove obsolete

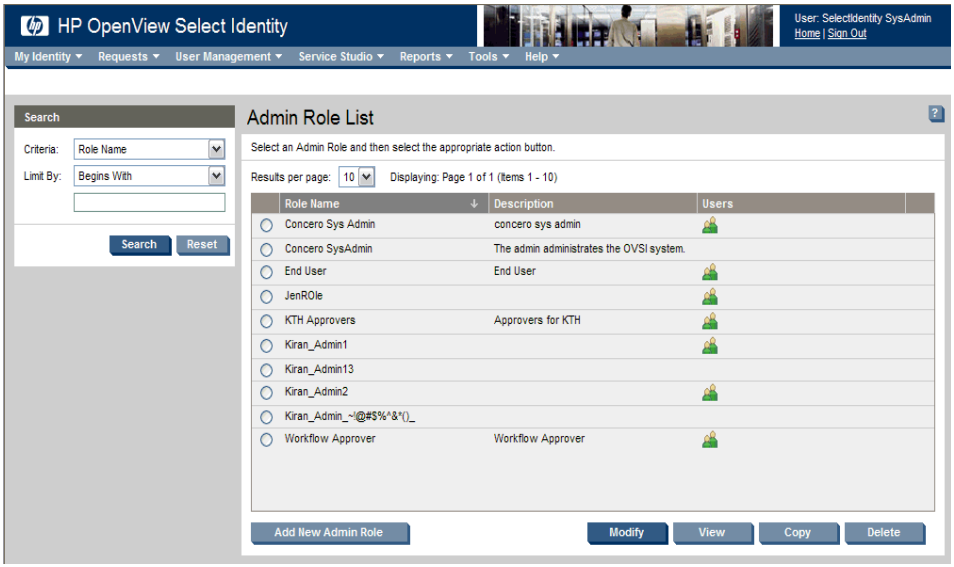
services and the functions they support prior to deleting a role. See Deleting a Service Role on page 205. Make sure valid services continue to be serviced by one or more admin roles.

Delete a Role

Follow the steps below to delete an admin role:

1 Select the **Tools > Admin Roles > Admin Role List** menu options.
The **Admin Role List** page opens.

Figure 17 Admin Role List



2 Select the role you want to delete.

3 Click **Delete.**
The confirmation dialog box opens.

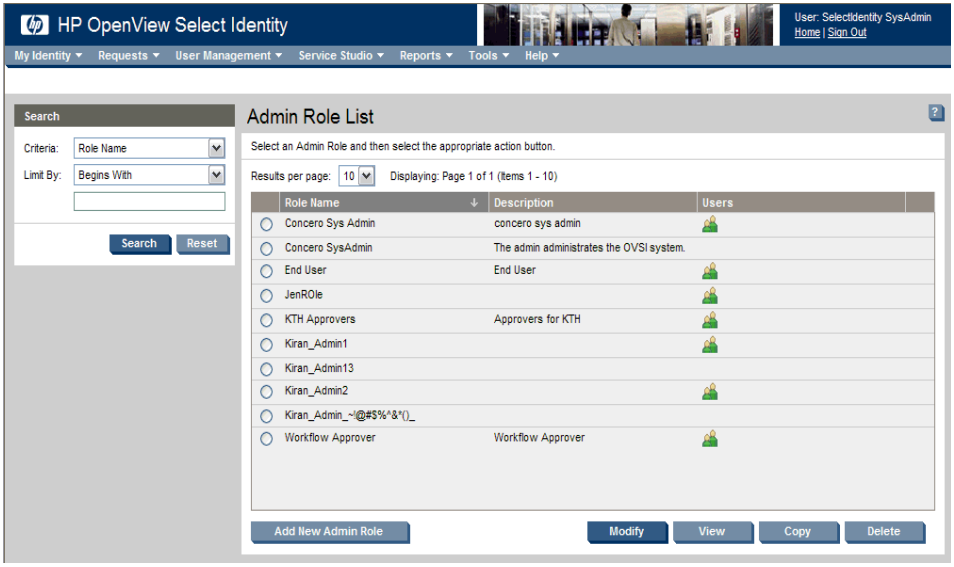
4 Click **OK**.
Deletes the role.

Viewing Admin Roles

Follow the steps below to view an admin role:

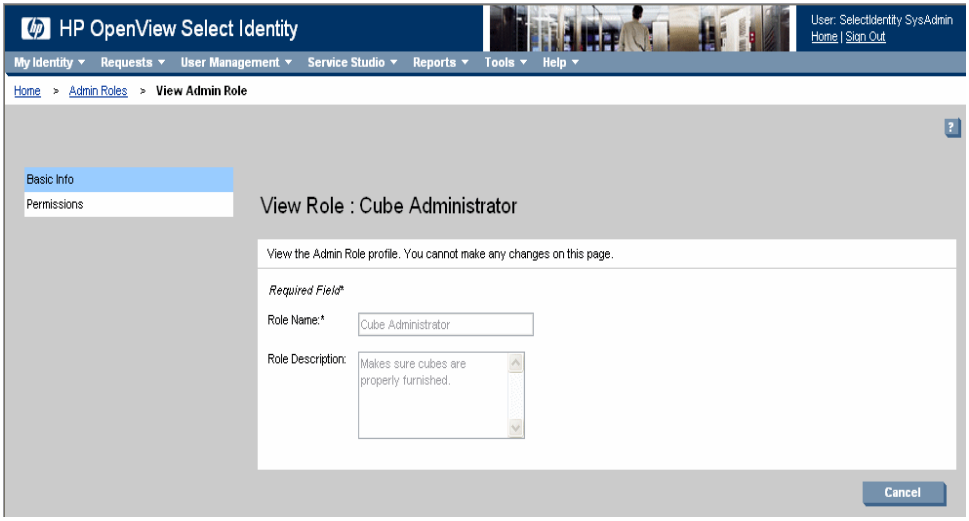
1 Select the **Tools > Admin Roles > Admin Role List** menu options. The **Admin Role List** page opens.

Figure 18 Admin Role List



2 Select the Admin Role you want to view and click **View.** The **View Role: Admin Name** page opens.

Figure 19 View Role: Admin Page



3 If you wish to see the permissions granted this role, click the **Permissions** link in the left pane.
The **View Role: Requests Permissions** page appears.

4 When finished, click **Cancel**.
Returns to the **Admin Role List**.

4 Service Studio

Select Identity provides a service-oriented architecture. Identities are viewed and managed within the context of the Services to which they have access. The Services pages enable you to create and manage the Services that are accessed by your customers and business partners. When creating Services, you define a number of elements that will determine how your users access the system and the entitlements that they are granted when doing so.

There are three types of services.

Admin Services – Provide a means of associating administrative roles to user accounts. For every business service created there must also be a companion administrative service for one or more administrators to manage users on the business service.

Business Services – Represent the business products and applications that are accessed by your customers and partners.

Composite Services – Enable Service grouping. Users registering for a composite service can have access to multiple Services, which usually include at least one admin service and one or more business services.

Each service also enables you to set and view Service Roles, which provide a secure management structure along custom views for your partners and customers. Service Roles are hierarchical and management can be delegated to any level.

This chapter provides details for all of the actions that you can perform within the Service Studio pages. Access to each of these functional areas is determined by the administrative roles assigned to your account by the Select Identity system administrator.

This chapter covers the following:

Building a Service Foundation from Service Studio

Services should be created only after all resources, attributes, notification templates, and workflows are in place. These are the foundations on which a well defined Service is built. Everything you need to manage your services is available to you from the Service Studio menu. You can set up and manage resources and resource attributes, develop workflows customized by External Calls and even create customized notification templates.

Once all the prerequisites are in place, then create and manage services. This section covers the following:

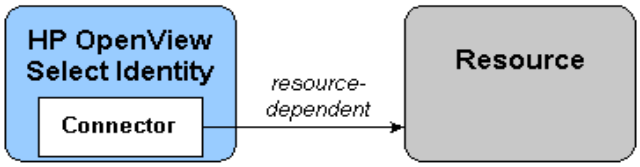
- Understanding Connectors
- Managing Connectors
- Managing Resources
- Managing Attributes
- Managing Notification Templates

Understanding Connectors

Select Identity enables you to connect to enterprise applications and resources to configure and manage user accounts and entitlements in those systems. The component that enables OVSI to access and interface with a resource server is called a **connector**. The connector acts as a gateway between OVSI and the resource.

OVSI supports two types of connectors:

- One Way
  A one-way connector initiates communication with a resource. If a resource is supported through the use of a one-way connector, provisioning operations initiated by Select Identity are synchronized with the resource through the connector. The following diagram illustrates the flow of data:



Current One Way Connectors include the following:

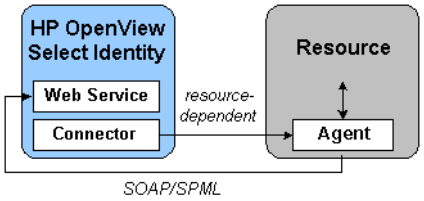
- AS400
- BOKS
- Domino
- LDAP
- NT Domain
- NT Local
- Peoplesoft
- RACF
- SAP
- Siteminder
- TAM
- Tandem
- Top Secret
- UNIX
- VMS
- UNIX BSH
- Universal

The connector resides on the Select Identity server and sends requests to the resource. The resource defines the protocol that must be used by the connector to issue the request. To create a one-way connector, you must create the connector and install it on the Select Identity server.

- Two Way
  A two-way connector contains the connector that resides on the OVSI server and an agent that resides on the resource. The connector

communicates with the agent and the agent performs the provisioning operations. The agent also listens for changes on the host resource and sends notices to Select Identity when changes are detected. Thus, a two-way connector enables data to flow in two directions, as illustrated in the following diagram. Changes to user accounts can occur on either system.

Figure 20 Data flow between Select Identity and a two-way connector, through a resource agent



Current two-way Connectors include the following:

- Active Directory
- DB2
- Oracle
- Lotus Notes
- MS SQL Server

The connector issues a request according to the resource's specifications. When the agent issues a request to Select Identity's web service, it does so through the Simple Object Access Protocol (SOAP) with a Service Provisioning Markup Language (SPML) payload through HTTP or HTTPS.

Creating and Installing a Connector

To create a connector that enables Select Identity to connect to a system resource in your environment, build a resource adapter using the J2EE connector Java Connector Architecture (JCA)). To do this, you must have an understanding of the Java Developer Kit (JDK) and you should be familiar with the JCA. In addition, Select Identity provides a Connector Access Protocol Interface (API) to be used in conjunction with JCA to create connectors. After you build the connector, install it on the Select Identity

server, which enables you to deploy it and create resources in the Select Identity client. Each connector is supplied with an installation guide that contains information about associated connector and attribute mapping files.

Install connectors by deploying the `connector.rar` file on the Select Identity application server. See the *HP OpenView Select Identity Connector Installation Guide*, which is included on the Select Identity Connector CD for more information. The *HP OpenView Select Identity Connector Guide* provides details about developing connectors, including methods to be implemented in the Select Identity Connector API. Refer to this guide for an API overview, packaging instructions, and an installation procedure. The Connector API is documented and available in online help.

Managing Connectors

You must have one connector interface gateway in order for Select Identity to communicate with your resource(s), but you may have many to choose from. Use one connector for each server resource type that you want to support. However more than one resource may use the same connector. For example, in order to connect to three LDAP servers, you install and deploy only one LDAP connector. Resources that share a connector are placed in a resource pool.

Before a Connector can interface between Select Identity and the designated resource(s) there must be a record of the connector in Select Identity. Connector records cannot be created unless the connector has already been installed on the server.

This section covers the procedures necessary to do the following:

- Deploying a Connector
- Modifying a Connector Record
- Deleting a Connector Record

Deploying a Connector

1. Select **Service Studio** → **Resources** from the menu bar options. Opens the **Resource List** page.
2. Click the **Manage Connectors** button, at the bottom of the page. The **Manage Connectors** page opens.

3 Tab from field-to-field and enter the required information.

Field	Action
Connector Name	Enter the complete name of the connector. **Note:** If the Attribute Mapper is available (as indicated by a "yes" in the **Mapper Available** column), the connector name must be *identical* to the second portion of the pool name (the section after `eis/`).
Pool Name	Enter the full name of the resource pool that you want this resource to belong to.
Mapper Available	Select **Yes** if Mapper is available to this connector or **No** if it is not. This file maps the connector to the resource, and defines where and how identity information is stored on that resource.

4 Click **Add**.
Inserts the newly created Connector record into the list below.

5 Click **OK**.
Saves your work and returns to the **Resource List** page.

Modifying a Connector Record

Sometimes Connector parameters change. When this happens you must modify the associated connector record in Select Identity.

1 Select **Service Studio** → **Resources** from the menu bar options.
Opens the **Resource List** page.

2 Click the **Manage Connectors** button at the bottom of the page.
The **Manage Connectors** page opens.

3 Select the connector you want to modify from the list of connectors displayed.

4 Click **Modify** at the bottom of the page.
Moves the connector details to the **Current Resource Connectors** section at the top of the page.

5 Tab from field-to-field and enter the required information.

Field	Action
Connector Name	Modify the name of the connector if necessary.
Pool Name	Change the resource pool to which you want this resource to belong if necessary.
Mapper Available	Select the **Yes** if Mapper is available to this connector or **No** if it is not. This file maps the connector to the resource, and defines where and how identity information is stored on that resource.

6 Click **Apply**.
Inserts the newly created Connector record into the list below.

7 Click **OK**.
Saves your work and returns to the **Resource List** page.

Deleting a Connector Record

If a resource is no longer used by your company, delete its connector as well.

1 Select **Service Studio** → **Resources** from the menu bar options.
Opens the **Resource List page**.

2 Select the resource you want to modify.

3 Click the **Manage Connectors** button at the bottom of the page.
Opens the **Manage Connectors** page.

4 Select the connector you want to delete from the list of connectors displayed.

5 Click **Delete**.
Opens the confirmation dialog box.

6 Click **OK**.
Deletes the connector from the list permanently.

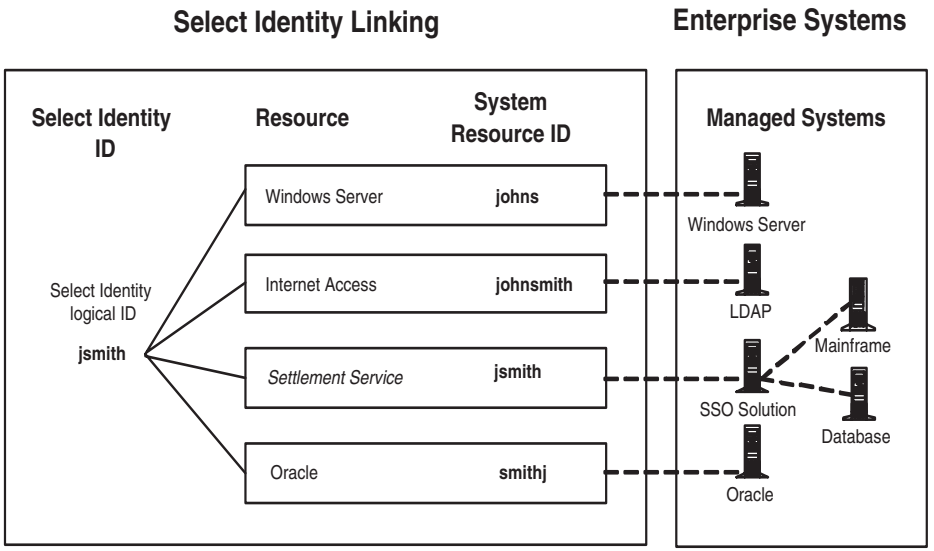
Managing Resources

Resources in the Select Identity system represent the physical applications, databases, and directories that Select Identity relies on for account information. Select Identity views resources as user data stores in which accounts and entitlements can be created, modified, and deleted. Typical resources in your environment might include Windows Server Systems or Oracle databases.

With the Resources section of the Select Identity client, add, view, copy, modify, and delete the resources to which Select Identity maps its users. The end result is that no matter how many back-end user data stores you have in your environment, Select Identity creates one user ID to provide access to the Services that they support.

The following illustrates this concept.

Figure 21 Select Identity Linking Example



For example, you may offer a Service to your customers that relies on a database, such as UNIX or web single sign-on service. Select Identity provides a unified view of a user identity named *jsmith*. Select Identity's concept of an

identity is not only system-wide, it is enterprise-wide. If a user leaves the company, for example, Select Identity tracks all of the various resources where the user has an identity (account and entitlements) and can act appropriately.

Using Authoritative Resources

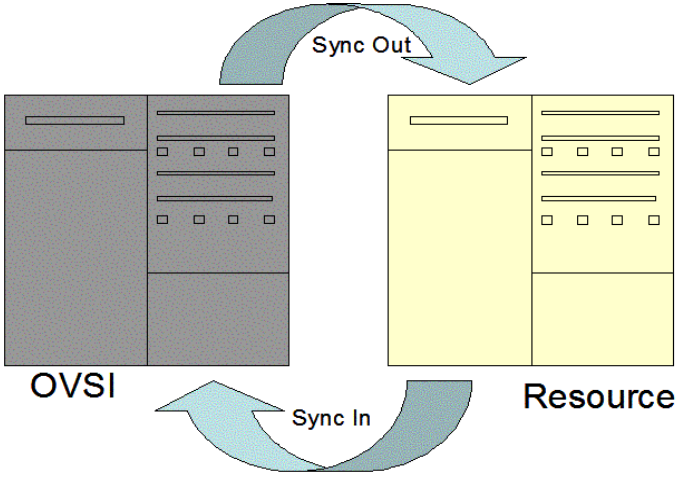
Select Identity provides you with the ability to establish a baseline resource used to keep all other accounts in sync. For example, your human resources system may control all of your company's most current identity profile information. If so, simply add this application as a resource and delegate the system as the authoritative source for user information.

Once you define a system as an authoritative source, you need only add a rule to detect changes within that resource. Any change propagates to all other accounts during the reconciliation process.

Understanding Sync In and Sync Out

Select Identity allows you the flexibility to determine whether you want changes to individual attribute fields updated by Select Identity or by the resource to which they belong or by both. Field attributes set to Sync In create updates to Select Identity. Attributes that are updated by Select Identity are set to Sync Out. Field attributes may be set to sync in and sync out, in which case a change made to the resource updates Select Identity and a change made to Select Identity updates the resource as well.

Figure 22 Sync In and Sync Out



Although all fields in an authoritative resource are set to sync out, you can override the setting so the field is sync in only. For example let's say you want your human resources system to be your authoritative resource and you want all identity management fields to update select identity and then propagate to other resources except location. You would prefer your facilities management system update that location, but the facilities management system has not been designated as authoritative. By removing the sync out setting in Select Identity for the location field of the human resource system resource, and setting the Facility System resource to Sync Out, you change the designated field attribute that updates Select Identity.

Field attributes can be both sync in and sync out if a change to the attribute in the resource would update Select Identity and a change to Select Identity would update the resource as well.

Managing Resources

Select Identity is installed with each of the resource connections your business requires. If you add new systems to your environment later, additional resource connectors can be acquired from HP OpenView Professional Services or developed using the Select Identity Connector Software Development Kit (SDK). Connectors can be deployed and managed through the Connectors section of the client. See Understanding Connectors on page 56 for more information.

This chapter provides details for all of the actions that you can perform within Resources. Access to each of these functional areas is determined by the administrative roles assigned to your account by the OVSI system administrator.

- When adding a user in Select Identity for UNIX, Tandem, and AS400 systems, avoid entering an entitlement (secondary groups) value that is the same value as the Default Group for the system resource. This may cause an entitlement to be inadvertently removed from the user if the user is modified and the Default Group value is changed for that user.
- In general, ensure that you can connect to a resource before trying to deploy it in Select Identity.

Once resources are added you must deploy a resource for each system on which users have accounts that relate to the Services you provide. The following procedures use an Lightweight Directory Access Protocol (LDAP) system as a resource example although there are many others that can be used as well.

The information entered for each of your system resources will vary according to the system itself. See the system connector *Installation Guide* for access information when creating a resource for a specific connector.

Complete these procedures to add a resource:

- Adding a Resource
- Viewing the Mapping File
- Mapping Resource Attributes
- Modifying Resources
- Copying Resources
- Delete a Resource

Adding and Managing System Resources

Select Identity comes installed with each of the resource connections that your business requires. If you add new systems to your environment related, Select Identity Professional Services an provide additional resource connectors. Connectors can also be developed wit the Select Identity Software Development Kit (SDK).

The following section covers:

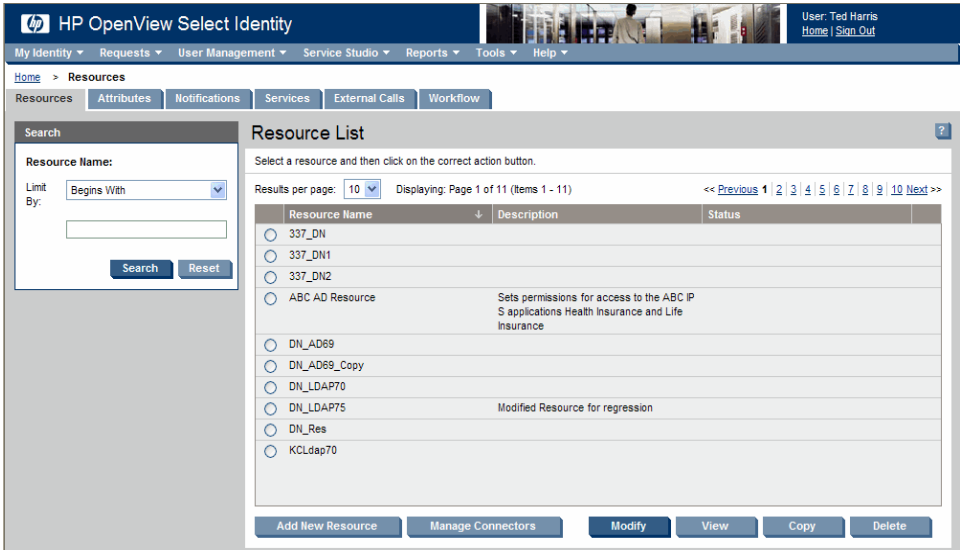
- Managing Resources
- Adding and Mapping New Attributes
- Creating and Modifying Notification Templates
- Understanding Service Context
- Understand Fixed and Optional Entitlements

Adding a Resource

Perform the following steps to add a resource:

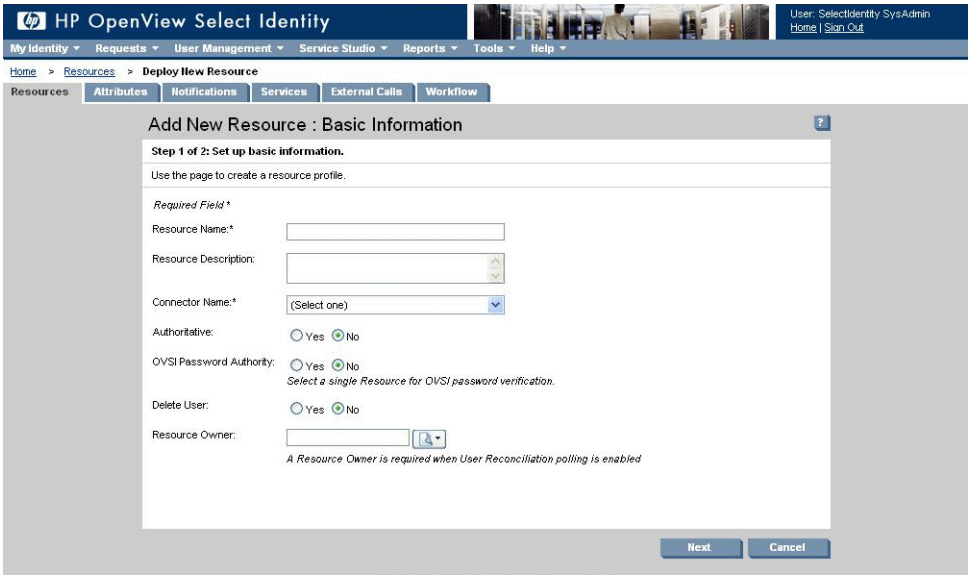
1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 23 Resource List page



2 Click **Add Resource**.
The **Add New Resource** page opens.

Figure 24 Add Resource page



You can compare resource information to a non-Authoritative Source, but you cannot add accounts from one. See Account Reconciliation on page 401 for information about Reconciliation.

3 Tab from field-to-field and enter the required information.

Field	Action
Resource Name	Enter the name of the resource.
Resource Description	Type a brief description of the resource.
Connector Name	Select the correct connector used to access the resource from Select Identity.

The connector must be included in the Managed Connectors list for you to select it here. If you do not see your connector, map the necessary connector before continuing. See Managing Connectors on page 59 for more details.

Authoritative	Select **Yes** if this is the resource you intend to be Authoritative. See Using Authoritative Resources on page 63 for more information. If you make this resource authoritative, the attributes mapped to this resource are also authoritative. When field attribute data is reconciled, the values for these attributes take precedence over other resource field attributes that do not sync out. See Adding and Mapping New Attributes on page 103 for more information about attributes.
OVSI Password Authority	Select **Yes** if the log in data should be synchronized across all resources so that the user only has to sign on once.
Delete User	Select **Yes** if you want a user to be deleted in this Resource when the user is deleted from an associated Service.
Resource Owner	Select the user ID of the contact in charge of this resource if a contact person has been assigned.

A resource owner must be designated if reconciliation polling has been enabled. Review the Reconciliation Policy page to determine whether or not reconciliation polling is enabled.

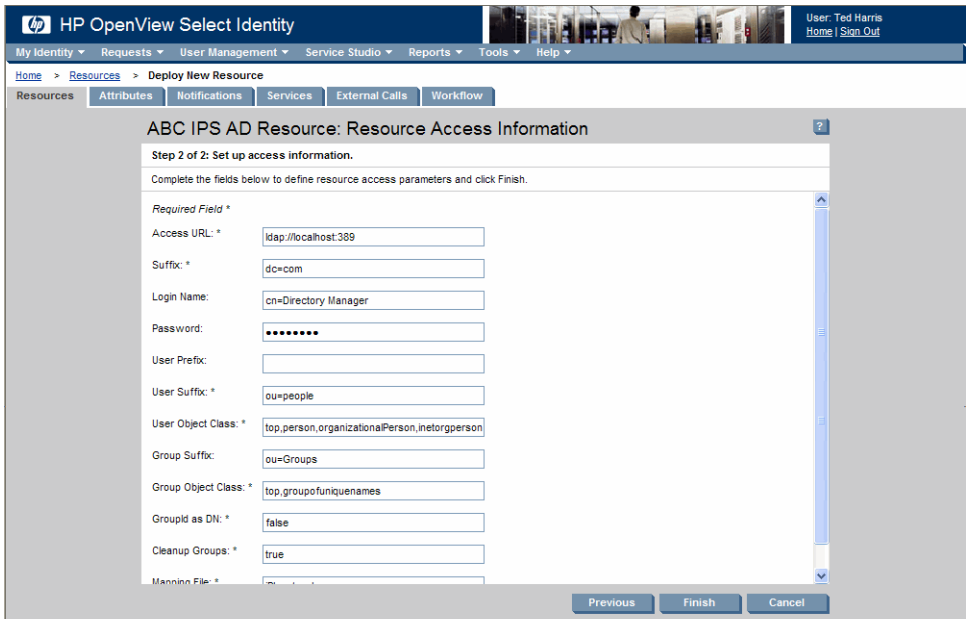
4 Click **Next** to proceed.
The **Resource Access Information** page opens. The fields displayed are based on the previous entries.

5 Enter the necessary connection credentials, which depend on how the database connector and agent are installed and configured:

- Using a JDBC data source, when an agent is not installed:
  In this configuration, the connector performs operations on the database directly through JDBC calls. You must specify the JDBC data source and mapping file when configuring the resource.
- Using a JDBC driver, when an agent is not installed:
  The connector uses the JDBC driver to communicate with the database. You must specify all parameters except the agent port and JDBC data source.

- Using a JDBC driver, with an agent installed:
  If the agent is installed and a JDBC driver is used to communicate with the database, you must specify all parameters except the JDBC data source.

Figure 25 Resource Access Information



6 Tab from field-to-field and enter the information required based on the fields displayed.

The fields in this example are defined as an example only and may change based on the connector selected.

Field	Action
Access URL	URL used when Select Identity needs to gain access to the resource.
Suffix	Connector naming convention. Do not change.
Login Name	Name used when Select Identity needs to login to a resource.

Field	Action
Password	Password used to gain access through Select Identity reconciliation to the resource to make changes.
User Suffix	Connector naming convention. Do not change.
User Object Class	Java based object class, which defaults from the resource selection.
Group Suffix	Connector naming convention. Do not change.
Group Object Class	Java based object class, which defaults from the resource selection.
Mapping File	File used to map field attributes between OVSI and the resource.

7 Determine whether you need to view the **Mapping File**.

If	Then
You need to review the Mapping file	Follow the Viewing the Mapping File procedure on page 70.
The mapping form is NOT authoritative	Continue

8 Click **Finish** to proceed.
The **[Resource Name]: User Reconciliation Policy** page opens.

9 Review the list of fields displayed and make any necessary changes.

10 Click **OK**.
Returns to the Resource List page.

Viewing the Mapping File

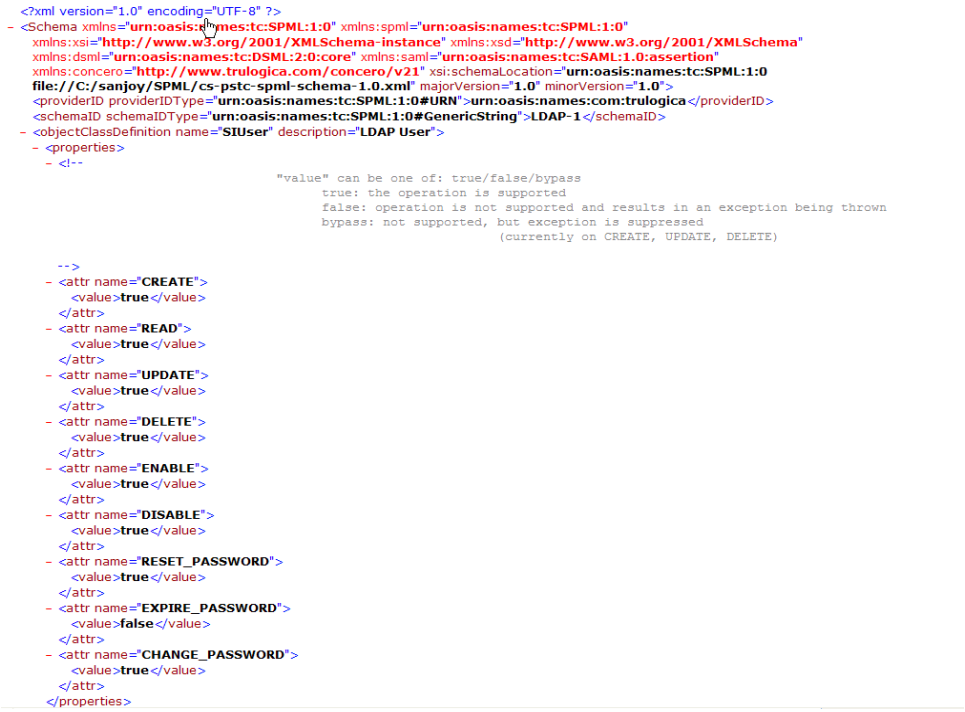
After the access information is entered a new XML file is created in the Select Identity home directory if the connector supports mapping. Read more about mapping connectors in the Deploying a Connector section on page page 59. Mapping XML files are stored in the `com/trulogica/truaccess/`

`connector/schema/spml` subdirectory. (This default location can be configured by setting the `com.hp.ovsi.connector.schema.dir` parameter in the `TruAccess.properties` file.)

If the specified mapping file exists, the Attribute Mapping Utility appears, connects to the database, and loads the existing settings in the mapping file You may want to view the **Mapping File** before you map the Resource attributes. Follow the procedure below to view the file.

1 Locate the **Mapping File** field on the page and click the **View** link beside the field.
The XML or SPML file opens in a new browser window.

Figure 26 Resource Mapping File



2 Review the information displayed.

3 Close the browser window.
Returns to the original page.

Mapping Resource Attributes

After creating a new resource you must map the resource field attributes to the corresponding Select Identity field attributes so that the correct data is updated during the reconciliation process. Learn more about Account Reconciliation on page 401.

Use the Adding a New Attribute procedure on page 104 to map a new Select Identity attribute to multiple resources. The following procedure works best when you are mapping a list of attributes for a new resource to the matching fields on Select Identity.

Follow the steps below to map each resource attribute to a corresponding Select Identity attribute:

1 Review the list of Resource Attributes.

2 Select the Select Identity attribute you want to map to from the **Attribute** drop down menu.

3 Determine how you want the field to update or be updated.

If	Then
All attributes in this resource to be authoritative	Select **Authoritative**.
This attribute to update Select Identity.	Select **Sync In**. If your resource is Authoritative, but you have removed the check from Sync In field, then that field will NOT update Select Identity.
This attribute to be updated by Select Identity	Select **Sync Out**. Authoritative resources may update Select Identity. Attributes marked Sync In may also be updated by Select Identity. Updates will be determined by the field with the latest revision date.

4 Click **Apply**.
Saves your work.

5 Repeat the process until each of the Resource Attributes has been properly mapped.

6 Click **OK**.
Returns to the **Resource List** page.

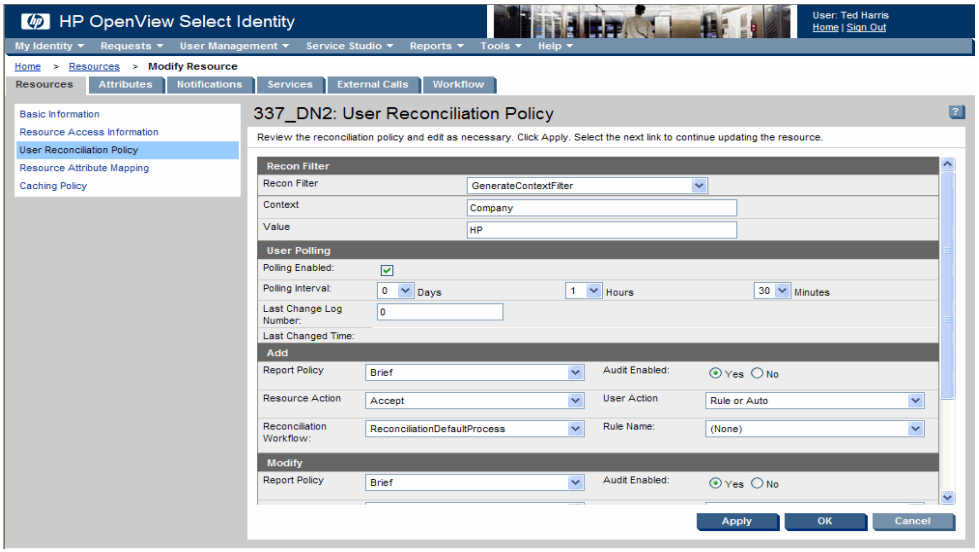
Setting Resource Reconciliation Policies

Select Identity offers a number of reconciliation policies. Use this page to determine the policies for the resource you are creating.

Follow the steps below to set a reconciliation policy:

1 Click the **User Reconciliation Policy** link in the left panel of the page.
The **Resource name: User Reconciliation Policy** page opens.

Figure 27 Resource Name: User Reconciliation Policy



2 Determine whether a reconciliation filter is necessary.

Reconciliation filters are designed to sort through the attributes looking for changes that meet the filter criteria so that only those changes are returned to Select Identity. Filters reduce the impact of data traffic on Select Identity and improve performance. They can also be used to “create” changed values.

3 Determine whether Select Identity should periodically poll this resource to determine if changes have been made to fields that update Select Identity in the **User Polling** section.

If	Then
You do NOT want Select Identity to poll this resource	Continue with the step.
You do NOT want Select Identity to poll this resource	Select the filter from the Recon Filter drop down list and continue.

4 Tab from field to field enter the required information necessary to define the polling parameters.

Field	Action
Polling Enabled	Select the field to indicate that Select Identity should poll this resource.
Polling Interval	Determine how often Select Identity will poll the resource by entering the appropriate values in the Polling Internal drop down menus: • **Days**: Number of days between each polling event • **Hours**: Number of hours between each polling event • **Minutes**: Number of minutes between each polling event.
Last Change Log Number	A one (1) indicates the change log is being updated. A zero (0) indicates the change log is available for edit.
Last Changed Time	Log that time stamps changes to the change log.

5 Review the list of fields displayed and make any changes necessary for the **Add** function.

Field	Action
Report Policy	Determine how you want addition transactions reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are added.
Resource Action	Determine what you want the resource to do when Select Identity receives information from the resource and select a new policy from the drop-down menu if necessary
User Action	Determine what you want the user to do in order to approve the addition of the record and select a new policy from the drop-down menu if necessary.
Reconciliation Workflow	Select a new Workflow template if necessary to support adding records.

6 Review the list of fields displayed and make any changes necessary for the **Modify** function.

Field	Action
Report Policy	Determine how you want modified transactions reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are modified.
Resource Action	Determines the overall reconciliation process on the resource/event: ignore, revert, or accept.

Field	Action
User Action	This is only used when the Resource Action is set to "Accept." Determines what to do in the event of a changed user record.
Reconciliation Workflow	Select a new Workflow template if necessary to support modifying records.
Serial Process	Determines whether all records for the same user should be processed sequentially. This should be set uniformly for add, modify, or delete. Serial processing is more accurate but slower.

7 Review the list of fields displayed and make any changes necessary for the **Delete** function.

Field	Action
Report Policy	Determine how you want deleted records reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are deleted.
Resource Action	Determine what you want the resource to do when OVSI attempts to delete a record and select a new policy from the drop-down menu if necessary
User Action	Determine what you want the user to do in order to approve the deletion of the record and select a new policy from the drop-down menu if necessary.
Reconciliation Workflow	Select a new Workflow template if necessary to support deleting records.

8 Click **Next**
Saves your work.

Defining Resource Entitlement Caching Policies

Use entitlement caching to reduce the impact of retrieving provisions called entitlements in Select Identity from resources on the overall performance of the system. Select Identity caches entitlement changes using the following methods:

- The Select Identity entitlement cache is initialized when that resource's entitlements are retrieved for the first time.
- A batch process periodically retrieves entitlements from resources and updates the Select Identity database where necessary

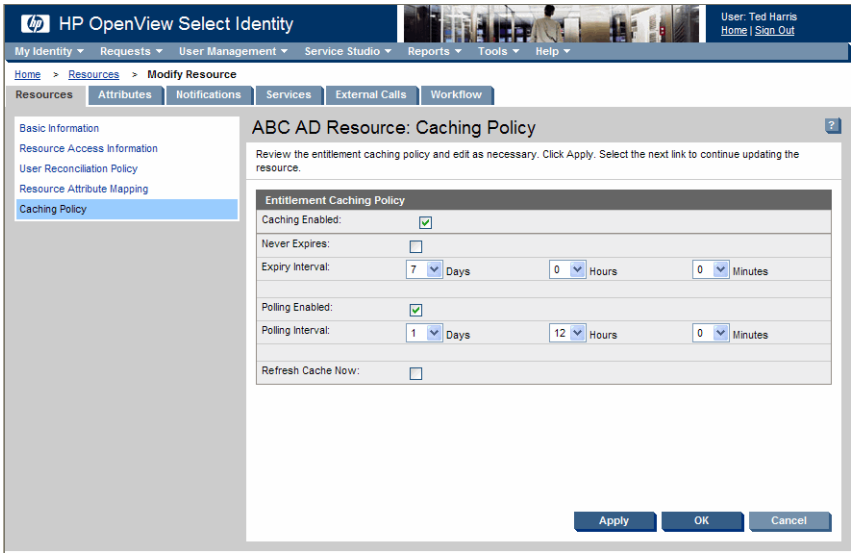
Select Identity periodically synchronizes the Select Identity database with Agent tables to make sure all tables are in sync. An agent must have the ability to detect entitlement changes on a resource before it can be used to facilitate caching. If you choose to set up no synchronization at all, then the entitlements are always be retrieved directly from the resource from its connector. This option should be used only under the following circumstances:

- No delay at all can be tolerated in the update and synchronization has been set
- The change log is not available for the resource
- The time required to retrieve the change log is comparable with the time required to retrieve the entitlement.

Follow the steps below to determine the policies used to manage caching for this resources:

1 Click **Caching Policy** in the left panel.
The **Resource Name: Caching Policy** page opens.

Figure 28 Resource Name: Caching Policy



2 Determine whether to enable resource caching.

If	Then
Resource caching is not necessary	Click **OK**. Returns to the **Resource List**. All entitlements are retrieved and updated through the connector during the reconciliation process.
Resource Caching is required	Continue.

3 Tab from field to field enter the required information necessary to define the polling parameters.

When polling is enabled, a Select Identity batch runs periodically, according to the polling interval for getting entitlement updates on the resource. This synchronizes Select Identity entitlements.

.

Field	Action
Polling Enabled	Select the field to indicate that Select Identity should poll this resource for changes to entitlements.
Polling Interval	Determine how often Select Identity polls the resource by entering the appropriate values in the Polling Internal drop down menus: • **Days**: Number of days between each polling event • **Hours**: Number of hours between each polling event • **Minutes**: Number of minutes between each polling event

4 Select **Refresh Cache Now** if you need to manually start a refresh.
Reviews entitlements at the resource level and updates the entitlement cache.

5 Click **Apply**.
Saves your work.

6 Click **OK**.
Returns to the **Resource List** page.

Modifying Resources

Modify the system resources on which your products and Services rely when necessary. You may need to modify a resource for the following reasons:

- the connector mapping has changed
- the resource application was moved to another machine
- the resource admin password has changed

This section covers the following:

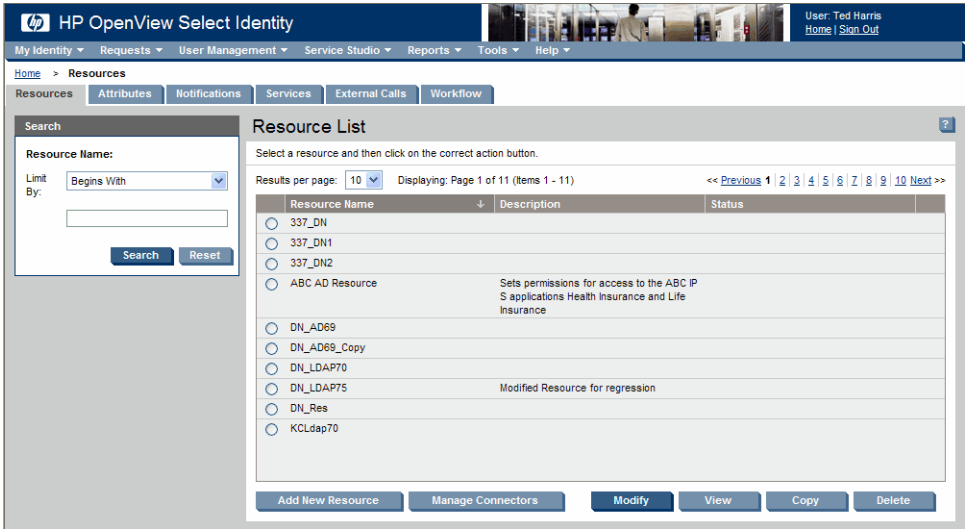
- Modifying Resource Information
- Changing Resource Access Information
- Modifying Resource Attribute Mapping

Modifying Resource Information

Follow the steps below to modify a resource:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 29 Resource List Page



2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens.

4 Review the entries displayed and change the required information if necessary.

Field	Action
Resource Description	Modify the description of the resource if necessary.
Authoritative	Select the **Yes** radio button if changes to this resource should update Select Identity.

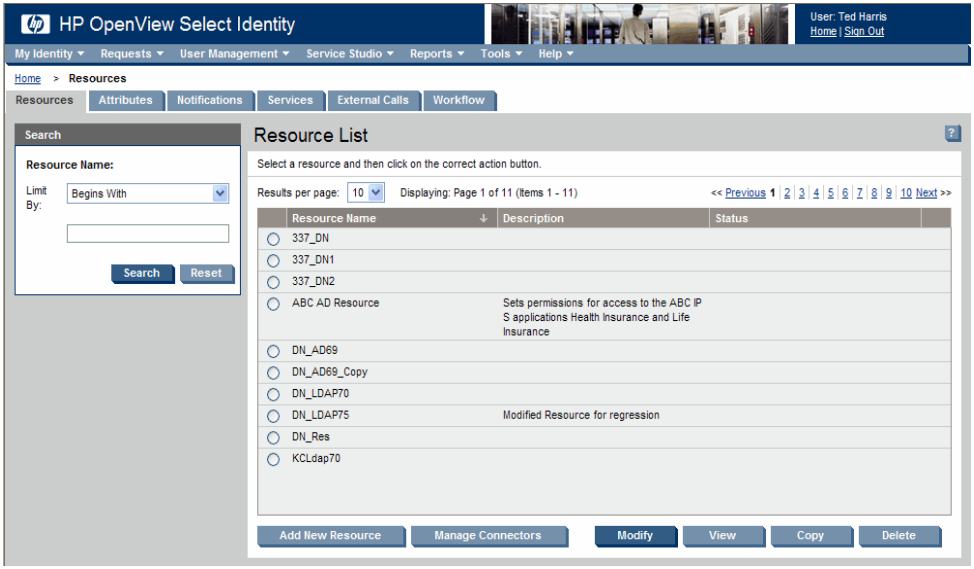
Field	Action
OVSI Password Authority	Indicates whether users assigned to this resource may access all resources using a single password.
Delete User	Select the **Yes** radio button if you want a user to be deleted in this Resource when the user is deleted from an associated Service.
Resource Owner	Select the user ID of the contact in charge of this resource if a contact person has been assigned.

5 Click **Apply**.

Changing Resource Access Information

1 Select **Service Studio** → **Resources** from the menu bar options. The **Resource List** page opens.

Figure 30 Resource List page

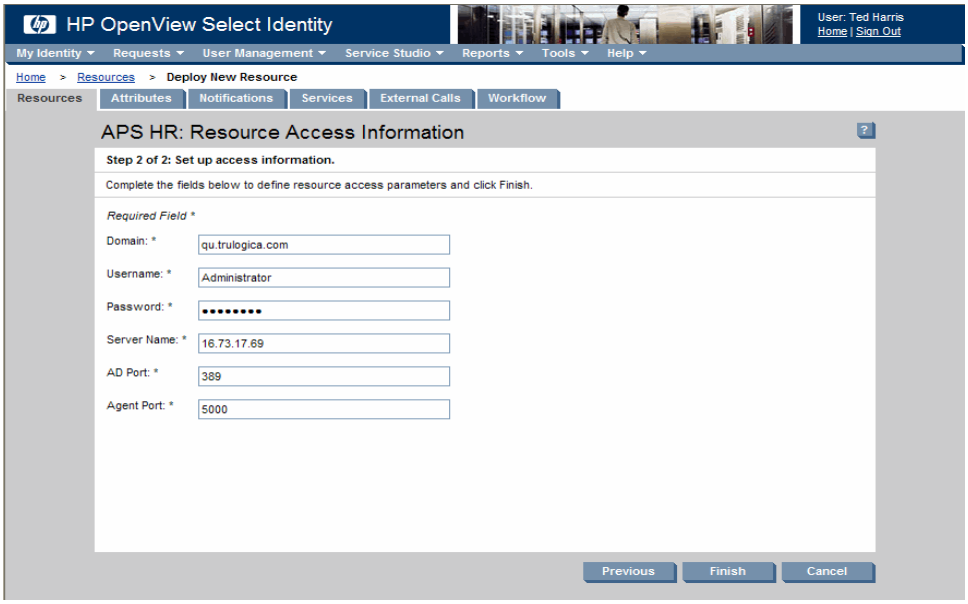


2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens.

4 Click the **Resource Access Information** link in the left panel of the page.
The page shows the required fields.

Figure 31 Modify Resource Access Information



5 Review the list of fields displayed and make any changes necessary.

Field	Action
Access URL	URL used when SI needs to gain access to the resource.
Suffix	Connector naming convention. Do not change.
Login Name	User ID used by OVSI to gain access to the connector during reconciliation.
Password	Unique password used by OVSI to gain access to the connector during reconciliation.
User Prefix	Connector naming convention. Do not change.
User Suffix	Connector naming convention. Do not change.

Field	Action
User Object Class	Java based object class, which defaults from the resource selection.
Group Suffix	Connector naming convention. Do not change.
Group Object Class	Set by the connector. Do not change.
Grouped as DN	Set by the connector. Do not change.
Cleanup Groups	Set by the connector. Do not change.
Mapping File	File used to map field attributes between OVSI and the resource.

6 Click **Apply**.
Saves your work.

Modifying the Resource Reconciliation Policy

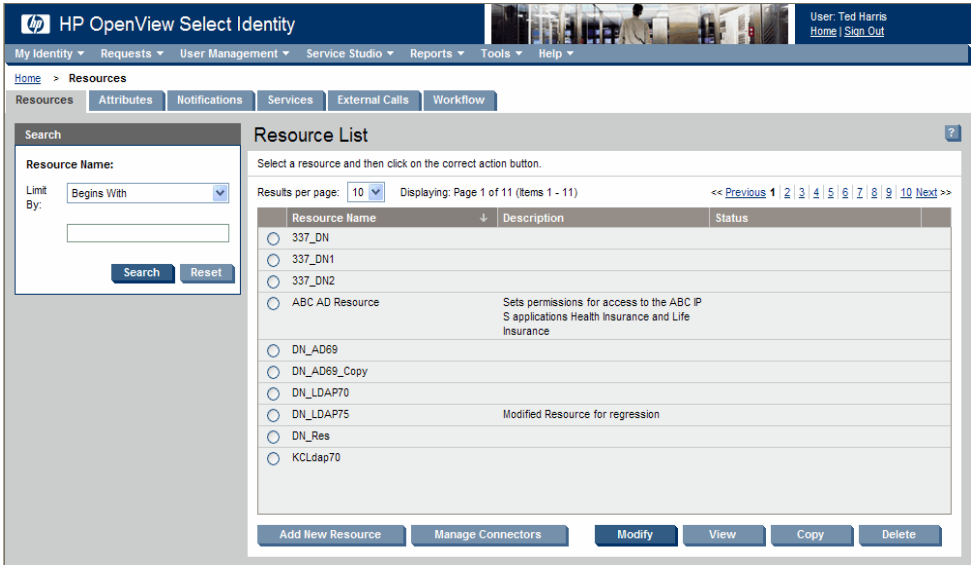
The Reconciliation process is used to export attribute value changes to Select Identity supported resources through the Sync Out process while importing changes to Select Identity system in the Since In process. Reconciliation Rules define the operations based on user properties. Reconciliation supports the following types of operations based on the policies you create:

- Add Service
- Delete Service
- Enable Service
- Disable Service
- Enable User
- Disable User
- Terminate User

Follow the steps below to modify a reconciliation policy:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 32 Resource List Page

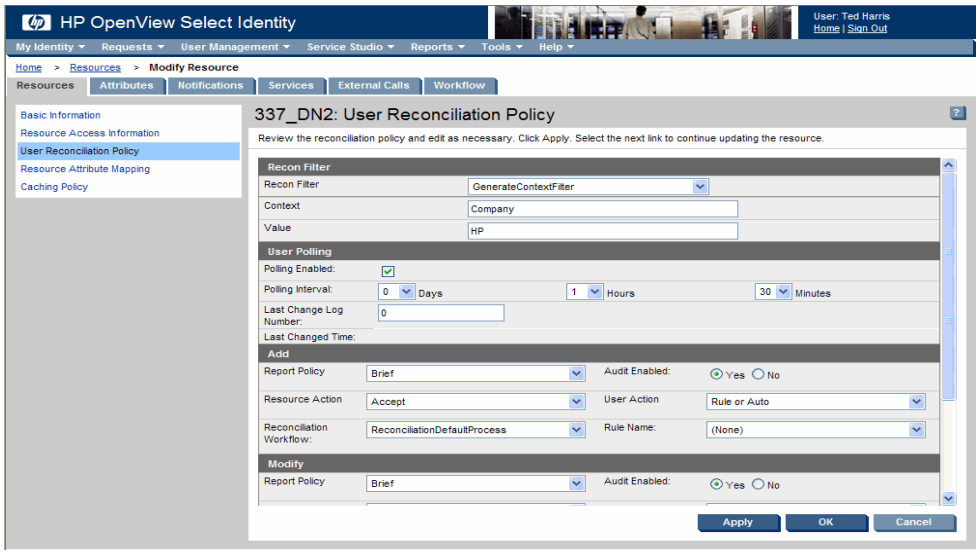


2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens.

4 Click the **User Reconciliation Policy** link in the left panel of the page.
The [**Resource Name]: User Reconciliation Policy** page opens.

Figure 33 Resource Name: User Reconciliation Policy



5 Determine whether a reconciliation filter is necessary.

Reconciliation filters are designed to sort through the attributes looking for changes meeting the filter criteria so that only those changes are returned to Select Identity. Filters reduce the impact of data traffic on Select Identity and improve performance.

6 Determine whether Select Identity should periodically poll this resource to determine if changes have been made to fields that update Select Identity in the **User Polling** section.

If	Then
You do NOT want Select Identity to poll this resource	Continue with the step.
You do NOT want Select Identity to poll this resource	Select the filter from the Recon Filter drop down list and continue.

7 Tab from field to field enter the required information necessary to define the polling parameters.

Field	Action
Polling Enabled	Select the field to indicate that Select Identity should poll this resource.
Polling Interval	Determine how often Select Identity will poll the resource by entering the appropriate values in the Polling Internal drop down menus: • **Days**: Number of days between each polling event • **Hours**: Number of hours between each polling event • **Minutes**: Number of minutes between each polling event.
Last Change Log	A one (1) indicates the change log is being updated. A zero (0) indicates the change log is available for edit.
Last Changed Time	Log that time stamps changes to the change log.

8 Review the list of fields displayed and make any changes necessary for the **Add** function.

Field	Action
Report Policy	Determine how you want addition transactions reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are added.

Field	Action
Resource Action	Determine what you want the resource to do when Select Identity attempts to add a record and select a new policy from the drop-down menu if necessary
User Action	Determine what you want the user to do in order to approve the addition of the record and select a new policy from the drop-down menu if necessary.
Reconciliation Workflow	Select a new Workflow template if necessary to support adding records.

9 Review the list of fields displayed and make any changes necessary for the **Modify** function.

Field	Action
Report Policy	Determine how you want modified transactions reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are modified.
Resource Action	Determine what you want the resource to do when OVSI attempts to modify a record and select a new policy from the drop-down menu if necessary
User Action	Determine what you want the User to do in order to approve the modification of the record and select a new policy from the drop-down menu if necessary.
Reconciliation Workflow	Select a new Workflow template if necessary to support modifying records.

10 Review the list of fields displayed and make any changes necessary for the **Delete** function.

Field	Action
Report Policy	Determine how you want deleted records reported and change the reporting policy if necessary.
Audit Enabled	Select **Yes** if you want the reconciliation process to be audited and logged when records are deleted.
Resource Action	Determine what you want the resource to do when OVSI attempts to delete a record and select a new policy from the drop-down menu if necessary
User Action	Determine what you want the user to do in order to approve the deletion of the record and select a new policy from the drop-down menu if necessary.
Reconciliation Workflow	Select a new Workflow template if necessary to support deleting records.

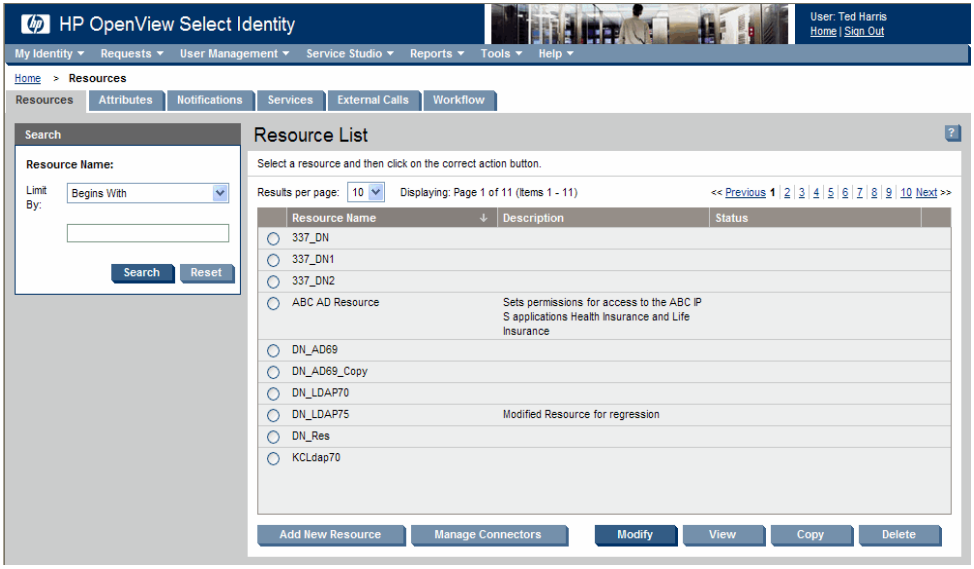
11 Click **Apply**.
Saves you work.

12 Click **OK**.
Returns you to the **Resource List** page.

Modifying Resource Attribute Mapping

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 34 Resource List

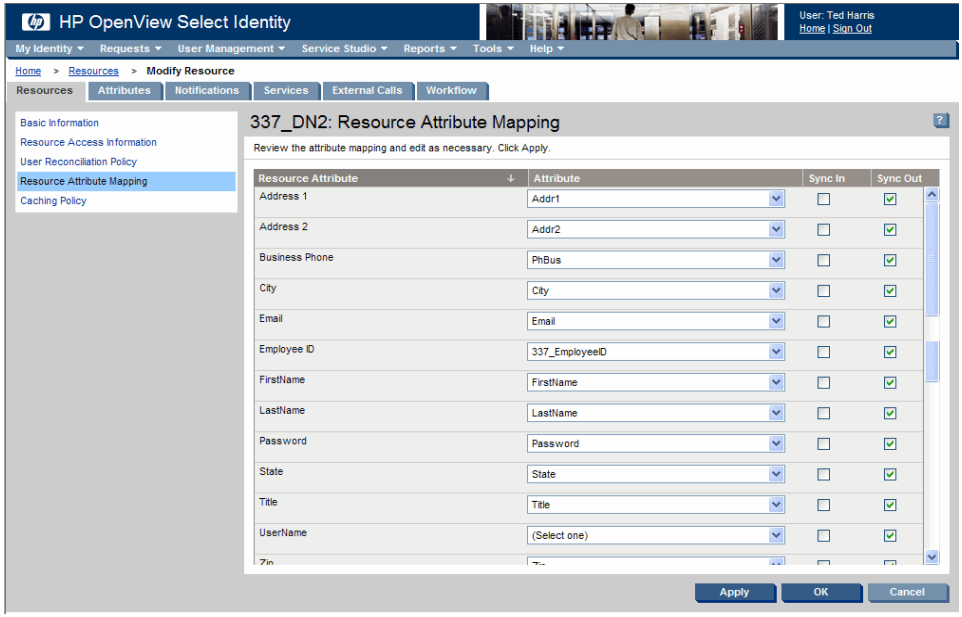


2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens

4 Click the **Resource Attribute Mapping** link in the left panel of the page.
The [**Resource Name]: Resource Attribute Mapping** page opens.

Figure 35 Resource Name: Resource Attribute Mapping



5 Review each of the attribute fields displayed and change the attribute mapping as necessary.

> Attribute fields depend upon the fields defined when the resource was set up.

6 Click **Apply**.
Saves your work.

7 Click **OK**.
Returns to the **Resource List** page.

If the resource fails to deploy due to the following error, "Unable to deploy resource at this time," check the following:

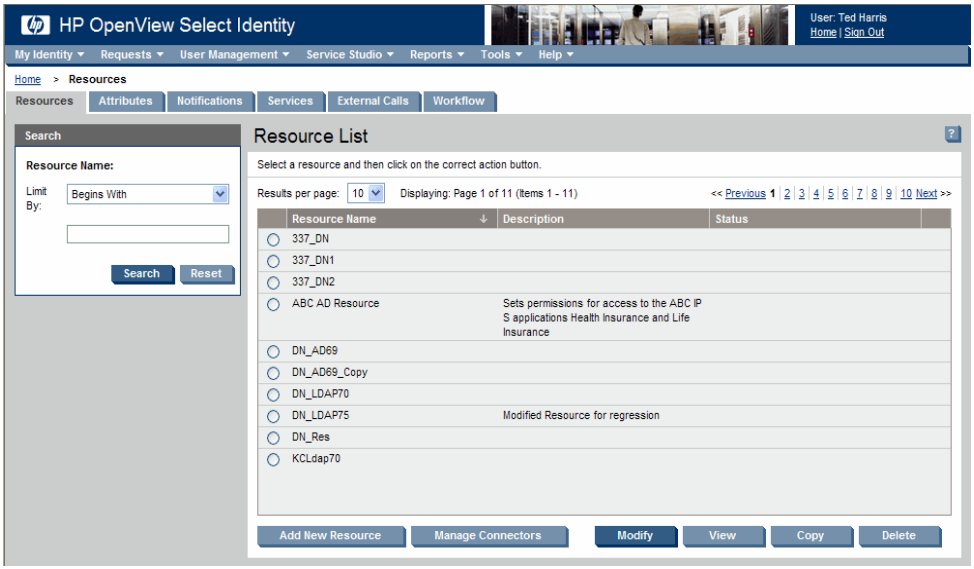
- the correct version of the Java Cryptography Extension security files (`local_policy.jar, us_export_policy.jar`) have been installed on the WebLogic server. See the *HP OpenView Select Identity Installation and Configuration Guide* for details.
- incorrect or incomplete version of WebLogic is installed.

Changing the Resource Entitlement Caching Policy

Follow the steps below to review and change the Resource Entitlement Caching Policy:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 36 Resource List

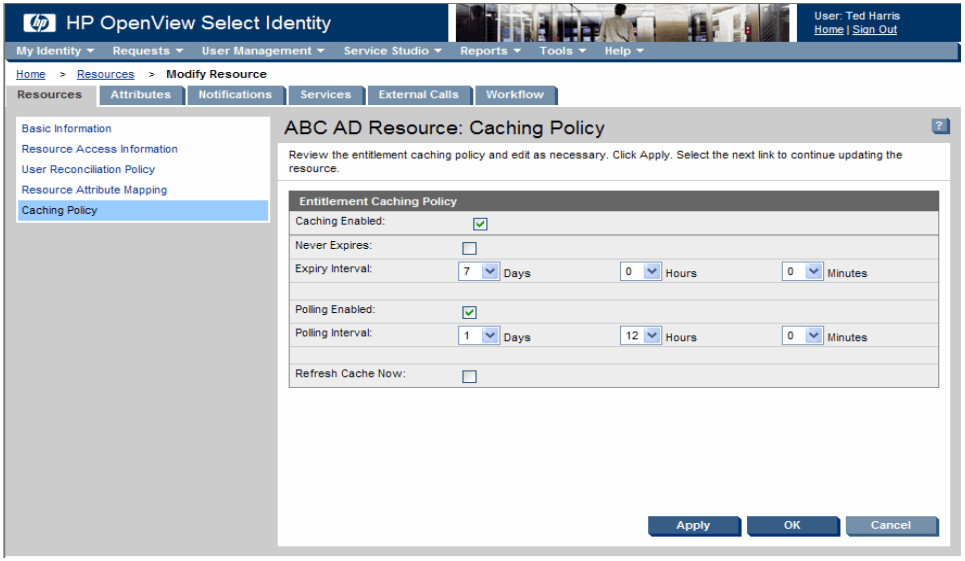


2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens.

4 Click **Caching Policy** in the left panel.
The **[Resource Name]: Caching Policy** page opens.

Figure 37 Resource Name: Caching Policy



5 Select **Caching Enabled.**
Shows the caching fields.

6 Select **Polling Enabled** and review the Polling Interval fields, then make any changes required.

7 Select **Refresh Cache Now** if you need to manually start a refresh.
Reviews entitlements at the resource level bringing back all attribute changes.

8 Click **Apply**.
Saves your work.

9 Click **OK**.
Returns to the **Resource List** page.

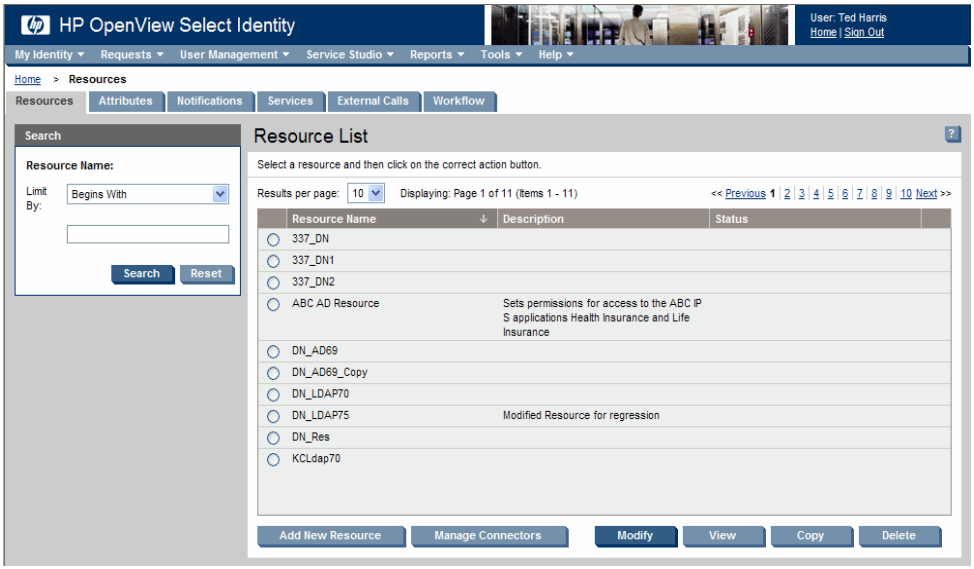
Capturing All Entitlement Changes without Caching

Occasionally you may want to retrieve entitlement changes in between scheduled synchronization events. Start a **Resource Entitlement Refresh** when you need to review entitlements at the resource level and bring back all attribute changes.

Use the procedure below to refresh the cache and retrieve changes to the resource in real time:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 38 Resource List Page

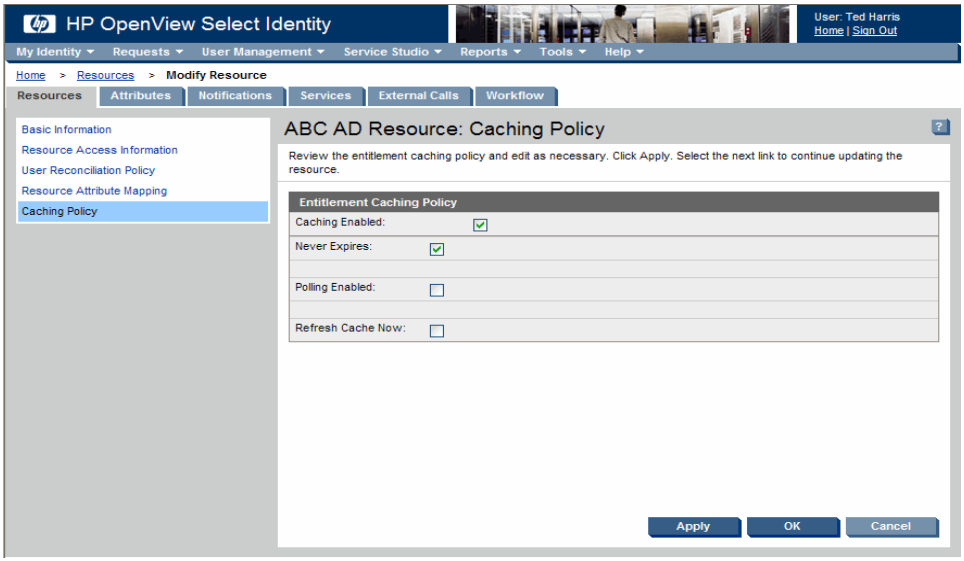


2 Select the resource you want to modify.

3 Click the **Modify** button.
The **[Resource Name]: Basic Information** page opens.

4 Click **Caching Policy** in the left panel.
The **[Resource Name]: Caching Policy** page opens.

Figure 39 Resource Name: Caching Policy



5 Reviews entitlements at the resource level bringing back all attribute changes.

6 Click **Apply**.
Saves your work.

7 Click **OK**.
Returns to the **Resource List** page.

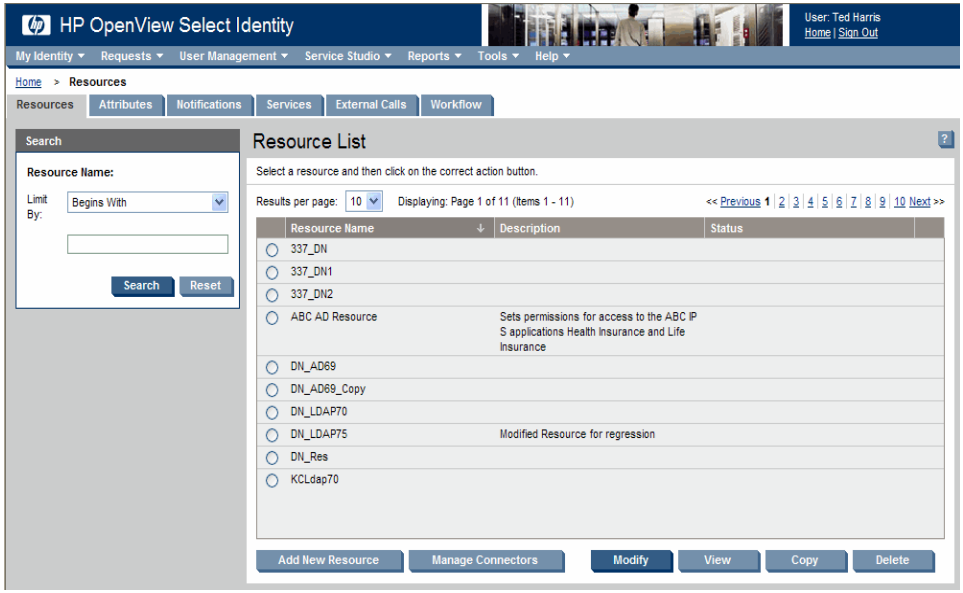
Copying Resources

If you have multiple resources to add that are very similar, save time by copying an existing resource and changing those fields that should be different. Note that all of the connection and configuration information is copied as well.

Complete the following steps to copy a system resource:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 40 Resource List



2 Click the **Copy** button.
The **Copy Resource: Resource Name** page opens.

3 Review the entries displayed and change the information available for update if necessary.

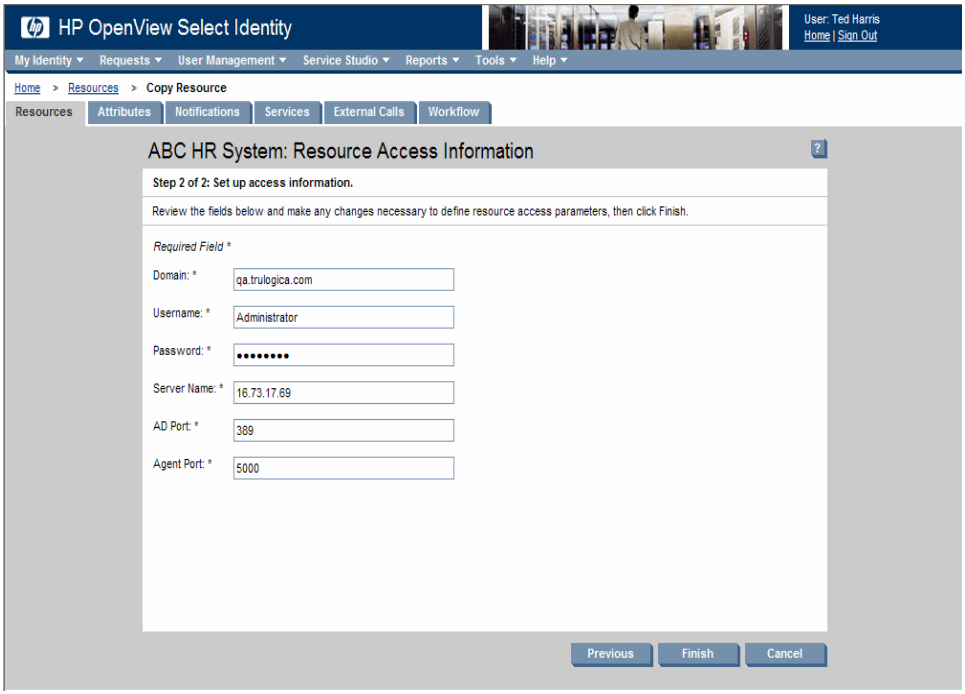
Field	Action
Resource Name	Type the complete name of the new resource.
Resource Description	Enter a brief description of the resource.
Authoritative	Select the **Yes** radio button if changes to this resource should update OVSI.

Field	Action
OVSI Password Authority	Indicates users can manage their accounts with a single signon password.
Delete User	Select the **Yes** radio button if you want a user to be deleted in this Resource when the user is deleted from an associated Service.
Resource Owner	Select the name of the Resource Owner if a contact person has been assigned to answer questions about this resource, such as how long the resource will be down.

A resource owner must be designated if reconciliation polling has been enabled. Review the Reconciliation Policy page to determine whether or not reconciliation polling is enabled.

4 Click the **Next** button.
The **Resource Name: Resource Access Information** page opens.

Figure 41 Resource Name: Resource Access Information



5 Review the list of parameters displayed and make any changes necessary.

> Resource access parameters are dependent upon the type of resource and the connector selected.

6 Click the **Finish** button.
Shows a confirmation dialog box.

7 Click **OK**.
The **Copy Resource; Attribute Mapping** page opens.

8 Change the attribute mapping as necessary.

9 Click **Apply**.
Saves your work.

10 Click **OK**.
Returns to the **Resource List** page.

Delete a Resource

Delete a system resource from Select Identity if your Services no longer requires access to it. Resources may still have users assigned. Once the resource is deleted you must make updates to any of the affected users from another account.

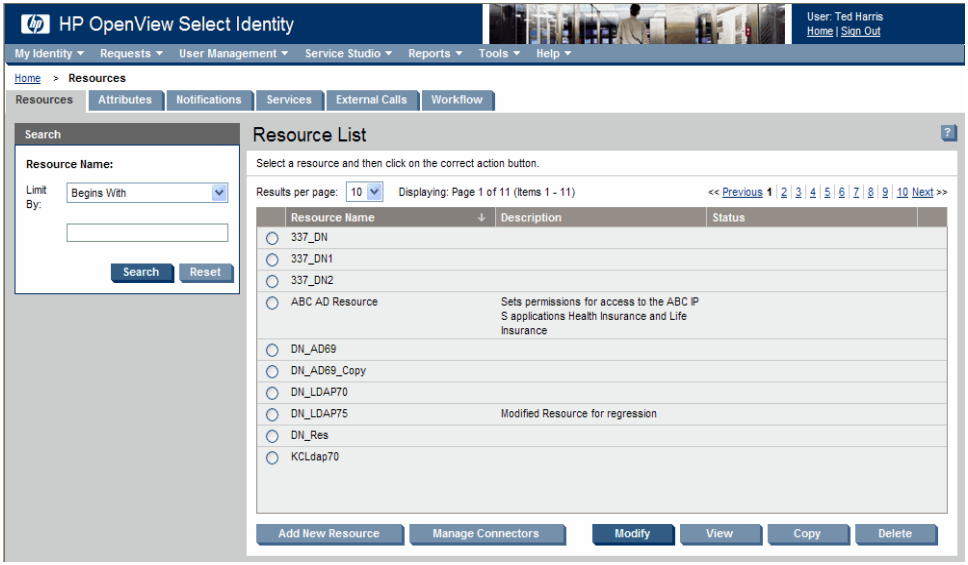
If a resource is still associated with a Service, it cannot be deleted.

Deleting a Resource

Perform the following steps to delete a resource:

1 Select **Service Studio** → **Resources** from the menu bar options.
The **Resource List** page opens.

Figure 42 Resource List



2 Select the resource you wish to delete.

3 Click the **Delete** button.
Shows the confirmation dialog box.

4 Click **OK**.
Deletes the resource.

Managing Attributes

Select Identity enables you to define the way in which user identities are managed and stored for multiple applications called resources. Each user profile can contain any number of field attributes, such as username, first name, last name, and email address. The resources that you add contain their own resource field attributes based on the operating system or application group's identity management information.

Each resource has a specified connector which operates as the interface between OVSI and the resource being provisioned. A mapping file is associated with each connector, which contains resource-specific attributes. This file maps the connector to the resource, and defines where and how identity information is stored on that resource. During the resource deployment procedure, you can view the file that the connector uses to map resource attributes.

The Select Identity Attribute pages allow you to map Select Identity fields to the fields defined in the Connector mapping file. The field attribute mapping process enables access to Services which control the provisioning of Resource accounts. Select Identity supports both large and small attribute deployment.

For example, let's say you define a Service called Finance. Users assigned to the Finance service have access to Oracle Financials and Hyperion Reports. Each applications is defined as a separate resource on Select Identity. Within each application, each of these resources has its own system administration function that manages the identity of users on that application alone.

On Oracle Financials, the user's first name is defined in a field called First. Hyperion Reports defines the field as Name First while you created an attribute in Select Identity that defines the field as FirstName. Select Identity allows you to map the FirstName field to each resource so that when you change the field in Select Identity, the reconciliation process updates First on Oracle Financials and First Name on Hyperion through the corresponding Connector mapping file.

The following is a sample of a mapping file

```
- <memberAttributes>
- <!--
 For iPlanet
```

```
-->

<attributeDefinitionReference name="UserName" required="true"
concero:tafield="[UserName]" concero:resfield="uid"
concero:isKey="true" concero:init="true" />

<attributeDefinitionReference name="Password" required="false"
concero:tafield="[Password]" concero:resfield="userpassword"
concero:init="true" />
```

Create attributes specific to Select Identity through the Attributes pages. Not all of these attributes will map to outside resources. These attributes may be specific to Select Identity or to your business. If attributes are not mapped to a resource, they are valid in Select Identity only and cannot be used to associate an account with a resource.

When you add a new user through any Service, you must define the following attributes (see Understanding Service Roles on page 143 for details):

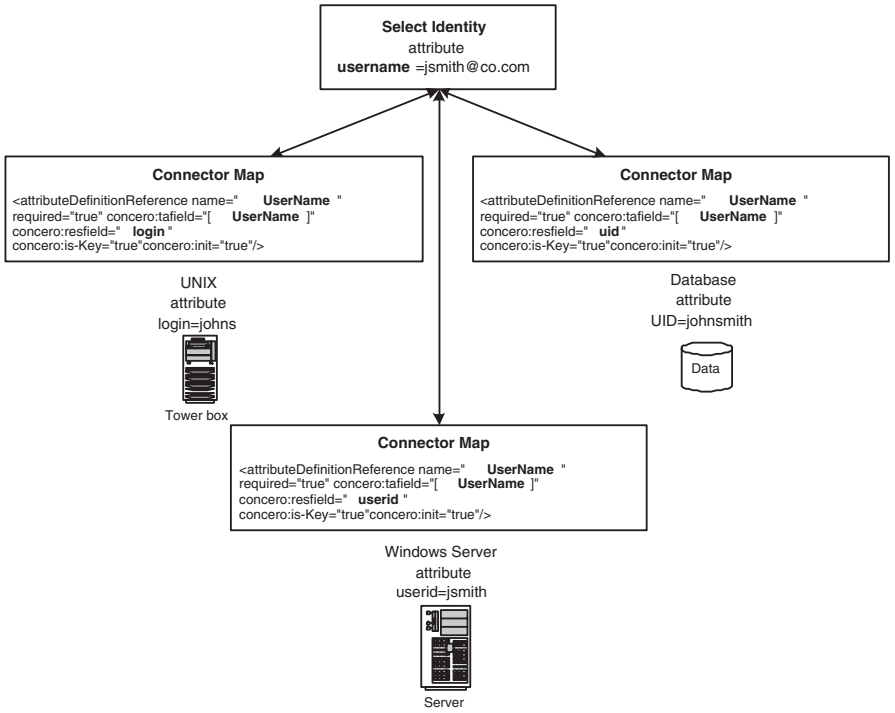
- UserName
- FirstName
- LastName
- Email
- Password

For all other operations, the UserName is required.

The Password attribute is required if Select Identity is managing the password. If however, a third-party single sign-on solution is being used to manage user passwords, then the password is not required.

The following diagram illustrates how the attribute “username” is mapped to multiple resources through each connector mapping file.

Figure 43 Attribute Mapping Example



If you offer a Service that relies on these three resources, users who register for the Service can be mapped accordingly. This enables you to create a standard set of profile attributes for your users that are relevant for your business and then map them to any of your system resource applications, regardless of how the attribute is defined on the resource.

Each connector defines its own attributes. OVSI attributes are mapped to connector attributes. Connectors can implement business logic to map connector attributes to resource attributes. Attributes that are automatically mapped between OVSI and resources are key (attributes that are required by the resource) and entitlement attributes.

When possible, it is recommended that you use constraints when configuring the Service attribute values. By using constraints, you may improve performance within OVSI. See Setting Service Attribute Values and Properties on page 158 for details.

When defining attributes, assign external calls for the following purposes:

- Value, which defines the acceptable values for an attribute.
- Generation, which generates a value for an attribute.
- Constraint, which constrains the attribute value to a particular format or requirement. You can specify values or choose a program that provides dynamic values.
- Validation, which calls an external program to validate the value of the attribute.

These functions are deployed through External Calls and are then made available when creating an attribute. For more information about creating external calls for attributes, see the *HP OpenView Select Identity External Call Guide*.

Using Attributes to Facilitate User Searches

User accounts can consist of many attributes. Typically, users are searched based on certain key attributes (email, SSN, employee ID). Certain user profile attributes can be added to the TruAccess.properties file and used to expedite search functions. If these attributes are set, the `TAUser` database table must be extended by adding extra columns that reflect these values. The extra attributes must then be mapped to those columns.

To specify searchable attributes you must do the following:

1. Identify the key attributes, such as SSN, EmployeeId, or email. You must make sure these are defined within OVSI and within the mapping file used for each system resource in which data is stored.
2. Add corresponding columns to the `TAUser` table in the database.
3. Add entries in the `TruAccess.properties` file.

See the *HP OpenView Select Identity Installation Guide* for information about editing the database tables and `TruAccess.properties` file.

Adding and Mapping New Attributes

Add any number of attributes to manage identity information. The attribute will then be mapped to resource attributes during account addition and updates as a part of the reconciliation process.

If you are adding a new resource with many attributes go to Mapping Resource Attributes on page 72 to map all of the resource attributes to the matching OVSI attribute fields at one time. The procedure that follows works best when you create a new attribute in OVSI that you want to map to multiple resources that already exist.

Complete the following tasks to create a new attribute:

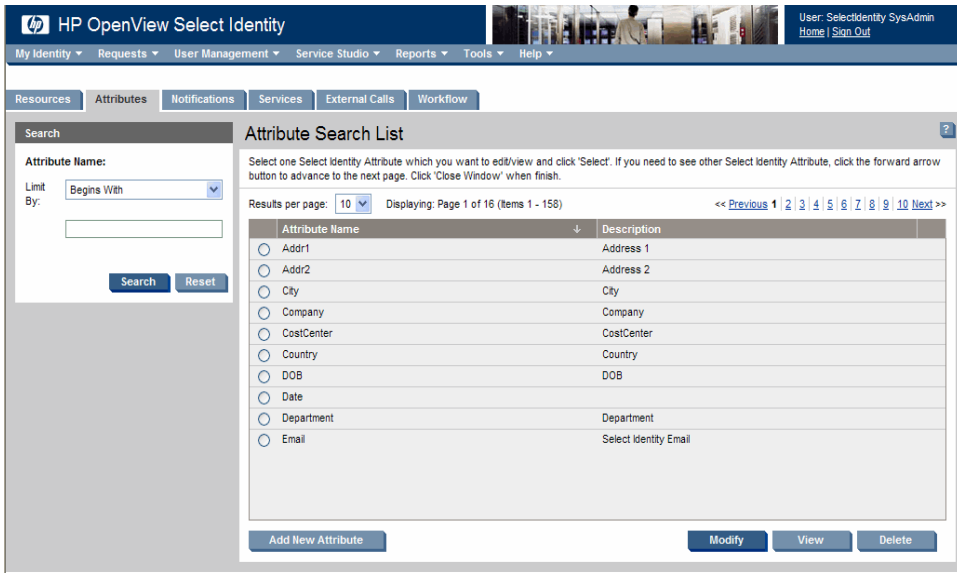
- Viewing the Attribute List
- Adding a New Attribute
- Selecting Resources to Map to the New Attribute
- Adding Constraints and External Calls to the New OVSI Attribute
- Viewing Existing Attributes
- Modifying Attributes
- Modifying Resource Attribute Mappings
- Modifying Attribute Constraints / External Calls
- Deleting an Attribute

Viewing the Attribute List

Follow the steps below to add an attribute:

1 Select **Service Studio** → **Attributes** from the menu bar options.
The **Attribute List** page opens.

Figure 44 Attribute List



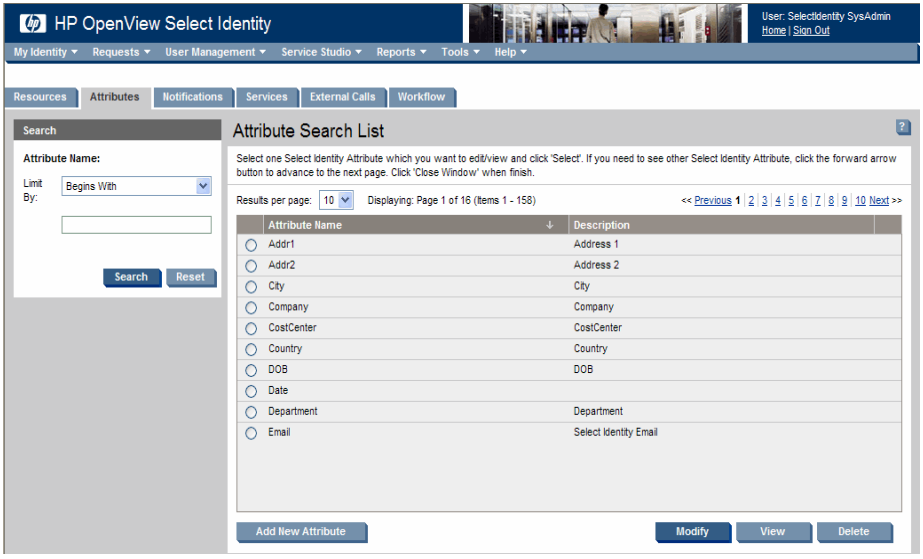
2 Review the list of attributes displayed and select the attribute you want to view.

Adding a New Attribute

Perform the following steps to add an attribute:

1 Select **Service Studio** → **Attributes** from the menu bar options. The **Attribute List** page opens.

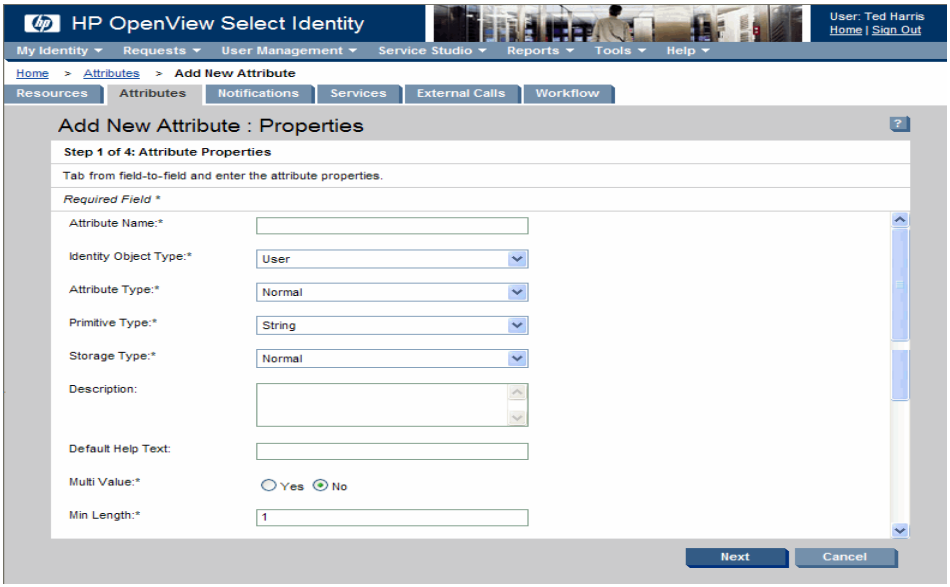
Figure 45 Attribute List



2 Review the list of attributes displayed to verify that the attribute you want to create does not already exist.

3 Click the **Add New Attribute** button.
The **Add New Attribute: Properties** page opens.

Figure 46 Add New Attribute: Properties



4 Tab from field-to-field and enter the required information..

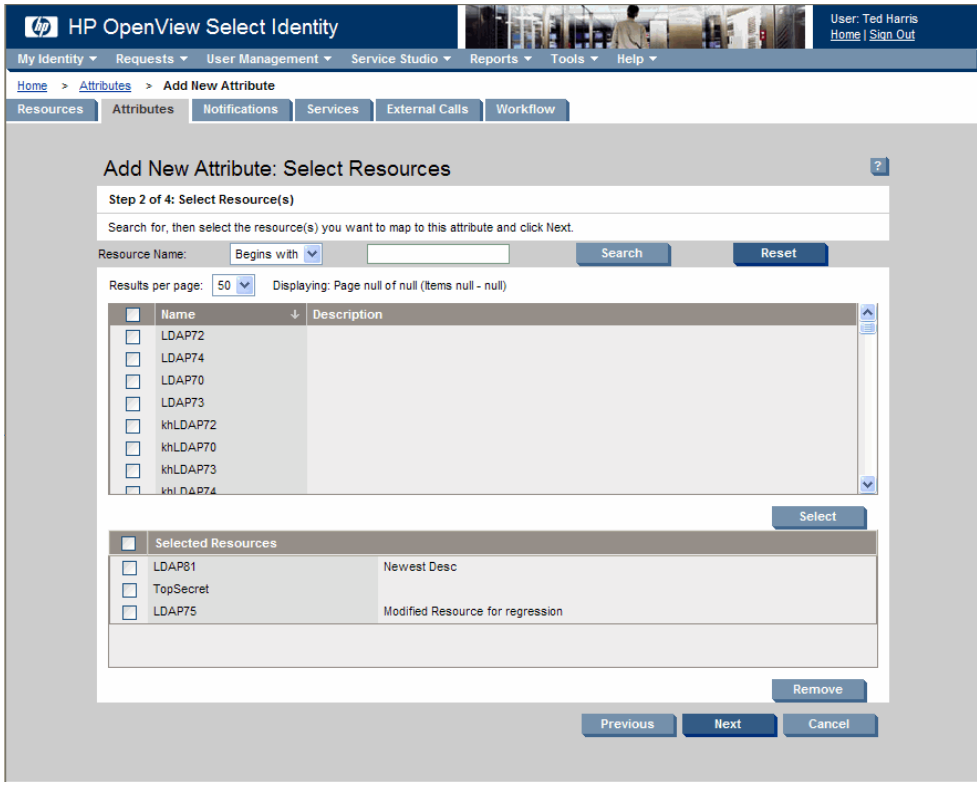
Field	Action
Attribute Name	Enter the name of the new attribute.
Identity Object Type	Select the correct attribute object type. Choose **User** if the attribute will define user profile information.
Attribute Type	Define the level of security required for this attribute by selecting the attribute type.
Primitive Type	Select the value type that you want assigned to this attribute such as string, numeric, or date.

Field	Action
Storage Type	Determine the encryption requirements for the attribute by selecting the appropriate option. This option determines if the attribute is stored with **OneWay** encryption and cannot be retrieved, or **TwoWay** as an encrypted value that can be retrieved. These options are useful for sensitive data such as passwords and tax ID numbers.
Description	Enter a brief description of the attribute if necessary
Default Help Text	Enter text to help the user understand what is required from this field in the text box.
Multi Value	Select **Yes** if this attribute can have multiple correct values.
Min Length	Enter a minimum length for the attribute value.
Max Length	Type a maximum length for the attribute value.
Value Pattern	Define the value pattern by entering a Jakarta style of regular expression. For example: `^([a-zA-Z]+)([a-zA-Z0-9_'\\.|\\-])*@((([a-zA-Z]+)\.))*([a-zA-Z]{2,4})$`
Self-Service Permission	Determine whether or not an End User may update this attribute in the My Identity self-service application by selecting the appropriate option from the drop-down menu. **Hidden** — Ensures the attribute cannot be seen when a user performs a view or modify profile in Self Service. **Masked Read Only** — The attribute's real value cannot be seen and instead is masked with asterisks when viewing or modifying a profile. **Read Only** — The attribute value cannot be modified and can only be viewed when the user modifies their profile. **Updateable** — The attribute value can be modified when the user modifies their profile.

Field	Action
Default Display Name	Type the name you want users to see when they are registering for a Service.
Default Display Mask	Enter a number in the Default Display Mask field if you want to mask all or part of the value accepted in this field with asterisks. Use this option to mask secure entries such as password entries.
Default Display Length	Enter the number of characters that you want displayed for the attribute value
Profile Attribute	Select the **Yes** radio button if this is a profile attribute and the **No** radio button if it is note.
Resource Action	Select the method used to update this attribute from the Resource.

5 Click the **Next** button.
The **Add New Attributes: Select Resources** page opens.

Figure 47 Add New Attributes: Select Resources Page



Selecting Resources to Map to the New Attribute

Use this mapping feature to save time when you have to map a new Select Identity attribute to more than one resource.

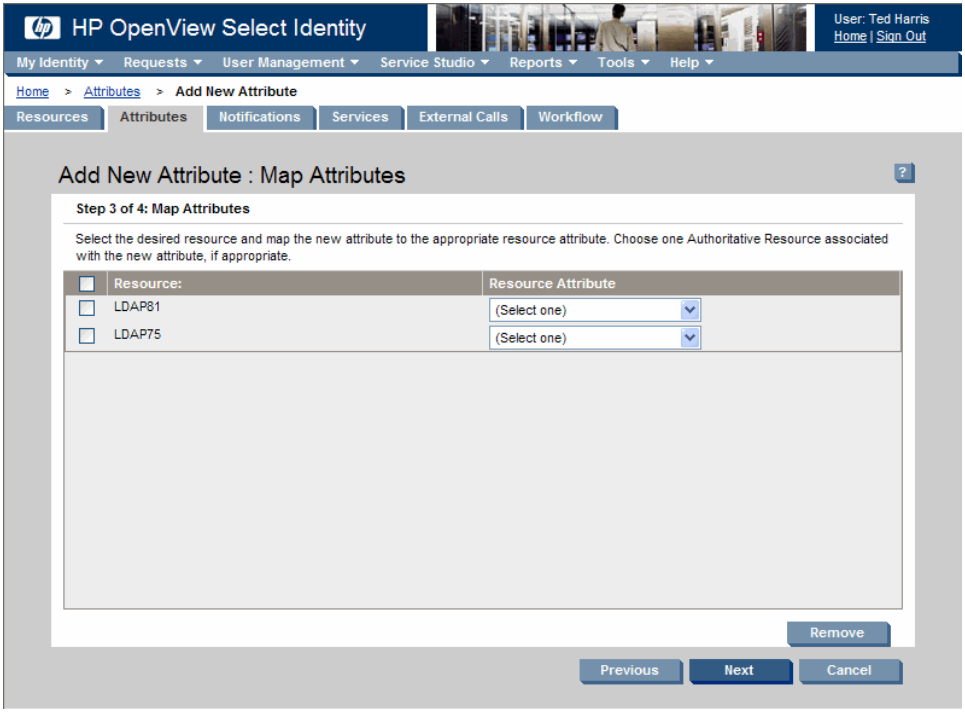
Use the Mapping Resource Attributes on page 72 procedure to map a new resource with multiple attributes to the corresponding Select Identity Attributes.

Follow the steps below to map a new attribute:

1. Review the list of resources displayed and select each resource you want to map to the new Select Identity attribute.
2. Click the **Select** button.
   Shows the selected list in the **Select Resources** panel.

