HP OpenView Select Identity

Administrator Guide

Software Version: 3.3.1

UNIX® (Sun Solaris, HP-UX, Red Hat Enterprise Linux) and Windows® Operating Systems

July 2005

Legal Notices

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

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

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 that increases efficiency, productivity, and security for the complex or extended enterprise. Select Identity uses a patent-pending technology to manage the entire identity life cycle (provisioning, maintenance, and termination). Select Identity offers key business functionality to drive even greater efficiency: delegation of authority, reporting, audits, integration of workflows, and approval processes.

Select Identity is the first truly scalable solution for managing identity within and between large enterprises. The Select Identity solution automates the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Along with robust workflow, user self-service, reporting, and delegated administration capabilities, Select Identity is the most comprehensive identity management system available.

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. 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. 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.

Key features of the Select Identity system include the following:

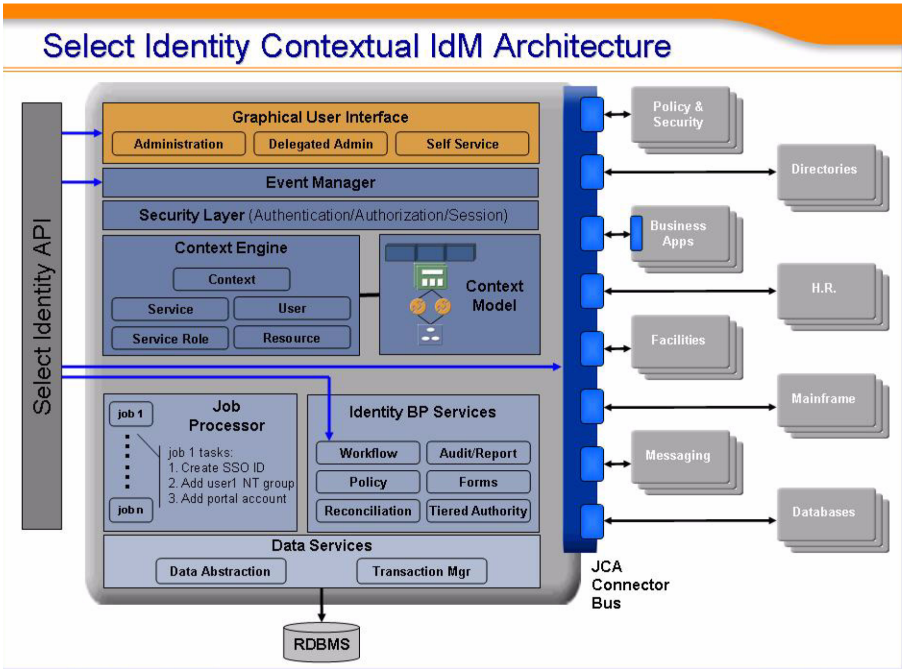
- **Centralized Management** – Provides a single point of control for the management of users and entitlements
- **Provisioning** – Automates the creation, update, and deletion of accounts and entitlements on information systems across the enterprise
- **Administrative Delegation** – Enables administrative rights to be distributed to multiple tiers of functional departments, customers, and partners
- **User Self-service** – Enables end users to initiate access to Services, change passwords, set password hints, and update general identity information through a simple web-based client
- **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 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.

System Architecture

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 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 Select Identity system capabilities 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 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.

These functions include

Context Management – Maintains the Context structure that defines identities and access for all users and resources in the extended enterprise.

Service Management – Provides a business-centric abstraction over resources, entitlements, and other identity-related entities. Services represent the products and services that you offer to customers and partners.

Service Role Management – Provides granular control over how groups of users access Services.

User Management – Provides consistent account creation and management across Services.

Resource Management – Provides a client to the physical information systems on which your Services rely for user account data.

Workflow Studio – Defines account provisioning processes that can be executed to grant access to Services for any event within the Select Identity system.

Reconciliation – Ensures the proper coordination of provisioning workflow across multiple resources.

Auditing and Reporting – Provides robust standard and custom reporting facilities for user entitlements and system event history.

Forms – Automates the creation of electronic forms presented to end users that are used to register for access to services, change passwords, set password hints, and update personal information.

Tiered Authority – Enables the secure, multi-tiered delegation of administrative roles, such as management of identity profiles and entitlements, to functional departments, customers, and partners.

Leveraging an open, standard, J2EE Connector Architecture (JCA) bus, Select Identity uses predefined connectors to access back-end system data stores. Connectors are configured during the installation process and are easy to deploy. If you wish to create your own connectors, Select Identity offers a software developer’s kit (SDK) that enables you to do so. See the *HP OpenView Select Identity Connector Guide* for information.

Configuring and Optimizing Select Identity

Optimizing Select Identity

It is strongly recommended that you customize Select Identity before you start using it. Performance during tasks such as Auto Discovery and Reconciliation is impacted if Select Identity is not optimized. Follow these guidelines before using the product:

- When creating the Oracle database connection, always enter the user name in uppercase. This prevents logging errors associated with converting the name to uppercase.
- Add **`ulimit -n 20480`** to one of the following WebLogic startup (wrapper) scripts created by the installer:

  ```
  Unix:      /opt/si3.3.1/weblogic/scripts/myStartWL.sh
  Windows:   C:/si3.3.1/weblogic/scripts/myStartWL.cmd
  ```

  Execute the script as follows:

  ```
  Unix:      sh /opt/si3.3.1/weblogic/scripts/myStartWL.sh
  Windows:   C:\si3.3.1\weblogic\scripts\myStartWL.cmd
  ```

  For procedures to install and execute these scripts, see “Installing on WebLogic Servers” in the *HP OpenView Select Identity Installation Guide*.
- Set the JVM Max Perm Size to 128 Megabytes or higher

  — For WebLogic, this can be accomplished by adding the following line to the `startWebLogic` script:

  ```
  MEM_ARGS="-XX:MaxPermSize=128M"
  ```
- Set the maximum JVM heap size as 1024 Megabytes or higher.

  — For WebLogic, add `-Xmx1024m` as a java option in the `startWebLogic.cmd` or `startWebLogic.sh` scripts.

  — For WebSphere, select the following through the WebSphere console: **Application Servers** → **server** →**Process Definition** →**Java Virtual Machine** →**Maximum Heap Size**.
- Be sure you have the most current `commons-logging.jar` file provided in the `library` directory on the Select Identity product CD.

- Set `JTA Timeout = 800.`
  - In the WebLogic Console, set the JTA timeout in: **Mydomain** → **Services** → **JTA**.
  - In the WebSphere Console, set the JTA timeout in: **WebSphere Administrative Domain → Servers → server_name → Application Servers → application_server_name → Transaction Service.**
- Increase the JDBC Connection Pool maximum size
  - In the WebSphere Console, set

    `Connections: Capacity Increment = 1` and `Maximum Capacity