3 Click the **Next** button.
The **Add New Attribute: Map Attribute** page opens.

Figure 48 Add New Attribute: Map Attribute



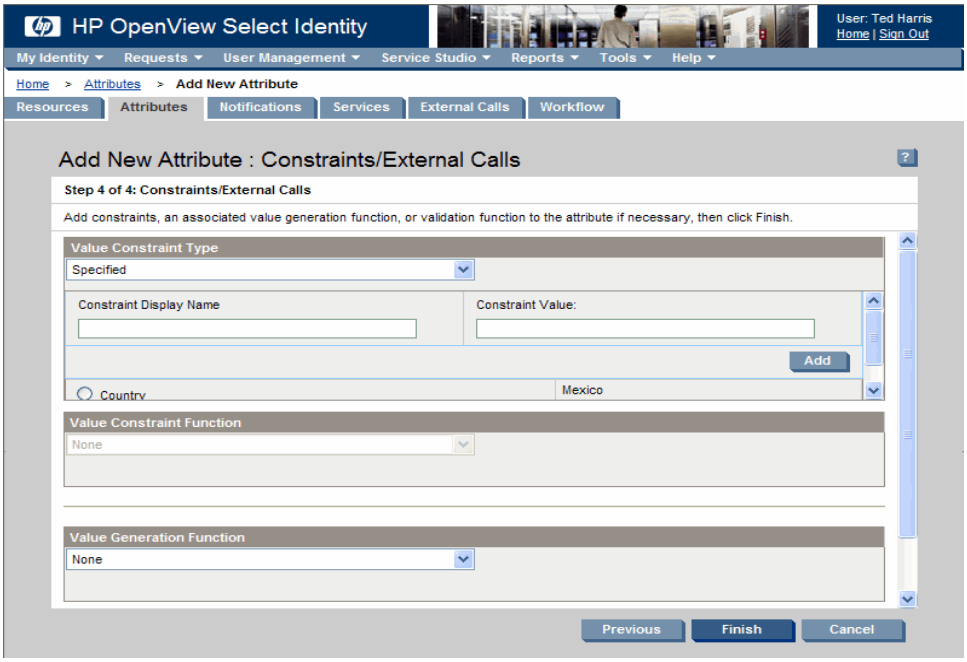
4 Select the first attribute you want to map.

5 Click the drop-down menu in the **Resource Attribute** column and select the attribute you want to match to the Select Identity attribute.

6 Repeat the procedure until all of the resources have been mapped.

7 Click the **Next** button.
The **Add New Attribute: Constraints / External Calls** page opens.

Figure 49 Add New Attribute: Constraints / External Calls



Adding Constraints and External Calls to the New OVSI Attribute

You may want to add constraints to the new Select Identity attribute that will be used during reconciliation. Constraints are optional, but will often speed the reconciliation process. Learn more about reconciliation at Account Reconciliation on page 401.

Follow the steps below to add a constraint or external call:

1 Determine if you want to add a constraint.

If	Then
You do not want a Constraint.	Select **None** from the **Value Constraint Type** drop-down menu.
You want to add a specific constraint to the attribute	Select **Specified** in the **Value Constraint Type** field, which enables you to specify values that a user can select for this attribute. Enter the name of the constraint in the **Constraint Display Name** field. Type the constraint value in the **Constraint Value** field. Click the **Add** button.
You want to add a dynamic constraint to the attribute	Select **Dynamic** from the **Value Constraint Type** drop-down menu.

2 Determine whether or not you want to add Value Constraint Functions to the attribute.

If	Then
You do not want a value constraint function	Select **None** from the **Value Constraint Functions** drop-down menu.
You want a resource for the value constraint function	Click **Search Connector** in the **Value Constraint Function** drop-down menu. Enter the name of the resource you want to use in the **resource_name** field.
You want to search for the value constraint function in the database table	Select **Search Table** in the **Value Constraint Function** drop-down menu. Enter the name of the resource you want to use in the **poolname** field. Type the query in the query field. Enter the expected value in the valuefield.

3 Determine if you want to call a function to generate the value of the attribute.

If	Then
You do not want to call a function to generate the value of the attribute	Select **None** from the **Value Generation Functions** drop-down menu.
You select UserIDValueGeneration	Click the **Attribute Name** field and enter the name of the attribute. Tab to the **Length** field and enter the character length of the value you want to generate. Tab to the **MaxRetryAttempts** field and enter a numeric value that determines the number of times the system should try to generate the value before the process fails.
You select IDValueGeneration	Click the **Prefix** field and enter the prefix required by the connector. Tab to the **Suffix** field and enter the suffix required by the connector.
You select PasswordValueGeneration	Enter the maximum number of characters that can be entered for a password can be created in the **maxLength** field. Enter the number of characters that are required before a password can be created in the **mimLength** field

4 Determine whether you want the new attribute to use Value Validation Functions.

If	Then
You do not want validations	Select **None** from the **Value Validation Functions** drop-down menu.
You want to validate the connector	Click **Validate Connectors** in the **Value Validation Functions** drop-down menu. Select the **resource_name** field and enter the name of the resource.
Use expirations with validations	Select **ManagerEXpire** from the **Value Validation Functions** drop-down menu.
You use functions to validate passwords	Select **PasswordValidation** from the **Value Validation Functions** drop-down menu. Enter the number of alpha characters that are required before a password can be created in the **Letters** field. Tab to the **Numerics** field and enter how many numbers are required before a password can be created. Tab to **UpperCase Letters** and enter the number of uppercase alpha characters that must be included in the entry before a password can be created.
You use any alphanumeric character	Select **iAlphaNumeric** from the **Value Validation Functions** drop-down menu.

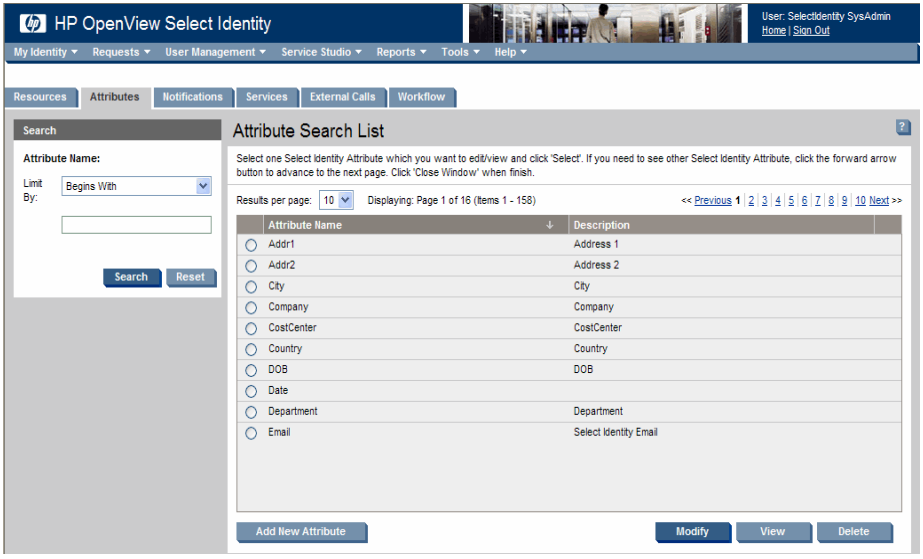
5 Click the **Finish** button.
Returns to the **Attribute List** page.

Viewing Existing Attributes

Perform the following steps to add an attribute:

1 Select **Service Studio** → **Attributes** from the menu bar options.
The **Attribute List** page opens.

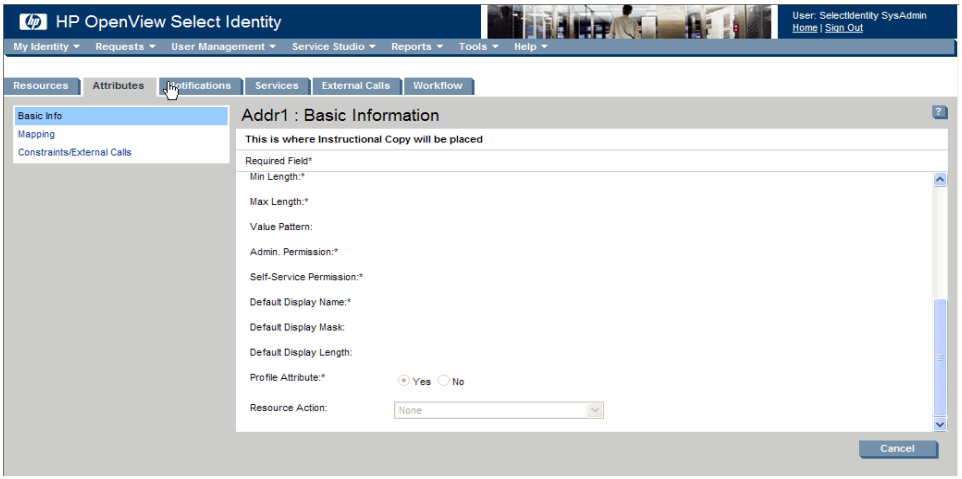
Figure 50 Attribute List



2 Review the list of attributes displayed and select the attribute you want to view.

3 Click the **View** button.
The **View Attribute: Attribute Name** page opens.

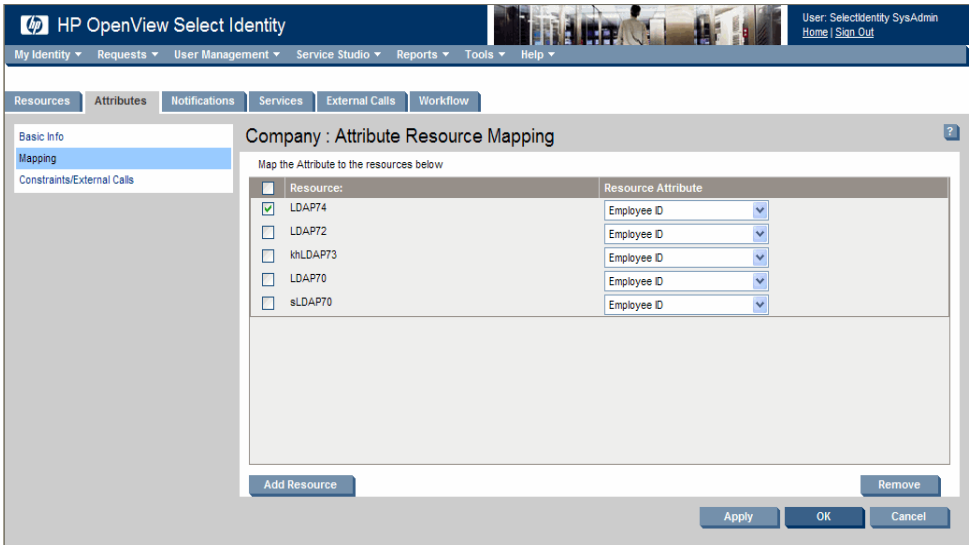
Figure 51 View Attribute: Attribute Name



4 Review the fields displayed.

5 Click the **Mapping** link in the left panel.
The **Attribute Resource Mapping** page opens.

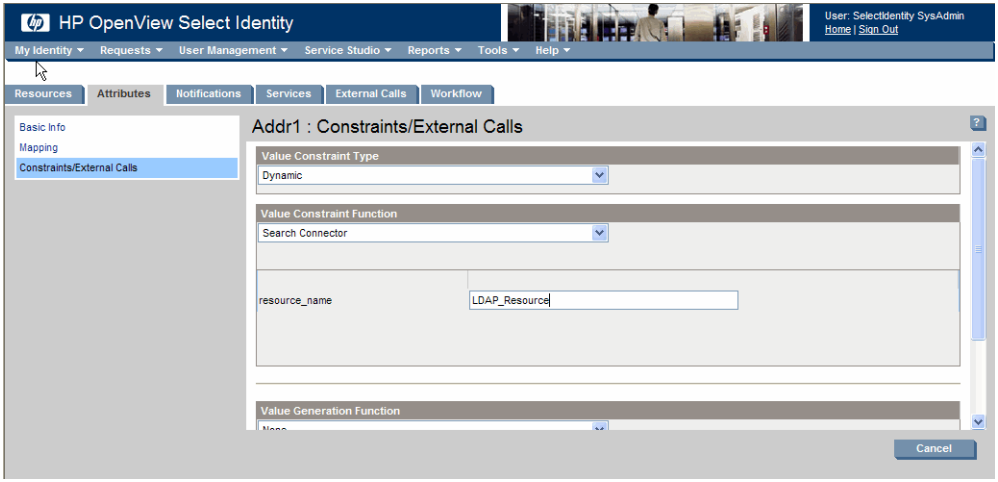
Figure 52 Attribute Resource Mapping



6 Review the fields displayed.

7 Click the **Constraints External Calls** link in the left panel.
The **View Attributes Constraints External Calls: Attribute Name** page opens.

Figure 53 View Attribute Constraints External Calls: Attribute Name



8 Click **Cancel**.
Returns to the **Attribute List**.

9 Click **Apply**.
Saves your work.

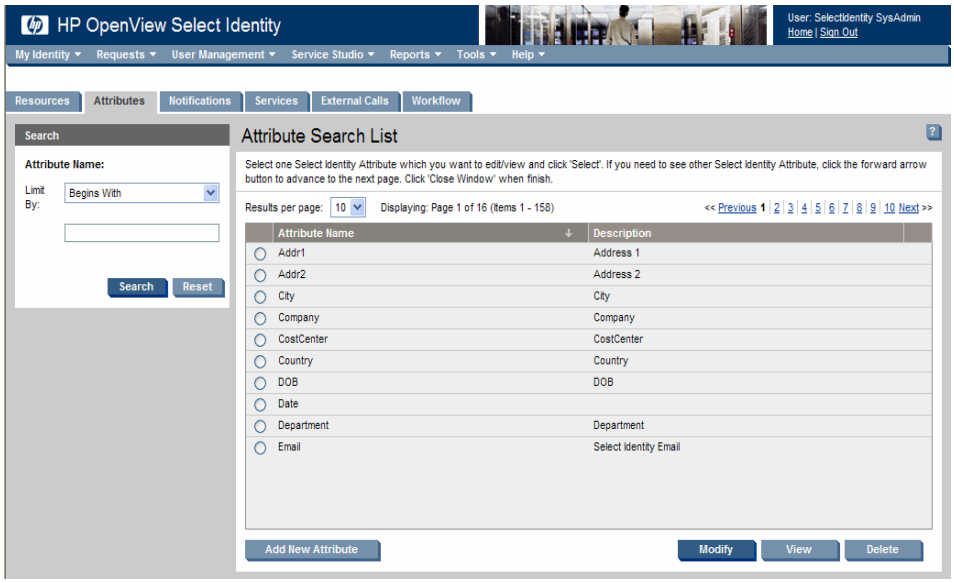
Specify password parameters by configuring the Password attribute on Select Identity. Select Identity uses a default password attribute called password. This attribute cannot be removed as it is used for Select Identity system authentication. Use this attribute to synchronize the same password to any number of resources.

Modifying Attributes

Follow the steps below to modify attributes:

1 Select **Service Studio** → **Attributes** from the menu bar options.
The **Attribute List** page opens.

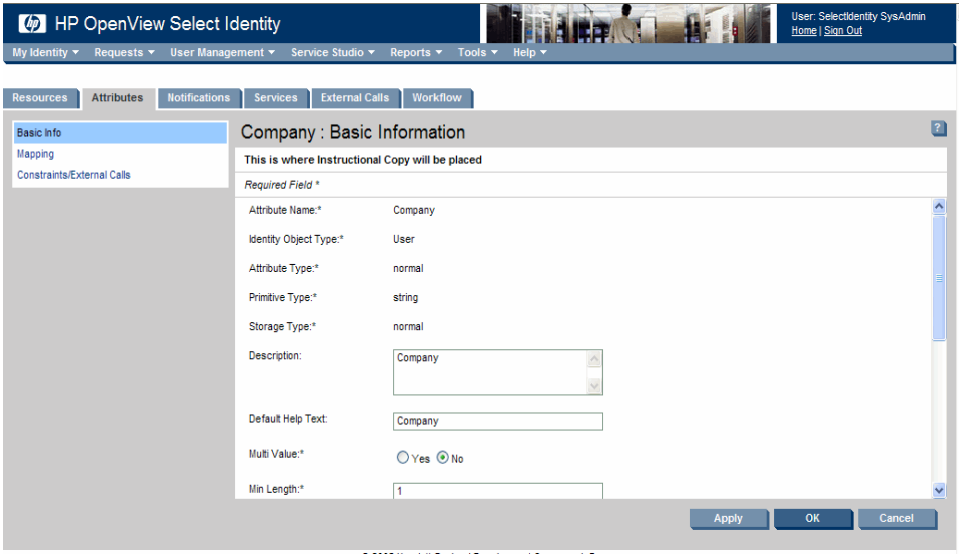
Figure 54 Attribute List



2 Review the list of attributes displayed and select the attribute you want to modify.

3 Click the **Modify** button.
The **Modify Attribute: Attribute Name** page opens.

Figure 55 Modify Attribute: Attribute Name



4 Tab from field to field and update any entry necessary.

Field	Action
Description	Enter a brief description of the attribute if necessary
Default Help Text	Enter text to help the user understand what is required from this field in the Default Help text box.
Multi Value	Select **Yes** if this attribute can have multiple correct values.
Min Length	Enter a minimum length for the attribute value.
Max Length	Type a maximum length for the attribute value.
Value Pattern	Define the value pattern by entering a Jakarta style of regular expression. For example: `^([a-zA-Z]+)([a-zA-Z0-9_'\\.|\\-])*@((([a-zA-Z]+)\\.))*([a-zA-Z]{2,4})$`

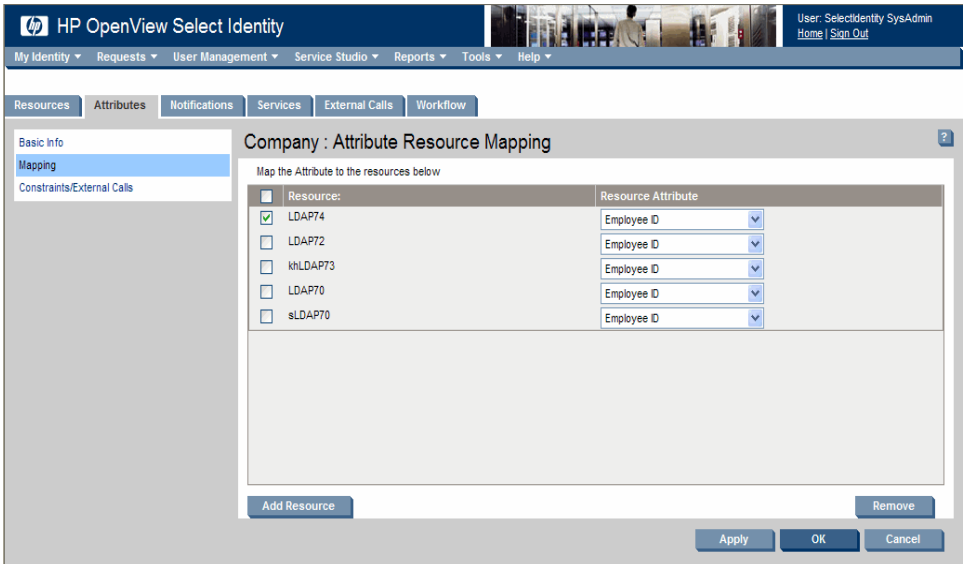
Field	Action
Self-Service Permission	Determine whether or not an End User may update this attribute in the My Identity self-service application by selecting the appropriate option from the drop-down menu.
Default Display Name	Type the name you want users to see when they are registering for a Service.
Default Display Mask	Enter a number in the Default Display Mask field if you want to mask all or part of the value accepted in this field with asterisks. Use this option to mask secure entries such as password entries. When you modify the attribute to set the Default Display Mask, you must follow the instructions for each of the following cases for the mask to work in the new service: • Existing attribute, new service: Modify the attribute to set the Default Display Mask and add this attribute to a new service. • Existing attribute, existing service:
Default Display Length	Enter the number of characters that you want displayed for the attribute value
Profile Attribute	Select the **Yes** radio button if this is a profile attribute and the **No** radio button if it is note.
Resource Action	Select the method used to update this attribute from the Resource.

Modifying Resource Attribute Mappings

Follow the steps below to modify resource attribute mappings:

1 Click the **Mapping** link in the left panel.
The **Modify Attribute Resource Mapping: Attribute Name** page opens.

Figure 56 Modify Attribute Resource Mapping: Attribute Name



2 Review the list of resources previously mapped to this attribute to determine what should be done.

If	Then
You want to add a new resource to the list	Click **Add Resource** and follow steps that describe Selecting Resources to Map to the New Attribute on page 109.
You want to remove a resource from the list	Select the resource you no longer want mapped to this attribute and click **Remove**.
You want to change the current mapping	Select the resource you want to change and then choose the correct attributable from the **Resource Attribute** drop-down menu.

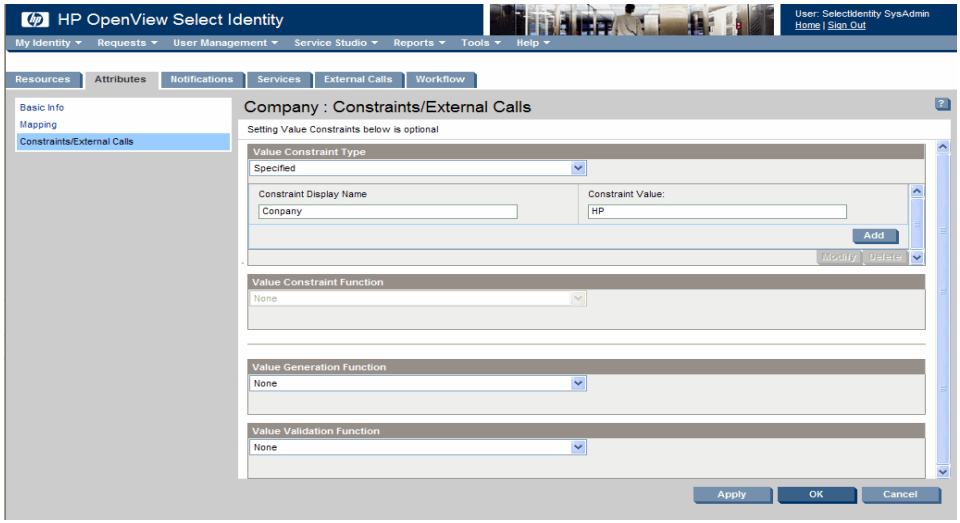
3 Click **Apply**.
Saves your work.

4 Click **OK**.
Returns to the **Attribute List** page.

Modifying Attribute Constraints / External Calls

1 Click the **Constraints / External Calls** link in the left panel.
Opens the **Modify Attribute Constraints / External Calls** page.

Figure 57 Modify Attribute Constraints / External Calls



2 Review the constraints and external calls already set up for this attribute.

If	Then
You do not want to call a function to generate the value of the attribute	Select **None** from the **Value Constraint Type** drop-down menu to remove the call information.
You want to remove an existing constraint	Select **None** from the **Value Constraint Type** drop-down menu to remove the constraint information.
You want to add an external call	Follow the steps outlined in Adding Constraints and External Calls to the New OVSI Attribute on page 111.
You want to add a new constraint	Follow the steps outlined in Adding Constraints and External Calls to the New OVSI Attribute on page 111.

3 Click **Apply**.
Saves your work.

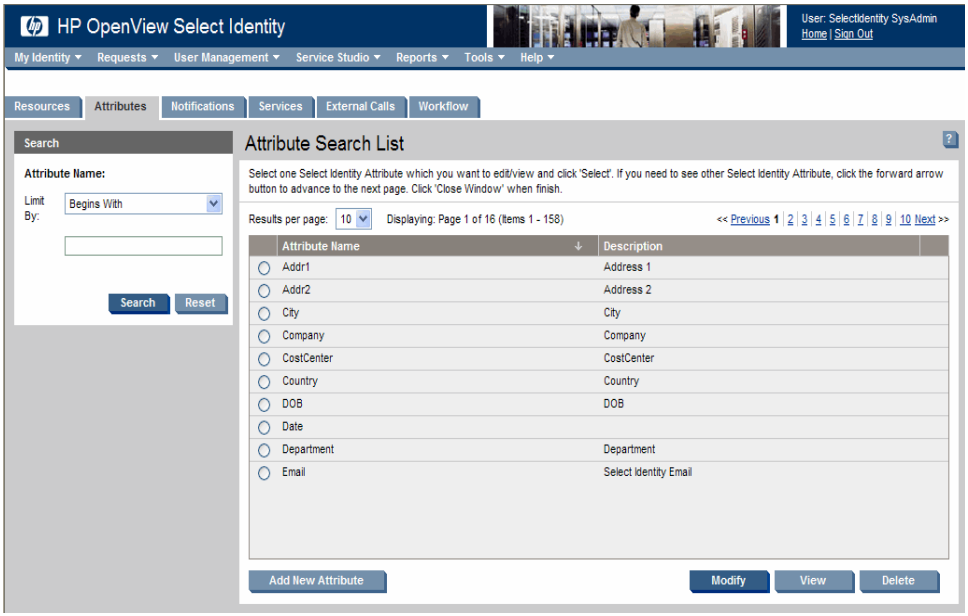
4 Click **OK**.
Returns to the Attribute List page.

Deleting an Attribute

Remove any Service or Service Role dependencies before deleting the attribute. Perform the following steps to delete an attribute:

1 Select **Service Studio** → **Attribute List** from the menu bar options.
The **Attribute List** page opens.

Figure 58 Attribute List



2 Review the list of attributes displayed and select the attribute you want to delete.

3 Click the **Delete** button.
Shows the confirmation dialog box.

4 Click **OK**.
Deletes the attribute.

Deleting an attribute from Select Identity does not have any effect on the corresponding attributes in other resources whether or not the attributes are mapped to each other.

Managing Notification Templates

The Notifications section of the client enables you to define the content of email notices that are sent to users when an account is created or removed or when an account attribute has changed. By creating these templates, you define the messages that the Select Identity system sends when an account event occurs.

This section covers:

- Notification Variables
- Creating and Modifying Notification Templates

Notification Variables

When creating notification templates, use variables inside the notification to inform the recipient of meaningful user data or request data. The variables are replaced with actual values when an email is sent using the email template.

Any sensitive fields that should be encrypted when stored in the database, must be wrapped with the tag `<ovsi-encrypt>`. This is to ensure that the sensitive field is not stored in clear text in the HP OpenView database. For example, use `<ovsi-encrypt>[RQT:Password]</ovsi-encrypt>` for a “New Account Password” notification.

Email Template Variables

Variable Type	Description	Variable
Request	Variables for the Request Object. The Request variable provides the ability to reference "request" information in an email template. Following are predefined Request variables: [REQ:ParentRequestId] [REQ:ServiceName] [REQ:RequestId] [REQ:RequestActionName] [REQ:RequestActionDescription]	**REQ:**
RequestTarget	Variables for the userID that is being created. The RequestTarget variable provides the ability to reference information about the target user being provisioned in an email template. Any attributes associated with the User for the given service in the request may be accessed. Example: [RQT:UserName]	**RQT:**

Variable Type	Description	Variable
User-Defined	The User-Defined variable provides the ability to reference user-defined variables defined in a workflow for use in an email template. Following are a list of predefined User-Defined variables that can be used in email notifications: [USERDEF:Status] — Denotes the status of the Service. [USERDEF:ResetStatus] — Denotes the status of provisioning for a resource within a service. [USERDEF:Action] — Action performed against the targeted user. [USERDEF:ServiceName] — The service associated with the workflow request. [USERDEF:pendingTaskURL] — If an approver is required for a request, this variable contains the URL string in OVSI used to approve the request.	**USERDEF:**
Requestor	Variables for the administrator making the request. The Requestor variable provides the ability to reference information about the person submitting a request in an email template. Any attributes associated with the admin or requestor requesting the action (such as modify user), can be accessed in the email template. Example: [RQSTR:UserName]	**RQSTR:**

Variable Type	Description	Variable
Workflow	Variables defined in the workflow template. The Workflow variable provides the ability to reference variables defined in the workflow template. Variable names of persisted variables begin with $and are stored in the Select Identity database, even when a workflow instance ends. Access these variables at any time once the workflow instance is created. Select Identity provides the AppoverComments variable, but you can create your own. Example: [WF:$ApproverComments]	**WF:**
Environment	Variables are defined for the environment within the properties file. The environment variable provides the ability to reference variables defined for the Java Virtual Machine (JVM) environment. By default, Select Identity adds all properties from the `truaccess.properties` file to the Java Virtual Machine (JVM) environment. Any value that performs a `System.getProperty()` can be used for this variable. Example: To access a version of Select Identity, you might use the following in an email template: [ENV:truaccess.version]	**ENV:**

Creating and Modifying Notification Templates

Notices are sent to a user when an account is approved, rejected, or modified. Email can also be sent when an account password or hint is reset.

This section provides details of the actions you can perform within the Notifications pages. Access to each of these functional areas is determined by the administrative roles assigned to your account.

This section covers the following:

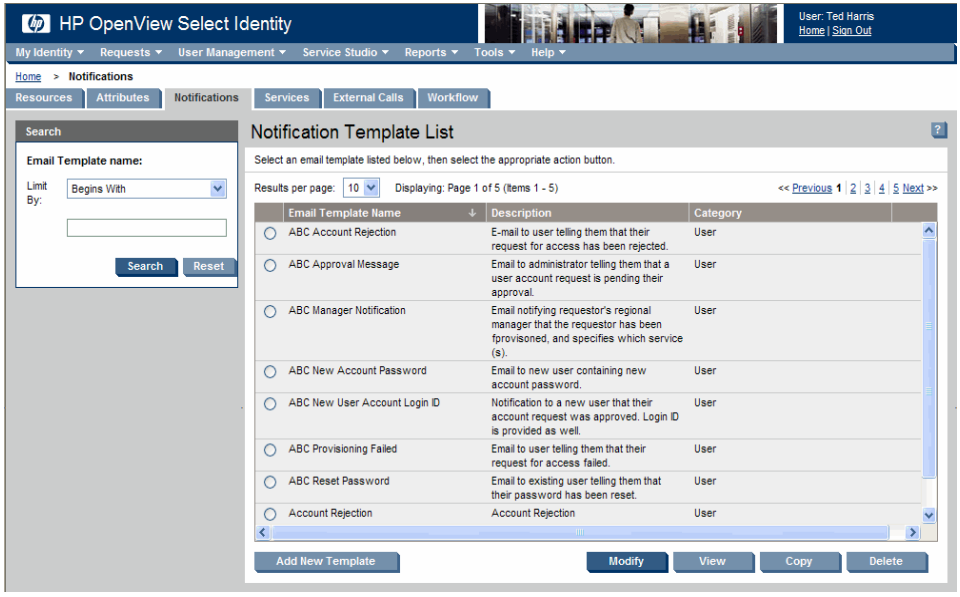
- Adding a Notification Template
- Copying a Notification Template
- Modifying a Notification Template
- Deleting a Notification Template

Adding a Notification Template

Perform the following steps to add a new notification template:

1 Select **Service Studio** → **Notifications** from the menu bar options.
The **Notification Template List** page opens.

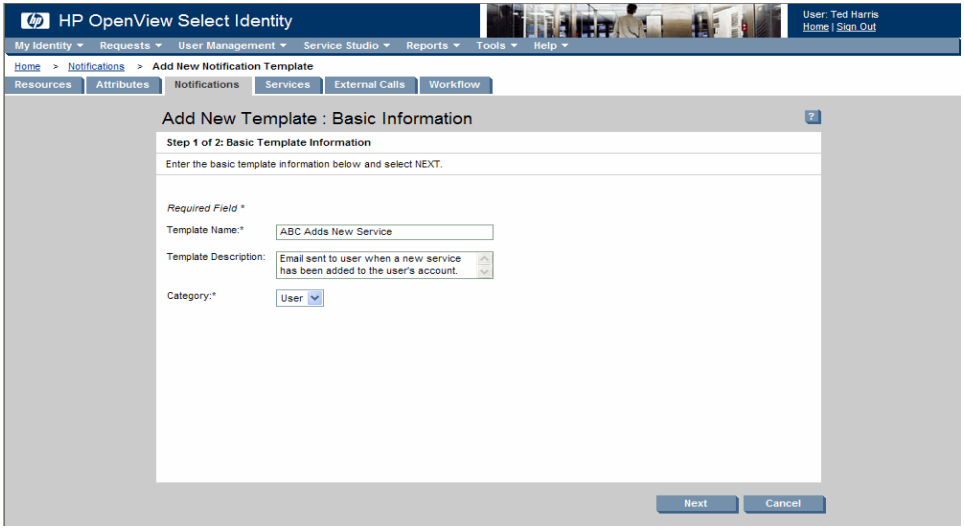
Figure 59 Notification Template List Page



2 Review the list of notification templates to make sure there is not a template existing already that meets your needs.

3 Click the **Add New Template** button.
Opens the **Add New Template: Basic Information** page.

Figure 60 Add New Template: Basic Information

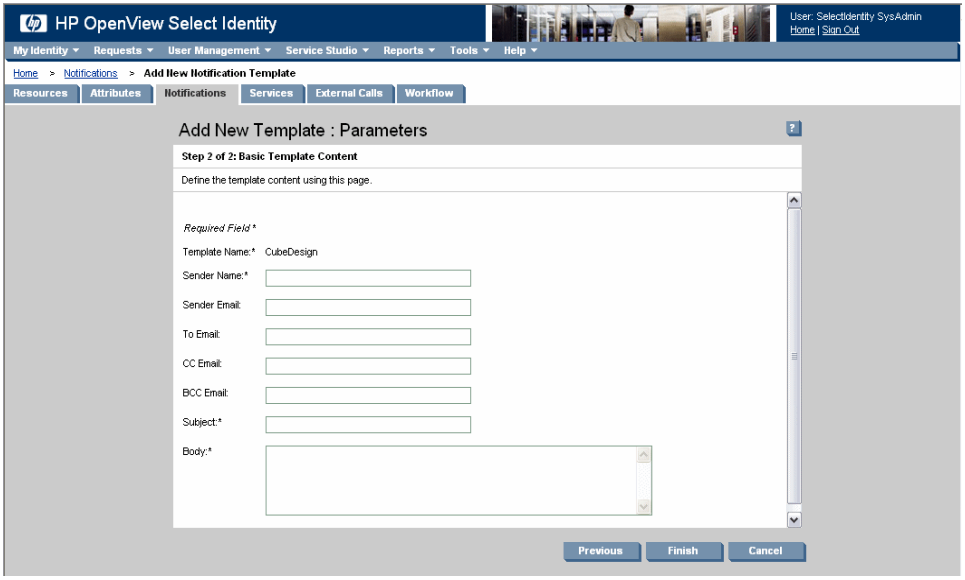


4 Tab from field-to-field to enter the required information.

Field	Action
Template Name	Enter the complete name of the template.
Template Descriptions	Type a brief description of the template.
Category	Select the correct notification category from the drop-down menu. Leave the default entry, **User** to define a notification template that users will see when their accounts are created or modified.

5 Click **Next**.
The **Add New Template: Parameters** page opens.

Figure 61 Add New Template: Parameters Page



Use predefined variables, such as [RQSTR:UserName], and the system enters the correct information for you. See Notification Variables on page 124 for more information.

6 Tab from field-to-field to enter the required information.

Field	Action
Sender Name	Enter the name of the person or entity that should display in the From field of the email such as System Administrator. The sender person or entity must have a valid email address.
Sender Email	Enter the sender email address in a sender@isp.com format.
To Email	Enter the email address of the recipient using the appropriate variables.

Field	Action
CC: Email	Enter the email address of a recipient(s) you want to copy using the appropriate variables, if necessary.
BCC: Email	Enter the email address of a recipient(s) you want to copy without the original recipient knowing using the appropriate variables, if necessary.
Subject	Enter the standard subject you want included on emails of this type using variables if necessary.
Body	Type the body of the message. Include any variables necessary to make the message meaningful based on the category of message you are wanting to send.

.

For a sensitive field that should be encrypted, such as the password in a "New Account Password" notification, be sure to wrap the field's tag with the tag `<ovsi-encrypt>`. For example, the email body text for a "New Account Password" notification might be:

> The following is your new account password for the indicated Service:
>
> Password: <ovsi-encrypt>[RQT:Password]</ovsi-encrypt>
>
> Service: [REQ:ServiceName]
>
> Thanks

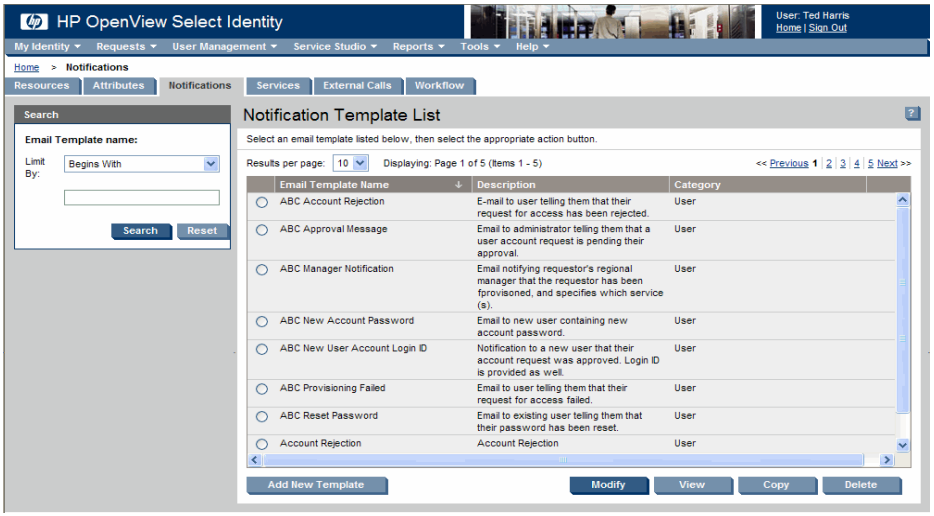
7 Click **Finish**.
Returns to the **Notification Template List** page with a confirmation message.

Viewing a Notification Template

Follow the steps below to view a notification template:

1 Select **Service Studio** → **Notifications** from the menu bar options.
The **Notification Template List** page opens.

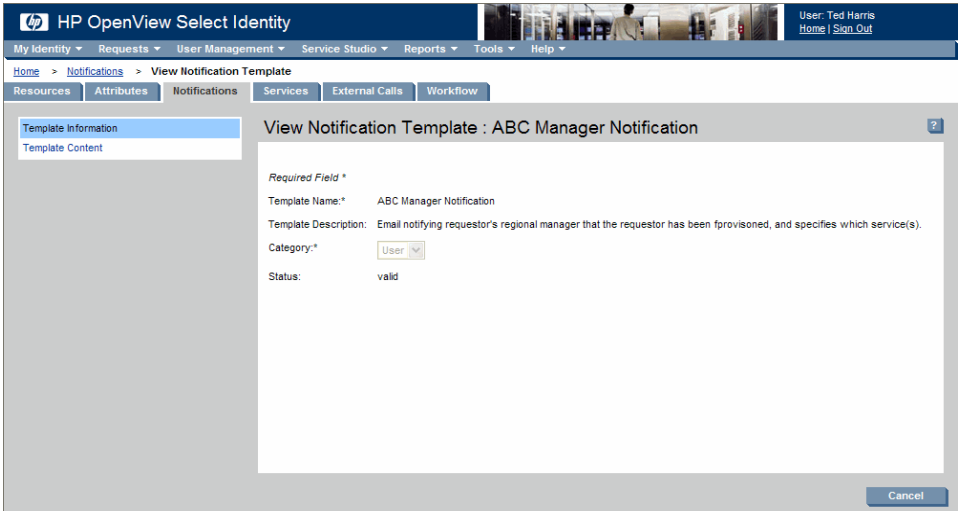
Figure 62 Notification Template List



2 Select the email template you want to view.

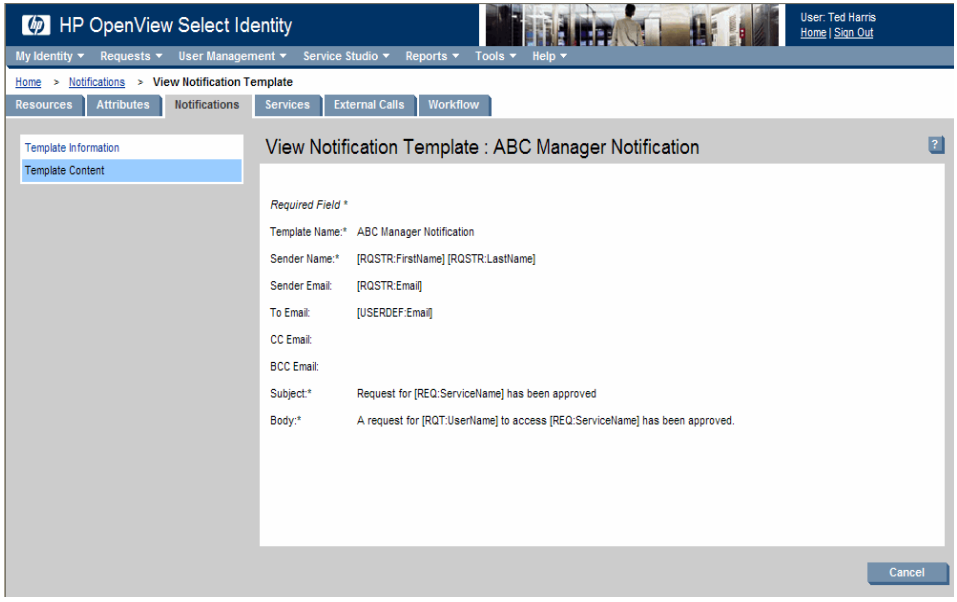
3 Click **View.**
The **View Notification Template: Template Name** page opens.

Figure 63 View Notification Template: Template Name



4 Click **Template Content.**
The **View Notification Template: Template Name** page opens.

Figure 64 View Notification Template: Template Name



5 Click **Cancel**.
Returns to the **Notification Template List** page.

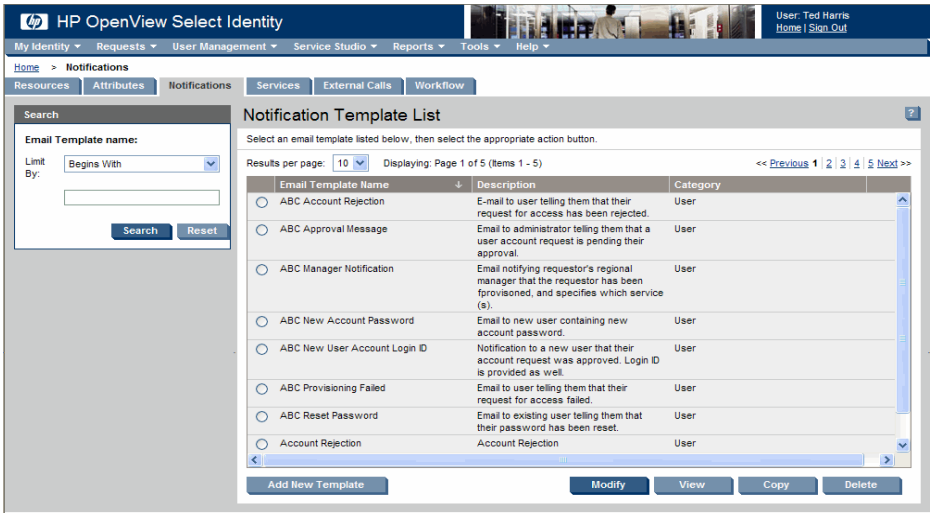
Copying a Notification Template

If you have several similar template requirements, you may want to create one and use the Copy Notifications action to create the rest. This enables you to copy all of the configuration information from the first template and edit only the fields that are different, instead of entering all of the information again.

Follow the steps below to copy a notification template:

1 Select **Service Studio** → **Notifications** from the menu bar options.
The **Email Template List** page opens.

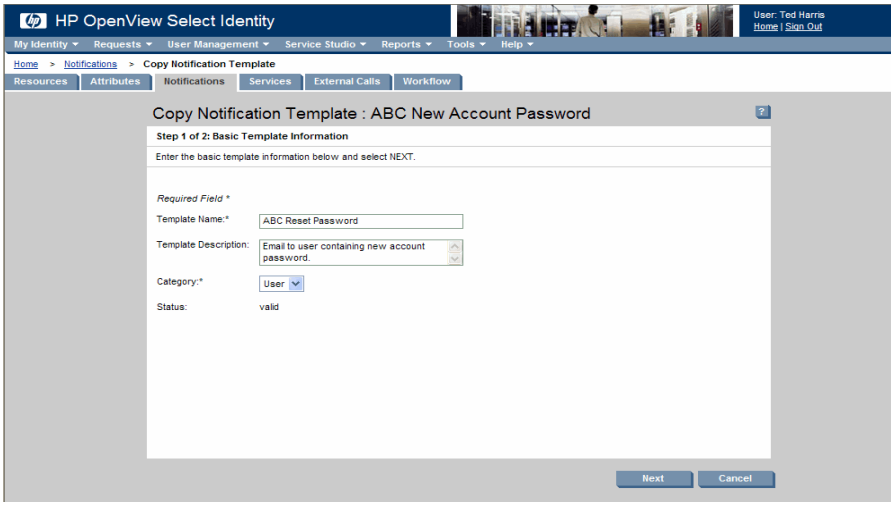
Figure 65 Notification Template List



2 Select the email template you want to copy.

3 Click **Copy.**
The **Copy Notification Template: Template Name** page opens.

Figure 66 Copy Notification Template: Template Name



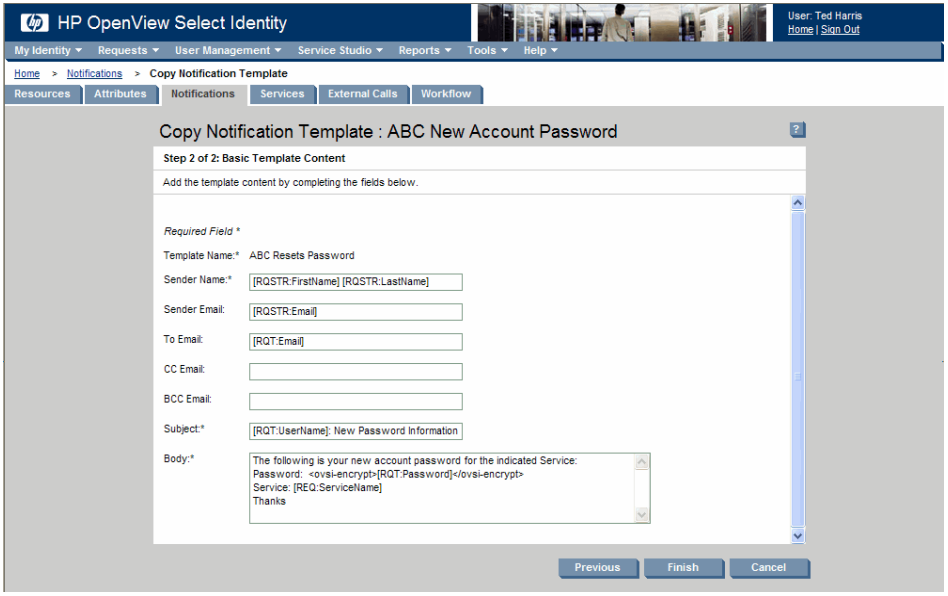
4 Tab from field to field and update the information required:

Field	Action
Template Name	Enter the complete name of the template.
Template Descriptions	Type a brief description of the template.
Category	Select the correct notification category from the drop-down menu. Leave the default entry, **User** to define a notification template that users will see when their accounts are created or modified.

5 Click **Next**.
The **COPY** page opens.

Use predefined variables, such as [RQSTR:UserName], so that the system enters the name of the administrator sending the request. See Notification Variables on page 124 for more information

Figure 67 Copy Notification Template: Template Name



6 Tab from field-to-field to update the required information.

Field	Action
Sender Name	Enter the name of the person or entity that should display in the From field of the email such as System Administrator.
Sender Email	Enter the sender email address in a sender@isp.com format.
To Email	Enter the email address of the recipient using the appropriate variables.
CC: Email	Enter the email address of one or more recipients you want to copy using the appropriate variables, if necessary.

Field	Action
BCC: Email	Enter the email address of a recipient(s) you want to copy without the original recipient knowing using the appropriate variables, if necessary.
Subject	Enter the standard subject you want included on emails of this type.
Body	Type the body of the message. Include any variables necessary to make the message meaningful based on the category of message you are wanting to send.

.

For a sensitive field that should be encrypted, such as the password in a "New Account Password" notification, be sure to wrap the field's tag with the tag `<ovsi-encrypt>`. For example, the email body text for a "New Account Password" notification might be:

> The following is your new account password for the indicated Service:
>
> Password: <ovsi-encrypt>[RQT:Password]</ovsi-encrypt>
>
> Service: [REQ:ServiceName]
>
> Thanks

7 Click **Finish**.
"Returns to the **Notification Template List** page with a confirmation message.

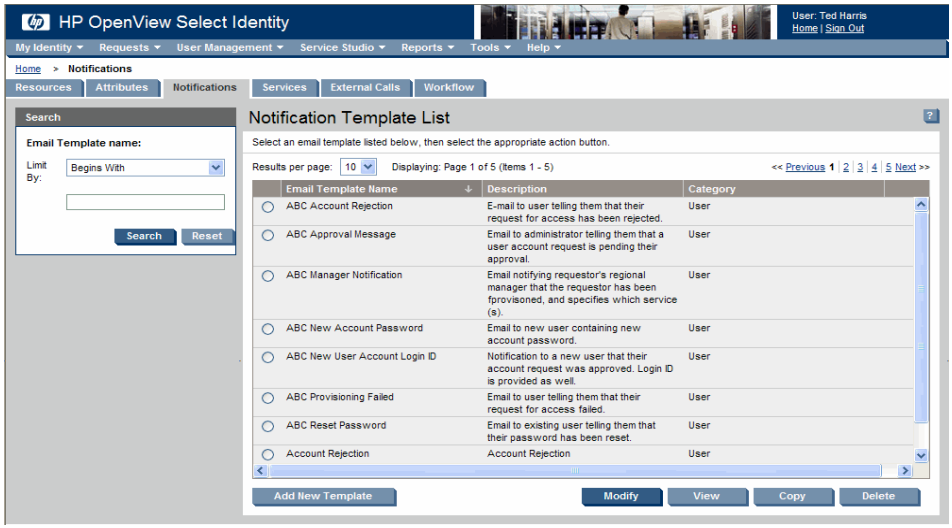
Modifying a Notification Template

After you change any of the template fields users and administrators see the new messages the next time an action prompts the system to send an email to the designated party.

Perform the following steps to modify a template:

1 Select **Service Studio** → **Notifications** from the menu bar options.
Opens the **Notification Template Search** page.

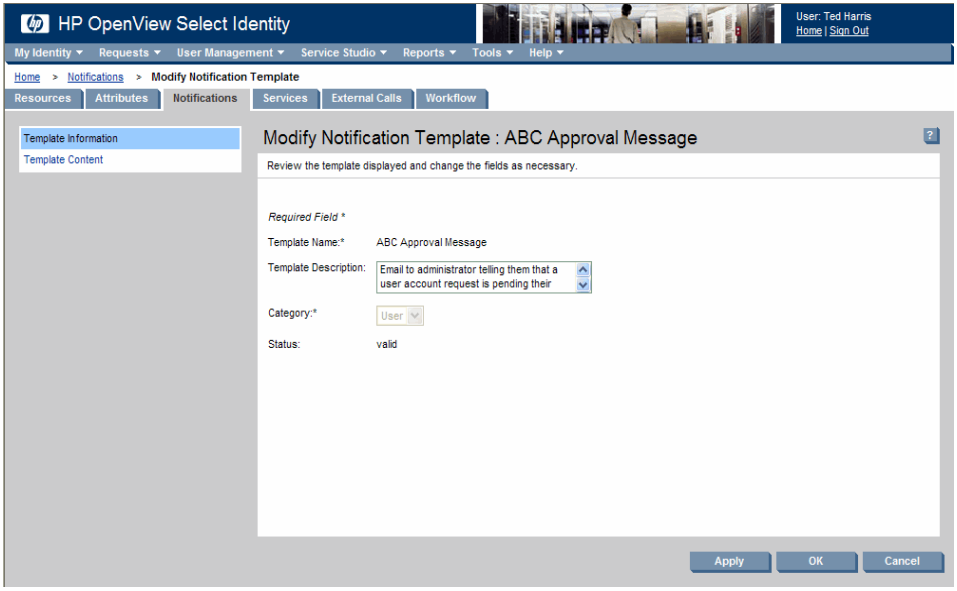
Figure 68 Notification Template List



2 Select the email template you want to modify.

3 Click **Modify.**
The **Modify Notification Template: Template Name** page opens.

Figure 69 Modify Notification Template: Template Name



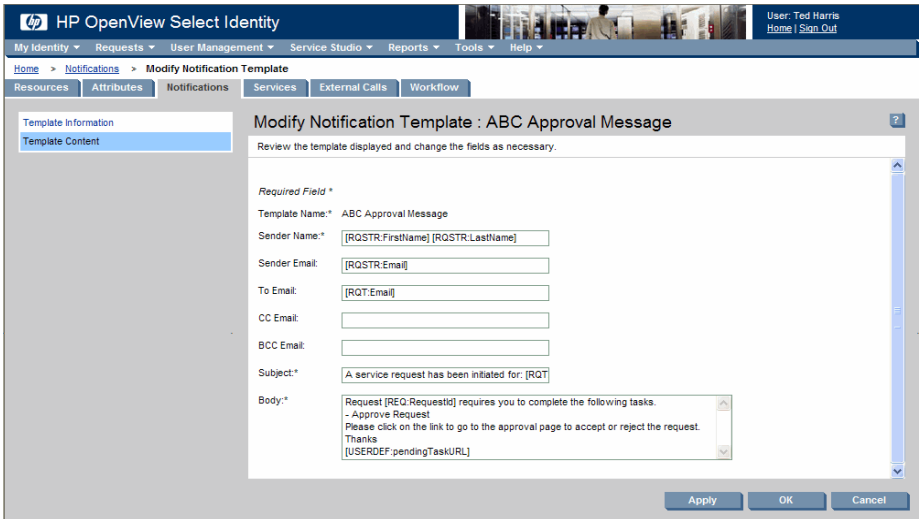
4 Tab from field to field and update the information required:

Field	Action
Template Name	Enter the complete name of the template.
Template Descriptions	Type a brief description of the template.
Category	Select the correct notification category from the drop-down menu. Leave the default entry, **User** to define a notification template that users will see when their accounts are created or modified.

5 Click **Apply**.
A message confirming the change appears at the top of the page.

6 Click Template Content.

Figure 70 Modify Notification Template: Template Name



.

Use predefined variables, such as [RQSTR:UserName], so that the system enters the name of the administrator sending the request. See Notification Variables on page 124 for more information

7 Tab from field-to-field to update the required information.

Field	Action
Sender Name	Enter the name of the person or entity that should display in the From field of the email such as System Administrator.
Sender Email	Enter the sender email address in a sender@isp.com format.
To Email	Enter the email address of the recipient using the appropriate variables.
CC: Email	Enter the email address of a recipient(s) you want to copy using the appropriate variables, if necessary.

Field	Action
BCC: Email	Enter the email address of a recipient(s) you want to copy without the original recipient knowing using the appropriate variables, if necessary.
Subject	Enter the standard subject you want included on emails of this type.
Body	Type the body of the message. Include any variables necessary to make the message meaningful based on the category of message you are wanting to send.

.

For a sensitive field that should be encrypted, such as the password in a "New Account Password" notification, be sure to wrap the field's tag with the tag `<ovsi-encrypt>`. For example, the email body text for a "New Account Password" notification might be:

> The following is your new account password for the indicated Service:
>
> Password: <ovsi-encrypt>[RQT:Password]</ovsi-encrypt>
>
> Service: [REQ:ServiceName]
>
> Thanks

8 Click the **Apply** button.
Saves your work.

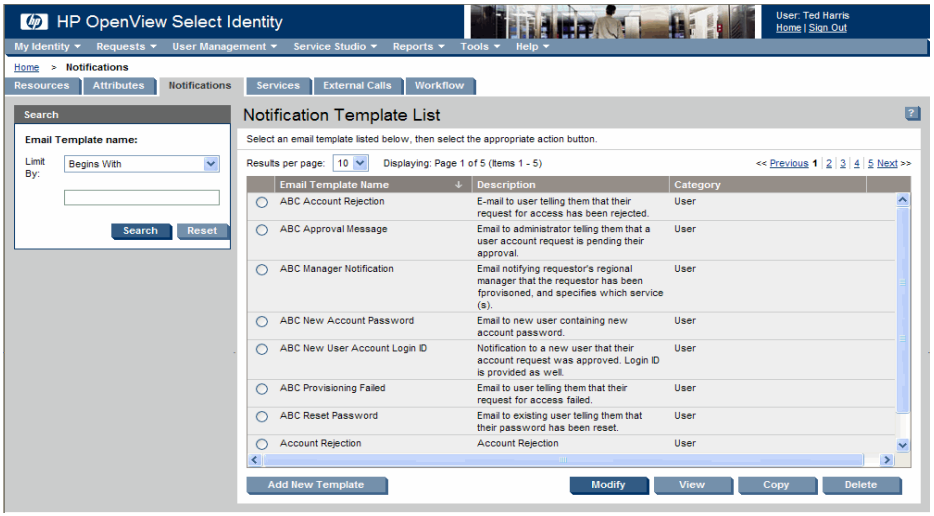
9 Click **OK**.
Returns to the **Notification Template List** page with a confirmation message at the top of the page.

Deleting a Notification Template

To delete a notification template, perform the following steps:

1 Select **Service Studio** → **Notifications** from the menu bar.
The **Notification Template List** page opens.

Figure 71 Notification Template List



2 Click the **Delete** button.
Opens the confirmation dialog box.

3 Click **OK**.
Deletes the notification.

Creating Services

Select Identity provides a service-oriented architecture. Identities are viewed and managed within the context of the Services to which each has access. The Services pages enable you to create and manage the Services that are accessed by your customer and business partners. When creating Services, you define a number of elements that will determine how your users access the system and the entitlements that they are granted when doing so.

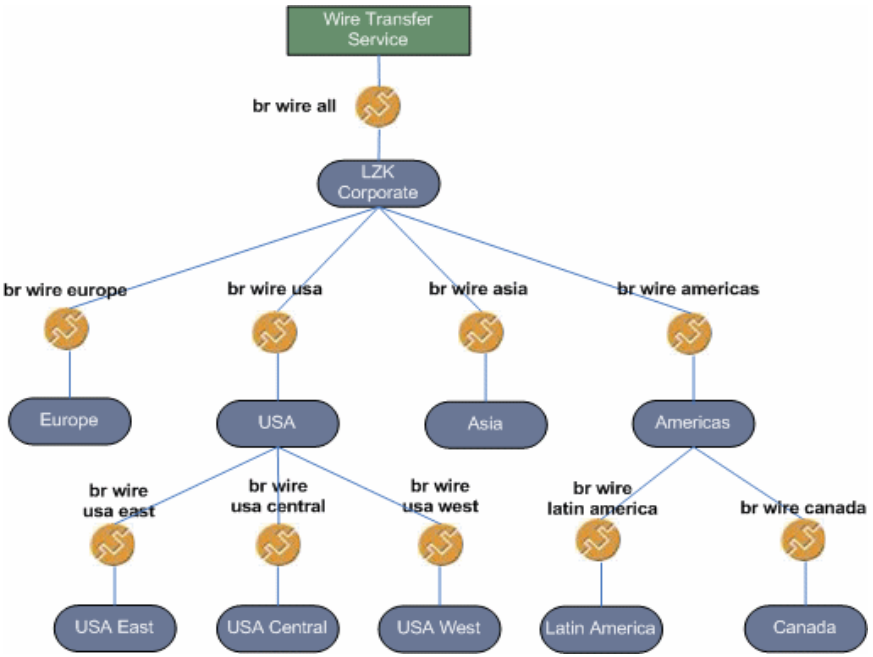
Services should be created only after all resources, attributes, notifications and workflows are in place.

Understanding Service Roles

Services are made available to your customers and partners by setting a Service Role in Select Identity. Management of Service Roles is hierarchical, which creates a secure way to share Services across different companies or locations. You can independently manage Service Role security requirements and user access throughout your Service hierarchy.

The following example illustrates a simple structure as defined by a Service Role hierarchy.

Figure 72 Service Role Hierarchy



LKZ Corporation can view and manage all Service Roles. As defined by the Service Roles, companies can view and manage partners that are lower in the Service hierarchy. This hierarchy creates a management structure that represents real Service Roles within the organization. This structure also protects the privacy and security of those roles.

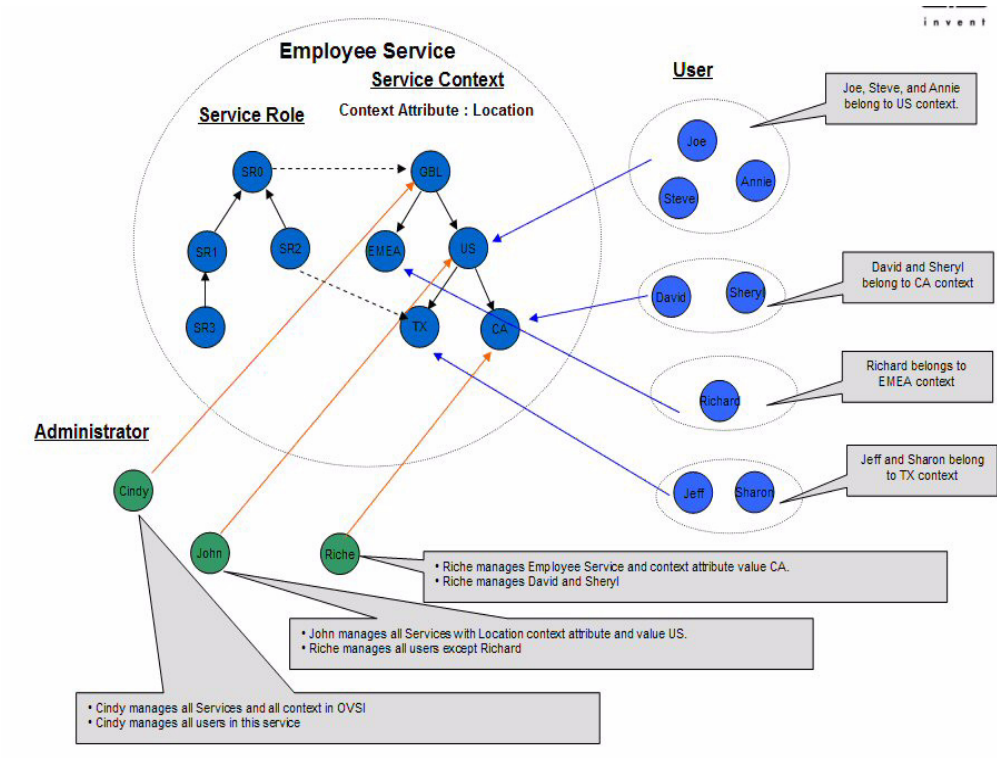
Service roles define business processes. You can select specific workflow for specific request events and also determine the form for that request. You can have fixed values for certain attributes or constrain the list of values. Child service role inherits attribute values or requests and notification event configuration from the parent service role. Parent service role inherits only from the attribute values from several level attribute values

Understanding Service Context

Service context defines the rights and permissions that a group of users receives based on the attached Service Role (such as Manager, Sales, and Clerk). Users are added to a context grouping according to the context attribute value you select. For example, you may want to group users by location. You would then select a location attribute as context attribute for your service and then create a context with values “USA,” “India,” and “France”. Service Role is attached to the Service Context. When users are added or modified or deleted from certain context attached business process in service role will be executed.

Service Context is hierarchical. Users in OVSI are managed through a service context hierarchical structure. Administrators manage certain nodes, eventually managing all users for that node and all child nodes.

Figure 73 Overall Service, User and Administrator relationship



Understand Fixed and Optional Entitlements

The Select Identity's service-oriented management structure enables you to offer sets of entitlements or privileges based on the Service Role. Entitlements or privileges can either be fixed (required) or optional.

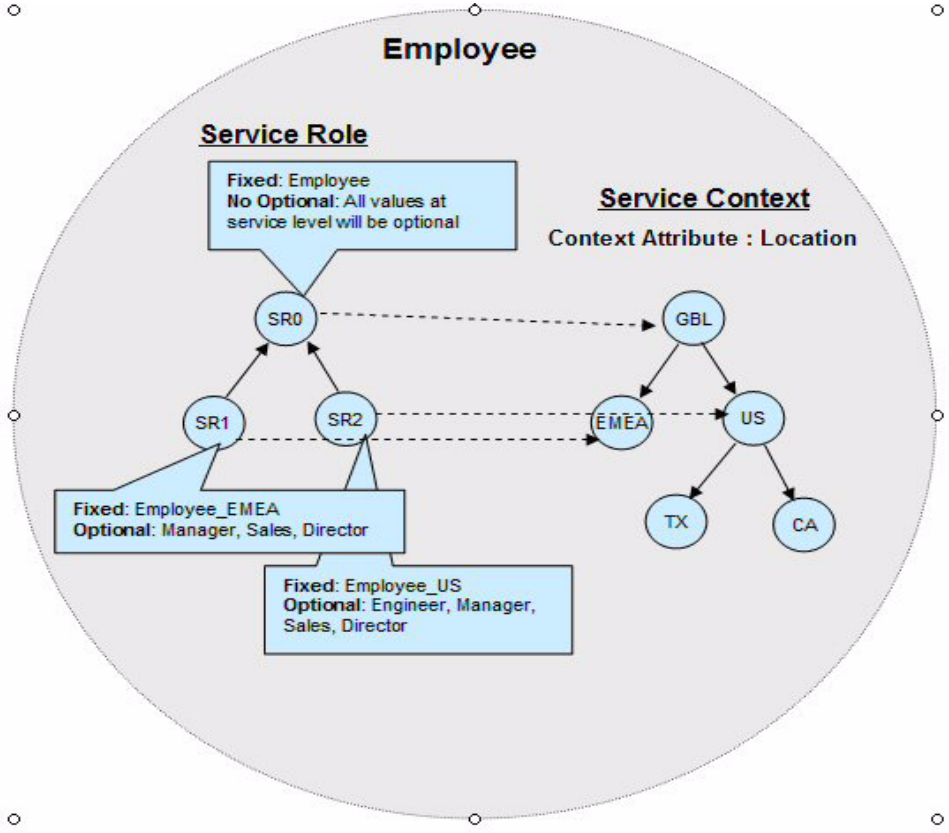
Service Roles belong to the services in which they are created. All entitlements available to any service role can first be defined at the service level. A service role can be assigned one or more entitlements belonging to the service but it cannot have an entitlement that does not belong to its service. In other words, the entitlements that are available at the Service Role level are defined by the Service. Any fixed or required Service entitlement is automatically inherited by the service role created within the service.

Optional entitlements provide a means of giving users additional entitlements through adminsitrator. Optional entitlements are defined in the Service role. The optional entitlement feature allows you to handle provisioning of those users who are exceptions to the general Service Role definition.

The root service role will inherit all values from parent service role if there is no definition at its level. Children will get all or only a subset of values defined in parent service role.

For example, your business has ‘Employee Service’ and every user in this service is required to have ‘Employee’ entitlement or privilege for certain resource. Users in the United States are required to have ‘Employee_US’ entitlement and may have one or more of following entitlements: Engineer, Manager, Sales, Director. Users in EMEA are required to have ‘Employee_EMEA’ entitlement and may have one or more of the following entitlements: Sales, Manager, Director. The following figure gives some idea about the entitlement setup in your service and how should a service role is attached to service context.

Figure 74 Service Role Attachment



Now, users belonging to US context will get Employee and Employee_US entitlements automatically. Administrators have the choice to select from Engineer, Manager, Sales or Director entitlements. Users belonging to TX or CA context have similar context.

To recap, all possible entitlement privileges are defined at the Service level. Within that set of entitlements, some are fixed and some are optional. A subset may be defined in service roles to constrain entitlements to different user contexts. Service Roles are divided into parents and children. Children receive all fixed entitlements and a subset of the optional entitlements available to the parent. Children can never have more entitlements than the

designated parent. See Adding a Service Role on page 169 for more detailed information.

Creating Services

The Services function enables you to add, modify, and delete the Services that are accessed by your employees, customers, and business partners who use your resource applications. These Services, in addition to the Service Role structure that you establish, form a management structure for users of the Select Identity system.

You can also set Service Roles and Context user groups from the Service pages. Services are made available to your customers and partners by creating a Service Role discussed in Defining Service Roles on page 169.

It is recommended that you use one type of service view to add users, and a different type of service view to modify users:

- View for adding users — Use the default service view or one you create that includes the following required attributes:

  UserName
  FirstName
  LastName
  Email
  Password

- View for modifying users — Use a service view you create that includes the following required attributes:

  UserName
  FirstName
  LastName
  Email

  Do not include the password attribute for modifying users. The password will not be pushed to any resource. Passwords should only be set when adding a user, or reset using the Reset Password action from the Users home page (see Resetting a User Password for One or More Accounts on page 295).

Creating a Service Overview

Creating a Service is the most important part in the deployment of your identity management solution.

The creation of a Service includes the following tasks:

- Creating the Service, which defines the Service type, the superset of resources, and the attributes that are required for access to the Service, including the context attribute.
- Defining attribute values and properties, which determine the attribute characteristics that are acceptable for this Service.
- Creating Service forms, which determine the registration criteria for access to the Service.
- Creating Service Roles, which define the way in which users access the Service.
- Creating Service Context groups, which defines a logical grouping of users accessing the Service.

This section covers the following:

Building a Service

Use services to provide one or more services to handle the needs of your user groups.

Prerequisites

Verify that all of the prerequisites listed below have been met:

- Resource applications and data stores required to support each service are already set up and that the appropriate
- Field attributes have been mapped
- Notification templates exist as necessary to support provisioning
- Workflows needed to create and maintain your services are built and require the necessary approvals.

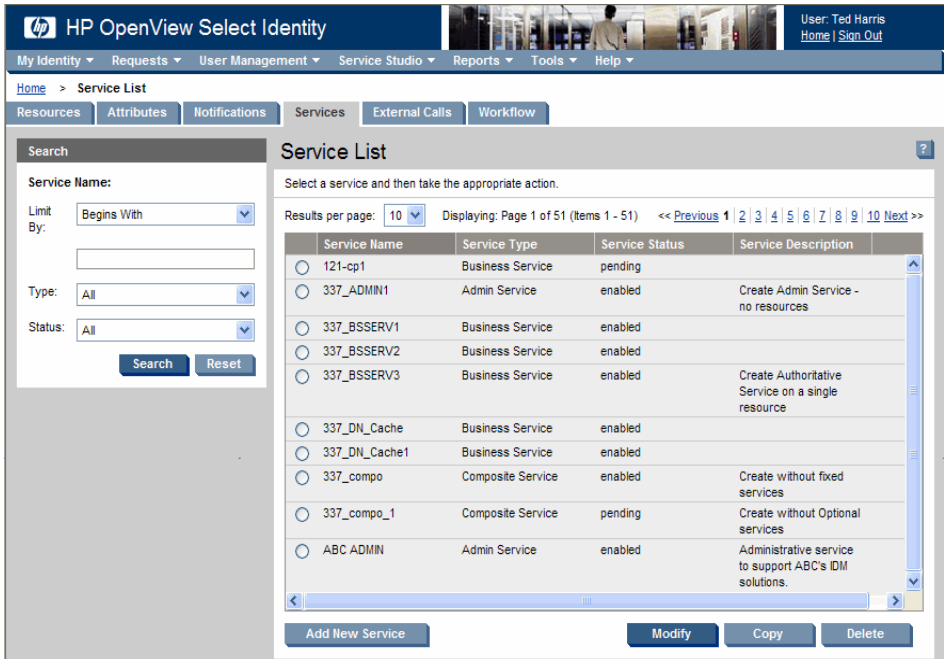
When possible, it is recommended that you use constraints when configuring the Service attribute values. By using constraints, you may improve performance within Select Identity. See Adding a New Attribute on page 104 for details.

Adding Business and Admin Services

Complete the following steps to add a Service:

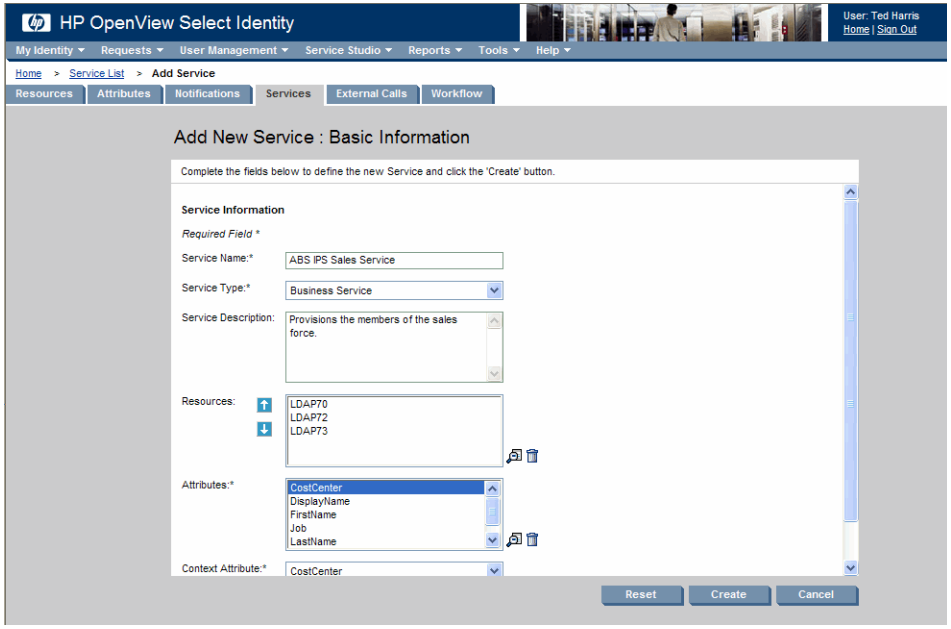
1 Select **Service Studio** → **Services** from the menu bar.
The **Service List** page opens.

Figure 75 Service List



2 Click **Add Service**.
The **Add New Service: Basic Information** page opens.

Figure 76 Add New Service: Basic Information Page



3 Tab from field to field and enter the correct information.

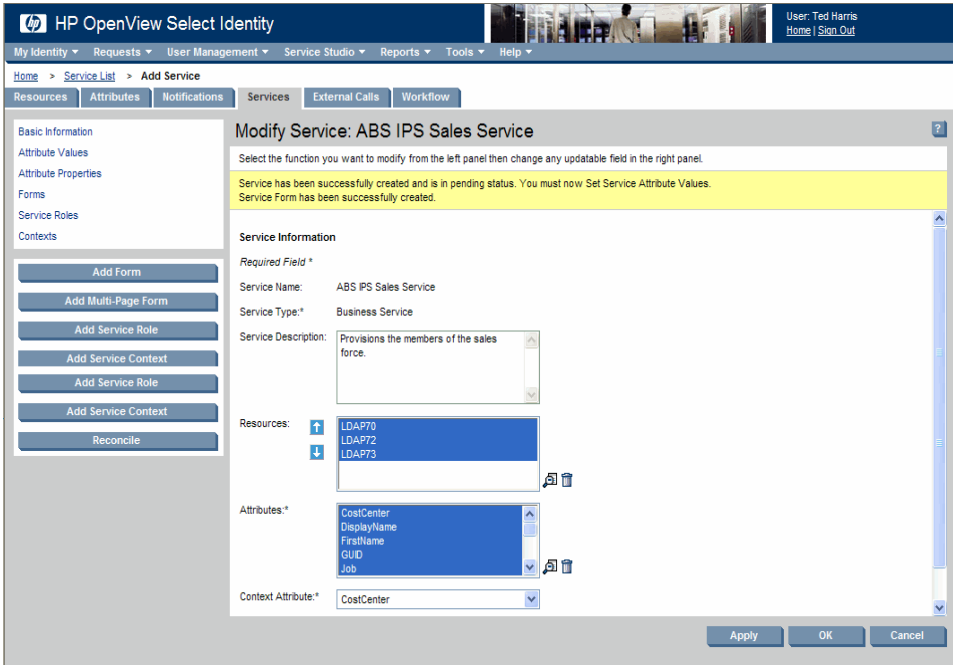
Field	Action
Service Name	Enter the name of the new service.
Service Type	Select the correct type of service from the drop-down menu. **Business Service** – a standard Service offered to customers and partners. **Admin Service** – a Service that assigns administrative roles to users for management purposes.
Service Description	Type a brief description of the service.
Resources	Click  to locate and add resources to support the Service. Add multiple resources at one time from the Search Results page.

Field	Action
Attributes	Click  to locate and add attributes to support the service. Add multiple attributes at one time from the Search Results page.
Context Attribute	Select the attribute you want to define the context, or logical grouping, for users of the Service. For example, if you want to group users by their location, use the “Country” attribute and users will be grouped by the value, such as “USA,” “India,” or “France.”
Primary User Key	Select an attribute from the Primary User Key drop-down list. This attribute establishes the default search criteria for users of this Service. For example, if you choose “Email,” you can search user accounts based on email values.

4 Determine which order you want the resources provisioned, then use the  and  arrows to change the resources into provision order.

5 Click **Create**.
Creates the Service and opens the **Modify Service: Service Name** page.

Figure 77 Modify Service: Service Name Page



6 Click **Basic Information** link in left panel of the page.

7 Review the Service you just created to make sure that it is correct.

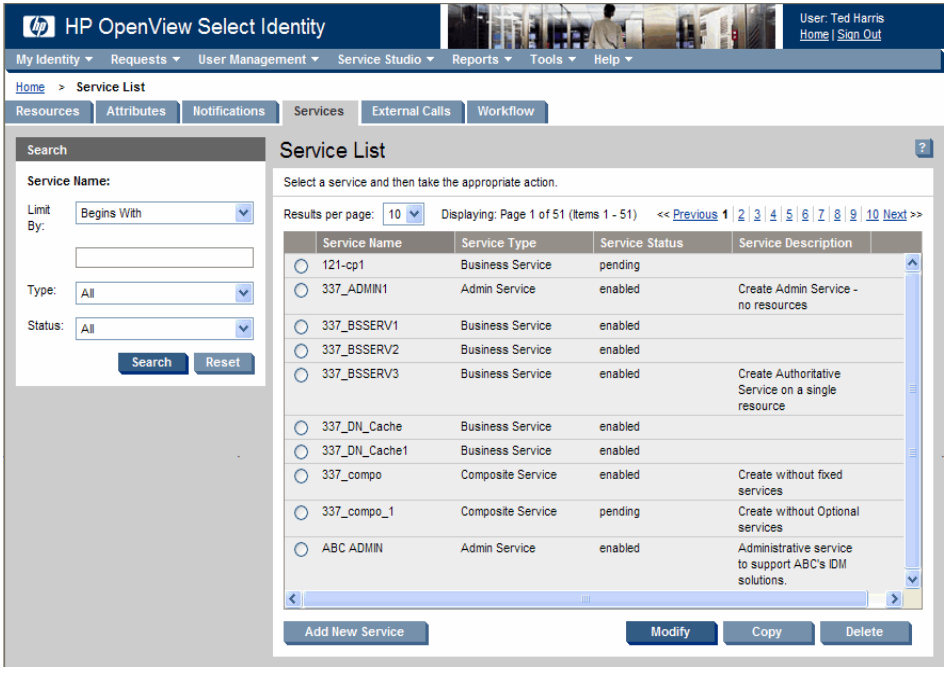
8 Continue to Setting Service Attribute Values and Properties on page 158.

Adding Composite Services

Create Composite Services to simplify maintenance by allowing you to update common attributes from one request. Composite Services combine two or more similar services into one composite service unit. Most Composite Services contain an Admin Service and at least one Business Service. Complete the following steps to add a Composite Service:

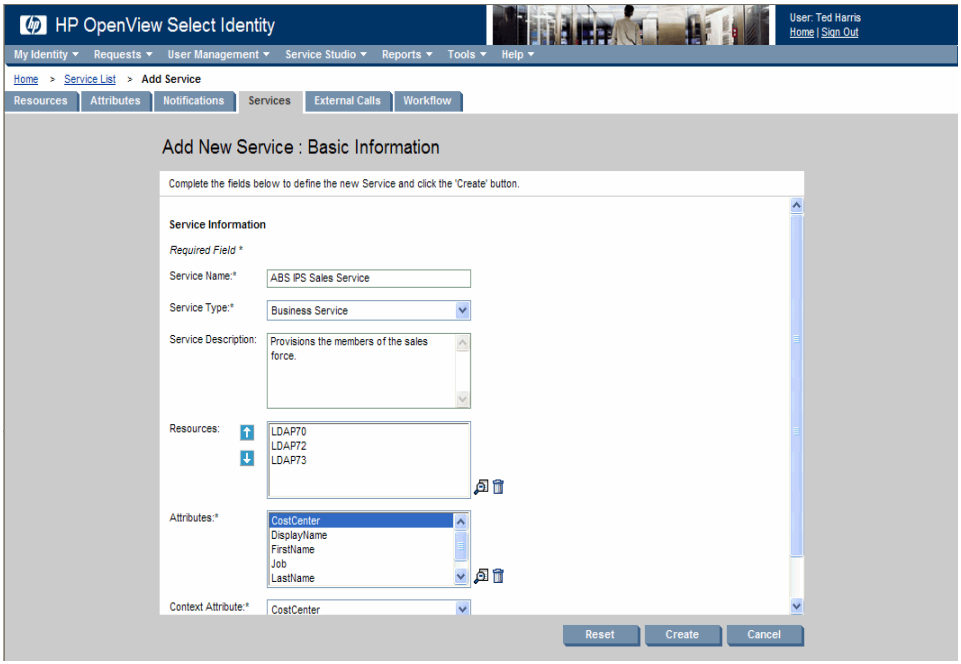
1 Select **Service Studio** → **Services** from the menu bar.
The **Service List** page opens.

Figure 78 Service List Page



2 Click **Add Service**.
The **Add New Service: Basic Information** page opens.

Figure 79 Add New Service: Basic Information Page



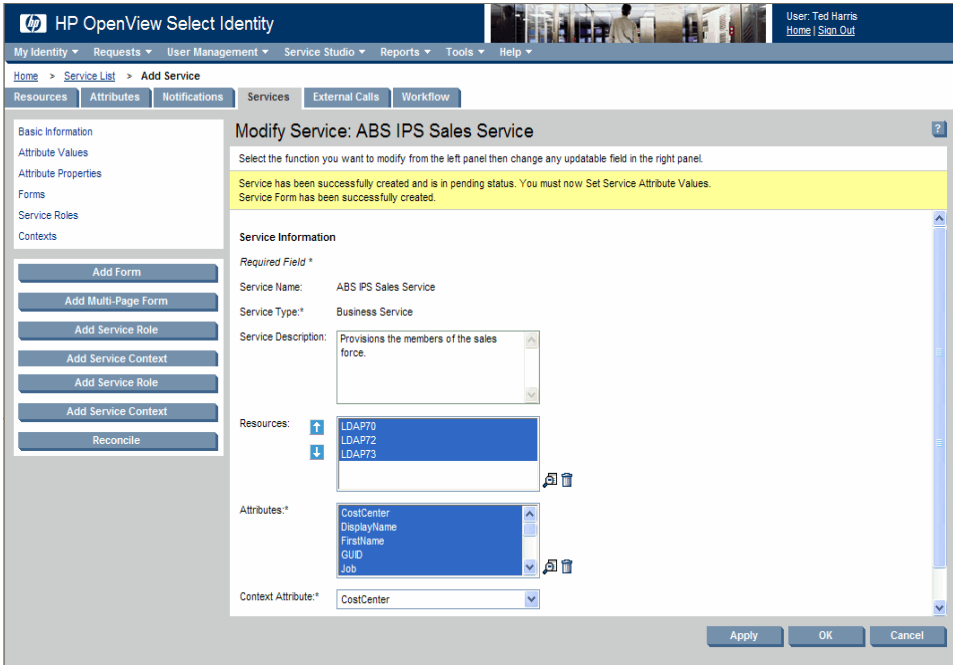
3 Tab from field to field and enter the correct information.

Field	Action
Service Name	Enter the name of the new service.
Service Type	Select Composite Service
Service Description	Type a brief description of the service.
Fixed Services	Click to locate and add services that must be updated together.
Optional Services	Click to locate and add services that may be updated together if the updated attributes are the same.
Attributes	Select the attributes that the services have in common.
Context Attribute	Select the user group context.

Field	Action
Attributes	Click  to locate and add attributes to support the service. Add multiple attributes at one time from the Search Results page.
Context Attribute	Select the attribute you want to define the context, or logical grouping, for users of the Service. For example, if you want to group users by their location, use the “Country” attribute and users will be grouped by the value, such as “USA,” “India,” or “France.”
Primary User Key	Select an attribute from the Primary User Key drop-down list. This attribute establishes the default search criteria for users of this Service. For example, if you choose “Email,” you can search user accounts based on email values.

4 Click **Create**.
Creates the Service and opens the **Modify Service: Service Name**.

Figure 80 Modify Service: Service Name for a Newly Created Service



5 Click the **Basic Information** link in left panel of the page.

6 Review the Composite Service you just created to make sure that it is correct.

7 Continue to Setting Service Attribute Values and Properties on page 158.

Setting Service Attribute Values and Properties

Restrict the values that a user selects from when registering for a Service. It is recommended that you do this to improve performance, especially if there are a large number of values. For example, you may have the attribute “Country” available and want to restrict value options to “USA,” “Korea,” and “Japan” for a particular Service.

This section covers the following:

- Understanding Service Attributes
- Setting Service Attribute Values

- Setting Service Attribute Properties

Understanding Service Attributes

Define a set of attributes and values that are available for or required by a Service. Attributes are created and managed through the Attributes pages. The attributes that are available for a Service are determined, in part, by the resources that are selected to support it. Additional attributes that are specific to the OVSI system or your business may also be available. Attributes and values that are defined specifically for a Service create a superset for Service Role and context creation.

The following attributes are required when you add a new user through any Service:

UserName
FirstName
LastName
Email
Password

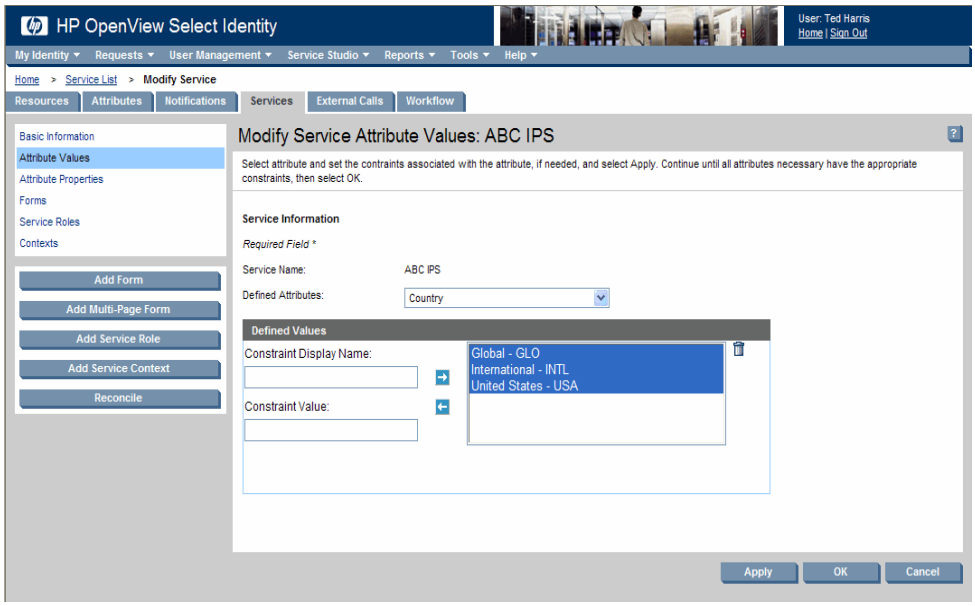
Setting Service Attribute Values

Perform the following steps to set Service attribute values:

1 Click the **Attribute Values** link in the left panel of the page.
The **Attribute Values** page opens.

2 Select the attribute you want to map from the **Defined Attributes** field.
Shows the **Defined Values** fields

Figure 81 Attribute Values



3 Enter the constraint name in the **Constraint Display Name** field.
Opens the appropriate **Constraint Display Name** fields.

4 Tab to the **Defined Attributes** field and enter the corresponding value you will use to validate correct entries.
Displays constraints in the **Displayed Values** panel.

5 Enter the name of the attribute value constraint in the Constraint Display Name field

6 Tab to the **Constraint Valu**e field and enter an acceptable value.

7 Click the  icon to enter the constraint into the right text list box.

8 Repeat the process from step 7 until all possible attribute value are entered.

9 Click **Apply**.
Saves your work.

10 Repeat the process until service attribute constraints are recorded.

Edit a constraint by selecting the item from the text box then selecting the  icon to move it to the edit fields. Make the necessary changes and click the  icon to return the item.

Setting Service Attribute Properties

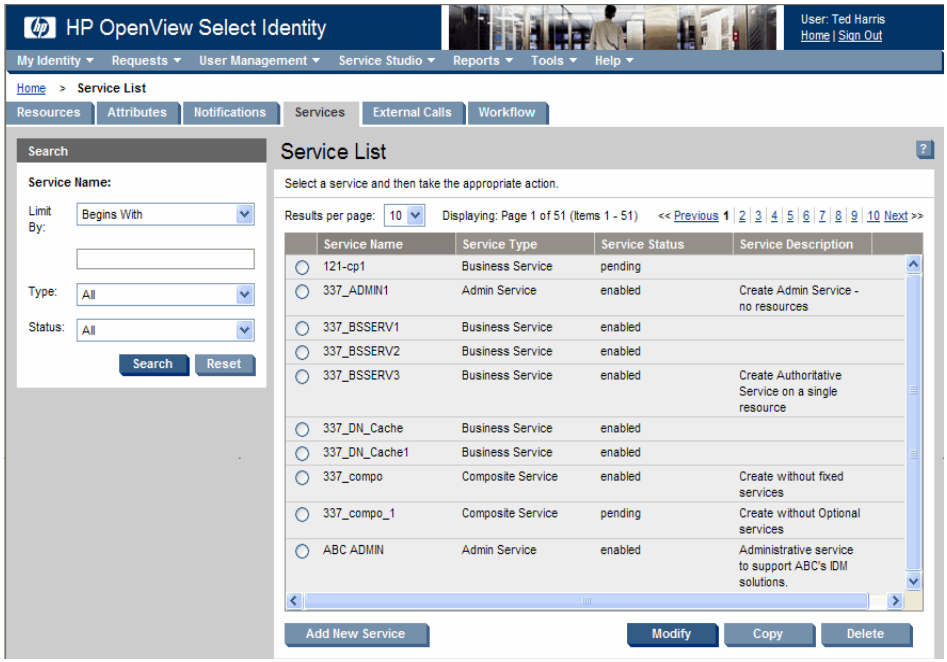
Use this page to map attributes to your new service. These properties define the fields that will display for users when maintaining their accounts using the self service function My Identity. This task also enables you to order the processing of attributes.

Note that this page is used to map multiple attributes to one new service and not to map one new attribute to multiple services. Use the Add Attributes (**Service Studio** →**Attributes** → **Add Attributes**) page to add a single attribute to multiple services.

Perform the following steps to set attributes properties for a Service:

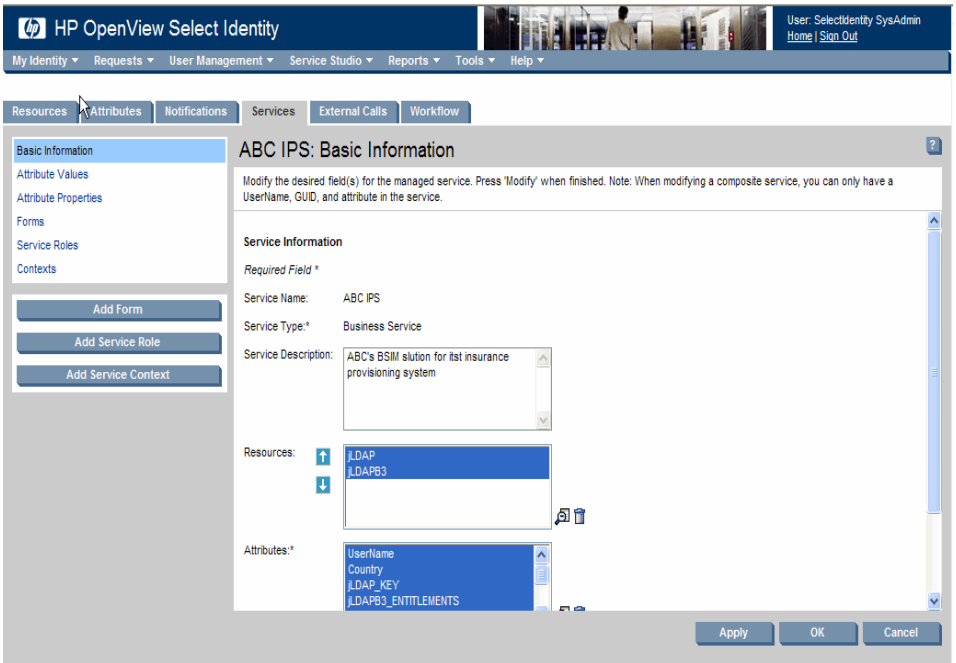
1 Select **Service Studio** → **Services** from the menu bar.
The **Service List** page opens.

Figure 82 Service List



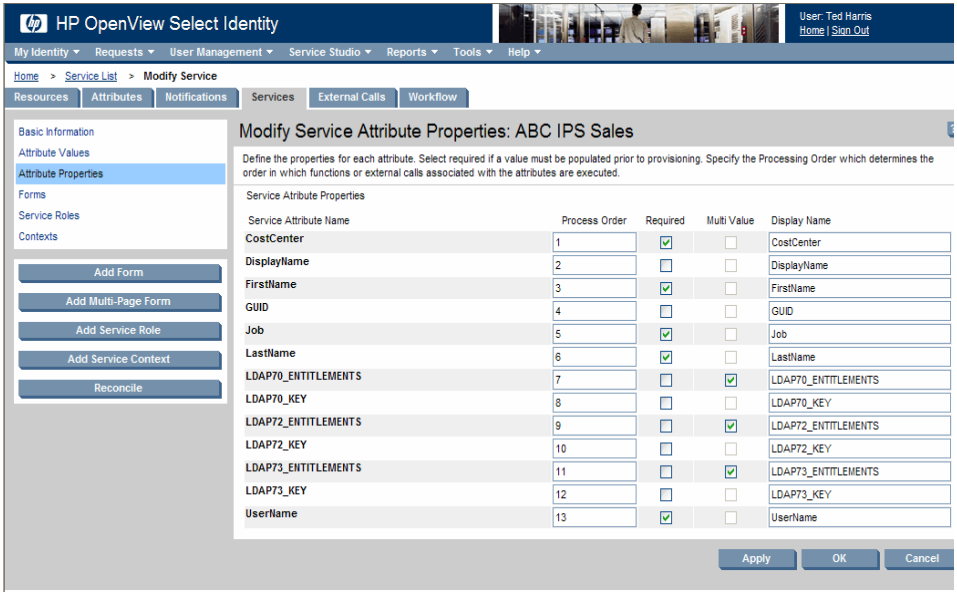
2 Select the service and click **Modify**.
The **Modify Service: Service Name** page opens.

Figure 83 Modify Service: Service Name Page



3 Click the **Attribute Properties** link in the left panel of the page. The **Modify Service Attribute Properties: Service Name** page opens.

Figure 84 Modify Service Attribute Properties: Service Name



4 Tab from field to field to enter the necessary information:

Field	Action
Service Attribute Name	Review the service attribute name (read only field).
Process Order	Enter a number indicating the sequence that you want the fields to be processed. he order defined here establishes the default order for any views created for this Service. It also determines the order in which attribute value generation functions are processed, if present.

Field	Action
Required	Click the check box to indicate the field is required. Attributes that are required by a Service must be present for user accounts that are added to Select Identity through the Reconciliation function and for any other assignment to this Service. If an account does not have a required attribute, it cannot access the Service
Multi Value	Click the check box to indicate the field has multiple correct values. Field will be restricted to only one value when this check box is left blank.
Display Name	Edit the name that is displayed to users in the Display Name fields.

5 Click **Apply**.
Saves your settings.

Working with Service Forms

After you create a Service, create forms that are valid for different groups of users. For example, if you want a specific set of users to see only certain fields when registering for the Service, define a form that makes only those fields available.

You can also use these forms to determine what information approvers see when requests are processed through workflow steps. Each approval block within a workflow can have a different Service form associated with it. See Adding a Service Role on page 169 for information on configuring forms for workflow approval blocks.

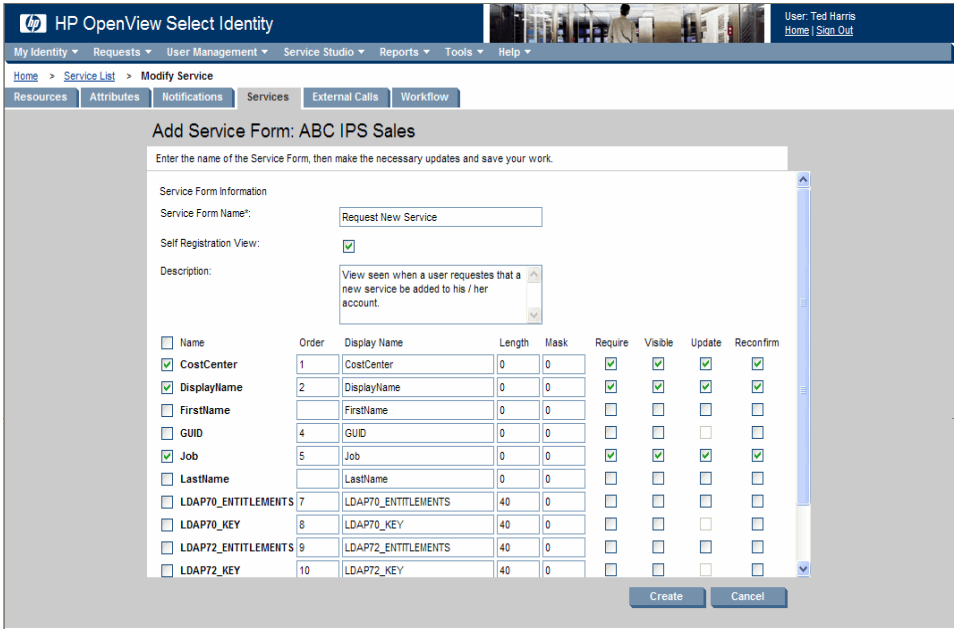
Additionally, Service forms can be used to create a multi-page form. A multi-page form can be used in delegated user management, self service, self registration, and the approval pages to determine what users see for each action. The display of these forms must be ordered accordingly.

Creating a Single Page Service Form

Complete the following steps to create a service form:

1 Click the **Add Form** button in the left panel.
Opens the **Add Service Form: Service Name** page.

Figure 85 Add Service Form: Service Name



2 Tab from field to field and enter the required information.

Field	Action
Service Form Name	Type the complete name of the service.
Self Registration View	Indicates this form may be seen during self registration.
Description	Enter a brief description of the form.
Name	Review the field name and insert a check in the check box if you want this field displayed on the page.

Field	Action
Order	Enter a number corresponding with the order that you want the field displayed on the form. For example if you enter 1 beside the LastName field then LastName would display first.
Display Name	Edit the name that is displayed to users in the Display Name fields.
Length	Define or change the maximum length of each value in the Length column.
Mask	Enter that number of characters you want hidden in the Mask column, if you want all or a portion of the value masked.
Required	Click on the check box to indicate the field is required. Attributes that are required by a Service must be present for user accounts that are added to OVSI through the Reconciliation capability and for any other assignment to this Service. If an account does not have a required attribute, it cannot access the Service
Visible	Select the check box if you want this field to be visible on the registration page. Fields that are required must be visible.
Update	Click this check box to give users permission to update a field value. Fields that are required must be updatable.
Reconfirm	Select the check box if you want the user to reconfirm a value for validation purposes.

3 Click **Create**.
Saves your work and return to the **Modify Service Form: Service Name** page. The new form can now be found in the **Service Form Name** menu.

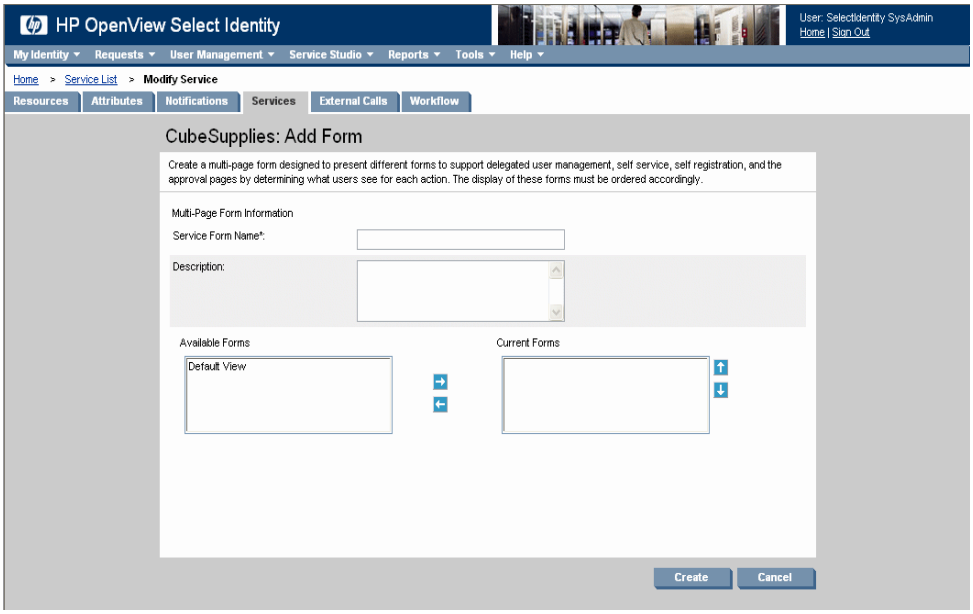
4 Repeat the process to create as many forms as necessary to meet your individual user group needs.

Creating a Multi Page Form

Complete the following steps to create a service form:

1 Click the **Add Multi-Page Form** button in the left panel.
Opens the **Service Name: Add Form** page.

Figure 86 Service Name: Add Form



2 Tab from field to field to enter the required information.

Field	Action
Service Form Name	Type a descriptive name.
Self Registration View	Indicates this form may be seen during self registration.

3 Review the list of forms available for your use in the **Available Forms** text box.

4 Select the each form you want to add to the form by clicking the  icon to enter the constraint into the **Current Forms** text box

5 Order the forms into the sequence each will be viewed by the user using the  and  arrows.

6 Click **Create**.

Defining Service Roles

Services are made available by creating a Service Role, which defines the entitlements, workflows, and policies that will be used to access the Service. Context enables you to assign a Service Role to a group of users with a common attribute, thus providing access to the Service under the terms you established.

Defining a Service Roles enables you to assign granular rights, or levels of Service, to your customers and partners. It is similar to a Platinum or Gold membership in a club.

Service Roles enable you to map an event to a workflow template that contains approval blocks. For each of these blocks you have the option of defining a different Service form to be used in that block. The initial delegated or self add/modify form will always use the default form defined, but any views defined in the block form are used in place of the default form for that block only. This enables you to define specific views for workflow approvers.

The Service deployment defines a superset of attributes that can be assigned to Service Roles. For example, if a Service is defined to require a three-stage approval process for new account registration, an administrator defining Service Roles for this Service must choose a subset of those approval processes.

The following procedures enable you to set and form Service Roles and define a context for each of your Services.

Adding a Service Role

Service Roles are hierarchical in terms of management and create a secure way to share Services across different companies or locations. Service Role settings take precedence over the Service configuration.

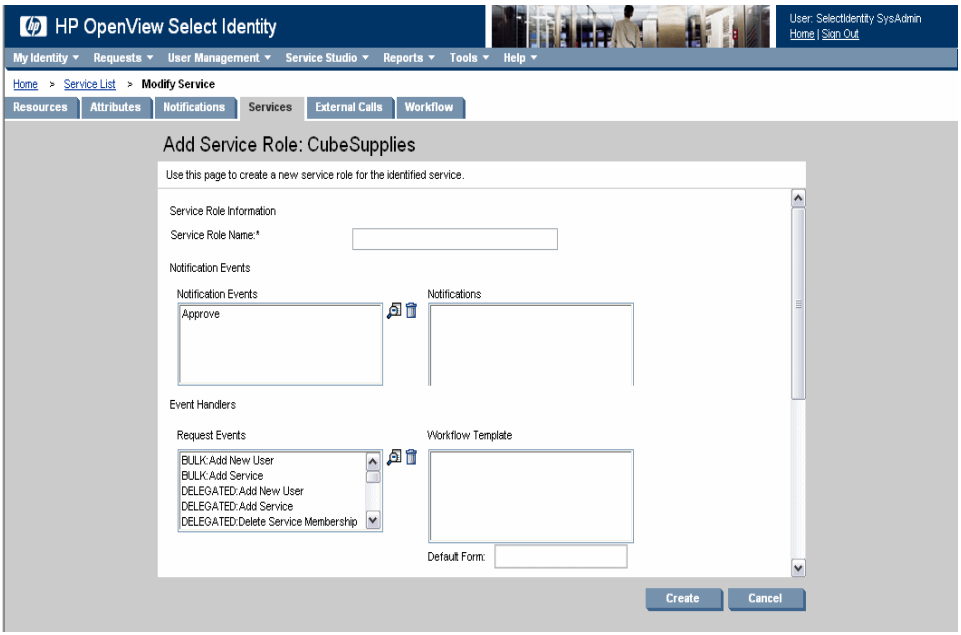
If this is the first Service Role that you are creating for this Service, you will not see the parent option.

The first Service Role that you create for each service defines the superset of options (parent) for all other Service Roles created for this service. In the Service Information Page, all the events and templates are populated by default for the first Service Role. Simply select and delete the events and templates you do not want to use.

Perform the following steps to create a Service Role:

1 Click the **Add Service Role**.
Opens the **Add New Service Role** page

Figure 87 Service Name: Add New Service Roles



2 Enter a unique name of the service role you are creating in the **Service Role Name** field.

If	Then
This is the first or parent service role	Continue. Displays the event fields.
This is an additional service role	Tab to the **Service Role** parent field and click  to locate and select the correct parent service role record. Displays the event fields. The Service Role Information page is populated with options determined by the parent selection.

3 Tab from field to field to enter the rest of the information:.

Field	Action
Service Role Name	Enter a unique name of the service role you are creating.
Notification Events	Click  to locate and add notification events to support the Service Role.
Notifications	Click the event listed in the **Notification Event** text box to see the Notification templates associated with the event. See Notification Variables on page 124 for information about notification policies.
Request Events	Select  to locate and add request events to support the Service Role.
Workflow Template	Click the event listed in the **Request Event** text box to see the Workflow Template(s) associated. See Workflow Studio on page 273 for information about Workflow Templates.
Default Form	. If you do not specify a form, the Default form is selected

4 Select the fixed attributes assigned to users that you want enabled for this Service Role by tabbing from field to field and entering the necessary information.

You can select multiple attributes. See Setting Service Attribute Values on page 159 for information about attributes and values.

Field	Action
Fixed Attributes (Name)	Select an attribute name from the drop-down menu. This list is provided by the parent Service Role.
Fixed Attributes (Value)	Search for or enter a value in the field. If you are creating an administrative Service, this is where you select roles.

5 Click  to move the attribute and value to the entry table.

Field	Action
Optional Attributes (Name)	Select an attribute name from the drop-down menu. This list is provided by the parent Service Role.
Optional Attributes (Value)	Search for or enter a value in the field. If you are creating an administrative Service, this is where you select roles.

6 Click  to move the attribute and value to the entry table.

Delete an attribute by clicking the attribute you do not want and selecting the  icon. Move the constraint from the text box by clicking on the constraint and then selecting the  icon and edit as appropriate. Enter your change by clicking  .

7 Click **Create**.
The Service Role is now active. However, the Service remains in a Pending state until the Context user group is defined.

Understand Event References

The following tables list the request events to which you can assign a workflow template when creating Service Roles:

Delegated-registration Request Events

- Adding a user
- Adding a service to a user
- Deleting a service membership
- Disabling a service membership
- Enabling a service membership
- Modifying a user
- Viewing a service membership

Reconciliation Request Events

- Adding a service to a user
- Deleting a service membership

Self-service Request Events

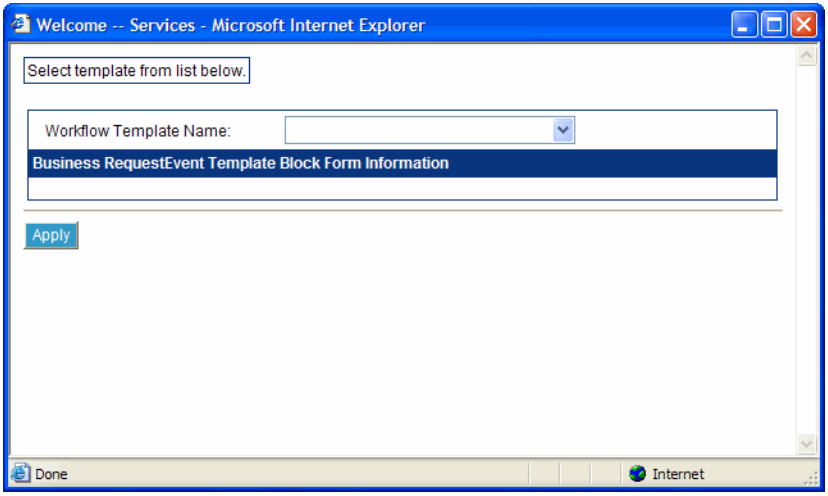
- Adding a user
- Adding a service to a user
- Modifying a profile

Creating a Multi-page Form

View a Service at the approval block level by completing the steps that follow;

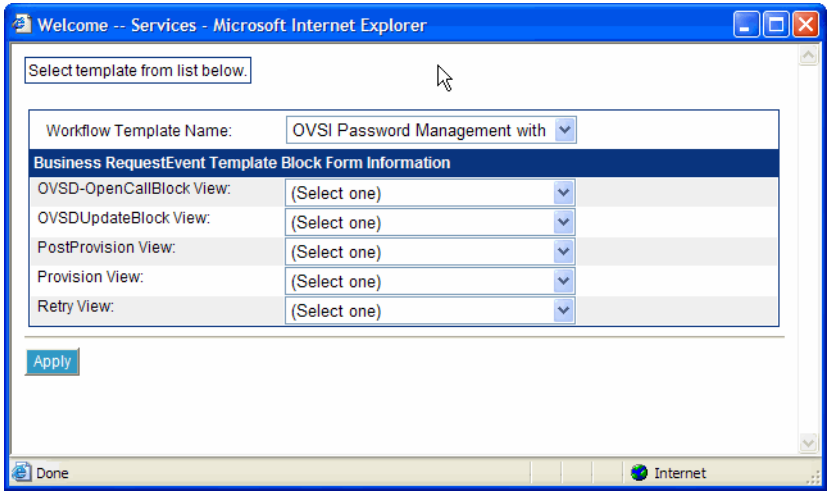
1. Click the **Request Event** you want to reference.
2. Select the associated workflow from the **Workflow Process** list.
3. Click the  icon to search for the correct work flow.
   Opens the **Welcome Services** dialog box.

Figure 88 Welcome Services



4 Select the Workflow you want to view from the drop-down menu in the **Workflow Template Name** field.
Displays the list of template blocks that can be associated with the form.

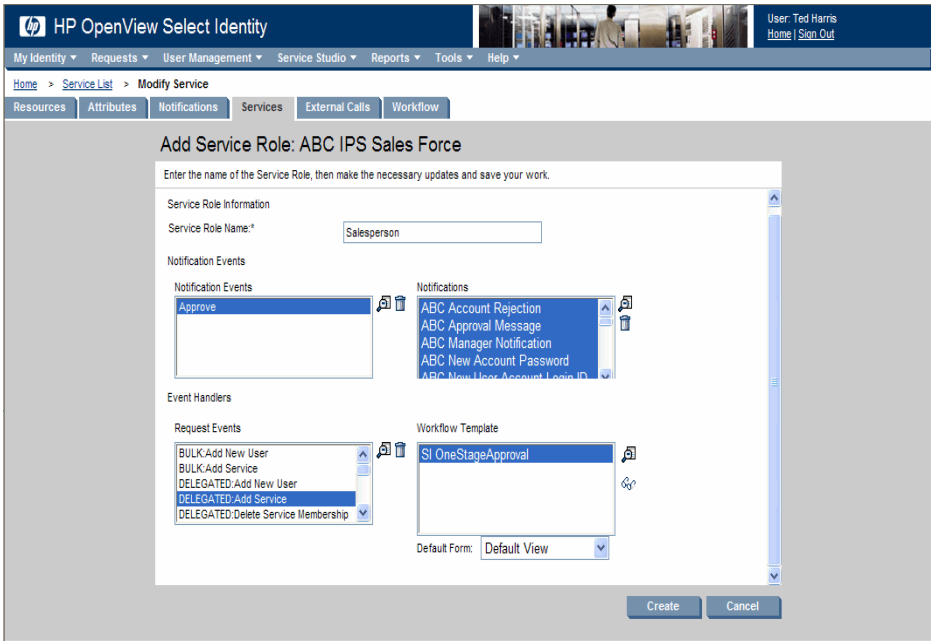
Figure 89 Welcome Services



5 Tab from block to block and select the appropriate form from the drop-down menu being sure to skip those blocks that need not have a form assigned.

6 Click **Apply**.
Returns to the original page.

Figure 90 Add Service Role Page



Creating Context User Groups

Context enables you to assign a Service Role to a group of users based on a common attribute. Managing Context instead of users saves you time by allowing you to place a user in a Context user group. OVSI propagates Service(s) and Resource assignments based on a standardized model created and customized to fit the needs of your organization during the reconciliation process. Learn more about reconciliation in Understanding Reconciliation Rules on page 403.

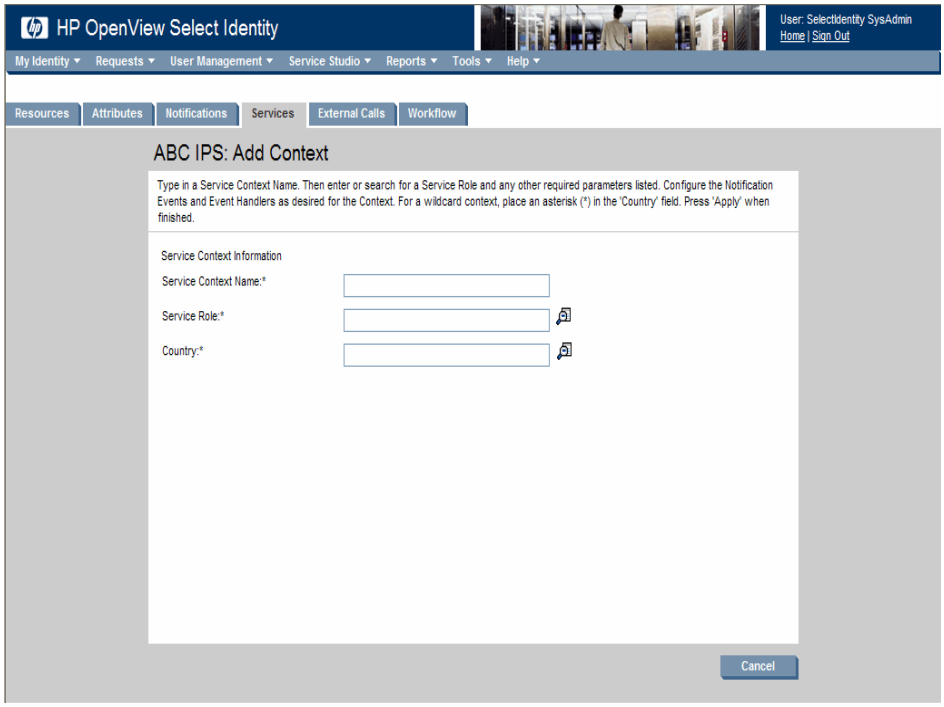
Creating Context

Context enables you to assign a Service Role to a group of users based on a common attribute, thus providing access to the Service.

Perform the following steps to set context for a Service Role:

1 Click the **Add Service Context**.
The **Add Context** page opens.

Figure 91 Add Context Page



2 Tab from field to field to enter the information necessary to define the Context.

Field	Action
Service Context Name	Click  to search for and select a parent context if one is available. If this is the first Context record created, you will not have a parent option. The parent provides a superset of attributes, workflow processes, and policies that you can choose from once it is available.
Service Role	Click  to locate the correct the Parent Service Role. Displays additional fields. The parent Service Role provides a superset of attributes, workflow processes, and policies that you can choose from when available.

3 Tab from field to field to complete the Context user group definition.

Field	Action
Service Context Name	Click  to search for and select a value for the context attribute that you defined when creating the service.
Service Role	Click  to search for and select a value for the service role that you defined when creating the service.
<Context>	Click  to search for and select a value for the context attribute constraint.
Notification Events	Click  to locate and add notification events to support the Service Role.

Field	Action
Notifications	Click on the event listed in the **Notification Event** text box, then click  to select the Notification policy templates you want associated with the event. See Notification Variables on page 124 for information about notification policies.
Request Events	Select  to locate and add request events to support the Service Role. See Notification Variables on page 124 for a list of events and actions within OVSI
Workflow Template	Click on the event listed in the **Request Event** text box, then click  to select the Workflow template(s) you want associated with the event. See Workflow Studio on page 273 for information about Workflow Templates.

4 Click **Apply**
Creates the Context and enables the service.

5 Repeat the process until all the Context user groups are defined.

Managing Services

Once your services are created they must be managed. Modifying a Service enables you to add, delete, or change the order of provisioning resources on which the Service relies. You can also add and delete the attributes that help define the Service.

This section covers the following:

- Copying a Service
- Modifying a Service
- Modifying Service Attribute Values

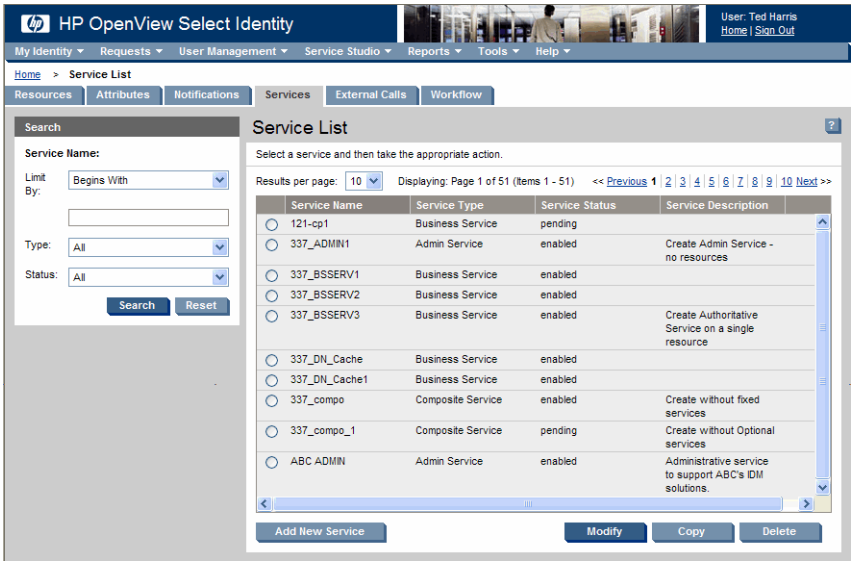
Copying a Service

When you want to create a service that is very similar to an existing service, copy the existing service. Once the service has been copied under a new name, then simply modify those part of the service that are different from the original

To copy a Service, perform the following steps:

1 Select **Service Studio** → **Services** from the menu bar.
The **Services List** page opens.

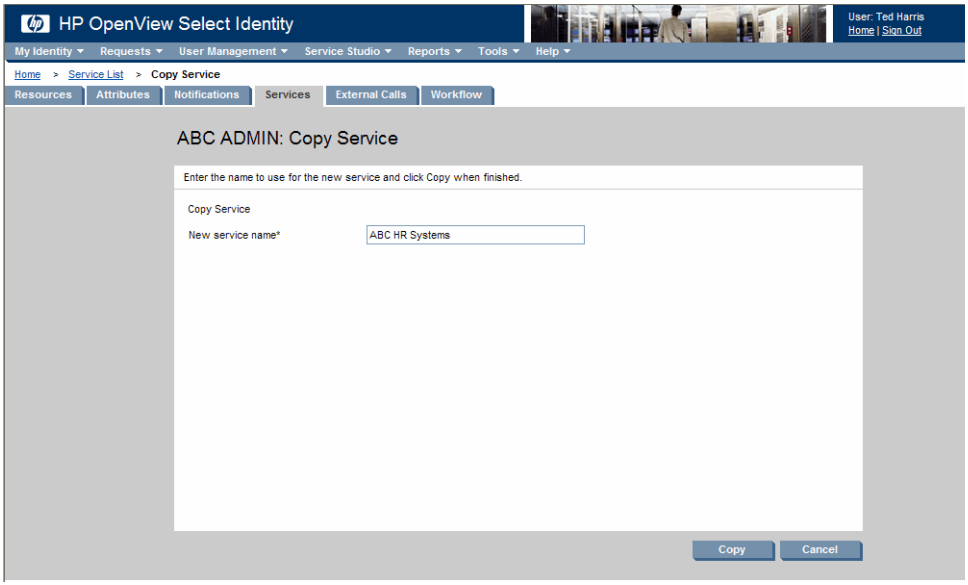
Figure 92 Service List



2 Select the Service you want to copy.

3 Click **Copy**.
The **Copy Service** page opens.

Figure 93 Service Name: Copy Service



4 Enter a unique name for this service in the **Service Name** field.

5 Click **Copy**.
Copies the selected service parameters into the newly created service and returns to the **Service List** page.

6 Review your newly created Service and make any modifications necessary.

Modifying a Service

Maintain services using the modify functionality. Make modifications to any part of any service as necessary. Make changes to Composite Services in order to make changes to many similar services connected by the composite relationship at one time.

This section covers the following.

- Modifying Service Information
- Modifying Service Attribute Properties
- Modifying a Service Form
- Deleting a Service Form

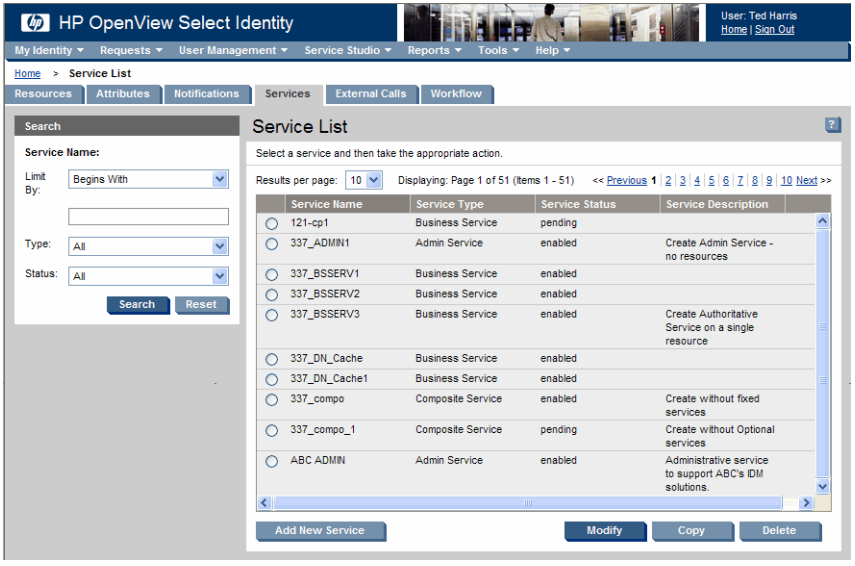
- Modifying a Service Role
- Deleting a Service Role
- Modifying a Service Role
- Deleting a Service Role
- Modifying Context
- Deleting Context

Modifying Service Information

To modify a service or the information that a user of the Service is required to provide at registration, perform the following steps:

1 Select **Service Studio** → **Service** from the menu bar.
The **Service List** page opens.

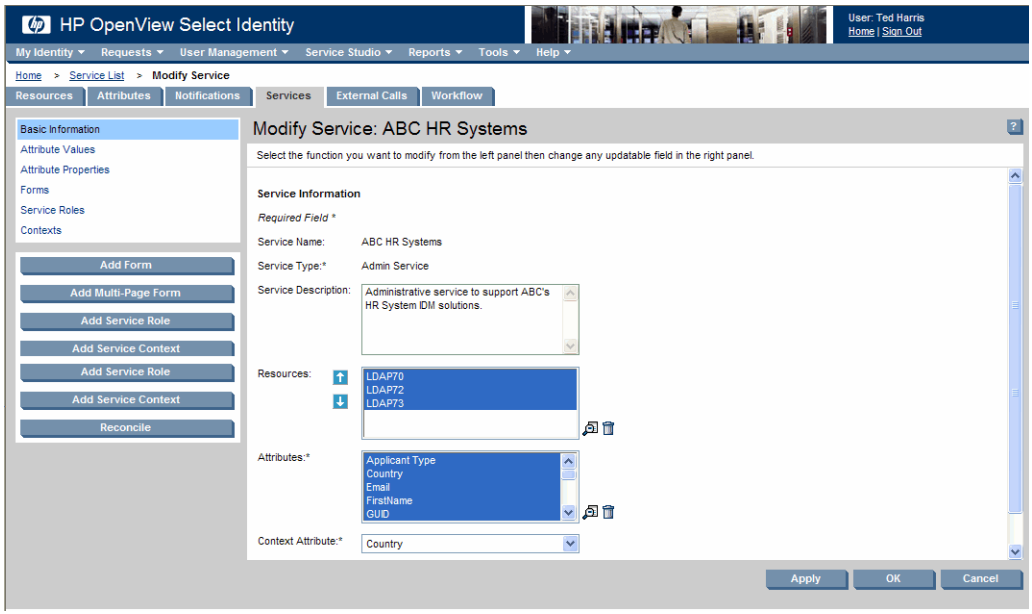
Figure 94 Service List Page



2 Select the service you want to modify.

3 Click **Modify**.
The **Modify Service: Service Name** page opens.

Figure 95 Modify Service: Service Name



4 Review the information in the **Service Description** field and edit the description of the service if necessary.

5 Review the list of resources in the **Resources** text box and determine whether changes should be made.

If	Then
You want to add a Resource	Click  to locate and add resources to the service.
You want to remove a resource from the list	Click on the constraint and then selecting the  icon.
You want to change the order in which resources are provisioned	Use the  and  arrows to change the order in which resources appear to change the provision order.
You want to leave the list the same	Continue.

6 Review the list of attributes in the **Attributes t**ext box, used to support this service and determine if revisions are necessary.

If	Then
You want to add an Attribute	Click  to locate and add resources to the service.
You want to remove an attributes from the list	Click on the constraint and then selecting the  icon.
You want to leave the list the same	Continue

7 Review the **Context Attribute** field and change the user group context if necessary.

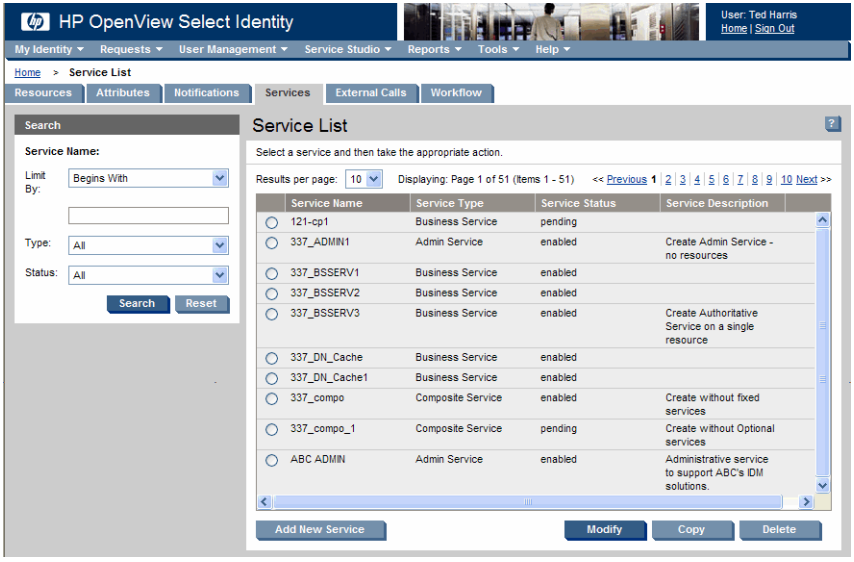
8 Verify that the **Primary Key User** is correct, if not select the appropriate user.

9 Click **Apply.**
Saves your changes

Modifying Service Attribute Values

1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

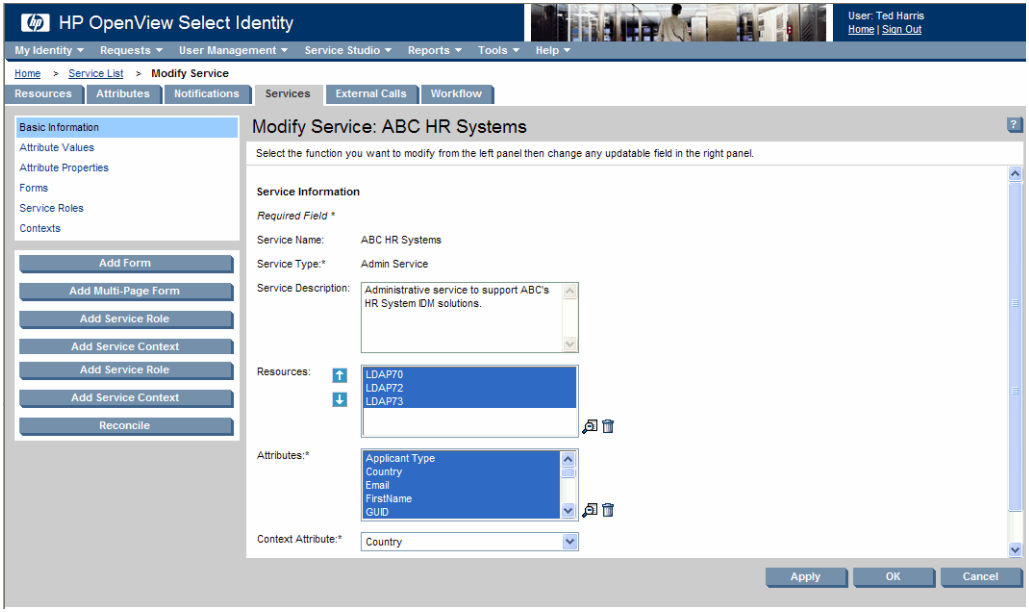
Figure 96 Service List



2 Select the service you want to modify.

3 Click **Modify**.
Opens the **Modify Service: Service Name** page

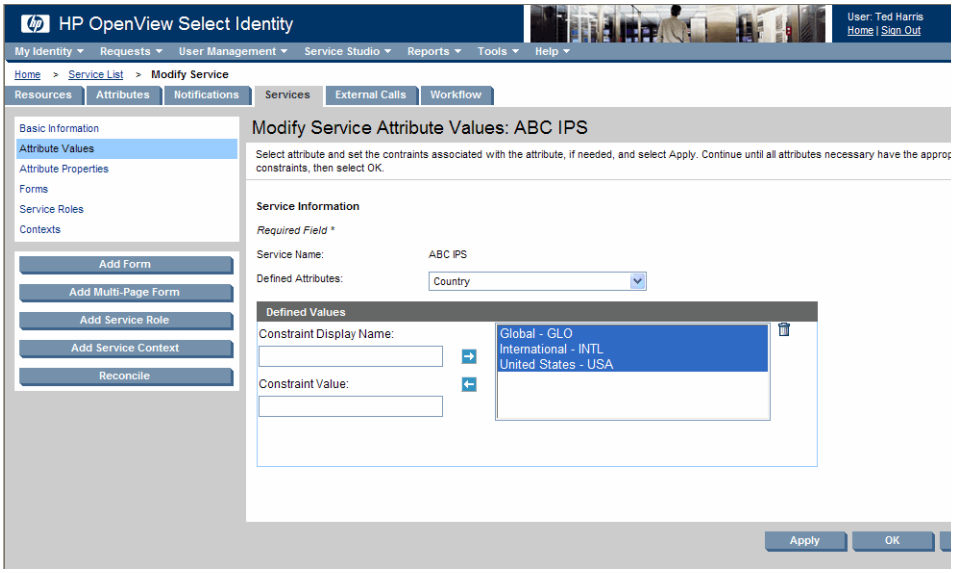
Figure 97 Modify Service: Service Name



4 Click the **Attribute Values** link in the left panel of the page.
Opens the **Modify Service Attribute Values: Service Name** page

5 Select the attribute you want to change from the **Defined Attributes** field.
Opens the **Defined Values** fields.

Figure 98 Modify Service Attribute Values: Service Name



6 Determine how you want to change the constraints.

If	Then
You want to add an attribute value	Continue
You want to remove an existing attribute value	Click on the constraint and then selecting the icon.
You want to edit an attribute value	Move the constraint from the text box by clicking on the constraint and then selecting the icon and edit as appropriate. Click the icon to enter the constraint into the right text box.

7 Enter the constraint name in the **Constraint Display Name** field.
Displays the appropriate **Constraint Display Name** fields.

8 Click **Apply**.
Saves your work.

9 Repeat the process until all attribute values and attribute value constraints are listed correctly.

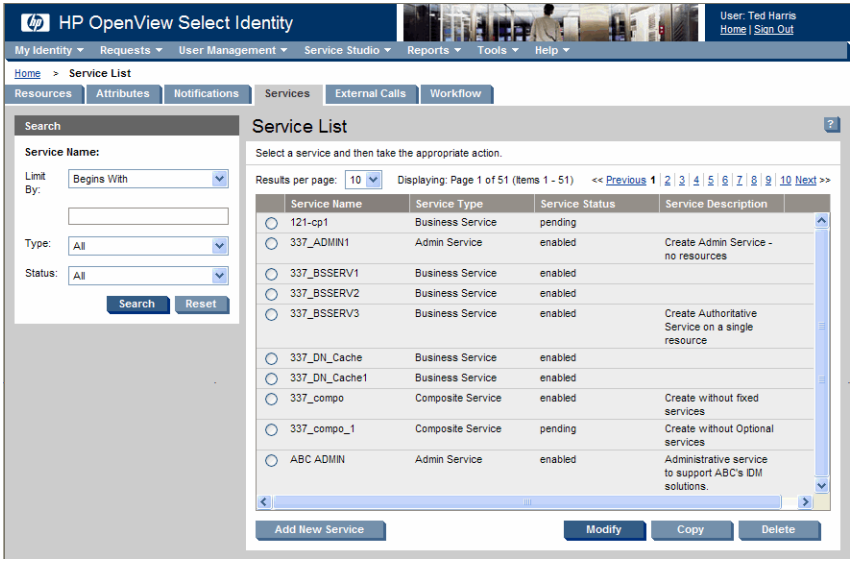
Modifying Service Attribute Properties

Modifying services attribute properties allows you to create a set of attributes or set properties that are specific for a Service. This task also enables you to order the processing of attributes and define the display names for each.

Perform the following steps to set attributes properties for a Service:

1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

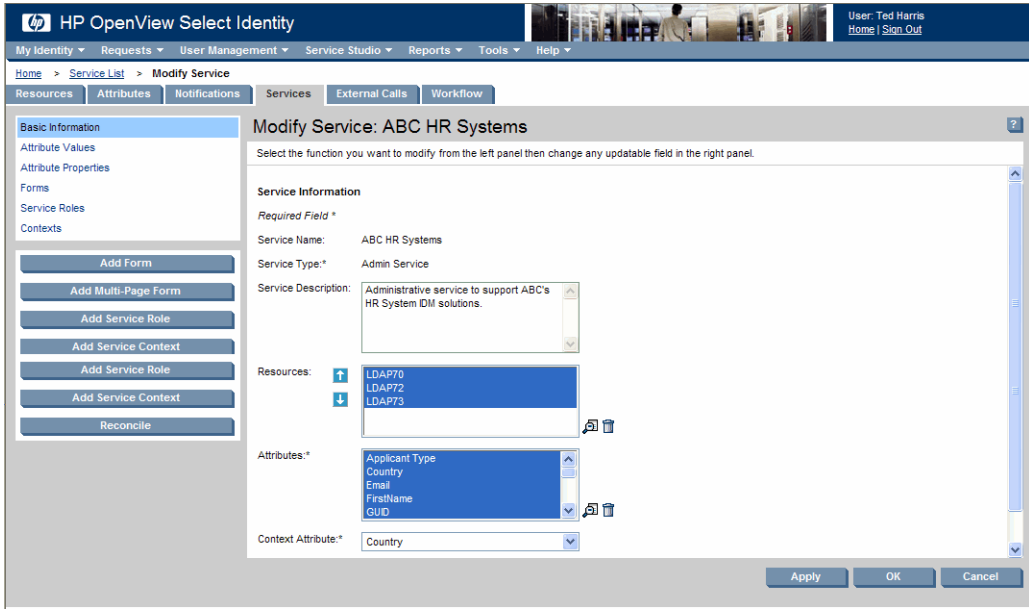
Figure 99 Service List



2 Select the service you want to modify.

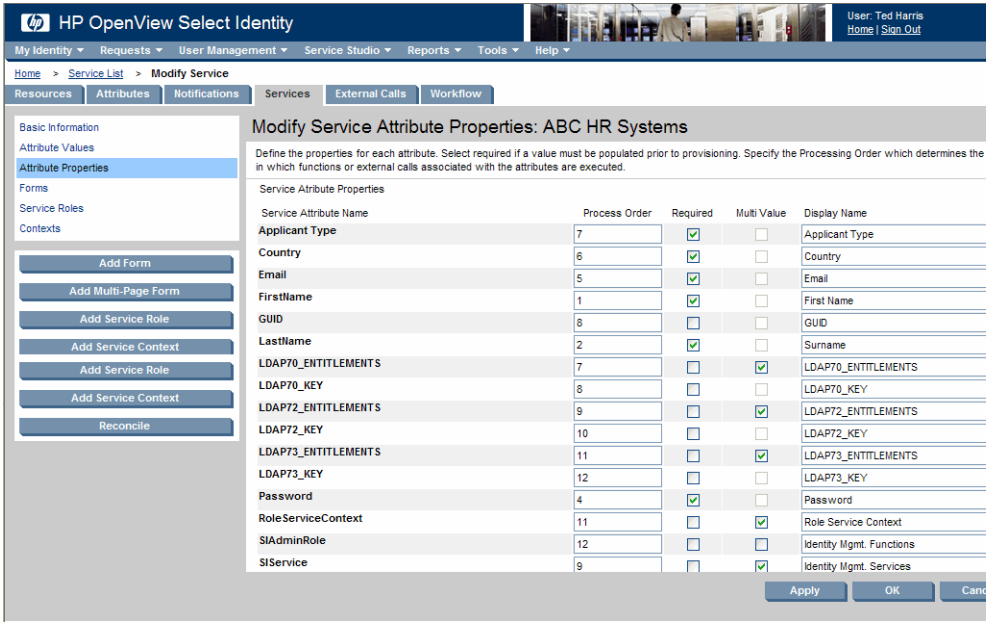
3 Click **Modify**.
Opens the **Basic Information** page.

Figure 100 Modify Service: Service Name



4 Click on the **Attribute Values** link in the left panel.
Opens the **Attribute Properties** page.

Figure 101 Service Name: Attribute Properties



5 Review the fields that display.

6 Make any changes necessary.

If	Then
You want to change the default order fields appear for any view created for this service	Order the fields in the order you want each field displayed by changing the numbers in the Order column. This order also determines the order in which attribute value generation functions are processed, if present.
You want to change the fields requirement status	Select the check boxes to the right of the fields that you want to change to add or remove a check in the **Required** column. Attributes that are required by a service must be present for user accounts that are added to OVSI through Reconciliation and for any other assignment to this Service. If an account does not have a required attribute, it cannot access the Service.
You want to change the Multi Value Selection	Select the check boxes to the right of the fields if you want to change, to add, or to remove a check in the **Multi-Value** column. No check means that the user is restricted to only one value.
You want to change the way field labels appear for users when they register for this service	Review the names listed in the **Display Names** column and make any changes necessary.

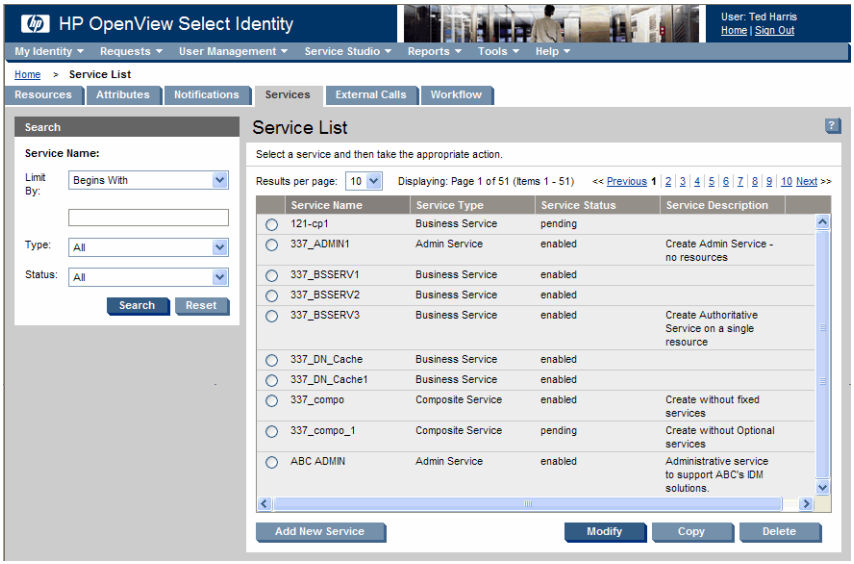
7 Click **Apply**.
Saves your work.

8 Click **OK**.
Returns to the **Service List** page.

Modifying a Service Form

1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

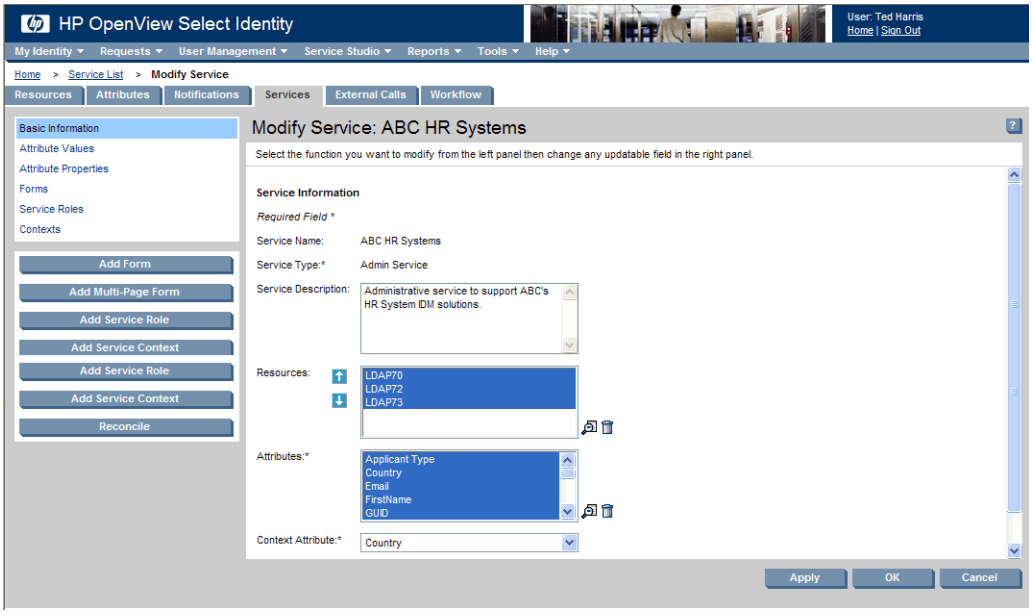
Figure 102Service List



2 Select the service you want to modify.

3 Click **Modify**.
Opens the **Modify Service: Service Name** page.

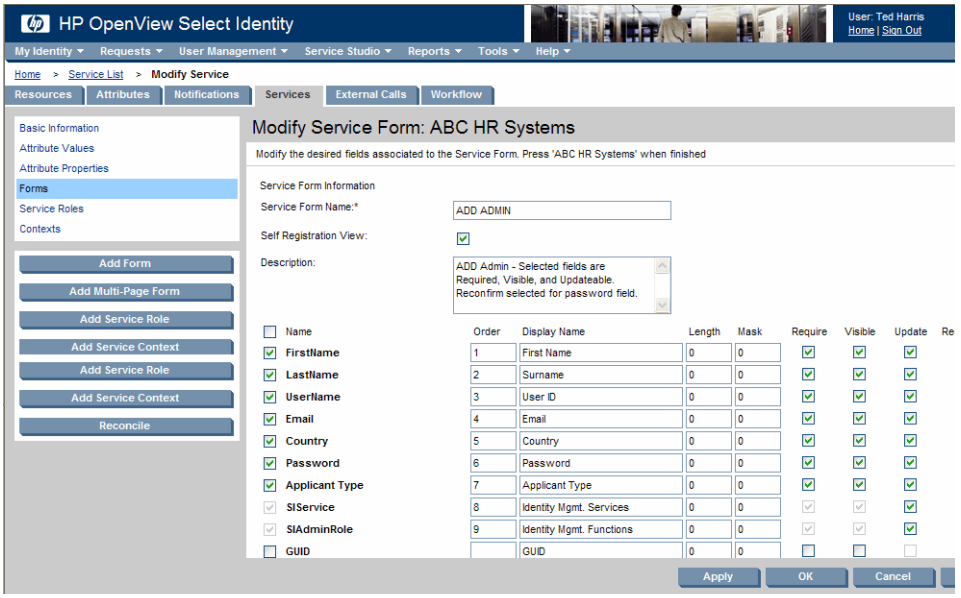
Figure 103 Modify Service: Service Name



4 Click on the **Forms** link in the left menu.
Opens the **Forms** page.

5 Select the form you want to modify from the **Service Form Name** field.
Opens the selected form.

Figure 104 Modify Service Form: Service Name



6 Review the fields that display.

7 Make any changes necessary.

Change	By
The name of the form	Click on the **Service Form Name** field and enter a new name.
Self Registration View	Indicate whether this form should be seen by users during self registration.
The description of the form	Click on the **Description** field and edit the description displayed.
The fields that display on the form	Select the check boxes to the right of the fields that you want to change to add or remove a check in the **Name** column.

Change	By
The order in which fields are displayed	Order the fields in the order you want each field displayed by changing the numbers in the Order column. The order defined here establishes the default order for any views created for this Service. It also determines the order in which attribute value generation functions are processed, if present.
The Display Name	Click on the **Display Name** field and edit the name as necessary.
The field length	Define or change the maximum length of each value in the **Length** column.
The masking properties	Indicate how many characters should be masked in order to protect the security of the input in the **Mask** column
The fields requirement status	Select the check boxes to the right of the fields that you want to change to add or remove a check in the **Required** column. Attributes that are required by a service must be present for user accounts that are added to Select Identity through the Reconciliation capability and for any other assignment to this Service. If an account does not have a required attribute, it cannot access the Service.

Change	By
The fields to be visible in the view	Select the check boxes to the right of the fields that you want to see on the form in the **Visible** column. No check means that the user is restricted to only one value.
The fields to update	Select the check boxes to the right of the fields that you want to be updateable on the form in the **Update** column.
The attributes to reconfirm	Select the check boxes to the right of the fields that you want to see entries reconfirmed in the **Reconfirm** column.

8 Click **Apply**.
Saves your work.

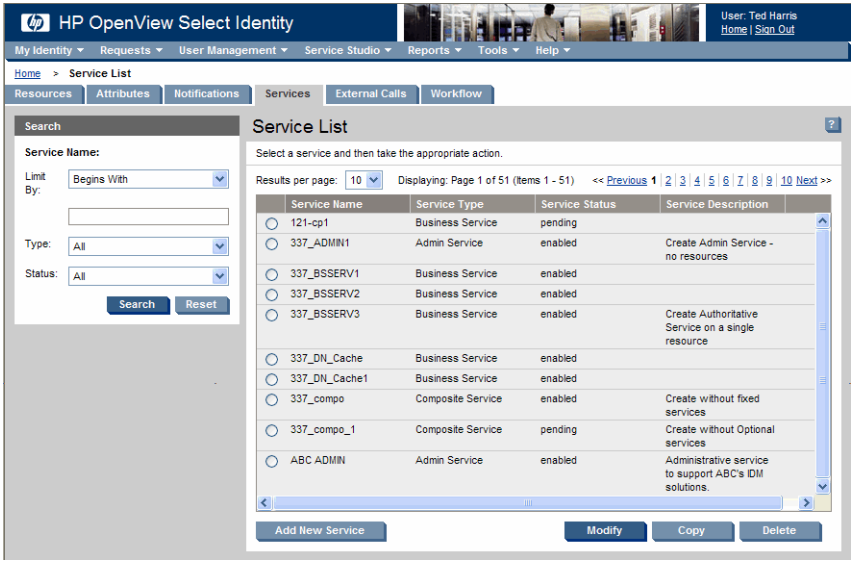
9 Click **OK**.
Returns to the **Service List** page.

Deleting a Service Form

Occasionally forms may become outdated and need to be removed from the Select Identity system. Follow the steps below to delete a form:

1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

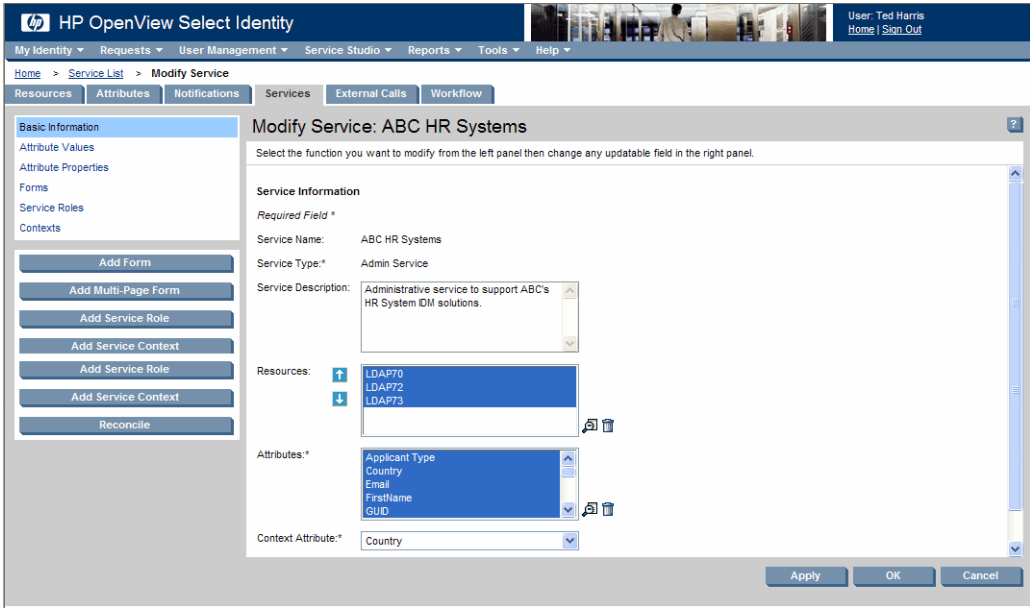
Figure 105Service List



2 Select the service you want to modify.

3 Click **Modify**.
Opens the **Modify Service: Service Name** page.

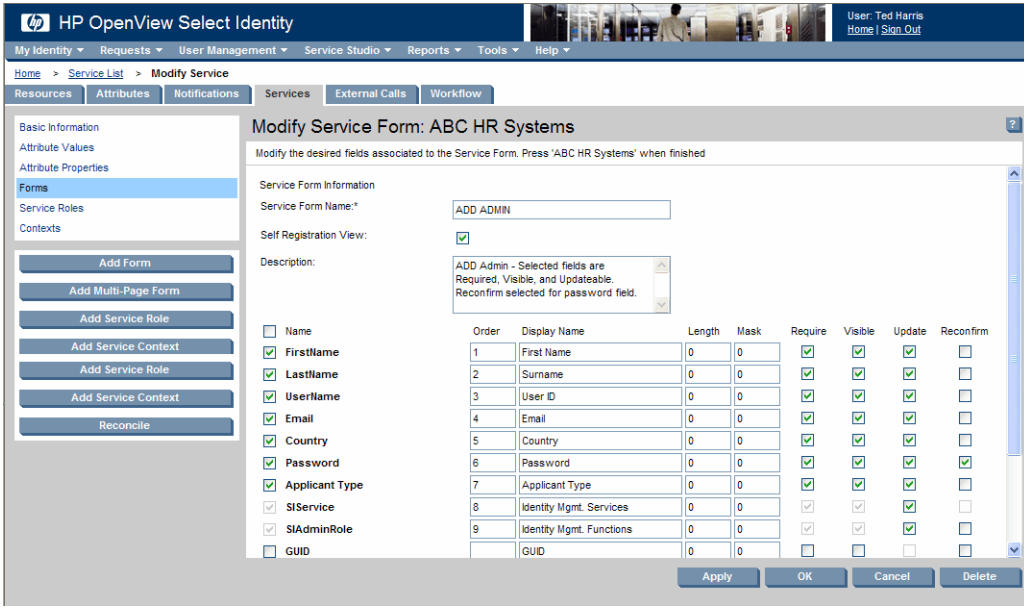
Figure 106 Modify Service: Service Name



4 Click the **Forms** link in the left menu.
Opens the **Forms** page.

5 Select the form you want to delete from the **Service Form Name** field.
Opens the selected form.

Figure 107 Modify Service Form: Service Name



6 Click **Delete**.
Opens the confirmation dialog box.

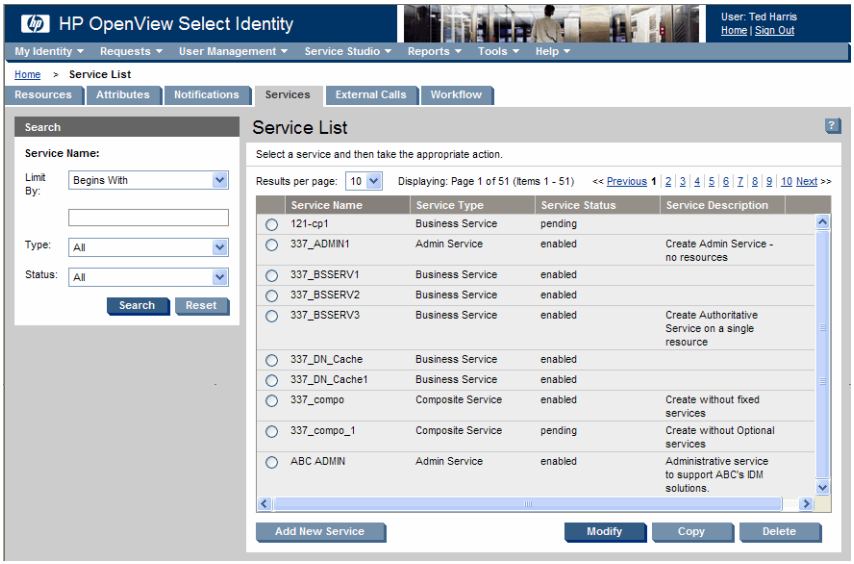
7 Click **OK**.
Deletes the form and returns to the **Service List** page.

Modifying a Service Role

Perform the following steps to modify a Service Role:

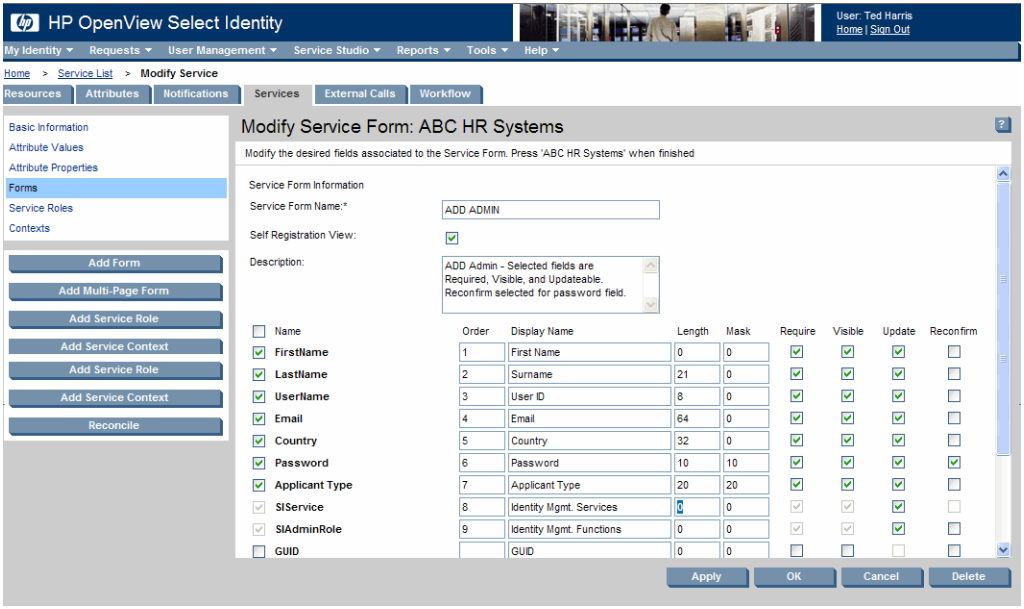
1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

Figure 108Service List



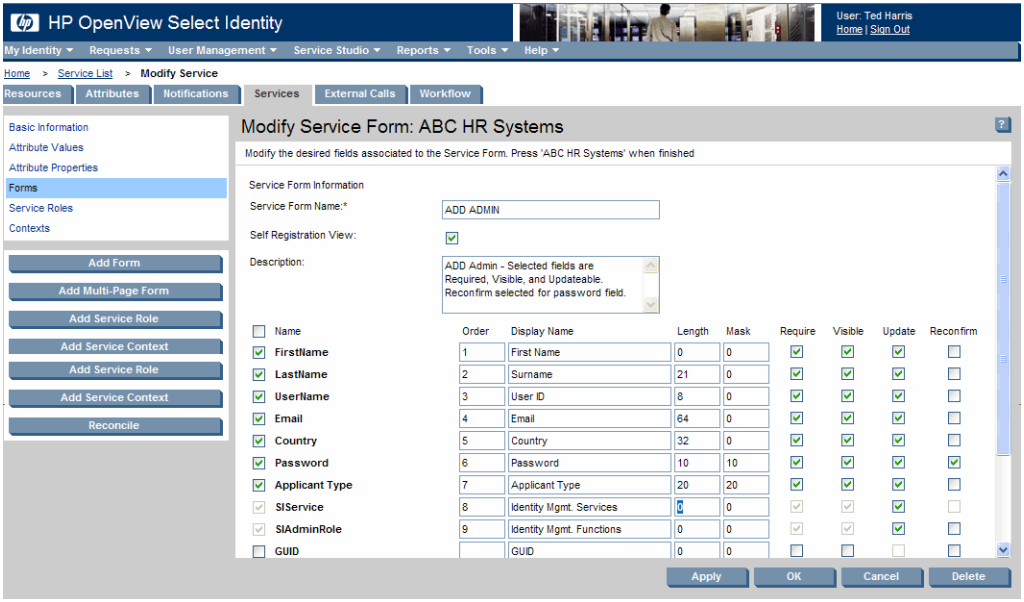
2 Select the **Service** you want to modify.
Opens the **Modify Service: Service Name** page.

Figure 109 Modify Service Role: Service Name



3 Click the **Service Roles** link in the left panel.
The Service Role fields appear in the right panel.

Figure 110Modify Service Role: Service Name



4 Select the service role you want to modify from the **Service Role Name** field. Opens the service role details.

Tab from field to field and modify the information necessary. See Notification Variables on page 124 for information about notification policies.

If	Then
If you want to add a Notification Event	Click to locate and add notification events to support the Service Role.
If you want to remove a Notification Event	Select the event you want to remove and click the icon.
If you want to add a Notification as so associated with an event	Select the event you want to change, then click to locate and add notifications to support the Service Role.

If	Then
Remove a Notification associated with an event	Select the event you want to change, then click the notification you want to remove and click the  icon.
Add a Request Event	Click  to locate and add a request event to support the Service Role.
Remove a Request Event	Select the event you want to remove and click the  icon.
Add a Workflow Template associated with an event	Select the event you want to change, then click  to locate and add a Workflow Template to support the Service Role. See Workflow Studio on page 273 for information about Workflow Templates.
Remove a Workflow template associated with an event	Select the event you want to change, then click the template you want to remove and click the  icon.

5 Modify the fixed attributes that you want assigned to users enabled for this Service Role.

You can select multiple attributes. See Setting Service Attribute Values and Properties on page 158 for information about attributes and values.

If	Then
You want to add a Fixed Attribute	Select an attribute from the **Name** field and enter a new name, then enter the appropriate variable in the **Value** field and click  .
You want to edit a Fixed Attribute	Move the attribute from the text box by clicking on the attribute, then selecting the  icon and edit as appropriate. Enter your change by clicking  .
You want to remove a Fixed Attribute	Select the attribute that you want to remove and click  .

6 Click to move the attribute and value to the entry table..

If.	Then
You want to add an Optional Attribute	Select an attribute from the **Name** field and enter a new name, then enter the appropriate variable in the **Value** field and click  .
You want to edit an Optional Attribute	Move the attribute from the text box by clicking on the attribute, then selecting the  icon and edit as appropriate. Enter your change by clicking  .
You want to remove an Optional Attribute	Select the attribute that you want to remove and click  .

7 Click  to move the attribute and value to the entry table.

Delete an attribute by clicking on attribute you do not want and selecting the  icon. Move the constraint from the text box by clicking on the constraint and then selecting the  icon and edit as appropriate if you make an error.

8 Click **Apply.**
Saves your work.

9 Click **OK**.
Returns to the **Service List** form.

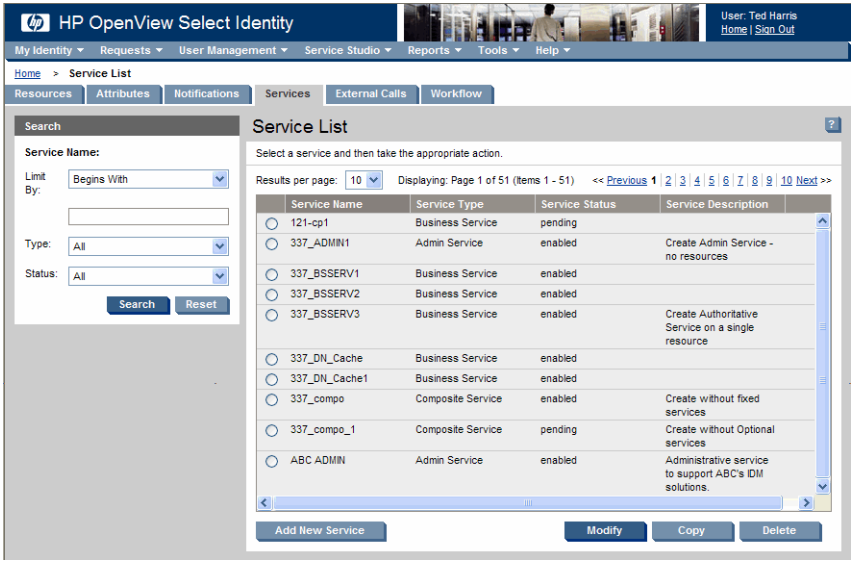
Deleting a Service Role

Before you delete a Service Role, make sure that the Context settings for this Service Role have been deleted.

Perform the following steps to delete a Service Role:

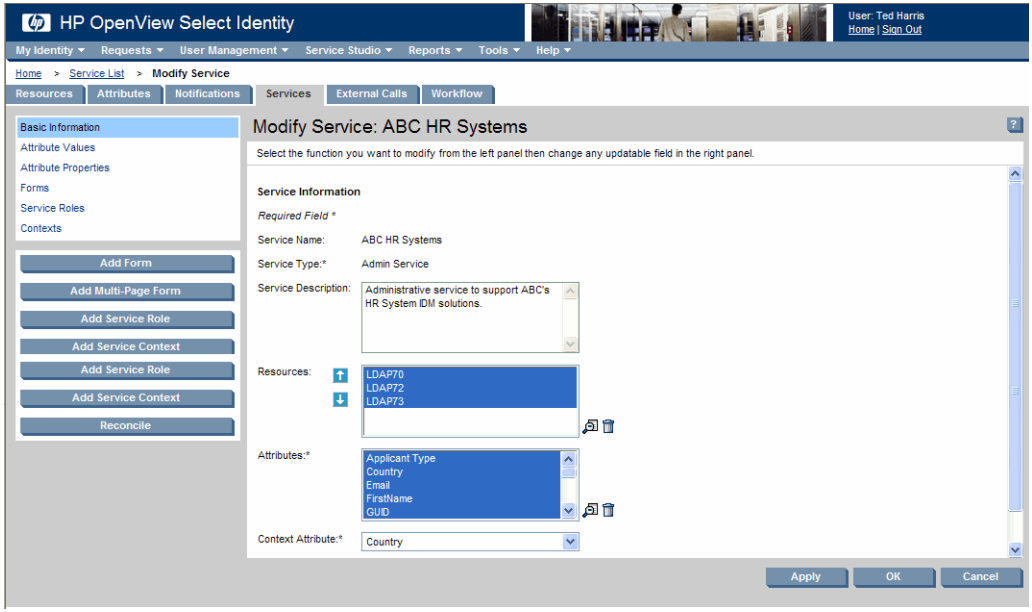
1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

Figure 111Service List



2 Click **Modify**.
Opens the **Modify Service: Service Name** page.

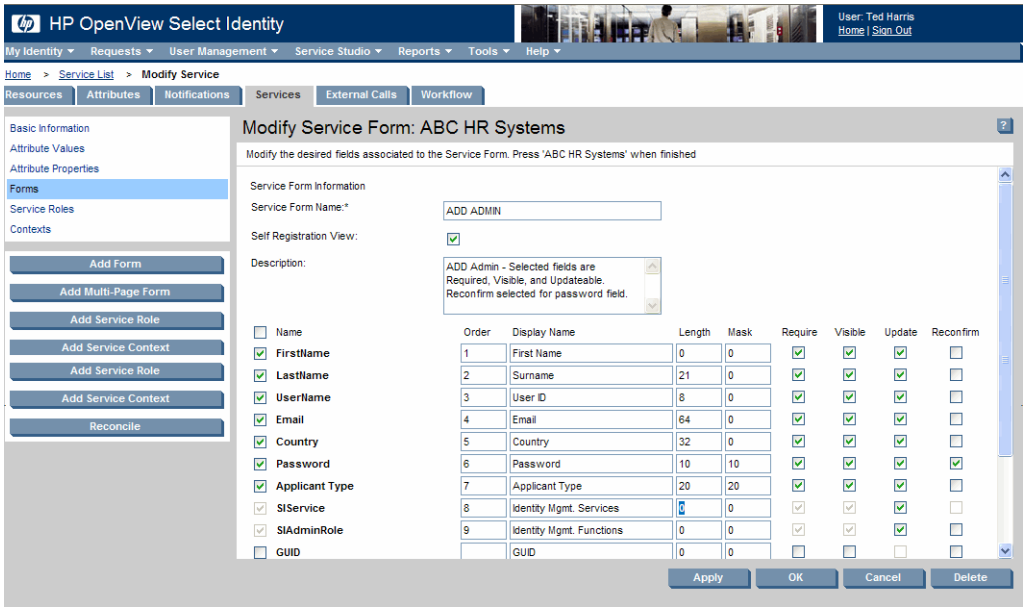
Figure 112 Modify Service: Service Name



3 Click the **Service Roles** link in the left panel.
Opens the **Service Roles** page.

4 Select the service role you want to modify from the **Service Role Name** field.
Opens the service role details.

Figure 113Modify Service Role: Service Name



5 Click **Delete**.
Opens the confirmation dialog box.

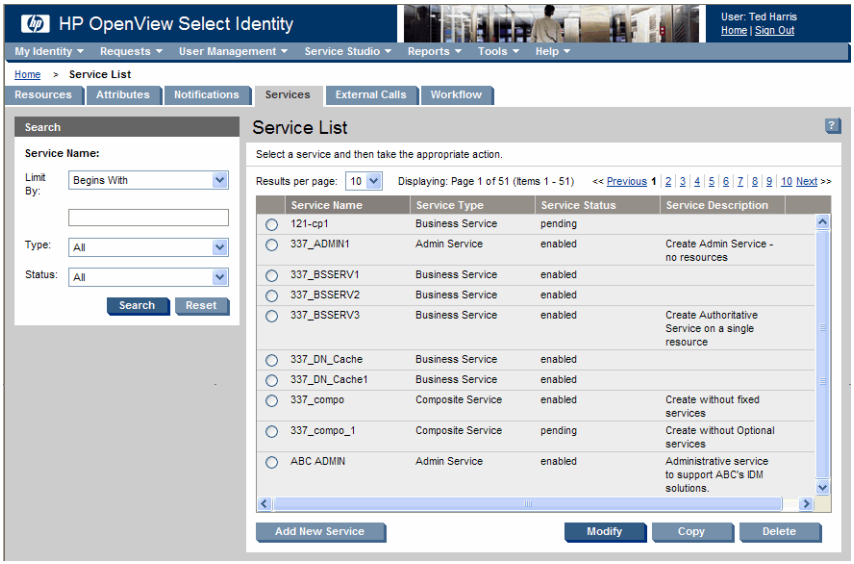
6 Click **OK**.
Deletes the service role.

Modifying Context Before Users are Added

Occasionally when you are creating services you may make an error during the addition of new context user groups. If users have NOT been imported follow the steps listed below to modify the context.

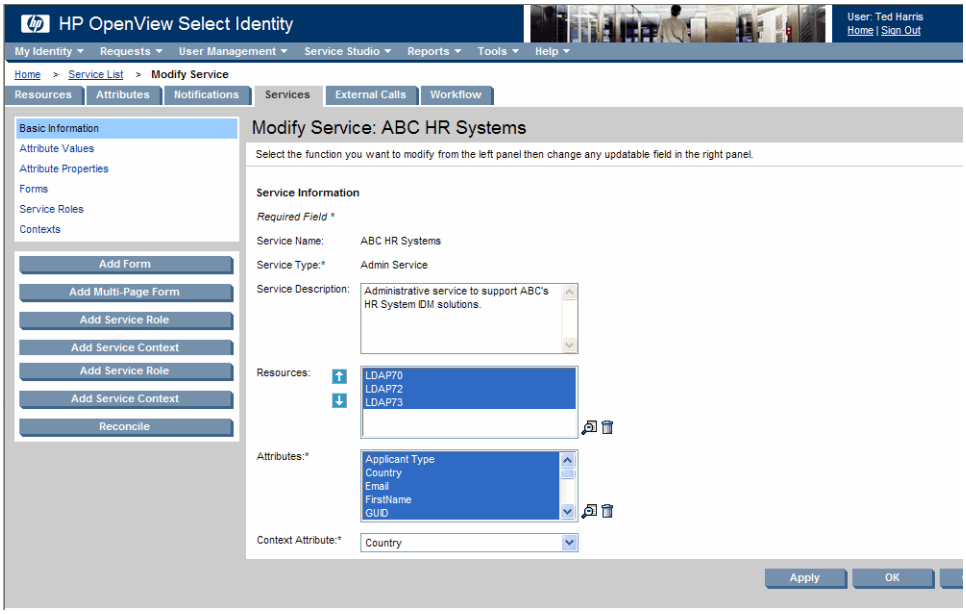
1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

Figure 114Service List



2 Click **Modify.**
Opens the **Modify Service: Service Name** page.

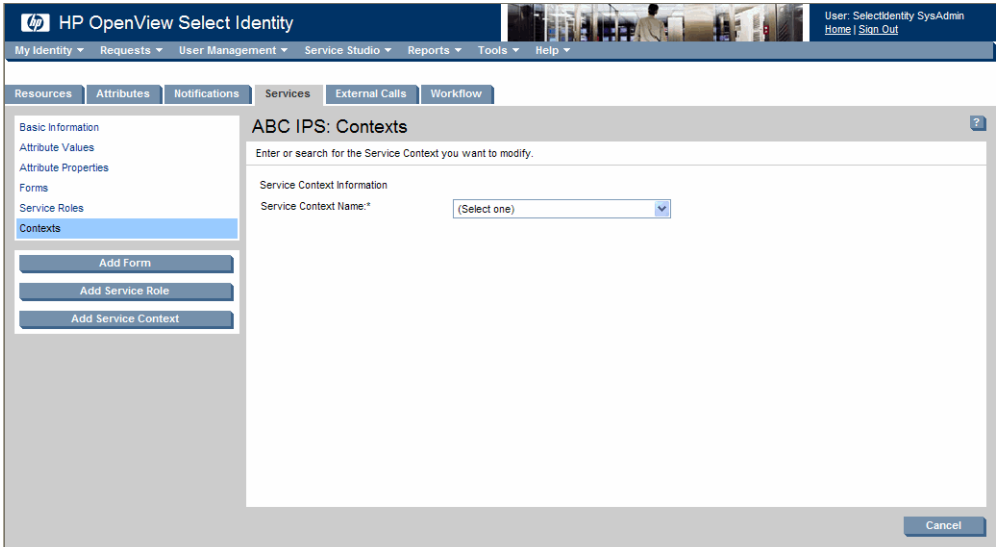
Figure 115 Modify Service: Service Name



3 Click on the **Contexts** link in the left panel.
Opens the **Modify Service Context: Service Name** page.

4 Select the context that you entered incorrectly from the **Service Context Name** field.
Opens the **Context** content fields.

Figure 116 Modify Service Context: Service Name

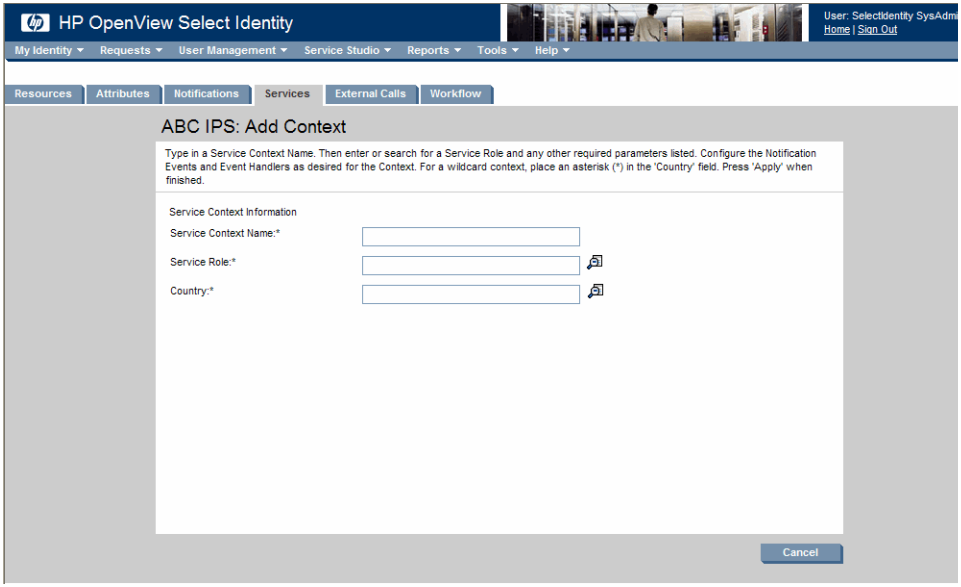


5 Click **Delete**.
Opens the confirmation dialog box.

6 Click **OK**.
Returns you to the original page.

7 Click the **Add Service Context** button on the left panel.
Opens the **Add Context** page

Figure 117Add Context



8 Tab from field to field to enter the information necessary to define the Context.

Field	Action
Service Context Name	Click to search for and select a parent context if one is available. If this is the first Context record created, you will not have a parent option. The parent provides a superset of attributes, workflow processes, and policies that you can choose from once it is available.
Service Role	Click to locate the correct the Parent Service Role. Displays additional fields. The parent Service Role provides a superset of attributes, workflow processes, and policies that you can choose from when available.

9 Tab from field to field to complete the Context user group definition.

Field	Action
Service Context Name	Click  to search for and select a value for the context attribute that you defined when creating the service.
Service Role	Click  to search for and select a value for the service role that you defined when creating the service.
<Context>	Click  to search for and select a value for the context attribute constraint.
Notification Events	Click  to locate and add notification events to support the Service Role.
Notifications	Click on the event listed in the **Notification Event** text box, then click  to select the Notification policy templates you want associated with the event. See Notification Variables on page 124 for information about notification policies.
Request Events	Select  to locate and add request events to support the Service Role. See Notification Variables on page 124 for a list of events and actions within OVSI
Workflow Template	Click on the event listed in the **Request Event** text box, then click  to select the Workflow template(s) you want associated with the event. See Workflow Studio on page 273 for information about Workflow Templates.

10 Click **Apply**
Creates the Context and enables the service.

11 Click **OK**.
Saves your work and returns to the original page.

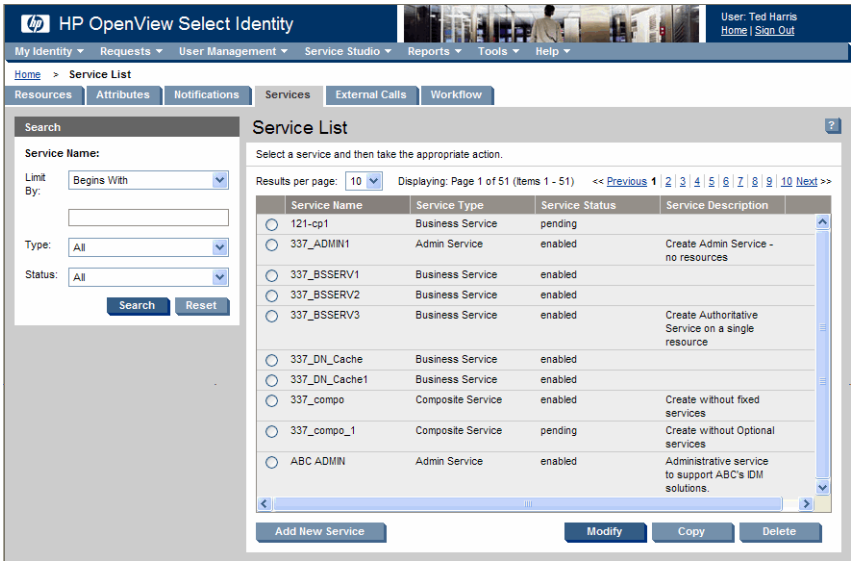
Modifying Context

Modify the context user group relationship of users assigned to a Service when you need to change the capabilities of an entire group of users at one time.

Perform the following steps to modify context:

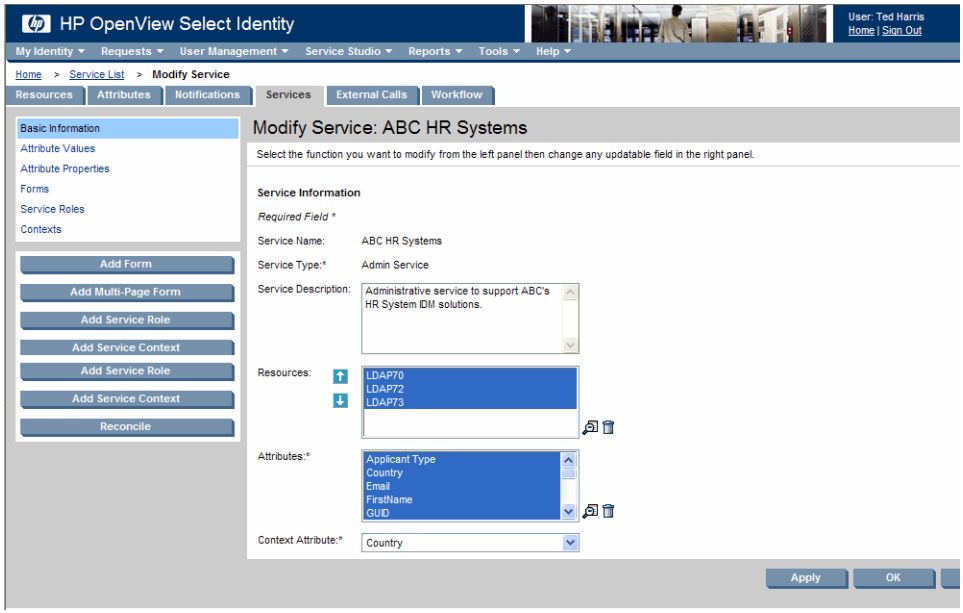
1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

Figure 118Service List



2 Click **Modify**.
Opens the **Modify Service: Service Name** page.

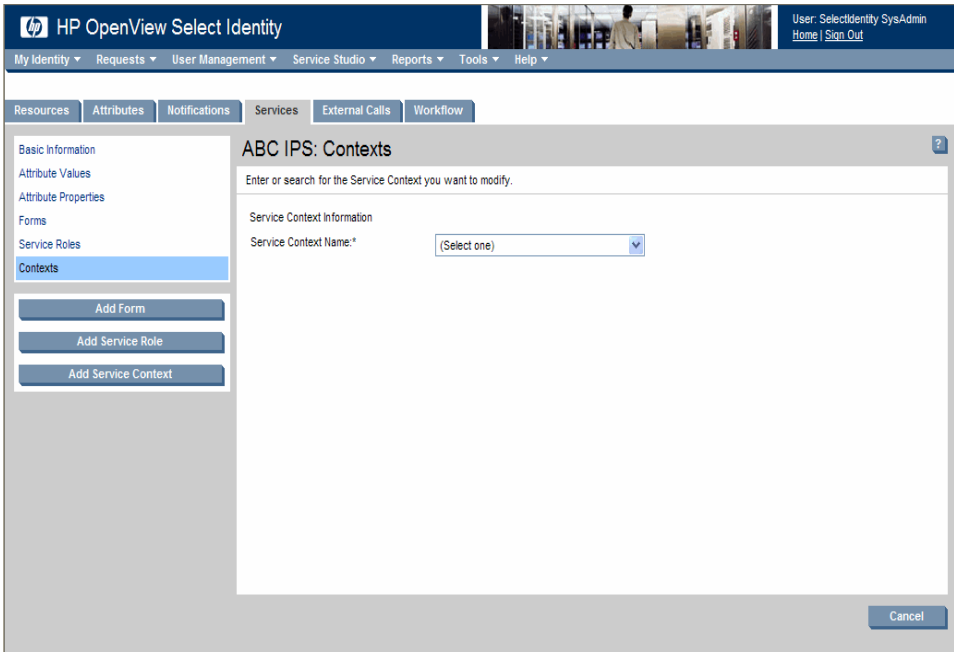
Figure 119 Modify Service: Service Name



3 Click on the **Contexts** link in the left panel.
Opens the **Modify Service Context: Service Name** page.

4 Select the context that you want to modify from the **Service Context Name** field.
Opens the **Context** content fields.

Figure 120Modify Service Context: Service Name



5 Review the information displayed.

6 Tab from field to field and modify the information necessary.

If	Then
You want to change the name of the role	Click on the **Service Role Name** field and enter a new name.
You want to change the name of the Context Variable	Enter a new context variable for the context displayed.
You want to add a Notification Event	Click to locate and add notification events to support the Service Role. See Notification Variables on page 124 for information about notification policies.
Remove a Notification Event	Select the event you want to remove and click the icon.

If	Then
Add a Notification associated with an event	Select the event you want to change, then click  to locate and add notifications to support the Service Role. See Notification Variables on page 124 for information about notification policies.
Remove a Notification associated with an event	Select the event you want to change, then click the notification you want to remove and click the  icon.
Add a Request Event	Click  to locate and add a request event to support the Service Role. See Adding a Service Role on page 169 for a list of events and actions within Select Identity.
Remove a Request Event	Select the event you want to remove and click the  icon.
Add a Workflow Template associated with an event	Select the event you want to change, then click  to locate and add a Workflow Template to support the Service Role. See Workflow Studio on page 273 for information about Workflow Templates.
Remove a Workflow template associated with an event	Select the event you want to change, then click the template you want to remove and click the  icon.

7 Click **Apply**
Saves your work.

8 Click **OK**.
Returns to the **Service List** form.

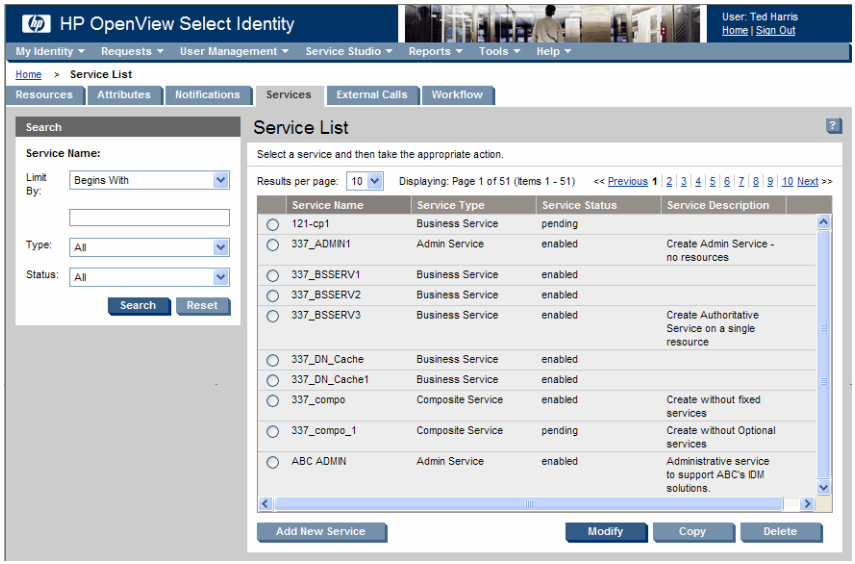
Deleting Context

Before you delete a context setting for a Service, make sure that all dependencies have been removed.

Perform the following steps to delete context:

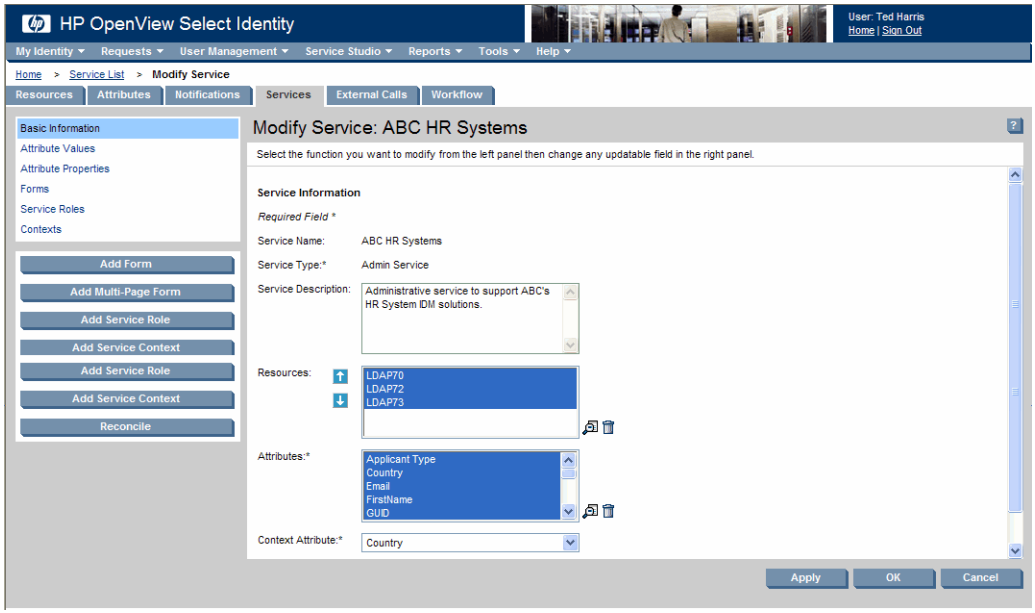
1 Select **Service Studio** → **Service** from the menu bar.
Opens the **Service List.**

Figure 121Service List



2 Click **Modify.**
Opens the **Modify Service: Service Name** page.

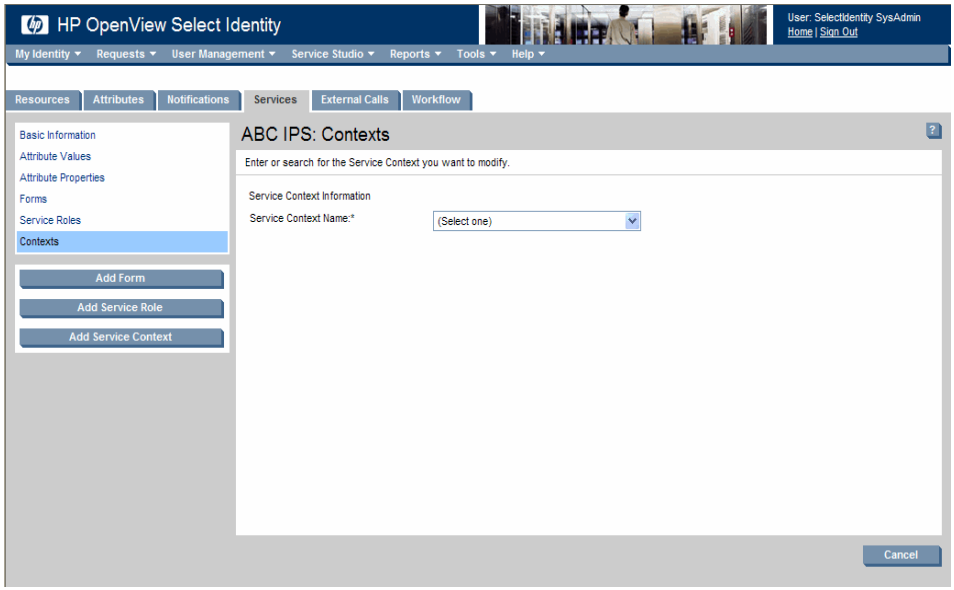
Figure 122Modify Service: Service Name



3 Click on the **Contexts** link in the left panel.
Opens the **Modify Service: Context Name** page.

4 Select the context that you want to modify from the **Service Context Name** field.
Opens the **Context** content fields.

Figure 123 Modify Service Context: Service Name



5 Click **Delete**.
Opens the confirmation dialog box.

6 Click **OK**.
Deletes the selected Context user group and returns to the **Modify Service: Service Name** page.

Reconciling a Service

Service reconciliation is used for updating existing users of the service upon following service changes:

- Add or delete of resources to service.
- Add or delete of fixed attribute values to a ServiceRole in the Service.

To reconcile a service, do the following:

1 Click the **Reconcile** button from the `Modify Service Screen` window to schedule a service reconciliation job for a Service.

The `Schedule Reconciliation Job` screen displays.

2 Enter the Start Date, or the date when to initiate the job . This information is required.

3 Enter the Start Time, ot the specific time to start the job on the selected date. This information is optoipnal.

4 Click **OK** to save the schedule information.

If a Service Reconciliation Job for this Service is `Pending`, meaning that the job has not started yet, then this page shows the scheduled start date and time information. New information can be entered to modify the schedule.

If a Service reconciliation Job for this Service is `InProgess`, meaning the job has started but not yet completed, then modifying the schedule of the job is not allowed.

If no changes are made for the Service that affect existing users, scheduling of the job is not allowed.

When the job starts, a request corresponding to the service reconciliation job is displayed in the `Request List` page. Click **View Request Status** to show the status of each child request.

Upon completion, a compressed report is sent to the user who created the job. The report will also be saved at:

```
<truaccess.batch.reportdir>/servicerecon/
ServiceReconReport_<ServiceName>_<JobID>_final.htm
```

5 User Import

The User Import function enables you to add a large group of your organization's existing users to Select Identity. User Import is used as a one time import mechanism to populate users into Select Identity. It does not provision users. Use this feature whenever you are adding a new service or resource. The list of users and their associated attributes are specified in an SPML file and are subsequently loaded to Select Identity through the **Schedule User Import** action.

Schedule User Import action is for one-time file upload only. Recurring jobs for user discovery can be scheduled by copying files to the (`adroot`) upload directory.

After users are added to Select Identity, entitlements or other resource specific attributes associated with the users are determined by specifying the Resource (any single application or information repository) from which the users originated. These entitlements, like the user attributes, are specified in an SPML file and associated to a user's unique identifier. After both the users and entitlements are loaded to Select Identity, the **Schedule Services Assignment** action is used to associate the users to the proper Services (business-centric abstraction representing resources, entitlements, and other identity-related entities). Associating users to Services creates an account which can now be maintained through Select Identity's Business Service Identity Management (BSIM) model.

Before starting the User Import process, you should optimize Select Identity for best performance. For details on configuring these settings and other important settings, see "Optimizing Select Identity" in the *Select Identity Installation Guide*.

This chapter covers the following information:

- User Import Procedure Overview
- Scheduling User Import

- Service Assignment List
- Schedule Service Assignment

User Import Procedure Overview

This chapter describes the process for adding a group of existing users to Select Identity. All detailed procedures are available later in this chapter and in the Select Identity online help.

You must have the Select Identity system administrator role with User Import permissions to perform **User Import** tasks.

This section covers the following:

- Defining Users and Attributes from an Authoritative Resource
- Prerequisites for Importing
- Creating an SPML file Containing Users and Attributes
- Creating an SPML File Containing Entitlements
- Checking for Service Membership Requirements
- Checking the TruAccess.properties File
- Uploading User Accounts, Attributes, and Entitlements

Defining Users and Attributes from an Authoritative Resource

Typically, businesses have an existing resource called an **Authoritative Resource**. It contains account information and attributes for each user account used to update all other accounts. For example, your **Authoritative Resource** might have an employee number and attributes associated with the employee number (First Name, Last Name, Address, Phone, Social Security). See Using Authoritative Resources on page 78 for detailed information and instructions. Before building your SPML file, identify your main source of user data and determine your list of attributes to be loaded to Select Identity.

Prerequisites for Importing

Prior to doing the user import:

- Define the resources in Select Identity
- When specifying attributes in the SPML file, be sure to use the mapped resource attribute's name. This may differ from the Select Identity attribute name. Attributes uploaded to Select Identity must be mapped to a resource. For information related to attribute mapping, see Mapping Resource Attributes on page 87.
- The Sync-In/Sync-Out flags are set correctly during resource attribute mapping. See Using Authoritative Resources on page 63 for further information.
- Use the mapped resource attribute names in the import SPML file
- If using an automated job for import, make sure the user import properties in the Truaccess.property file are configured. Unlike Reconciliation and Bulk, automated User Import jobs are not scheduled through UI. The User Import SPML files have to be dropped in the upload directory. See Upload Requirements on page 230 for more information

To see an example of an add user request file, refer to the HP OpenView product CD in the `\SampleXML` directory.

Creating an SPML file Containing Users and Attributes

Many resources today have a utility or mechanism for exporting user data to an XML or SPML format. Create the SPML format needed for User Import, using one of the following processes:

- Use the Select Identity SPML Generator tool to convert the data to SPML from CSV and XML inputs. See SPML Generator Utility on page 543.
- Export your data in the resource to LDIF format and use a parser to convert the data to SPML. To see an example of an User Import file after the LDIF format to SPML conversion, view the sample files located in the `\SampleXML\Auto-Discovery` directory on the HP OpenView product CD.
- Export your data in the resource to XML or DSML format. Convert it to SPML using an XML parser and XSLT style sheet.
- Use a third-party mapping tool to convert your data to SPML format.

- Programmatically build the file by reading through your resource and writing out a data record for each user.

The syntax used must comply with SPML; the semantics differ according to the Select Identity tags. When creating the input file containing the user attributes, specify the unique identifier attribute associated with each user. The `<operationalAttributes xmlns=>` section of the SPML file specifies the identifier and is designated as a value in the `keyFields` attribute. Select Identity's default attribute for identifying accounts is **UserName**. The following is a sample of this section of the SPML file:

```
<operationalAttributes xmlns="">
   <attr name="urn:hp:selectidentity#keyFields"><value>
   UserName</value></attr>
</operationalAttributes>
```

In addition to specifying the operational attribute in the header of the file, you need to specify two operational attribute values for each add user request. The following shows a sample of the SPML file:

```
<addRequest requestID="1">
  <operationalAttributes xmlns="">
    <attr name="urn:hp:selectidentity#taUserName">
    <value>avaughan</value></attr>
    <attr name="urn:hp:selectidentity#taResourceKey">
    <value>AQ4100</value></attr>
  </operationalAttributes>
```

In the above examples, attribute name can be either `<attr name="urn:hp:selectidentity#keyFields">` or `<attr name="urn:trulogica:concero:2.0#keyFields">` as Select Identity has backwards compatibility.

`Test1_1user.xml`

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<batchRequest xmlns:countries="countries.uri"
smlns:cities="cities.uri" smlns:dsml
```

The `taUserName` field value represents the unique value used to identify each account in Select Identity. The `taResourceKey` uniquely identified the account on the resource from which the user originates.

The file data portion must begin and end with `<batchRequest></batchRequest>`.

Each account to be added begins and ends with <addRequest></addRequest>. Select Identity requires the operational attributes and values listed for each add request. An account cannot be added without these attributes and values.

If the UserName attribute is set up with a value generation function and a User Import request is made from an Authoritative Resource, the taUserName does not need to be specified in the SPML file and the UserName should not be specified as keyField in the operational Attribute section. Select Identity invokes the value generation function to generate the UserName. The user is provisioned in Select Identity with this generated UserName.

If another resource attribute is mapped to Select Identity UserName and is present in the SPML record, then the taUserName is not needed and that reource attribute is used as the UserName.

Following is a sample SPML file without the taUserName:

```
<batchRequest xmlns:countries="countries.uri"

xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
   <operationalAttributes xmlns="">
      <attr name="urn:trulogica:concero:2.0#keyFields">
        <value>Email</value></attr>
   </operationalAttributes>
<addRequest requestID="1">
   <operationalAttributes xmlns="">
      <attr
name="urn:trulogica:concero:2.0#taResourceKey"><value>firstname.
lastname@yourdomain.com</value></attr>
   </operationalAttributes>
   <attributes xmlns="">
       <attr name="Employee ID"<value>HP</value></attr>
       <attr name="LastName"><value>Jones-Smythe</value></attr>
      <attr name="Email"><value>john.smith@hp.com</value></attr>
       <attr name="FirstName"><value>John</value></attr>
       <attr name="State"><value>TX</value></attr>
       <attr name="Address2">
             <value>Info Field 1 from Recon file</value>
             <value>Info Field 2 from Recon file</value>
             </attr>
```

```
        <attr name="city"><value>Plano</value></attr>
        <attr name="Title"><value>Manager</value><?attr>
        <attr name="Business Phone"><value>8886661122</value></
attr>
        <attr name="Zip"<value>77777</value></attr>
        <attr name="Address 1"><value>Rolling Drive</value></
attr>
        <attr name="Password"><value>abc123</value></attr>
   </attributes>
</addRequest>
</batchRequest>
```

Creating an SPML File Containing Entitlements

After building the SPML file containing your list of users and associated attributes, review the resources containing the entitlements or permissions associated with your users. Users may have entitlements from multiple resources. To upload these entitlements, create a separate SPML file containing the entitlements for each resource. Use one of the methods described in Creating an SPML file Containing Users and Attributes on page 220 to create this SPML file.

For each resource file created, determine the unique identifier on the resource linking the entitlement to the designated user. This unique identifier is specified in the SPML file as the `taResourceKey` field. In addition, specify the userId or user name so you can associate the entitlements to the correct Select Identity account. This is designated in the identifier tag as follows:

```
<identifier xmlns=""
type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName"><id>AEE
200</id></identifier>
```

When specifying the entitlement, the identifier type `UserIDAndOrDomainName` specifies the username or account in Select Identity associated with the entitlement. In the example above, the entitlement is associated with an account called `AEE200` in Select Identity.

The operational attributes `keyFields`, and `taResourceKey` are required for assigning entitlements. These are specified in the file you created to add users to the system. The attribute `keyFields` is only listed once at the beginning of each file. The attribute `taResourceKey` is listed for each user account. If the attribute `keyFields` value exists in SPML, it is used to locate the user in Select Identity. Otherwise an identifier is used.

To see an example file for adding entitlement to an existing user, refer to `\SampleXML` directory on the Select Identity product media.

Checking for Service Membership Requirements

Once added, users can be assigned service memberships based on their defined attributes For users to gain a service assignment through reconciliation, the following must be true:

- Users must have access to all of the resources that a service requires.
- Users must have all required attribute values for a service.
- Users must have matching values for the service's context attribute.
- Users must have matching fixed attribute values for a service based on context value. The set of all fixed attribute values starting from the current context or business role level all the way up to the root is a subset of the corresponding user attribute set. When no fixed attribute value is defined, this evaluation is skipped.
- Users must have matching optional attribute vallues for a service based on context value. The optional attribute value set is gathered starting from the current context or business role. When a value set is defined, the lookup process stops. Otherwise, the search continues up to the root level. The optional value set is a super set of the corresponding user attribute set. When no optional attribute value is defined, this evaluation is skipped.
- When an attribute is present, the length and pattern must match the field definition.
- When an attribute is present and the field has a constrained value set, the attribute value must be one of the constrained values. The constrained values are either from the static atribute definition, or an external call function is defined for the attribute.

Checking the TruAccess.properties File

Upload Requirements

Be sure to set the following properties in the `TruAccess.properties` file to facilitate the upload process. See "Configuring TruAccess.properties" in the *HP OpenView Select Identity Installation Guide* for detailed descriptions of all properties in the `TruAccess.properties` file.

If using **Cluster**, every directory set up here must be a shared directory with read/write permission.

- `truaccess.batch.reportdir=c:/temp/reports`
- ```
  ovsi.ad.rootdir=/opt/si4.0/weblogic/adroot
  ovsi.ad.backupdir=/opt/si4.0/weblogic/adbackup
  ovsi.ad.stagingdir=/opt/si4.0/weblogic/adstaging
  #ovsi.ad.subdir=subdir
  ovsi.ad.userid=2
  ovsi.ad.file.threshold=2
  ovsi.ad.emailcc=your.eamil@yourdomain.com
  ```

  These properties are necessary for all user import functions. If `rootdir` and `backupdir` are not provided in the property file, no user-discovery is scheduled.

  The format of the input batch file is:

`&lt;resourceName&gt;_&lt;datetime&gt;&lt;randomNumber&gt;.eml`

The default separator is an underscore ("_"). You can define the separator to be any character you wish in TruAccess.properties (`com.hp.ovsi.spml.resourcename.separator`). For example, `com.hp.ovsi.spml.resourcename.separator = +`

Please note the first underscore "_" from the end is used as a delimiter to identify the resourceName. That is, the resourceName can have embedded underscores as in `LDAP_71+&lt;datetime&gt;&lt;randomNumber&gt;`. Therefore, do not use an underscore "_" in `&lt;datetime&gt;&lt;randomNumber&gt;`.

Following are descriptions of each property:

— `ovsi.ad.rootdir=/opt/si4.0/weblogic/adroot`

Specifies the location of User Import input batch files.

— `ovsi.ad.backupdir=/opt/si4.0/weblogic/adbackup`

Specifies the location of processed User Import batch files.

— `ovsi.ad.stagingdir=/opt/si4.0/weblogic/adstaging`

Specifies the location of the working directory used for processing the file.

— `#ovsi.ad.subdir=subdir`
  ```

Specifies the location of the subdirectory of `/opt/si4.0/weblogic/adroot` where the files are retrieved. This property is optional.

— `ovsi.ad.userid=2`

Specifies `sisa (userid 2)` as the user running the User Import job. Defaults to `sisa` if a number is not provided.

— `ovsi.ad.file.threshold=2`

Indicates the number of User Import files simultaneously uploaded. The maximum recommendation is two 10K simultaneous files. Defaults to three if a number is not provided.

Certain user profile attributes can be added to the `TruAccess.properties` file and used to expedite search functions, such as employee ID or tax ID number. Having an attribute mapped in the `TruAccess.properties` file for search purposes facilitates the User Import process.

The `TruAccess.properties` file is described in detail in the *HP OpenView Select Identity Installation Guide*.

Uploading User Accounts, Attributes, and Entitlements

You can now upload the user accounts, attributes, and entitlements through the *User Import* pages assuming you deploy the correct connectors. Learn more about connectors in Connectors on page 61. See Scheduling the User Import for instructions.

You can improve the performance of **User Import** tasks by breaking large files into smaller ones and running the files in parallel. Performance improves significantly when running on a multi-CPU server. You should run multiple files in parallel when uploading files for User Import. Select Identity processes authoritative resource files before non-authoritative resources.

Using User Import

This section describes how to use the User Import features. It covers the following:

- Viewing Job Status

- Scheduling User Import
- Service Assignment List
- Scheduling Services Assignment

Viewing Job Status

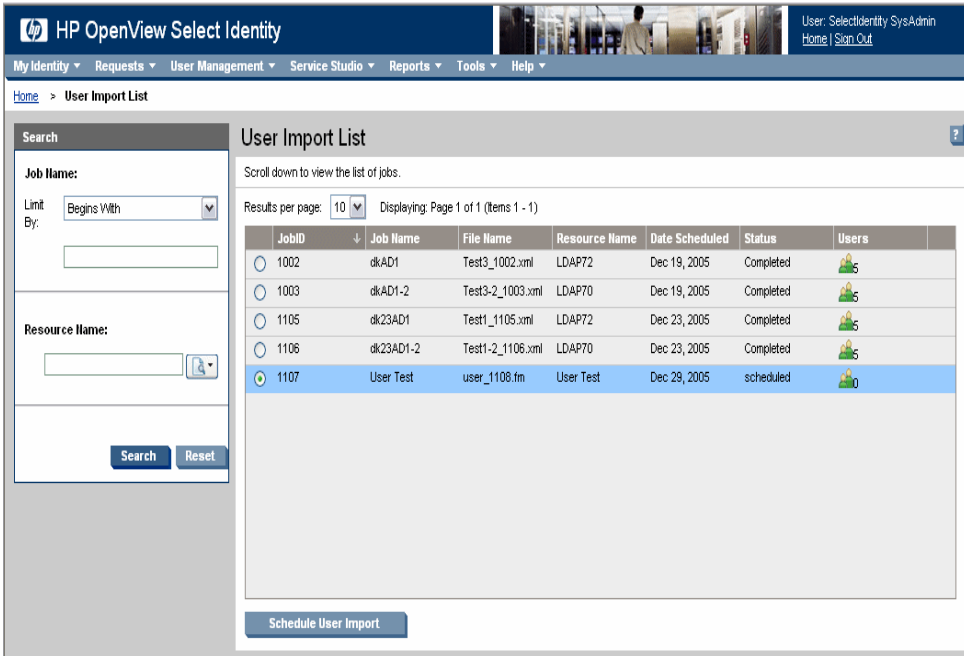
The **User Import List** shows the status of previously scheduled batch tasks. Authoritative resources process before non-authoritative resources. This is an information only page. It contains the following information:

Field	Purpose
JobID	The unique number assigned by the system
Job Name	The unique name assigned by the Administrator when creating the job.
File Name	The SPML file name uploaded to perform the user import job.
Resource Name	The resource from where the file is imported.
Date Scheduled	The date scheduled for the import to run.
Status	Tells you if the import is complete, pending, or if it failed.
Users	The number of users imported.

Perform the following steps to view job status:

1 Select **Tools** → **User Import** → **User Import List**.
The **User import List** page opens.

Figure 124 User Import List Page



2 Review the list.

To search for a specific job:

1 Enter the parameters in the **Search** panel. For information on how to perform a search, see Using the Search Features in Select Identity on page 37 in Getting Started.

Parameter	Action
Job Name	Select the parameter from the drop-down box and enter the appropriate information in the next field.
Resource Name	Click  to open the **Resource Name** selection box, then click **Filter** and select the resource name from the list.

2 Click **Search.**
The jobs matching the criteria appear in the **User Import List**.

Scheduling User Import

You can configure Select Identity to add user accounts on a specified date. This process enables Select Identity to add account data to the system from a data file you create. See Creating an SPML file Containing Users and Attributes on page 220 for information about creating a data file. Connectors and Resources must be deployed for systems with identity information you want to import. All necessary Resource and Select Identity attributes must be mapped within the connector mapping and file and the OVSI **Attributes** function.

It is best to import all the users before assigning them to services. Wait until the import is finished before assigning user services.

This section covers the following:

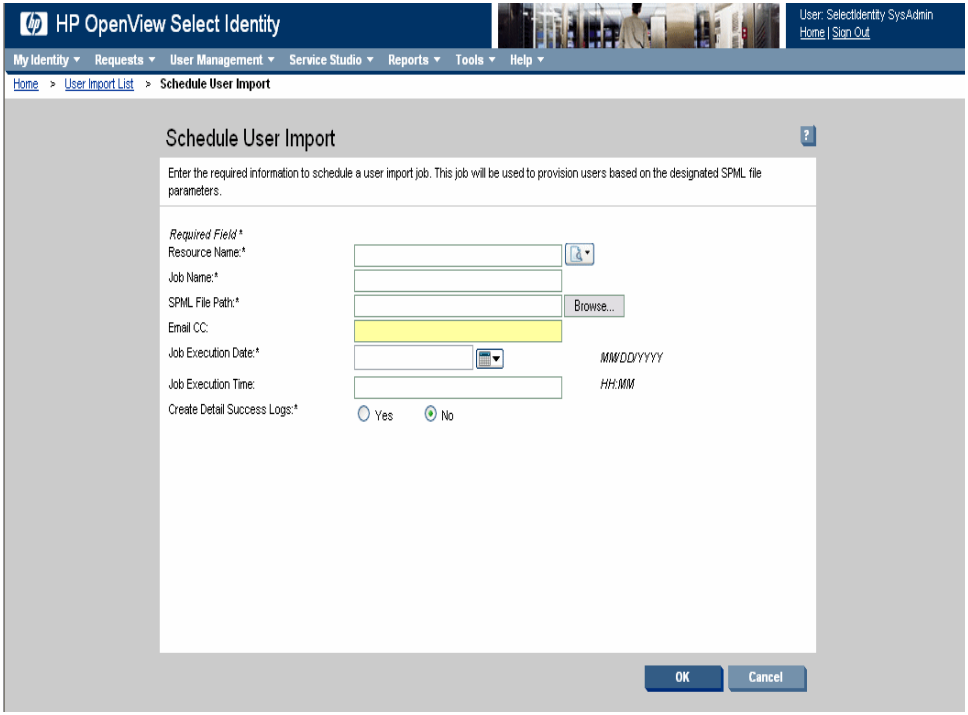
- Scheduling the User Import
- Reviewing Job Results
- Viewing User Import Status

Scheduling the User Import

Perform the following steps to schedule user account import:

1 Select **Tools** → **User Import** → **Schedule User Import**.
the **Schedule User Import** page opens.

Figure 125 Schedule User Import Page



Alternatively, select **Tools** → **User Import** →**User Import List**.
When the **User Import** page opens, click the Schedule User Import button.
The **Schedule User Import** page opens.

2 Tab from field-to-field to enter the correct information:

Field	Action
Resource Name	Select the resource you want to import from.
Job Name	Enter a unique name for your job.
SPML File Path	Click **Browse** to locate and select the data file you want to upload. See Creating an SPML file Containing Users and Attributes on page 220 for information about data files.

Field	Action
Email CC	Select Identity sends email to the administrator creating and running the job when the job completes. If you want an email sent to another administrator, enter an address in the Email CC field.
Job Execution Date	Click the **Calendar** icon to choose a date for this job to run. If you select the current day from the calendar, the job runs immediately
Job Execution Time	Enter the time (in HH:MM format) you want the job to run on the date specified earlier.
Create Detail Success Logs	Select **Yes** if you want to generate a detailed log after the User Import runs successfully or **No** if you do not. Selecting **Yes** slows down the process. If there are errors, an error log is generated automatically.

3 Click **OK.**
The job is added to the job list and runs when scheduled.

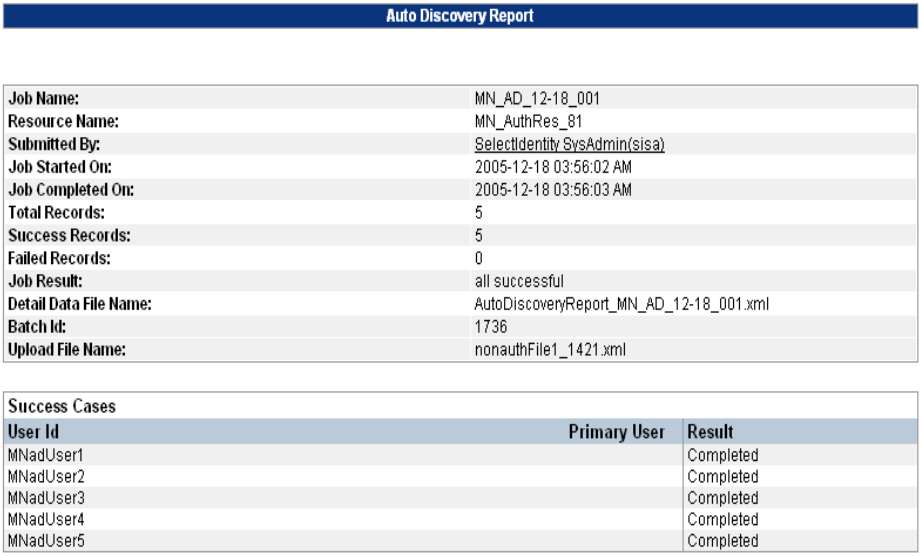
Reviewing Job Results

After each of the User Import jobs completes, the creator of the job receives a compressed HTML report. The report lists the users that were successfully created and those users that failed to be created.

The report is emailed automatiucally. A request for the report can also be accomplished through the GUI by clicking the Users link on each job.

The following shows a sample report without any errors:

Figure 126 User Import Sample Report Without Errors



Auto Discovery Report

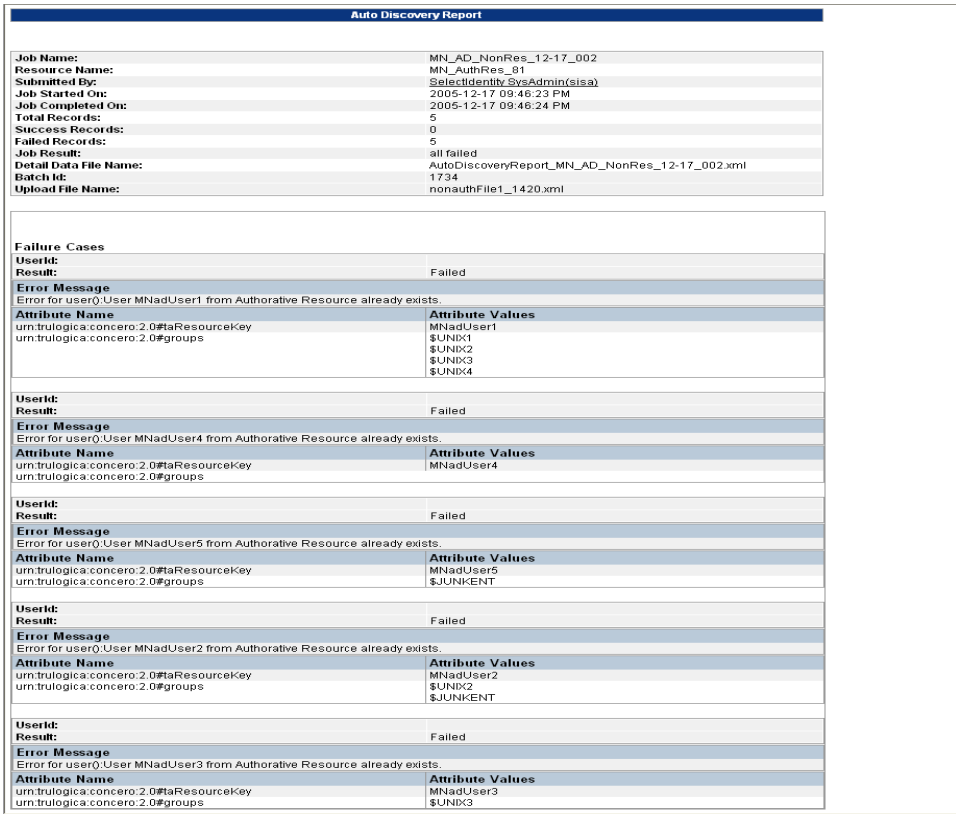
Job Name:	MN_AD_12-18_001
Resource Name:	MN_AuthRes_81
Submitted By:	SelectIdentity SysAdmin(sisa)
Job Started On:	2005-12-18 03:56:02 AM
Job Completed On:	2005-12-18 03:56:03 AM
Total Records:	5
Success Records:	5
Failed Records:	0
Job Result:	all successful
Detail Data File Name:	AutoDiscoveryReport_MN_AD_12-18_001.xml
Batch Id:	1736
Upload File Name:	nonauthFile1_1421.xml

Success Cases

User Id	Primary User	Result
MNadUser1		Completed
MNadUser2		Completed
MNadUser3		Completed
MNadUser4		Completed
MNadUser5		Completed

This is an example of a report with errors.

Figure 127 User Import Sample Report With Errors



Auto Discovery Report

Job Name:	MN_AD_NonRes_12-17_002
Resource Name:	MN_AuthRes_81
Submitted By:	SelectIdentity SysAdmin(sisa)
Job Started On:	2005-12-17 09:46:23 PM
Job Completed On:	2005-12-17 09:46:24 PM
Total Records:	5
Success Records:	0
Failed Records:	5
Job Result:	all failed
Detail Data File Name:	AutoDiscoveryReport_MN_AD_NonRes_12-17_002.xml
Batch Id:	1734
Upload File Name:	nonauthFile1_1420.xml

Failure Cases

UserId:	
Result:	Failed
Error Message	
Error for user():User MNadUser1 from Authorative Resource already exists.	
Attribute Name	**Attribute Values**
urn:trulogica:concero:2.0#taResourceKey	MNadUser1
urn:trulogica:concero:2.0#groups	$UNIX1 $UNIX2 $UNIX3 $UNIX4

UserId:	
Result:	Failed
Error Message	
Error for user():User MNadUser4 from Authorative Resource already exists.	
Attribute Name	**Attribute Values**
urn:trulogica:concero:2.0#taResourceKey	MNadUser4
urn:trulogica:concero:2.0#groups	

UserId:	
Result:	Failed
Error Message	
Error for user():User MNadUser5 from Authorative Resource already exists.	
Attribute Name	**Attribute Values**
urn:trulogica:concero:2.0#taResourceKey	MNadUser5
urn:trulogica:concero:2.0#groups	$JUNKENT

UserId:	
Result:	Failed
Error Message	
Error for user():User MNadUser2 from Authorative Resource already exists.	
Attribute Name	**Attribute Values**
urn:trulogica:concero:2.0#taResourceKey	MNadUser2
urn:trulogica:concero:2.0#groups	$UNIX2 $JUNKENT

UserId:	
Result:	Failed
Error Message	
Error for user():User MNadUser3 from Authorative Resource already exists.	
Attribute Name	**Attribute Values**
urn:trulogica:concero:2.0#taResourceKey	MNadUser3
urn:trulogica:concero:2.0#groups	$UNIX3

After reviewing the report, make any needed corrections and resubmit the file with only those accounts that failed. Create a new job to upload this file in the Select Identity client.

If you created the job that ran initially, you cannot give the new job the same name. Each job you create as an administrator must have a unique name.

Viewing User Import Status

To review the status of previously scheduled imports select **Tools** → **User Import** → **User Import List**. SeeViewing Job Status on page 233 for details.

Service Assignment List

Scheduling Service Assignments functionality associates newly discovered users with existing Services in Select Identity. To take advantage of Select Identity's Business Services Identity Management, a user must be associated with a service. Service assignment is generally a one-time event and is used in the early phase of establishing the Select Identity environment.

Service assignment is the last step of the User Import process. Service assignment should only be done after all user accounts and entitlements are loaded into Select Identity. All Services should be created before performing this action.

Select Identity assigns all user accounts qualifying for an existing service to the qualifying service automatically. Qualification is based on attribute and entitlement matches for each account. An administrator assigns newly created accounts to all or a subset of existing services. Once you assign services, use Select Identity's User Management functionality to maintain user accounts.

The system goes through each user account and evaluates whether that user is exists the specified service's resources. The user must be assigned to all required resources for the assignment to succeed.

For example, if Service #1 provisions to iPlanet and Service #2 provisions to iPlanet and SAP, the following are true:

- User1, found in iPlanet only, will be assigned to Service#1.
- User2, found in SAP only, cannot be assigned to Services #1 or #2.
- User3, found in iPlanet and SAP, will be assigned to Service#1 and #2.

Therefore, User Import of each resource must be 100% complete before the Service Assignment process starts.

Service Assignment List Page

The **Service Assignment List** page shows all scheduled Service Assignments. This is an information only page. It contains the following information:

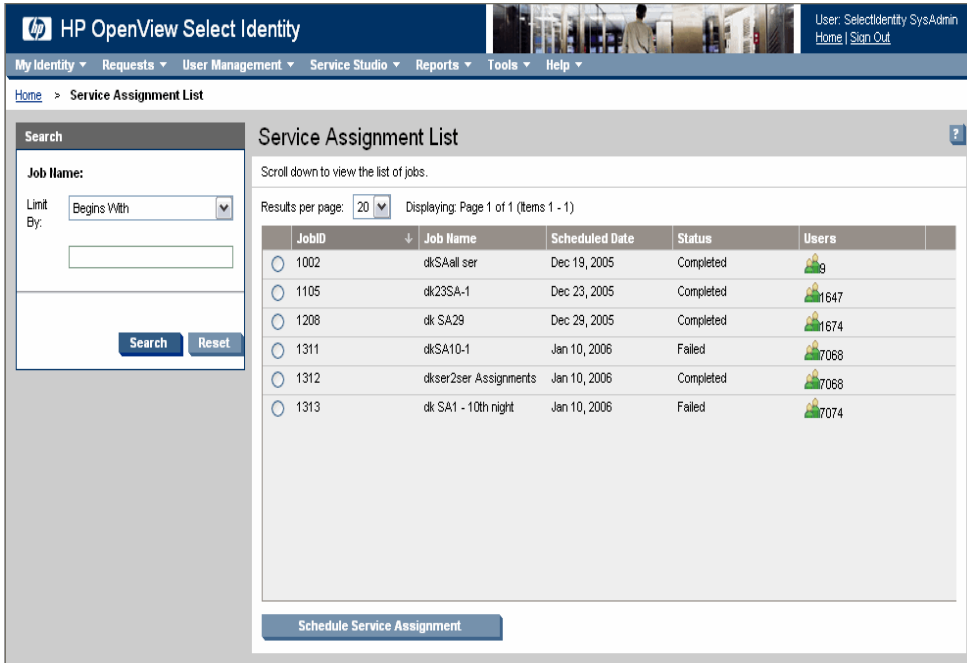
- **JobID**—the unique number assigned by the system
- **Job Name**—the unique name assigned by the Administrator when creating the job

- **Date Scheduled**—the date scheduled for the import to run
- **Status**—tells you if the Service Assignment is complete, pending, or if it failed
- **Users**—the number of users evaluated for the service

Perform the following steps to view job status:

1 Select **Tools** → **User Import** → **Service Assignment List**.
The **Service Assignment List** page opens.

Figure 128 Service Assignment List Page



2 Review the list. If you need to create and schedule a new service assignment, click **Schedule Service Assignment**.

To search for a specific Service Assignment:

1 In the Search panel, enter the **Job Name** parameters from the drop-down box and enter the appropriate information in the next field.

For information on how to perform a search, see Using the Search Features in Select Identity on page 37 in Getting Started.

2 Click **Search.**
The jobs matching the criteria appear in the **Service Assignment List**.

Scheduling Services Assignment

Service assignments must be performed by a Select Identity system administrator who has access to all contexts on all services.

As users are added to the system, you can schedule service access. This is particularly helpful when a new system is coming online and you must set up access for many users at one time. You can do the Service and Resource assignment early knowing the assignment will take place on the appropriate go live date.

This section covers the following topics:

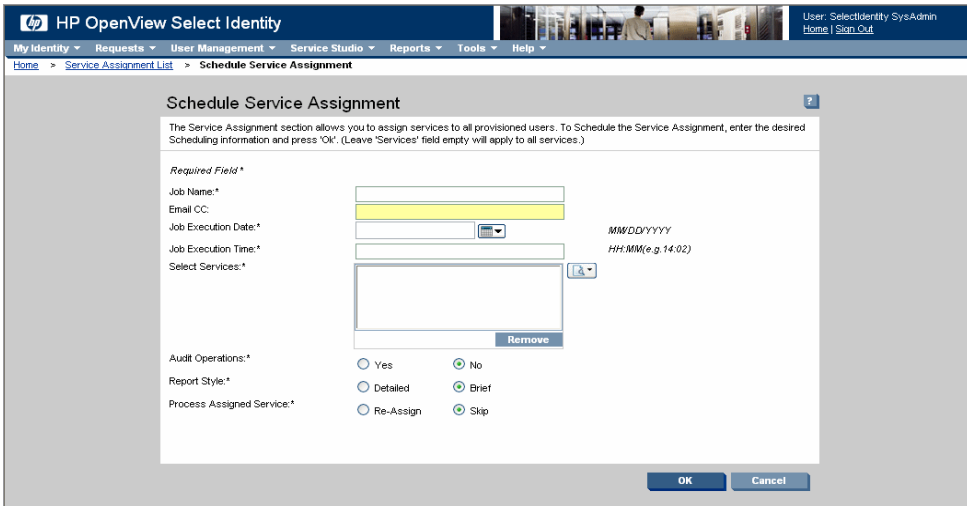
- Scheduling a Service Assignment
- Reviewing Job Results
- Viewing Service Assignment Reports
- Modifying Service Assignment Reports

Scheduling a Service Assignment

Perform the following steps to schedule assignments:

1 Select **Tools** → **User Import** → **Schedule Service Assignment**.
The **Schedule Service Assignment** page opens.

Figure 129 Schedule Service Assignment



2 Tab from field-to-field to enter the correct information:

Field	Action
Job Name	Enter a unique name for your job.
Email CC	Select Identity sends email to the administrator creating and running the job when the job completes. If you want an email sent to another administrator, enter an address in the Email CC field.
Job Execution Date	Click the **Calendar** icon to choose a date for this job to run. If you select the current day from the calendar, the job runs immediately
Job Execution Time	Enter the time in a HH:MM format you want the job to run on the date you specified earlier.

Field	Action
Select Services	Click the  icon to select the services you want to assign to provisioned users. Remove any service included on the list by clicking the resource and clicking the **Remove** button. Only highlighted services are assigned. If you do not select any services, all the services are included by default.
Audit Operations	Select the radio button indicating whether or not you want the assignment procedure audited.
Report Style	Determine whether you want an brief or very detailed report of the assignment results and select the appropriate radio button.
Process Assigned Service	If the user already has the service assigned, then the operation is skipped or repeated.

3 Click **OK**.
A dialog box opens asking if you want to create a new Service Assignment job.

4 Click **OK** again.
Schedules the service assignment job.

Reviewing Job Results

By default, the job resutls are emailed to the creator of the job request as a compressed HTML file.

To request and view a compressed job report from the Select Identity GUI, follow these steps:

1 Select **Tools** → **User Import** → **Service Assignment List**.
The **Service Assignment List** page opens.

Figure 130Service Assignment List Page

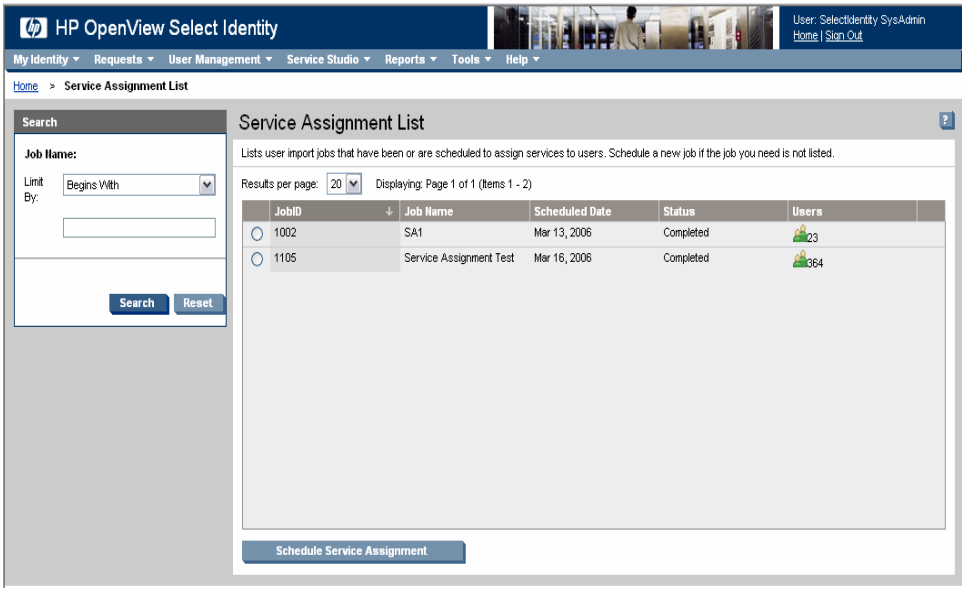
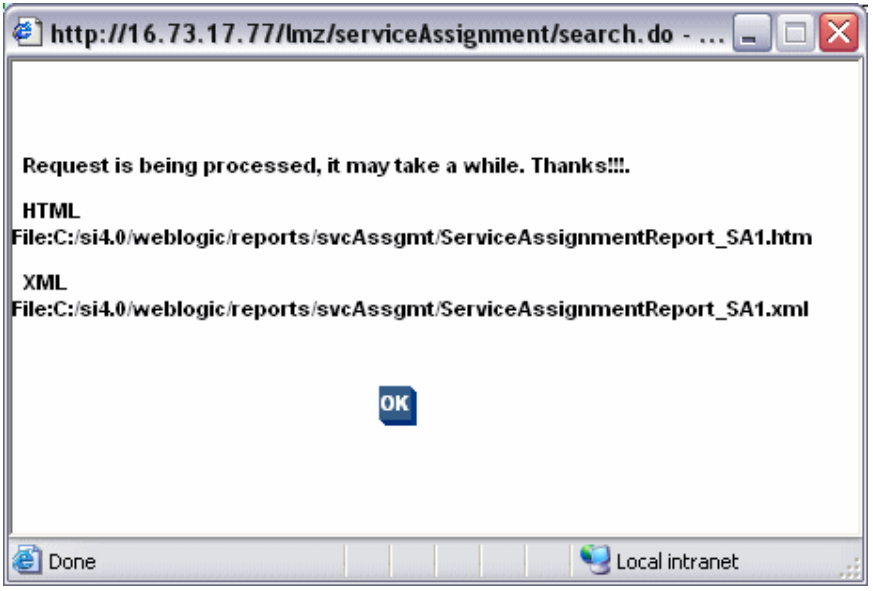


Figure 131Request Dialog



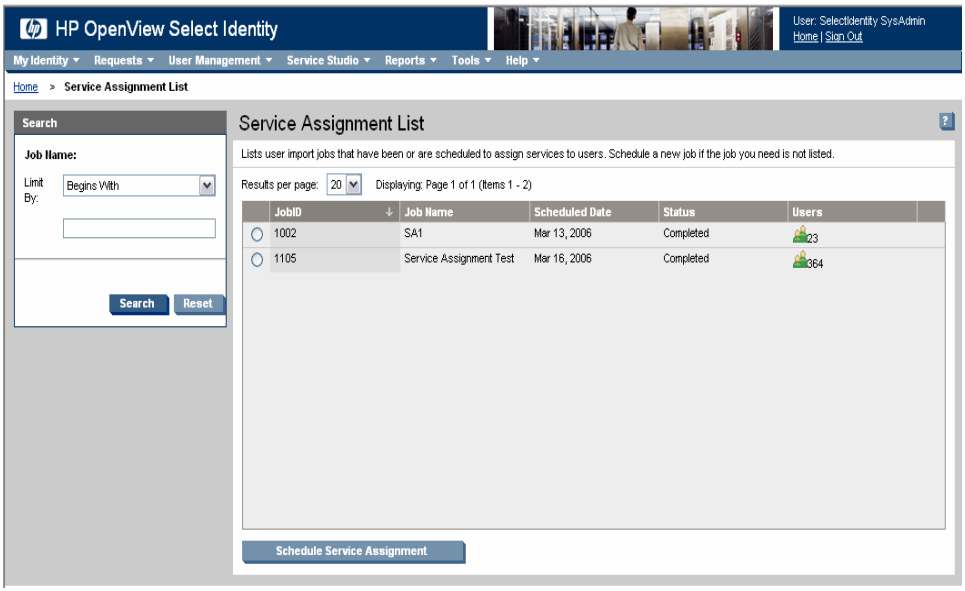
2 Click **OK**.

Viewing Service Assignment Reports

To view a job result, follow these steps:

1 Select **Tools** → **User Import** → **Service Assignment List**.
The **Service Assignment List** page opens.

Figure 132Service Assignment List Page



- The JobID
- The Job Name
- The Scheduled Date
- The Status
- The number of Users

Modifying Service Assignment Reports

A single service assignment report may e too big to read. In this case, the service assignment report is split into multiple segments and compressed together.

When the number of services to assign is greater less than five, a default segmentation is suggested. Otherwise, the segment size needs to be decreased.

The `TruAccess.properties` file specifies the size of each segment as follows:

`si.serviceassignment.report.partsize = X (default to 6000 users)`

6 External Calls

Select Identity workflow processes and attributes support the ability to perform actions on external systems. This functionality, called **External Calls**, enables integration of access approval processes with other business processes and systems. External system calls can also constrain or verify the value of identity attributes.

Select Identity supports the ability to invoke calls to external systems. You can use external calls to perform the following:

- Approver Selection — executes an external program to retrieve a list of workflow approvers
- Value generation — generates the values of an attribute
- Value constraint — provides a list of possible values for an attribute
- Value validation — validates the value of an attribute
- Value verification — verifies the value is what was previously saved. Used to verify passwords.
- Certification management — enables you to retrieve a certificate from an external system
- SPML request filter — invoked before an SPML request is processed
- Workflow action — performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems

You must code the classes called by external calls using the External Call API and Workflow API. After you create the Java file(s) that comprise an external call, you can register it with Select Identity through the External Calls capability. Refer to the *Select Identity External Call Developer Guide* for information about creating external calls.

The Select Identity External Call and Workflow APIs define a Java-based interface for creating external callouts. Although the Select Identity-facing

portion of the interface must be Java, it can be a “wrapper” for a program written in any language.

For workflow external calls, the APIs support synchronous communication. Select Identity requires the external system to complete its processing and provide status information as part of the callout, which is required to return status indicating how Select Identity will proceed with the workflow.

Default External Calls

Select Identity provides default external calls to enable you to interact with external systems. Each external call is within one of the following call types:

- Approver selection — searches an external system for a list of users who can approve provisioning requests during a workflow
- Attribute value generation — generates the name or ID of a user, the user’s password, and any other attribute, such as the user’s company, department and so on
- Attribute value constraint — provides a list of possible values for an attribute
- Attribute value validation — validates the value of an attribute
- Attribute value verification — verifies the value of an attribute
- CertificateManagementFunction - retrieves a certificate from an external system
- SPML Request Filter - used to process an SPML request
- Workflow action — performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems

Most external calls have predefined parameters you can modify. The following sections list and describe the functions of the external calls and their parameters, by call type.

ApproverSelection External Calls

Searches an external system for a list of users who can approve provisioning requests during a workflow.

WFGetApproverSampleExtCall

Sample external call that specifies a list of users to use for Approvals.

Parameters:

Parameter Name	Parameter Value Description
SampleApprovers	Comma delimited list of users to use for Approvals

AttributeValueGeneration External Calls

Attribute value generation generates the name or ID of a user, the user's password, and any other attribute, such as the user's company, department and so on. Following are the Attribute Value Generation external calls:

- IDValueGeneration
- PasswordValueGeneration
- UserIDValueGeneration
- ValueGenerateFunction

IDValueGeneration

Generates an attribute that is a unique number.

Parameters:

Parameter Name	Parameter Value Description
Suffix	Use after the number
Prefix	Use before the number

PasswordValueGeneration

Generates a password that can contain letters and numbers. Must contain at least one number, and the letters must be lowercase. Value is constrained by the minimum and maximum parameters. Special characters ("/", "+", "-") cannot be included.

Parameters:

Parameter Name	Parameter Value Description
minLength	Minimum length of the password
maxLength	Maximum length of the password

UserIDValueGeneration

Generates a UserID based on another attribute.

Parameters:

Parameter Name	Parameter Value Description
AttributeName	Attribute name from which the UserID is generated (such as from email)
Length	Length of the generated ID
MaxRetryAttempts	Maximum number of attempts that can be tried to create a unique ID

ValueGenerateFunction

Generates a value for an attribute based on specified parameters which can include other attribute values.

Parameters

Parameter Name	Parameter Value Description
Expression	Value to be generated; has attributes inclosed in brackets (example, [username]). Useful for combining attributes.

AttributeValueConstraint External Calls

Provides a list of possible values for an attribute. Following are the Attribute Value Constraint external calls:

- Search Connector
- Search Table

Search Connector

Constrains attribute based on the resource_name specified. This is automatically implemented by all entitlement attributes.

Parameters:

Parameter Name	Parameter Value Description
resource_name	Select Identity resource name

Search Table

Constrains attributes based on the specified query and valuefield. The query is executed using the specified poolname.

Parameters:

Parameter Name	Parameter Value Description
poolname	JNDI name for the data source and poolname for which the query is to be executed
query	Query invoked to look up valid values from the database dynamically
valuefield	Value from the query to use for constraining the attribute

AttributeValueValidation External Calls

Validates the value of an attribute. Following are the Attribute Value Validation external calls:

- IsAlphaNumeric
- ManageExpireValidation
- Password History And Dictionary Validation
- PasswordDictionaryValidation
- PasswordValidation
- ValidateConnector

IsAlphaNumeric

Validates if the attribute is alphanumeric — no parameters. An alphanumeric attribute must contain at least one letter and one number.

Parameters

None

ManageExpireValidation

Validates the value of the **ExpirationDate** attribute, which must be more than 30 days from the current date — no parameters. If the value of the **ExpirationDate** attribute is less than 30 days, an error message appears. This ensures the expiration date is after the date the notification email is sent, and requires the notification date to be after the current date. Thirty (30) days is the default notification date.

Parameter

None

Password History And Dictionary Validation

Function to validate the history and dictionary of the password attribute — no editable parameters. Combines functionality individually provided by **PasswordDictionaryValidation** and **PasswordHistoryValidation**.

Parameters

None

PasswordDictionaryValidation

Function to validate the dictionary check of the password attribute— no editable parameters. Checks to make sure the attribute value is not contained in an admin defined dictionary

Parameters

None

PasswordHistoryValidation

Function to validate the history of the password attribute— no editable parameters.

Parameters

None

PasswordValidation

Validates that the password contains at least the number of each type of characters specified.

Parameters:

Parameter Name	Parameter Value Description
Letters	Number of required letters
Numerics	Number of required numeric values
Lower Case Letters	Number of required lowercase letters
Upper Case Letters	Number of required uppercase letters

ValidateConnector

Function to check if an entitlement value(s) are valid— no editable parameters. This is automatically implemented by entitlement attributes.

Parameters:

Parameter Name	Parameter Value Description
resource_name	

AttributeValueVerification External Call

An external call executed when a user tries to log onto Select Identity. It is used to verify the user's credentials.

PasswordVerification

A simple password validation that checks that matches the entered password with the user's Select Identity password.

Parameters

None.

CertificationManagementFunction External Call

Implements validation and generation functions for the certificate. The Certification Management Function external call is VerisignCertImpl. For detailed information about Verisign certificate management, see Appendix E in the *HP Select Identity Workflow Studio Guide*.

VerisignCertImpl External Call

Called by the WorkFlowCertificateRequest external call, validates certificate requests — no parameters. For more information, see Chapter 2 in the *HP Select Identity Workflow Studio Guide*.

Parameters

None.

SPML Request Filter External Call

An external call that can be executed against a request prior to reconciliation workflow processing

ExtendedSPMLRequestFilter

Converts extended SPML requests into standard SPLML requests.

Parameters

None.

WorkflowExternalCall

Performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems. Following are the Workflow External Call external calls:

- ExclusionRuleCall
- LoadUserServices
- UserEnableDisableWFExtCall
- WorkflowCertificateRequest

ExclusionRuleCall

Function to execute the Exclusion rule

Parameters:

Parameter Name	Parameter Value Description
RuleName	Name of the rule to execute.
WFVariableName	Name of workflow variable storing the rule evaluation result.

LoadUserServices

Adds Services to a user based on context change. See Scenario: Adding Services to a User of the Workflow Studio Guide for an example of how to use this external call.

Parameters:

Parameter Name	Parameter Value Description
ServicesRule	Specifies the rule name

UserEnableDisableWFExtCall

Enables or disables a user based on the value stored in a specified attribute.

Parameters:

Parameter Name	Parameter Value Description
AttributeName	Attribute name for which the value is checked
EnableValue	If the value of the attribute of the user matches the **EnableValue**, then enable the user if the user is disabled
DisableValue	If the value of the attribute of the user matches the **DisableValue**, then disable the user if the user is enabled
UserName	Admin with authority to modify users that will be using this external call
Password	Admin's password
url	Webservices URL

WorkflowCertificateRequest

Manages certificates. For information on using this external call, see Chapter 2 in the *HP Select Identity Workflow Studio Guide*.

Parameters:

Parameter Name	Parameter Value Description
ExternalCallName	Name of the CA-specific Java class that implements validation and generation functions for the certificate.
CertificateProviderName	Certificate provider name. In the case of Verisign, the name must be “Verisign.” In all other cases, the administrator can assign the name.
EmailTemplateName	Default email template from Select Identity, to send email to the user.
CertificateFieldName	Challenge password assigned at the time of user registration.
DN_FieldName	Attribute name that stores the user’s distinguished name (DN) from the certificate.

Creating an External Call For Workflow Templates

Select Identity also allows you to create your own external calls. To create an external call, you must write the code that issues a request to the external system. See the *HP OpenView Select Identity External Call Guide* for complete information regarding the creation of external calls.

When the external call returns information, it must return data that is valid in Select Identity. For example, for Approval Lookups, the external call must return a valid user ID existing in Select Identity. Therefore, when you create the external call, provide a way for it to map the returned user ID to the Select Identity user ID.

If the external system cannot send the Select Identity user ID, the workflow process terminates and an error is sent.

After you create the call, copy the Class files or jar files to a directory on the Select Identity server. Copying the files to a directory in the Select Identity installation path saves you a step in the deployment procedure.

Creating an External Call for Attributes

You can assign external functions to different attributes for the following purposes:

- Value, which defines the acceptable values for an attribute
- Constraint, which constrains the attribute value to a particular format or requirement
- Validation, which calls an external program to validate the value of the attribute
- Verification, which verifies that the value is what was previously saved. This is used to verify passwords
- Generation, which automatically generates a value for an attribute

These functions are created and made available in the Select Identity system through the External Calls pages. For examples, see the *HP OpenView Select Identity External Call Developer Guide*.

Deploying an External Call

After you create the files you need to make the external call, you can deploy them through the Select Identity client. You can create external calls to enhance a workflow process or support attribute management.

Perform the following steps to deploy an external call:

1. Select **Service Studio** → **External Calls**.
   The **External Call List** page opens.
2. Click **Register External Call**.
   The **Register New Call** page opens. Fields marked with an asterisk (*) are required.
3. Enter a unique name for the new call in the **External Call Name** field.
4. If you choose, enter a description in the **Description** text box.
5. Enter the name of the class that implements the Java interface in the **Class Name** field.
6. Enter the fully qualified path to the interface in the **Class Path** field. It must be the full path of the class files or jar files.

   If the path is within the Select Identity installation path, this information is not required.
7. Select the type of call you are adding from the **Call Type** drop-down list. Choices for a workflow process are as follows:

Call	Purpose
Attribute Value Verification	verifies the value is what was previously saved. Used to verify passwords.
Certificate Management Function	implements validation and generation functions for the certificate.
WorkFlow External Call	Calls an external program or system during a workflow process.
SPML Request Filter	Filters the SPML data
Attribute Value Generation	Generates the value of an attribute.

Call	Purpose
Approver Selection	Executes an external program to retrieve a list of workflow approvers.
Attribute Value Constraint	Restricts the value of an attribute.
Attribute Value Validation	Validates an attribute value.

8 Click **Next**.
The **Set Parameters** page opens.

9 Enter the name and value for each parameter you want to pass to the external call. It may or may not be passed to an external system.

10 Click **Sensitive** if you want the value to be encrypted, such as for a password. If Sensitive is not checked, the value appears in plain text.

11 Click **Finish**.
The new call is registered with Select Identity.

Modifying an External Call

If you need to change the external call description, class path, or the parameters passed from Select Identity, you can modify this information in the Select Identity client.

Perform the following steps to modify an external call:

1 Select **Service Studio** → **External Calls**.
The **External Call List** page opens.

2 Select the External Call you want to modify.

3 Select **Modify**.
The **External Call Name: Basic Information** page opens.

4 Modify the **Description** and **Class Path** as necessary.

5 Click **Apply**.
Saves your work.

6 If finished, Click **OK** to return to the **External Call List** page.

7 To review the parameters or add or modify parameters to the External Call, click **Parameters** in the left pane.
The **Set Parameters** page opens.

8 Add a parameter by entering the **Parameter Name** and **Parameter Values**.

9 Review the **Sensitive** selection and change the value as necessary.

10 Clicking **Apply**.
The new parameter appears in the bottom panel.

11 Modify an existing parameter by selecting it and clicking **Modify**.
The parameter appears in the top panel.

12 Enter the corrections and click **Apply**.

13 Click **Apply**.

14 Delete an existing parameter by selecting the external call and clicking **Delete**.

Viewing an External Call

Perform the following steps to view external call settings:

1 Select **Service Studio** → **External Calls**.
The **External Call List** page opens.

2 If the external call you wish to view is not listed, enter the search parameters in the **Search** pane. For information on how to perform a search, see Using the Search Features in Select Identity on page 37 in. Getting Started. You can search by:

- Entering the exact external call name or first few letters
- Selecting the call type from the **Function Type** drop-down list, clicking **Search** and selecting the external call displayed in the list.

3 Click **View**.
The **Basic Information** page opens.

4 View the parameters associated with the call by clicking **Parameters** in the left panel.

5 Click **Cancel** to return to the **External Call List** page.

Deleting an External Call

Perform the following steps to delete an external call:

1 Select **Service Studio** → **External Calls**.
The **External Call List** page opens.

2 Select the external call you want to delete.

3 Click **Delete**.
Opens the confirmation dialog box.

4 Click **OK.**
Deletes the call.

7 Workflow Studio

The complexity of the workflow process can vary widely depending on your provisioning needs. You can simply provision a user by creating the user in Select Identity then pushing the user account to the external resource. Or, provisioning can require approval by multiple Select Identity administrators. The approval process may also rely on external calls to third-party systems or databases.

For example, when an employee is promoted to manager, the employee needs access to the company's HCM system to manage other employees. To support these new responsibilities, the employee must be granted new entitlements and access privileges. Before giving the employee access to these systems, upper-level management must approve the access requests and the employee must be created in the supporting systems.

Thus, the workflow process involves retrieving the names of managers, requesting their approval to add the employee to the HCM systems, provisioning the employee's account, and notifying the employee that authorization to manage others has been approved.

This chapter covers the following:

Workflow Studio Overview

Workflow Studio enables you to create the workflow templates representing the provisioning process. A workflow template models this process in order to automate the actions approvers and systems management software must

perform. The workflow process can also rely on an external call to a third-party system or database. See Default External Calls on page 240 for more information.

An administrator with access to Workflow Studio actions defines the workflow templates and processes by which users are added to, updated, or removed from the system. A workflow may require one or more steps before completion.

Each approver is notified by email when a new account needs to be reviewed. That administrator can then log in and access the **Worklist** section of the Select Identity client, where a **Pending Tasks** notification appears at the bottom of the home page, in the section titled **Requests**.

The template creation process can be as complex as your business security policies dictate. The *HP OpenView Select Identity Workflow Studio Guide* describes how to use Workflow Studio to create workflow templates and the building blocks you will use. The concepts and procedures for the Workflow Studio function are in the *HP OpenView Select Identity Workflow Studio Guide*.

Workflow Templates in Select Identity

Using the Select Identity client, you can assign workflow templates to request events in a Service Role. (A Service Role is created as part of a Service. See Defining Service Roles on page 164.) For example, you can assign a simple provisioning template to an add service request for self service. This template might perform user provisioning and request a single approval. Then, when a user requests access to the new service via the **Add Services** option on the My Services page, the template is invoked and an administrator must approve the request before the user is added to the supporting systems.

As Select Identity invokes a template, it creates a workflow instance and performs activities as defined in the template. (“Workflow” refers to a workflow instance.) If you create a more complicated workflow, activities might include the following:

- Selecting a list of approvers by specifying a role created on the Admin Roles page.

  See Administrative Roles on page 41 for more information.

- Sending email using one of the email templates created on the Notifications page.

  See Notification Variables on page 129 for more information.

- Executing an external call to access 3rd party systems.

  See External Calls on page 249

8 Users

The Select Identity Users function enables you to manage user accounts within your organization. The System Administrator delegates user management processes to one or more administrators by delegating the user management function for each administrator role and determining which user accounts are managed by which administrators.

The assigned administrators in turn, determine the Services made available to each account and the relevant attributes. As new users are created to access Services, workflow templates define the process by which Select Identity approves and provisions user requests.

Administrators should be familiar with your company's Service structure. Many of the actions performed in the Users section are dependant upon Service, context, and profile attribute information. See Service Studio on page 55 for information about Services and context. See Understanding Service Attributes on page 113 for information about attributes.

Select Identity allows you to search for users throughout Select Identity's other functional areas. User searches are based on the attributes making up the user account profile. Additional attributes for users are added through the `TruAccess.properties` file that can be used in searches. See the *HP OpenView Select Identity Installation and Configuration Guide* for information about the `TruAccess.properties` file

Access to each of these functional areas is determined by the administrative roles assigned to your account.

This chapter covers the following:

- Viewing Reports

Adding a User

When users are assigned and subscribed to services, Select Identity provisions the Resources to which they belong. Enable access to Services and Resources managed by Select Identity by adding accounts for users within your organization.

Complete the following procedures to create a new user:

- Creating a User
- Creating Context and Defining Attributes
- Subscribing to Services
- Viewing User Records

Creating a User

Follow the steps below to add a **User Account**.

1. Select **User Management** → **Create User**.
   The **Add New User: Select Services** page opens
2. Select each of the services you want to assign to this user account.
3. Click **Select**.
   Each selected service appears in the lower panel of the page.
4. Click **Next**.
   The **Add New User: Context** page opens.

Creating Context and Defining Attributes

Once you have determined what services the new user belongs to, it is time to place the user in a user group. Select the correct context user group and then define the user profile by completing the attribute fields that display. Available user group contexts are set up in **Services**. Context and Attribute fields vary according to the service and user group context selected. To learn more about context see Understanding Service Context on page 144.

Fields shown on this page depend upon the service and context selected.

5 Enter the context user group and click **Update**.
Associated context fields appear.

Notice each service you selected earlier appears in the left panel of the page. The highlighted service is the service you are currently updating.

Each service must be updated, however the information required depends on the attribute fields supported by the service. Many services have duplicate fields such as last name, company, email, etc. Once you enter information in a field once the same data is automatically populated when required by each additional service.

6 Review the attributes shown, then tab from field to field to make any updates necessary being sure that all required fields are complete.

The types of fields listed below are examples of typical user attribute fields. Each context user group has its own list of attributes. The fields shown depend upon the context selected.

Field Type	Action Required
Data Field	Type data in these fields.

Field Type	Action Required
Multi-Line Text Box	Enter text into the field, then click **Add** to insert it into the multi-line text box. Repeat the process until all data is entered. Delete unwanted data by highlighting the text and clicking **Remove** or by deselecting a highlighted item Only highlighted text is applied.
List Box	Click the  icon to add data to the list. Remove unwanted data by deselecting the text. Only highlighted text is applied.
Calendar	Click the  icon and select the date.

7 Click **Next**.
A confirmation message appears.

8 Repeat the process until all services have been assigned.

9 Click **Finish**.
Submit the request. The **User List** page opens

You can view the status of this request from **Request Status List** (**Requests** → **Request Status List)**. If the **Request Status** is "Completed — Success," the new user is created successfully. If the Request status is "In Process," and the corresponding Workflow shows the request is waiting for approval, an admin has to approve the request. Administrators use the Request Worklist to manage approvals (Requests → **Request Worklist)**. (See Approving or Rejecting Pending Requests on page 339.

Subscribing to Services

Once you have added the **User Profile** and selected the applicable services, you may want to subscribe the user to additional services. Follow the steps below to subscribe the user to additional services:

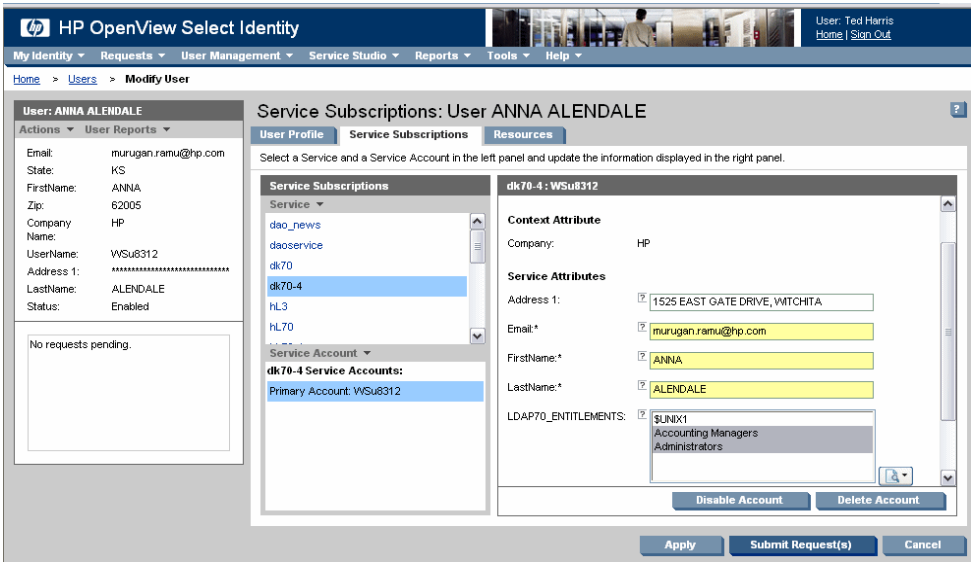
1 Select **User Management** → **User List** from the menu options.
The **User List** page opens with users presented in alphabetical order by last name.

2 Select the user record you want to modify.

3 Click **Modify**.
The **Modify** page for the user opens with the **Service Subscriptions** tab active.

4 Select **Subscribe to Service** either from the **Actions** drop-down menu in the top-left panel or the **Services** drop-down menu in the **Service Subscriptions** menu.
Opens the **Subscribe to Service: Select Services** page.

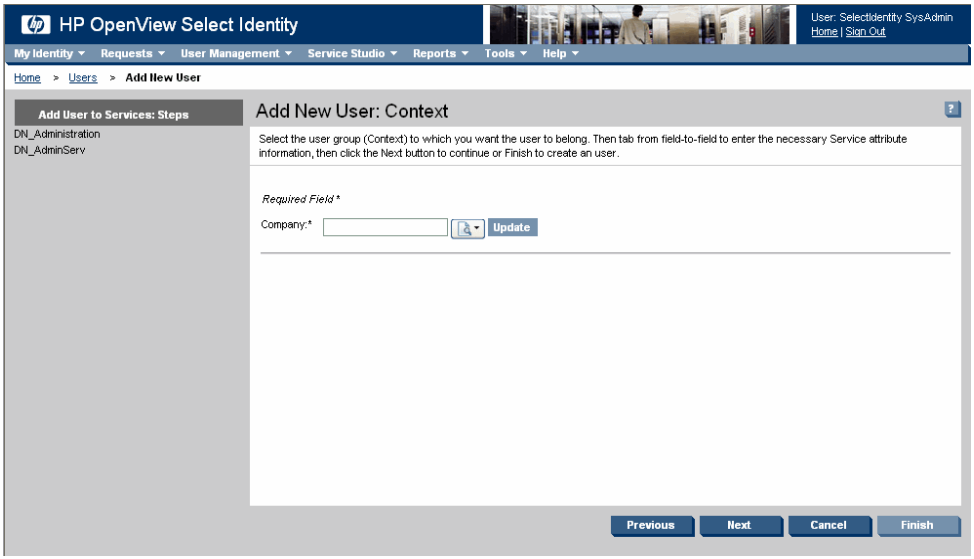
Figure 133 Modify User: User Name



5 Select the services you want to assign to the user.
Services appear in the lower panel.

6 Click **Next**.
Open the **Add New Users Details: Context** page.

Figure 134 Add New User Details: Context Page



7 Enter the context user group and click **Update**.
The **Add New User Details: Context** page opens.

If the same context attribute name, this page is skipped

8 Review the attributes shown, then tab from field to field to make any updates necessary being sure that all required fields are complete.

9 Repeat the process until all new services are updated.

10 Click **Finish**.
Submits the request and returns to the original page.

This only submits the request, it does not approve it. The person making the request may not approve it (if approval is required). See Approving or Rejecting Pending Requests on page 339 for instructions.

Clicking **Apply** creates a pending request in the current session for the changes made on the current page (**User Profile** or **Service Subscriptions**; the **Resources** tab is read-only). You may create as many pending requests as you want (by clicking **Apply**) while switching between the **User Profile** and **Service Subscriptions** tabs and changing the attribute values on those pages. All the pending requests are persisted (stored on the database) at once when you click **Submit Request(s)**. If you exit the **Modify User** setup without clicking **Submit Request(s)**, all the changes are lost. Clicking **Apply** stays in the same page whereas **Submit Request(s)** takes you back to the **User List**.

Upon clicking **Submit Request** or **Cancel**, you return to the **User List** page.

Enabling Services

Before enabling a service, first make sure it is disabled.

1. Select **User Management** → **User List** from the menu options.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Select the user record you want to modify.
3. Click **Modify**.
   The **Modify** page for the user opens with the **Service Subscriptions** tab active.
4. Select the service you want to modify in the **Service Subscription** panel.
5. Open the **Services** menu and select **Enable Service(s)**. The **Enable Service(s)** dialog displays. Select services and click **Enable**.
6. Click the **Process Request(s)** button.
   Returns to the **Service Subscriptions** page with a confirmation message.

Disabling Services

1. Select **User Management** → **User List** from the menu options.
   The **User List** page opens with users presented in alphabetical order.
2. Select the user record you want to modify.
3. Click **Modify**.
   The **Modify** page for the user opens with the **Service Subscriptions** tab active.
4. Select the service you want to disable in the **Service Subscription** panel.
5. Open the **Services** menu and select **Disable Service(s)**. The **Disable Service(s)** dialog displays. Select services and click **Disable**.
6. Click **Process Request(s)**.
   Returns to the **Service Subscriptions** page. The confirmation message with the request number appears at the top of the page.

Viewing User Records

Once you create a user account you can view it at any time. Selecting view rather than modify gives you view only access. You cannot make any changes. This section covers the following:

- Viewing Service Membership
- Viewing a User Profile
- Viewing Resource Assignments

Viewing Service Membership

Use the **User List** to view the attributes and values that make up a user account by following the steps below:

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by the last name.

2 Select the user record you want to view.

You can also search for the user as well using the standard **Search** panel or by clicking on the **Advanced Search** link for more search options. See Using Select Identity Search Features on page 17 to learn more.

3 Click **View**.
The **View** page showing the user's account opens with the **Service Subscriptions** tab active.

4 Select the service you want to view in the **Service Subscriptions** panel.
The associated accounts appear in the bottom left panel.

5 Click **Cancel** to close the form.
Returns to the **User List**.

Viewing a User Profile

Use the **User List** to view the attributes and values making up a user account by following the steps below:

1 Select **User Management** → **User List** from the menu options.
The **User List** page opens with users presented in alphabetical order by the last name.

2 Select the user record you want to view.

You can also search for the user as well using the standard Search panel or by clicking the **Advanced Search** link for more search options. See Using Select Identity Search Features on page 17 to learn more.

3 Click **View**.
The **View** page showing the user's account opens with the **Service Subscriptions** tab active.

4 Click the **User Profile** tab.
The **User Profile** page opens.

Fields displayed depend upon the attributes defined from the attributes as **Profile** attributes.

5 Click **Cancel**.
Returns to the **User List** page.

Viewing Resource Assignments

Use the **User List** to view the attributes and values that make up a user account by following the steps below:

1. Select **User Management** → **User List** from the menu options.
   Displays the **User List** page with users presented in alphabetical order by last name.
2. Select the user record you want to view.
3. Click **View**.
   Displays the user's account with the **Service Subscriptions** tab selected.
4. Click the **Resources** tab.
5. Select the resource you want to view in the **Resources** panel of the **Resources** tab.
   Displays the associated accounts in the bottom panel.
6. Click **Cancel** to close the form.
   Returns to the **User List**.

Removing Users

Users access rights to company resources need to be changed from time to time. A user may take a leave of absence, return to the job, or leave the company.

This section covers the following topics for removing a user's account from Select Identity:

- Disabling a User Account
- Enabling a User Account
- Terminating a User Account

Disabling a User Account

Follow the steps outlined below to disable a user's account. Disabled users may be re-enabled at any time by an Administrator with the correct authority level.

Do NOT disable a user's account if the user has left and is NOT expected to return. Instead see Terminating a User Account on page 288.

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user you want to disable
3. Click **Disable**.
   Submits a request to disable the user.

You can also click **Modify** and select **Disable User** from the **Actions** menu, then click **OK** from the pop-up confirm window.

You can view the status of this request from **Request Status List** (**User Management** → **Request Status List**).

Enabling a User Account

Once a user's account has been disabled the person cannot access the system until an administrator re-enables it.

Follow the steps outlined below to enable a disabled User.

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user you want to enable.
3. Click **Enable**.
   Submits a request to enable the user.

You can view the status of this request from **Request Status List** (**User Management** → **Request Status List**).

Terminating a User Account

Terminate a user's account when the user no longer needs access to system. Select Identity allows you to disable the user's account before it is removed from the system if the disable before terminate flag in TruAccess.properties is set to true (`truaccess.disable=true`). The `truaccess.disabledays=1` flag determines the number of days the account must be disabled prior to being deleted. If needed, you can enable the user's account during this suspended time period and prevent the termination. Once removed, it must be re-created before the user can access the system again.

Select Identity allows you the flexibility to schedule a user's termination for a date in the future. Use this feature when employees give notice they are leaving the company or when employees, consultants, or contractors are given a User Account only for a specified length of time. The **User Expiration Date** can be changed as often as necessary, allowing you the flexibility to handle extensions past the assigned expiration date as long as the user is still active.

When the expiration date arrives, the user is terminated from both OVSI and the resource if truaccess.disabled=FALSE in the TruAccess.properties file. See "Configuring TruAccess.properties" in the Select Identity Installation Guide for more information). Otherwise, if the TruAccess property reads truaccess.disabled=TRUE the user is first disabled on the expiration date and then terminated 24 hours later

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user record you want to terminate.
3. Click **Terminate**.
   The **Terminate User** page opens.

You can also click **Modify** and select **Terminate User** from the **Actions** menu, then click **OK** from the pop-up confirm window.

The top panel contains the **User Expiration Current Settings**. If the user has not been terminated, the fields are blank. If the user is awaiting termination, the fields show the following information:

- **Expiration Date** — the date scheduled for the user to be terminated from the system

- **Manager Notification Sent** — the message indicates how many days prior to the expiration date, a manager notification is sent. The default is {0} day(s) prior to expiration date.
- **Expiration Process Status** — shows the current status of the termination request. It displays one of the following values depending on the system date (today's date), expiration date and manager notification days:
  - **Ending** — if **System Date** is prior to "Expiration Date minus Manager Notification Days"
  - **In Progress** — if **System Date** is later than **Expiration Date minus Manager Notification Days**, but prior to **Expiration Date**
  - **Completed** — if **System Date** is later than **Expiration Date**
  - **Not Applicable** — if the user is not terminated

The bottom panel allows you to cancel a termination, change the termination date, or to establish the parameters for terminating a user. Use these fields to:

- **Remove Expiration Date** — cancel the termination
- **Terminate Now** — remove the user from the system immediately
- **Set/Change User Expiration** — has two additional fields:
  - **New Expiration Date** — click the calendar icon to select the date and then select the time.

Manager Notification — the default is 30 days.

4 Enter the information and click **Submit**.
Submits a request to **Terminate** the User Account.

This disables the user account and suspends access to all Services and Resources, in preparation for termination within 24 hours. The administrator can view the user status by viewing the user profile - termination date shown in the left panel.

You can also terminate a User's account from the **Modify User** page:

1 Select the user from the **User List.**

2 Click **Modify**.
The **Modify** page opens with the **Services Subscriptions** tab active.

3 Either click **Actions** in the left panel and select **Terminate User** or click the **User Profile** tab in the right panel and click **Terminate User** at the bottom of the page.

Maintaining User Service Accounts

User Accounts need maintenance for the user to have access to and / or be restricted from all the required Service Accounts. User Accounts must be modified in a timely manner to accurately reflect changes in the User's responsibilities within the company.

You may need to do any of the following:

- Defining the End User Role
- Modifying a User Profile
- Resetting Passwords

Defining the End User Role

Select Identity offers you the opportunity to delegate self administrative permissions to end users when users are logged into the My Identity function. Permissions granted here are granted to all end users with access to My Identity. However, end users ONLY have the authority to make changes to their own account. A user must have an Admin Role to make changes that affect other user's accounts. See Creating and Managing Administrative Roles on page 38 to learn more.

Specify the self administration permissions granted to an End User by following the procedure below:

1. Select **Tools** → **Admin Roles** → **Admin Role List** from the menu options.
   The **Admin Role List** page opens with roles presented in alphabetical order.
2. Locate and select the **End User** role.
3. Click **Modify**.
   The **Modify Admin Role: End User** page opens.
4. Click the **Permissions** link in the left panel.
   The **Modify Admin Role: Request Permissions** page opens.

5 Review the list of persmissions available and click the check box beside each permission you want activated or deactivated.

Permission	Result
Include All Permissions	Grants all permissions to the End User by selecting all of the available check boxes. Take great care before selecting this option. Make sure that you understand the ramifications of each selection before permitting all end users access.
My Identity	Authorizes end user access to the My Identity self service function.
Change Password	Permits end users to change their own password at will.
Change Password Reset Questions	Requires the user to select and provide answers to selected Challenge Response questions when setting up access to My Identity. These questions are used to identify a user before allowing access to self service **Change Password** and **Reset Password**.
View My Profile	Grants end users the right to view their own **User Profile**.
Modify My Profile	Authorizes end users to request changes to their own profile
View Request Status	Permits users to view the status of requests to modify their profiles and access to Services and Resources provisioned by Select Identity.
Add Service	Allows users to request access to additional Services.
Delegate Admin Role	Authorizes the End User to delegate their assigned services and resources to another End User if the user has administrative authority.
View Service Memberships	View Services subscribed to.
View My Role	View your own role

6 Click **Apply**.
Saves your changes.

7 Click on the **OK** button.
Submits your changes and returns to the **Admin Role List** page.

Viewing Service Membership

All Select Identity users automatically are assigned an End User Role. However, some users will have additional roles that give them additional privileges within the system. End Users with an Admin Role may view the services they are assigned to manage. They may only see those services assigned to them. They cannot services other End Users with Admin Roles are assigned to manage.

Follow the steps below to view service membership:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Select the correct user record.

3 Click **View**.
The **Service Subscriptions: User Name** page with the **Service Subscriptions** tab active opens.

4 View the list of services shown in the **Service Subscriptions** panel.

5 Select the service you would like to view.

6 Review the **Service Accounts** shown in the Service Account panel.

7 To view the resources assigned to the selected account, click the **Resources** tab.
The **User Resources: User Name** tab opens.

Viewing Managed Services

End Users with permission may view the services to which they are assigned. End Users may only see their own services. They cannot view services assigned to other users.

Follow the steps below to view service membership:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order.

2 Select the correct user record.

3 Click **View**.
The **Service Subscriptions: User Name** page with the **Service Subscriptions** tab active opens.

4 View the list of services shown in the **Service Subscriptions** panel.

5 Select the service you would like to view.

6 Review the **Service Accounts** shown in the Service Account panel.

7 View resources assigned to the selected account by clicking on the Resources tab.
Opens the **Service Subscriptions: User Name Resources** tab.

Modifying a User Profile

The User's Profile contains the user's contact information. An up-to-date profile is key to managing users well.

Follow the steps below to update the profile:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Select the correct user record.

3 Click **Modify**.
The **Modify User** page with the **Service Subscriptions** tab active opens.

4 Click the **User Profile** tab.
The **User Profile: User Name** page opens.

The left panel shows the **Actions** and **User Reports** for the selected user.

Clicking **User Reports** produces the list of available reports for the user. These reports are view only. To learn more about Reports, see Chapter 17, Audit and Configuration Reports. The center panel shows the available **Service Subscriptions** and **Service Accounts**. The right panel shows the attributes for the selected **Service Subscription**.

5 Review the user profile displayed and change any field as necessary.

Fields displayed depend upon the attributes defined from the attributes as Profile attribute.

6 Click **Apply**.
Saves your change request.

7 Click **Submit Requests**.
Submits the change request for approval and returns to the **User List**.

Resetting Passwords

Select Identity offers you the flexibility to determine whether an administrator should always reset passwords or users may reset their own. If the flag in TruAccess.properties is `com.hp.ovsi.forgetpassword.autogenerate=true`, Select Identity generates the password for the user. If the flag is `com.hp.ovsi.forgetpassword.autogenerate=false`, users can reset their own passwords. The system administrator establishes the number of times a user must set a unique password before reusing one.

When users are allowed to reset their own passwords OVSI uses a Challenge and Response method to authenticate the user. See Challenge Response Questions on page 307 for further information. Even when users are allowed to reset their own passwords there may be times when the assigned administrator should reset the password instead.

Passwords may be reset by an administrator three ways:

- Resetting a User Password for One or More Accounts
- Resetting a User Password for Specified Resources
- Resetting a Password for a Single Resource

Resetting a User Password for One or More Accounts

Use this method when you want the password change propagated across all accounts assigned to the user. Follow the procedure detailed below to reset a user's password:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Locate and select the user record.

3 Click **Passwords**.
The **Reset Password(s)** page opens showing all accounts assigned to the user.

> You can also click **Modify** and select **Reset Password** from the **Actions** menu.

4 Select the account password(s) you want to reset.
The page changes to show the **Password** fields.

5 Enter the new password in the **New Password** field.

6 Enter the new password once more in the **Confirm New Password** field.

7 Review the accounts listed.

If	Then
You need to change additional account passwords	Click **Reset Selected Password(s)** Opens a confirmation dialog box.
All password changes are complete	Click **Reset and Close.** Opens a confirmation dialog box.

8 Click **OK**.
Submits the request.

.

> If the associated workflow requires that password changes must be approved then the request is submitted for approval. If password changes do not require approvals an email notification is sent to the user verifying that the requested change has been made.

Resetting a User Password for Specified Resources

Some organizations require that users maintain different passwords for different types of systems and resources. When this is true, one or more passwords may need to be reset for predetermined resources, but NOT for all resources to which the user has access.

Follow the procedure detailed below to reset a user's password upon request:

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user record you want to update.
3. Click **Passwords**.
   The **Reset Password(s): UserID** page opens showing all resources assigned to the user.
4. Review the resources shown and select each resource with a password you want to change.
   Displays the password fields.
5. Enter the new password in the **New Password** field.
6. Enter the new password once more in the **Confirm New Password** field.
7. Review the accounts listed.

If	Then
You need to change additional account passwords	Click **Reset Selected Password(s)** Opens a confirmation dialog box.
All password changes are complete	Click **Reset and Close.** Opens a confirmation dialog box.

8. Click **OK**.
   Submits the request.

.

If the associated workflow requires that password changes must be approved then the request is submitted for approval. If password changes do not require approvals an email notification is sent to the user verifying that the requested change has been made.

Resetting a Password for a Single Resource

Use this method when you want the password change for a single resource. This is a convenient way of changing the password when the administrator is viewing the details of the user's account on a particular resource.

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user record.
3. Click **Modify**.
   The **Modify** page with the **Service Subscriptions** tab active opens showing all the services assigned to the user.
4. Click the **Resources** tab.
   The **User Resources** page opens showing all the resources on which the user has an account.
5. Select the resource for which you want to reset the passwords.
6. Click **Reset Password**.
   The page changes to show the **Password** fields.
7. Enter the new password in the **New Password** field.
8. Enter the new password once more in the **Confirm New Password** field.
9. Review the accounts listed.

If	Then
You need to change additional account passwords	Click **Reset Selected Password(s)** Opens a confirmation dialog box.
All password changes are complete	Click **Reset and Close.** Opens a confirmation dialog box.

10 Click **OK**.
Submits the request.

If the associated workflow requires that password changes must be approved then the request is submitted for approval. If password changes do not require approvals an email notification is sent to the user verifying that the requested change has been made.

Maintaining User Services and Resources

From time to time users' needs change. They may need additional services and Resources or they may no longer need some of the services and Resources currently assigned to them. Select Identify offers you the flexibility to maintain the user's accounts in a variety of ways.

This section describes how to perform the following tasks:

- Subscribing a User to a New Service
- DisablingUser Access to a Service
- Enabling User Access to a Disabled Service
- Deleting User Access to a Service
- Moving a User to a Different Context

Subscribing a User to a New Service

Often users need additional Services to give them access to Services and Resources they have not had before. Follow the steps below to add a new Service to the User's account:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Locate and select the user record you want to modify.

3 Click **Modify**.
The **Service Subscriptions** page opens.

4 Scroll through the list of **Service Memberships** assigned to the user in the **Service Subscriptions** panel to make sure the user has not already been assigned to the service.

5 Click the **Actions** drop-down menu in the left panel and select **Subscribe to Service...**
The Subscribe to **Service: Select Services** page opens.

> You can also select **Subscribe to Service(s)** by clicking the **Service** drop-down menu in the **Service Subscriptions** panel.

6 Select the service(s) you want to add to the selected user's account.

7 Click **Select**.
The selected service(s) appear in the lower panel.

8 Click **Next**.
Displays the **Add User to Service Set Context** page.

9 Tab from field-to-field to enter the correct information.

> The fields displayed vary based on the service you select. Items in list boxes must be highlighted to be updated. Click the  icon to add additional items to a Search List Box. Remove items from the list by deselecting each one to remove. Only highlighted items are applied.

10 Click **Finish**.
Saves your changes and submits the service subscription request.

11 Click **Cancel** to return to the **Subscriptions** page.

DisablingUser Access to a Service

Users may temporarily change positions, changing their access needs. Disable a service while it is no longer needed and then re-enable the same service when the user returns to their new responsibilities.

> If the user longer needs the service permanently, then delete the service instead. See Deleting User Access to a Service on page 302.

Follow the steps below to disable service memberships:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order.

2 Locate and select the user record you want to disable.

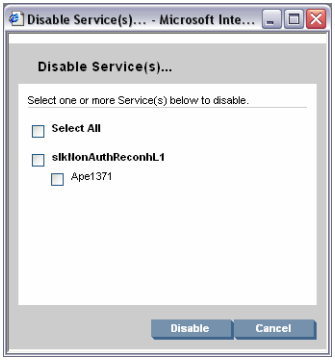
3 Click **Modify**.
The **Modify User** page with the **Service Subscriptions** tab active opens.

4 Scroll through the list of Services assigned to the user in the **Service Subscriptions** panel and select the service you want to disable.
Updates the associated resource list displayed in the bottom-left-panel.

5 Review the Service profile displayed in the right panel of the page to be sure you selected the correct service.

6 Select **Disable Service** from the **Service Subscription** menu.
A confirmation page opens and asks you to select the service (or all services)

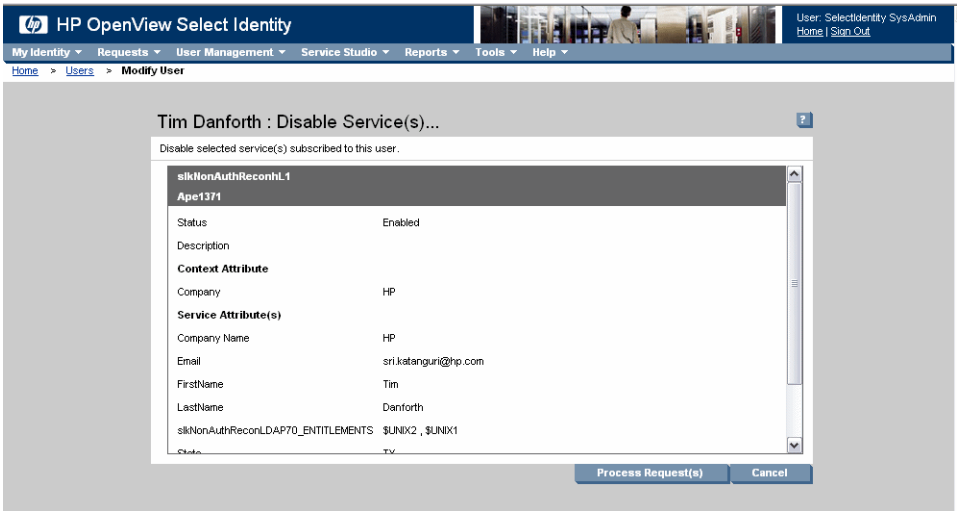
Figure 135Disable Service Confirmation Page



7 Select the service(s)

8 Click **Disable**.
The **User Name: Disable Service(s)** page opens

Figure 136 User Name: Disable Service Page



9 Click **Process Request** to disable the selected service for the user.
A confirmation message appears.ss

10 Click **OK**.
Returns to the **Service Subscription: User Name** page. A message confirming the disabling appears at the top of the page.

Enabling User Access to a Disabled Service

Enable a disabled service by following the steps described below:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Locate and select the user record you want to enable.

3 Click **Modify**.
The **Modify** page opens with the **Service Subscriptions** tab active.

4 Scroll through the list of Services assigned to the user in the **Service Subscriptions** panel and select the service you want to change.
Updates the associated resource list displayed in the bottom-left-panel.

5 Review the Service profile displayed in the right panel of the page to be sure that you selected the correct service.

6 Click **Enable Account**.
The **Enable Accoun**t page opens.

7 Click **Process Request**.
Displays the confirmation dialog box.

8 Click **OK**.
Enables the account and returns to the **User List** page.

Deleting User Access to a Service

Select Identity offers you the flexibility to customize user access to meet users ever changing needs. When a user changes responsibilities and no longer needs a Service membership, then delete the Service from the user's account. Even services that are part of a Context group to which the user still belongs can be deleted.

If it is possible that the user will need the service again, do NOT delete the service membership, instead temporarily disable the membership. See DisablingUser Access to a Service on page 299. If the user is leaving the company and will no longer be allowed ANY access then remove the user's account from OVSI along with all associated resources, see Terminating a User Account on page 288.

Perform the following steps to delete a user from a service:

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Locate and select the user record from which you want to delete the service.

3 Click **Modify**.
The **Modify** page with the **Service Subscriptions** tab active opens.

4 Scroll through the list of Services assigned to the user in the **Service Subscriptions** panel and select the service you want to delete.
Updates the associated resource list displayed in the bottom-left-panel.

5 Review the **Service**profile displayed in the right panel of the page to be sure that you selected the correct service.

6 Click **Delete Account**.
The **Delete Account** page opens.

You can also click **Service** and select **Unsubscribe From Service(s)** from the drop-down menu.

7 Click **Process Request**.
Displays the confirmation dialog box.

8 Click **OK**.
Returns to the **User List** page.

Moving a User to a Different Context

You can move a user from one Service context to another. For example, if a user transfers from the marketing department to the sales department, you can move the account from one entitlement structure to the other. If you need to move a group of users from one Service context to another, see Bulk Add or Move on page 341 for details.

Move User automatically adds entitlements and other attributes to a user when the context value is changed. Existing Services for the user are evaluated to determine what new entitlements or attributes are given to the the user. If you need to add additional Services to a user's account when moving a user, reference the Adding Services to a User scenario in the *HP OpenView Select Identity Workflow Studio Guide*. Select Identity enables you to add Services to a user based on a modification made to the user's context. By using rules and external calls from workflow, you can control what additional services are added to a user when the user is moved from one context to another.

To perform Move user, the Move User event must be defined in the service role and associated with correct workflow such as SI Bulk One Stage Approval, and the service view.

During the move the administrator can modify some user attribute values, and add or delete additional entitlements when it is applied.

If you need to move a user from one context to another, follow these steps.

1 Select **User Management** → **User List**.
The **User List** page opens with users presented in alphabetical order by last name.

2 Locate and select the user you want to move to a different context.

3 Click **Modify**.
The **Modify User** page with the **Service Subscriptions** tab active opens.

4 Review the information and complete any missing fields.

5 Select the **User Profile** tab.
The **User Profile** page opens.

You can also click **Actions** and select **Move User** from the drop-down menu.

6 Click **Move User**.
The **Move User** page opens.

7 Fill in the fields as required.

Field	Action
Context Attribute	Select from the list.
New Context Value	Click the  icon to find the new context

8 Click **Move**.
The **Confirm Move** page opens.

This page displays the following information:

— **Delete** - New context value is not a value available in the service. In this case, the user is deleted from the service (service that has static context, such as Company= HP only)

— **Modify** - New context value is available in the service. In this case, the user is modified in the service - all the user's information is updated based on the move transaction to a new context.

9 Modify any new values if necessary.

10 Click **OK**.
Returns to the **User List**.

Viewing Reports

User Management provides you with a variety of reports. The reports shown here can be used to help you better understand and manage individual users. Additional reports are available from the Reports menu bar option. Learn more about other reports by reviewing Audit and Configuration Reports on page 461.

Viewing User Reports

1. Select **User Management** → **User List**.
   The **User List** page opens with users presented in alphabetical order by last name.
2. Locate and select the user whose report you want to view.
3. Click **Modify**.
   The **Service Subscriptions: User Name** page with the **Service Subscriptions** tab active opens.
4. Click **User Reports** in the left panel.
5. Select the report from the drop-down list
   The selected report opens in a new window.

   There are three report types:

   - User Subscription Report
   - User Resource Report
   - User Audit Report
6. Print the report by right clicking and selecting **Print** from the floating context menu.
7. Click **Close**.
   The report closes.
8. Return to the **User List** page by clicking **Cancel**

9 Challenge Response Questions

Secure access to services is defined using attributes and challenge and response policies. The Select Identity Challenge/Response capability determines the generic security policy for the system.

The Select Identity challenge and response policy governs password hints for the system. You can restrict login attempts with this policy and force users to configure a password hint the first time they log in.

This chapter contains the following sections:

What is Challenge/Response?

Users sometimes forget their passwords; Select Identity can allow users to reset their password by anwering Challenge/Response questions. The user is asked a question (the challenge) and must provide the correct answer (the response).

In Select Identity, System Administrators create sets of standard challenges (questions). In the settings area, Administrators select the number of standard and personal questions the user must answer. Users create their own personal questions when they establish themselves in the system.

Formulating a good challenge question requires careful planning and forethought. In an increasingly global and multi-cultural world, a question may have relevance to some people and no relevance to others. This distinction is not always obvious. For example, in some countries, the

American standard challenge questions of “your mother’s maiden name” or “your father’s middle name” do not translate meaningfully because of cultural differences.

Modifying the Challenge and Response Policy

Perform the following steps to modify the Select Identity challenge and response policy:

1. Select **Tools** → **Challenge/Response**.
   The **Challenge/Response Settings** page opens.

The page has two sections: Challenge/Response Questions, and Challenge/Response Settings.

2. Make the desired changes.
3. Click **OK**.

Challenge/Response Questions

The Questions section allows you to:

- Adding a New Hint
- Modifying an Existing Hint
- Deleting a Hint

Adding a New Hint

Administrators can create one or more hints. The default is set to three.

Follow the steps below to add a new hint:

1. Select **Tools** → **Challenge/Response**.
   The **Challenge/Response Settings** page opens.
2. Type your question text in the Question field in the Challenge/Response Questions area of the page.
3. After checking the text for accuracy, click **Add** to add the question.
4. Click **OK** at the bottom of the page to save the changes.
   A confirmation screen opens

5 Click **OK**.
Returns you to the **Select Identity** home page.

Modifying an Existing Hint

To change the text of an existing hint:

1 Select **Tools** → **Challenge/Response**.
The **Challenge/Response Settings** page opens.

2 Select the hint question in the Challenge/Response Questions area of the page.

3 Click **Modify**. The question opens in the **Question** box.

4 Make the desired changes to the text and click **Apply** to accept the changes and **Cancel** to reject the changes.

5 Click **OK** at the bottom of the page to save the changes.
A confirmation screen opens

6 Click **OK**.
Returns you to the **Select Identity** home page.

Changing Challenge/Response Settings

Follow the steps listed below to modify Challenge / Response Settings.

To force the user to set hints at initial login:

1 Select **Tools** → **Challenge/Response**.
The **Challenge/Response Settings** page opens.

Response Settings are in the lower half of the page.

2 Tab from field to field to change any setting necessary.

Field	Action
Force Hint Set Up on Initial Log In	This makes it a required action to set up a password hint the first time a user logs in. Select **Yes** if you want to activate this feature.
Number of standard challenges required to reset a password	This sets the number of standard challenges that must be answered before the password can be changed. Enter the number required
Number of personal challenges required to reset a password	Sets the number of personal challenges that must be answered before the password can be changed. Enter the number required
Incorrect allowable challenge response submissions	Sets the number of incorrect challenge question responses allowed before password change access is blocked. Enter the number of incorrect submissions allowed before the account is locked.

3 Click **OK**.
A confirmation screen opens.

4 Click **OK.**
Saves the changes and returns you to the **Select Identity** home page.

Deleting a Hint

To delete a hint:

1 Select **Tools** → **Challenge/Response**.
The **Challenge/Response Settings** page opens.

2 Select the hint question in the Challenge/Response Questions area.

3 Click **Delete**. A confirmation screen opens.

4 Click **OK** to confirm and **Cancel** to reject the deletion.

5 Click **OK** at the bottom of the page to save the changes.
A confirmation screen opens.

6 Click **OK**.
Returns you to the **Select Identity** home page.

10 Managing My Identity

This chapter describes how to set up the My Identity self service function for end users. After users are added to the OVSI system, you can give them permission to perform some simple administrative tasks. This alleviates the burden of some of the most common administrative tasks from your IT or support staff.

To see how end users perform the My Identity tasks, see the *HP OpenView Select Identity My Identity User Guide*.

This chapter covers the following:

- Setting Up My Identity Tasks
- Setting Up Self-Registration

Setting Up My Identity Tasks

End users can perform My Identity tasks through the **My Identity** menu or panel, if you give them permission to do so. The following sections show how to give or remove permissions for the My Identity main tasks:

- Setting Up Profile Tasks
- Setting Up Password Tasks
- Setting Up Service Tasks

Setting Up Profile Tasks

You can give users permission to perform the following tasks to manage their identity profile through the Admin Role function (select **Tools** → **Admin Roles**).

- Viewing My Profile

- Modifying Profile Information
- Viewing Request Status
- Viewing Role Permissions
- Delegating or Removing Administrative Roles

Viewing My Profile

All users have permission by default, but you can remove this permission so that users cannot see their profile information.

Users can view the following information on the Home page or on the **My Profile** page (select **My Identity** → **My Profile**) about their account profile:

- UserID
- First Name
- Last Name
- Email address

Modifying Profile Information

You can give users permission to modify their profile information. Resource attributes that are mapped within OVSI are updated when user profile information is updated. The user cannot modify the OVSI unique UserID.

When given permission, users can modify their profile on the My Profile page as shown in the figure above.

If you do not give users permission to modify their profiles, the profile information appears as uneditable labels, and the **Submit** button does not display.

Viewing Request Status

If you have given end users permission to modify their profiles, passwords, or subscribe to a service, then also give them permission to view the status of their requests. See the *HP OpenView Select Identity My Identity User Guide* to see the end user View Request Status instructions.

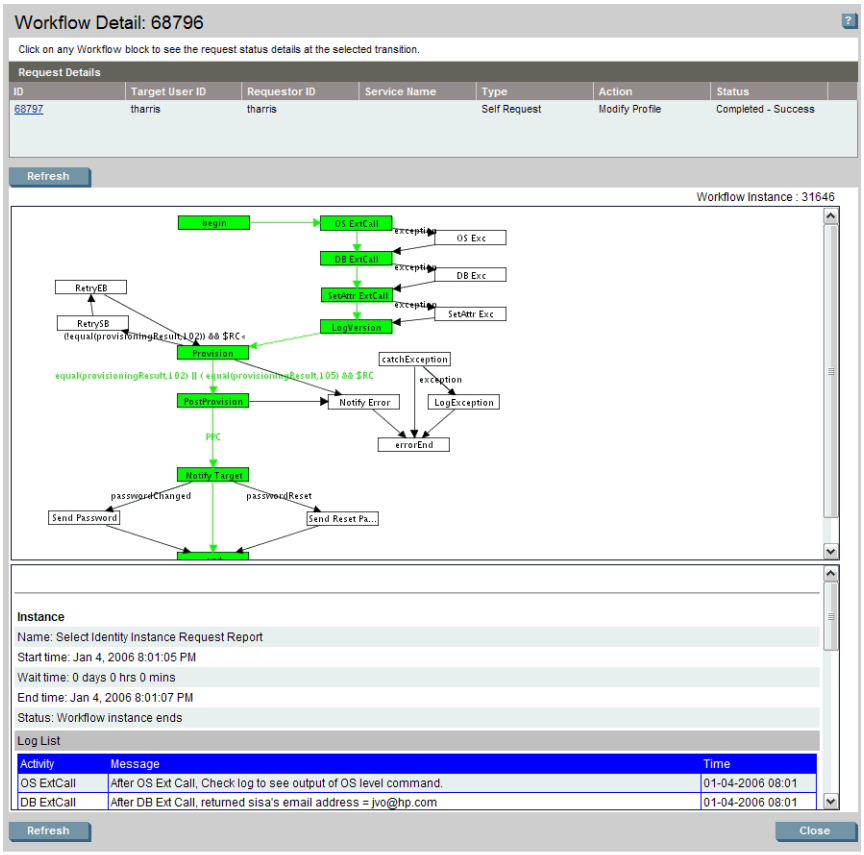
End users can view their request status by doing the following:

1. Select the **My Identity** → **My Requests** menu options.
   The **My Requests** page opens.
2. Select the Request ID you wish to view.
3. Click **View Request Status**.
   The **Workflow Detail** page opens. Pending requests for the user display in the left panel.

If you are an Administrator, Details of your role is delegated to the other administrator/end user displayed on the bottom of the left panel if it is applied.

See Viewing Request Status for a detailed description of this page

Figure 137 Sample Workflow Detail Page



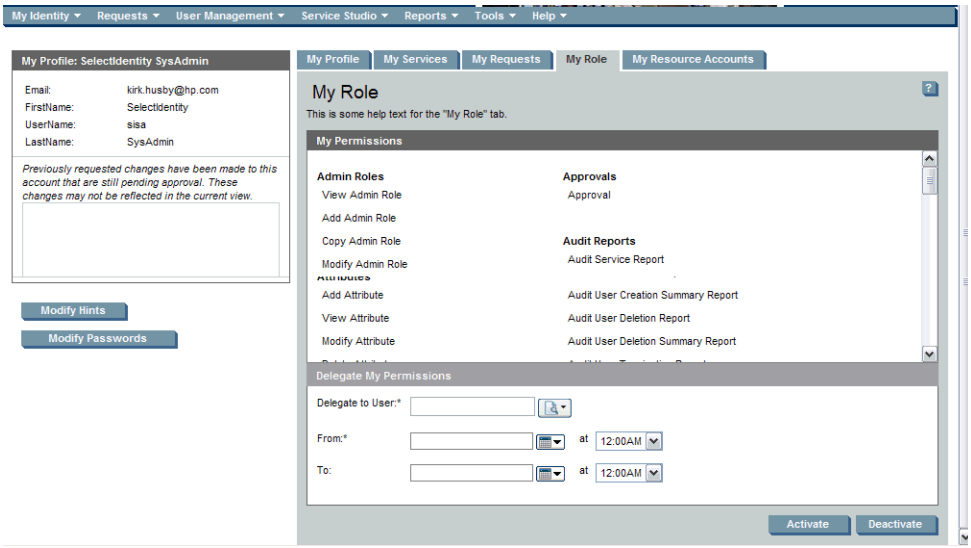
Viewing Role Permissions

Users can see their role permission only if they are granted the View Role Permissions.

End users can view their role permissions by doing the following:

- Select **My Identity** → **My Role Permissions**.
  The **My Role** page opens.

Figure 138 Sample My Role Page



The Delegate My Permissions section appears only for users with the **Delegate Admin Role** permission and **View My Role** permission. See the next section, Delegating or Removing Administrative Roles for instructions

Delegating or Removing Administrative Roles

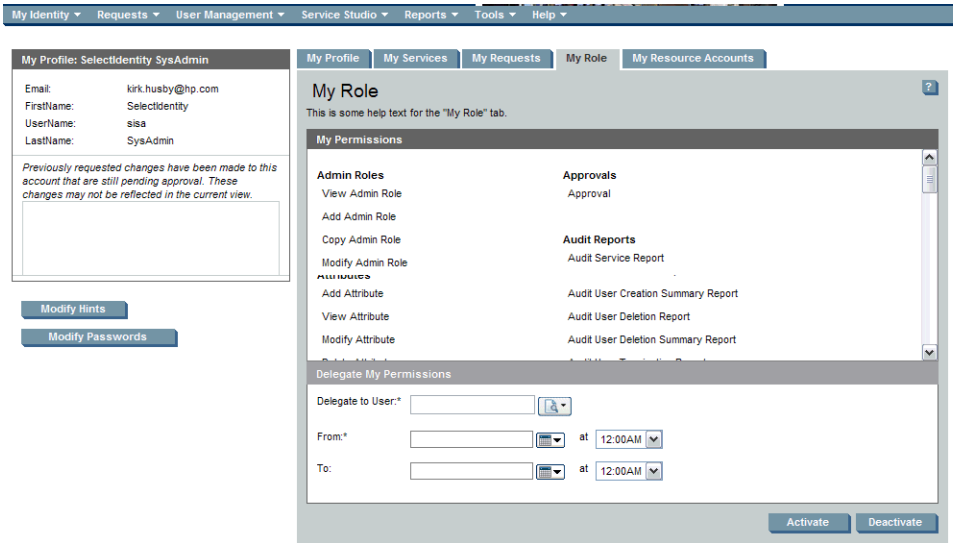
You can give users with administrative privileges permission to delegate their administrative roles to another OVSI administrator or end user within their Service context. Or remove roles that were delegated. Users can delegate their role for a specific period of time or an indefinite period of time.

You can also give end users the **View My Role** permission to allow them to view their own delegated role given to them. In order to do the Delegate Admin Role, the user must have the View My Role permission.

The following steps show how to delegate or remove delegated roles:

1 Select the **My Identity** → **My Role Permissions** menu options (or click the **My Role** link on the **My Identity** panel).
The **My Role** page opens.

Figure 139 My Role Page



On this page you can see which actions you have permissions to perform. The delegated user acquires all the same permissions.

The Delegate My Permissions section appears only for users with the Delegate Admin Role permission and View My Role permission. If you don't have View My Role permission, the My Role tab does not display.

2 Click the icon to locate and select a user to whom you want to delegate your role.

3 Click the calendar icon to select a date for the **From** field.

4 Select a beginning time for the **From** date.

5 Select a date and time for the **To** field if you want to specify a certain period of time.

6 Click the **Activate** button to activate the delegated request.

7 Click **Deactivate** to stop the request at any time, even if the delegation period has begun.
Submits the request.

When you deactivate a delegated request, the deactivation is immediate. If you have already delegated your roles to other users, their names and delegation periods appear in the left panel (below the pending requests). A drop-down list appears with the list of names, from which you can select a user to change the Activation or Deactivation period.

Setting Up Password Tasks

You can give users permission to perform the following tasks to manage their password tasks through the Admin Role function (select **Tools** → **Admin Roles**).

- Change Passwords Permission
- Change Password Questions Permission

Change Passwords Permission

You can give end users permission to change their Select Identity login password, or change their password or passwords on one or more Resources on which their account is located.

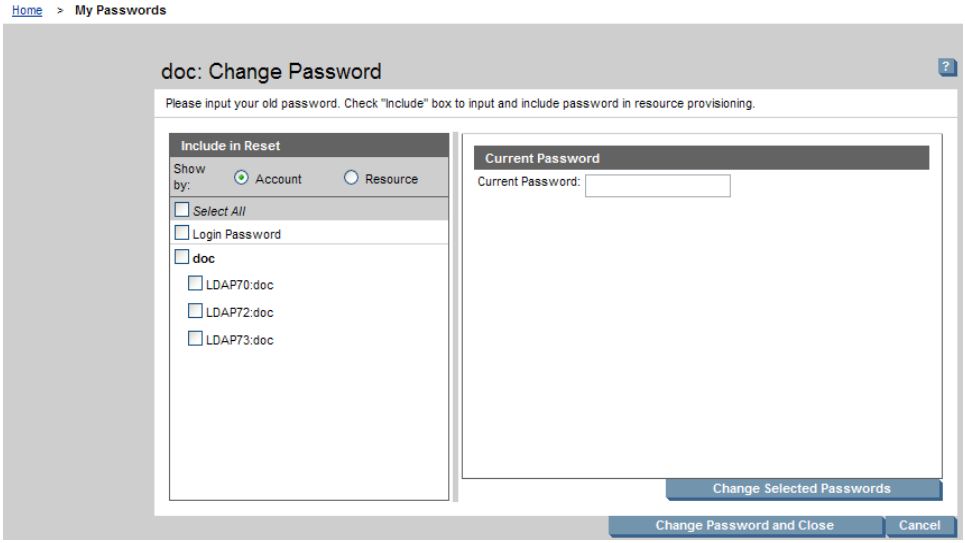
End users change their passwords by doing the following:

1. Select the **My Identity** → **My Profile** menu options or click the **My Profile** link in the **My Identity** panel.
   The **My Profile** page opens.
2. Click the **Change Passwords** button.
   The **Change Passwords** page opens.

   This page varies depending on whether the user account is on one resource or multiple resources. If the user does not **Change Password** permission, the Change Passwords button does not display.

   The following sample **Change Passwords** page shows multiple resources.

Figure 140 Sample Change Passwords Page with Multiple Resources



.

See Chapter 3 in the *HP OpenView Select Identity My Identity User Guide* for the complete end user Change Password instructions.

Change Password Questions Permission

You can give end users permission to change their password reset questions (hints).

You initially specify the password reset questions through the **Challenge/ Response** page. See Changing Challenge/Response Settings on page 309 for details on setting the password policies for users.

Users need permission to change their password questions before they can reset their passwords if they forget their password (see Change Passwords Permission on page 319).

End users can change their password questions by doing the following:

- Select the **My Identity** → **My Hint Questions** menu options.
  The **My Password Hints** page opens.

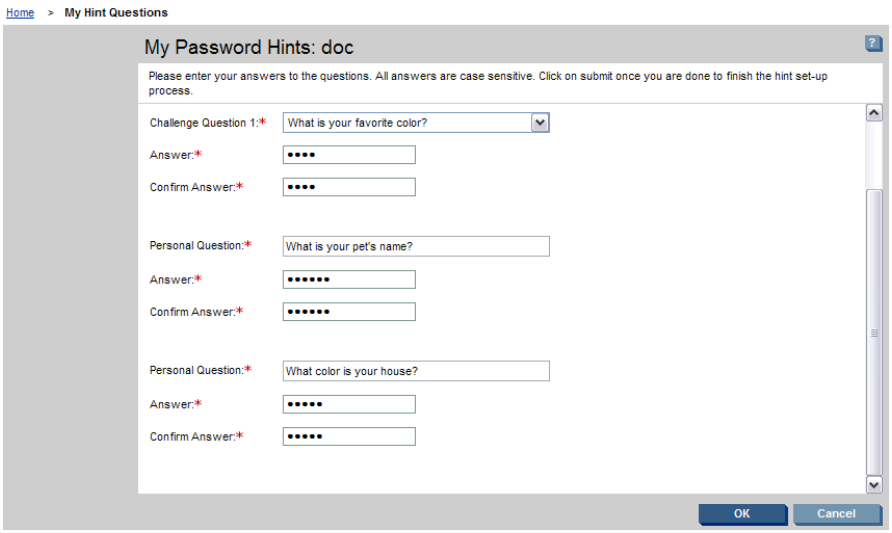
  Or you can select the **Modify Hints** button on the bottom of the left panel when you are on one of the other tabs.

  This page varies depending on how many questions you specified through the **Challenge/Response** page.

  If you do not give users Change Password Reset Questions permission, the Modify Hints button does not display, nor does the Modify Hints not display on My Identity menu list.

  Following is a sample **My Password Hints** page.

Figure 141 Sample My Password Hints Page



- .

See the *HP OpenView Select Identity My Identity User Guide* for the complete end user Change Password Questions instructions.

Setting Up Service Tasks

You can give users permission to perform the following tasks to manage their service tasks through the Admin Role function (select **Tools** → **Admin Roles**).

- View Services Permission
- Self-Subscribe Permission
- View Resource Accounts Permission

View Services Permission

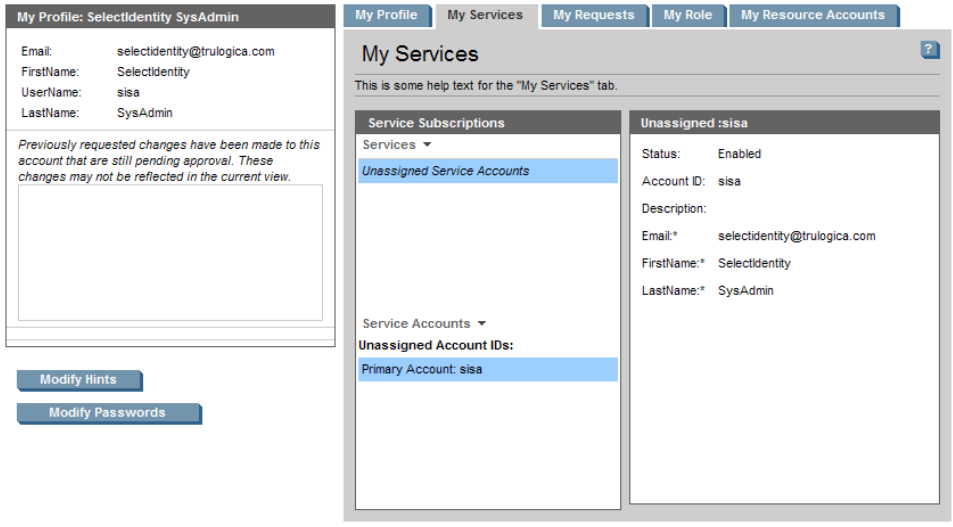
Users must have View Service Membership permission to view their services.

End users can view their services by doing the following:

1 Select the **My Identity** → **My Services** menu options (or click the **My Services** link on the **My Identity** panel).
The **My Services** page opens.

Following is a sample **My Services** page.

Figure 142 Sample My Service Page



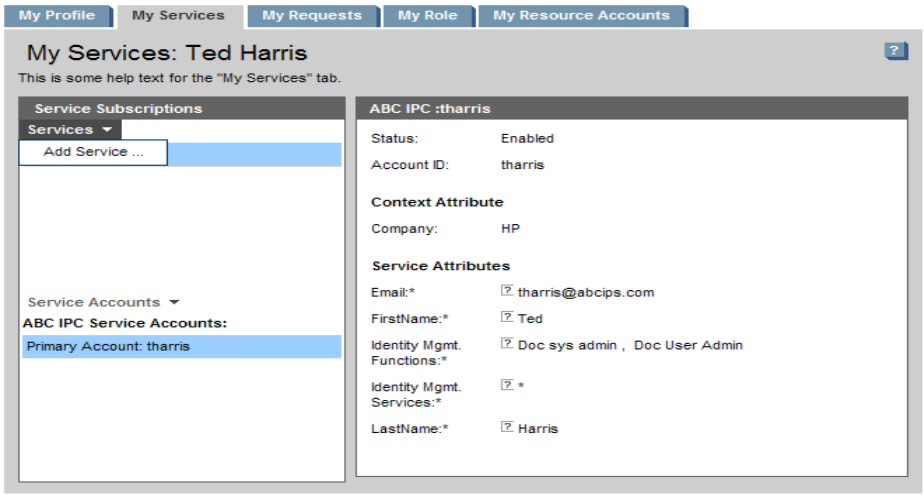
Self-Subscribe Permission

You can give end users permission to add themselves to additional Services.

End users can begin to subscribe themselves to a Service by doing the following:

1 Select **My Identity** → **My Services**.
The **My Services** page opens.

Figure 143 My Service Page with Add Service Selected



2 Click **Add Service** from the **Services** drop-down menu in the Service Subscription panel.

For end users who do not have permission to subscribe to a service, the **Services** drop-down menu does not display. For complete end user Subscribe to Service instructions, see the *HP OpenView Select Identity My Identity User Guide*. See also Subscribing to Services on page 280 for more information.

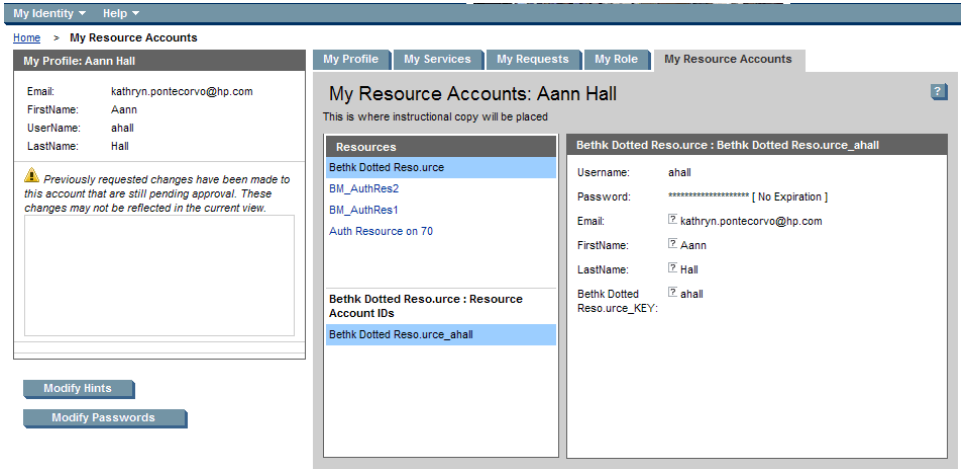
View Resource Accounts Permission

If you have given end users permission to view their profile information, they can also view their resource accounts.

End users can view their resource accounts by doing the following:

- Select the **My Identity** → **My Resource Accounts** menu options (or click the **My Resource Accounts** link on the **My Identity** panel).
  The **My Resource Accounts** page opens.

Figure 144 Sample My Resource Accounts Page



Setting Up Self-Registration

Users can add themselves to Select Identity through the Self-Registration process. (For a general description of workflow templates, see Workflow Templates in Select Identity on page 274, and for detailed information and examples, see the *HP OpenView Select Identity Workflow Studio Guide*.)

For a Service, the Self Add New User event must be defined with a workflow and view in the Service Role. The Self-Registration page opens differently based on how you configure it.

You perform the following tasks to set up Self-Registration:

- Configuring the Self-Registration Form
- Setting the Self-Registration URL

Configuring the Self-Registration Form

You can configure the Self-Registration form to open for the end user as one of the following forms:

- Self-Registration form with a pre-defined context and context value. See Adding a Service Role on page 169 for more information.
- Self-Registration blank form in which the end user selects the context.

For both these forms, the administrator can set the default self registration view in the service view (form) which displays what attributes should be on the first page.

You can also configure the Self-Registration form to display (true) or not display (`false`) the Schedule time field. This is done by setting the following property in the `TruAccess.properties` file, located in the`%InstallDir%\sysArchive` directory (see "Configuring TruAccess.properties" in the *HP OpenView Select Identity Installation Guide* for more information):

```
com.hp.si.selfreg.schedule = true
```

Setting the Self-Registration URL

When the Admin sets up the service, the user is sent an email notification with a specific URL to access the Self-Registration form. (For information about creating notifications, see Notification Variables on page 124.)

The URL you use determines which Self-Registration form opens first:

- Self--Registration Form with Predefined Context and Context Value
- Self-Registration Blank Form

Self--Registration Form with Predefined Context and Context Value

Specify the following URL, which is sent to the end user to open the Self-Registration form with a pre-defined context and context value. The context and context value are specified when you define the Service View. See Adding a Service Role on page 169 for details.

```
http://<host_name>:<port_num>/lmz/selfregistration.do?
serviceName=<service>&contextvalue=<value>&contextName=<name>
```

When the following is true:

- `<host_name>` is the application server (WebLogic or WebSphere)
- `<port_num>` is the server port number

- <service> is the service name
- <value> is the context attribute value
- <name> is the context attribute name

For example, if you replace the values with the following options:

- <host_name> is **localhost**
- <port_num> is **7001**
- <service> is **gvA1**
- <value> **HP**
- <name> is **Company**

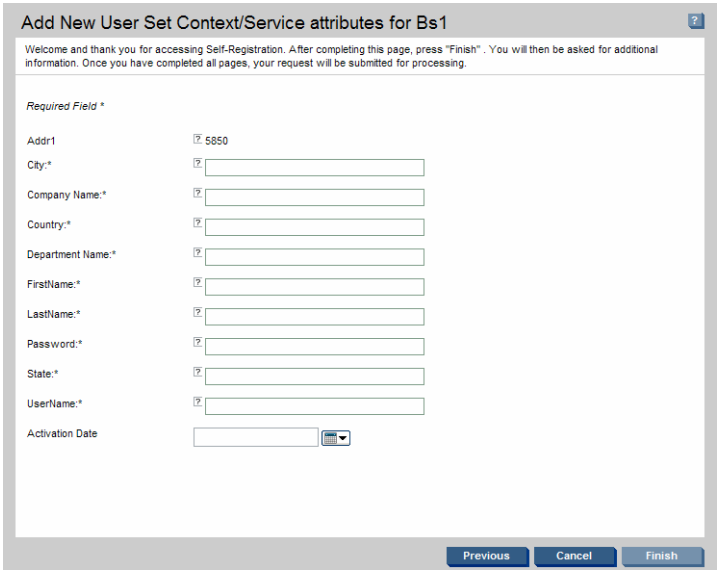
then the following URL would be correct:

```
http://localhost:7001/lmz/selfregistration.do?
serviceName=gvA1&contextvalue=HP&contextName=Company
```

The supporting service role must have a WorkFlow defined to handle the Add New User Self Registration event. To learn more about creating Service Roles see Adding a Service Role on page 169.

When the end user clicks on this URL, the **Register to Service: Service Name** page opens with the pre-defined context and context value. In Figure 145, the administrator has predefined the context (Addr1) and the context value (5850**)**.

Figure 145 Register to Service Form with Pre-Defined Context and Context Values



Self-Registration Blank Form

Specify the following URL, which is sent to the end user to open the Self-Registration blank form. This URL works for any service type (business, admin, and composite) as long as the event is defined:

`http://<host_name>:<port_num>/lmz/selfregistration/services.do?=serviceName=<name>`

When the following is true:

- `<host_name>` is the application server (WebLogic or WebSphere)
- `<port_num>` is the server port number
- `<service_name>` is the name of a Service that was specified in the workflow.

For example, if you replace the values with the following options:

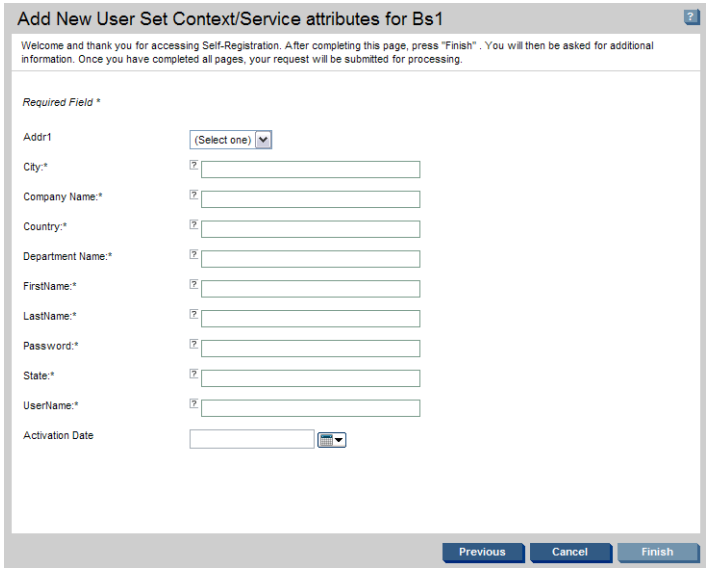
- `<host_name>` is Weblogic
- `<port_num>` is 7001
- `<service_name>` LDAP70

then the following URL would be correct:

```
http://WebLogic:7001/lmz/selfregistration.do?serviceName=LDAP70
```

When the end user clicks on this URL, the **Register to Service** page opens with blank fields.

Figure 146 Register to Service Form with Blank Fields



11 Request Status

The Request Status function enables you to view the complete transaction status for account events within Select Identity. You can view status whether or not the request has been initiated, if you have permission to see the account affected. Users who have Admin Roles can see every request for Users, Services, and Resources within their control by default. This default is set using the `com.hp.ovsi.parentrequestlist.contextcheck=true property` in the `TruAccess.properties` file.

End users make their own administrative requests with the appropriate permissions. However, they only see requests for their User Account if their role is configured to allow access to their own Request Status. See Defining the End User Role on page 290 for more information.

This chapter covers the following:

Viewing Request Status

Locate request status in one of two ways: Use the **Detailed Status** menu, in the left panel, to view requests by status:

- **All**: All requests regardless of status
- **Created**: Requests that have been created but not submitted for processing
- **In Process**: Requests that are being processed, with some processing actions complete.
- **Completed – Success:** Requests that have completed all processing without any errors.

- **Completed – Error:** Requests that have completed all processing steps without success.
- **Pending:** Requests that are paused and awaiting user intervention, such as approval.
- **In Process – Partial Failure:** Requests that are partially complete and that have completed one or more steps with errors. Requests that have this status will eventually end up with Complete - Partial Success or Complete - Error status.
- **Completed – Partial Success:** Requests that have finished all processing steps but not all steps were successful. For example, a request involving several resources may fail to complete on one resource, but process successfully on others.
- **Terminated:** Requests that a user has terminated from the browser interface.

Request Status enables you to view the status of account events based on the assigned workflow process. If the workflow template has multiple activities grouped into a block, you can view the status of those activities. Requests display from the most recent to the last for a default number of days. The default value is specified in the `com.hp.si.request.report.day` property in the `TruAccess.properties` file. You can change the default value by editing this property in the `TruAccess.properties` file.

If the default value is removed for `com.hp.si.request.report.day`, then Select Identity attempts to retrieve all the requests.

Viewing Request Status

Perform the following steps to view the status of requests:

1. Select **Requests > Request Status List**.
   The **Request Status List** opens.

2 Narrow the list of requests displayed by using the search options in the **Search** panel.

If you want to view...	Then
A specific request	Search for the request using the fields available in the first section of the **Filter** panel.
Requests within a specific time frame	Enter a time period in the **Period** section of the **Filter** panel.
Requests with a specified status	Select the status of the records you want to view in the **Detailed Status** menu on the **Search** panel.

➤ Change the number of items per page by selecting from the **Results Per Page** list.

3 Check the box beside the status record you want to view.

4 Click **View Request Status**.
The **Workflow Detail [*Request ID*]** page opens in your browser window.

5 Click a workflow block to view its status in the bottom panel.

6 To refresh the workflow, click **Refresh Image**.

7 Use the scroll bars. if necessary, to view all available information.

8 Click **Close**.
Closes the Workflow **Detail [*Request ID*]** page.

Terminating a Request

Sometimes requests do not process properly. In some cases, retrying the request (see Retrying a Request on page 332 for instructions) solves the problem. If it does not, you must terminate the request

Terminating a request stops the request where it is in the workflow process. A terminated request cannot be restarted, it must be recreated. Requests are terminated for various reasons, the most common, the request is caught in a

loop: it does not fail, but it hangs so that it continues in a loop without ever completing. Requests that have already completed successfully cannot be terminated.

Requestor and Approver are independent roles, assigned indvidually. Only a person with approval rights can approve requests. See Approvals on page 333 for information on **Approvals**.

Follow the steps below to terminate a request:

1. Select **Requests > Request Status List**.
   The **Request Status List** opens.
2. Click the radio button to the left of the request you want to terminate.
3. Click **Terminate**.
   Displays the Terminate dialog box.
4. Click **OK** to terminate the request or **Cancel** if you do not want to terminate the request.

Retrying a Request

If a request does not process properly, you may be able to solve the problem by retrying it. If the request remains incomplete, you must terminate it. See Terminating a Request on page 331 for instructions).

Follow the steps below to retry a request:

1. Select **Requests > Request Status List**.
   The **Request Status List** opens.
2. Click the radio button to the left of the request you want to retry.
3. Click **Retry Request.**
4. The remaining steps vary accirding to the request type. For example, there is an intermediate page when a request has multiple sub-requests such as adding a user to two services at once. In this case, click the radio button for each sub-request you want to retry.

   Select Identity displays a confirmation message when the request has been successfully placed, or alerts you with an error message if the retry fails, and the Request Status List reopens.

12 Approvals

The Approvals function enables you to manage change requests with an approval hierarchy specific to the needs of your organization. Each request may require one or more approvals based on the nature of the request. End Users and Administrators with approval responsibilities receive email notifications of requests waiting for action. Requests may be modified, approved, or rejected. However, a user's ability to modify a request depends upon the admninistrator roles assigned in Select Identity.

Approvals are managed by the Workflow. Workflow is the process by which Select Identity approves and provisions user requests for Services. These provisioning events include the modification, addition, and removal of accounts. Read more about Workflows in the *HP OpenView Select Identity Workflow Studio Guide*.

An approver added to the system after a set of requests are made does not have access to existing requests. The new approver does, however, have access to any requests made after the approver's account is enabled within Select Identity.

This chapter covers the following:

- Reviewing Requests
- Modifying a Pending Request
- Approving or Rejecting Pending Requests

Request Worklist Filters

The Request List may contain several pages of requests. Use the filters in the left panel of the page to filter out all requests that do not have the appropriate status. Requests can have three status designations:

- **Pending** — Requests which have neither been approved nor rejected.
- **Approved** — Requests that have been approved.

- **Rejected** — Requests that have been rejected.

Other UI features also reduce the matching items shown on any list page. Increase the Results Per Page, for example, to view more items on a single page, or use the page number list at the top right to jump to a new page.

Reviewing Requests

This page allows you to review the requests listed to do the following:

- Open the request
- Approve the request
- Reject the request
- View the request status

Perform the following steps to review pending requests:

5 Select **Requests** → **Request Worklist**.
Opens the **Request List** page.Narrow the list of requests shown by using the following features in the **Filter** panel on the left side of the page:

View	By
Requests by high level status (Pending, Approved, Rejected)	Select the status option (**Pending**, **Approved**, **Rejected**) in the list at the top left of the panel. The requests pertinent to the selected status appear in the **Request List**.

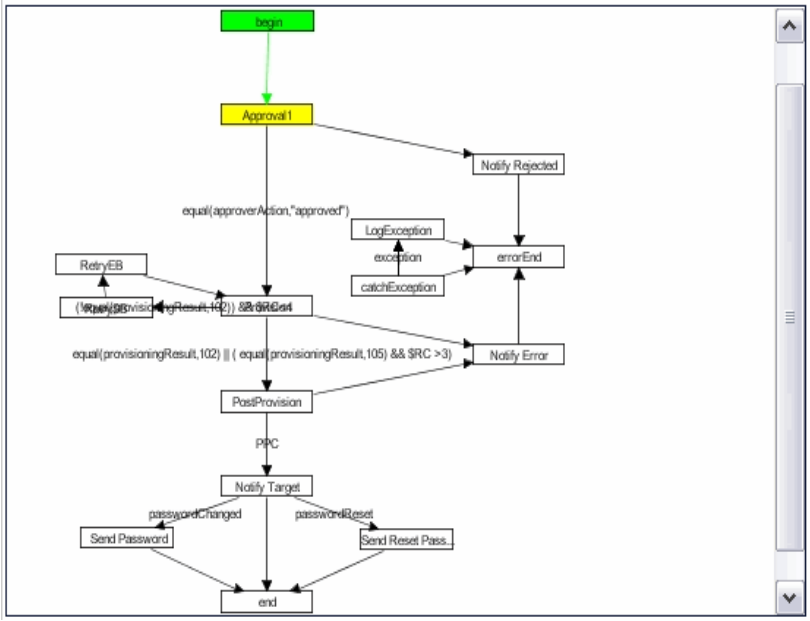
View	By
A specific request	Search for the request using the fields available in the first section of the **Filter** panel.
Requests within a specific time frame	Enter a time period in the **Period** section of the **Filter** panel.
Requests with a specified status	Select the status of the records you want to view in the **Detailed Status** drop-down menu on the **Search** panel: • Pending • Approved - Any Admin • Approved - Self Only • Rejected - Any Admin • Rejected - Self Only • Terminated • Time Out • All

Change the number of items per page that you can view by selecting the appropriate number from the **Results Per Page** drop-down list.

6 Check the box to the left of the request you want to view.
The record becomes highlighted on the page.

7 Click **View Request Status**.
Opens the **Workflow Detail** page in a new window. Learn more about the request in Viewing Request Status.

Figure 147Workflow Detail: ID page



This page is view-only.

8 Click a block in the workflow to view its detailed status information.Refresh the workflow if necessary by clicking the **Refresh Image** button.

9 Continue to review the workflow blocks until you have viewed all the information you need.

10 Click the **Close** button.
Closes the **Workflow Detail** page.

Modifying a Pending Request

Occasionally, you may need to modify a request prior to approval.

Keep in mind, the file is not locked against editing by others. More than one user with the appropriate permissions can make changes at the same time so take care not to work on a record being modified by another user.

Depending on the Workflow configuration, the change to the request may or may not need approval. See Workflows in the *HP OpenView Select Identity Workflow Studio Guide*.

Follow the steps below to modify a request:

1 Select **Requests** → **Request Worklist**.
Opens the **Request List** page.

2 Click all pending requests in the top left panel to see all pending requests, then select the request you wish to modify.

Only pending requests can be modified.

3 Click **Open**.
The **Modify Request Worklist** page opens.

.

The left side of the page shows a summary, including who checked out the request at what time. The appearance of the **Modify Request** page depends on the type of request. For example, the **Modify Request** page for **Bulk Move User** requests is different from the **Modify Request** page for **Add New User**. An admninistrative service request has an additional tab, **Managed Service**. For non-service requests (for example, **Modify Profile**), the fields are non-editable.

Modification page attributes are controlled (editable/visible) by the view specified for the service. The attributes presented to the approver when modifying come from the corresponding **Service View**. See Creating Services on page 148 for details on setting up a service view for the **Approval** block in the workflow.

4 Click **View Detail** in the left panel, under the **Status Summary**.
Opens the **Approval Status Detail** page.

.

This view-only page provides information about all the approvers who may approve this request, who has viewed the request, and who has given approval.

5 Click **Close** when you have reviewed the **Approval Status Detail** page.
Returns to the **Modify Request** page.

6 Tab from field to field to change any information necessary.

If	Then
Remove an account ID from the Request	Click the check box beside the account ID to remove the account from the request. Click **Remove**. Deletes the account ID, however, each request must have at least one account ID. You cannot delete the last account ID. **Reject** the request instead.
Review and make changes to a user's Services or entitlements	1 Click the check box beside the account ID you want to modify. 2 Review the services or entitlements listed. 3 Click the  icon to add items to the list, then highlight those services or entitlements you wish to keep. 4 Deselect any services or entitlements you do not wish to grant. 5 Click **Apply,** in the bottom right corner of the main panel. Saves the changes. 6 Repeat the process to make changes for additional account ID.
Clear Changes	Remove unsaved changes by clicking **Reset,** in the bottom right corner of the main panel. Cancels any unsaved changes to user service attributes.

7 Make any comments concerning this request by entering them in the **Comments** field in the lower left panel.

Comments are saved only if you **Approve** or **Reject** the request. Leaving the request in **Pending** status does not save the comment.

8 After making your changes, you can do any of the following:

Action	Result
View the status request	View the status of the request
Approve the request	Return to the **Request List**
Reject the request	Return to the **Request List**
Click **Cancel**	Return to the **Request List**, leaving the request in **Pending** status. You will lose any comments you entered in the **Comments** field in the left panel.

Approving or Rejecting Pending Requests

Follow the steps below to approve or reject a request:

1 Select **Requests** → **Request Worklist**.
Opens the **Request List** page.

2 Locate and select the request you want to open.

3 Determine the action you want to take.

If	Then
You want to review the request before you decide	Follow the step to Reviewing Requests onpage 334.
You want to approve the request	Click **Approve**. Opens the confirmation dialog. Approves the request and either notifies the next level approver or the user by email that the request is Approved, when an action is configured to do so. Initiates the change.
You want to reject the request	Click **Reject**. Opens the confirmation dialog. Rejects the request. Sends an email notification to the appropriate parties, when an action is configured to do so.

13 Bulk Add or Move

Select Identity allows uploading of multiple user accounts to multiple Services. This enables you to populate your system without having to add hundreds or thousands of individual user accounts. Use **Bulk** for accounts not already existing in a resource or in the Select Identity system. Accounts are added to both the Services you select and the resources supporting it. You can also add existing users to different services.

User accounts are uploaded to the system using an SPML data file. The data file maps all Select Identity attributes defined for a Service to the new accounts. Unlike Reconciliation and User Import, bulk file uses SI attribute names, not resource attribute names.

This chapter covers the following:

Bulk Dependencies

Before running a bulk job, ensure the following dependencies are met:

- Connectors and resources are deployed for systems for which you want to upload data.
- All necessary resource and Select Identity attributes are mapped within the connector mapping files and Select Identity Attributes function.

- One or more Services are created to use the resources with which you want to upload data and the default workflow template for bulk jobs (`SIBulkOneStageApproval`) is associated in the service. You can also create and assign a custom template. See the *HP OpenView Select Identity Workflow Studio Guide* for information about workflow templates.
- Two event handlers are added in the service you want to add to users:
  - Bulk - add new user
  - Bulk - add service

  The event handler is set in the service (business role) to validate the request. If it is not added, the bulk job fails.

Make sure the following is in place when creating the SPML data file:

- The file name must begin with an underscore `(_)` if it is used by an automated job and stored in the `reconroot` directory. Select Identity reads data files from the `reconroot` directory and the underscore enables the system to differentiate bulk upload files from reconciliation files. If the files are uploaded using onetime task, there are no naming restrictions.

The property `"com.hp.ovis.spml.resourcename.separator=+"` is set, then the file name should begin with (+), if it is used by an automated job and stored in `reconroot` directory.

- You can specify the Services to which you want to add users through the job creation pages or in the data file. You can specify services to which to add users at batch level, request level, or you can choose it when you upload the job from the UI.

```
</xml version-"1.0" encoding="ISO-8859-1"?>

<batchRequest xmlns:countries="countries.uri"
smlns:cities.uri"
smlns:dsml="urn:oasis:names:to"DSML:2:0:core"
xmls:spml="urn:oasis:names:tc:SPML:1.0"
xmls="urn:oasis:names:tc:SPML:1.2" requestID="1085774668899>
```

Batch Level

```
<operationalAttributes smlns="">
<attr
name="urn.trulogica:concero:2.0#keyFields"><value>UserName</
value></attr>
</operationalAttributes>
```

Request Level

```
<addRequest requestID="7">
   <operationalAttributes xmlns="">
       <attr name="urn:trulogica:concero:2.0#serviceName">
             <value>dkserLDAP72</value>
       </attr>
   </operationalAttributes>
```

Common to Both

```
   <attributes xmlns=""
       <attr name="FirstName"><value>Auto2</value></attr>
       <attr name="LastName"><value>Auto2</value></attr>
       <attr name="UserName"><value>Auto2</value></attr>
       <attr name="Password"><value>abc123</value></attr>
       <attr name="Company"><value>HP</value></attr>
       <attr name="State"><value>TX</value></attr>
       <attr name="SSN"><value>345678987</value></attr>
       <attr name="ExpirationDate"><value>2006-12-01</
value></attr>
       <attr name="Email"><value>joseph.doe@hp.com</value></
attr>
       <attr name="Date"><value>2006-02-01</value></attr>
       <attr name="State"><value>TX</value></attr>
       <attr name="Zip"><value>12345</value></attr>
       <attr name="Info>
             <value>val1</value>
             <value>val2</value>
        </attr>
       <attr name="dkLDAP72_ENTITLEMENTS">
             <value>Group4</value>
             <value>Group5</value>
       </attr>
   </attribures>
</addRequest>

</batchRequest>
```

Request Level has the highest priority, then batch level. If there is no service in either place, then you need to specify the service from the UI when you upload a job. If you do not, the job fails. If the data file does not meet the service constraints, the job fails.

All of the attributes required for registration to this Service must be represented in this file. If one of the required attributes is not represented here, the addition of the account fails. Unlike regular add, required attributes are defined in Attribute Properties of the particular service you are trying to add. Required attributes are not defined in the service view for bulk.

- Each account added must have a unique user ID within Select Identity. When adding accounts, you can specify a key for the user name for each addition.
- Avoid using the bulk upload process for Services having multiple resources with different resource key fields.
- If the data file has no entitlements listed and you attempt to add a user to a service that has defined entitlements, then the user gets added to that entitlement.

Bulk Procedure Overview

Select Identity bulk jobs use the same SPML data file type as discussed in Create an SPML File Containing Users and Attributes on page 345. This file should include the new account information and attributes required by the Services to which you are adding. The file is then uploaded to Select Identity.

The Select Identity installation establishes several settings in the `TruAccess.properties` file to enable bulk jobs:

```
truaccess.upload.filedir=c:/si4.0/weblogic/upload
truaccess.upload.maxfilesize=10485760
```

The first line specifies a temporary directory the bulk upload can use, and the second line specifies the maximum file size in bytes.

See the *HP OpenView Select Identity Installation and Configuration Guide* for details about this file and its properties.

You must have the Select Identity system administrator role with bulk permission granted to perform bulk tasks.

You may need to increase the JTA time-out seconds to 300 on WebLogic for bulk jobs to work properly.

This section describes the procedures for performing bulk jobs:

- Check the Application Server Properties
- Create an SPML File Containing Users and Attributes
- Upload Data Files
- Viewing Job Results

Check the Application Server Properties

Set up the necessary parameters in the `TruAccess.properties` file and create relative directories on the application server host. For instructions in establishing the parameters, consult the *HP OpenView Select Identity Installation and Configuration Guide.*

Set the following are key properties in the `TruAccess.properties` file to facilitate the upload process.

- `truaccess.batch.inprogresstimeout=18000000`
- `truaccess.batch.reportdir=c:/temp/reports`

The *HP OpenView Select Identity Installation and Configuration Guide* describes this file in detail. See Application Server Properties on page 427 for more information about bulk and reconciliation-specific property settings.

Create an SPML File Containing Users and Attributes

All attributes specified in this file are Select Identity attributes, not resource attributes. The `requestID` for each request must be unique to reflect properly in the results report. When the request fails or the user name cannot be parsed, Select Identity uses the `requestID` to indicate the error location in the original SPML file.

The file must begin and end with `<batchRequest></batchRequest>`.

Each account to be added begins and ends with `<addRequest>` `</addRequest>`.

When creating the data file containing the user attributes, specify the unique identifier attribute associated with each user. The `<operationalAttributes xmlns=>` section of the SPML file specifies the identifier and is designated as a

value in the keyFields attribute. Select Identity's default attribute for identifying accounts is **UserName**. The following is a sample of this section of the SPML file:

Batch Level

```
<operationalAttributes xmlns="">

   <attr name="urn:trulogica:concero:2.0#keyFields">
   <value>UserName</value></attr>
</operationalAttributes>
```

The "urn:trulogica:concero:2.0#keyFields" operational attributes specify the field in an individual request to use to check for the existence of a user in Select Identity. If this field is not provided, no check is performed and the job generates a create user internal event. If a the user already exists, the job generates an add service internal event.

In addition to specifying the operational attribute in the header of the file, you can specify operational attribute values for the Services you want assigned for each add user request:

Request Level

```
- <addRequest requestID="1">
    - <operationalAttributes xmlns="">
      - <attr name="urn:trulogica:concero:2.0#serviceName">
          <value>FinanceService</value>
        </attr>
      </operationalAttributes>
    - <attributes xmlns="">
      - <attr name="UserName">
          <value>JohnB</value>
        </attr>
      - <attr name="Password">
          <value>abc123</value>
        </attr>
      - <attr name="Email">
          <value>johnb@company.com</value>
        </attr>
      </attributes>
    </addRequest>
```

Use the following methods to specify the **Services** you want assigned to users:

- Specify the **Services** in the batch level of the file to add all users to all add requests in the file.
- Specify a group of common **Services** listed in the batch level of the file and add others specific to the user within the user's add request (as displayed above). Request level **Services** take precedence over those at the batch level
- If you specify Service 1 in the batch level and Service 2 in the request level, the user is added to both services.

The attributes listed for each account are the Select Identity attribute names defined in this Service through the Services pages. The attribute name must match the field name exactly. If a required field is missing or a data field does not meet the service constraints, an exception is listed in the results file. See Building a Service on page 149 for more information.

Example: Adding Users to Services with Common Attributes

The following example adds one user to the Finance Service and another user to the Finance and Market Services. The listed attributes are required attributes for the Services.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
<operationalAttributes xmlns="">
<attr name="urn:trulogica:concero:2.0#serviceName">
     <value>dkLDAP70</value>
     <value>dkLDAP70-2</value>
     <value>dkLDAP70-3</value>
     <value>dkLDAP70-4</value>
</attr>
</operationalAttributes>

<addRequest requestID="1">
  <operationalAttributes xmlns="">
  <attr name="urn:trulogica:concero:2.0#serviceName">
       <value>dkLDAP70-5</value>
```

```
        <value>dkLDAP74</value>
        <value>dkLDAP74-2</value>
  </attr>
  </operationalAttributes>
  <attributes xmlns="">
    <attr name="FirstName"><value>Anne</value></attr>
    <attr name="LastName"><value>Alexander</value></attr>
    <attr name="UserName"><value>dk1582</value></attr>
    <attr name="Password"><value>abc123</value></attr>
    <attr name="Company"><value>HP</value></attr>
    <attr name="Email"><value>devi.krishnaswamy@hp.com</value></
attr>
    <attr name="State"><value>TX</value></attr>
    <attr name="Zip"><value>12345</value></attr>
    <attr name="Addr1"><value>1224 hidden</value></attr>
    <attr
name="urn:trulogica:concero:2.0#serviceName#dkLDAP70#LDAP70_ENTI
TLEMENTS">
          <value>$UNIX1</value>
          <value>$UNIX2</value>
          <value>$UNIX3</value>
          <value>$UNIX4</value>
    </attr>
   </attributes>
</addRequest>

<addRequest requestID="2">
  <operationalAttributes xmlns="">
  <attr name="urn:trulogica:concero:2.0#serviceName">
        <value>dkLDAP72-2</value>
        <value>dkCombo</value>
  </attr>
  </operationalAttributes>
  <attributes xmlns="">
    <attr name="FirstName"><value>Anne</value></attr>
    <attr name="LastName"><value>Alexander</value></attr>
    <attr name="UserName"><value>dk1583</value></attr>
    <attr name="Password"><value>abc123</value></attr>
    <attr name="Company"><value>HP</value></attr>
    <attr name="Email"><value>devi.krishnaswamy@hp.com</value></
attr>
    <attr name="State"><value>TX</value></attr>
```

```
    <attr name="Zip"><value>12345</value></attr>
    <attr name="Addr1"><value>1224 hidden</value></attr>
    <attr
name="urn:trulogica:concero:2.0#serviceName#dkLDAP70#LDAP70_ENTI
TLEMENTS">
          <value>$UNIX1</value>
          <value>$UNIX2</value>
          <value>$UNIX3</value>
          <value>$UNIX4</value>
    </attr>
    <attr
name="urn:trulogica:concero:2.0#serviceName#dkLDAP70-2#LDAP70_EN
TITLEMENTS">
          <value>$UNIX2</value>

    </attr>
    </attributes>
</addRequest>
</batchRequest>
```

Example: Adding Users to Services with Specified Entitlements

The same user can be added to different **Services** relying on common resources. For this operation to succeed, you must specify the entitlements you want the user to have across shared resources within the add request. If you use this feature, the **Service** name specified in the bulk task can not have the pound sign (#) as part of its name.

In the following example, the user name is generated:

```
  <?xml version="1.0" encoding="ISO-8859-1" ?>
- <batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
    <operationalAttributes xmlns="" />
  - <addRequest requestID="1">
    - <operationalAttributes xmlns="">
      - <attr name="urn:trulogica:concero:2.0#serviceName">
          <value>Service1</value>
          <value>Service3</value>
```

```
        </attr>
      </operationalAttributes>
    - <attributes xmlns="">
      - <attr name="Email">
          <value>bulk1@company.com</value>
        </attr>
      - <attr name="FirstName">
          <value>Bulk1</value>
        </attr>
      - <attr name="LastName">
          <value>Bulk</value>
        </attr>
      - <attr name="State">
          <value>TX</value>
        </attr>
      - <attr name="Company">
          <value>TL</value>
        </attr>
      - <attr name="LDAP70_ENTITLEMENTS">
          <value>$UNIX1</value>
        </attr>
      - <attr name="urn:trulogica:concero:2.0
#serviceName#Service1#LDAP70_ENTITLEMENTS">
          <value>$UNIX2</value>
        </attr>
      - <attr name="urn:trulogica:concero:2.0
#serviceName#Service3#LDAP70_ENTITLEMENTS">
          <value>$UNIX3</value>
        </attr>
      </attributes>
    </addRequest>
  </batchRequest>
```

Upload Data Files

Upload the data files including user accounts, attributes, and entitlements through the **Bulk** pages. See Scheduling Bulk Jobs on page 351 for a complete procedure.

Viewing Job Results

After each of the jobs completes, use **Tools** → **Bulk** → **Bulk Task List** and request a report. The report lists users that were successfully created and those that failed. Use this report to make any needed corrections to your SPML file and resubmit the file with only those accounts that failed. You must create a new job with a unique name to upload the file in the Select Identity client.

If you created the job that ran initially, you cannot give the new job the same name. Each job you create as an administrator must be assigned a unique name.

The XML report can be used to extract failed users to be resubmitted after corrections are made.

Scheduling Bulk Jobs

Bulk jobs provide a means of adding or moving users in large blocks. Provision blocks of users using the Bulk Add functionality. Use Bulk Move to schedule bulk jobs to move a Context user group from one context to another. For example, if the Northwest division closes and all the employees within that division move to the North division, move the users in one block using Bulk Move.

This section covers the following topics:

- Scheduling a Bulk Move User Task
- Scheduling a Bulk Add Job

Scheduling a Bulk Move User Task

Perform the following steps to create a job to move a group of users from one Service context to another. This is a job that runs one time. For example, if the context attribute for a Service is “City” and you need to move a division in your company from one city to another, you can do so with the bulk function.

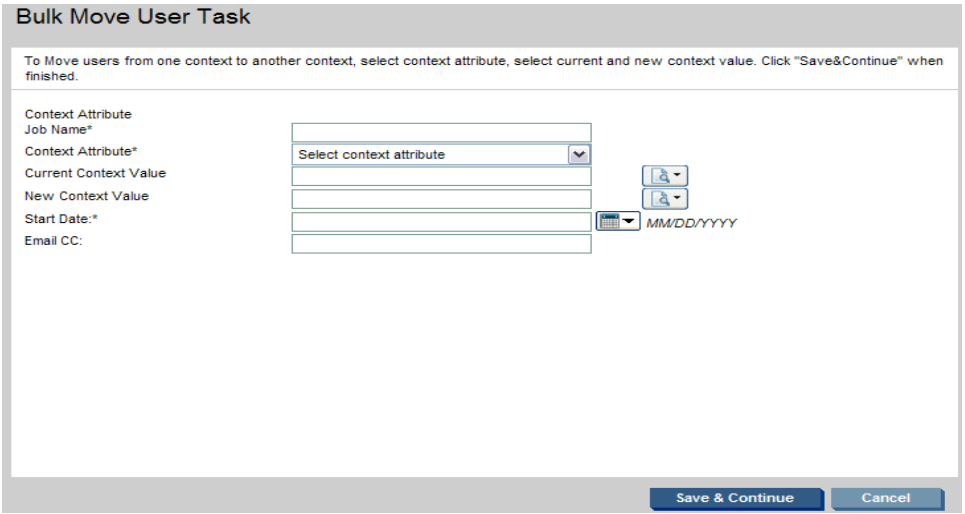
Changing a user's context may remove access to a Service or modify the entitlements granted within the Service. A user cannot be added to a Service with this function. A user is added to services as the External call, Rules, and workflow are defined.

To perform this task, you must have administrative rights to the Services affected by the context change. You need bulk move permission granted.

Perform the following steps to create and run a job that moves a group of users from one Service context to another:

1 Select **Tools** → **Bulk** → **Schedule Bulk Move**.
The **Bulk Move User Task** page opens.

Figure 148 Bulk Move User Task Page.



Alternatively, you can select **Tools** → **Bulk** → **Bulk Job List** then click the **Schedule Bulk Move** button or click **Bulk Move User Task** from the **Bulk Job List** page

2 Enter a unique name for the job in the **Job Name** field.

3 Choose the context attribute that you want to change for this group of users from the **Context Attribute** drop-down list.

4 Click  to search for and select the current value for this group of users in the **Current Context Value** field.

5 Click to search for and select the new value in for this group of users in the **New Context Value** field.

6 Click the calendar icon in the **Start Date** field to choose a day for the job to run.

If you select today's date, the job runs immediately. The job runs at 12:00 A.M. on all other dates.

7 The system sends email to the creator of the job when the job completes. If you want to send a copy of the email to another user, enter the address in the E**mail CC** field.

8 Click **Save & Continue**.

Shows the **Services** affected by the move.

9 Review the **Services**, and click **OK**.

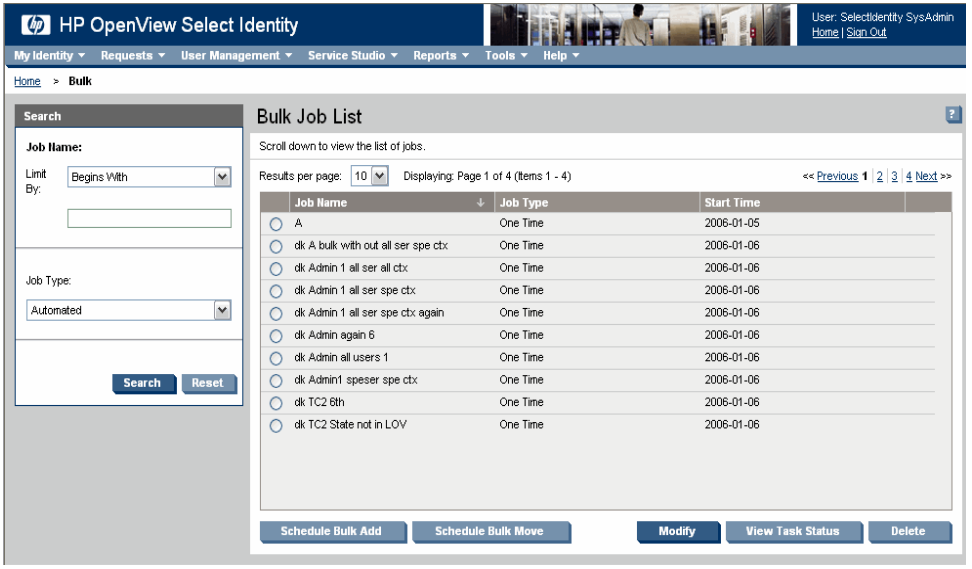
The job is created and runs when scheduled.

Scheduling a Bulk Add Job

Perform the following steps to schedule a bulk upload of user accounts to one or more Services:

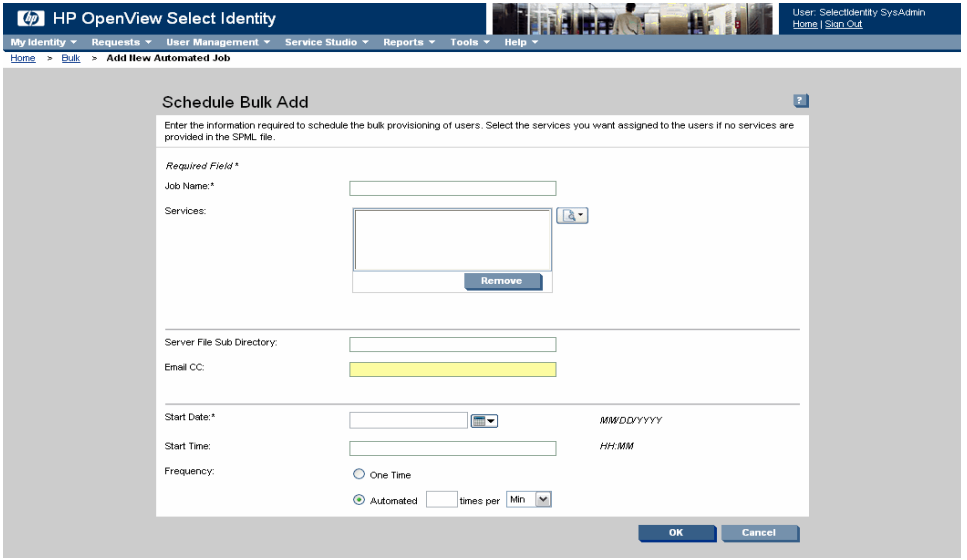
1 Select **Tools** → **Bulk** → **Bulk Job List**.
The **Bulk Job List** page opens.

Figure 149 Bulk Job List page



2 Click **Schedule Bulk Add**.
The **Schedule Bulk Add** page opens.

Figure 150 Schedule Bulk Add Page



3 Tab from field to field to enter the required information.

Field	Action
Job Name	Enter a unique name for this job.
Services	Click  , then click **Filter** and select each target Service if services were not specified in the SPML file. Remove services from the list by clicking the Remove button or deselecting a highlighted item. Only highlighted items will be included in the Bulk Add transaction.
Service File Sub Directory	Enter the name of the sub directory used to locate the services. If you add a subdirectory under `reconroot`, you must also add the same subdirectory under the `reconstaging` directory.
Email C.C:	Enter the complete email address of a user you want to inform when the move is complete. The job creator will be informed automatically.
Start Date	If you select today's date, the job runs immediately. The job runs at 12:00 A.M. on all other dates.
Start Time	Time you want the job to begin.

Select Identity reads data files from the `reconroot` directory. You may have multiple files and multiple jobs to run

4 Choose how frequently you want Select Identity to pick up the data file from the specified directory in the **Frequency** section.

Field	Action
One Time	Picks up the data file once. You are prompted to confirm that you want to create a bulk job. Click **OK**.
Automated	Pick. up the data file incrementally. • Enter a value for the number of times per increment Select Identity will pick up the data file. • Select an increment of time from the drop-down list (**Minute**, **Hour**, or **Day**)

5 Click **OK**.
A confirmation dialog asks if you want to create a new bulk job.

6 Click **OK**.
Schedules the job and returns to the **Bulk Job List** page.

Managing Bulk Jobs

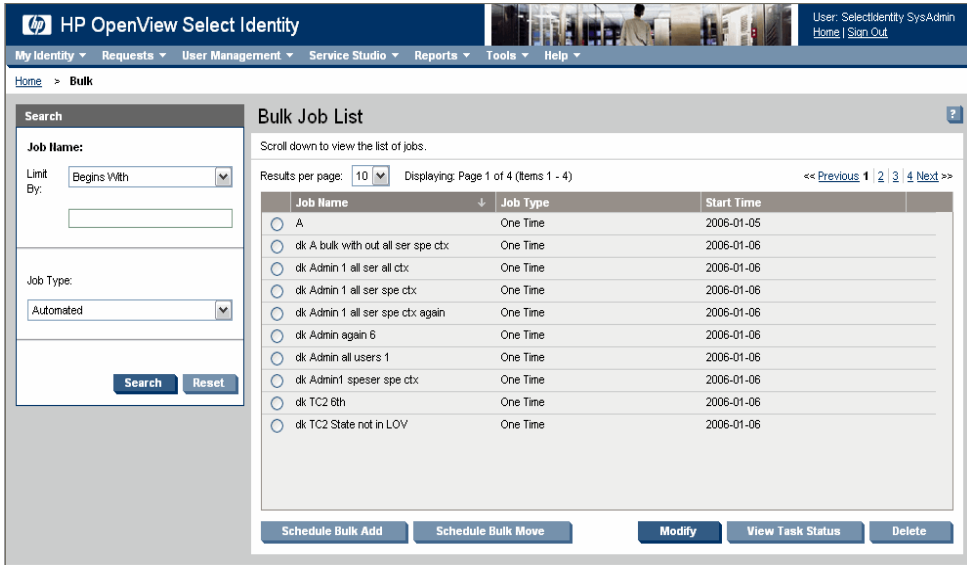
Complete the following procedures to mange your jobs:

- Modifying a Bulk Job
- Deleting a Bulk Job

Viewing Bulk Jobs

1 Select **Tools** → **Bulk** → **Bulk Job List**.
The **Bulk Job List** page opens.

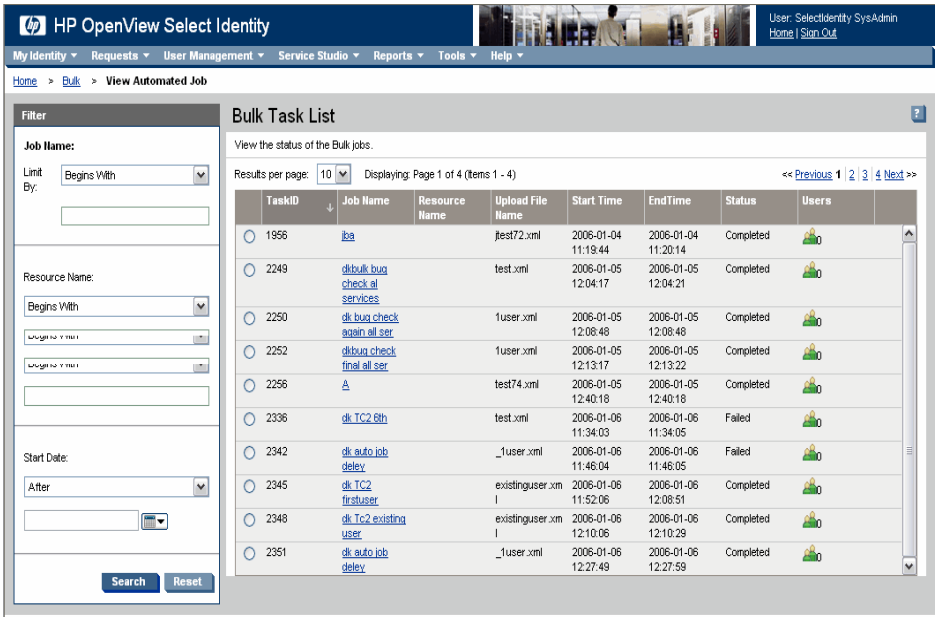
Figure 151 Bulk Job List page



2 Review the list of jobs shown.

3 View task details by selecting the job you want to view and clicking **View Task Status**.
Opens the **Bulk Task List** page.

Figure 152 View Task Status page



4 Review the list of bulk job tasks displayed.

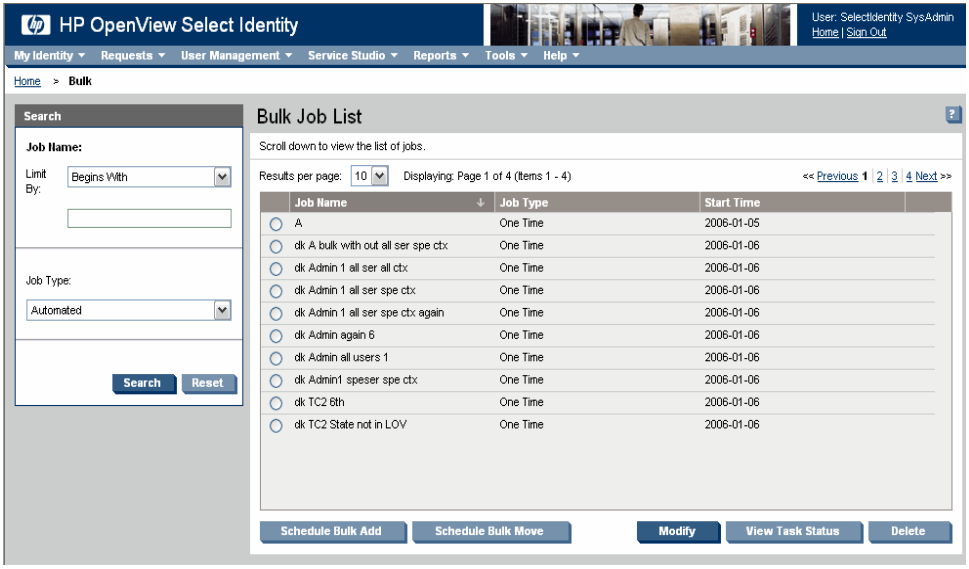
Modifying a Bulk Job

Perform the following steps to modify a bulk job:

You cannot modify a one time job. Only automated bulk jobs can be modified.

1 Select **Tools** → **Bulk** → **Bulk Job List**.
The **Bulk Job List** page opens.

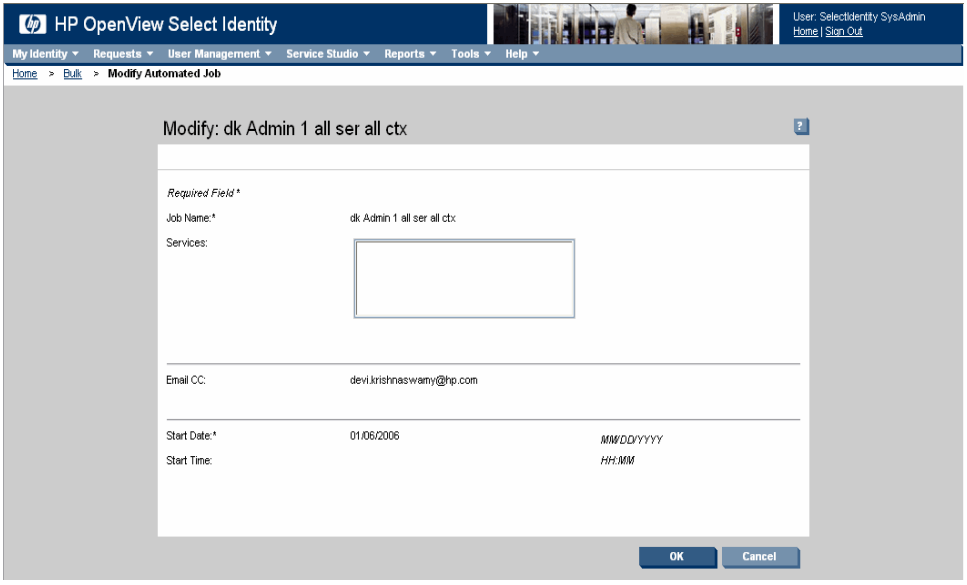
Figure 153 Bulk Job List page



2 Select the job from the list.

3 Click **Modify**.
Opens the **Modify: Bulk Job Name** page.

Figure 154 Modify: Bulk Job Name



Tab from field to field and make any changes necessary

> Only highlighted services in the Services Search List Box will be included in the bulk transaction.

4 Click **OK**.
Saves the change.

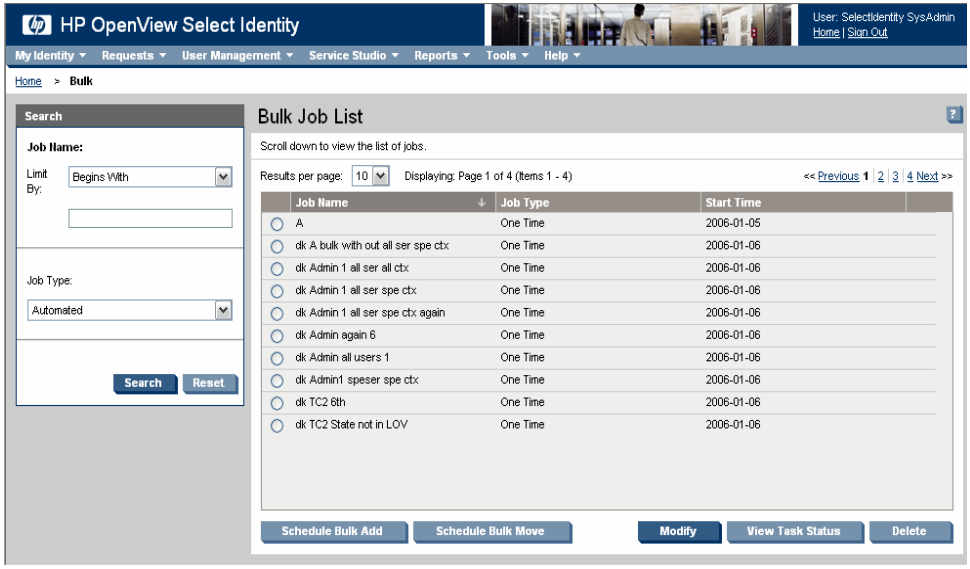
Deleting a Bulk Job

Perform the following steps to delete a job:

> You cannot delete a one time job. Only automated jobs can be deleted.

1 Select **Tools** → **Bulk** → **Bulk Job List**.
The **Bulk Job List** page opens.

Figure 155 Bulk Job List page



2 Select the job from the list. If necessary, perform a search to locate the one you want.

3 Click **Delete**.
Opens the confirmation dialog box.

4 Click **OK**.
Deletes the job.

5 View the tasks in the list.

6 To view the task, select it from the list and click the Job Name.
The **Modify: Job Name** page opens. It is read only. You cannot make changes.

14 Rules

Reconciliation rules specify the operations required to add and maintain a user account based on user properties. Rules control user assignment and provisioning during request processing.

You add and manage rules through the rules pages. You must create an XML file that adheres to the **Document Type Definition (DTD)** to build a rule. See DTD Rule Overview on page 367 for details. Once the file is complete, upload it to the Rule List. Rules on the list are available for assignment to resources and can be used in Workflows and External Calls.

This chapter covers the following topics:

Operations Supported

The following types of operations are supported in release 4.0:

- Add Service
- Delete Service
- Enable Service
- Disable Service
- Ennable User
- Disable User
- Terminate User

Understanding User Status Dependencies

The following limitations exist based on the status of a user account:

- New user accounts may only be added
- Disabled user accounts may have services deleted, but not added.
- Disabled users may only be enabled with the authority to add
- Enabled user accounts may receive any action
- Terminated user accounts may not be enabled

New Users

When a reconciliation request is received by Select Identity from an authoritative resource and all required conditions are met, the system makes the change. The event must be supported based on the status of the user, the rule definition, and the rule policy. (See Using Authoritative Resources on page 63 for a description of authoritative resources.)

When a rule is attached to a resource, if the user meets the criteria specified in the rule and qualifies for a Service, the user account is added or changed based on criteria in the rule. Rules can also be used to assign additional services to a user during Move User using an external call to read the rule from a designated workflow.

In an external call, the rules are defined in the workflow external call type. Rule is defined as a parameter in this workflow external call. The rule defined in the external call should be defined with the add rule functionality. When you add the rule, the XML rule file is uploaded to the Select Identity database.

Reconciliation Rules

Select Identity allows you the flexibility to create an XML file that adheres to the DTD rule to manage reconciliation events. No complete reconciliation rules exist when you install the system although a template is included. Each rule must be built and customized to meet your company's specific needs.

The XML rule files are loaded into Select Identity. Once available they are triggered by Workflows and external calls. Each policy is evaluated in a logical order.

This section describes the following:

- DTD Rule Overview
- Action Dependencies
- Tips
- Complete DTD Rule Definition

DTD Rule Overview

The Document Type Definition (DTD) rule is based on the DTD markup language mechanism, which defines the structure for XML files. If you are unfamiliar with XML and DTDs, refer to the specification at:

`http://www.w3.org/TR/2000/REC-xml-20001006#sec-well-formed`

This section covers the following:

- XML Building Blocks
- Complete DTD Rule Definition

XML Building Blocks

All XML documents are made up of the following simple building blocks,

Event Type	Description
`Elements`	The main building blocks of XML documents. Elements can contain text, other elements, or be empty.
`Attributes`	Extra information about elements. Attributes are always placed inside the starting tag of an element and always come in name/value pairs.
`Entities`	Variables used to define common text. Entities are expanded when a document is parsed by an XML parser. The following entities are predefined in XML: < for < `>` for > `&` for & `&quot;` for “ `&apos;` for '
`PCDATA`	Text parsed by a parser. Tags inside the text are treated as markup and entities are expanded.
`CDATA`	Text not parsed by a parser. Tags inside the text are not treated as markup and entities are not expanded.

Action Dependencies

Consider the following when creating a rule:

Event Type	Description
`Elements`	The main building blocks of XML documents. Elements can contain text, other elements, or be empty.
`Attributes`	Extra information about elements. Attributes are always placed inside the starting tag of an element and always come in name/value pairs.
`Entities`	Variables used to define common text. Entities are expanded when a document is parsed by an XML parser. The following entities are predefined in XML: < for < `>` for > `&` for & `&quot;` for “ `&apos;` for '
`PCDATA`	Text parsed by a parser. Tags inside the text are treated as markup and entities are expanded.
`CDATA`	Text not parsed by a parser. Tags inside the text are not treated as markup and entities are not expanded.

Tips

Listed below are a few tips to consider while writing XML reconciliation rules:

- Make sure that your parameters are consistent throughout the file.
- Do not nest your code. Select Identity does not support nesting.
- Review your key field (keyField). Make sure the attribute field selected is a unique identifier in Select Identity.
- Keep in mind that requests may be audited. The audit flag is set based on the resource policy. See Modifying the Resource Reconciliation Policy on page 83 for more information.

- Remember that the processor class should implement a process (int request id) method which the request broker calls back. An integer identifies a processor class that will be loaded dynamically to process the request without a workflow.
- Review the event types you used to make sure they are spelled correctly.
- Remember that event types are case sensitive.

Complete DTD Rule Definition

Following is the complete Select Identity DTD rule. Each element contains an explanation of its children and attributes:

```
<!-- Rules are scripts that are executed with reference to
specific events
   @title TruAccess Rule Language
   @root Rule
-->
<!--
A Rule has a collection of InputObjects and one or more scripts
that work on the input object
-->


<!ELEMENT Rule (InputObject*,Script+)>
<!--
RuleId is an identifier that is used to identify the rule Comment
is a piece of information associated with a rule Under debug mode
the Comment is printed in the log
-->
<!ATTLIST Rule
RuleId ID #REQUIRED
Comment CDATA #IMPLIED>
<!--
InputObject is an object that is used in the rule. Most of the
time the InputObject will be created and passed to the rule.
Optionally the input object will be created if specified. Please
note that one should not specify variables as InputObjects.
Variables are treated differently.
```

```
-->
<!ELEMENT InputObject EMPTY>
<!--
type is the type of the object. It can be any valid fully
qualified Java type name. The primitive types can be declared as
int, String and boolean. The actual type when passed needs to be
Integer, String and Boolean.
name is the name of the object
create specifies whether the object has to be created. The
assumption is that the object supports a no-argument constructor
-->
<!ATTLIST InputObject
type CDATA #REQUIRED
name CDATA #REQUIRED
create (yes|no) #IMPLIED>
<!--
Script is the body of a Rule, where conditions are checked and
actions taken
-->
<!ELEMENT Script (ConditionScript | ActionScript | AssertScript |
PlainText | PrintScript)*>
<!--
Comment in a script can be used to trace the execution for
debugging
-->
<!ATTLIST Script
Comment CDATA #IMPLIED>
<!--
ConditionScript is a condition statement
-->
<!ELEMENT ConditionScript (Condition,TrueAction,FalseAction?)>
<!--
Comment in a script can be used to trace the execution for
debugging
-->
```

```
<!ATTLIST ConditionScript
Comment CDATA #IMPLIED>
<!--
ActionScript models action. currently only one type of action is
specified
-->
<!ELEMENT ActionScript (AssignStmt)>
<!--
Comment in a script can be used to trace the execution for
debugging
-->
<!ATTLIST ActionScript
Comment CDATA #IMPLIED>
<!--
AssignStmt allows assignment of values to fields or variables
-->
<!ELEMENT AssignStmt (Field, Expression)>
<!--
Condition is a boolean expression
-->
<!ELEMENT Condition (Not?,(OrCondition | AndCondition |
UnitCondition)>
<!--
OrCondition models logical or
-->
<!ELEMENT OrCondition (UnitCondition+)>
<!--
AndCondition models logical and
-->
<!ELEMENT AndCondition (UnitCondition+)>
<!--
UnitCondition is a nested condition or a relation
-->
<!ELEMENT UnitCondition (Condition | Relation)>
```

```
<!--
Relation is between two expression
-->
<!ELEMENT Relation (Expression,Expression?)>
<!--
Relation supports the following operations:
 <ul>
  <li><b>eq</b> equal</li>
  <li><b>ne</b> not equal</li>
  <li><b>gt</b> greater than</li>
  <li><b>lt</b> less than</li>
  <li><b>ge</b> greater than or equal</li>
  <li><b>le</b> less than or equal</li>
  <li><b>contains</b> contains</li>
  <li><b>startswith</b> startswith</li>
  <li><b>endswith</b> endswith</li>
  <li><b>matches</b> matches</li>
  <li><b>eqic</b> equals ignore case</li>
 </ul>
contains is a special operation. It can be applied to String,Map
and Collection types. startswith, endswith, matches, equal can be
applied to String only. The semantics are the same as that of
java string class.
<!ATTLIST Relation
op ( eq | ne | gt | lt | ge | le | contains ) #REQUIRED>
<!--
TruAction is executed when the condition is true
-->
<!ELEMENT TrueAction (Script*)>
<!--
FalseAction is executed when the condition is false
-->
<!ELEMENT FalseAction (Script*)>
<!--
```

```
Field represents a field in a bean or a variable
-->
<!ELEMENT Field EMPTY>
<!--
name is the name of the field. If the field has a . then it is
assumed that it is an attribute of an InputObject otherwise it is
a temporary variable.
type is the type of the variable. The following types are
supported:
<ul>
<li><b>int</b> integer</li>
<li><b>boolean</b> boolean</li>
<li><b>java.lang.String</b> Java String</li>
<li><b>java.util.Collection</b> Java Collection</li>
<li><b>java.util.Map</b> Java Map</li>
</ul>
For variables, the collection is implemented as an ArrayList and
Map is implemented as a HashMap
fieldKey is used to access the object in the collection/map
hasG(S)etter and setter is used to generate accessing functions
Y => has a function get<Name> and set<Name>
N => no function ... direct access assuming that it is public
D => has generic function: get(<name>) and set(<name>) of string
type
-->
<!ATTLIST Field
name CDATA #REQUIRED
type ( int | boolean | java.lang.String | java.util.Map |
java.util.Collection ) #REQUIRED
fieldKey CDATA #IMPLIED
hasGetter ( Y | N | D) "D"
hasSetter (Y | N | D) "D" >
<!--
Expression is an expression
-->
```

```
<!ELEMENT Expression (Field | FixedValue | ArithExp | BoolExp)>
<!--
BoolExp is a boolean expression
-->
<!ELEMENT BoolExp (Field | True | False | Relation | Condition)>
<!--
True represents a true value
-->
<!ELEMENT True EMPTY>
<!--
False is a false value
-->
<!ELEMENT False EMPTY>
<!--
ArithExp is an Arithmatic Expression
-->
<!ELEMENT ArithExp (AddExp|MultExp | Field | FixedValue)>
<!--
AddExp is an additive expression
-->
<!ELEMENT AddExp (ArithExp,ArithExp)>
<!--
AddExp supports two operations
<ul>
<li><b>plus</b> addition</li>
<li><b>minus</b> subtraction</li>
</ul>
AddExp support concatanation of two Strings
-->
<!ATTLIST AddExp
op ( plus | minus ) #REQUIRED>
<!--
MultExp supports two operations
```

```
<ul>
<li><b>mult</b> multiplication</li>
<li><b>div</b> division</li>
</ul>
-->
<!ELEMENT MultExp (ArithExp,ArithExp)>
<!ATTLIST MultExp
op ( mult | div ) #REQUIRED>
<!--
FixedValue is a literal which can be a quoted string or an
integer
-->
<!ELEMENT FixedValue (#PCDATA)>
<!--
AssertScript is an assertion
Condition is checked and if it is false then an exception is
generated with the Message
-->
<!ELEMENT AssertScript (Condition,ExceptionName?,Message?)>
<!--
Comment in a script can be used to trace the execution for
debugging
-->
<!ATTLIST AssertScript
Comment CDATA #IMPLIED>
<!--
This signifies a not condition
-->
<!ELEMENT Not EMPTY>
<!--
A message for assertion failure
-->
<!ELEMENT Message (#PCDATA)>
<!--
```

```
Any BeanShell script
-->
<!ELEMENT PlainText (#PCDATA)>
<!--
class name of the assertion failed exception
-->
<!ELEMENT ExceptionName (#PCDATA)>
<!--
Statement to print an expression
-->
<!ELEMENT PrintScript (Expression)>
```

Managing Rules

Create your own rule XML files, or edit and use the existing XML rule template to add rules to Select Identity. Use existing rules by copying the rule, renaming the file, and making modifications when you need a new rule similar to an existing rule. Maintain rules by downloading the file, making required changes and uploading the file again. All XML rule files must be uploaded for the most recent version to appear in the Rule List.

Rules on the list are available to those functions that are supported by the reconciliation process. Your imported rules can be attached to resources, used in external calls, or triggered by workflows as required.

This section covers the following:

- Adding a Rule to the Rule List
- Creating a New Rule Using the Rule Template
- Viewing a Rule
- Deleting a Rule
- Troubleshooting Reconciliation Rules

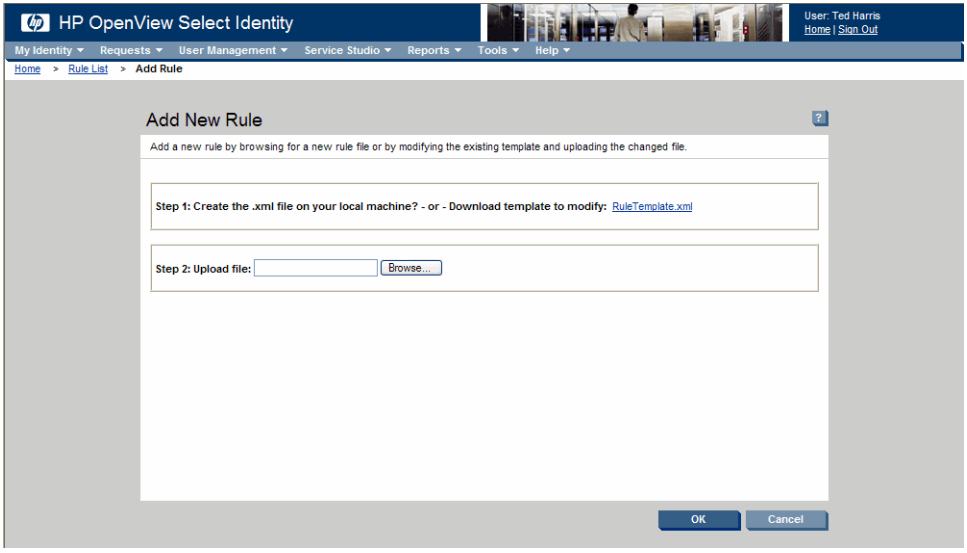
Adding a Rule to the Rule List

Complete the steps that follow to upload an existing XML file.

Perform the following to define a rule:

1 Select the **Tools** → **Rules** → **Add Rule** menu option.
The **Add New Rule** page opens.

Figure 156Add New Rule page



2 Click **Browse** and select the XML rule file you want to upload.
The file name appears in the **Upload File** field.

3 Click **OK**.
A confirmation dialog box appears.

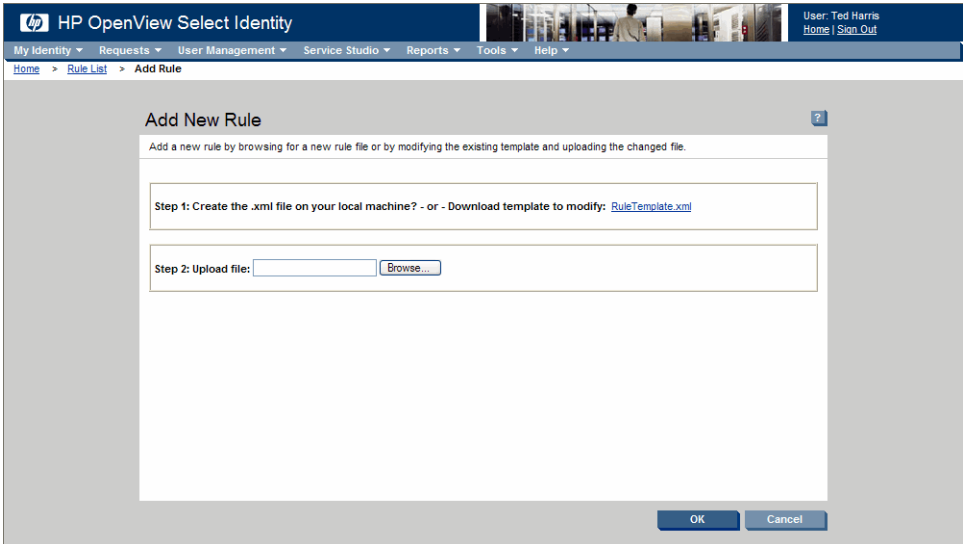
4 Click **OK**.
Returns to the **Rule List** page.

Creating a New Rule Using the Rule Template

Complete the steps that follow to upload an existing XML file.

1 Select the **Tools** → **Rules** → **Add Rule** menu options.
The **Add New Rule** page opens.

Figure 157Add New Rule Page



2 Click the **RuleTemplate.xml** link.
Open the **File Download** dialog box.

3 Click **Save**, then save your file using a new name.
Opens the **DownLoad Complete** dialog box.

4 Click **Open**.
Opens the XML rule template file.

Figure 158 XML Rule Template

```
<?xml version="1.0" standalone="no" ?>
- <Rule Comment="Rule Template" RuleId="RuleTemplate">
    <InputObject name="user" type="java.lang.Object" />
    <InputObject name="groups" type="java.util.Map" />
    <InputObject name="service" type="java.lang.String" />
  - <Script Comment="Test Condition">
    - <PlainText>
        <![CDATA[                    import com.trulogica.truaccess.util.DumpObject;                myLog.debug
        ("object="+DumpObject.getDump(user));  ]]>
      </PlainText>
    - <ConditionScript>
      - <Condition>
        - <AndCondition>
          - <UnitCondition>
            - <Relation op="eq">
              - <Expression>
                  <Field name="service" type="java.lang.String" />
                </Expression>
              - <Expression>
                  <FixedValue>"Firewall Service"</FixedValue>
                </Expression>
              </Relation>
            </UnitCondition>
          - <UnitCondition>
            - <OrCondition>
              - <UnitCondition>
                - <Relation op="eq">
                  - <Expression>
                      <Field name="user.Business Phone" type="java.lang.String" />
                    </Expression>
                  - <Expression>
                      <FixedValue>"999"</FixedValue>
                    </Expression>
                  </Relation>
                </UnitCondition>
              </OrCondition>
            </UnitCondition>
          </AndCondition>
        </Condition>
        <TrueAction />
      </ConditionScript>
    </Script>
  </Rule>
```

5 Make any changes required following industry standards for creating XML and save the file.

6 Return to the **Add New Rule** page.
The **Add New Rule** page appears.

7 Click **Browse** and select the XML rule file you just created.
The file name appears in the **Upload File** field.

8 Click **OK**.
A confirmation dialog box appears.

9 Click **OK**.
Returns to the **Rule List** page.

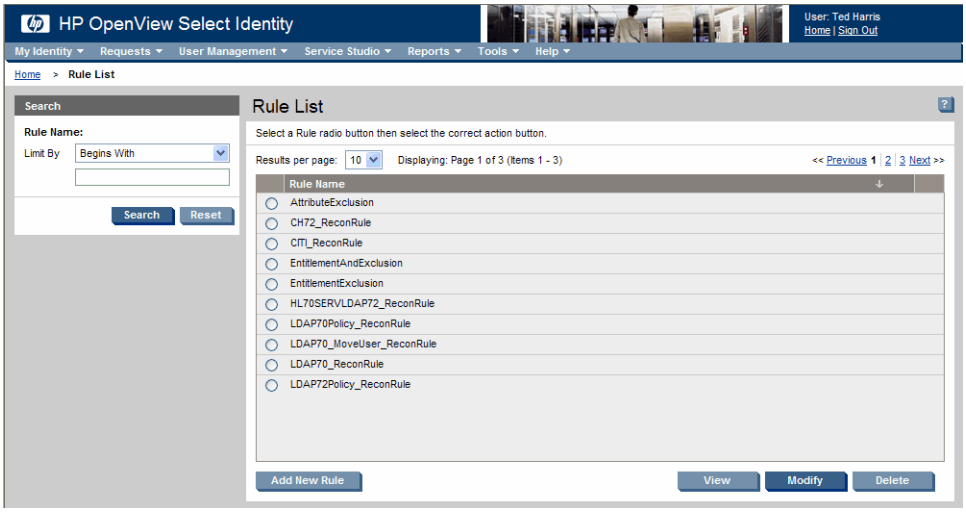
Copying and Modifying an Existing Rule

Rules may be modified within Select Identity as long as you do not change the name of the file. This functionality gives you the flexibility to make changes to the XML files as your business needs change.

Follow the steps below to modify an existing rule.

1 Select the **Tools** → **Rules** → **Rule List** menu options.
The **Rule List** page opens.

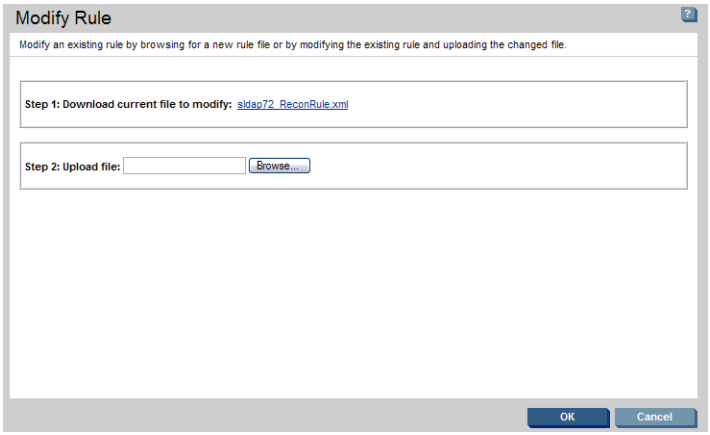
Figure 159 Rule List



2 Select the rule you want to modify.

3 Click **Modify**.
The **Modify Rule: Rule Name** page opens.

Figure 160Modify Rule: Rule Name Page



4 Click the rule file name link.
Open the **File Download** dialog box.

5 Click **Save** and change the name of the file if necessary.
Opens the **DownLoad Complete** dialog box.

If you are copying the file, it is a good practice to change the name right away to avoid any confusion.

6 Click **Open**.
Opens the XML rule template file.

7 Make any changes required following industry standards for creating XML and save the file.

8 Return to the **Modify Rule** page.
The **Modify Rule: Rule Name** page appears.

9 Click **Browse** and select the XML rule file you just modified.
The file name appears in the **Upload File** field.

10 Click **OK**.
A confirmation dialog box appears.

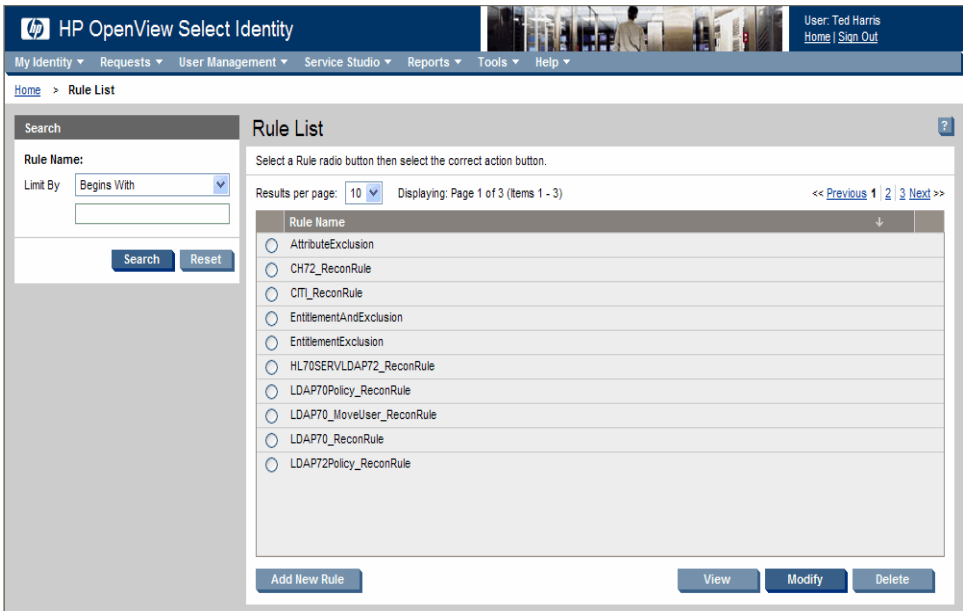
11 Click **OK**.
Returns to the **Rule List** page.

Viewing a Rule

Perform the following steps to view a rule:

1 Select the **Tools** → **Rules** → **Rule List** menu options.
The **Rule List** page opens

Figure 161 Rule List



2 Select the rule you want to view.

3 Click **View**.
The **File Download** dialog box appears

4 Click **Open** to view the file in a new window.

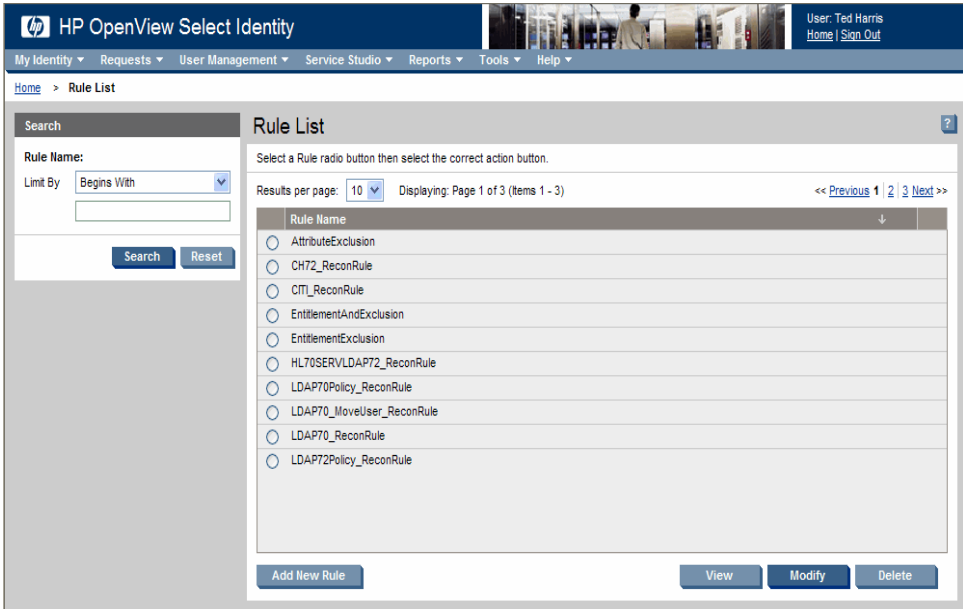
5 Close the window when you are finished viewing the file.
Returns to the **Rule List** page.

Deleting a Rule

Perform the following steps to delete a rule:

1 Select the **Tools** → **Rules** → **Rule List** menu options.
The **Rule List** page opens.

Figure 162 Rule List



2 Select the rule you want to delete.

3 Click **Delete**.
The confirmation dialog box appears.

4 Click **OK**.
Deletes the rule from the Rule List.

Troubleshooting Reconciliation Rules

The list that follows contains answers to frequently asked questions:

The initial AddRequest creates the user in Select Identity, however it does not create a Workflow instance for the request.

Make sure the user attributes are stored correctly.

Validate that the Context attribute value is specified as required. If the Context attribute value is not specified or is not provided at all the user is created, but not assigned to any service. As this point the request is created only when the user is assigned a service of any kind.

How do I enable and disable all services for a specific user?

Send a modify request to Select Identity specifying the correct attribute values based on the resources the target services provision to disable or enable all services for a specific user.

The `<value>code:urn:trulogica:concero:2.0#generalError,desc:Exception in processing request: null,</value>` error appears.

Review your key field (keyField). Make sure the attribute field selected is a unique identifier in Select Identity.

Validate the name of the field. The key field should be a Select Identity attribute field name. Look in your XML file and compare the resource attribute name with the Select Identity name (Service Studio > Resources > Modify Resources). View the Select Identity name on the right in the Attribute column. If the keyField name is incorrect, then change it now.

Exclusion Rules

There are two types of exclusion rules:

- Service Exclusion Rule
- Attribute Exclusion Rule
- Entitlement Exclusion Rules

Service Exclusion Rule

This is a conflict rule used in workflows. It compares rules. For example, if a user is in Service 1, then the user cannot also have Service 2. Replace Service 1 and gvA1 with the name of the service to check for. Also replace gvL3 with the name of the service to exclude.

```
//When one of these values exists on user
valueList.add("Service1");
valueList.add("gvA1");
//This value is excluded
valueMap.put("gvL3", valueList);
```

Attribute Exclusion Rule

This rule specifies excluded values:

```
//Entitlement name goes here
String entitlementName = "LDAP72_ENTITLEMENTS;
String attributeName = "FirstName";
```

Replace `LDAP72_ENTITLEMENTS` with the name of the entitlement attribute to exclude. And replace `"FirstName"`with the single value attribute.

```
//These values are excluded
excludedList.add("HR Managers");
excludedList.add("QA Managers");
//When this value is used
valueMap.put("Greg", excludedList);
```

Replace `"HR Managers"` and `"QA Managers"` with the entitlement values to exclude, and replace `"Greg"` with the attribute name to check.

Entitlement Exclusion Rules

Similar to Service Rules these rules state if the user belongs to Entitlement 1, the user cannot also belong to Entitlement 2, or if the user does belong to both Entitlement 1 and 2, the user cannot belong to Entitlement 3.

EntitlementExclusion

```
//Entitlement name goes here
String EntitlementName = "LDAP72_ENTITLEMENTS";
```

Replace `LDAP72_ENTITLEMENTS` with the name of the entitlement attribute to exclude.

```
//These values are excluded
valueList.add("HR Managers");
valueList.add("QA Managers");
//When this value is used
valueMap.put("PD Managers", valueList);
```

Replace `"HR Managers"` and `"QA Managers"` with the entitlement values to exclude, and replace `"PD Managers"` with the entitlement value to check for.

EntitlementAndExclusion

```
//Entitlement name goes here
String EntitlementName = "LDAP72_ENTITLEMENTS";
```

Replace `LDAP72_ENTITLEMENTS` with the name of the entitlement attribute to exclude.

```
//If all of these condition values are used
valueList.add("HR Managers");
valueList.add("QA Managers");
//Then this value is not allowed
valueMap.put("PD Managers", valueList);
```

Replace `"HR Managers"` and `"QA Managers"` with the entitlement values to exclude, and replace `"PD Managers"` with the entitlement value to check for.

Sample Rules

This section provides sample rules supporting a variety of actions. These are samples only. Many of the actions would not be included in the same rule. For example, you would not add a user and delete the same user moments later.

The RuleId MUST match the rule name defined in the reconciliation policy. The conditions are based on the user attribute map whose key is the Select Identity attribute name and value is the string value.

Multi-value attribute conditions are NOT supported.

This section includes the following:

- Rule Standards and ServiceNameMap
- Sample Rule One
- Sample Rule Two

Rule Standards and ServiceNameMap

This rule provides examples of multiple actions for both single service and all services scenarios. The user actions are specified in the ServiceNameMap. The following table is the list of tags for user actions.

Key	Meaning	Value	Meaning
-*-	User Level	Disable	Disable User
-*-	User Level	Enable	Enable User
-*-	User Level	Terminate	Terminate User
*	All Services (for specified resource)	+OK	Add All Services
*	All Services (for specified resource)	-OK	Delete All Services
**	All Services (for specified resource)	Disable	Disable All Services
**	All Services (for specified resource)	Enable	Enable All Services
Service Name	String name of a specific service	+OK	Add to this Service
Service Name	String name of a specific service	-OK	Delete from this Service
Service Name	String name of a specific service	Disable	Disable this Service
Service Name	String name of a specific service	Enable	Enable in this Service

Sample Rule One

```
<?xml version="1.0" standalone="no"?>
<!--
<!DOCTYPE Rule PUBLIC "http://www.trulogica.com/truaccess/rule"
```

```
"file:///C:/sanjoy/TruAccess/scriptengine/src/rule/Rule.dtd">
-->
<Rule RuleId="Resource_ReconRule" Comment="Reconciliation
Resource Rules">
    <!-- name of the resource, input parameter -->
    <InputObject name="ResourceName" type="java.lang.String"/>
    <!-- input parameter, user "final" attribute set -->
   <InputObject name="AttributeMap" type="java.util.HashMap"/>
    <!-- input parameter, user "current" attribute set -->
    <InputObject name="OldAttrMap" type="java.util.HashMap"/>
    <!-- service name -->
    <InputObject name="ServiceNameMap" type="java.util.HashMap"/
>
        <Script>
       <ConditionScript Comment="Service Operation if conditions
meet, Process=SvcAssign">
            <Condition>
                <AndCondition>
                    <UnitCondition>
                        <Relation op="contains">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="0"/>
                            </Expression>
                            <Expression>
                               <FixedValue>&amp;quot;Company&amp;quot;</
FixedValue>
                            </Expression>
                        </Relation>
                    </UnitCondition>
                    <UnitCondition>
                        <Relation op="eq">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="&amp;quot;Company&amp;quot;"/>
                            </Expression>
                            <Expression>
                              <FixedValue>&amp;quot;GE&amp;quot;</Fixed-
Value>
                            </Expression>
```

```
                        </Relation>
                    </UnitCondition>
                </AndCondition>
            </Condition>

            <TrueAction>
                <ActionScript Comment="Assign Services">
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;AcctManagers&quot;"/>
                        <Expression>
                            <FixedValue>&quot;+OK&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;PayrollManagers&quot;"/>
                        <Expression>
                            <FixedValue>&quot;-OK&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;AllManagers&quot;"/>
                        <Expression>
                          <FixedValue>&quot;Enable&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;HRManagers&quot;"/>
                        <Expression>
                            <FixedValue>&quot;Disable&quot;</
FixedValue>
                        </Expression>
                    </AssignStmt>
                </ActionScript>
```

```
            </TrueAction>
        </ConditionScript>
        <ConditionScript Comment="All Service Operation if condi-
tions meet, Process=AllSvcAssign">
            <Condition>
                <AndCondition>
                    <UnitCondition>
                        <Relation op="contains">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="0"/>
                            </Expression>
                            <Expression>
                               <FixedValue>&amp;quot;Company&amp;quot;</
FixedValue>
                            </Expression>
                        </Relation>
                    </UnitCondition>
                    <UnitCondition>
                        <Relation op="eq">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="&amp;quot;Company&amp;quot;"/>
                            </Expression>
                            <Expression>
                              <FixedValue>&amp;quot;AM&amp;quot;</Fixed-
Value>
                            </Expression>
                        </Relation>
                    </UnitCondition>
                </AndCondition>
            </Condition>

            <TrueAction>
                <ActionScript Comment="Assign Services">

                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&amp;quot;*&amp;quot;"/>
                        <Expression>
```

```
                            <FixedValue>&quot;+OK&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;*&quot;"/>
                        <Expression>
                            <FixedValue>&quot;-OK&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;**&quot;"/>
                        <Expression>
                          <FixedValue>&quot;Enable&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;**&quot;"/>
                        <Expression>
                            <FixedValue>&quot;Disable&quot;</
FixedValue>
                        </Expression>
                    </AssignStmt>
                </ActionScript>
            </TrueAction>
        </ConditionScript>
        <ConditionScript Comment="User level Operation if condi-
tions meet, Process=uerLevelOperation">
            <Condition>
                <AndCondition>
                    <UnitCondition>
                        <Relation op="contains">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="0"/>
```

```
                            </Expression>
                            <Expression>
                                <FixedValue>&quot;Company&quot;</
FixedValue>
                            </Expression>
                        </Relation>
                    </UnitCondition>
                    <UnitCondition>
                        <Relation op="eq">
                            <Expression>
                                <Field name="AttributeMap"
type="java.util.Map" fieldKey="&quot;Company&quot;"/>
                            </Expression>
                            <Expression>
                              <FixedValue>&quot;HP&quot;</Fixed-
Value>
                            </Expression>
                        </Relation>
                    </UnitCondition>
                </AndCondition>
            </Condition>

            <TrueAction>
                <ActionScript Comment="Assign Services">
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;-*-&quot;"/>
                        <Expression>
                          <FixedValue>&quot;Enable&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&quot;-*-&quot;"/>
                        <Expression>
                          <FixedValue>&quot;Disable&quot;</Fixed-
Value>
                        </Expression>
                    </AssignStmt>
```

```
                    <AssignStmt>
                        <Field name="ServiceNameMap"
type="java.util.Map" fieldKey="&amp;quot;-*-&amp;quot;"/>
                        <Expression>
                            <FixedValue>&amp;quot;Terminate&amp;quot;</
FixedValue>
                        </Expression>
                    </AssignStmt>
                </ActionScript>
            </TrueAction>
        </ConditionScript>
    </Script>
</Rule>
```

Sample Rule Two

The following is a sample of an XML rule for reconciliation. This checks to see if a user exists on an Authoritative resource called `LDAPv3_Auth` and has an attribute or field called `Company` with a value of `ABCCorp`. If so, the rule adds new user to the Services `reconSvc1` and `reconSvc2`.

```
<?xml version="1.0" standalone="no"?>
<!--
<!DOCTYPE Rule PUBLIC "http://www.trulogica.com/truaccess/rule"
"file:///C:/sanjoy/TruAccess/scriptengine/src/rule/Rule.dtd">
-->
<Rule RuleId="LDAPv3_Auth_ReconRule" Comment="Reconciliation
Authoritative Resource Service Assignment Rules">
    <InputObject name="ResourceName" type="java.lang.String"/>
    <InputObject name="AttributeMap" type="java.util.HashMap"/>
    <InputObject name="ServiceNameMap" type="java.util.HashMap"/
>
  <Script>
    <ConditionScript Comment="Check Resource Name and Company
Name">
      <Condition>
        <AndCondition>
          <UnitCondition>
            <Relation op="eq">
              <Expression>
```

```
                <Field name="ResourceName"
type="java.lang.String"/>
              </Expression>
              <Expression>
                <FixedValue>&amp;quot;LDAPv3_Auth&amp;quot;</FixedValue>
              </Expression>
            </Relation>
          </UnitCondition>
          <UnitCondition>
            <Relation op="contains">
              <Expression>
                <Field name="AttributeMap" type="java.util.Map"
fieldKey="0"/>
              </Expression>
              <Expression>
               <FixedValue>&amp;quot;Company&amp;quot;</FixedValue>
              </Expression>
            </Relation>
          </UnitCondition>
          <UnitCondition>
            <Relation op="eq">
              <Expression>
                <Field name="AttributeMap" type="java.util.Map"
fieldKey="&amp;quot;Company&amp;quot;"/>
              </Expression>
              <Expression>
               <FixedValue>&amp;quot;ABCCorp&amp;quot;</FixedValue>
              </Expression>
            </Relation>
          </UnitCondition>
        </AndCondition>
      </Condition>
      <TrueAction>
        <ActionScript Comment="Assign Services">
           <AssignStmt>
              <Field name="ServiceNameMap" type="java.util.Map"
fieldKey="&amp;quot;reconSvc1&amp;quot;"/>
              <Expression>
                <FixedValue>&amp;quot;+OK&amp;quot;</FixedValue>
              </Expression>
            </AssignStmt>
            <AssignStmt>
```

```
                <Field name="ServiceNameMap" type="java.util.Map"
fieldKey="&amp;quot;reconSvc2&amp;quot;"/>
                  <Expression>
```

15 Account Reconciliation

Account Reconciliation provides the ability to automatically update and synchronize Select Identity accounts with changes made to those accounts on external resources. Although changes to user accounts are generally managed through Select Identity's Services functionality, changes may occur outside of Select Identity. When this occurs, changes can be reconciled by configuring Select Identity to reconcile those changes made on a resource so that the account on the resource and the account in Select Identity are synchronized. Select Identity allows you to reconcile changes made to both authoritative and non-authoritative resources.

For example, If a user account attribute is changed on the authoritative resource (Like Human resources), this change can be provisioned to OVSI and another Non Authoritative resource. A user's permissions or entitlements, however, may be updated from a non-authoritative resource. Select Identity provides the capability to allow updates from both types of resources.

You must have the Select Identity system administrator role with access to all contexts to perform Reconciliation tasks.

This chapter covers the following:

- Reconciliation Procedure Overview
- Creating the SPML Data File
- Application Server Properties
- Understanding Job Results

Reconciliation Procedure Overview

Before you start the Reconciliation process, it is strongly recommended that you optimize Select Identity for best performance. See Configuring and Optimizing HP OpenView Select Identity on page 3 for a list of specific optimization settings. For details on configuring these settings and other important settings, see the *HP OpenView Select Identity Installation Guide*.

To perform reconciliation tasks, determine the method used to reconcile changes in your resource with data in Select Identity. Reconciliation can be executed through the following methods:

- Uploading changes to the resource through an SPML file
- Using an agent or utility to capture changes and send the changes to Select Identity through a Web Service interface.
- Polling a resource with two-way connector polling support

Regardless of the method you use, you follow the same sequence of steps to perform reconciliation.

- Reviewing Prerequisites
- Understanding Reconciliation Rules
- Evaluating Policies
- User Reconciliation Resource Level Policy
- User Reconciliation Attribute Level Policy

Reviewing Prerequisites

Identify the following before starting the reconciliation process:

- The authoritative and non-authoritative resources used in reconciliation.
- The user's unique ID and attributes from a resource participating in reconciliation.
- The entitlements from a resource associated with each user account involved in reconciliation.
- The attributes to be synchronized across various resources.

- Any reconciliation rules associated with the addition of accounts from authoritative resources.
- Reconciliation Policies defined for each resource that set the parameters used during reconciliation. See Modifying the Resource Reconciliation Policy on page 83.

Understanding Reconciliation Rules

Use reconciliation rules to control how users (new or existing) are assigned and provisioned in Select Identity. When Select Identity receives a reconciliation request for a resource, the system applies a reconciliation rule to the user. If the user meets the criteria specified in the rule and qualifies for a service, the user is added to that service.

In addition, use rules to assign additional services to a user. This is done using an external call to read the rule from a workflow or resource or attribute. Once a rule is created, deploy and manage it through the Rules pages.

Rules are created outside of Select Identity and then uploaded to the system. You must create an XML file that adheres to the rules DTD used by the Workflow Template. For Move User, the RuleID must be set to the Parameter Value defined in the external call that reads the rule. You can save the file in any directory on the Select Identity server. When you add the rule in the Rules capability, the XML rule file is uploaded to the Select Identity database.

To see SPML file examples, refer to the `\SampleXML\Reconciliation` directory on the Select Identity product media. A sample rule and overview of the DTD are available in Rules on page 365.

Evaluating Policies

Consider the way policies are evaluated in Select Identity when writing your XML reconciliation rule files. Each reconciliation request is built based on the evaluation results. One request per user is created. Multiple operations will be set as different targets in the request. Policies are evaluated in the following manner:

Actions	Use
Actions exist after the Attribute Level	Select Identity uses the action with the most coverage. This precedes the resource level action.
No Attribute level Action global polices are configured	Select Identity uses actions defined at the resource level.
No Resource level Action global polices are configured	Select Identity applies system defaults.

User Reconciliation Resource Level Policy

Each row defines the process for a reconciliation event type from a source resource. The event types are Add, Modify, or Delete. The following explains the meaning of each policy item.

Resource Level	Description
`Audit`	Determines whether to audit operations. Defaults to false.
`Report Policy`	Details level on the selected report. Defaults to brief. • brief • detailed
`ResourceAction`	Policy to perform operations for the user at the resource level. • Accept • Revert • Basic

Resource Level	Description
wfTemplateName	When using workflow for this resource/event, the name of the workflow template. Reconciliation default process work flow is used by default.
`ruleName`	Any rule associated with this resource/event combination that performs extra operations based on user properties.
`userAction`	Only applicable when the resource action is `Accept`. The following actions apply for Add and Modify event types, in ascending order: • Basic • Sync (Modify event type only) • Auto • Rule • Auto or Rule • Auto and Rule (Modify event type only)

A user action can be specified for each Select Identity attribute. When a reconciliation Modify request is received, all of the attributes that changed are collected. Select Identity checks the reconciliation user action for each changed attribtue, and performs one of the following actions:

- When a user action is configured, the highest ordered action is performed.
- When no attribute level plocy is found, the resource level policy is performed.

When the user level action does not involve a rule, only Basic and Sync user actions are executed.

User Reconciliation Attribute Level Policy

The attribute level policy defines the process when an attribute is changed during reconciliation. Event types are case sensitive.

The attribute reconciliation policy only applies when the resource action is set to Accept in modification mode and the attribute has changed.

Event Type	Description
`userAction`	Policy used to perform user operations at the user level. • Auto • Basic • Rule • Rule or auto • Rule and auto. • Sync resource

Reconciliation Jobs

Reconciliation jobs can be done one time or auto.

Create one-time reconciliation jobs to handle special needs or schedule jobs to maintain Select Identity and the application and datastore resources it serves.

Auto jobs can be used in case of polling changes from a resource in a particular time period. Auto jobs can also be used to scan a preconfigured file system directory to upload files automatically.

This section covers the following:

- Understanding Prerequisites
- Using an Agent or Web Service Interface
- Tips
- Reconciling with Authoritative Resources
- Reconciling with Non-authoritative Resources
- Understanding Request Actions
- Using Reconciliation Rules
- Understanding Service Membership Requirements

Understanding Prerequisites

If you are planning to use reconciliation through the Select Identity interface the following tasks must be completed first:

- Add all resources and specify an authoritative resource. See Using Authoritative Resources on page 63 for details.
- Identify and map the attributes to be updated in Select Identity accounts by mapping specific attributes to resource attributes in the Authoritative Resource. Do this by using the Modify Resource Attributes Mapping feature in the Resources functionary or by using the Attributes functions. See Modifying Resource Attribute Mappings on page 120 for details.
- Map any attributes from non-authoritative resources that need to be maintained in Select Identity to Sync Out from Select Identity. See Understanding Sync In and Sync Out on page 63.
- Determine the attributes that belong to non-authoritative resources that must update Select Identity. Mark these attributes to Sync In to Select Identity. The sync in and sync out attributes are marked at resource.
- Create an SPML file that contains user additions, modifications, or deletions from the authoritative resource.
- Create an SPML file for the entitlements associated to the user for all non-authoritative resources. This contains add, modify, and delete requests.

Using an Agent or Web Service Interface

Reconciliation can also be done through an agent or Web Service Interface. The format of the requests in Web Services is different from the format accepted using the Reconciliation pages. If you are planning to use reconciliation through an agent or Web Service interface, you will need to perform the following tasks:

- Create resources and attributes as described in Adding and Managing System Resources on page 65 and Managing Attributes on page 99.
- Create batch requests or single requests compatible with Select Identity's Web Services Interface. See the `SampleXML\Reconciliation\Web Service` folder on the Select Identity product CD for examples of Web Services requests.

- Invoke the Web Service from an agent, utility, or another web service.
- Create SPML requests using supported SPML elements and attributes mapped in Select Identity to handle the request events supported.

See the *HP OpenView Select Identity Web Service Online Help* and the Web Services section of the *HP OpenView Select Identity Connector Developer Guide* for more details.

System Configuration Prior to Reconciliation

The reconciliation process relies heavily on the configuration of resources, attributes, and Services. You may want to review these respective chapters in addition to the following information before performing any reconciliation tasks. Before running a reconciliation job, ensure that the following dependencies are met:

- Connectors and resources are deployed for systems you want to reconcile.
- Validate that all necessary resource and Select Identity attributes are mapped within the connector mapping file, which is designated when adding a resource.
- Verify all Select Identity attributes updated are mapped to the appropriate resource attributes using the Attributes functionality or the Modify Resource Attributes Mapping feature in the Resources functionality.
- Make sure one or more Services are created to use the resources with which you want to reconcile data, and a workflow template for reconciliation is assigned in the `TruAccess.properties` file, on the Service Role of all Services, or on the Resource. You can use the default template, `ReconciliationDefaultProcess`, or create and specify a custom template. See the *Select Identity Workflow Studio Guide* for information about workflow templates.
- Be sure that reconciliation events are in the Service to be updated.
- Be aware certain user profile attributes can be added to the `TruAccess.properties` file and used to expedite search functions, such as employee ID or tax ID number. Having an attribute mapped in the `TruAccess.properties` file for search purposes will facilitate the Reconciliation process. See the *HP OpenView Select Identity Installation Guide* for more information about search settings in this file.

Tips

Listed below are a few tips to consider while setting reconciliation policy:

- Make sure your parameters are consistent throughout the file.
- Review your key field (keyField). Make sure the attribute field selected is a unique identifier in Select Identity.

Reconciling with Authoritative Resources

When resources are created, they can be designated as authoritative sources. These resources generally have the most up-to-date account information and are often used to store the master account records for an identity. For example, an enterprise may have twenty different applications that contain user or account data. However, the human resources application only stores the user's personal data on one resource. This human resources system would be considered the authoritative source. All individuals must exist on this resource before they can be added to other applications or resources in the enterprise. See Managing Resources on page 64 for more information on defining an authoritative resource.

You must identify and designate an authoritative resource before performing reconciliation in Select Identity. Once an authoritative resource is designated, you can begin adding user accounts through reconciliation.

An account on Select Identity cannot be added or updated from any other resource, unless it is first added from an authoritative resource. Once the account is added from the authoritative resource, you can begin adding entitlements and other attributes from other resources.

Add requests from authoritative resources typically add new accounts in Select Identity. However, if an account exists and an add request comes in for the user, then the user's attributes will be replaced with the new add request. As a result, the user's Service membership may be re-evaluated to determine which services are assigned or removed. If an add request for a user comes in from reconciliation and the user was previously disabled on the resource, then the user will become enabled after the add request has been processed.

During reconciliation with an authoritative source, any existing rules associated with the resource and event are checked to determine if Service access should be given. See Reconciliation Rules on page 366 for more information about rules.

Reconciling with Non-authoritative Resources

Non-Authoritative resources typically contain entitlements for user accounts, but may contain other data as well. After adding user accounts from the authoritative resource, you should process non-authoritative changes to user accounts. Changes may include the addition or removal of entitlements. Entitlements are automatically considered authoritative and values are always updated in Select Identity when a change comes in from a non-authoritative resource.

In some cases, you may need to synchronize other attributes from non-authoritative resources. Select Identity enables you to set an attribute as a Sync In attribute. By doing this, you are telling Select Identity to synchronize with any changes to that attribute on the non-authoritative resource. In this scenario, the Sync In attribute will always be maintained in Select Identity when changes are made to the attribute on the non-authoritative resource. Learn more about Understanding Sync In and Sync Out on page 63.

If, however, the attribute changed on the non-authoritative resource and the attribute was not designated as Sync In, one the following scenarios occurs:

- The systems uses the revert feature set in the user Reconciliation Policy at the Resource Level. See Viewing Existing Reconciliation Jobs on page 431.
- If you do not activate this feature, the following happens when a Sync In attribute is received from a non authoritative resource:
  - Select Identity rejects the attribute change. Select Identity and any other resources are not be updated with the attribute value.
  - Select Identity and all other resources will be out of sync with the Non Authoritative Resource after the change was received.

When reconciling changes from a non-authoritative source, remember the following:

- Account changes from a non-authoritative resource require that the user originate from an authoritative resource and that the user exist in Select Identity.
- Updates to a user attribute from a non-authoritative source are only allowed if the attribute is not already present in Select Identity or the attribute has no value. If the attribute exists and has a value in Select

Identity, it needs to be defined as sync out to enable an override of an existing value. Authoritative attributes can be set using the Modify Resource Attributes Mapping feature in the Resources functionality.

- Sync Out attributes that are mapped to multiple resources automatically synchronize across resources if the user's change request contains the mapped attribute and the user belongs to a Service containing the mapped attribute and the resource.

Understanding Request Actions

There are several types of user actions Select Identity performs for user requests:

- Basic - the minimum that should be done based on the request event type
- Re-Sync - synchronized to other mapped resources
- Auto Service Assignment - assign user to qualified services based on the predetermined evaluation rules
- Rule- use actions specified in the XML rule

If the SPML filter is configured for the resource, the filter function is invoked on the incoming SPML request for any customer requiring pre-processing.

Reconciliation supports the following request actions.

Authoritative Resources

Event	Resource Policy	New User	Request Action
Add	Ignore	N/A	Nothing happens
Add	Revert	N/A	Revert Add
Add	Accept	Yes	Add, Add Service
Add	Accept	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users
Modify	Ignore	N/A	Nothing happens
Modify	Revert	No	Revert / Modify
Modify	Accept	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users
Delete	Ignore	N/A	Nothing happens
Delete	Revert	No	Revert Delete
Delete	Accept	No	Terminate

Non-authoritative Resources

Event	Resource Policy	New User	Request Action
Add	Ignore	N/A	Nothing happens
Add	Revert	N/A	Revert Add
Add	Accept New	Yes	Add Service
Add	Accept Accept New	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users

Event	Resource Policy	New User	Request Action
Modify	Ignore	N/A	Nothing happens
Modify	Revert	No	Revert / Modify
Modify	Accept	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users
Delete	Ignore	N/A	Nothing happens
Delete	Revert	No	Revert Delete
Delete	Accept	No	Delete Service

Revert

Event	Resource Policy	New User	Request Action
Add	Ignore	N/A	Nothing happens
Add	Revert	N/A	Revert Add
Add	Accept	Yes	Add Service
Add	Accept	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users
Modify	Ignore	N/A	Nothing happens
Modify	Revert	No	Revert / Modify
Modify	Accept	No	Add / Modify / Delete / Enable / Disable Services Enable / Disable / Terminate Users
Delete	Ignore	N/A	Nothing happens
Delete	Revert	No	Revert Delete
Delete	Accept	No	Delete Service and Resource keys

Using Reconciliation Rules

When adding user accounts through reconciliation, you may want to control how accounts are added within the enterprise. In some cases, you may want to provision a user to a resource when the account is added from the authoritative source.

Reconciliation Rules are associated with Reconciliation Events in the Reconciliation Policy. Rules are defined in XML and are uploaded to Select Identity through the Rules functionality. These Rules specify the services that users are eligible for based on particular parameters defined in the rule. Rules make assignments after validating requests to determine if the request meets the rule criteria.

For example, you may have a business rule stating that all employees hired into the Information Technology (IT) department are added to Active Directory. In this case, create a reconciliation rule that examines a new employee's department and provisions the user to the Active Directory resource if the employee's department is equal to "IT." To execute the rule properly, you create a Service containing the Active Directory resource. Specify the rule with unit condition of employees department attribute value equals "IT", then add the service. This rule needs to be specified, either as a resource, attribute, or external call parameter.

Each resource can have one defined reconciliation rule for this purpose. Users will only be added to Services stated in the rule if they meet the criteria for the rule. If they do not meet the rule or no rule is defined, users will only be assigned a Service for which they are qualified. For more information about Rules, see Reconciliation Rules on page 366.

To see reconciliation examples including rules, refer to the `\SampleXML\Reconciliation` directory on Select Identity product CD. A sample rule and overview of the DTD are available in Reconciliation Rules on page 366.

If you need to add additional Services to a user's account when changing a user's context, reference the Adding Services to a User scenario in the *HP OpenView Select Identity Workflow Studio Guide*. This process enables you to build rules and external calls to add new Services to an account while modifying the account.

Understanding Service Membership Requirements

Once a user is added or modified through reconciliation, Select Identity evaluates the user's Service memberships as a result of the change. Based on the changes to the user's attributes, Service memberships are assigned to or removed from the user.

Adding Service Assignments During Reconciliation

For a user to gain a Service assignment through reconciliation, the user must have:

- Access to all the resources contained in the Service
- All required Service attribute properties defined by the Service

- All assigned attribute values contained within the Service
- A matching context value defined in one of the Service's Contexts
- All fixed entitlements defined in the Services' Service Roles related to the user's context value. If a user's context is associated to the third level of a Service Role, then the user must also have all fixed entitlements assigned to the first and second levels of that same Service Role structure.
- All optional entitlement values for the service based on the user's context value
- Matching attributes field values present must also match all field proprietors such as length and pattern

A matching attribute value for any attributes in the Service included in a constraint list. Constraints may be part of the static attribute definition contained in Select Identity or they may be a part of an external call if a call has been defined for the attribute.

If the context attribute or any fixed attribute has a one-way connector as the storage type, then service assignment checking will be by-passed. There is no way to restore a one-way encrypted value from Select Identity data storage

Removing Service Assignments During Reconciliation

A user will be removed from a Service if the user's account no longer meets the requirements of the Service based on the reconciliation change request.

Modifying Service Assignments During Reconciliation

Changes to a user's attributes during reconciliation do not cause provisioning in the resource to occur unless the following is true.

- The attribute being changed is mapped to other resources and the user belongs to the Service containing the attribute
- A reconciliation rule is being executed to add a user from an authoritative resource
- A workflow, other than the default reconciliation workflow, is associated with the reconciliation change. The workflow can invoke an external call to change a user's entitlements or add the user to a Service.
- The Add Service and Delete Service Membership Reconciliation events exist in the target Service's Service Role

- New attributes are added to a user through rule service easement

Creating the SPML Data File

The reconciliation function uses an SPML data file type to make account changes. This file should reflect changes from a specified resource, including entitlement and attribute changes. The file is then uploaded to Select Identity.

All SPML data files for automated jobs must follow the `ResourceName_yyyy_mm_dd_hh_mm` naming convention and are stored in the reconciliation root directory as specified in the `TruAccess.properties` file. See the *HP OpenView Select Identity Installation and Configuration Guide* for information about this properties file and Application Server Properties on page 427 for reconciliation specific settings.

Jobs that are not automated can use any naming convention.

Resource Names

Resources may follow any naming convention. If, however, resource names contain underscores then you must change the following TruAccess. Property `com.hp.ovsi.spml.resourcename.separator` setting to other characters such as `com.hp.ovsi.spml.resourcename.separator = +` to define the separator string in the reconciliation SPML file name between the resource name and the date/time portion. For example the file name will be Resource Name +yyy_mm_dd_hh_mm. This prevents reconciliation jobs from being lost when special characters are included in the names.

Creating an SPML File Containing Users and Attributes

Many resources today have a utility or mechanism for exporting user data to an Extensible Markup Language (XML) or Service Provision Markup Language (SPML) format. To create the SPML format needed for reconciliation, perform one of the following:

- Export your data in the resource to LDIF format and use a parser to convert the data to SPML.

- Export your data in the resource to XML or DSML format. Convert it to SPML using an XML parser and XSLT style sheet.
- Use a third-party mapping tool to convert your data to SPML format.
- Use the SPML Generator tool provided in your Select Identity product CD. Learn more about the SPML Generator Utility on page 543.
- Programmatically build the file by reading through your resource and writing out changed records for each user.

Many connectors support a change detection utility called reverse synchronization. This utility enables the resource to send changes to the Select Identity server. See the *HP OpenView Select Identity Connector Developer Guide* for a complete description of reverse synchronization.

To see an example of using an LDIF format to SPML conversion, view the sample files located in the `\SampleXML\Reconciliation` directory on the HP OpenView Select Identity product CD.

Writing SPML

When creating the input file containing the user attributes, specify a unique identifier attribute associated with each user. The identifier is specified in the `<operationalAttributes xmlns=>` section of the SPML file and is designated as a value in the `keyFields` attribute. Select Identity's default attribute for identifying accounts is `UserName`. The following is a sample of this section of the SPML file:

```
<operationalAttributes xmlns="">
   <attr name="urn:trulogica:concero:2.0#keyFields">
   <value>UserName</value></attr>
</operationalAttributes>
```

This is the attribute name and value that Select Identity uses to determine if the account exists. In addition to specifying the user ID operational attribute in the header of the file, you must specify two other operational attribute values for each add user request:

```
<addRequest requestID="1">
  <operationalAttributes xmlns="">
    <attr name="urn:trulogica:concero:2.0#taUserName">
    <value>avaughan</value></attr>
    <attr name="urn:trulogica:concero:2.0#taResourceKey">
    <value>AQ4100</value></attr>
```

```
</operationalAttributes>
```

The taUserName field value represents the unique value used to identify each account in Select Identity. The taResourceKey represents the corresponding key used to identify the account on the resource from which the user originates. It is only for resources where there is no generation.

If the UserName attribute is set up with a value generation function, and a Reconciliation request is made from an Authoritative resource, the taUserName does not need to be specified in the SPML file. Select Identity will invoke the value generation function to create the UserName. The user will be provisioned in Select Identity with this generated UserName.

SPML Tips

- The file must begin and end with <batchRequest></batchRequest>.
- Each account to be added begins and ends with <addRequest></addRequest>. The operational attributes and values listed for each add request are required by Select Identity. An account cannot be added without these attributes and values.
- The keywords required by reconciliation processing must present in operational attributes.
- The admin username/password, source resource, resource business key fields, reverse sync flag are required for all operations in the BATCH section for Web Service SPML.
- taUserName is required for add operation from an authoritative resource in sub request section.
- taResourceKey is required for add operation in sub request section.
- Identifier (not an operational attribute) is required for Modify/Delete operations in sub request section.
- If you need to have multiple values for an attribute within Select Identity, use the following syntax:

```
<attr name="name">
    <value>value1</value>
    <value>value2</value>
</attr>
```

Where “name” is mapped to the Select Identity attribute.

SPML Examples

SPML File without taUserName

Following is a sample SPML file without the `taUserName`:

```
<batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
    <operationalAttributes xmlns="">
       <attr name="urn:trulogica:concero:2.0#keyFields">
         <value>Email</value></attr>
    </operationalAttributes>
<addRequest requestID="1">
    <operationalAttributes xmlns="">
       <attr name="urn:trulogica:concero:2.0#taResourceKey">
         <value>ResAD051801</value></attr>
    </operationalAttributes>
    <attributes xmlns="">
       <attr name="State">
         <value>TX</value></attr>
       <attr name="LastName">
         <value>Smith</value></attr>
       <attr name="Email">
         <value>john.smith@hp.com</value></attr>
       <attr name="FirstName">
         <value>John</value></attr>
    </attributes>
</addRequest>
</batchRequest>
```

SPML File Identifying an Account with Two Fields

It is possible to identify an account using two different fields. In the example below, `LastName` and `FirstName` are used to search for a unique account by specifying them in the `keyFields` section of the Operational Attributes.

When using multiple fields, there should not be multiple occurrences in Select Identity. The fields combined must ensure a unique occurrence when searching for a user in Select Identity.

Use the most distinct key as the first value in the file. In the following example, `LastName` is specified before `FirstName` since it is the more unique of the two fields:

```
<batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
   <operationalAttributes xmlns="">
      <attr name="urn:trulogica:concero:2.0#keyFields">
         <value>LastName</value>
         <value>FirstName</value></attr>
   </operationalAttributes>

<addRequest requestID="1">
   <operationalAttributes xmlns="">
      <attr name="urn:trulogica:concero:2.0#taUserName">
         <value>chU54500</value></attr>
      <attr name="urn:trulogica:concero:2.0#taResourceKey">
         <value>ch54500</value></attr>
   </operationalAttributes>

   <attributes xmlns="">
      <attr name="Employee ID">
         <value>HP</value></attr>
      <attr name="LastName">
         <value>Kellerman</value></attr>
      <attr name="Email">
         <value>Billy.Kellerman@trulogica.com</value></attr>
      <attr name="FirstName">
         <value>Billy</value></attr>
      <attr name="State">
         <value>TX</value></attr>
   </attributes>
</addRequest>
</batchRequest>
```

Single Operation SOAP Request

```
<!--
      SPML Request to Add a new User from a recon auth resource
through webservice
      ****************************
  -->
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/
envelope/">
 <soap:Body>
  <addRequest requestID="12345"
execution="urn:oasis:names:tc:SPML:1:0#asynchronous">
   <operationalAttributes>
    <attr
name="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName"><value>
sisa</value></attr>
    <attr
name="urn:trulogica:concero:2.0#password"><value>abc123</
value></attr>
    <attr
name="urn:trulogica:concero:2.0#resourceId"><value>Auth_LDAP_1</
value></attr>
    <attr
name="urn:trulogica:concero:2.0#keyFields"><value>UserName</
value></attr>
    <attr
name="urn:trulogica:concero:2.0#reverseSync"><value>true</
value></attr>
    <attr
name="urn:trulogica:concero:2.0#taUserName"><value>webrecon1</
value></attr>
  <attr
name="urn:trulogica:concero:2.0#taResourceKey"><value>webrecon1<
/value></attr>
   </operationalAttributes>
     <attributes>
    <attr name="UserName"><value>webrecon1</value></attr>
    <attr name="Email"><value>QA1@trulogica.com</value></attr>
    <attr name="State"><value>TX</value></attr>
    <attr name="urn:trulogica:concero:2.0#groups">
```

```
      <value>HR Managers</value>
      <value>PD Managers</value>
      </attr>
    </attributes>
   </addRequest>
 </soap:Body>
</soap:Envelope>
```

Batch Operation SOAP Request

```
<!--
      SPML Request to batch add new User from a recon auth
resource through webservice

      ****************************

  -->
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/
envelope/">
 <soap:Body>   <batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
    xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
    xmlns="urn:oasis:names:tc:SPML:1:0"
requestID="1085774668899">

    <operationalAttributes xmlns="">
      <attr
name="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName"><value>
sisa</value></attr>
      <attr
name="urn:trulogica:concero:2.0#password"><value>abc123</
value></attr>
      <attr
name="urn:trulogica:concero:2.0#resourceId"><value>Auth_LDAP_1</
value></attr>
      <attr
name="urn:trulogica:concero:2.0#keyFields"><value>UserName</
value></attr>
      <attr
name="urn:trulogica:concero:2.0#reverseSync"><value>true</
value></attr>
    </operationalAttributes>
```

```
    <addRequest requestID="2"
execution="urn:oasis:names:tc:SPML:1:0#asynchronous">
      <operationalAttributes>
        <attr
name="urn:trulogica:concero:2.0#taUserName"><value>webrecon2</
value></attr>
        <attr
name="urn:trulogica:concero:2.0#taResourceKey"><value>webrecon2<
/value></attr>
      </operationalAttributes>

         <attributes>

        <attr name="UserName"><value>webrecon2</value></attr>

        <attr name="Email"><value>QA2@trulogica.com</value></
attr>
        <attr name="State"><value>TX</value></attr>
        <attr name="urn:trulogica:concero:2.0#groups">
          <value>HR Managers</value>

          <value>PD Managers</value>
        </attr>
       </attributes>
     </addRequest>

         <addRequest requestID="3"
execution="urn:oasis:names:tc:SPML:1:0#asynchronous">

      <operationalAttributes>
        <attr
name="urn:trulogica:concero:2.0#taUserName"><value>webrecon3</
value></attr>
        <attr
name="urn:trulogica:concero:2.0#taResourceKey"><value>webrecon3<
/value></attr>
      </operationalAttributes>

         <attributes>

        <attr name="UserName"><value>webrecon3</value></attr>

        <attr name="Email"><value>QA3@trulogica.com</value></
attr>
```

```
        <attr name="State"><value>TX</value></attr>
        <attr name="urn:trulogica:concero:2.0#groups">
          <value>HR Managers</value>
          <value>PD Managers</value>
        </attr>
      </attributes>

  </addRequest>
       </batchRequest>
 </soap:Body>
</soap:Envelope>
```

Specifying Attributes in SPML

When specifying attributes in the SPML file, be sure to use the mapped resource attribute's name. This may differ from the Select Identity attribute name. Attributes uploaded to Select Identity must be mapped to a resource. For information related to attribute mapping, see Service Studio on page 55.

To see sample request files, refer to the Select Identity product CD in the `\SampleXML\Reconciliation` directory.

Creating an SPML File Containing Entitlements

After building the SPML file containing your list of users and associated attributes, you may need to add entitlements from other resources to your users. Users may have entitlements from multiple resources. To upload these entitlements, a separate SPML file containing the entitlements must be created for each resource.

Entitlement additions/changes from a non-authoritative resource can only be added if the entitlements were added/changed on the resource. You do not need to create a reconciliation file with entitlements. when a user is added to an authoritative resource.

For each resource file created, determine the unique identifier on the resource that links the entitlement to the designated user. This unique identifier is specified in the SPML file as the `taResourceKey` field. If the keyField appears in the data section, use the keyField value, otherwise use the value of the identifier. Specify the userId or user name so that you can associate the entitlements to the correct Select Identity account. This is designated in the identifier tag as follows:

```
<identifier xmlns=""
type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName">
<id>AEE200</id>
</identifier>
```

When specifying the entitlement, the identifier type `UserIDAndOrDomainName` is used to specify the username or account in Select Identity associated with the entitlement. In the example above, the entitlement is associated with an account called `AEE200` in Select Identity.

The operational attributes `keyFields`, and `taResourceKey` are required for assigning entitlements. These are specified in the file that you created to add users to the system. The attribute `keyFields` is only listed once at the beginning of each file. The attribute `taResourceKey` is listed for each user account.

To see an example file for adding entitlement to an existing user, refer to the Select Identity product CD in the `\SampleXML\Reconciliation` directory.

Understanding Dependencies

SPML files must be imported to handle reconciliation events. However, the successful import of a file does not mean that the functionality associated will work as expected. All dependencies must be met and any other supporting files on which the function depends must be present in order for the SPML functionality to work as planned.

Dependencies are detailed below:

Area	Dependences
KeyFields	`KeyFields` must be defined. If `KeyFields` are not defined then the default value is `UserName`.
Attributes	Attributes must exist and be properly mapped between the resource and Select Identity.
Resource	Rules used to provision the resource during reconciliation must exist unless the resource Reconciliation Policy is stet to Auto or Basic. Resources must exist and be accurately defined. See Understanding Reconciliation Rules on page 403.
Service	Services must exist and be accurately defined.
Rules	The specified rule file must be imported and work as planned.
User Account	User Accounts must be set up on Select Identity unless the accounts are being added through reconciliation.
Connector	Connector must exist and be accurately defined.

Application Server Properties

Reconciliation relies on settings defined on the web application server. You can configure the necessary parameters in the `TruAccess.properties` file and create relative directories on the application server host.

The `TruAccess.properties` file is described in detail in the *HP OpenView Select Identity Installation and Configuration Guide*. The following is a sample section of the reconciliation-related property entries in the file:

```
#The attributes for reconciliation
truaccess.recon.rootdir=c:/temp/reconroot
truaccess.recon.stagingdir=c:/temp/reconstaging
truaccess.recon.backupdir=c:/temp/reconbackup
truaccess.recon.filename.timeformat=yyyy_MM_dd_H_mm

#The attributes for batch processing
truaccess.batch.inprogresstimeout=18000000

#the template for the password reset
truaccess.fixedtemplate.passwordreset=SI\ Provisioning\ Only
truaccess.fixedtemplate.terminate=SI\ Provisioning\ Only
truaccess.fixedtemplate.disable=SI\ Provisioning\ Only
truaccess.fixedtemplate.enable=SI\ Provisioning\ Only
truaccess.fixedtemplate.expiration=UserAccountExpirationWF
truaccess.fixedtemplate.securityviolation=SI\ Email\ Only
truaccess.fixedtemplate.modifyprofile=SI Provisioning Only
truaccess.fixedtemplate.passwordexpirenot=SI\ PasswordExpire\
Email
truaccess.fixedtemplate.passwordexpire=SI\ Provisioning\ Only
truaccess.fixedtemplate.disable.terminate=SI\ Provisioning\ Only

truaccess.fixedtemplate.reconciliation=ReconciliationDefaultProc
ess


si.recon.webservice.report.generate=2
```

TruAcess Properties Used for Reconciliation

The following table explains properties supporting reconciliation in Select Identity.

Property	Required	Default	Description
`truaccess.recon.rootdir`	Yes	None	The root directory for reconciliation data files. If you add a sub directory to this directory, you must add the same to the `truaccess.recon.staging` directory
`truaccess.recon.stagingdir`	Yes	None	The working directory for reconciliation.
`truaccess.recon.backupdir`	Yes	None	The backup directory for completed automated job data files.
`truaccess.recon.filename.timeformat`	No	yyyy_MM_dd_H_mm	The format of the time section within the reconciliation filename. (Disabled for current implementation)
`truaccess.recon.task.check.threshold`	Yes	Default = 30. No less than **3** recommended	The number of non-authoritative resource tasks to hold to enable the authoritative resource tasks to complete first. Adjust according to application server configuration and performance.
`truaccess.batch.inprogresstimeout`	Yes	18000000 seconds	The time-out for when an in-progress batch can be processed again.
`truaccess.batch.reportdir`	No	None	The directory to store XML reports for reconciliation, user import, and service assignment. These reports are sent to the administrator who created the job.
`com.hp.ovsi.connector.changLogFiel`	Yes	c:\\Temp\ \recon_modify.xml	Directory where the log file is stored.

Property	Required	Default	Description
si.reconciliation.polling.keyfield.LDAPLocal	No	UserName	Specifies the default keyfield in an SPML request.
truaccess.resource.record.max	Yes	1000	This parameter specifies the maximum number of users during reconciliation.
com.hp.ovsi.default.workflowtemplate.service.change.recon	Yes	SI\ Provisioning\ Only	Workflow template used to make changes to services
si.recon.webservice.report.generat	Yes	2	Determines whether to generate and send a report each time Web Service Recon completes 0=Never 1= Only at the initial request when no request is processed 2=Always

Sample Modify Request

For example, suppose Select Identity receives a reconciliation modify request from a resource called LDAP_Users:

1. The system first checks the `TruAccess.properties` file to see if the property `truaccess.fixedtemplate.recon_modify.LDAP_Users` is defined. If it is, then the specified workflow is picked up.
2. If not, then the system checks to see if there is a workflow template defined in the Resources page of Select Identity.

View a resource by navigating to **Service Studio Æ Resources** then selecting the Resource you want to view and clicking the **View** button. See the defined workflow by selecting User Reconciliation Policy from the left panel.

3 If not, the system checks for the property `truaccess.fixedtemplate.recon_modify` (this time without any resource). If so, this template is picked up.

4 If not, the system checks for the property `truaccess.fixedtemplate.reconciliation`, and picks up the template defined here.

Managing Reconciliation Jobs

Create and schedule a job to reconcile data. You must create an SPML file used to capture and disperse the necessary data before creating a Reconciliation Job. You may need an XML Rule file as well. See Rules on page 365 to learn more about creating Reconciliation Rules files.

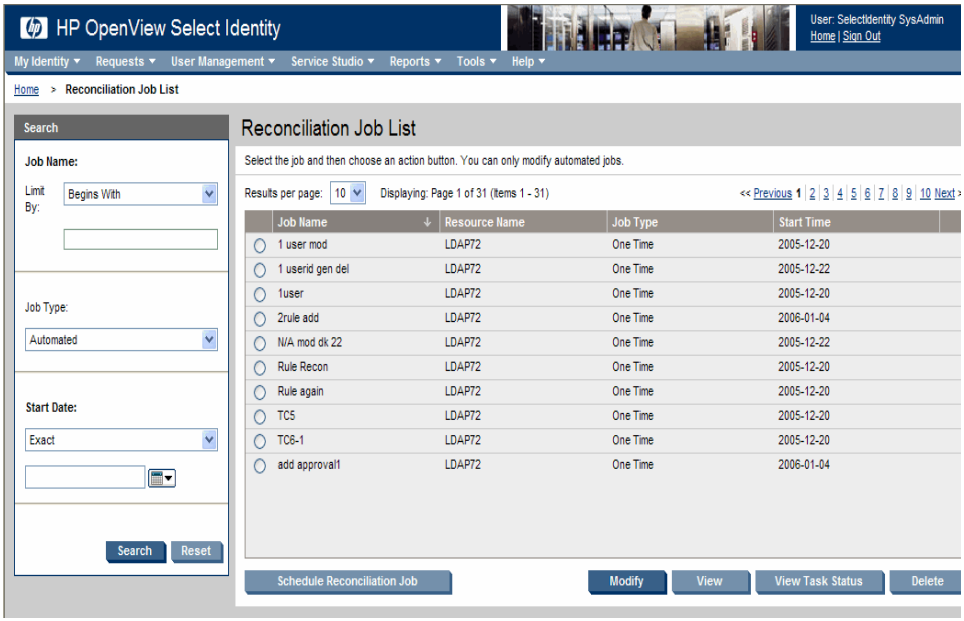
This section covers the following:

- Viewing Existing Reconciliation Jobs
- Scheduling Jobs
- Modifying Scheduled Jobs
- Deleting a Scheduled Job

Viewing Existing Reconciliation Jobs

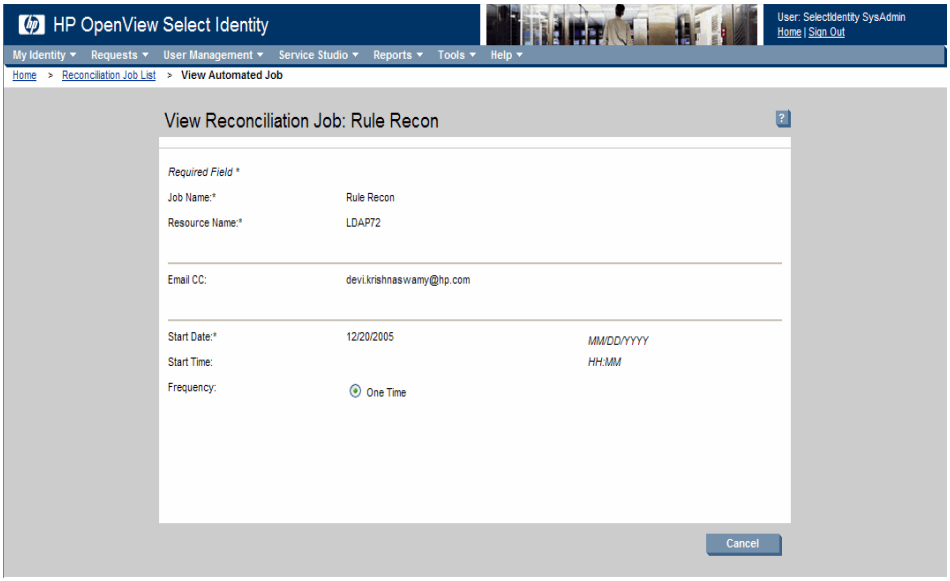
1 Select **Tools > Reconciliation > Reconciliation Job List** menu options. The **Reconciliation Job List** opens.

Figure 163 Reconciliation Job List



2 Select the job you want to view and click **View**.
The **View Reconciliation Job: Job Name** page opens.

Figure 164 View Reconciliation Job: Job Name



3 Review the job details.

4 Click **Cancel**.
Returns to the **Reconciliation Job List** page.

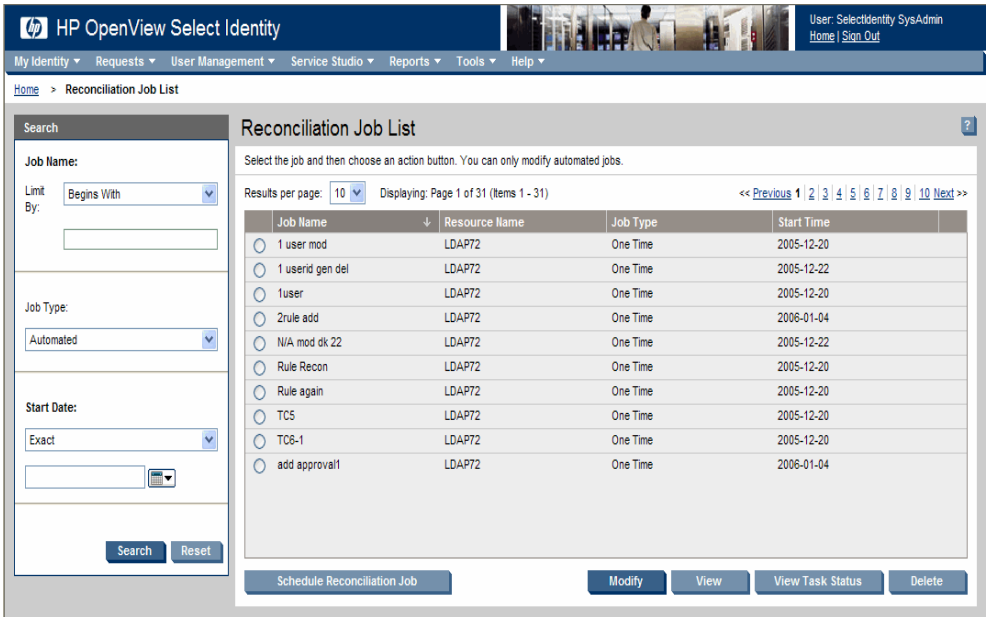
Select any job and click **View Task Status** to see the status of the job.

Scheduling Jobs

Perform the following steps to run a reconciliation job once:

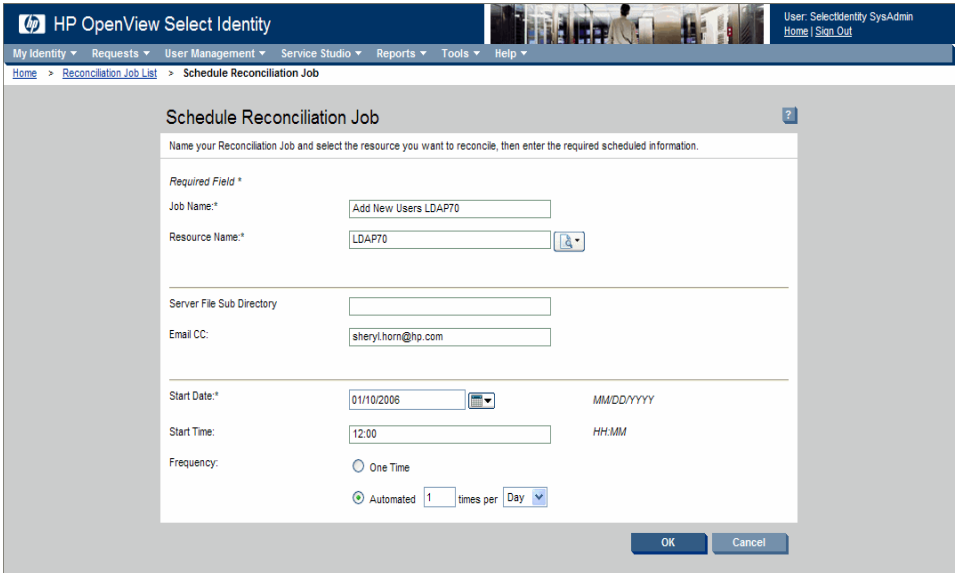
1 Select **Tools > Reconciliation > Reconciliation Job List** menu options.
The **Reconciliation Job List** opens.

Figure 165 Reconciliation Job List.



2 Click **Schedule Reconciliation Job**.
The **Schedule Reconciliation Job** page opens.

Figure 166 Schedule Reconciliation Job



3 Tab from field to field and enter the required information.

Field	Action
Job Name	Enter a descriptive name.
Resource Name	Enter the name of the resource you want to provision. By clicking the browse button, you can filter the resource name.
Server File Sub Directory	If it's a one time job mention the path and filename by clicking the browse button. If it's a automated job by default, the file is picked up from the path mentioned in the truaccess.properties file. You need to place the files in that path on server, which is usually recon root folder, and the field can be kept null in this case.

Field	Action
Email C.C:	Enter the email address of another user if you want someone notified when the job creates in addition to the job creator. Select Identity automatically notifies the creator of the job.
Start Date	Enter the date you want the job to run in the designated format.
Start Time	Enter the time in an HH:MM format that you want the job to begin.

4 Determine the frequency of the job.

If	Then
This is a job you only want to run once	Select **One Time**.
This is a job you want to schedule to run two or more times	Select **Automated**, then enter the number of times per time period that you want the job to run and select the time period from the drop down menu. For example if you select 1 time per Hour, then the job will begin at the Start Time specified and run every hour thereafter. Make sure the job has time to finish before being started once more.

5 Click **OK.**
Schedules the job.

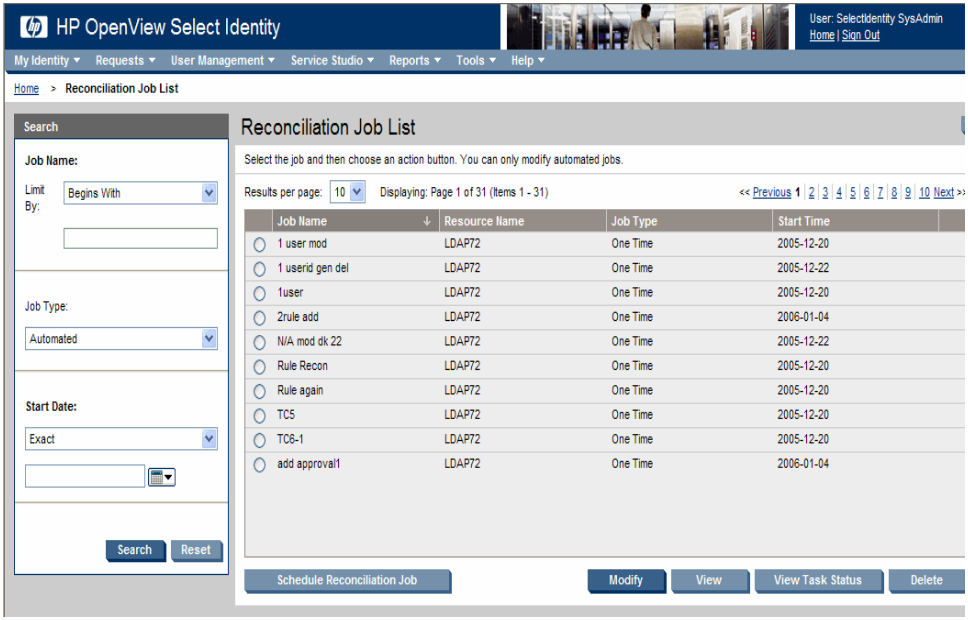
Modifying Scheduled Jobs

Perform the following steps to modify a scheduled job.

One time jobs and jobs that have completed cannot be modified.

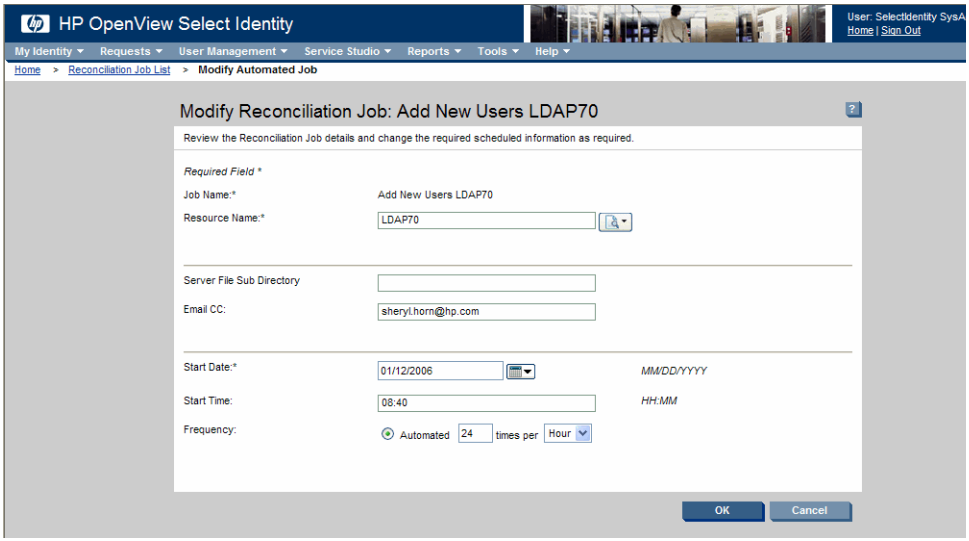
1 Select **Tools > Reconciliation > Reconciliation Job List** from the menu options. The **Reconciliation Job List** opens.

Figure 167 Reconciliation Job List.



2 Click **Modify**.
The **Modify Schedule Reconciliation Job** page opens.

Figure 168 Schedule Reconciliation Job



3 Review each field and modify the information as required.

Field	Action
Job Name	A descriptive name.
Resource Name	The resource you want to provision.
Server File Sub Directory	Specifies a sub directory where the resource resides. If nothing is mentioned, by default the system picks the path from the Truaccess.properties file.
Email C.C:	The email address of another user if you want someone notified when the job creates in addition to the job creator. Select Identity automatically notifies the creator of the job.
Start Date	The date you want the job to run in the designated format.
Start Time	The time in an HH:MM format that you want the job to begin.
Frequency	Entries determine how often the job runs.

4 Click **OK.**
Saves the changes and returns to the **Reconciliation Job List**.

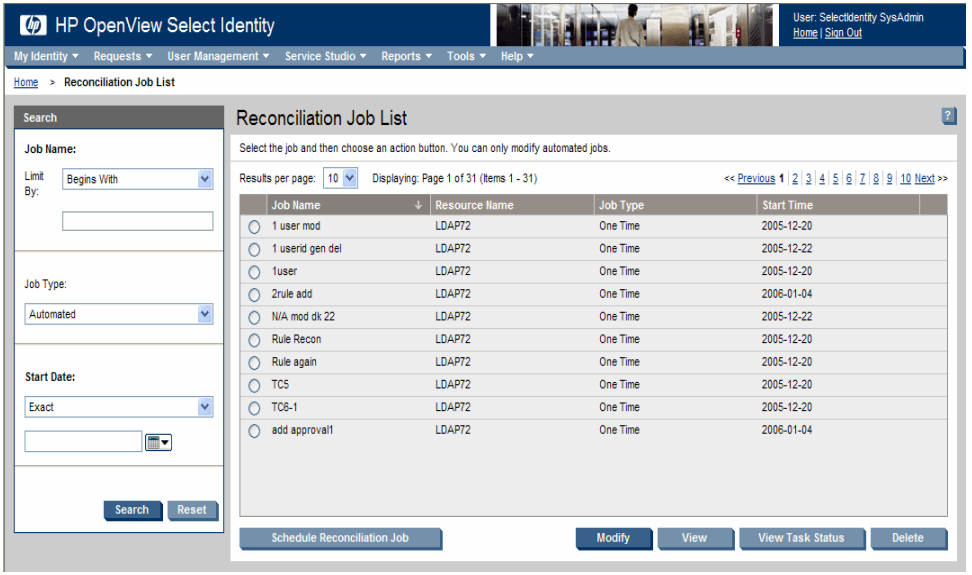
Deleting a Scheduled Job

Perform the following steps to delete a periodically scheduled reconciliation job:

One time jobs cannot be deleted.

1 Select **Tools > Reconciliation > Reconciliation Job List** menu options.
The **Reconciliation Job List** opens.

Figure 169 Reconciliation Job List.



2 Select the job you want to delete.

3 Click **Delete**.
Opens the confirmation dialog box.

4 Click **OK**.
Deletes the scheduled job.

Task Status

Each time a reconciliation request is scheduled, Select Identity creates a corresponding task. Tasks are generated from multiple sources.

- A one time scheduled task
- A scheduled task repeated at specified intervals
- A Web Service Reconciliation Request
- A Resource Change Polling Request

Tasks are listed in the Reconciliation Task List and can be viewed at any time. If a task is marked complete the Select Identity request has been generated successfully. View the status of the request on the Request Status List page. Learn more about Reviewing Requests on page 334 The system also provides additional information in detailed reports you can generate for each task.

This section covers the following:

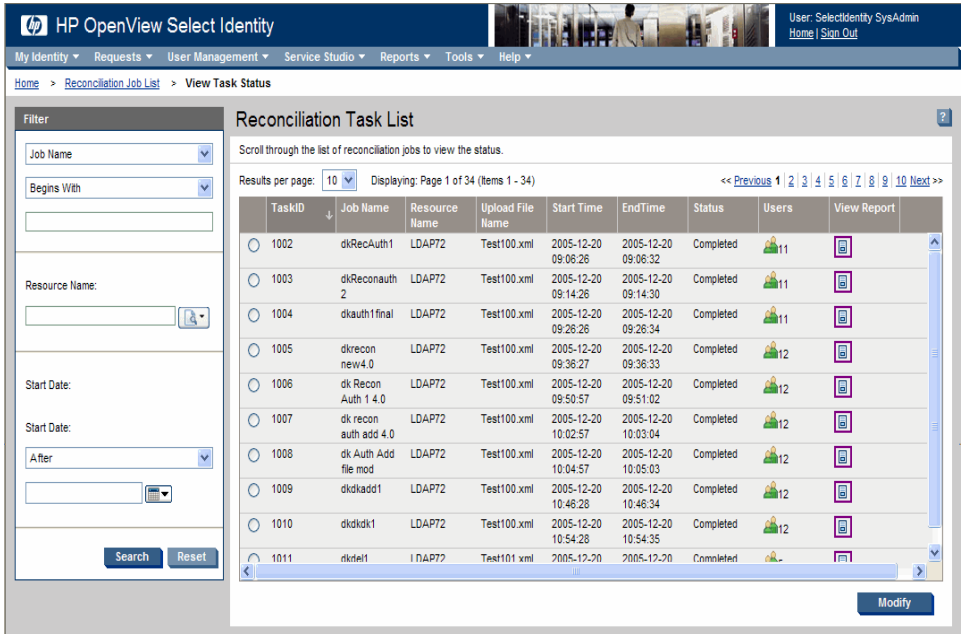
- Viewing the Task Status
- Generating a Reconciliation Task Report

Viewing the Task Status

Perform the following steps to view the task status:

1 Select **Tools > Reconciliation > Reconciliation Task List** menu options. The **Reconciliation Task List** opens.

Figure 170 Reconciliation Task List.

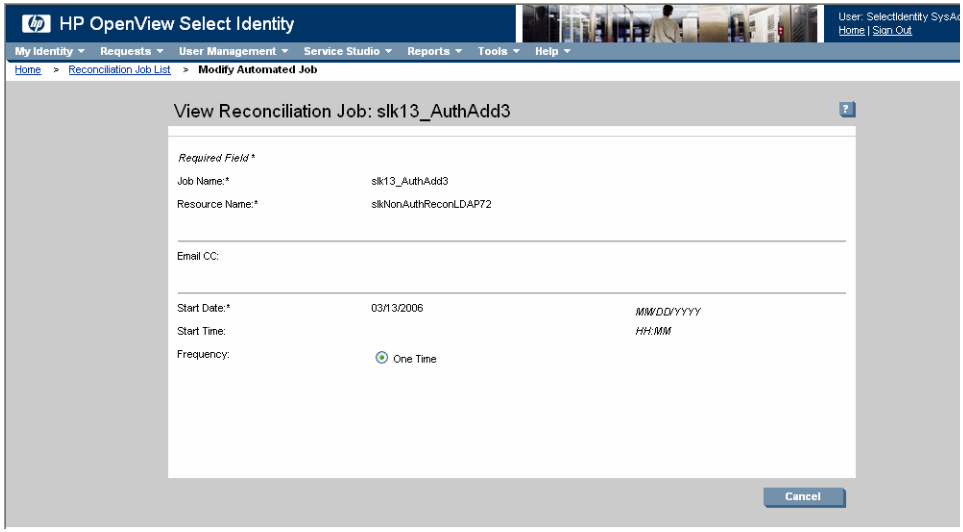


2 Select the task you wish to view. Use the filter options in the left pane to narrow the selection. Filter by:

- Job Name or TaskID
- Resource Name
- Start Date
- Status

3 Click **Modify**.
The **View Reconciliation Job [Job Name]** page opens.

Figure 171 View Reconciliation Job Page



Understanding Job Results

After each of the reconciliation jobs completes, an email is sent with the report details such as Is the job successful or not and Total users, how many passed and failed. A final report can be generated to see the results if necessary. Using this report, you can make any needed corrections to your SPML file and resubmit the file with only those accounts that failed. You will need to create a new job with a unique name to upload the file in the Select Identity client once more.

If you are the creator of the job that ran initially, you cannot give the new job the same name. Each job you create must be assigned a unique name.

This section covers the following:

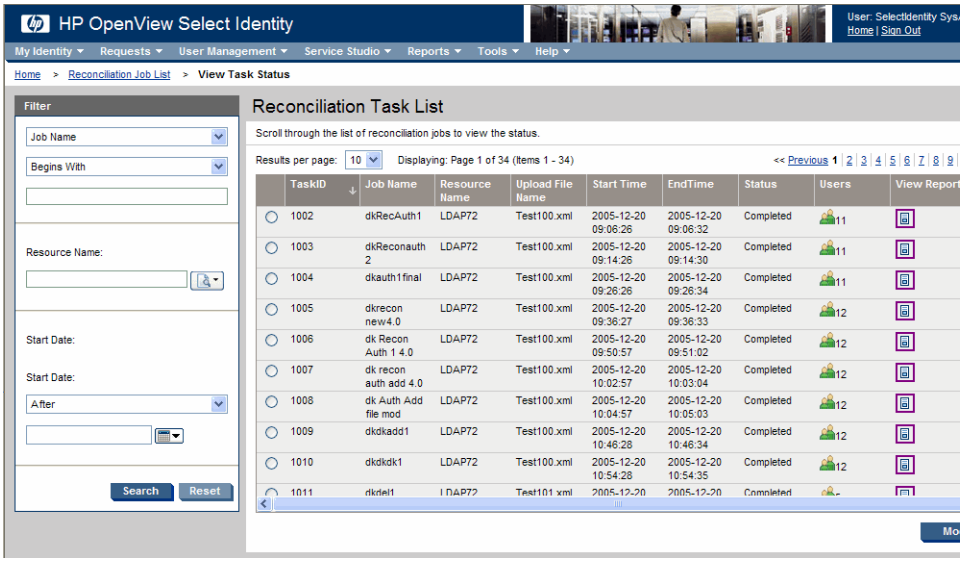
- Understanding Results
- Non-Authoritative Results
- Managing Reconciliation Jobs

Generating a Reconciliation Task Report

Perform the following to manually generate a Reconciliation Task report.

1 Select **Tools > Reconciliation > Reconciliation Task List** menu options.
The **Reconciliation Task List** opens.

Figure 172 Reconciliation Task List.



2 Select the task you would like reported.

3 Click the icon.
Opens the confirmation dialog box.

4 Click **OK**.
Generates the report. A window opens with the path and filename where the report was generated.

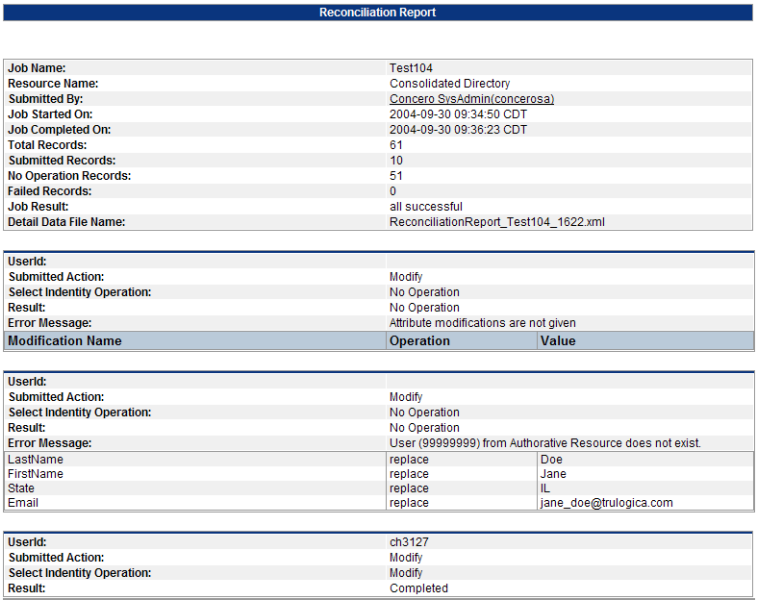
> Reports may take several minutes to generate.

5 Locate the report in the directory you designated to store reports.

> If you included your name and email address when creating the job, the report is emailed to you.

6 Open the report.
Report appears in your default browser.

Figure 173 Sample Report



Reconciliation Report

Job Name:	Test104
Resource Name:	Consolidated Directory
Submitted By:	Concero SysAdmin(concerosa)
Job Started On:	2004-09-30 09:34:50 CDT
Job Completed On:	2004-09-30 09:36:23 CDT
Total Records:	61
Submitted Records:	10
No Operation Records:	51
Failed Records:	0
Job Result:	all successful
Detail Data File Name:	ReconciliationReport_Test104_1622.xml

UserId:		
Submitted Action:	Modify	
Select Indentity Operation:	No Operation	
Result:	No Operation	
Error Message:	Attribute modifications are not given	
Modification Name	**Operation**	**Value**

UserId:		
Submitted Action:	Modify	
Select Indentity Operation:	No Operation	
Result:	No Operation	
Error Message:	User (99999999) from Authorative Resource does not exist.	
LastName	replace	Doe
FirstName	replace	Jane
State	replace	IL
Email	replace	jane_doe@trulogica.com

UserId:	ch3127
Submitted Action:	Modify
Select Indentity Operation:	Modify
Result:	Completed

7 Review the report online.

8 Print the report if necessary by selecting the **File** → **Print** options on your browser.

9 Close the report.

Understanding Results

Results are determined by policies evaluated based on the Select Identity request. One request per user handles multiple operations.

Policy Evaluation

Policies are evaluated an acted upon according to the priorities listed below:

- Attribute level policy actions are evaluated and applied first.
- Global level policy actions are evaluated and applied when no attribute level policies exist.

- Resource level actions are applied when no policies exist.

Actions

Based on the policies evaluated, Select Identity performs the following actions on a User Request:

- Basic - performs the minimum allowed actions based on the request event type.
- Re-sync - synchronizes the actions to other mapped resources.
- Rule - completes the actions in the specified rule as designated by the rule.
- Rule or Auto - Action is either performed based on the rule given if the rule is appropriate for the user. Else predefined rules are executed.
- Auto - predefined rules are executed.
- Rule and Auto - Action is performed based on the rule given if the rule is appropriate for the user and predefined rules are executed.

Authoritative Resource

- Action = **add**
  Expect the following results for each action when the default is set to Rule and the Resource Action is set to Accept.
  - If user account does not exist in Select Identity, and it is listed in the data file, the account is created with all specified attributes and values.
  - If an account already exists in Select Identity but is disabled, the workflow process is started to enable the account. The account attributes are then modified based on the authoritative resource.
  - If there are rules enabled for this action, Select Identity checks to see if new Service access should be granted to the user. Each resource can only have one rule for reconciliation. This action can only take place for new accounts. Only one resource can be authoritative.
  - If a rule is not assigned, user accounts are added to all Services that rely on the specified resource. The user account is also added to all other resources on which each Service relies. All attributes are updated based on the configuration of each Service.

- Provisioning occurs for resources other than the source resource managed through the new Service additions. The workflow requests should be encapsulated in a single request per user.
- Select Identity attributes used for storage are changed first, such as key fields mentioned in Creating an SPML File Containing Users and Attributes on page 417. Service mapping and additional attributes (for example, fixed attributes) are saved based on the provisioning result and post provisioning policy set in `TruAccess.properties` file.

- Action = **modify**
  Expect the following results whenResourceAction is set to Accept and no policies can be located from change attributes causing reconciliation to default to Rule.
  - If a user account does not exist in Select Identity, the account is skipped and it is listed as an error in the job results report.
  - If there is no attribute or value change for an account, the action is rejected.
  - A modify request is submitted for each user. Provisioning will determine which resources need to be synchronized.
  - When the workflow returns to the reconciliation post provisioning, the attribute values in Select Identity are updated based on the provisioning result and post provisioning policy set in the `TruAccess.properties` file.
  - The user profile is checked against Service mapping (no fixed attributes will be assigned to the user), to see if any new Service assignments are gained or lost. The Services to be checked should meet these conditions:
    - The Service uses this resource or the user is already assigned to the Service.
    - The user has access to all the resources required by the Service.
    - The Service has attributes that are changed.

    If the user can be assigned to a new Service, the account is added to or modified in the Service.

    If the modification makes the user ineligible for a Service, the user will be removed from the Service and the appropriate entitlements are deleted. The Authoritative Resource Key attribute will never be

deleted. Non-Authoritative Resource Keys may be deleted if the user is removed from the last Service on the Resource, depending on the Resource “Delete User” setting.

- Action = **delete**
  Expect the following results when ResourceAction is set to Accept.
  - If user is not on Select Identity, the action is skipped and reported.
  - The assigned workflow is started to terminate the user. Depending on the termination policy, the user may just be disabled for a period of time.
  - When the workflow returns to the reconciliation post provisioning, update the attribute/values on Select Identity based on the provisioning result and post provisioning policy set in the `TruAccess.properties` file.

Non-Authoritative Results

- Action = **add**
  Expect the following results for each action when the default is set to Rule and the ResourceAction is set to Accept or Accept New.
  - If the user account does not exist on Select Identity, the action is skipped and reported.
  - If the attributes to be added are not defined as authoritative or they contain a value in Select Identity, the add action is ignored.
  - The `Resource_KEY` attribute is added.
  - If Modify Attributes has the Sync-in property set to true then Select Identity is updated and appropriate resources are synchronized.
  - An add request is submitted for each user. Provisioning will determine which resources need to be synchronized.
  - When the workflow returns to the reconciliation post provisioning, the attribute values in Select Identity are updated based on the provisioning result and post provisioning policy set in the `TruAccess.properties` file.
  - The user profile is checked against Service mapping (no fixed attributes will be assigned to the user), to see if any new Service assignments are gained or lost. The Services to be checked should meet these conditions:

- The Service uses this resource or the user is already assigned to the Service.
- The user has access to all the resources required by the Service.
- The Service has attributes that are changed.

- Action = **modify**
  - If the user account does not exist on Select Identity, the action is skipped and reported.
  - The action will be rejected if
    - there are no entitlement changes.
    - the attributes to be modified in Select Identity are not defined as authoritative attributes or they contain a value
  - The `Resource_KEY` attribute will not be added if not present.
  - A modify request is submitted for each user. Provisioning will determine which resources need to be synchronized.
  - When the workflow returns to the reconciliation post provisioning, the attribute values in Select Identity are updated based on the provisioning result and post provisioning policy set in the `TruAccess.properties` file.
  - The user profile is checked against Service mapping (no fixed attributes will be assigned to the user), to see if any new Service assignments are gained or lost. The Services to be checked should meet these conditions:
    - The Service uses this resource or the user is already assigned to the Service.
    - The user has access to all the resources required by the Service.
    - The Service has attributes that are changed.
- Action = **delete**
  - If the user account does not exist on Select Identity, the action is skipped and reported.
  - Run this user profile against the Service mapping, delete user from all assigned Services that use this resource and delete the entitlements and `Resource_KEY` attribute.

— There is single request per user. When the workflow returns to the reconciliation post provisioning stage, the attributes and values are updated on Select Identity based on the provisioning result and post provisioning policy set in the `TruAccess.properties` file.

Troubleshooting in Reconciliation

Listed below are some common issues.

Failed Requests Using Reconciliation to Add Thousands of Users from Oracle

Consider the following options:

- Use User Import to add new users to the system when you plan to add thousands of users to the system
- Ask your DBA to schedule more frequent jobs to gather statistics
- Run the following script manually every 50K to 100K users.

```
exec dbms_stats.gather_schema_stats ('OVSI_SCHEMA_NAME',
estimate_percent=>DBMS_STATS.AUTO_SAMPLE_SIZE,
method_opt=>'FOR ALL COLUMNS SIZE SKEWONLY', cascade=>TRUE);
```

- Make sure that old executions plans are flushed from the system. Flush all execution plans, using this command:

```
alter system flush shared_pool;.
```

Other smart databases may encounter this same issue.

16 Export and Import Configurations

HP OpenView Select Identity provides a configuration management function that enables you to import and export the following configuration types from one environment to another:

- Attributes
- Notification Templates
- Request instance Reports
- Resources
- Services
- Workflow Application Definitions
- Workflow Templates

There may be many times when you want to export a configuration and import it into a new instance of HP OpenView Select Identity. For example, you may have set up your HP OpenView Select Identity system in a test environment and now you want to export your configuration to a production environment. Use the Import / Export Configuration functionary to export the configuration to your production environment using XML files. All data is imported and exported through XML files.

This chapter covers the following:

Exporting a Configuration

Configurations may be exported in any order. However, it is a good idea to export configurations in the order that your services were created to make sure that you do not miss any dependent configurations.

Create a directory to store your exported XML files so that you can easily validate that you captured all configurations necessary.

This section covers the following topics:

- Understand Dependencies
- Export a Configuration File
- Editing an XML file

Understand Dependencies

Exported configuration files that do not contain errors import into HP OpenView Select Identity without issues. However, the successful import of data does not mean that the functionality associated will work as expected. All configurations and any other supporting files on which the function depends must be present in order for the imported functionality to work as planned.

For example, resource configurations can depend on attribute configurations when a resource attribute is mapped to an HP OpenView Select Identity attribute. Resource configurations may contain rule names that are part of the User Reconciliation Policy and if the Rule has not been added to HP OpenView Select Identity the imported resource will not have the rule name populated. Rules can not be imported or exported but can be added (similar to import) and modified (similar to export). Take great care to export all dependent configurations. Dependencies are detailed below:

Functional Area	Dependences
Attributes	No dependencies
Notification Templates	Workflows that use the notification templates.
Request Instance Report	Associated Workflows which include the report in an instance block.

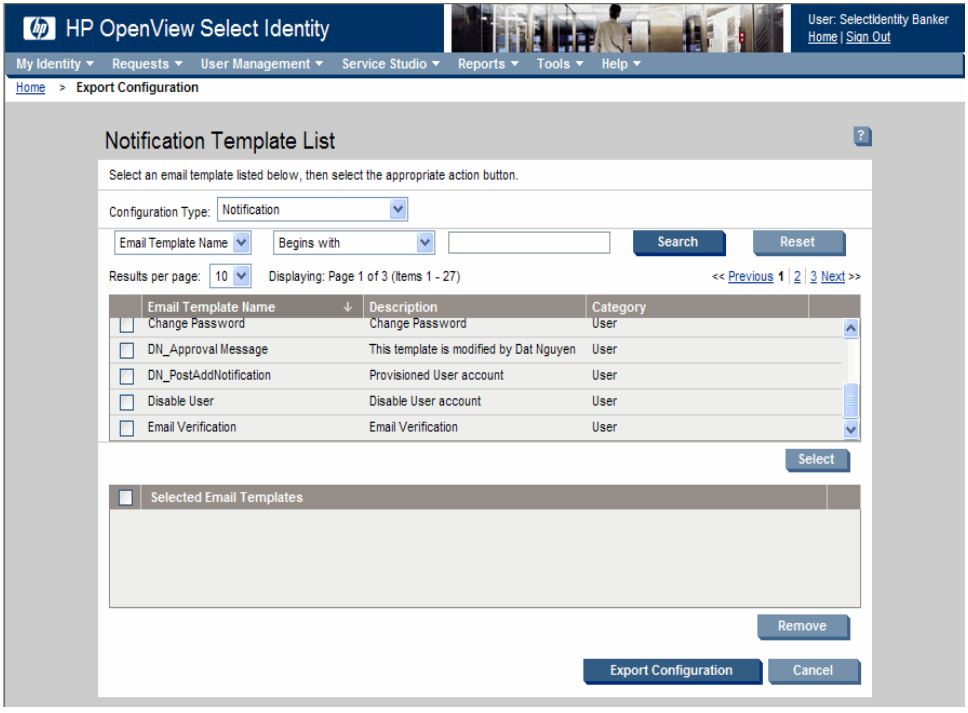
Functional Area	Dependences
Resource	Attribute configurations associated with the resource. Rules used to provision the resource during reconciliation.
Service	All resource configurations associated with the service. All attribute configurations associated with any associated resource. Any notification templates associated with Workflows used to provisioning the service. Workflows used to provision the service. External calls on which any associated Workflows depend.
Rules	Resources provisioned by the reconciliation rules imported.
Workflow Application Definitions	Associated Workflow template. Do NOT export or import the WfAppDefine and wfReport xml files. Request assistance from HP Support if you need to move these files.
Workflow Template	Notification templates required by the Workflow. All resource configurations associated with the service. All attribute configurations associated with any associated resource. Services provisioned by the Workflow. Request Instance Report associated with the Workflow. Workflows application definition associated with the Workflow. External calls on which the Workflow depends.

Export a Configuration File

Perform the following steps to export configuration information:

1. Select the **Tools** → **Import/Export Configurations** → **Export Configuration** menu options.
   The **Export Configuration** page opens.
2. Select the configuration option you want to export from the **Configuration Type** drop-down list.
   Opens the corresponding list of configurations available for export.

Figure 174 Sample Exported XML File



3. Review the list displayed and select the items you want to export.
4. Click the **Select** button.
   The selected items appear in the bottom panel.
5. Click **Export Configuration**.
   Opens the **File Download** dialog box.

6 Click **Save** and save the file to any location.
Opens the **Open** dialog box.

7 Click **Open** to verify the file downloaded correctly.
Opens the selected XML file

Figure 175 Sample Exported XML File

```
<ns1:Keys>
<ns1:Key Value="Add User" />
</ns1:Keys>
</ns1:Header>
<ns1:Body>
<XMLItem>
<?xml version="1.0" encoding="UTF-8" ?>
<java version="1.4.2_08" class="java.beans.XMLDecoder">
<object class="com.trulogica.truaccess.emailtemplate.model.EmailTemplateModel">
<void property="body">
<string>Your account has been successfully created. Login: [RQT:UserName] Service:
[REQ:ServiceName] Thanks</string>
</void>
<void property="categoryID">
<string>0702B969-9FCD-384B-42B8-DFEDAE06AB6F</string>
</void>
<void property="description">
<string>New User account</string>
</void>
<void property="domainID">
<int>1</int>
</void>
<void property="name">
<string>Add User</string>
</void>
<void property="replace">
<object class="java.util.Hashtable">
<void method="put">
<string>[RQT:Salutation]</string>
<string />
</void>
<void method="put">
<string>[RQT:UserName]</string>
<string />
</void>
<void method="put">
<string>[RQT:Password]</string>
<string />
</void>
<void method="put">
<string>[RQT:SIAdminRole]</string>
<string />
</void>
<void method="put">
<string>[RQSTR:FirstName] [RQSTR:LastName]</string>
<string />
</void>
<void method="put">
<string>[RQT:Domain]</string>
<string />
</void>
<void method="put">
<string>[RQSTR:Email]</string>
<string />
</void>
<void method="put">
<string>[REQ:ServiceName]</string>
<string />
</void>
</object>
</void>
<void property="senderEmail">
<string>[RQSTR:Email]</string>
</void>
<void property="senderName">
<string>[RQSTR:FirstName] [RQSTR:LastName]</string>
</void>
<void property="subject">
<string>[RQT:UserName] : Account created successfully</string>
</void>
<void property="toEmail">
<string>[RQT:Email]</string>
</void>
</object>
</java>
</XMLItem>
</ns1:Body>
</ns1:ConfigInfo>
```


8 Close the XML window to return to the **Export Configuration** page.

Editing an XML file

HP OpenView Select Identity exports all configurations in XML generated files. These files may be edited and changed following best practice XML editing techniques. For example, you may export a service configuration that matches the service you are creating exactly, except for the service name. Change all references to the service name in the XML file, then import the configuration file into the target application.

Errors in editing an XML file such as changing a service name in one reference but not in all, will cause the imported data to generate application errors once imported into the target HP OpenView Select Identity application.

1. Export the XML configuration file.
2. Edit the file.
3. Import the XML file into the target application.
4. Verify that all dependent configurations have been imported.
5. Test the import to make sure that the data behaves as expected.

Importing a Configuration

All configurations can easily be imported from one instance to another.

This section covers the following:

- Import Dependencies
- Import a Configuration File

Import Dependencies

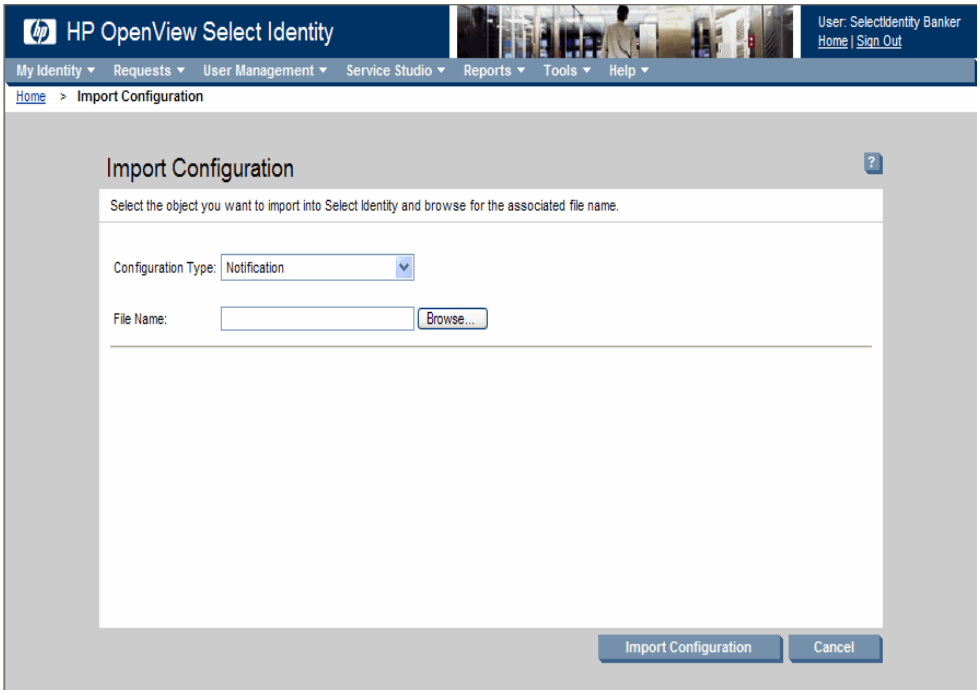
There are no dependencies required to import configurations. Configurations may be imported in any order. However, functionality that is dependent upon information in another configuration will not work properly until the dependent configuration has been imported. See Understand Dependencies on page 452 for more information.

Import a Configuration File

Perform the following steps to import a configuration file:

1 Select the **Tools** → **Import/Export Configurations** → **Import Configuration** menu options.
The **Import Configuration** page opens.

Figure 176 Import Configuration page



2 Select the configuration type you want to import from the **Configuration Type** drop-down list:

3 Click **Browse** and locate the correct XML file.

4 Select **Import Configuration** to import the XML data file.
A confirmation message displays.

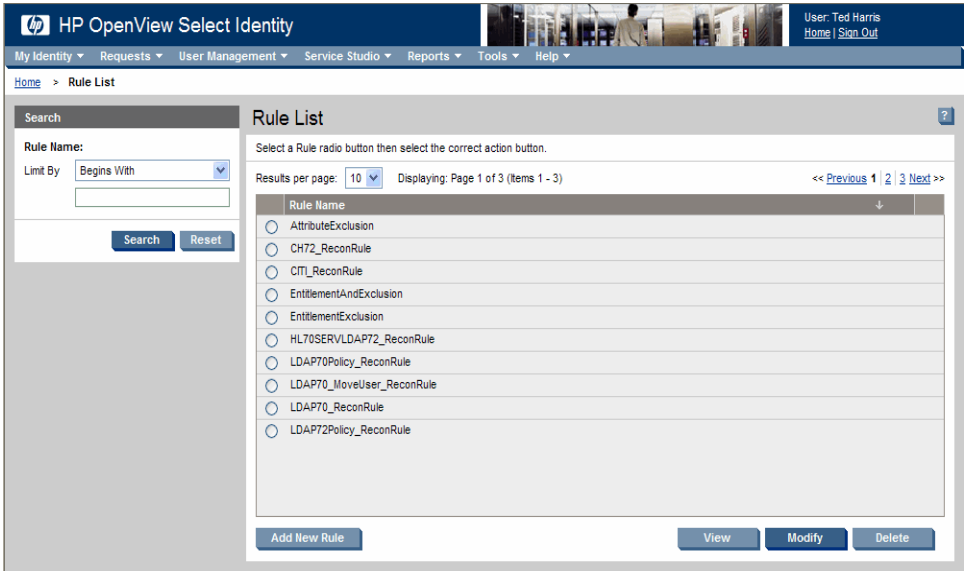
Adding Rules to Support New Configurations

Reconciliation rules must be included in the new configuration in order for Services to be provisioned through the reconciliation process correctly. Review the rules located on the import target application, then add any missing rule files from the export application necessary to support the imported configurations.

Add Rules

1. Open the HP OpenView Select Identity application used to export the selected configurations.
2. Select the **Tools** → **Rule** → **Rule List** menu options.
   The **Rule List** page opens.

Figure 177 Rule List from Export System



3. Review the list of rules to determine which ones are necessary to support the imported configurations.
4. View any rule in question in more detail by selecting the rule and clicking on **View**.
   Opens the Rule XML file.

5 Make a note of each Rule XML file name you want to add to the system containing the imported configurations.

6 Locate the XML file and open the target configuration.

7 Navigate to **Tools** → **Rule** → **Add New Rule**.
Opens the **Add New Rule** page.

8 Click on the **Step 2: Upload file** field and browse for the first XML file you want to import.

9 Click **OK**.

10 Continue until all necessary Rule XML files have been added to the target HP OpenView Select Identity configuration.

Troubleshooting Configurations

Listed below are common errors along with the information necessary to resolve the issue in most cases.

Service can not be found.

Make sure that all dependent configurations were imported when you imported your service. If not, import the required configurations now.

Validate any changes made to the service exported XML file. If errors exist, correct them and import the file.

Password not found.

Review the imported resource to determine if you imported the dependent Password attribute. If not, import the password attribute now.

Resource not found.

Check to make sure that all dependent configurations were imported when you imported your resource. Attributes fields required by the resource must exist in the target application. Import any missing attribute configurations now.

Validate any changes made to the resource exported XML file. If errors exist, correct them and import the file.

Import Failed

Verify that all known dependent configurations have been imported into the target application. If not, import the missing configuration now.

Validate any changes made to any exported XML files. If changes were verify that the changes are correct. Make sure that any name change was made consistently in each instance the name is used. Correct any errors and import the corrected configuration.

17 Audit and Configuration Reports

Select Identity auditing and reporting features enable your organization to produce context-driven, standard, and custom reports of user entitlements and system event history. Better reports and audits allow tighter control over information, reduced risk of security breach, and enforce higher levels of compliance with requirements and regulations.

This chapter provides details for all of the actions that you can perform within Audit Report and Configuration Report capabilities. Access to each of these functional areas is determined by the administrative roles assigned to your account by the Select Identity system administrator.

These reports are not the only reports available in HP OpenView Select Identity. You can generate reports pertaining to specific areas of Select Identity such as User Management in those areas.

Audit Reports

HP OpenView Select Identity provides audit reports for all Select Identity system functions. Audit reports provide the history of activities within the system. Audit reports detail historical transactions that have occurred in Select Identity. Select Identity does not record changes to the documents themselves. You can generate a single report or create a report template, which can be accessed each time you click Audit Reports.

The system audits changes to document attributes by logging the change to the document ID. You may choose to use a third party tool to view more extensive audit logging reports. The information necessary to access audit logging data is described in detail in Auditing XML and Client Sample beginning on page 553.

This section covers the following:

Available Audit Reports

Audit reports include both detailed reports and summary reports.

Generate an Audit report to view configuration activities for one or more specified accounts or services over a period of time. These reports detail all actions related to any user within HP OpenView Select Identity. These user actions include: Add New User, Modify User, Delete Service Membership, Enable All Services, Disable All Services, Reset Password, Add Service, Change Password, Forget Password, Enable Service Membership, Disable Service Membership, Terminate User, Login, Security Violation and Logout.

These reports can be generated based on different input data including specific user, Service, or Service and context. Data displayed for each report is configurable and may include a wide variety of columns.

Audit reports include:

- Audit User
- Audit User Summary
- Audit Summary
- Audit User Creation
- Audit User Deletion
- Audit User Termination
- Audit User Password
- Audit User Login
- Audit Hint

Audit User Summary Reports
These reports summarize all user account actions within Select Identity and provide a count for each action per Service and context. Only the number of changes is reported when you select a summary report. These user actions include: Add New User, Modify User, Delete Service Membership, Enable All

Services, Disable All Services, Reset Password, Add Service, Change Password, Forget Password, Enable Service Membership, Disable Service Membership, Terminate User, Security Violation, Login, and Logout.

The report can be generated either by specific Service or by specific Service and context. The report displays three columns per action which include Service Name, Context, and Count.

User Audit Summary reports include:

- Audit User Creation Summary
- Audit User Deletion Summary
- Audit User Termination Summary
- Audit User Password Summary
- Audit Summary Hint

Audit Service Report
Generate an Audit Service Report to view configuration activities for one or more specified services over a period of time. This report details all actions related to one or multiple Services within Select Identity.

Generating Audit Reports

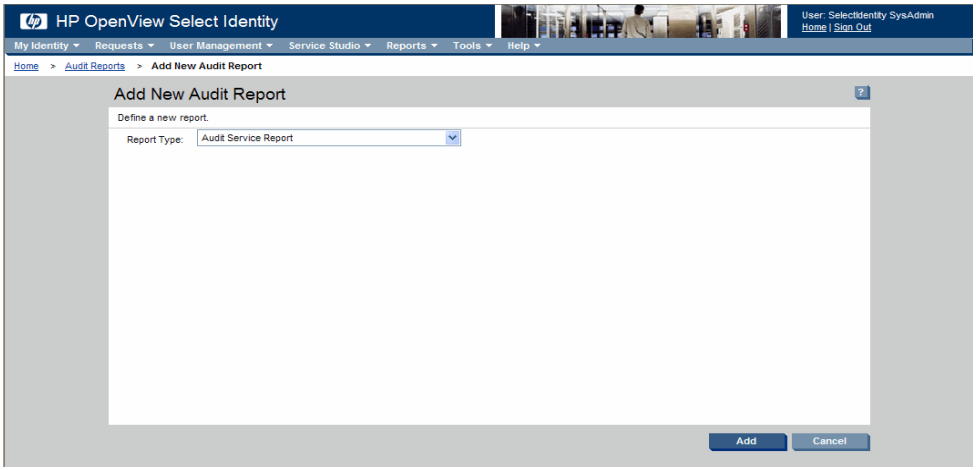
Reports are generated based on specific actions including delete, modify, import, and add. The type of data displayed for each report is configurable and is completely dependent upon the parameters selected during the generation process.

The procedure that follows uses the Audit Service report as an example of the steps necessary to generate a report. Steps required to generate a report are the same although the each report has different parameter options. See Understanding Report Parameters on page 485 for report parameter field definitions for each standard report

Follow the steps below to generate an audit report.

1 Select **Reports** → **Audit Reports** → **Add New Audit Report.**
The **Add New Audit Report** page opens.

Figure 178 Add New Audit Report Page



2 Select the type of audit report you want to generate from the drop-down list and click **Add**.
The **Add New Report** page opens with fields for adding the report parameters.

3 Complete in the fields as required to specify the parameters of your report.

The fields shown depend upon the type of report selected and may include fields not documented here. See Understanding Report Parameters on page 485 for report parameter field definitions for each standard report. When an optional parameter field does not contain a value the default value is All. For example, if you want to see the modifications to a specified user's accounts but you do not specify a service then all modifications made on any service supported will be reported. However, when one or more options are listed in a list box, only those options that are highlighted will be reported. Remove items from a list box by selecting the item and clicking the icon.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Actions	Highlight the item you want reported.
Fields	Highlight the fields you want reported.

.

Verify that all options you want reported listed in each list box are highlighted. Only highlighted items are reported even if you searched for and selected the item earlier.

4 Choose one of the following options for generating the report.

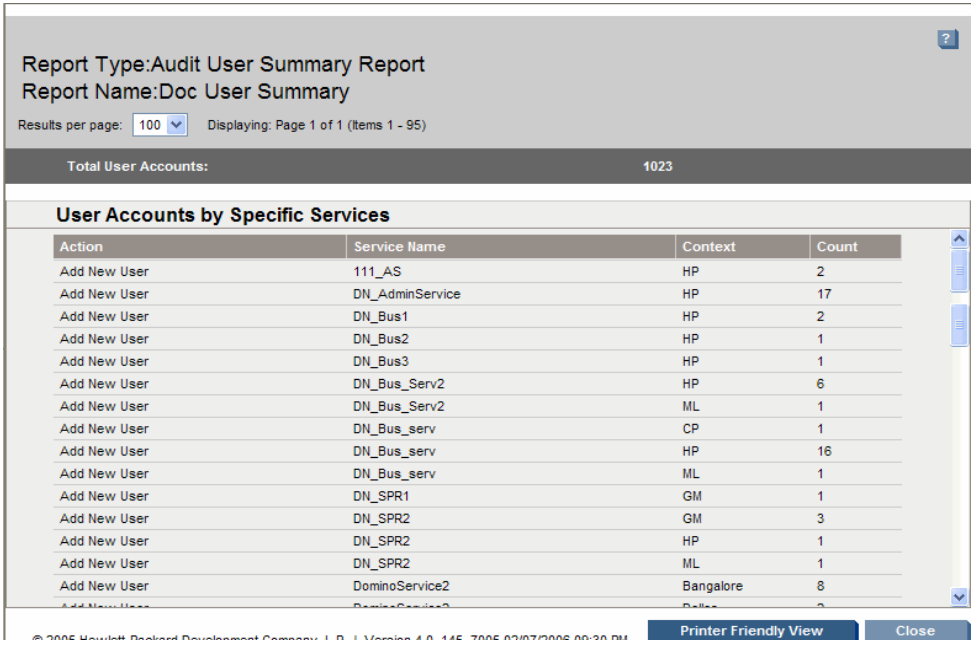
If	Then
You want to run the report without saving it	Click **Run Now.**
You want to save the changes you made and continue working	Click **Add and Run Now.**
You want to change report scheduling	Follow the instructions for Modifying a Report Schedule on page 477.

If	Then
You want to save your changes and close the page without printing the report	Click **Add and Schedule**.
You want to close this page without printing the report or saving your changes	Click **Cancel.** Returns to the Audit Report List.
You want to close the page without making any changes	Click **Cancel.** Returns to the appropriate report list.
You want to print the report	Complete the steps described in Printing a Report on page 479.

.

You must have authorization to view the information generated on a report. If you have the correct authorization the report opens in your browser window, if not an error message displays instead. Batch reports must be scheduled. The **Run Now** option may not be selected.

Figure 179 Sample Report Page



Configuration Reports

HP OpenView Select Identity provides configuration reports for user, administrator, and Service management activities. Configuration reports represent the state of Select Identity at the time the report is created. For example, an administrator can display all users associated with a Service context at a given time. You can generate a single report or create a report template that can be accessed each time you click **Configuration Reports**.

The following are descriptions of the available configuration reports.

User Configuration Report
Generate a User Configuration report to view active user accounts within Select Identity sorted by context. You can only view users that are currently active within your Service context. The report can be generated based on a

specific user, a specific Service, or specific Service and context. The type of data displayed for each report is configurable and may include User ID, First Name, Last Name, Email, Service, and Context.

User Configuration Summary Report
Generate a User Configuration Summary Report to summarize all current user accounts by Service and context within Select Identity. The report can be generated either by specific Service or by specific Service and context. The report displays data columns including Service Name, Context, and Count.

User Configuration Detail Report
Generate a User Configuration Detail Report to summarize all current user accounts by context attribute and value. The report displays data columns including Service Name, Context, and Count.

Admin Configuration Report
Generate an Admin Configuration Report to summarize all current users with administrative privileges. This report displays user information, administrative Service and context affiliation, and managed contexts and Services.

Resource Users Report
Generate a Resource Users Report to summarizer users/entitlements that are different between HP OpenView Select Identity and the Resource. Only differences are reported.

Resource Entitlements Report
Generate a Resource Users Report to summarizer users/entitlements that are in HP OpenView Select Identity, but are not provisioned to a Resource. Only differences are reported.

Resource Reconciliation Report
Generate a User Resource Reconciliation Report to compare users/entitlements in the Select Identity database with a selected LDAP or UNIX Resource. The report only displays the users/entitlements that are in a specified Resource that are not in Select Identity.

Generating Configuration Reports

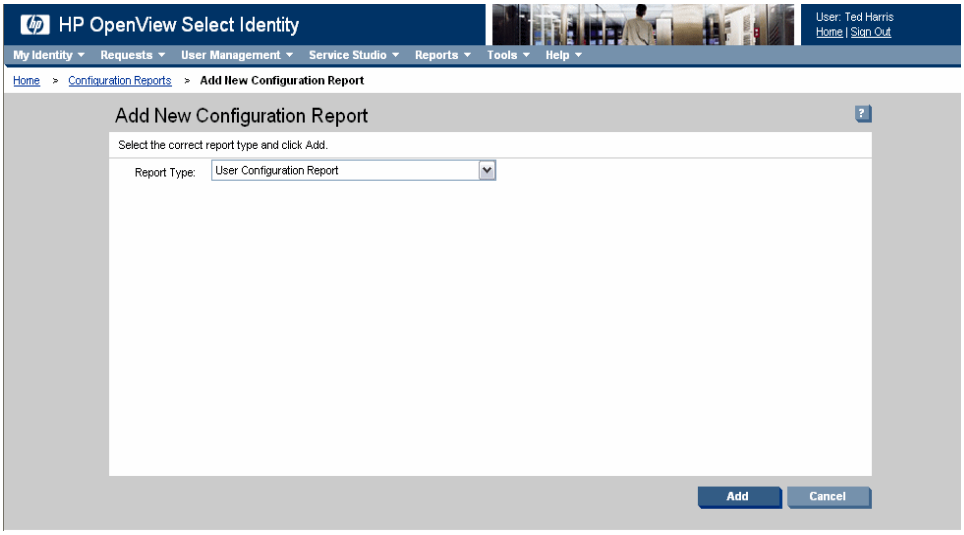
The configuration procedure for each report is similar. The following procedure uses the User Configuration Summary report as an example.

The procedure that follows uses the Audit Service report as an example of the steps necessary to generate a report. Steps required to generate a report are the same although the each report has different parameter options. See Understanding Report Parameters on page 485 for report parameter field definitions for each standard report

Perform the following steps to generate a configuration report.

1 Select **Reports → Configuration Reports → Add New Configuration Report.**
The **Add New Report** page opens.

Figure 180 Add New Configuration Report Page



2 Select the type of configuration report from the drop-down list and click **Add**.
The **Add New Report** page opens.

3 Select the report type from the drop-down menu.

4 Complete the fields required to define the parameters of your report.

The fields shown depend upon the type of report selected and may include fields not documented here. See Understanding Report Parameters on page 485 for report parameter field definitions for each standard report. When an optional parameter field does not contain a value the default value is All. For example, if you want to see the modifications to a specified user's accounts but you do not specify a service then all modifications made on any service supported will be reported. However, when one or more options are listed in a list box, only those options that are highlighted will be reported. Remove items from a list box by selecting the item and clicking the  icon

5

Field	Action
Report Name	The name for this report. This is a required field.
Items per page	Select the number from the drop-down list.
Order By	Select the order from the drop-down list.
Service Selection	Click the search icon to see a list of services. Select the service.
Context Attribute Selection	Select the actions that you want to audit from the **Actions** list by scrolling through the list to find the one(s) you want, You can select as many as applicable.
Fields	Choose the categories of information that you want to view from the **Fields** list.

Verify that all options you want reported listed in each list box are highlighted. Only highlighted items will be reported even if you searched for and selected the item earlier.

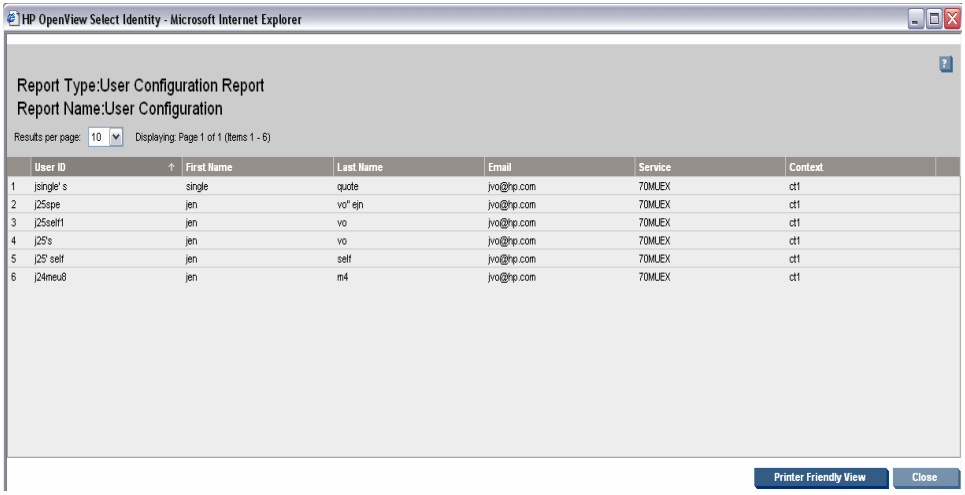
6 Determine how best to handle the report.:.

If	Then
You want to run the report without saving it.	Click **Run Now.**
You want to save the changes you made and continue working.	Click **Add and Run Now**.
You want to change report scheduling	Follow the instructions for Modifying a Report Schedule on page 477.
You want to save your changes and close the page without printing the report.	Click **Add and Schedule**.
You want to close this page without printing the report or saving your changes.	Click **Cancel.** Returns to the Configuration Report List.
You want to close the page without making any changes.	Click **Cancel.** Returns to the appropriate report list.
You want to print the report	Complete the steps described in Printing a Report on page 479.

.

You must have authorization to view the information generated on a report. If you have the correct authorization the report opens in your browser window, if not an error message appears instead.The Run Now option is not available for detailed reports.

Figure 181 Sample Report



Managing Scheduled Reports

Reports may be scheduled to run once on a designated time and day or to run at regularly determined intervals. When a scheduled report is generated HP OpenView Select Identity emails the report if it is within the predetermined size limit or emails a notification that the report is ready to designated recipients. Email notifications include a designated path link to the generated report, which is automatically stored at a predetermined location.

The report size limitation and report storage location are configurable through the `TruAccess.properties` file, which is described in the *HP OpenView Select Identity Installation Guide*.

This section covers the following:

- Scheduling a Report
- Editing Scheduled Report Settings
- Modifying a Report Schedule
- Printing a Report
- Copying a Report

- Inactivating and Reactivating a Scheduled Report
- Deleting a Report

Scheduling a Report

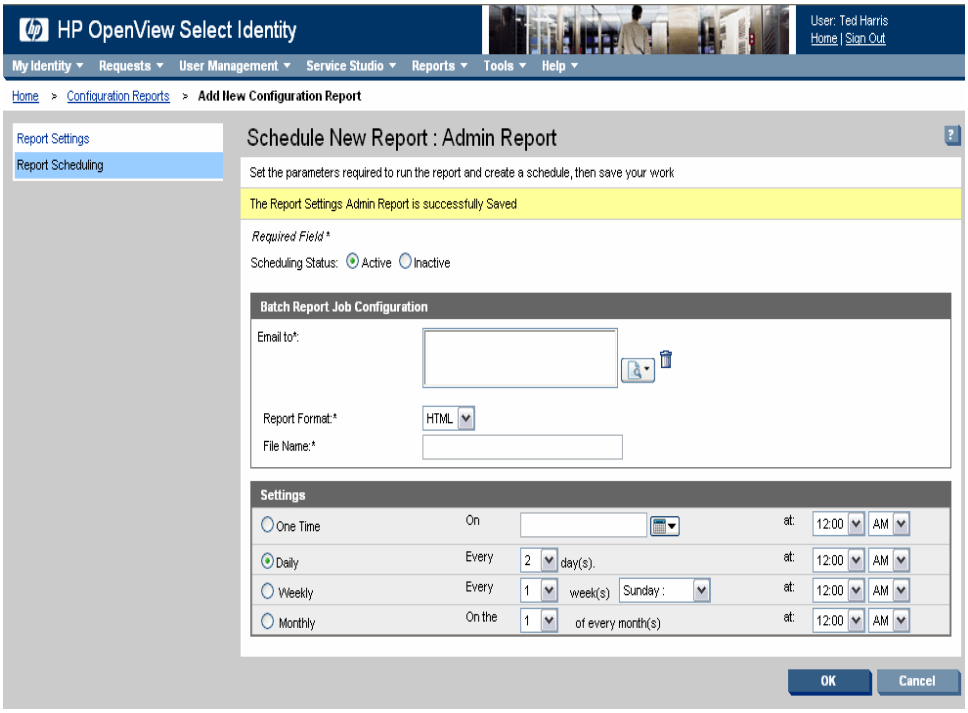
Although any report may be scheduled, detailed reports must be scheduled to run in batch mode. Reports may be scheduled from any report list page. Follow the steps below to schedule a batch report:

1 Create a report following the correct procedure.

If	Then
You want to create an Audit Report	Follow the steps documenting in the Generating Audit Reports section on page 463.
You want to create a Configuration Report	Follow the steps presenting in the Generating Configuration Reports section on page 469

2 Click **Add and Schedule**.
The **Schedule New Report: Report Name** page opens.

Figure 182Schedule NewReport Page



3 Complete the following fields. as necessary

Field	Action
Scheduling Status	Accept the default **Active**.
Email to	Click the icon and select the email addresses of those individuals you want to receive the scheduled report.

Field	Action
Report Format	Choose the proper format from the drop-down menu.
File Name	Enter a unique file name.
Report Scheduling	Review the radio button options and determine the appropriate time period. • One Time • Daily • Weekly • Monthly Determine how frequently you want the report to run within the selected time period, then select the time of day you want to generate the report.

If the report is larger than the maximum size allowed to be sent by email, you will receive an email notifying you that the report file is saved at a specified location on your server.

4 Click **OK**.
Schedules the report and returns to the Configuration Report List page.

Editing Scheduled Report Settings

Once you have created a scheduled report, you can modify the settings at any time.

When an optional parameter field does not contain a value the default value is All. For example, if you want to see the modifications to a specified user's accounts but you do not specify a service then all modifications made on any service supported will be reported. However, when one or more options are listed in a list box, only those options that are highlighted will be reported.

Remove items from a list box by selecting the item and clicking the  icon.

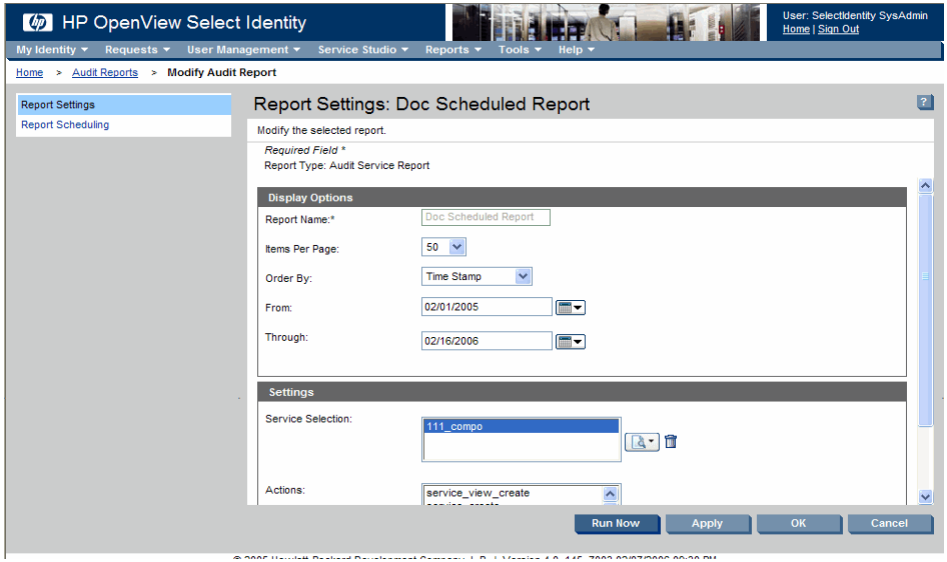
Complete the steps below to modify report settings:

1 Navigate to the appropriate report list page.

If	Then
You want to modify the schedule on an Audit Report	Click **Reports** → **Audit Reports** → **Audit Reports List**. Opens the **Audit Report List** page.
You want to modify the schedule on an Configuration Report	Click **Reports** → **Configuration Reports** → **Configuration Reports List**. Opens the **Configuration Reports List** page.

2 Select the report you want to modify and click **Modify Settings**.
The **Report Settings: Report Name** page opens.

Figure 183Report Settings: Report Name Page



3 Review the display options and settings shown and make changes as necessary.

Settings shown depend upon the report selected.

4 Determine how best to handle the report.:

If	Then
You want to run the report without saving it.	Click **Run Now.**
You want to save the changes you made and continue working.	Click **Add and Run Now.**
You want to change report scheduling	Follow the instructions for Modifying a Report Schedule on page 477.
You want to save your changes and close the page without printing the report.	Click **Add and Schedule**.
You want to close this page without printing the report or saving your changes.	Click **Cancel.** Returns to the Configuration Report List.
You want to close the page without making any changes.	Click **Cancel.** Returns to the appropriate report list.
You want to print the report	Complete the steps described in Printing a Report on page 479.

Modifying a Report Schedule

Reports scheduled may be modified from any report list page.

When an optional parameter field does not contain a value the default value is All. For example, if you want to see the modifications to a specified user's accounts but you do not specify a service then all modifications made on any service supported will be reported. However, when one or more options are listed in a list box, only those options that are highlighted will be reported.

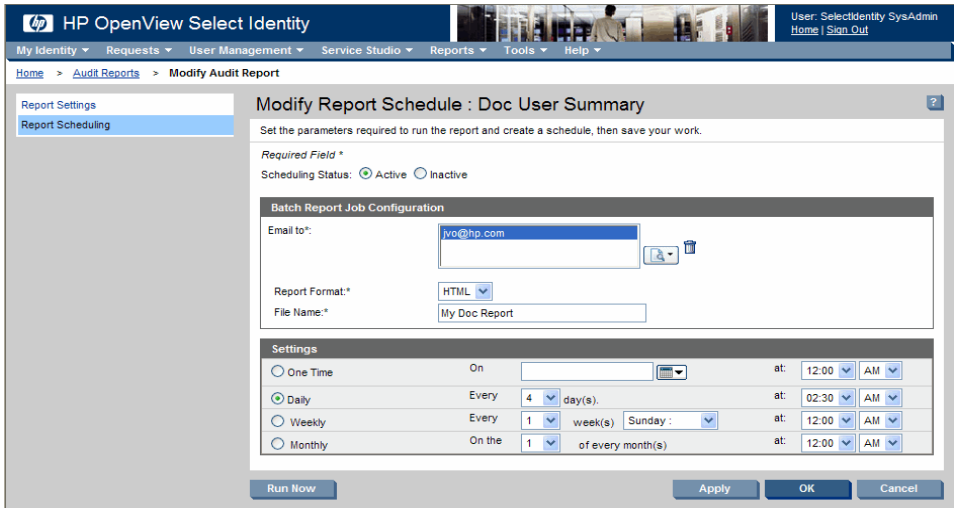
Remove items from a list box by selecting the item and clicking the  icon.

Follow the steps below to modify the schedule of a batch report:

1 Navigate to the correct report list page.

If	Then
You want to modify the schedule on an Audit Report	Click **Reports** → **Audit Reports** → **Audit Reports List**, then select the report you want to modify and click the **Modify Scheduling** button.
You want to modify the schedule on an Configuration Report	Click **Reports** → **Configuration Reports** → **Configuration Reports List**, then select the report you want to modify and click the **Modify Scheduling** button.
You already navigated to the page from the Report Settings: Report Name.	Continue

Figure 184Modify Report Schedule: Report Name Page



2 Modify the following fields. as necessary

Field	Action
Scheduling Status	Accept the default **Active**.
Email to	Click the  icon and select the email addresses of those individuals you want to receive the scheduled report.
Report Format	Choose the proper format from the drop-down menu.
File Name	Enter a unique file name.
Report Scheduling	Review the radio button options and determine the appropriate time period. • One Time • Daily • Weekly • Monthly Determine how frequently you want the report to run within the selected time period, then select the time of day you want to generate the report.

If the report is larger than the maximum size allowed to be sent by email, you will receive an email notifying you that the report file is saved at a specified location on your server.

3 Click **OK**.
Schedules the report and returns to the appropriate report list page.

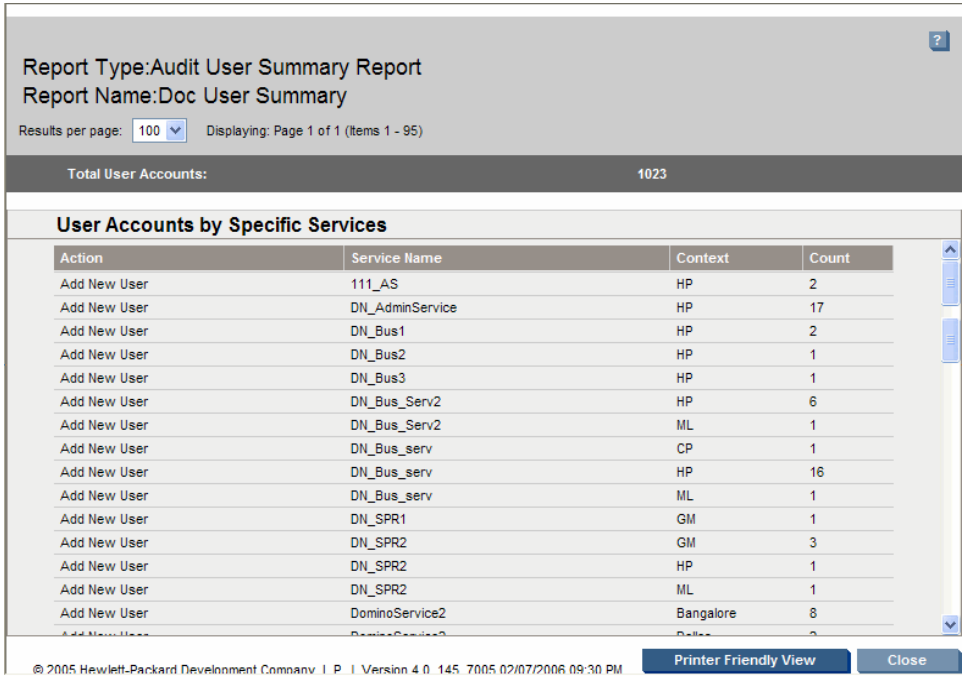
Printing a Report

1 Generate the report.

2 Click **Run Now.**
Generates the report and presents the data in your default browser.

You must have authorization to view the information generated on a report. If you have the correct authorization the report opens in your browser window, if not an error message appears instead.

Figure 185Sample Report



3 Click **Printer Friendly View.**
Changes the browser view.

4 Select **File** → **Print** from your browser menu.
Prints the report to your default printer.

5 Click **Close**.
Returns to the original page.

Copying a Report

Save time creating reports by copying a similar report, then editing the report display options and settings to fit your needs. Follow the steps below to copy a report.

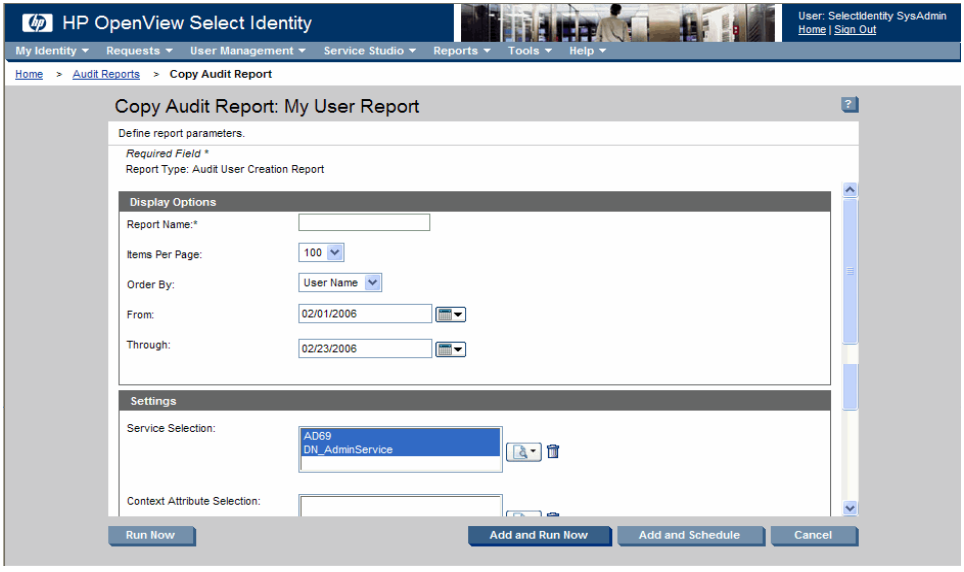
1 Navigate to the appropriate report list page.

If	Then
You want to copy an Audit Report	Click **Reports** → **Audit Reports** → **Audit Reports List**. Opens the **Audit Report List** page.
You want to copy a Configuration Report	Click **Reports** → **Configuration Reports** → **Configuration Reports List**. Opens the **Configuration Reports List** page.

2 Select the report you want to copy.

3 Click **Copy**.
The **Copy Type Report: Report Name** page opens.

Figure 186Copy Type Report: Report Name Page



4 Click the **Report Name** field and enter a unique name.

5 Review the display options and settings shown and make changes as necessary.

Settings shown depend upon the report selected.

6 Determine how best to handle the report.:

If	Then
You want to run the report without saving it.	Click **Run Now.**
You want to save the changes you made and continue working.	Click **Add and Run Now.**
You want to change report scheduling	Follow the instructions for Modifying a Report Schedule on page 477.
You want to save your changes and close the page without printing the report.	Click **Add and Schedule**.
You want to close this page without printing the report or saving your changes.	Click **Cancel.** Returns to the Report List.
You want to close the page without making any changes.	Click **Cancel.** Returns to the appropriate report list.
You want to print the report	Complete the steps described in Printing a Report on page 479.

Inactivating and Reactivating a Scheduled Report

Inactivating a report keeps the report from printing until it is reactivated although report settings can still be changed. If the report will not be used again, do not inactivate the report, delete the report instead.

Complete the steps below to inactivate or reactivate a report.

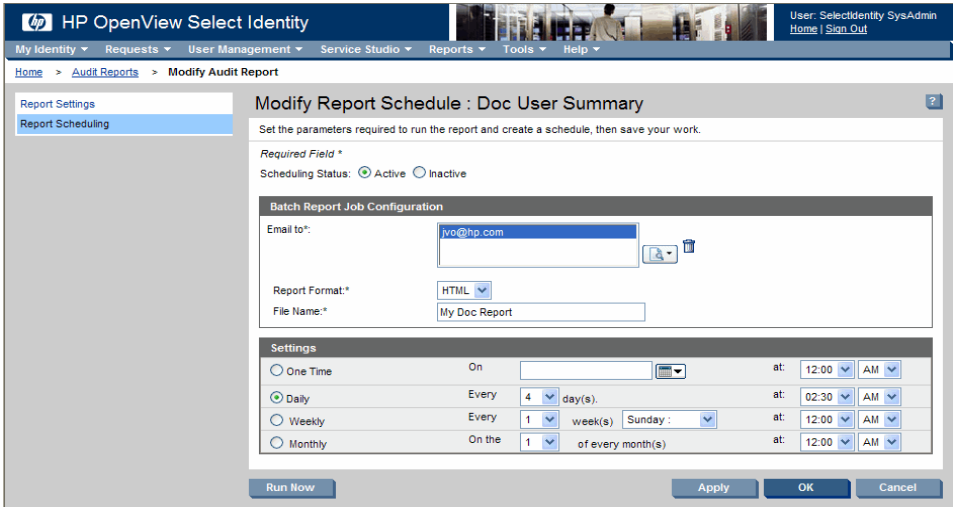
1 Navigate to the appropriate report list page.

If	Then
You want to inactivate or reactivate an audit report	Click **Reports** → **Audit Reports** → **Audit Reports List**. Opens the **Audit Report List** page.
You want to inactivate or reactivate a configuration report	Click **Reports** → **Configuration Reports** → **Configuration Reports List**. Opens the **Configuration Reports List** page.

2 Select the report you want to modify.

3 Click **Modify Scheduling**.
The **Modify Report Schedule: Report Name** page opens.

Figure 187Modify Report Schedule: Report Name Page



4 Review the **Scheduling Status** field.:

If	Then
You want to deactivate an active report	Click **Inactive**.
You want to reactivate an inactive report	Click **Active**.

5 Click **Apply.**
Saves your changes.

6 Click **OK**.
Returns to the appropriate report list page.

Deleting a Report

Deleting a report removes it from HP OpenView Select Identity. It cannot be retrieved at a later date. If you think you may need this report at some time in the future, deactivate the report instead.

Follow the steps below to delete a report.

1 Navigate to the appropriate report list page.

If	Then
You want to delete an Audit Report	Click **Reports** → **Audit Reports** → **Audit Reports List**. Opens the **Audit Report List** page.
You want to delete a Configuration Report	Click **Reports** → **Configuration Reports** → **Configuration Reports List**. Opens the **Configuration Reports List** page.

2 Select the report you want to delete.

3 Click **Delete**.
The confirmation dialog box opens.

4 Click **OK**.
Deletes the report and returns the appropriate report list page.

Understanding Report Parameters

Most reports within HP OpenView Select Identity can be generated as standard reports providing high level information, detailed reports providing information at the transaction level, and summary reports providing numeric totals only. Reports are defined below along with the parameter fields provided to help you customize each report to your business needs.

When an optional parameter field does not contain a value the default value is All. For example, if you want to see the modifications to a specified user's accounts but you do not specify a service then all modifications made on any service supported are reported. However, when one or more options are listed in a list box, only those options that are highlighted are reported. Remove items from a list box by selecting the item and clicking the  icon.

See Generating Audit Reports on page 463 or Generating Configuration Reports on page 469 for a detailed example of the steps to generate a report.

Audit Report Parameters

Audit Service Report

Reports all changes to user accounts related to one or more specified Services within HP OpenView Select Identity over a defined period of time.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.

Field	Action
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Actions	Highlight the functional action you want reported such as add, modify, and / or delete.
Fields	Highlight the fields you want reported.

Audit User Report

Reports all changes to specified user accounts related to one or more specified Services within HP OpenView Select Identity over a defined period of time. The Audit User Report may be filtered so that only specified changes are reported such as only accounts that have been added or deleted.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.

Field	Action
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Actions	Highlight each functional action you want reported such as add, modify, and / or delete.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit User Summary Report

Creates a summary report of all actions pertaining to users.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Field	Action
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Actions	Highlight each functional action you want reported such as add, modify, and / or delete.

Audit User Creation Report

Creates a detailed report listing the users added to services.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.

Field	Action
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit User Creation Summary Report

Creates a summary report listing the number of users added to each service.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Field	Action
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Actions	Highlight each functional action you want reported such as add, modify, and / or delete.

Audit User Deletion Report

Creates a detailed report listing the users deleted from services.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.

Field	Action
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit User Deletion Summary Report

Creates a summary report listing all the users deleted from each service.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.

Field	Action
Items per page	Enter the maximum number of items you want to display on each page of the report.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.

Audit User Termination Report

Creates a detailed report listing all the users terminated from the system.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit User Termination Summary Report

Creates a summary report listing all the users terminated from the system.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Audit User Password Report

Creates a detailed report listing all password actions and activites.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.

Field	Action
Actions	Highlight each functional action you want reported such as add, modify, and / or delete.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit User Password Summary Report

Creates a summary report showing the number of users involved in each type of password action.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Audit User Login Report

Creates a detailed report listing how many times users log in and out of the system.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.

Field	Action
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit Hint Report

Creates a detailed report showing how many times users set their password hints.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Fields	Highlight each field you want reported.
UserName	Click the  icon to select one or more users you want included on the report.

Audit Hint Summary Report

Creates a summary report showing the number of users who set their password hints.

Field	Action
Report Name	The name for this report.
From	Enter the first date you want reported by clicking the  icon.
Through	Enter the last date you want reported by clicking the  icon.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Configuration Report Parameters

User Configuration Report

Creates a report indentifying the all users who are registered for services.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.

Field	Action
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Fields	Highlight each field you want reported.

User Configuration Summary Report

Creates a summary report showing which users are registered to which service.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.

User Configuration Detail Report

Creates a batch report that provides detailed information on all users.

Field	Action
Report Name	The name for this report.
Order By	Select the sort method from the drop-down list.
Context Attribute Name Selection	Click the down arrow to see the list of Context Attribute Names. Select the one pertinent to the report.
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.

Admin Configuration Report

This report identifies all administrators in the system. It shows who manages what service and what roles the administrator of that service has.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
Service Selection	Click the  icon then click the **Filter** button to select from a list of services.

Field	Action
Context Attribute Selection	Click the  icon then click the **Filter** button to select one or more context user groups. Only those context user groups associated with the services you have selected will be available for your report. Therefore, you must select a service in order to select a context user group.
Fields	Highlight each field you want reported.
Managed Services	Click the  icon then click the **Filter** button to select from a list of services.
Managed Contexts	Click the  icon then click the **Filter** button to select from a list of contexts.
Admin Roles	Click the  icon then click the **Filter** button to select the Admin type.
UserName	Click the  icon to select one or more users you want included on the report.

Resource Users Report

Creates a report showing how ma;ny users belong to what resource. It shows all users for the resources. This report is used only by head administrators.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.

Field	Action
Order By	Select the sort method from the drop-down list.
Resouces	Click the  icon then click the **Filter** button to select from a list of resouces.
Fields	Highlight each field you want reported.

Resource Entitlement Report

Entitlements belong to resources. This creates a report that lets administrators find users who have the entitlement AND who belong to the resource. This report is used only by head administrators.

Field	Action
Report Name	The name for this report.
Items per page	Enter the maximum number of items you want to display on each page of the report.
Order By	Select the sort method from the drop-down list.
Resouces	Click the  icon, and then click the **Filter** button to select from a list of resouces.
Entitlements	Click the  icon, and then click the **Filter** button to select from a list of entitlements. Note that the list of entitlements displays only when the number of items exceed a threshold, which is configurable and defined in the `TruAccess.properties` file.
Fields	Highlight each field you want reported.

Resource Reconciliation Report

Creates a batch report used only by top administrators to find those SI users out of sync with resources and entitlements. It shows the discrepencies between SI and other resources.

Field	Action
Report Name	The name for this report.
Order By	Select the sort method from the drop-down list.
Compared Resouce	Click the  icon then click the **Filter** button to select from a list of resouces.
Comparison Type	Select either All Users, SI Users Only, or Resouce Users Only.

18 Server Management

The Server Management function lets you view the status of requests within any designated application server that are running the Select Identity application. Use this functionality to track down all the request instances that are affected by an ungraceful sever shutdown of HP OpenView Select Identity. For more information about installing and configuring Select Identity, see *HP OpenView Select Identity Installation and Configuration Guide*.

This chapter covers the following:

- Understanding the Server Work List
- Managing Requests
- Recovering Requests in the Event of Server Failure

Understanding the Server Work List

The Server Worklist lets you view the status of one or more servers. Use this page to view the status of each server instance that is running or has run the Select Identity application.

The Server Name column identifies the server running (or that has run) the Select Identity application. It contains identification information about the server-like host, port, and so on. This identification information varies among different application servers.

The Server Status is updated periodically by each server running Select Identity. Select Identity updates the status of all of its active Select Identity servers as `Running`. When a server is shutdown gracefully, the server status indicates `Not Running`. If a server is terminated abruptly, its status remains `Running`; however, after a timeout period, its status is changed to `Error`. Thus, due to the length of the timeout period, there may be a delay when an abruptly terminated server reports an `Error` status.

The Start Time shows the time when the server started. The Modified Time shows the time when server last updated the status. The End Time shows the time when the server was gracefully shut down.

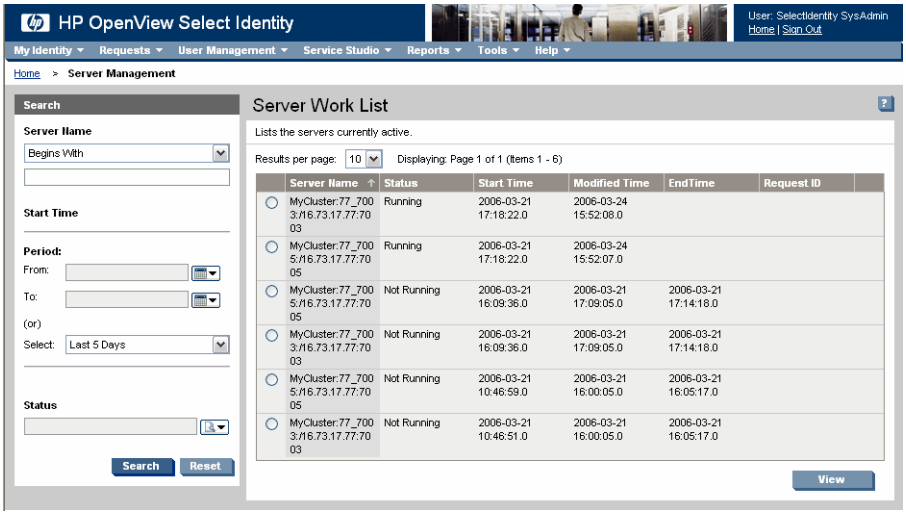
The View button takes you to a Request List that displays all impeded requests against the selected server.

Viewing the Server Work List

Complete the following steps to view a complete list of servers interacting with HP OpenView Select Identity.

1 Select the **Tools**→ **Server Management** → **Server Instance List** menu bar options.
Displays the **Server Work List** page.

Figure 188 Server Work List



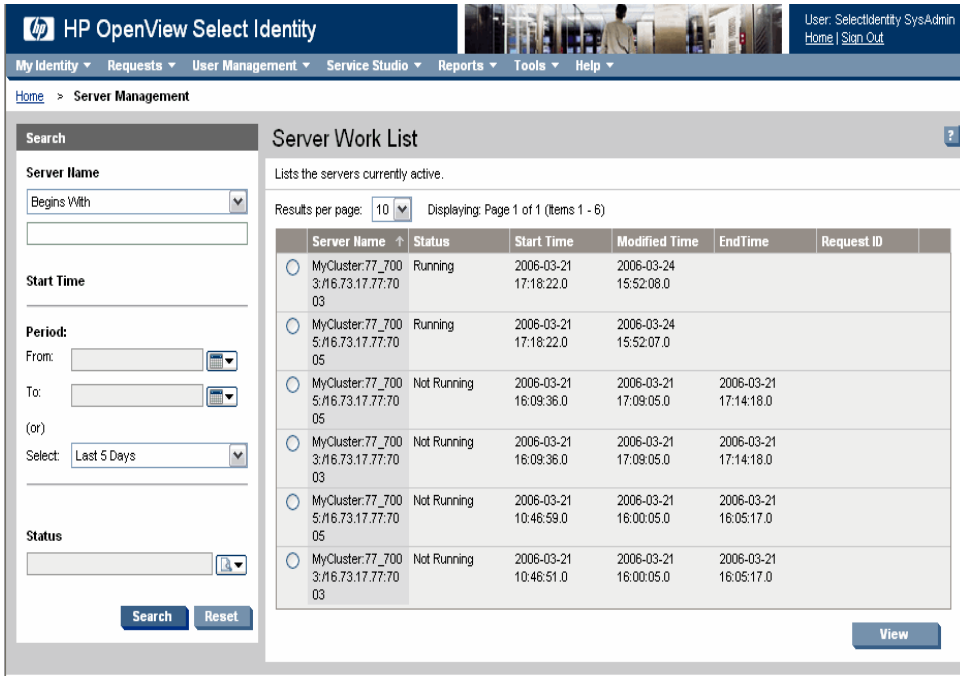
2 Review the list of servers for server status details as well as a list of request IDs currently in process on each server.

Viewing Individual Request Status

Use the Server Work List page to identify and view impeded requests. Follow the steps below to view the Request Status List for a selected server:

1 Select the **Tools** → **Server Management** → **Server Instance List** menu bar options.
Displays the **Server Work List** page.

Figure 189 Sever Work List page



2 Select the server you want to view.

3 Click **View**.
Opens the **Request Status List** page.

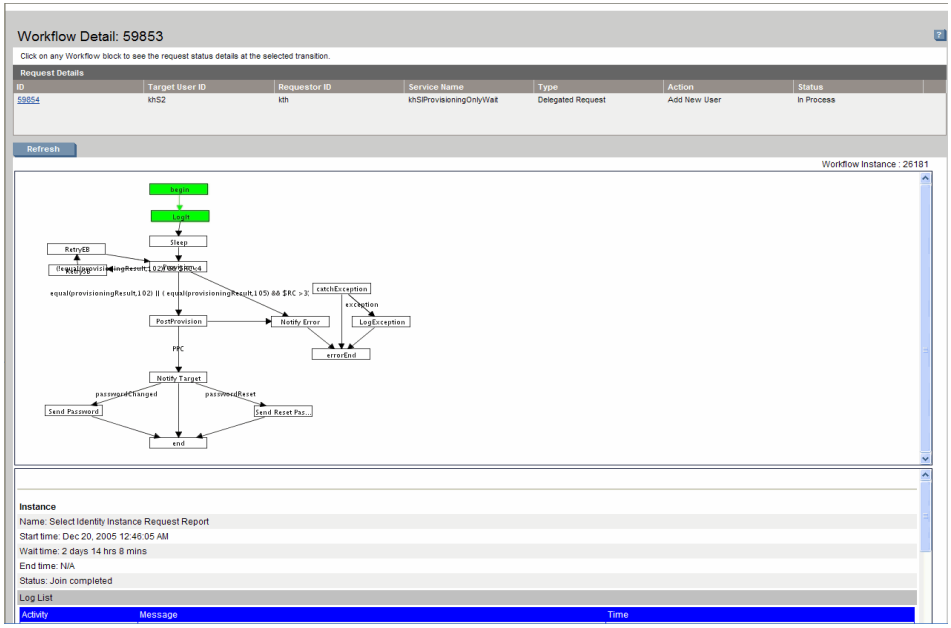
Each status in the status column corresponds to a server instance status as described below:

- Running - the server instance is currently running
- Error - the server instance has been ungracefully terminated
- Not Running - the server instance has been gracefully terminated

4 Select the request you want to view.

5 Click **View Requests**.
Opens the **Workflow Detail: Workflow Name** page.

Figure 190 Workflow Detail: Workflow Name



.

> You may be able to view the status of individual blocks in the workflow, depending upon the configuration of your workflow template. Learn more about Workflow in Chapter 7, Workflow Studio.

6 View updates to the Workflow image by clicking on the **Refresh** button.

7 Continue to review the workflow blocks until you have viewed all the information you need.

8 Close the page.
Returns to the **Request Status List** page.

Managing Requests

HP OpenView Select Identity generates requests that are sent to the servers that store the supported resources through a connector interface. When requests fail for what ever reason, you have the flexibility to manage the request and determine the next best course of action

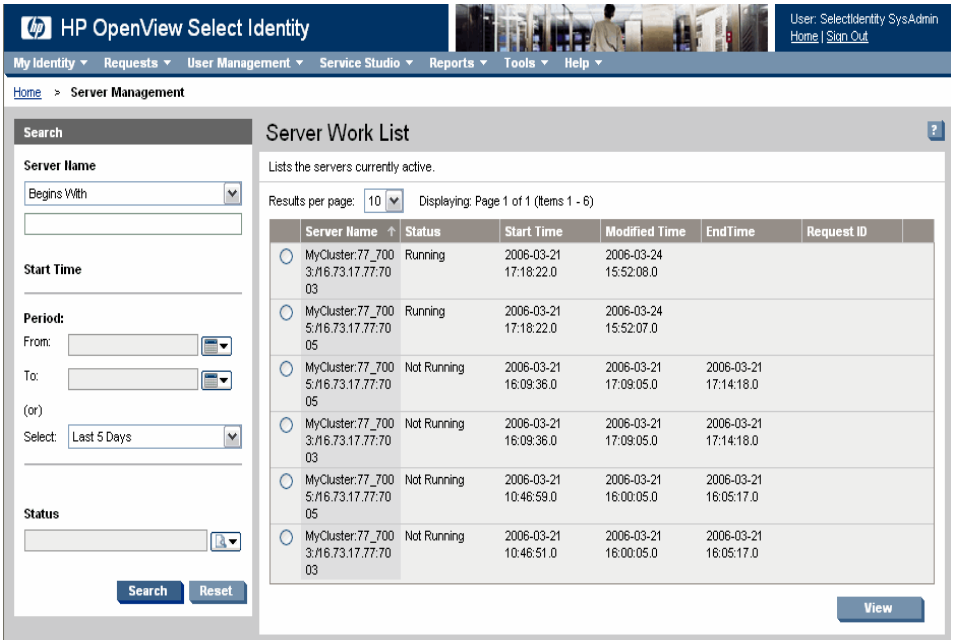
Terminating a Request

Terminate requests that error or are incorrect. Terminating a request stops the request where it is in the workflow process. Requests that have already completed successfully cannot be terminated.

Follow the steps below to end a request:

1 Select the **Tools** → **Server Management** → **Server Instance List** menu bar options.
Displays the **Server Work List** page.

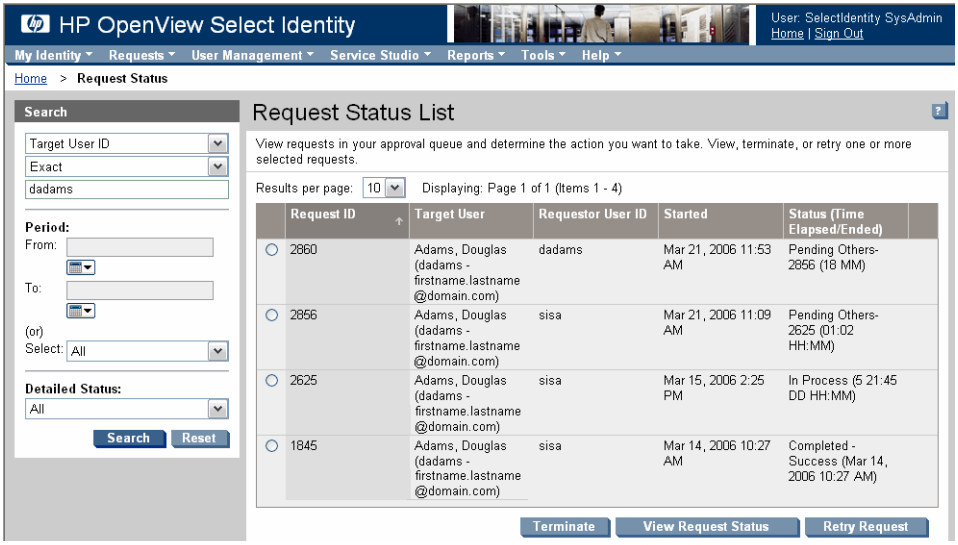
Figure 191 Sever Work List page



2 Select the server you want to view.

3 Click **View**.
Opens the **Request Status List** page.

Figure 192 Request Status List



4 Select the request you want to terminate from the list.

5 Click **Terminate**.
Displays the confirmation dialog box.

6 Click **OK**.
Terminates the request listed.

Recovering Requests in the Event of Server Failure

If there is a database or application server failure that causes an unexpected shutdown, Select identity requests can become suspended in the In Process state due to loss of the database connection, JMS message store failure, or other abnormal conditions.

Select Identity can recover the majority of these requests without intervention, using the **Terminate and Retry** option. In addition, manual procedures are available to recover any requests that Select Identity does not recover automatically.

Locating Requests for Recovery

To locate requests for recovery, perform the following steps:

1. Perform the following steps to determine the time period during which the database connection and/or Select Identity application server was non-operational. This assists you in isolating the requests that need to be recovered.
   a. Use the database management interface to check the database server downtime.
   b. In Select Identity, open the Server Management / Service Instance List page and check the Select Identity server downtime.
2. Locate requests that should be finished as suggested by the performance statistics supported by the current system configuration.

Recovery Procedures

The recovery procedures that you need to follow depend upon the type of request to be recovered:

- Recovering Delegated and Self-Service Requests
- Recovering User Reconciliation Requests
- Recovering Bulk Add/Move Requests
- Recovering Service Reconciliation Requests

Recovering Delegated and Self-Service Requests

To recover delegated and self service requests, perform the following steps:

1. Open the Request Status List
2. Use the search filters to locate requests created within the downtime period and which remain in the “In Process” state.
3. Copy and save the request IDs.
4. Select all of the requests using the check boxes in the list.
5. Click **Terminate and Retry**.

Recovering User Reconciliation Requests

User Reconciliation requests cannot be retried directly from the Select Identity request interface as Delegated and Self-Service requests can. To recover User Reconciliation requests, perform the following steps:

1. Navigate to the Reconciliation Task List.
2. Locate tasks during the downtime period that remain in the ‘Submitted” or “In Progress” states.
3. Copy and save the IDs of the tasks.
4. Query the Reconciliation Task report and save the reports.
5. Navigate to the Request Status List.
6. Search for requests created within the downtime period that remain in the “In Process” state.
7. Select all affected requests and click **Terminate**.
8. After all requests are terminated, return to the Reconciliation Task List.
9. Verify that the Submitted or In Process tasks have completed after a suitable period of time.
10. Query the reconciliation task reports again to locate any tasks that need additional intervention.
11. If incomplete tasks were submitted through File Upload, prepare a new file with the records that are not processed properly and submit the file again.
12. If incomplete tasks were submitted through Web Service or Resource Polling, prepare Web Service reconciliation SPML files with the data from the report and submit the Web Service requests again through Web Service client.

Recovering Bulk Add/Move Requests

Bulk add/move requests cannot be recovered directly from the Select Identity user interface. To recover requests of this type, perform the following steps:

1. Save Bulk Job initial reports if they are sent.
2. Query the **Bulk Add** report from the **Bulk Task List** interface.
3. Navigate to the **Request Status List**.

4 Use the search filter to search for requests created within the downtime period and that remain in the “In Process” state.

5 Select all requests that fit the search criteria and click **Terminate**.

6 After all the requests are terminated, upload the Bulk Add job again, or create a new Bulk Move job.

Recovering Service Reconciliation Requests

This type of request cannot be retried directly from the OVSI request interface. To recover requests of this type, perform the following steps:

1 Open the **Request Status List**.

2 Use the search filters to locate any service reconciliation requests that were initiated during the server downtime period and that remain in the “in process” state.

3 Select each request by checking the box on the left of the request entry in the list.

4 Click **Terminate**.

5 After the request has terminated, you must submit a new Service Reconciliation job, using the settings for each affected request, from the **Service** tab.

Glossary

Acronyms

A

AC

access control

ACL

access control list

AD

Adaptive Connector

AD Connector

Active Directory Connector

ADK

application development kit

ADO

ActiveX Data Objects

ANSI

America National Standards Institute

APA

auto port aggregation

API

application program interface

ARPA

Advanced Research Projects Agency

ASCII

American Standard Code for Information Interchange

B

BSIM

Business Service Identity Management

D

DBA

database analyst

DLL

dynamic-link library

DNS

domain name system

DHCP

dynamic host configuration protocol

DHTML

dynamic hypertext markup language

DSML

Directory Structure Markup Language

DSN

data source name

DSN

digital switched network

DTD

document type definition

E

EJB

enterprise java bean

F

FQDN

fully qualified domain name

FTP

file transfer protocol

G

GIF

graphics interchange format

GUID

globally unique identifier

H

HSRP

Hot Standby Router Protocol

HTTP

hypertext transfer protocol

HTTPS

Hypertext Transfer Protocol Secure

I

IBM

International Business Machines

IP

internet protocol

ISO

International Organization for Standardization

J

J2C

Java 2 connector

J2SDK

Java 2 software developer kit

J2EE

Java 2 enterprise edition

JAR

Java application resource

JCA

Java connection architecture

JDBC

Java database connectivity

JMS

Java messaging services

JNDI

Java naming directory interface

JSP

Java server protocol

JVM

Java virtual machine

K

KB

kilobyte

L

LDAP

lightweight directory access protocol

LDIF

lightweight data interchange format

LLB

local location broker

M

MAPI

messaging application programming interface

MB

megabyte

MHz

megahertz

MSSQL

MicroSoft Structured Query Language

MTA

message transfer agent

OVSI

HP OpenView Select Identity

P

PDF

portable document format

R

RAR

resource adapter archive

RDF

reporting data feeder

RPC

remote procedure call

S

SDK

software developer kit

SHA

secure hash algorithm

SMTP

simple mail transfer protocol

SNMP

simple network management protocol

SOAP

simple object access protocol

SP

service pack

SPML

Service Provisioning Markup Language

SSL

secure socket layer

SS0

single sign on

SPML

service provisioning markup language

SQL

structured query language

T

TCP / IP

transmission control protocol / internet protocol

U

URI

uniform resource identifier

URL

uniform resource locator

UTF-8

unicode transformation format (eight-bit character conversion)

V

VM

virtual machine

VNC

virtual network computing

W

WAS

web application server

WAR

web application repository

X, Y, Z

XML

extensible markup language

XSD

XML schema definition

XSL

Extensible Style Sheet Language

Terms

A

Access Control List (ACL)

An abstraction that organizes entitlements and controls authorization. An ACL is list of entitlements and users that is associated with a secured object, such as a file, an operation, or an application. In an ACL-based security system, protected objects carry their protection settings in the form of an ACL.

access management

The process of authentication and authorization.

action

When the context is a user action in the user interface, an operation that can be carried out by an OpenView application. Actions are typically performed on managed object. Select manually executed actions through a menu item or tool bar buttons. Actions can also be configured to automatically occur in response to an event, message, or a change in information in the management database.

When the context is based on OVSI policy, an actions is an operation carried out as a result of the activation of a reconciliation policy and the successful evaluation of a rule or conditions within that policy.

See also: capability

activate

To make active or functional

activity

A logical step in a process; A task that may occur when a workflow template is executed (in Workflow Studio). Activities are the core components of workflow templates; they do the work necessary to provision users. An activity can set a property to be used throughout the workflow, track approvals, start a subworkflow, send email, call an external application, and so on.

adapter

Software that allows information interpretation between two or more software products or components.

AD Connector

Active Directory Connector. A type of interface used to connect HP OpenView Select Identity with the applications it serves on servers that communicate using the Active Directory protocol.

admin role

A template that defines the administrative actions performed by a user. Create an Administrative Service to provide access to roles so that users gain

access to the Service. Users with administrative roles may grant their set of roles to another administrator within their Service context.

advanced customization

Less common types of customization which are more flexible in their capabilities and complex in their implementation than typical customizations. As with other customizations, advanced customizations are done to meet the needs and preferences of a particular customer or user.

agent

A program or process running on a remote device or computer system that responds to management requests, performs management operations, or sends performance and event notification. An agent can provide access to managed objects and MIB variables, interpret policy for resources and do configuration of resources; The component of an agent-based connector that resides in the same system as the resource. It listens for a changes in the user data made in the resources, then reports that change to HP OpenView Select Identity by communicating through a connector interface.

agent-based connectors

Two-way connector interface. There are two components: the connector that resides in the same system as HP OpenView Select Identity, and the agent, which resides in the same system as the resource. The agent listens for changes made in the resource, and contacts the resource about changes made in Select Identity.

agentless connectors

One way connectors. Connectors reside in the Select Identity server and does the communication brokering with the resource.

application

Packaged software that provides functionality that is designed to accomplish a set of related tasks. An application is generally more complex than a tool.

application deployment

The installation and activation of application components so that they work in the business environment.

Application Program Interface (API)

A set of routines, protocols, and tools used to build a software application; An interface that enables programmatic access to an application.

approval process

The process of approving the association, modification, or revocation of entitlements for an identity. This process is automated of these through workflow templates.

approver

A Select Identity administrator who has been given approval actions through an Admin Role.

assigned policy

A policy that has been assigned to one or more resources in the computing environment but which has not yet been deployed or installed on those resources.

asynchronous subprocess

A process that proceeds at its own pace independent of other processes and subprocesses.

attribute

An individual field that helps define an identity profile. For each identity, an attribute has a corresponding value. For example, an attribute could be "department" with possible values of "IT," "sales," or "support."

attribute external call

Small programs that are written to generate values automatically for that attribute (value generation), define constraint values for the attribute (value constraint), or validate the value that is entered for that attribute (data validation). Each attribute can have each of these types of external calls.

attribute name-value pair

An attribute name-value pair is combination of an attribute identifier and the value of that attribute for a specific object. An example of an attribute-name-value pair for a person would be Name: John Smith.

audit engine

logs and stores all audit-related activities, e.g., when changes are made and who made them.

Audit Report

A report that provides regular account interaction information.

authentication

Verification of an identity's credentials.

authoritative source

A resource that has been designated as the "authority" for identity information. Select Identity accounts can be reconciled against accounts in an authoritative source.

automatic action

A pre-configured program or script that is executed in response to an event, message, or a change in information in the management database. without operator intervention.

B

bandwidth

The transmission capacity of an electronic line such as a communications network, computer bus, or computer channel. It is expressed in bits per second (for example, 56 kbps), bytes per second or in Hertz (cycles per second). When expressed in Hertz, the frequency may be a greater number than the actual bits per second, because the bandwidth is the difference between the lowest and highest frequencies transmitted. (TECH).

block

A special type of activity that serves two purposes: to define information to be used by a subset of activities (block-level properties) and to provide block-level reporting. For example, you might define a block that submits an approval request, waits for the response, and returns the status of the request to the workflow. In other words, think of a block as a process within a template.

block type

A property assigned to a block in a workflow template using the blockType property in end block activity. The report template uses this property to identify how block information is rendered in the resulting report.

Boolean operator

A logical operator that defines the context in which attribute values are compared to satisfy a query or policy. For example:

AND - Both conditions have to be satisfied.

OR - At least one condition has to be satisfied.

NOT - No instance of this condition is allowed.

browser

A module within a work space that presents one or more views of objects and provides functionality for interacting with the objects and the views.

business service

A product or facility offered by, or a core process used by, a business in support of its day-to-day operations. Example business services could include an online banking service, the customer support process, and IT infrastructure services such as email, calendaring, and network access.

See also: service

Business Service Identity Management (BSIM)

An organizational model that introduces new abstractions that simplify and provide scale to the business processes associated with identity management. These abstractions are modeled after elements that exist in businesses today and include Services and Service Roles.

C

capability

Actions that can be performed within the HP OpenView Select Identity client.

See also: action

challenge and response

A method of supplying alternate authentication credentials, typically used when a password is forgotten. Select Identity challenges the end user with a question and the user must provide a correct response. If the user answers the question correctly, HP OpenView Select Identity resets the password to a random value and sends email to the user. The challenge question can be configured by the administrator. The valid response is stored for each user with the user's profile and can be updated by an authenticated user through the Self Service pages.

client

When the context is network systems, a computer system on a network that accesses a service from another computer (server).

When the context is software, a program or executable process that requests a service from a server

client console

An instance of the user interface that appears on the client system while the application runs on a server.

condition type

An abstraction or categorization of a condition that determines to the particular kind of data that is valid for the parameter values in the condition and how those values will be used.For example a condition type could be Source IP Address which indicates that values must have 4 numbers separated by decimals with the value for each number being in the range of 0 to 255. Since the condition type is "Source" IP Address, the IP addresses will only be evaluated for sources not destinations.

configuration file

A file that contains specifications or information that can be used for determining how a software program should look and operate.

configuration

In a hardware context, a particular set of inter-related components that make up a computer system. For example the components of a computer system may include a keyboard, pointing device, memory, disk drives, modem, operating system, applications and printer. The configuration of the computer system determines the way that it works and the way that it is used.

In a network context, the complete set of inter-related systems, devices and programs that make up the network. For example the components of a network may include computer systems, routers, switches, hubs, operating systems and network software. The configuration of the network determines the way that it works and the way that it is used.

In a software context, the combination of settings of software parameters and attributes that determine the way the software works, the way it is used, and how it appears.

configure

To define and modify specified software settings to fulfill the requirements of a specified environment, application or usage.

Configuration Report

A report that provides current system information for user, administrator, and Service management activities.

connection

A representation of a logical or physical relationship between objects.

connector

A J2EE connector interface that communicates with the system resource applications that contain your identity profile information.

console

An instance of the user interface from which the user can control an application or set of applications.

context

An HP OpenView Select Identity concept that defines a logical grouping of users that can access a Service.

credential

A mechanism or device used to verify the authenticity of an identity. For example, a user ID and password, biometrics, and digital certificates are considered credentials.

customization

The process of designing, constructing or modifying software to meet the needs and preferences of a particular customer or user.

customize

To design, construct or modify software to meet the needs and preferences of a particular customer or user.

D

database

A repository of data that is electronically stored. Typically databases are organized so that data can be retrieved and updated.

data file

An SPML file that enables you to define user accounts to be added to Select Identity through Auto Discovery or Reconciliation.

data type

A particular kind of data; for example character, string, integer, date, currency, etc.

deactivate

To deliberately stop a component or object from working.

delegated administration

The ability to securely assign a subset of administrative roles to one or more users for administrative management and distribution of workload. Select Identity enables role delegation through the Self Service pages from one administrator to another user within the same Service context.

delegated registration

Registration performed by an administrator on behalf of an end user.

See also: self-registration

deploy

To install and start software, hardware, capabilities, or services so that they work in the business environment.

deployed application

An application and its components that have been installed and started to work in the business environment.

deployed policy

A policy that is deployed on one or more resources in the computing environment.

deployment

The process of installing and activating software, hardware, capabilities or services so that they work in the business environment.

deployment package

A software package that can be deployed automatically and installed on a managed node.

deprecate

To lower the status of a hardware or software object to indicate that it can be taken out of use in the future

device

A generic term for a piece of hardware equipment that can be attached to a computer or a network. Examples of a device are a printer, a router, a switch, a load-balancer, a disk drive or a modem.

disable

To make unable to be used.

dismiss

Dismiss is an action that causes a message or other notification associated with a problem or situation to be removed from the browser. Messages are typically dismissed when the operator has resolved the situation that led to the message.

disown

The act of relinquishing responsibility for resolving a problem or situation associated with a message or other notification.

DNS domain

A set of computers and other network devices that are collectively addressable by a portion of an IP address or by the highest subdivision of the domain name that indicates the entity owning the address. For example all computers whose host name share the suffix.hp.com are in the same DNS domain.

domain

A set of computers and other network devices that are treated or managed as a unit.

double-click

To press and release a pointing device's button twice in rapid succession. Double-clicking is a time-dependent action. Clicking twice in the same location at slow speed (click-delay-click) is not a double-click.

downtime

The amount or percentage of time that a service, software, or hardware resource remains non-functional.

dynamic parameters

Parameters whose values are determined during program execution.

E

enable

To make able to use.

end user

A role associated to every user in the Select Identity system that enables access to the Self Service pages.

entitlement

An abstraction of the resource privileges granted to an identity. Entitlements are resource-specific and can be resource account IDs, resource role memberships, resource group memberships, and resource access rights and privileges. Entitlements are also considered privileges, permissions, or access rights.

event

An event is an unsolicited notification such as an SNMP trap or WMI notification generated by an agent or process in a managed object or by a user action. Events usually indicate a change in the state of a managed object or cause an action to occur.

event attribute

A characteristic or property of an event.

event correlation

The evaluation of multiple events or notifications that are related to a single incident or problem, to produce a single message. Event correlation is used to reduce the number of messages that are presented to an operator in a message browser.

event creation time

The time an event was created in Universal Coordinated Time (UTC)

event syntax

The rules governing the structure and content of an event.

event type

A classification of an event into a particular category that further defines the nature of the event.

export

To format and move information from the current application to a location outside the current application.

expression

A combination of workflow variables and constant values to be evaluated. An expression can be assigned to a new variable or passed to an application as an argument. If you are familiar with a programming language, an expression used in a workflow template is like C or Java expression. Example of expressions can be found in action input parameters, application return values, and transition conditions.

extend

The act of increasing the capabilities, scope, or effectiveness of a program.

extensible

Capable of being extended.

external call

A programmatic call to a third-party application or system for the purpose of validating accounts or constraining attribute values.

external system ID

An identifier that uniquely identifies a principal that is an external system.

F

filter

A software feature or program that functions to screen data so that only a subset of the data is presented or passed. Filters allow matching-relevant information to be extracted and acted on while non-matching-irrelevant information is held back.

find

The act of seeking of specific data or objects within the management application or set management applications based on specified criteria.

form

An electronic document used to capture information from end users. Forms are used by Select Identity in many business processes for information capture and system operation; A presentation mechanism that contains information and controls for obtaining user input (for example, text fields, radio buttons, lists).

foundation

A program that acts as the basic structure to support other software modules or programs that provide additional functionality for the user.

function

A general term for a portion of a program that performs a specific task.

H

hierarchy

Elements organized in successive levels with each lower level being subordinate to the one above.

HP OpenView

A family of network and system management products, and an architecture for those products. HP OpenView includes development environments and a wide variety of management applications.

I

icon

An on-screen image that represents objects that can be monitored or manipulated by the user or actions that can be executed by the user.

icon class

The portion of an icon that identifies the type or classification of the object being represented by the icon. For example, the network object class is represented by a circle surrounding a more complex image.

ID

identifier

identifier

A name that within a given scope that uniquely identifies the object with which it is associated.

identity

The set of authentication credentials, profile information, and entitlements for a single user or system entity. Identity is often used as a synonym for “user,” although an identity can represent a system and not necessarily a person.

identity management

The set of processes and technologies involved in creating, modifying, deleting, organizing, and auditing identities.

import

To format and move information from a location outside the current application into the current application.

install

To load a product or component of a product onto a computer system or other network or system device. Installation typically involves running initial configuration scripts that are part of the installation process.

instance

See: workflow instance

internationalization

The design of software so that a single binary can support the varied cultural and linguistic conventions that exist in different countries or locales. Internationalized software allows users to interact with the software in the user's native language including the input and output of data in the native language, as well as support for the conventions and rules applicable to the user's locale. The ANSI locale model is used in internationalized software.

J

Java

Object oriented programming language.

JCA

Java Connection Architecture. Architecture used to build interfaces between J2EE compliant products and other resources.

JVM

Java Virtual Machine. A platform independent execution environment that conversant Java bytecore into machine language then executes it.

L

LDIF

File that modifies and deletes directory objects.

list

If the context is a GUI, a set of selectable items. If the context is data, a variable-length ordered set of values all of the same data type.

locale

The locale collectively represents the location or country of the user, the language of the user, and the code set in which the user's data is represented. The locale is related to the language sensitive presentation of applications.

locale model

The software through which the user declares their desired language at application start up. The local model determines the set of files, tables, or collection of programs that are used to initialize an application so that it is sensitive to the user's language.

localization

Localization refers to the set of tasks that need to be accomplished to enable a product to work acceptably in a specific locale. The localization tasks include translating documentation, translating text and graphics that are presented to the user, and providing locale specific fonts and other functionality when needed.

M

management

The ongoing maintenance of an object or set of objects, including creating, modifying, deleting, organizing, auditing, and reporting.

message key

A message attribute that is a string used to identify messages that were triggered from particular events.The string summarizes the important characteristics of the event. Message keys can be used to allow messages to acknowledge other messages, and allows for the identification of duplicate messages.

N

node

When the context is network, a computer system or device (for example, printer, router, bridge) in a network.

When the context is a graphical point to point layout, a graphical element in a drawing that acts as a junction or connection point for other graphical elements.

notifications

The capability that enables you to create and manage templates that define the messages that are sent when a system event occurs.

P

package

A set of related programs or software files grouped together as a single object for a common purpose.

password reset

The ability to set a password to a system-generated value. Select Identity uses a challenge and response method to authenticate the user and then allow the user to reset or change a password.

persistent variable

A variable that is persisted after an instance is passivated. To extend the variable life cycle to the entire instance, you must create the variable to be persistent. This enables the variable to be created before a wait activity, and it will be accessible after the workflow instance resumes. To make a variable persistent, precede the name with $. For example, the $retryCount variable is persistent while retryCount is not.

See also: workflow variable

policy

A set of regulations set by an organization to assist in managing some aspect of its business. For example, policy may determine the type of internal and external information resources that employees can access.

policy management

The process of controlling policies (for example, creating, editing, tracking, deploying, deleting) for the purposes of network, system or service management.

port

If the context is hardware, a location for passing information into and out of a network device.

process

A repeatable procedure used to perform a set of tasks or achieve some objective. Whether manual or automated, all processes require input and generate output. A process can be as simple as a single task or as complicated a multi-step, conditional procedure.

See also: approval process

profile

Descriptive attributes associated with an identity, such as name, address, title, company, or cost center.

property

See:workflow property

provisioning

The process of assigning authentication credentials to identities.

R

reconciliation

The process by which Select Identity accounts are synchronized with a system resource. Accounts can be added to the Select Identity system through the use of an SPML data file.

registration

The process of requesting access to one or more resources. Registration is generally performed by an end user seeking resource access, or by an administrator registering a user on a user's behalf.

See also: delegated registration, self-registration

request

An event within the Select Identity system for the addition, modification, or removal of a user account. Requests are monitored through the Request Status capability.

resource

Any single application, database, or information repository. Resources typically include applications, directories, and databases that store identity information.

role

A simple abstraction that associates entitlements with identities. A role is an aggregation of entitlements and users, typically organized by job function.

See also: admin role

rule

A programmatic control over system behavior. Rules in Select Identity are typically used for programmatic assignment of Services. Rules can also be used to detect changes in system resources.

S

self-registration

Registration performed by an end user seeking access to one or more resources.

See also: delegated registration

self service

The ability to securely allow end users to manage aspects of a system on their own behalf. Select Identity provides the following self-service capabilities: registration, profile management, and password management (including password change, reset, and synchronization).

service

A business-centric abstraction representing resources, entitlements, and other identity-related entities. Services represent the products and services that you offer to customers and partners.

service attribute

A set of attributes and values that are available for or required by a Service. Attributes are created and managed through the Attributes pages.

See also: attribute

service role

A Select Identity abstraction that defines how a logical grouping of users will access a Select Identity Service. The Select Identity Service is a superset of all the identity management elements of a business service.

service view

A restricted view of a Service that is valid for a group of users. Views enable you to define a subset of Service registration fields, change field names, reorder fields, and mask field values for specific users.

single sign-On (SSO)

A session/authentication process that permits a user to enter one set of credentials (name and password) in order to access multiple applications. A Web SSO is a specialized SSO system for web applications.

SPML Data File

See: data file

submodule

A portion of a software module that provides a subset of the functionality provided by the module. A sub-module performs a specific task or presents a specific set of data.

suspend

To halt for a time a computer operation preserving the state of that operation.

synchronous subprocess

A process that must complete before the invoking process can proceed.

syntax

The rules governing the structure and content of a language or the description of an object.

system administrator

The role of a person who does configuration and maintenance on a computer system or the software on the system.

T

template

See: workflow template

trace log

An output file containing records of the execution of application software

transit delay

The difference between current time and the event's creation time.

transition

The definition of a relationship between activities. You can define that one activity always follows another, or you can define a condition that must be met before the workflow transitions from an activity to one or more others. For example, you can define a transition that only allows the workflow to progress if at least two administrators approve a request. If the request is not approved, the workflow can transition to an activity that sends email notification to an administrator.

U

URL

Acronym for Uniform Resource Locator or Universal Resource Locator, the address of a computer or a document on the Internet.

user import

The process of adding user accounts to the Select Identity system for a specified Service through the use of a data file.

users

The functionality that provides consistent account creation and management across Services.

V

variable

See: workflow variable

variable expression

See: external call

W

Web Service Definition Language (WSDL)

File format that the Application Definition file uses to define a web service application to be a workflow application. The workflow engine reads the web service invocation parameters through WSDL. A web service can reference a WSDL URL remotely or download it first as a local file and then read the file locally at run-time.

workflow engine

A system component that executes workflows and advances them through their flow steps.

workflow external call

A “subroutine” that is called during the workflow process. This could be an external application invocation such as a small custom application that calls external processes outside of the normal workflow process

workflow instance

An invocation of a workflow template. An instance starts when it is created and ends when it completes (when the last activity is executed). An instance’s status and other associated information can be viewed once an instance is created.

workflow process

The tasks, procedural steps, organizations or people involved, and required input and output information needed for each step in a business process. In identity management, the most common workflows are for provisioning and approval processes.

workflow property

A name-value pair, where the value is a text string. A property stores static data that cannot be changed at runtime. It can be accessed by the workflow API and report template. There are three levels of properties: global, block, and activity.

workflow studio

The functionality that enables you to create and manage workflow templates.

workflow template

A model of the provisioning process that enables Select Identity to automate the actions that approvers and systems management software must perform.

workflow variable

A name-value pair that can be created or changed at runtime in a workflow instance through actions, a workflow API call, or returned by an application invocation. It can be accessed by workflow API, workflow template, and report template. There are levels of variables: global, block, and activity.

See also: persistent variable

A SPML Generator Utility

HP OpenView Select Identity provides a utility called the SPML Generator, which converts CSV and XML file formats into Service Provisioning Markup Language (SPML). While there are many ways to create SPML files, this is a convenient way for developers who are more familiar with CSV and XML to create SPML files for User Import and Reconciliation.

This chapter covers the following:

SPML Generator Utility Package

The SPML Generator package includes all the files you will need to get started. Copy the files from the `utilities` directory on the HP OpenView Select Identity product CD to any directory convenient for you.

File	Description
`runGenerator.bat`	Windows DOS batch file used to run the SPML Generator utility. This batch file is based on one of the `spmlgenerator*.properties` configuration files listed in this table. See Running the Utility on page 545 for details. You must change the `@shell` script file to show the location of `JAVA_HOME` according to the installation on the target host.
`runGenerator.sh`	UNIX shell script used to run the SPML Generator utility. This script is based on one of the `spmlgenerator*.properties` configuration files listed in this table. See Running the Utility on page 545 for details. You must change the batch file to show the location of `JAVA HOME` according to the installation on the target host.
`SPMLGenerator.jar`	SPML Generator utility executable files
`spmlgeneratorcsv.properties`	Sample configuration file for CSV-based input for User Import. Edit this file according to your requirements.

File	Description
spmlgeneratorreconcsv.properties	Sample configuration file for CSV-based input for Reconciliation. Edit this file according to your requirements.
spmlgeneratorxml.properties	Sample configuration file for XML-based input for User Import. Edit this file according to your requirements
spmlgeneratorreconxml.properties	Sample configuration file for XML-based input for Reconciliation. Edit this file according to your requirements.

Understanding Dependencies

The following files must be on your system for the utility to work:

- commons-logging.jar — for logger and log factory
- ovsii18n.jar — for internationalization

Running the Utility

Complete the following steps to run the SPML Generator utility:

1. Copy the package to a single directory.
2. Be sure that JRE (>=1.4) is installed properly and included in the path. See the *HP OpenView Select Identity Installation Guide* for installation instructions.
3. Select one of the following sample files to use as a template based on your requirements.
   - spmlgeneratorcsv.properties — Used to convert CSV-format to SPML for User Import.
   - spmlgeneratorreconcsv.properties — Used to convert CSV-format to SPML for Reconciliation.
   - spmlgeneratorxml.properties — Used to convert XML-format to SPML for User Import.

- `spmlgeneratorreconxml.properties` — Used to convert XML-format to SPML for Reconciliation.

4 Edit the batch file or shell script to do the following:

- Enter the `JAVA_HOME` location according to the installation on the target host.

Enter the appropriate properties configuration file name as a command line argument. Do not use the dot and the extension

If the JAVA_HOME variable is set in your environment, any new path will be ignored.

5 Run the batch file or shell script.

Example

Following is an example of the `runGenerator.bat` file that is ready to be run to convert a CSV format to SPML for Reconciliation:

```
set JAVA_HOME=C:\bea\jdk142_05

SET CLASSPATH=./SPMLGenerator.jar;./
commons-logging.jar;./ovsii18n.jar;

%JAVA_HOME%\bin\java -classpath %CLASSPATH%
com.ovsi.spmlgenerator.core.SPMLGenerator
spmlgeneratorreconcsv
```

Properties Descriptions for the Properties Configuration Files

Following are the properties and their descriptions by category as they appear in any of the properties configuration files. The categories are listed in the order of relevance to users.

#csvplugin parameters

- `reader.filename`

  File name with the full path of the CSV input file.

Note that slashes (\) in a Windows path name must be specified as double slashes (\\).

For example:

```
reader.filename=C:\\tools\\eclipse\\workspace\\SPMLGenerator\
\bin\\samplefiles\\reconcsv.csv
```

- `reader.colnames`

  List of column names for the data to be specified in the CSV input file. Be sure the name and order of the columns are not altered. The order is referenced in the properties file and in the SPML Generator utility.

  For example:

  ```
  reader.colnames={username,ssn,firstname,lastname,email,profil
  e,role,accounttype,primaryAcctValue,recontype}
  ```

- `reader.coldelimiter`

  Separator character that is used between two columns in the CSV file.

  For example:

  ```
  reader.coldelimiter=#
  ```

- `reader.datadelimiter`

  Separator character that is used between multiple values to be given in one column. This is typically used in the case of multi-valued attributes.

  For example:

  ```
  reader.datadelimiter=,
  ```

- `reader.quotechar`

  Escape sequence to represent a double quote within the data in the CSV file.

  For example:

  ```
  reader.quotechar=\"
  ```

- `reader.encoding`

  Encoding of the characters in the CSV file.

  For example:

  ```
  reader.encoding=UTF-8
  ```

Recon or User Import Flag

- `writer.isrecon`

Flag to specify whether the conversion run is for Reconciliation or User Import.

For Reconciliation, the value is **Yes**. For User Import the value is **no**.

For example:

```
writer.isrecon=no
```

- If the reconciliation value in `writer.isrecon` is **yes**, then specify the following reconciliation values.
- If the reconciliation value in `writer.isrecon` is **no** then specify the # User Import global operational attributes values.

- `writer.reconcol`

  Field that specifies which column in the CSV format represents the Reconciliation Action Type. Refer to `reader.colnames` above.

  The value specified for this property refers to the Reconciliation Type column in `reader.colnames`. The CSV data records typically have a value of Add, Modify or Delete as the Reconciliation type.

  For example:

  ```
  writer.reconcol=recontype
  ```

- `writer.reconopattr`

  Specifies which item key in **writer.map** below (SPML file properties) maps to the Reconciliation Operational Attributes.

  For example:

  ```
  writer.reconopattr=operation
  ```

User Import global operational attributes

- `writer.globalop.keyFields`

  Specifies the key fields under the global operational attributes section of the SPML file.

  For example:

  ```
  writer.globalop.keyFields=UserName,Email
  ```

- `writer.globalop.isprimary`

Specifies whether the SPML file has a global operational attribute entry for the primary user.

For example:

```
writer.globalop.isprimary=yes
```

- `writer.globalop.primaryAcctKey`

  Specifies which attribute represents the Primary Account Key in the global operational attributes.

  For example:

  ```
  writer.globalop.primaryAcctKey=Email
  ```

Specify adduser operational attributes

- `writer.requestop.isUIDGenerated`

  Set to **yes** if the userId needs to be generated.

  For example:

  ```
  writer.requestop.isUIDGenerated=yes
  ```

- `writer.requestop.taUserNameAttr`

  Refers to the column corresponding to the UserName Attribute.

  For example:

  ```
  writer.requestop.taUserNameAttr=username
  ```

- `writer.requestop.taResourceKey`

  Refers to the column corresponding to the Resource Key.

  For example:

  ```
  writer.requestop.taResourceKey=ssn
  ```

- `writer.requestop.primaryAcctKey`

  Specifies the string representation of primaryAcctKey.

  For example:

  ```
  writer.requestop.primaryAcctKey=urn:hp:selectidentity#taResou
  rceKey
  ```

- `writer.requestop.primaryAcctValue`

Specifies the string representation of primaryAcctValue.

For example:

```
writer.requestop.primaryAcctValue=primaryAcctValue
```

- `writer.requestop.typecolumn`

  Specifies the string representation of `typecolumn`.

  For example:

  ```
  writer.requestop.typecolumn=accounttype
  ```

- `writer.requestop.multientcolnames`

  Provides column names corresponding to the multi-valued columns.

  For example:

  ```
  writer.requestop.multientcolnames=profile,role
  ```

#SPML file parameters

- `writer.spmlfile`

  Specifies the full path and name of the output SPML file.

  Note that slashes (\) in a Windows path name must be specified as double slashes (\\).

  For example:

  ```
  writer.spmlfile=C:\\tools\\eclipse\\workspace\\SPMLGenerator
  \\bin\\samplefiles\\spmlfromxml.xml
  ```

- `writer.usersperfile`

  Specifies the number of users to include in a file in order to limit the file size. The file size should not grow larger than.10 MB in order to avoid degradation of performance Follow the suggestions below or experiment to find out what works best for you.

  — For ten or fewer attributes o set the value at 500 users per file.

  — For eleven or more attribute set the value at 250 users per file.

  For example, if the value is set to 2, the file is closed after writing the SPML entries corresponding to two user requests. If there are more users in the CSV input file (or other input file), multiple files will be written

with the same name. Each file will be given a suffix integer numbered from 1 to `n-1`, where `n` is the total number of files required to represent the whole input as SPML.

For example:

`writer.usersperfile=2`

- `writer.isauthoritative`

  Specifies whether the resource represented is authoritative or non-authoritative. Enter **yes** for Authoritative.

  For example:

  `writer.isauthoritative=yes`

- `writer.map1`

  Specifies one of the several maps you can specify. These maps provide a way to map the column from the input file under `reader.colnames` to the SPML output.

  `map1` maps `username` in `reader.colnames` to the SPML output.

  For example:

  `writer.map1=username|UserName`

- `writer.map2`

  `map2` maps `ssn` in `reader.colnames` to the SPML output.

  For example:

  `writer.map2=ssn|SSN`

- `writer.map3`

  `map3` maps `firstname` in `reader.colnames` to the SPML output.

  For example:

  `writer.map3=firstname|FirstName`

- `writer.map4`

  `map4` maps `lastname` in `reader.colnames` to the SPML output.

  For example:

  `writer.map4=lastname|LastName`

- `writer.map5`

`map5` maps `email` in `reader.colnames` to the SPML output

For example:

```
writer.map5=email|Email
```

- `writer.map6`

  `map6` maps `profile` in `reader.colnames` to the SPML output

  For example:

  ```
  writer.map6=profile|Profile
  ```

- `writer.map7`

  `map7` maps `role` in `reader.colnames` to the SPML output

  For example:

  ```
  writer.map7=role|Role
  ```

- `writer.map8`

  `map8` maps `operation` in `reader.colnames` to the SPML output

  For example:

  ```
  writer.map8=operation|Operation
  ```

B Auditing XML and Client Sample

HP OpenView Select Identity can pass event auditing data to third-party auditing tools (such as HP Select Audit) as an XML stream. An extensible schema definition (XSD) and a sample Audit Client are packaged with Select Identity.

The Audit Client is an example program that illustrates how to connect to an application server via JMS and subscribe to the audit XML stream.

The audit XML schema provided can be used to develop an application that interprets the Audit XML stream and presents it in a user-readable format such as a report. The XML stream can be processed into a database, for example, and analyzed using a reporting tool.

The XML stream can also be translated into a Java Object Hierarchy, which must be undertaken using a third party tool. Appropriate development tools are available from several sources, such as Sun Microsystems and Apache.

This appendix describes how to run the Audit Client and provides details of the sequences, types, and elements that are defined in the Select Identity Audit XSD.

Processing the Audit XML Stream into a Database

The steps below provide a brief high-level outline of the process that must be used to translate the Audit XML stream into a format that can be used to build reports in a database:

1. Determine in advance how the database schema and tables will be set up and create these so that they are compatible with the converted Java objects.
2. Select a third-party tool to map XML to a java object hierarchy and insert the result into the database.

3 Map the java objects to the database schema.

Using the Audit Client

The Audit Client displays the audit stream in a terminal window in real-time. It is located in the `/utilities/auditclient` subdirectory.

The Audit Client consists of the component files listed in the table below:

File or Directory	Purpose
`/doc`	Contains API documentation in HTML format.
`runclient.bat`	The batch file used to run the Audit Client
`jndi.properties`	Connection properties for interfacing with WebLogic.
`readme.txt`	Release notes and other information
`auditbroadcastlistener.java`	Sample code demonstrating how to connect to the application server and subscribe to the audit stream
`auditbroadcastlistener.class`	compiled version of the AuditBroadcastListener class
`new-audit.xsd`	The XML schema definition for Select Identity audit XML
`weblogic.jar`	The Audit Client Java executable

Configuring Connection Properties

The Audit Client is configured by default to connect to Select Identity on `localhost` to receive the audit stream. If you need to connect to a different host, edit the host name in the `jndi.properties` file before running the Audit Client.

Running the Audit Client

To run the Audit Client:

1. Copy the entire contents of the following directory from the HP OpenView Select Identity product CD into an appropriate subdirectory in your Select Identity install directory:

   `/utilities/auditclient/WebLogic_client`

2. Ensure that WebLogic and HP OpenView Select Identity are running.

3. Run the Audit Client batch file by entering the following command at the WebLogic admin server command line:

   `./runclient.bat`

The Select Identity Audit XSD

Select Identity Auditing data is output in XML form as set out in the Audit XML Schema Definition, named `Audit.xsd`. This file is located on the HP OpenView Select Identity Product CD, under `\utilities\auditClient`.

The sections and tables that follow define the XML elements in the Audit XSD, grouped to show their hierarchical relationships. The Element Reference table provides detailed information about each individual element, since some can belong to more than one complex.

Event Sequences

Event sequences allow related audit event data elements to be processed as a group. Some elements are optional and others are required.

Sequences can reference one another as element types. Thus, `configChangeSeq` and other sequence names appear in some of the elements as the element type in the same way as integer or string types. For complete detail about the possible contents of event sequences or any other auditing element, refer to the XSD (`audit.xsd`).

The sequences used in Select Identity audit data are listed below, together with the possible child elements:

configChangeSeq: Configuration changes

```
OVSIAuditConfigChange
```

EnitiyChangeSeq: Changes to entities

```
entity
```

EventSeq: The beginning of an event sequence of any type defined in the XSD.

MembershipSeq: Changes to service or resource membership

```
MembershipType
```

OVSIAuditAttrChangeDataSeq: Changes to attribute data

```
OVSIAuditAttrChangeData
```

PropertySeq: Changes to properties

```
property
```

PropertyValueSeq: Changes to property values

```
entity
value
name
key
```

SvcConfigChangeSeq: Service configuration changes

```
OVSIAuditConfigChange
```

TargetSeq: The target of the event

```
OVSIAuditTarget
```

UserSeq: User-related changes

```
OVSIAuditUser
```

ValueSeq: Changes to values

```
value
```

Data Types

Child elements of each event sequence are structured according to the types listed in this section. Some of these are simple elements consisting of a single value or string, while others contain multiple child elements.

AttrChangeData

```
attrId
attrName
oldValue
newValue
opType
sensitiveLevel
```

auditType and auditSubType

These are simple type elements that contain a single value indicating the audit type or subtype.

ConfigChangeType

```
type
fieldId
fieldName
properties
```

EntityType

```
PropertySeq
```

EntityListType

```
property
entity
```

EventType

```
adminRole
auditType
auditSubType
adminId
adminName
requestMethod
requestType
requestId
parentRequestId
causeByRequestId
status
timestamp
serviceName
```

ctxVarName

ctxVarValue

ctxVarId

auditTargets

auditUsers

auditResourceChanges

auditServiceChanges

auditAttrs

auditAdminRoles

auditConnectors

auditNotifications

auditExtCalls

auditRules

auditWorkflows

MembershipType

userId

membershipId

membershipOperation

membershipType

OpType

This is a simple type element that contains a single value indicating the type of operation performed in an audit event.

PropertyType

```
delete
add
entityChanges
```

requestType

This is a simple type element that contains a single value indicating the request type.

SvcConfigChangeType

```
type
serviceId
serviceName
fieldId
fieldName
properties
```

targetType

```
targetId
targetName
targetType
```

UserType

```
primaryId
primaryName
userId
name
attrChangeDatas
memberships
```

Constraints

The `minoccurs` and `maxoccurs` attributes define the value range for each element:

MinOccurs=1: the element is required in an event sequence.

MinOccurs=0: the element is optional in an event sequence.

MaxOccurs=unbounded: the element can occur any number of times in an event sequence.

MaxOccurs=1: the element can occur once only if it is present in an event sequence.

Element Definitions

The table below provides detailed information about each element.

Element Name	Type	Constraints	Definition
(ConfigChange) Type	Integer		The type of configuration change: TYPE_RESOURCE = 1 TYPE_ADMIN_ROLE = 4 TYPE_EXT_CALL = 5 TYPE_SERVICE = 6 TYPE_SERVICE_CTX = 7 TYPE_SERVICE_ROLE = 8 TYPE_SERVICE_VIEW = 9 TYPE_ATTRIBUTE = 10 TYPE_WORKFLOW = 11 TYPE_RULE = 12 TYPE_NOTIFICATION = 13 TYPE_CONNECTOR = 14
add	PropertyValueSeq	Optional	A property that was added
adminID	String	Required, once per event	The Admin account ID requesting the operation
adminName	String	Optional, once per event	The name of the administrator requesting the operation
adminRole	String	Required, once per event	The role name that authorized the operation

Element Name	Type	Constraints	Definition
attrChangeData	OVSIAuditAttr ChangeDataSeq	Optional	Affected user attributes/ properties
attrId	Integer	Required, once per event	Attribute ID affected
attrName	String	Required, once per event	Attribute name affected
auditAdminRoles	ConfigChangeSeq	Optional, once per event	Any changes to admin roles
auditAttrs	ConfigChangeSeq	Optional, once per event	Any attribute changes
auditConnectors	ConfigChangeSeq	Optional, once per event	Any changes to connectors
auditExtCalls	ConfigChangeSeq	Optional, once per event	Any changes to external calls
auditNotifications	ConfigChangeSeq	Optional, once per event	Any changes to email templates
auditResourceChanges	ConfigchangeSeq	Optional, once per event	Any resource changes
auditRules	ConfigChangeSeq	Optional, once per event	Any changes to rules
auditServiceChanges	SvcConfigChange Seq	Optional, once per event	Any service changes

Element Name	Type	Constraints	Definition
auditTargets	Targetseq	Optional, once per event	The target of the request (eg. a user, service, or resource)
auditType	Integer	Required, once per event	UNKNOWN_VAL = 0 APPROVAL_VAL = 1 PROVISIONING_VAL = 2 POST_PROVISIONING_VAL = 3 EXTERNAL_CALL_VAL = 4 RESERVED_1_VAL = 5 RESERVED_2_VAL = 6 RESERVED_3_VAL = 7 RESERVED_4_VAL = 8 RESERVED_5_VAL = 9
auditUsers	UserSeq	Optional, once per event	Users affected by the request
auditWorkflows	ConfigChangeSeq	Optional, once per event	Any changes to workflows
causeByRequestId	Integer	Optional, once per event	If an event was triggered by another event, the ID of the triggering event.
ConfigChangeType	Complex		Details of a configuration change
ctxVarId	String	Optional, once per event	For service-specific requests, the context variable ID
ctxVarName	String	Optional, once per event	For service-specific requests, the context variable name

Element Name	Type	Constraints	Definition
ctxVarValue	String	Optional, once per event	For service-specific requests, the context variable value
delete	PropertyValueSeq	Optional	A property that was deleted
entity		Optional, unbounded	When this change is relative to an entity change the entity for this property
entityChanges	EnitityChangeSeq	Optional	A collection of changed items. If you change a resource attribute mapping, each attribute of the resource that change will be included in the entity changes for the property “attrs.” Each entity change is similar to a property change.
EntityListType	Complex	Optional	A Group of changed entities
fieldId	Integer	Required	ID of configuration item that changed. i.e. ServiceRole ID, Context ID
fieldName	String	Required	The name of the configuration item that changed, i.e. resource name, service name, rule name
key	String		The key name of the entity
membershipId	Integer	Required, once per event	Affected service or resource IDs
membershipName	String	Required	The name of the service or resource in a membership operation

Element Name	Type	Constraints	Definition
membershipOperation	Integer	Required	Whether the membership was added or deleted: ADD_VAL = 1 DEL_VAL = 2
memberships	MembershipSeq	Optional	Affected memberships
membershipType	Integer	Required	Whether the membership was to a service or resource: RESOURCE_VAL = 1 SERVICE_VAL = 2
name	String	Required	Affected user name
name	String	Required	The name of a changed property
newValue	String	Required	The value to which the attribute was changed.
oldValue	String	Optional	The value that was changed.
opType	Integer	Required	A simple type that contains a value indicating the type of operation: Add_VAL = 1 Change_VAL = 2 Delete_VAL = 3
OVSIAuditAttrChangeData	Complex		Attribute change details.
OVSIAuditUser	UserType	Optional, unbounded	Represents the user affected by the event.
parentRequestId	Integer	Optional, once per event	The ID number assigned to a parent request.
primaryId	Integer	Optional	Primary affected user ID (if affected user ID is secondary).

Element Name	Type	Constraints	Definition
primaryName	String	Optional	Primary affected user name (if affected user name is secondary).
properties	PropertySeq	Required	The Properties that changed as a result of an operation.
property	propertyType	Required	An individual property that changed as a result of an operation.
PropertyType	Complex	Optional	Property change type
requestID	Integer	Optional, once per event	The ID number assigned to a request

Element Name	Type	Constraints	Definition
requestMethod	Integer	Optional, once per event	The method via which the operation was performed, *e.g.* API, Web, WebService, File: DELEGATED_API = 1 all requests from UI have value. DELEGATED_WEB whether delegated or self service, name is not precise. DELEGATED_WEB = 2 all requests from web service have value. DELEGATED_WEBSERVICE no matter delegated or self service, name is not precise DELEGATED_WEBSERVICE = 3 RECONCILIATION_ FILEUPLOAD = 10 RECONCILIATION_ WEBSERVICE = 11 BULK_FILEUPLOAD = 12 BULK_WEBSERVICE = 13; BULK_MOVEUSER = 14; RECONCILIATION_POLLING = 15

Element Name	Type	Constraints	Definition
requestType	Integer	Optional, once per event	The type of request DELEGATED_REGISTRATIO N = 1 SELF_REGISTRATION = 2 AUTO_DISCOVERY = 3 RECONCILIATION = 4 SYSTEM = 5 BULK_UPLOAD = 6 PROVISION = 7 SERVICECHANGE_RECONCI LIATION = 8
sensitiveLevel	Integer	Optional	Indicates a field that is marked “sensitive.”
serviceId	Integer	Required	Service ID of the item that changed
serviceName	String	Optional, once per event	For service-specific requests, the service that initiated the request
serviceName	String	Required	Service name of the item that changed
status	Integer	Required, once per event	PENDING_VAL = 1 SUCCESS_VAL = 2 FAILURE_VAL = 3 PARTIAL_SUCCESS_VAL = 4 APPROVED_VAL = 5 APPROVED_CHANGES_VAL = 6 REJECTED_VAL = 7
SvcConfigChangeType	Complex		Specialized form of ConfigChangeType
targetId	Integer	Required	The ID of the target

Element Name	Type	Constraints	Definition
targetName	String	Required	The name of the target
targetType	Integer	Required	The type of target: USER_NORMAL_VAL = 1 USER_PRIMARY_VAL = 2 USER_SECONDARY_VAL=3 USER_CLUSTER_VAL = 4 RESOURCE_VAL = 5 SERVICE_VAL = 6 SERVICE_CONTEXT_VAL = 7 SERVICE_ROLE_VAL = 8 SERVICE_VIEW_VAL = 9 ATTRIBUTE_VAL = 10 WORKFLOW_VAL = 11 RULE_VAL = 12; NOTIFICATION_VAL = 13 CONNECTOR_VAL = 14 EXTERNAL_CALL_VAL = 15 ADMIN_ROLE_VAL = 16
TargetType	Complex		Audit operation target details
timestamp	Long Integer	Required, once per event	The time at which the event occurred, relative to server time, expressed as the number of mlliseconds since Jauary 1st, 1970.
type	Integer	Required	As for ConfigChangeType
userId	Integer	Required	Affected user ID

Event Types

Event Type elements indicate the action that occurred in an audit event. The table below lists the possible event types.

Action Type	Action
Service Change Reconciliation	SVCCHG_RECON_MODIFY_USER = 51 SVCCHG_RECON_ADD_RESOURCE = 52 SVCCHG_RECON_DELETE_RESOURCE = 53
Resource Reconciliation	RESOURCE_RECONCILIATION_DELETE = 56 RESOURCE_RECONCILIATION_MODIFY = 57 RESOURCE_RECONCILIATION_REPLACE = 58
User Role Delegation	USER_ROLE_DELEGATION_ACTIVATE = 54 USER_ROLE_DELEGATION_DEACTIVATE = 55

Action Type	Action
User Request	ADD_NEW_USER = 1 MODIFY_USER = 2 DELETE_SERVICE_MEMBERSHIP = 3 ENABLE_ALL_SERVICES = 4 DISABLE_ALL_SERVICES = 5 RESET_PASSWORD = 6 COPY_USER = 7 ADD_SERVICE = 8 CHANGE_PASSWORD = 9 FORGET_PASSWORD = 10 ENABLE_SERVICE_MEMBERSHIP = 11 VIEW_SERVICE_MEMBERSHIP = 12 TERMINATE_USER = 13 MANAGE_USER_EXPIRATION = 14 DISABLE_SERVICE_MEMBERSHIP = 15 SECURITY_VIOLATION = 16 MODIFY_PROFILE = 17 PASSWORDEXPIRE_NOT = 18 MOVE_USER = 19 LOGIN = 20 LOGOUT = 21 IMPORT = 22 EXPIRE_PASSWORD = 24 HINTSETUP = 30 DISABLE_TERMINATE = 31 REVERT_MODIFY = 32 REVERT_ADD = 33 REVERT_DELETE = 34 IGNORE_ADD = 35 IGNORE_MODIFY = 36 IGNORE_DELETE = 37

Action Type	Action
Cluster Operations	CREATE_CLUSTER = 40 MODIFY_CLUSTER = 41 DELETE_CLUSTER = 42 ADD_SECONDARY = 43 REMOVE_SECONDARY = 44
Service	SERVICE_CREATE = 2000 SERVICE_DELETE = 2001 SERVICE_MODIFY = 2002 SERVICE_COPY = 2003 SERVICE_SET_ATTR_VALUES = 2004 SERVICE_SET_ATTR_PROPS = 2005 SERVICE_VIEW_CREATE = 2006 SERVICE_VIEW_DELETE = 2007 SERVICE_VIEW_MODIFY = 2008 SERVICE_ROLE_CREATE = 2009 SERVICE_ROLE_DELETE = 2010 SERVICE_CONTEXT_CREATE = 2011 SERVICE_CONTEXT_DELETE = 2012 SERVICE_CONTEXT_MODIFY = 2013 SERVICE_IMPORT = 2014 SERVICE_ROLE_MODIFY = 2015 SERVICE_EXPORT = 2016
Resource	RESOURCE_CREATE = 3000 RESOURCE_DELETE = 3001 RESOURCE_MODIFY = 3002 RESOURCE_VIEW = 3003 RESOURCE_COPY = 3004 RESOURCE_ATTR_VIEW = 3005 RESOURCE_ATTR_MODIFY = 3006 RESOURCE_IMPORT = 3007 RESOURCE_EXPORT = 3008

Action Type	Action
Attribute	ATTRIBUTE_CREATE = 4000 ATTRIBUTE_DELETE = 4001 ATTRIBUTE_MODIFY = 4002 ATTRIBUTE_VIEW = 4003 ATTRIBUTE_COPY = 4004 ATTRIBUTE_IMPORT = 4005 ATTRIBUTE_EXPORT = 4006
Workflow	WORKFLOW_CREATE = 5000 WORKFLOW_DELETE = 5001 WORKFLOW_MODIFY = 5002 WORKFLOW_VIEW = 5003 WORKFLOW_COPY = 5004 WORKFLOW_IMPORT = 5005 WORKFLOW_EXPORT = 5006
External Call	EXT_CALL_CREATE = 6000 EXT_CALL_DELETE = 6001 EXT_CALL_MODIFY = 6002 EXT_CALL_VIEW = 6003 EXT_CALL_COPY = 6004
Notification	NOTIFICATION_CREATE = 7000 NOTIFICATION_DELETE = 7001 NOTIFICATION_MODIFY = 7002 NOTIFICATION_VIEW = 7003 NOTIFICATION_COPY = 7004 NOTIFICATION_IMPORT = 7005 NOTIFICATION_EXPORT = 7006

Action Type	Action
Connectors	CONNECTOR_CREATE = 8000 CONNECTOR_DELETE = 8001 CONNECTOR_MODIFY = 8002
Rules	RULE_CREATE = 9000 RULE_DELETE = 9001 RULE_MODIFY = 9002
Admin Roles	ADMINROLE_CREATE = 10000 ADMINROLE_DELETE = 10001 ADMINROLE_MODIFY = 10002

C Attribute Mapping

The Attribute Mapping utility helps you create or modify XML and XSL mapping files of the connectors. This feature is supported on database connectors. For other connectors, the resource typically defines a fixed set of attributes. Hence, the mapping files cannot be modified.

In the case of database connectors, you can provision users and entitlements into a database. Since the database schema can be defined in a number of ways, the mapping files can also vary widely, and can be modified. For instance, the attribute mapping utility gives you the flexibility to map table columns and stored procedures to HP OpenView Select Identity attributes. After you map the attributes and save, an XML file for forward mapping and an XSL file for reverse synchronization are generated. Learn more about deploying connectors in Managing Connectors on page 59.

Attribute Mapping Utility Overview

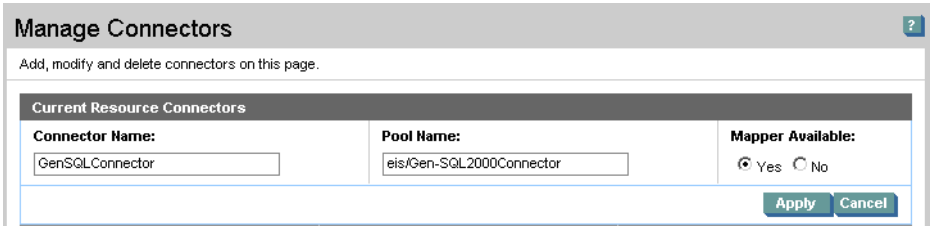
The Attribute Mapping utility lets you load the resource schema directly from the resource and map its attributes onto OVSI attributes, thereby creating an XML mapping file that is used by the OVSI connectors. The connectors are supplied with a default XML mapping file and this is usable in most cases. You can use the Attribute Mapping Utility to create a new mapping file or edit an existing mapping file. The Attribute Mapper can also let you provision entitlements into the resource.

Accessing the Attribute Mapping Utility

To access the Attribute Mapper utility from the Select Identity home page, do the following:

1 While deploying a new connector on Select Identity using the Manage Connectors option, select the radio button labeled **Mapper Available** to make the Attribute Mapper Utility available for that particular connector.

Figure 193 Manage Connectors page



2 Click the Resources tab.

3 Click **Deploy New Resource**.

4 Enter the necessary values into each field (refer to the connector's installation guide for more information on the values needed to deploy the resource), and then click **Save & Continue**.

5 On the Access Info page, enter the necessary connection credentials, which depend on how the database connector and agent are installed and configured:

- Using a JDBC data source without an agent installed:

  In this configuration, the connector performs operations on the database directly through JDBC calls.

Field	Value
Mapping File	The name of the XML file that will be generated.
JDBC Datasource String	The JNDI name of the JDBC data source that was created on the Select Identity server to connect to the target database.

Make sure all of the other fields are empty.

Using a JDBC driver without an agent installed

The connector uses the JDBC driver to communicate with the database. You must specify all parameters except the agent port and JDBC data source.

Field	Value
SQL URL	The name of the JDBC driver to use to connect to the database.
Mapping File	The name of the XML file that will be generated.
Server Name	The name of the database server.
Server Port	The database server's listening port.
Username	The database user ID.
Password	The password of the specified user.
Database/Service Name	The name of the database.
Database Driver String	The JDBC driver being used.

Using a JDBC driver with an agent installed

If the agent is installed and a JDBC driver is used to communicate with the database, you must specify all parameters except the JDBC data source.

Field	Value
SQL URL	The name of the JDBC driver to use to connect to the database.
Mapping File	The name of the XML file that will be generated.
Server Name	The name of the database server.
Server Port	The database server's listening port.

Field	Value
Username	The database user ID.
Password	The password of the specified user.
Database/Service Name	The name of the database.
Database Driver String	The JDBC driver being used.
Agent Port	The port of the listening agent.

6 Click the **Edit** link next to the Mapping File field.

To create or modify a mapping file of an existing resource, select the connector on the Resource tab, and then select **Modify Resource** from the Actions drop-down menu. View the Access Info page for the resource, and then click **Edit** next to the Mapping field.

When you click `Edit`, the Attribute Mapping Utility page appears and connects to the database using the values entered on the Access Info page. If you are creating a mapping file, a new XML file is created in the Select Identity home directory, in the `com/trulogica/truaccess/connector/schema/spml` subdirectory. (This default location can be configured by setting the `com.hp.ovsi.connector.schema.dir` parameter in the `TruAccess.properties` file.)

If the specified mapping file exists, the Attribute Mapping Utility appears, connects to the database, and loads the existing settings in the mapping file.

Configuring the JDBC Datasource for a Connector

Ensure that for creating the JDBC Datasoure on Weblogic, you perform the following configuration:

- Uncheck the **Honor Global Transactions** option.
- Check the **Emulate Two-Phase Commit for non-XA Driver** option.

This configuration must be done to allow the newly created Datasource to co-exist with the OVSI JDBC Datasource. Refer to the *Connector Installation Guide* supplied with your connector for details.

Attribute Mapper Menus and Pages

If you access the Attribute Mapping Utility by loading its URL in a browser, the page, which appears first, prompts you to enter connection information.

If you are editing an existing XML file, the mapped attributes are listed in the Attribute Mappings section of the page.

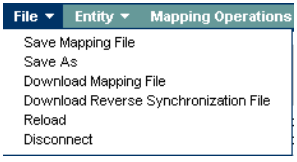
The Attribute Mapping Utility home page contains:

- Menus
- Mapping pages

Attribute Mapper Menus

The following menus and options are available.

- **File Menu**



File menu has the following options:

— **Save Mapping File**
It saves the XML and XSL file in the directory specified in the Base Directory field on the Select Identity server. If the base directory is not specified while logging in, Select Identity the value of `com.hp.ovsi.connector.schema.dir` property of the `TruAccess.properties` file. If none of these values are available, the files are stored in the home directory of the application server.

— **Save As**
It saves the XML and XSL files with another name, other than the one specified when you logged in to the utility. This displays a pop-up dialog where you need to enter base directory and file name.

— **Download Mapping File**
It lets you download the XML file from the Select Identity server if you are running the utility from a remote client. This displays a download dialog, which enables you to save the XML file locally.

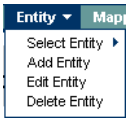
— **Download Reverse Synchronization File**
It lets you download the XSL file from the Select Identity server if you are running the utility from a remote client. This displays a download dialog, which enables you to save the XSL file locally on the client.

— **Reload**
It reloads the XML file in the Attribute Mapping Utility.

— **Disconnect**
It disconnects the connection from the utility to the database.

- **Entity Menu**

An entity is a logical grouping of attributes for users or groups (entitlements). By default, a user entity exists. If you want to provision entitlements, you need to create an additional entity. Each new entity is a group entity that represents user entitlements.



These are the options on this menu:

— **Select Entity**
It enables you to select the entity to edit.

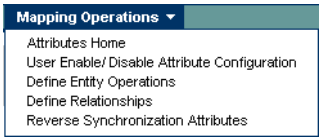
— **Add Entity**
It enables you to create a new entity in the utility, which enables you to map attributes for entities other than users. This displays a dialog prompting you to name the new entity.

— **Edit Entity**
It enables you to edit an entity name using this option. The default entity (user) cannot be edited.

— **Delete Entity**
It deletes the currently selected entity. You cannot delete the default entity (user).

- **Mapping Operations Menu**

This menu lists all of the operations that can be performed using the utility, which are the same operations through which you are guided if you use the wizard (see Mapping Pages on page 584). The following shows the menu when the user entity is selected:



These are the options on this menu:

— **Attributes Home**
It displays the Attributes page, which enables you to map database columns to Select Identity attributes.

— **User Enable/Disable Attribute Configuration**
It displays the Enable/Disable page, which enables you set values that are assigned when a user is enabled or disabled during provisioning.

— **Define Entity Operations**
It displays the Specify Supported Operations page, which enables you to define the operations that the connector can perform on the schema.

— **Define Relationships**
It displays the Define Relationship Definitions page, which enables you to define how tables in the schema relate.

— **Reverse Synchronization Attributes**
It displays Reverse Synchronization Attributes page, which enables you to map key fields that are used during reverse synchronization.

- **Help Menu**

This menu is represented by the icon shown below.

This menu opens the help system, which provides an overview of the Attribute Mapping Utility.

Mapping Pages

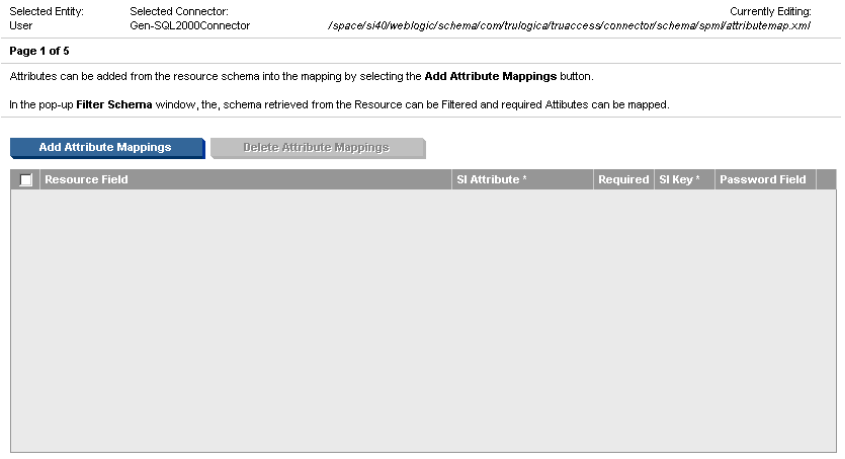
Mapping pages are the interface through which you can modify mapping files, define operations, define relationship between tables, and so on. You can access the mapping pages either by user entity or by group entity. By default, you can access these pages by user entity.

When you use user entity, you can find five mapping pages. You can navigate to them either by **Previous** or **Next** button at the bottom of the window, or using the **Mapping Operations** Menu.

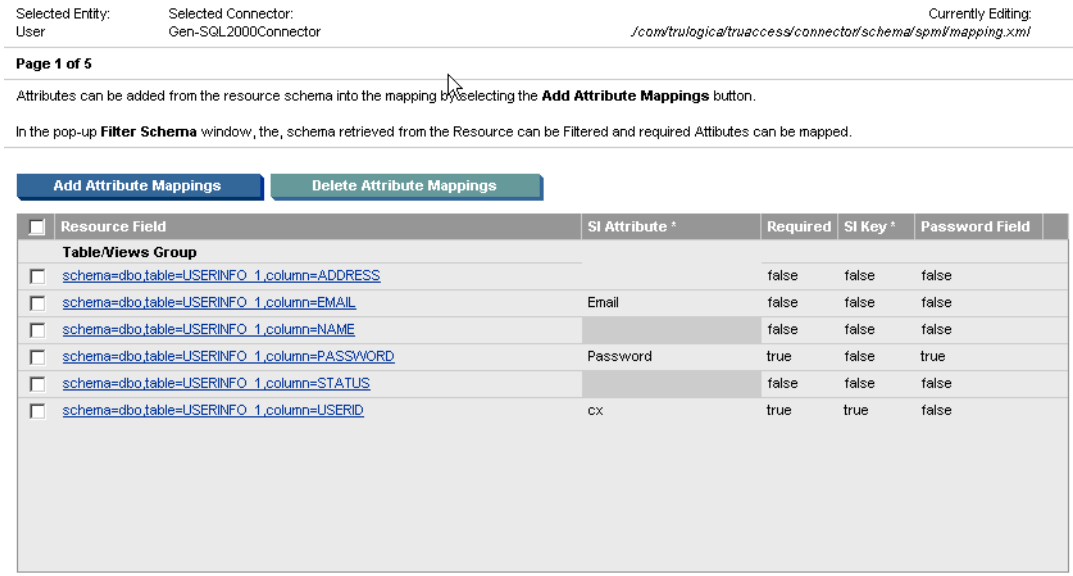
Attributes Home (Page 1)

This page lets you add or delete attributes from a database to Select Identity.

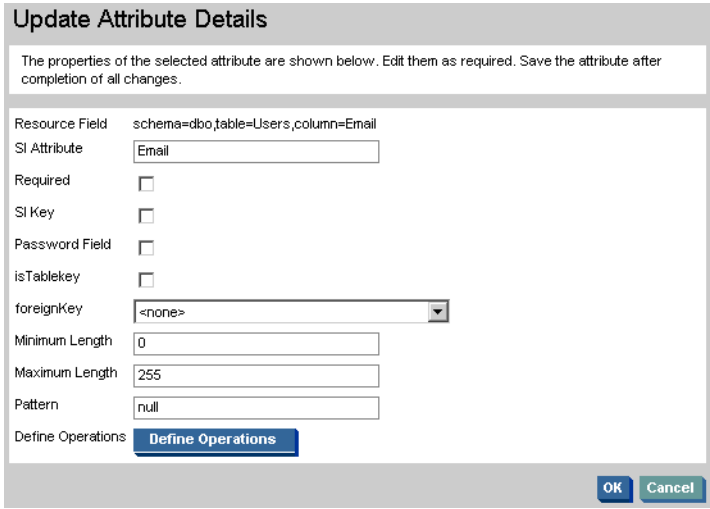
If you create a new mapping file, no mappings are listed on this page in the beginning, and the page looks like the screenshot below:



If you load an existing mapping file, the page lists the mappings that are currently defined in the file, as in this example:



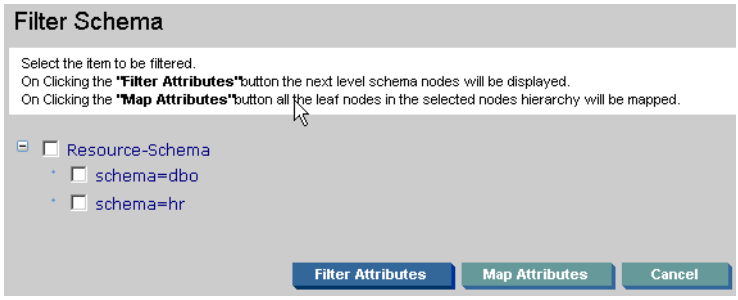
Each database column listed under Resource Field has a link. If you click the link, the properties of that mapping are displayed, which you can modify:



Mapping Attributes to Select Identity

The Attribute Mapping Utility maps the attributes of a database resource to Select Identity. To achieve this mapping, perform the following steps:

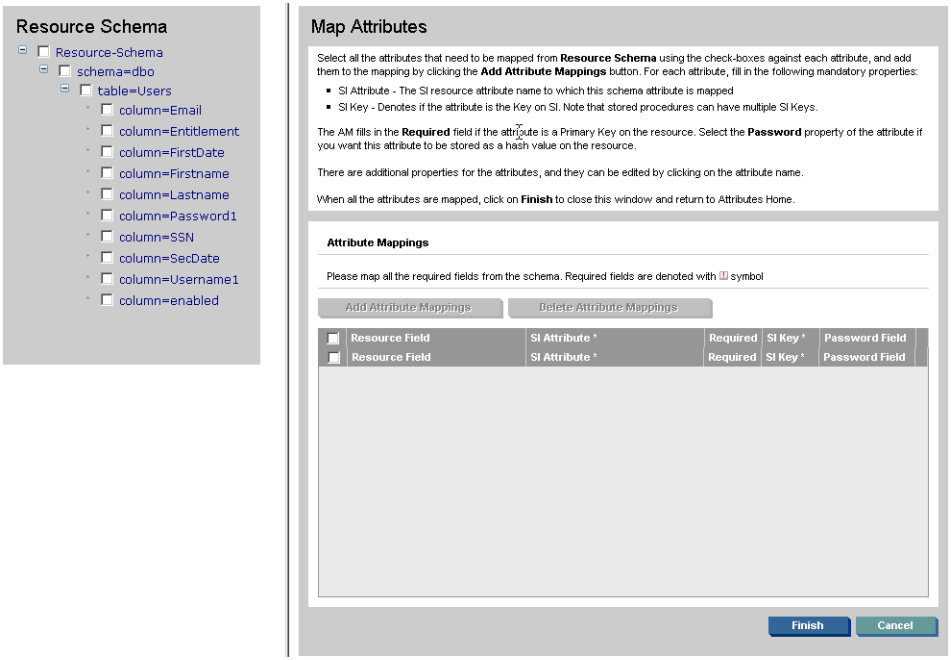
1. Load the mapping page of the connector, through the Select Identity user interface (see Usage Scenarios on page 592).
2. Click **Add Attribute Mappings** to open the Filter Schema page, which reads the database schema and provides a listing in a pop-up dialog. This displays the database schema in a hierarchical tree.



Select the schema, and then click one of the action menus at the bottom:

- Click **Filter Attributes** to display the next level of database schema. For example, if you select a schema, and then click **Filter Attributes**, the Tables and Stored Procedures under the Database Schema will be displayed.
- Click **Map Attributes** to display the Map Attributes page where the Database schema can be mapped into the mapping file. When a table schema is selected and **Map Attributes** is clicked, all the columns of the table become available for mapping.

3 Click **Map Attributes** to display the Map Attributes window, which reads the database schema of the resource and provides a listing on the left side of the window of the Selected Items from the Filter Schema page.



If you try to edit a mapping file without connecting to the database, the schema is not displayed.

4 Select the schema items (table, columns or Stored Procedure parameters) from the left frame, and then click **Add Attribute Mappings** to map them into the mapping file.

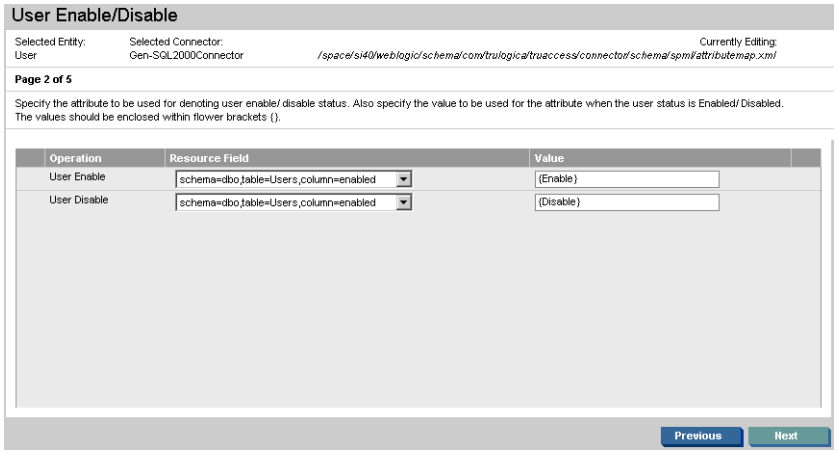
After mapping the required attributes, click **Finish** to return to the Attribute Home page that displays the attribute mappings and the associated properties.

5 Save the modified or newly created mapping file by clicking **File → Save Mapping File**.

For advanced operations, you can navigate to other pages.

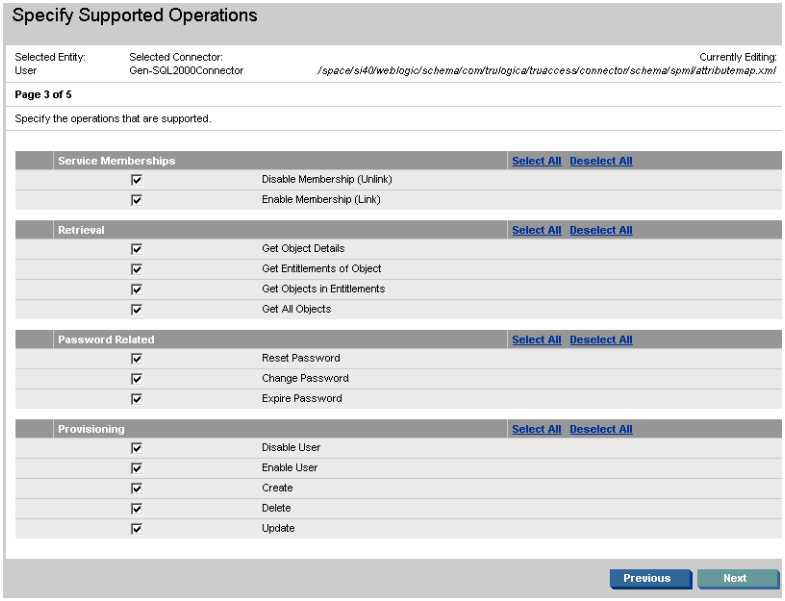
User Enable/Disable (Page2)

This lets you select the Status attribute from the **Database** menu and set values that are assigned when a user is enabled or disabled during provisioning.



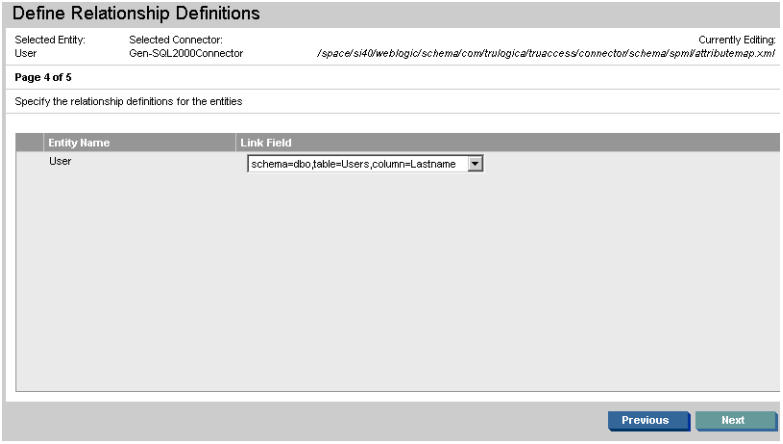
Specify Supported Operations (Page 3)

This lets you define the operations that the connector can perform on the entity.



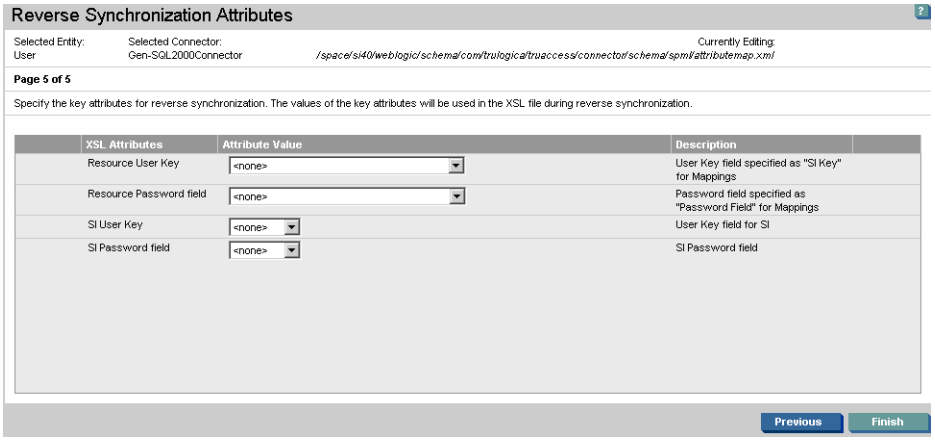
Define Relationship Definitions (Page 4)

The Define Relationship Definitions page defines how tables in the schema relate and lets you specify how user and entitlement information is linked in the database schema. The Define Relationship Definitions page defines which table columns are used to store the LINK (user-entitlement relationship) information for User or Group Entities.



Reverse Synchronization Attributes (Page 5)

It lets you map key fields that are used during reverse synchronization. This information is used to generate the corresponding XSL file for the XML mapping file.



For additional operations, access mapping pages through group entity. The follow mapping pages are available:

1. Attributes Home Page
2. Specify Supported Operations Page
3. Define Relationship Definitions Page
4. Provisioning Information Page

Provisioning Information page

This page displays the attributes that are mapped for the group entity, except for the attribute that is linked to the user attribute. You can provision entitlements directly in to the database. The Attribute Mapping Utility provisions group entities only.

See Mapping Pages on page 584 for procedures that illustrate how to set properties in these sections of the window.

Usage Scenarios

The database schema that stores user and entitlement data can be created in a number of ways. Usage Scenarios describe the most common schema configurations. The scenarios used in this chapter are the most likely configurations and provide a broader view of the required steps to define mappings for XML and XSL files.

Table Scenario

For user provisioning and entitlement provisioning procedures, three tables are used to store provisioning data:

- A user table called GEN_SQL_USERS that contains six columns, which define user attributes. For example, the table may contain the UserName, Password, Firstname, Lastname, Email, and City columns, which store user-related information.
- An entitlement table called GEN_SQL_ENTITLEMENTS that contains one column, which stores the list of possible entitlements that can be assigned to users. For example, the table may contain the EntitlementID and Description columns, which store entitlement information that can be assigned to users.
- A normalized mapping table called GEN_SQL_USER_TO_ENT that defines user-to-entitlement mappings and contains two columns, one to store user IDs and one to store the assigned entitlements. For example, the table may contain the UserName and EntitlementID columns, which store user name-to-entitlement mappings.

The user column in the mapping table uses the user column in the user table as its foreign key. Similarly, the entitlements column in the mapping table uses the entitlement column in the user table as its foreign key. Finally, when users and entitlements are provisioned, there can be one user ID per user and zero or more entitlements per user.

Stored Procedure Scenario

The database connectors allow the usage of stored procedures for provisioning and other user-related operations. A set of stored procedures can be written to perform operations that are typically done by the connector. These operations include creating a user, modifying a user, deleting a user, and so on. Hence, a stored procedure provides a way to abstract connector operations.

Stored procedures can be customized for the necessary operations.For more information on the most common schema configurations, see Usage Scenarios on page 592. The scenario used in this chapter is one of the more likely configurations. Here is a description of the scenario:

Three stored procedures are created in the database:

- The addUser stored procedure can create a user in the database, in the Users table. Values are passed as parameters to the procedure.
- The modifyUser stored procedure can modify user attributes for an existing user in the database. This procedure modifies all columns in the Users table except the UserName and Password columns.
- The deleteUser stored procedure takes a user name as a parameter and deletes the user from the database table.

Defining User Mappings

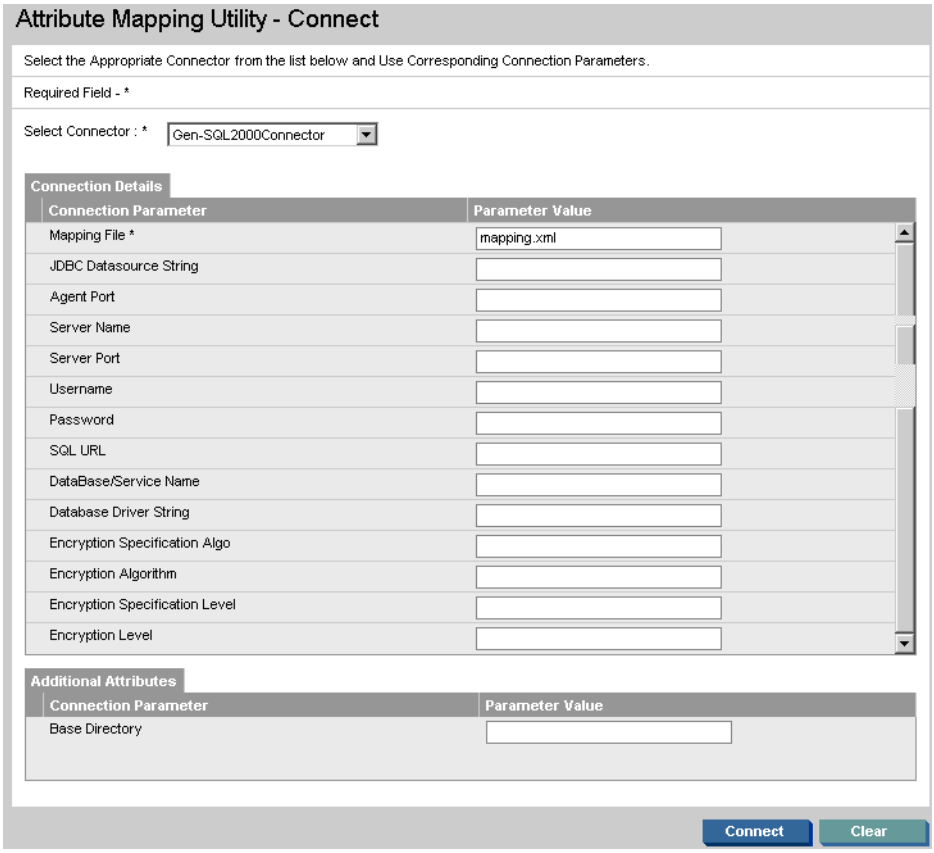
The following procedure describes how to map user and entitlement attributes to Select Identity attributes. When you finish defining the mappings, the XML mapping file is generated in the directory, which is specified in the Base Directory field when you logged into the Attribute Mapping Utility and connected to the schema.

1. Start the Attribute Mapping Utility by entering the following URL in the browser:

http://*hostname:port*/attributemapper/index.jsp

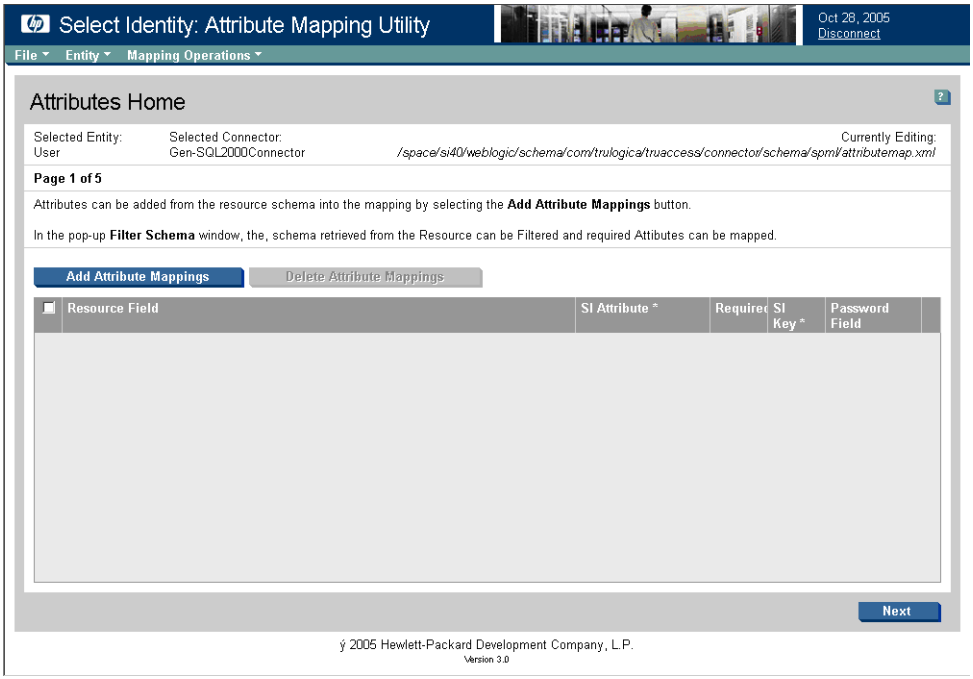
where *hostname* is the name or IP address of the application server on which Select Identity is deployed and *port* is the application server's port.

2 Connect to the database by selecting the deployed connector from the Select Connector drop-down list and entering connection information for the database. For this scenario, a JDBC data source is used to connect to the database. Therefore only the mapping file name and JDBC data source are specified. The Base Directory field specifies where the mapping files are stored on the Select Identity server.



Then, click **Connect**.

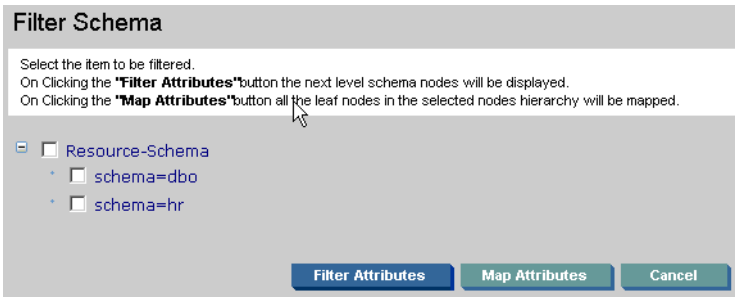
If the utility successfully connects to the database, the Attributes page displays to let you map user attributes. By default, the user entity is selected.



You can also use the Select Identity user interface to arrive at this step. For details, see Accessing the Attribute Mapping Utility.

3 Map each user attribute defined in the database schema to a Select Identity attribute:

   a Click **Add Attribute Mappings** to display the Filter Schema page, which provides a listing of the database schema in a pop-up dialog. It displays the database schema in a hierarchical form.



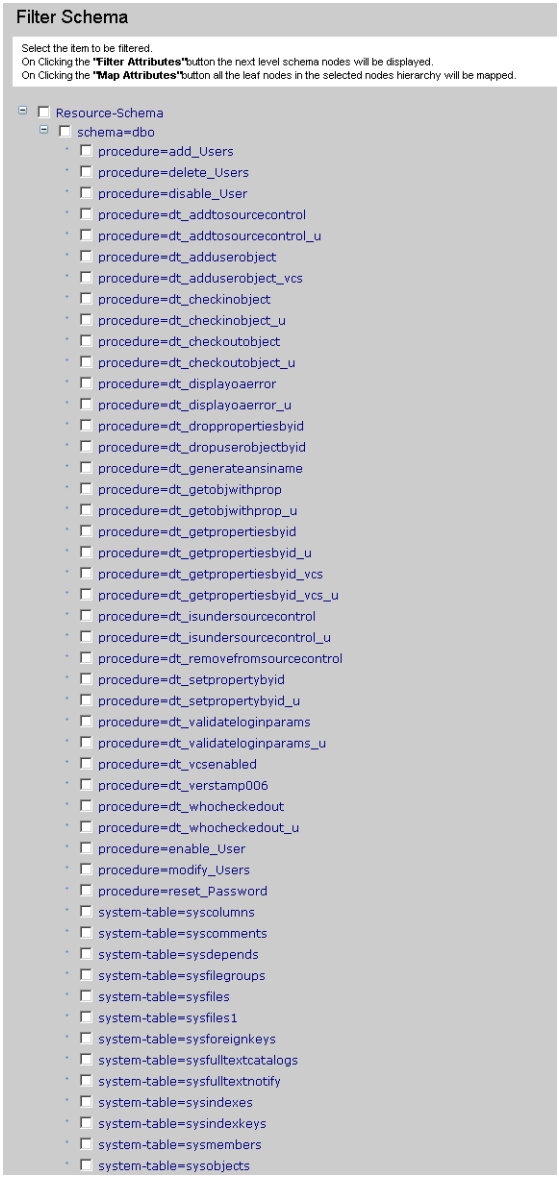
From this page, you can filter the tables, views, and stored procedures that you wish to map from the the rest of the database schema. This reduces the schema retrieval time and also provides a better view by showing only the selected schema when mapping attributes.

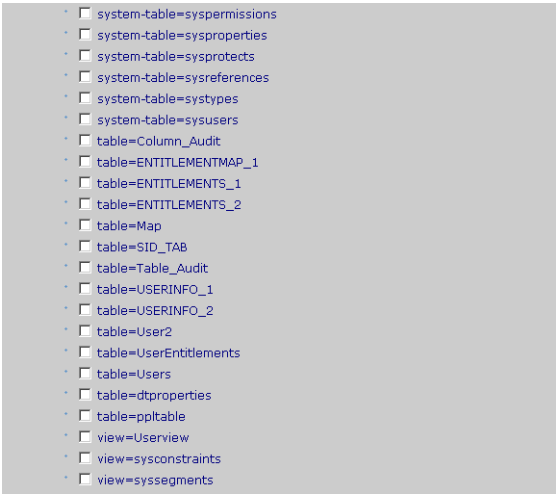
Note the following points when using Attribute Mapping Utility for Oracle:

– The Filter Schema page shows the schema for all users in Oracle. Here is an example of the Oracle schema displayed on the Filter Schema page:

- Select the schema where the required tables are present and click **Filter Attribute** to show only the tables or stored procedures in that schema.
- Make sure that the you have access privileges for the selected schema on the Filter Schema page. If not, the Map Attributes window will not display a schema. If more than one schema is selected and access privileges are available for a subset of the selected schemas, only the subset of schemas is displayed on the Map Attributes window.

b To select part of the schema for mapping, select the **Schema** check box and click the **Filter Attributes** button to display the schema. (You can also click the **Map Attributes** button to view the entire schema while mapping attributes.)


Filter Schema
Select the item to be filtered.
On Clicking the "Filter Attributes"button the next level schema nodes will be displayed.
On Clicking the "Map Attributes"button all the leaf nodes in the selected nodes hierarchy will be mapped.
Resource-Schema
schema=dbo
procedure=add_Users
procedure=delete_Users
procedure=disable_User
procedure=dt_addtosourcecontrol
procedure=dt_addtosourcecontrol_u
procedure=dt_adduserobject
procedure=dt_adduserobject_vcs
procedure=dt_checkinobject
procedure=dt_checkinobject_u
procedure=dt_checkoutobject
procedure=dt_checkoutobject_u
procedure=dt_displayoaerror
procedure=dt_displayoaerror_u
procedure=dt_droppropertiesbyid
procedure=dt_dropuserobjectbyid
procedure=dt_generateansiname
procedure=dt_getobjwithprop
procedure=dt_getobjwithprop_u
procedure=dt_getpropertiesbyid
procedure=dt_getpropertiesbyid_u
procedure=dt_getpropertiesbyid_vcs
procedure=dt_getpropertiesbyid_vcs_u
procedure=dt_isundersourcecontrol
procedure=dt_isundersourcecontrol_u
procedure=dt_removefromsourcecontrol
procedure=dt_setpropertybyid
procedure=dt_setpropertybyid_u
procedure=dt_validateloginparams
procedure=dt_validateloginparams_u
procedure=dt_vcsenabled
procedure=dt_verstamp006
procedure=dt_whocheckedout
procedure=dt_whocheckedout_u
procedure=enable_User
procedure=modify_Users
procedure=reset_Password
system-table=syscolumns
system-table=syscomments
system-table=sysdepends
system-table=sysfilegroups
system-table=sysfiles
system-table=sysfiles1
system-table=sysforeignkeys
system-table=sysfulltextcatalogs
system-table=sysfulltextnotify
system-table=sysindexes
system-table=sysindexkeys
system-table=sysmembers
system-table=sysobjects



The database schema is shown on the Filter Schema page in a tree that you can expand.

Here is an explanation of the tree:

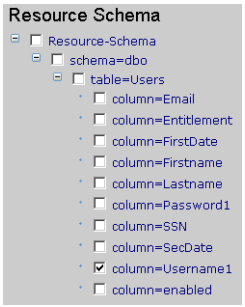
```
Database Name
|
| - Schema Names
|| - Table Names
|| - Procedure Names
||- View Names
```

c Select the user tables that you wish to map. After you select tables, click the **Map Attributes** button. This displays the Map Attributes window, which displays the expanded schema items selected on Filter Schema page.

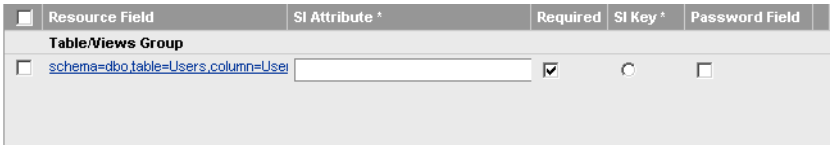
Here is the explanation of the tree:

```
Database Name
|
| - Schema Names
|| - Table Names
||| - Column Names
|| - Procedure Names
||| - In Parameters
||| - Out Parameters
```

d From the left side of the window, select the database column(s) that you want to map to a Select Identity attribute:

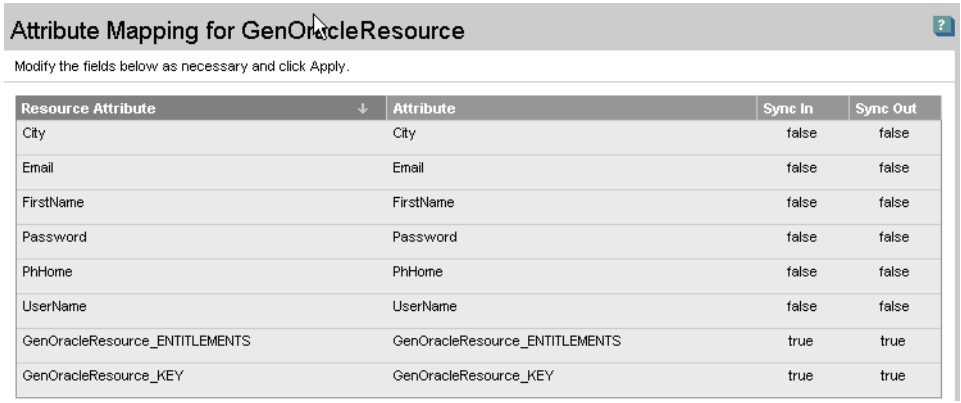


Then, click **Add Attribute Mappings** button. The selected column is added to the table:

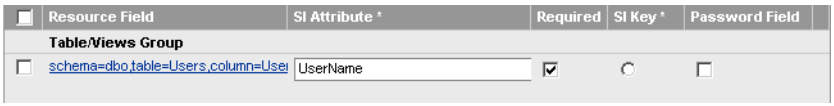


If you map a stored procedure, another section named Stored Procedure Group is added to the page below the Table/Views Group section.

e In the SI Attribute field, enter the name of the Select Identity attribute to which you want to map the selected database column. This value is the same as the value displayed in the Name column while creating attributes for the connector's resource on the Select Identity client. Here is a snapshot of the resource attributes for this scenario:



Because UserName is the attribute name in this scenario, enter **`UserName`** in the SI Attribute field for the USERID column:

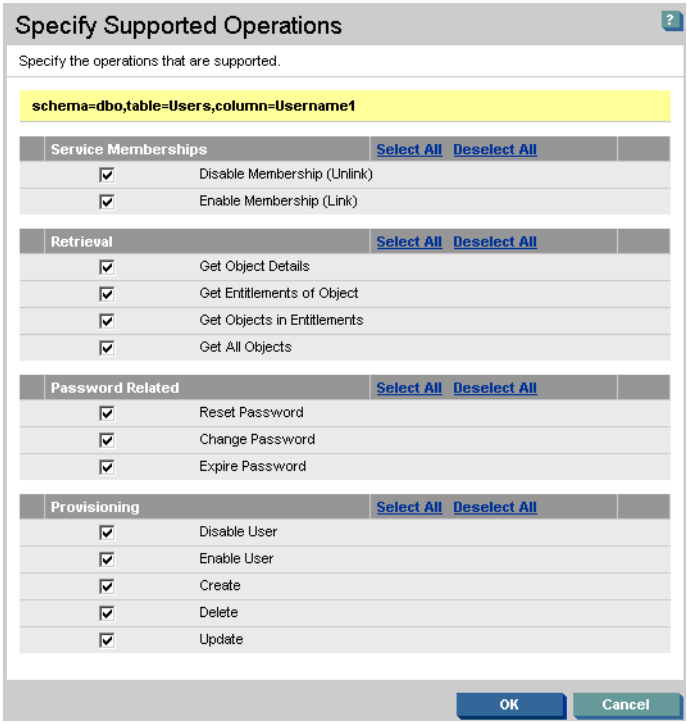


The **Required** option is selected if the chosen database column is the schema's primary key.

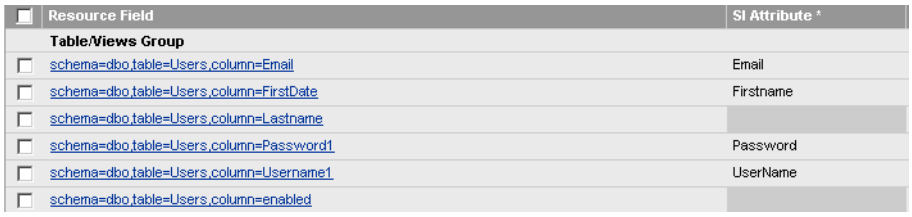
f Select the **SI Key** option if the specified attribute is a key field in Select Identity. If you add a stored procedure, you can select multiple attributes as key fields.

g To treat an attribute as `password` type, which can be used in the Reset Password or Change Password operation in Select Identity, select the **Password Field** option.

h If you wish to define the actions that the connector can perform for the attribute (not the entire entity), click the **Define Attribute Operations** button and select the allowed operations. A pop-up window appears in which you can select the operations, and then click **OK**.



i Repeat Step d through Step h for each user column you wish to map. The columns are added to the right side of the page in alphabetical order. Here is a snapshot of the defined user mappings for this scenario:



Resource Field	SI Attribute *
Table/Views Group	
schema=dbo,table=Users,column=Email	Email
schema=dbo,table=Users,column=FirstDate	Firstname
schema=dbo,table=Users,column=Lastname	
schema=dbo,table=Users,column=Password1	Password
schema=dbo,table=Users,column=Username1	UserName
schema=dbo,table=Users,column=enabled	

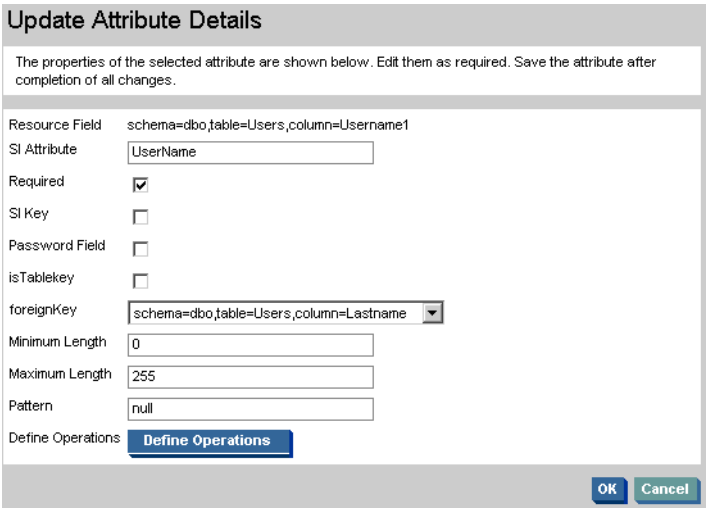
The Select Identity attribute specified for the STATUS column is arbitrary. You must map the column but the Enable/Disable settings (Step 4) control what is provisioned to this column.

j If you provision entitlements and the database schema includes two tables (one for user data and one for entitlements), you must map the user column from the entitlement table. If the database schema includes at least three tables, including a user-to-entitlement mapping table, you must map the columns of this table accordingly.

You can specify any value in the SI Attribute field for this mapping.

The user column in the mapping table is a foreign key to the USERID column of the GEN_SQL_USERS table. You must specify this for the mapping. Click the column name in the Resource Field:

The Update Attribute Details page appears. From the foreignKey drop-down list, select the user column of the user table.



Also, select the **isTableKey** option, and then click **OK**.

k Click **Finish** at the bottom of the Map Attributes window. The window closes and the mapped attributes are listed on the Attribute Mapping Utility page.

4 Define the Enable and Disable settings for the connector. This enables you to define the attribute that will be used for denoting user status. Complete the following steps:

a. Click **Next** under the Attribute Mappings section of the page or select **Mapping Operations → User Enable/Disable Attribute Configuration**. The User Enable/Disable section is displayed.

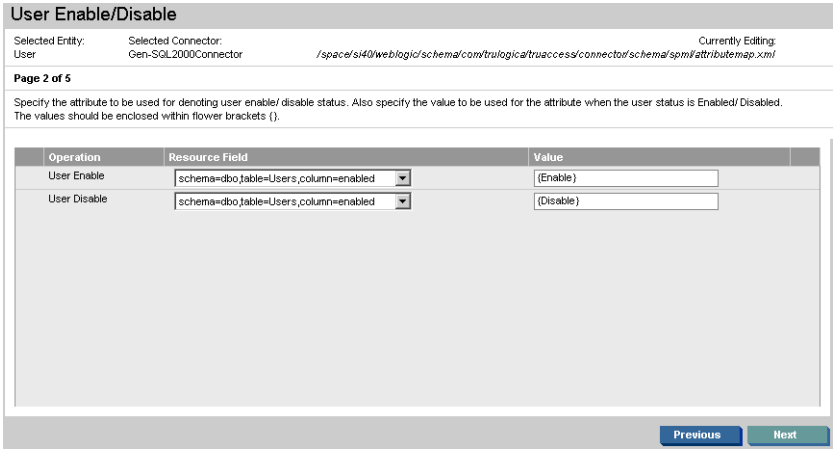
b. In the User Enable row, select a database table from the Resource Field drop-down list that will store a status value if the user is enabled. This column will be used by Select Identity's Enable All operation.

c. Specify the value to be stored when the user is enabled. If you intend to provision static text, surround the specified value with brackets (`{ }`).

d. In the User Disable row, select a database table from the Resource Field drop-down list that will store a status value if the user is disabled. This column will be used by Select Identity's Disable All operation.

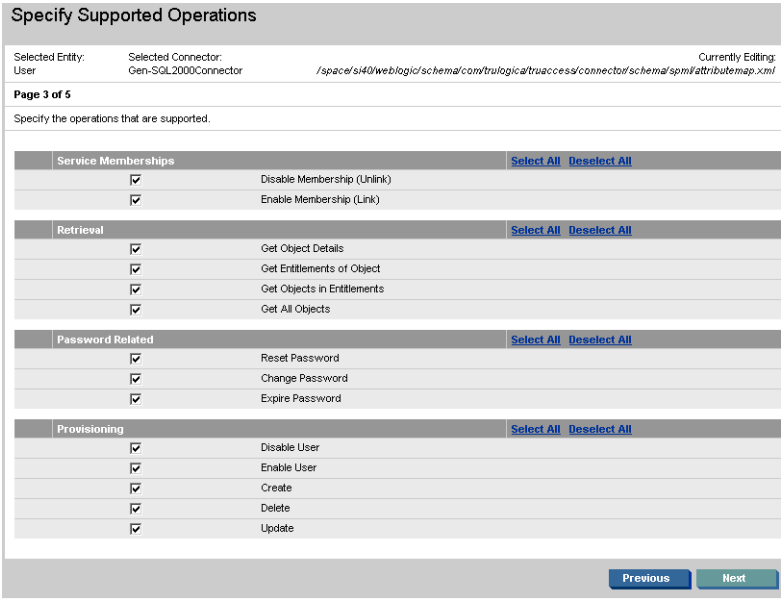
e. Specify the value to be stored when the user is disabled. If you intend to provision static text, surround the specified value with brackets (`{ }`).

Here is a snapshot of the values specified for this scenario:



5. Define the operations that Select Identity can perform on the database schema:

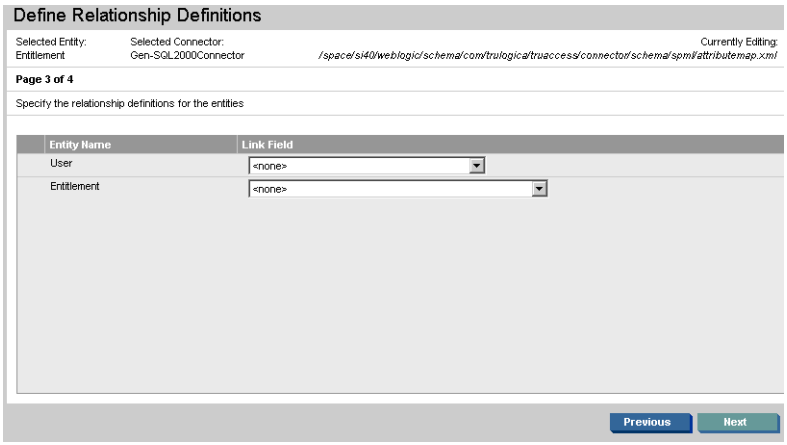
a. Click **Next** under the User Enable/Disable section of the page or select **Mapping Operations → Define Entity Operations**. The Specify Supported Operations section appears:



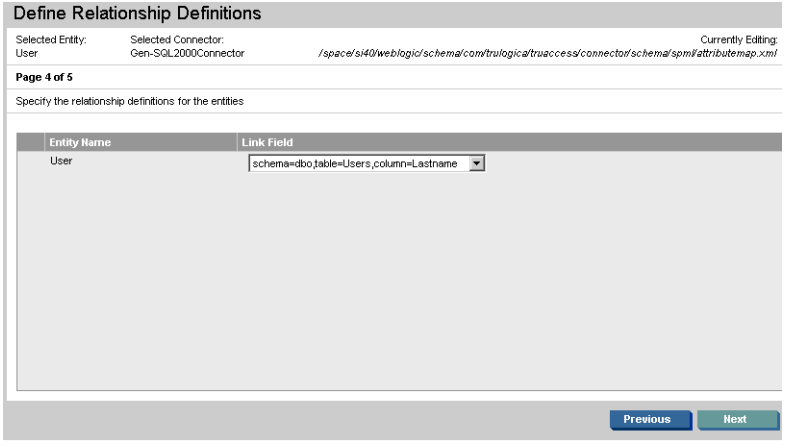
b Select or deselect the operations you want the connector to perform when provisioning users in the database schema (in the user table).

6 Define the relationship between entities and database tables by completing the following steps:

a Click **Next** under the Specify Supported Operations section of the page or select **Mapping Operations** → **Define Relationships**. The Define Relationship Definitions section is displayed:



If the entitlement entity has not been created in the Attribute Mapping Utility, the entitlement entity is not displayed here:



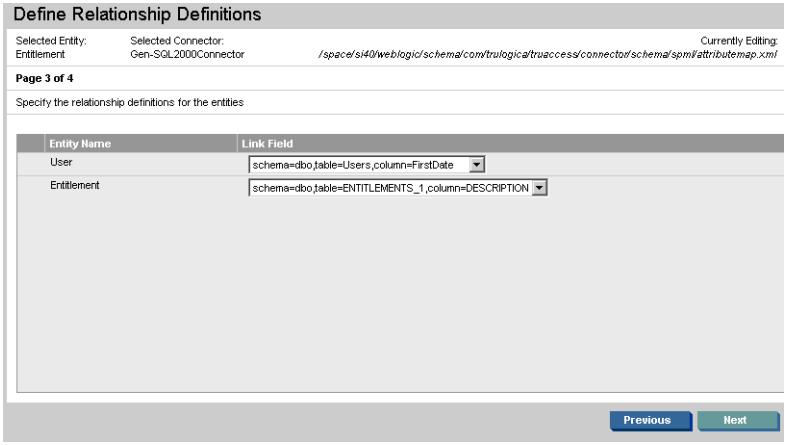
If you wish to provision entitlements, complete the steps in Defining Entitlement Mappings on page 609 then return to this step.

b For the user entity, select the column that stores the User entity's Key field for operations that involve entitlements. In this scenario, the user column in the mapping table is selected.

If there is no entitlement table and the connector will not perform group or entitlement operations, you can leave this field empty. If a column is selected from the **Link Field** list, it will not be available for provisioning user information.

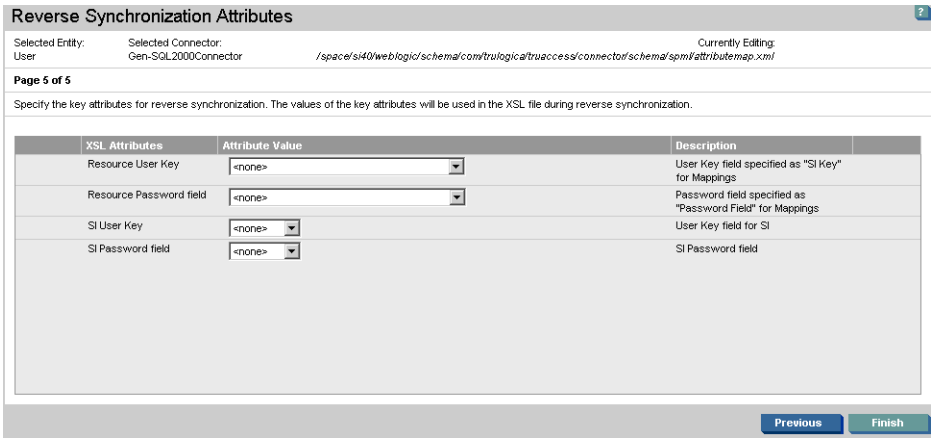
c For the entitlement entity, select the column that stores the user's entitlements. In this scenario, select the entitlement column in the mapping table.

Here is a snapshot of the relationships for the example scenario:



7 If you have configured the agent to perform reverse synchronization, you must define reverse mappings:

a Click **Next** under the Define Relationship Definitions section of the page or select **Mapping Operations** → **Reverse Synchronization Attributes**. The Reverse Synchronization Attributes section is displayed:



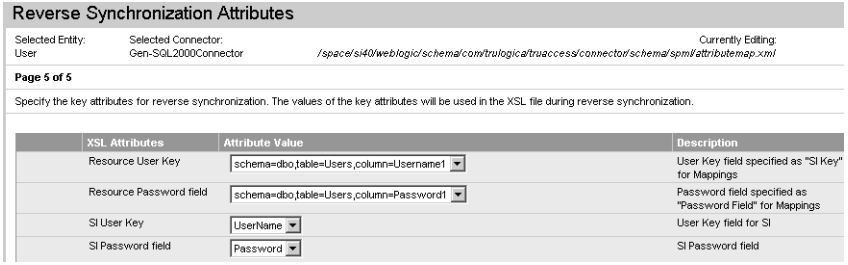
b From the Resource User Key drop-down list, select the database column that was mapped to the Select Identity attribute that is the Select Identity key.

c From the Resource Password field drop-down list, select the database column that was mapped to the Select Identity password attribute.

d From the SI User Key drop-down list, select the Select Identity attribute that is the Select Identity key for the user.

e From the SI Password field drop-down list, select the Select Identity attribute that stores the user password.

Here is a snapshot of the values specified for this scenario:



8 Select **File** → **Save Mapping File** to generate the XML and XSL files in the location specified in the Base Directory field when you connected.

You may want to verify that the `com.hp.ovsi.connector.schema.dir` property is set in the `TruAccess.properties` file, which resides in the *`install_dir`*`/sysArchive` directory on the Select Identity server. It

should be set to the top-level directory where the mapping files will be created, which is specified in the Base Directory field on the Attribute Mapping Utility interface.

If no value was specified in the Base Directory field, the `com/trulogica/truaccess/connector/schema/spml` directory structure was created in the application server's home directory.

For example, if you enter `C:\SI_3.3\schema` in the Base Directory field, the `com/trulogica/truaccess/connector/schema/spml` directory structure is created under that directory, and the XML and XSL files are created there. In this example, the files reside in this directory:

```
C:\SI3.3\schema\com\trulogica\truaccess\connector\schema\spml
```

Thus, you would set the `com.hp.ovsi.connector.schema.dir` property as follows:

```
com.hp.ovsi.connector.schema.dir = C:/SI3.3/schema
```

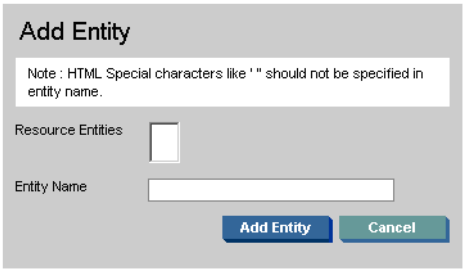
If you wish to download the XML and XSL files to the local system, select **File → Download Mapping File** or **File → Download Reverse Synchronization File**, respectively. To disconnect from the database or log out from the utility, click **Disconnect**.

Defining Entitlement Mappings

If the database schema contains entitlement data and you wish to provision entitlements, you must create an entitlement entity in the Attribute Mapping Utility. Otherwise, performing the steps in Defining User Mappings on page 593 generates the XML and XSL files required to provision users only.

Complete the following steps to create an entitlement entity and map its attributes. This procedure assumes that you are logged in to the Attribute Mapping Utility.

1. Add the entitlement entity to the Attribute Mapping Utility:
   a. Select **Entity → Add Entity**. The following displays:

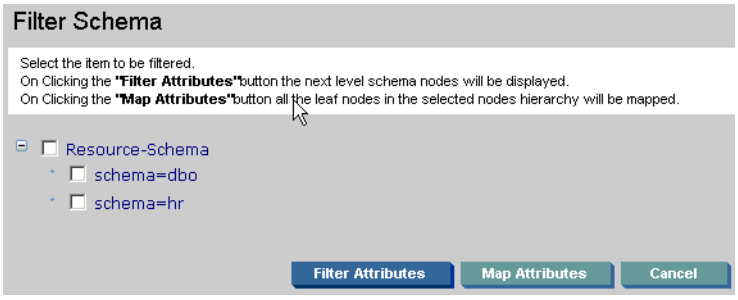


b In the Entity Name field, specify a name for the entitlement entity.

c Click **Add Entity**. The entitlement entity is selected in the utility window.

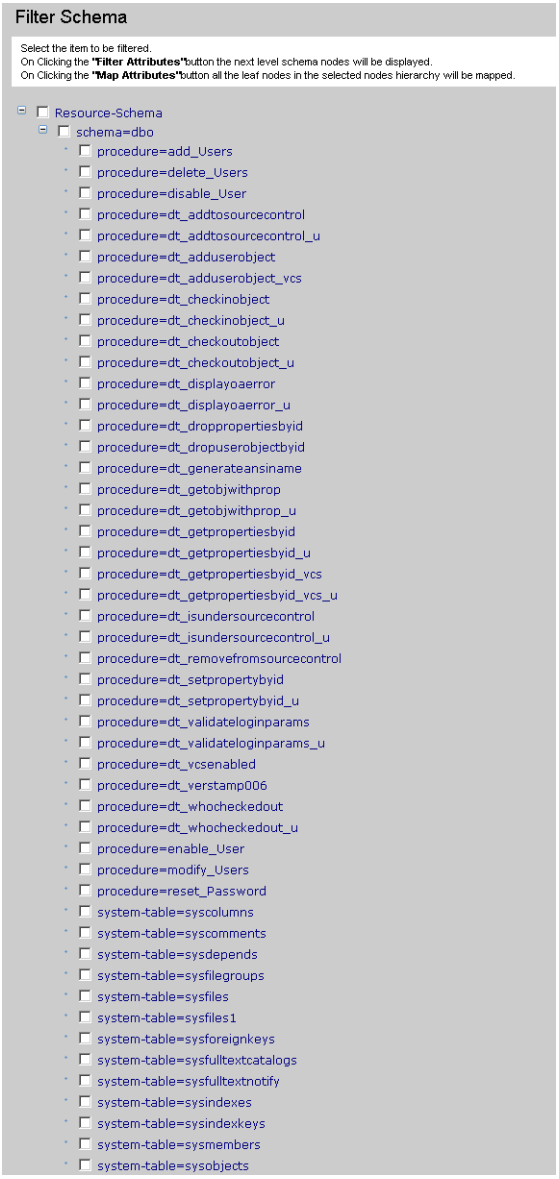
2 Map each entitlement attribute defined in the database schema to a Select Identity attribute:

a Click **Add Attribute Mappings** to display the Filter Schema page, which provides a listing of the database schema in a pop-up dialog. This displays the database schema in a hierarchical form.



From this page, you can filter the tables,views, and stored procedures that you wish to map from the the rest of the database schema. This reduces the schema retrieval time and also provides a better view by showing only the selected schema when mapping attributes.

b To select part of the schema for mapping, select the **Schema** check box and click the **Filter Attributes** button to display the schema. (You can also simply click the **Map Attributes** button to view the entire schema when mapping attributes.)



The database schema is shown on the Filter Schema page in a tree that you can expand.

Here is an explanation of the tree:

```
Database Name
|
| - Schema Names
|| - Table Names
|| - Procedure Names
||- View Names
```

c Select the entitlement tables that you wish to map. After you select tables, click on the **Map Attributes** button. This displays the Map Attributes window, which displays the expanded schema items selected on Filter Schema page.

Here is the explanation of the tree:

```
Database Name
|
| - Schema Names
|| - Table Names
||| - Column Names
|| - Procedure Names
||| - In Parameters
||| - Out Parameters
```

d In the left side of the window, select the database column that you would like to map to a Select Identity attribute:

Then, click the **Add Attribute Mappings** button. The selected column is added to the table:

e In the SI Attribute field, enter the name of the Select Identity attribute to which you want to map the selected database column. For this scenario, map the ENT_NAME column,and enter **`Entitlements`** in the SI Attribute field.

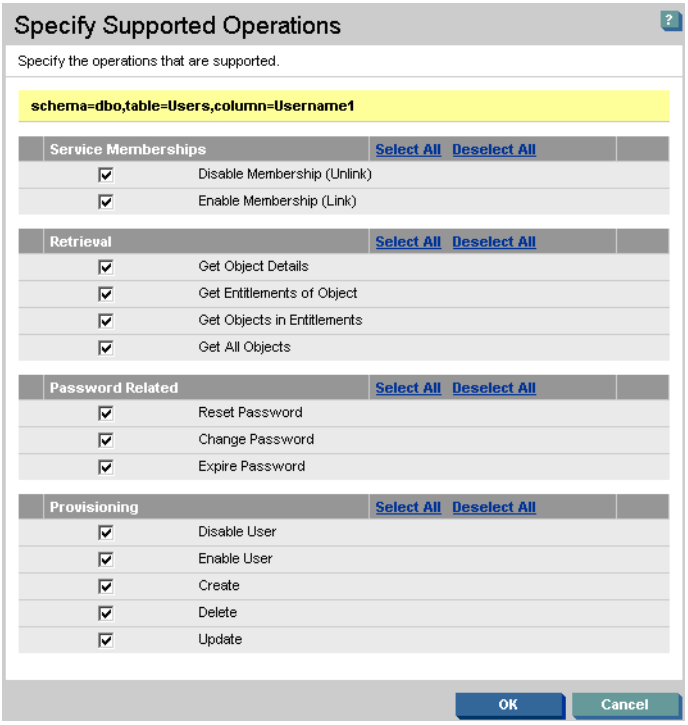
The **Required** option is selected if the chosen database column is the schema's primary key.

f Select the **SI Key** option if the specified attribute is a key field in Select Identity. This table column is the entitlement column that stores the entitlements that need to be retrieved using the connector.

g To treat an attribute as `password` type, select the **Password Field** option.

> Typically, attributes of an entitlement or group entity do not require this password behavior. Hence, this option can be ignored unless required.

h If you wish to define the actions that the connector can perform for the attribute (not the entire entity), click the **Define Attribute Operations** button and select the allowed operations. A window displays in which you can select the operations, and then click **OK**.



i Repeat Step d through Step h for additional entitlement columns you wish to map to Select Identity attributes. For this scenario, only the ENT_NAME column is mapped to a Select Identity attribute.

3 *If a mapping table is defined in the database schema:*
Map the entitlement column in the mapping table:

a. Select the entitlement column in the mapping table and click **Add Attribute Mappings**. The selected column is added to the list of mapped columns and attributes:

b. In the SI Attribute field, enter an arbitrary value. You simply need to provide a value to enable you to include this column in the mappings.

4. *If an entitlements table (in addition to a user table) is defined in the database schema:*
   Map the member column in the entitlements table to the entitlement column in the user table:

   a. Select the member column in the entitlement table and click **Add Attribute Mappings**. The selected column is added to the list of mapped columns and attributes.

   b. In the SI Attribute field, enter an arbitrary value. You simply need to provide a value to enable you to include this column in the mappings.

5. Click **Finish** at the bottom of the Map Attributes window.

6. If you have not done so, return to Step 6 on page 605 to define the relationship between the user entity and the entitlement entity.

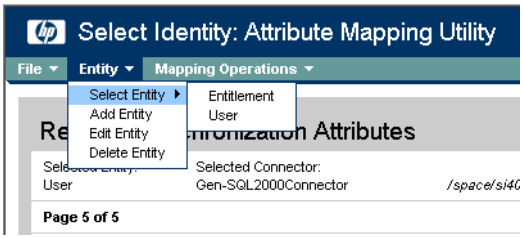
7. Select **File** → **Save Mapping File** to generate the XML and XSL files in the location specified in the Base Directory field when you connected.

If you wish to download the XML and XSL files to the local system, select **File** → **Download Mapping File** or **File** → **Download Reverse Synchronization File**. To disconnect from the database or log out of the utility, click **Disconnect**.

Provisioning Entitlements in the Database

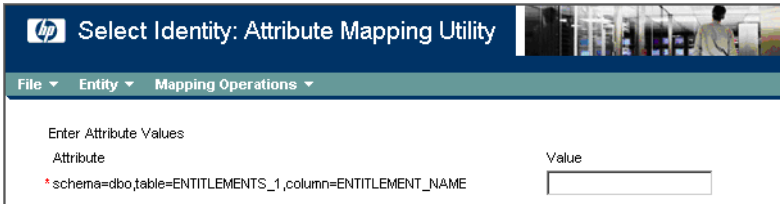
The Attribute Mapping Utility enables you to provision entitlements directly in to the database. Complete the following steps to provision entitlements using the utility:

1. Select the entitlement entity.



2 Select **Provision Entity** from the Mapping Operations menu. The Provisioning Information section displays and lists the attributes that are mapped for the entity.

3 Click **Add Attribute** to modify the values assigned to the attributes. The following window displays:



4 Change or enter a value in each Value field for the attributes you wish to provision in the database.

5 Click **OK** when you are done. The value is provisioned in the database.

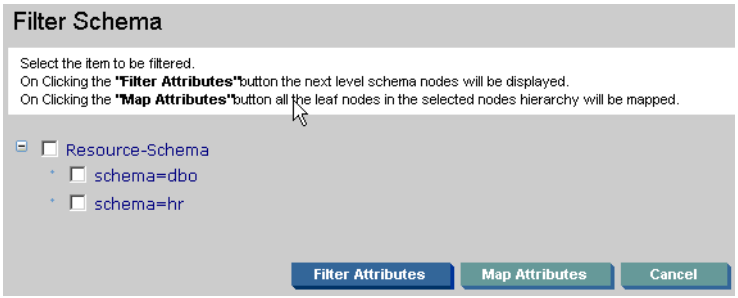
Mapping Stored Procedure Parameters

The following procedure describes how to map stored procedure parameters to Select Identity attributes. When you finish defining the mappings, the XML mapping file is generated in the directory specified in the Base Directory field when you logged in to the Attribute Mapping Utility.

These steps assume that you are logged in to the Attribute Mapping Utility and connected to the database.

Map each parameter for the stored procedure defined in the database schema, as follows:

1. Click **Add Attribute Mappings** to display the Filter Schema page, which provides a listing of the database schema in a pop-up dialog. This displays the database schema in a hierarchical form.



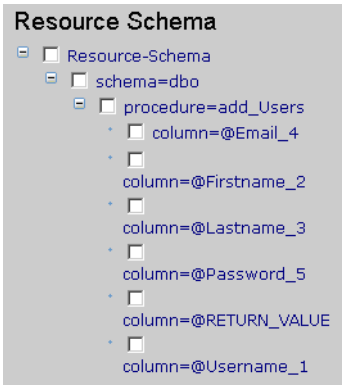
2. To select part of the schema for mapping, select the **Schema** check box and click the **Filter Attributes** button to display the schema. (You can also simply click the **Map Attributes** button to view the entire schema when mapping attributes.)

The database schema is shown on the Filter Schema page in a tree that you can expand.

Here is an explanation of the tree:

```
Database Name
|
| - Schema Names
|| - Table Names
|| - Procedure Names
||- View Names
```

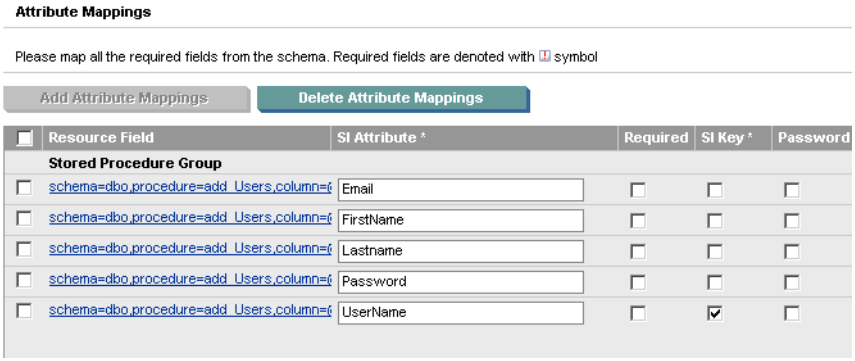
c Select the stored procedure tables that you wish to map. After you select tables, click on the **Map Attributes** button. This displays the Map Attributes window, which displays the expanded schema items selected on Filter Schema page.



Here is the explanation of the tree:

```
Database Name
|
| - Schema Names
|| - Table Names
||| - Column Names
|| - Procedure Names
||| - In Parameters
||| - Out Parameters
```

3 From the left side of the window, select the stored procedure parameters that you would like to map to Select Identity attributes. In the example below, all of the parameters for the addUser stored procedure (except the RETURN VALUE) are mapped:

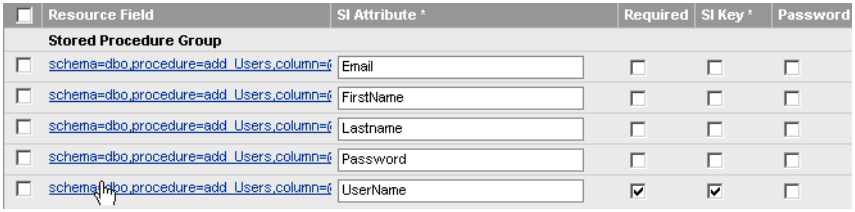


4 Map the parameters of the modifyUser and deleteUser stored procedures.

> Be sure to specify the Select Identity attributes exactly as they appear in the Select Identity client.
>
> Note that similar parameters may occur multiple times in the mapping, such as in this scenario; the Username parameter is required by all stored procedures. It is recommended that all Username parameters and table columns specify the same Select Identity attribute name.

5 Map the key column of the table into which the stored procedures are provisioning data. This is the column used to uniquely identify a user in the database tables and is used as a field to verify that the user is available to the connector.

In this scenario, all the stored procedures use the Username column of the Users table as the key field. Hence, this is mapped in the utility.



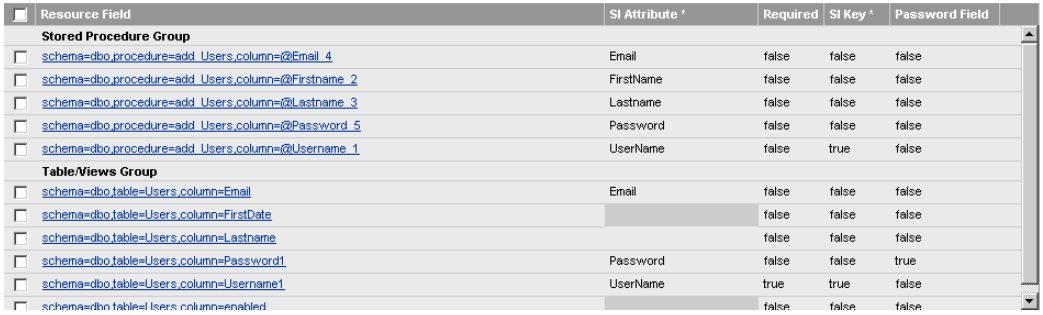
6 Provide the Select Identity key information for the mapped attributes. There are two cases here:

— The table column that is mapped is present in a separate group and the SI Key radio button is available. A radio button is available because only one SI Key attribute is supported for table column-related scenarios. Hence, the table column that is designated as the SI Key is the Select Identity key field.

— The store procedures parameters are grouped separately and the **SI Key** check box is available for each. Check boxes are available because you may have multiple Select Identity keys for stored procedures. Thus, check the **SI Key** option for all of the parameters that are analogous to the Select Identity key attribute of the mapped table column.

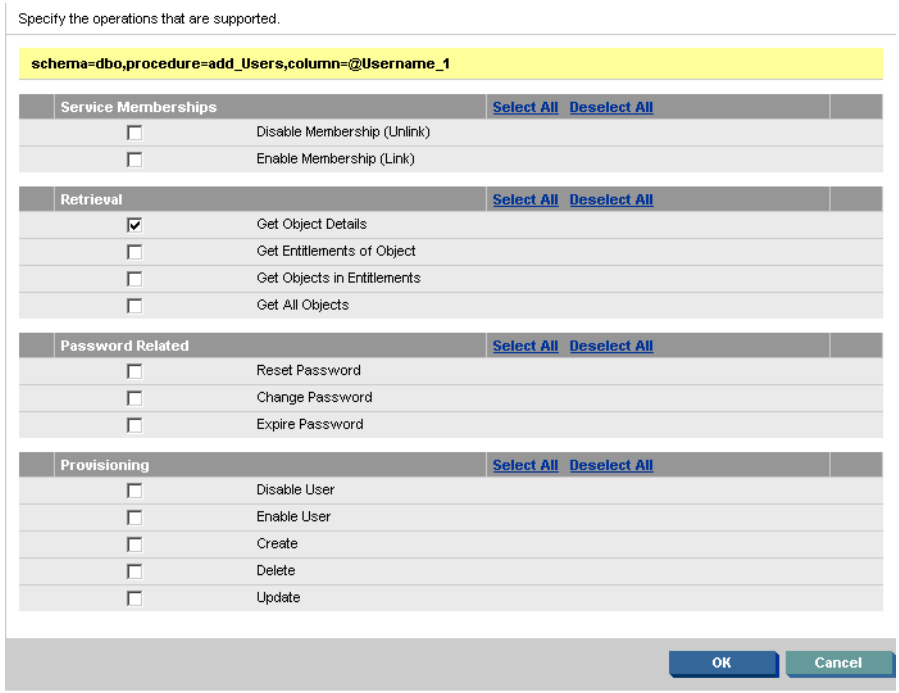
In the example scenario, the Username column in the Users table is the key field in Select Identity. For this column, the **SI Key** checkbox is selected in the Table/View Group.

In the Stored Procedure group, the **SI Key** checkbox is selected for all of the parameters that correspond to this table column (mapped to the Username parameter of adduser, modifyUser, and deleteUser stored procedures).



Resource Field	SI Attribute *	Required	SI Key *	Password Field
Stored Procedure Group				
schema=dbo,procedure=add_Users,column=@Email_4	Email	false	false	false
schema=dbo,procedure=add_Users,column=@Firstname_2	FirstName	false	false	false
schema=dbo,procedure=add_Users,column=@Lastname_3	Lastname	false	false	false
schema=dbo,procedure=add_Users,column=@Password_5	Password	false	false	false
schema=dbo,procedure=add_Users,column=@Username_1	UserName	false	true	false
Table/Views Group				
schema=dbo,table=Users,column=Email	Email	false	false	false
schema=dbo,table=Users,column=FirstDate		false	false	false
schema=dbo,table=Users,column=Lastname		false	false	false
schema=dbo,table=Users,column=Password1	Password	false	false	true
schema=dbo,table=Users,column=Username1	UserName	true	true	false
schema=dbo,table=Users,column=enabled		false	false	false

7 Click the **Define Operations** button for the mapped table column that is used for verifying that the user exists in the database table. For this attribute, select only the **Get Object Details** operation (deselect all other operations).



8 Click **Define Operations** for each of the stored procedure parameters and select only the relevant operations for which the parameter is used.

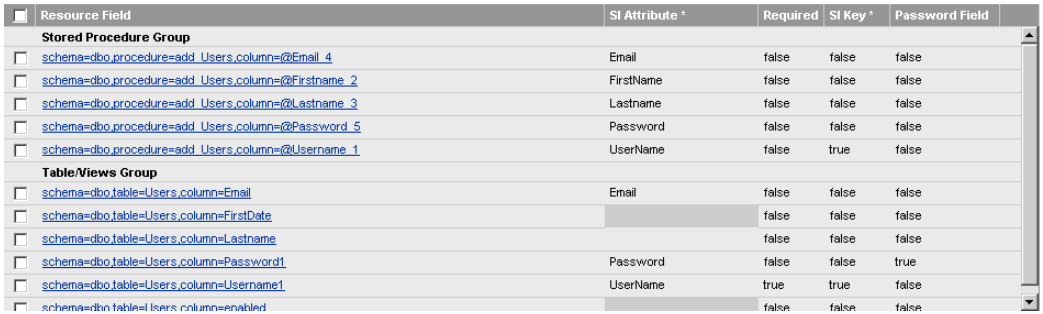
For example, the Username parameter of the addUser stored procedure will be used when performing Add operations only. Therefore, only the Create operation must be selected for this parameter.

Similarly, the Email parameter is required by the addUser and modifyUser procedures. The Email parameter of addUser should be enabled for Create operations only and the Update operation should be enabled for the Email parameter of the modifyUser stored procedure.

The Update operation must be enables for the Username parameter of the modifyUser procedure.

Finally, the Delete operation must be enabled for the Username parameter of the deleteUser procedure.

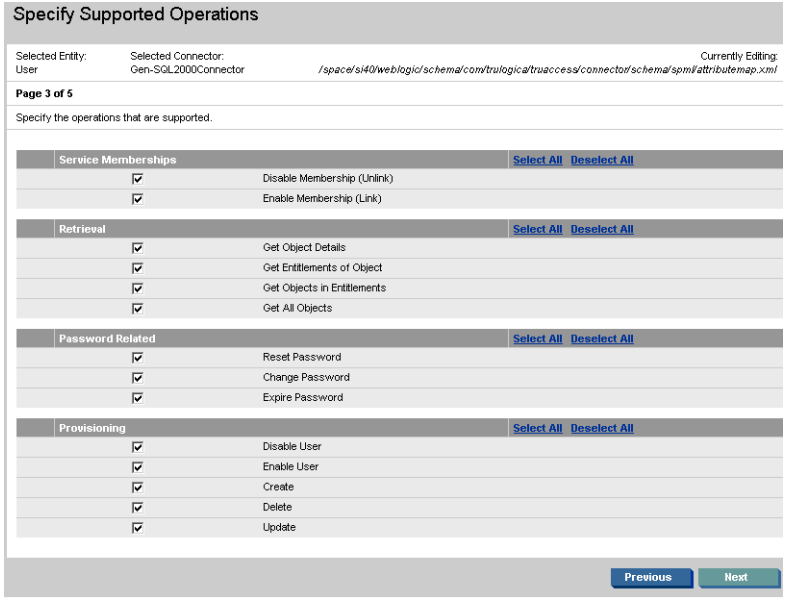
9 Click on the **Finish** button to return to the Attributes page. This displays the mappings for the table columns and stored procedure parameters. You can click on the **Edit** link for any attribute to modify the details.



Resource Field	SI Attribute *	Required	SI Key *	Password Field
Stored Procedure Group				
schema=dbo,procedure=add_Users,column=@Email_4	Email	false	false	false
schema=dbo,procedure=add_Users,column=@Firstname_2	FirstName	false	false	false
schema=dbo,procedure=add_Users,column=@Lastname_3	Lastname	false	false	false
schema=dbo,procedure=add_Users,column=@Password_5	Password	false	false	false
schema=dbo,procedure=add_Users,column=@Username_1	UserName	false	true	false
Table/Views Group				
schema=dbo,table=Users,column=Email	Email	false	false	false
schema=dbo,table=Users,column=FirstDate		false	false	false
schema=dbo,table=Users,column=Lastname		false	false	false
schema=dbo,table=Users,column=Password1	Password	false	false	true
schema=dbo,table=Users,column=Username1	UserName	true	true	false
schema=dbo,table=Users,column=enabled		false	false	false

10 From the **Mapping Operations** menu, select **Define Entity Operations**.

11 On the page that appears, select the operations that are required to support the entity.



12 From the File menu, select the **Save Mapping File** option to save the XML file.

User Tables and Stored Procedures Scenarios

The scenarios provided in this section describe possible ways to provision identity information through the use of user tables, stored procedures, and a combination of user tables and stored procedures.

One User Table

A single database table is created and contains all user information. This table has columns for all the user attributes, such as the name, ID, password, email address, and so on.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user table as resource attributes. You can then map Select Identity attributes to the table columns and provision users.

One User Table, One Entitlements Table

A single database table is created and contains all user information. This table has columns for all user attributes, such as the name, ID, password, email address, and so on. In addition, the user table provides a column that contains all of the user's entitlements (such as memberOf). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "group1, group2, group3".

Another table is created to store the entitlements. This table has columns that define each entitlement, such as the name and description. In addition, this table has a column for listing users belonging to this entitlement (such as members). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "user1, user2, user3, user4". Populate the entitlement table with entitlements that are to be associated and dissociated with the user.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user table as resource attributes. You can then map Select Identity attributes to the table columns and provision users.

Select Identity also retrieves the entitlements during the Service configuration or user creation, and connector loads all entries from the entitlement table.

The users are provisioned in the members column of the database.

For example, if you create a group entity names Entitlement for the entitlement table in the schema, and you provision a user with the administrator entitlement (in Select Identity), the memberOf column of that user will have a value “administrator”. If more than one entitlement is assigned, they are comma separated, as in this example: administrator,guest. Similarly, the user will be provisioned in the members column of the Entitlement table for each entitlement assigned to him or her. If more than one user is given the same administrator entitlement, the members column for the administrator row will have “user1,user2” as its value.

One User Table, One Entitlements Table, One Map Table

A single database table is created and contains all user information. This table has columns for all user attributes, such as the name, ID, password, email address, and so on.

Another table is created to store the entitlements. This table has columns that define each entitlement, such as the name and description. In addition, this table has a column for listing users belonging to this entitlement (such as members). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "user1, user2, user3, user4". Populate the entitlement table with entitlements that are to be associated and dissociated with the user.

A third table is created to store the user-to-entitlement mappings. This table refers to the primary keys (PKs) of user table and entitlements table. This map table has columns such as user name and entitlements.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user table as resource attributes. You can then map Select Identity attributes to the table columns and provision users.

Select Identity also retrieves the entitlements during the Service configuration or user creation, and connector loads all entries from the entitlement table.

If more than one entitlement is assigned to a user, the values are provisioned in separate rows in the map table.

For example, if the user1 user is assigned the administrator and guest entitlements, the map table will have two rows, user1-administrator and user1-guest.

Multiple User Tables

A table is created to store some user information. This table can have columns to store such attributes as user name, ID, password, email address, and so.

Additional tables can be created to store additional user information. These tables can contain columns to store data such as company, department, costcenter, address, phone number, and so on. The tables must have a foreign key constraint against the main user table.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user tables as resource attributes. You can then map Select Identity attributes to the table columns and provision users. Provisioning should populate the user tables.

Two User Tables, One Entitlements Table

A table is created to store some user information. This table can have columns to store such attributes as user name, ID, password, email address, and so. In addition, the user table provides a column that contains all of the user's entitlements (such as memberOf). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "group1, group2, group3".

Another table is created to store additional user information. This table can contain columns to store data such as company, department, costcenter, address, phone number, and so on. This table has a foreign key constraint against the main user table.

A third table is created to store the entitlements. This table has columns that define each entitlement, such as the name and description. In addition, this table has a column for listing users belonging to this entitlement (such as members). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "user1, user2, user3, user4". Populate the entitlement table with entitlements that are to be associated and dissociated with the user.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user tables as resource attributes. You can then map Select Identity attributes to the table columns and provision users.

Select Identity also retrieves the entitlements during the Service configuration or user creation, and connector loads all entries from the entitlement table.

Two User Tables, One Entitlements Table, One Map Table

A table is created to store some user information. This table can have columns to store such attributes as user name, ID, password, email address, and so.

Another table is created to store additional user information. This table can contain columns to store data such as company, department, costcenter, address, phone number, and so on. This table has a foreign key constraint against the main user table.

A third table is created to store the entitlements. This table has columns that define each entitlement, such as the name and description. In addition, this table has a column for listing users belonging to this entitlement (such as members). This is a multi-valued attribute and the mapping could implement it as a CSV, such as "user1, user2, user3, user4". Populate the entitlement table with entitlements that are to be associated and dissociated with the user.

A fourth table is created to store the user-to-entitlement mappings. This table refers to the primary keys (PKs) of user table and entitlements table. This map table has columns such as user name and entitlements.

When the resource is deployed in Select Identity, the connector loads all of the column names from the user tables as resource attributes. You can then map Select Identity attributes to the table columns and provision users.

Select Identity also retrieves the entitlements during the Service configuration or user creation, and connector loads all entries from the entitlement table.

Multiple User Tables, Multiple Entitlement Tables

Multiple user tables and entitlement tables can be created, where the user information is store in several tables. Each entitlement table has a specific type of entitlements. For example, there could be a table for user groups, one for roles, and one for access control levels.

Because there is more than one entitlement table, you must create more than one group entity for the connector's mapping file (using that attribute mapping utility). For example, if the Roles and ACL entitlement tables exist in schema, you must create two entities to map these two entitlement tables.

Single Stored Procedure

A stored procedure is created in the database, which will be called by the connector for all provisioning operations. When mapping attributes (such as using the attribute mapping utility), map all of the Select Identity user attributes to the arguments of the stored procedure. When the connector provisions users, the stored procedure is called with the argument values as attributes.

Multiple Stored Procedures

A separate stored procedure is created in the database for each of the user provisioning operations, such as to add a user, modify a user, delete a user, get a user, enable a user, disable a user, reset a password, and so on. When mapping attributes (such as using the attribute mapping utility), map all of the Select Identity operations to the stored procedures. Then, map all of the Select Identity user attributes to the arguments of the stored procedures. When the connector provisions users, the stored procedures are called with the argument values as attributes.

A mapping file for this scenario must map the parameters of the stored procedures and it must specify the attribute level operations (Define Operation) for each parameter. For example, the UserID parameter of the createUser stored procedure will have “create” in its defined operations because the parameter should be used only for the Add User operation.

Stored Procedure for Attributes

Certain attribute information must be encrypted before being stored in the database. The connector passes data to the stored procedure that it calls. You can create one or more stored procedures to be called for encryption of attribute information. Then, map the attributes to the stored procedures.

Tables and Stored Procedures

There may be scenarios in which a user is provisioned using a combination of updating table and invoking stored procedures in the database. For example, a user could be added to tables but a stored procedure is invoked to enable or disable the user. Review the table and stored procedure scenarios above to understand the necessary configuration.

Index

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X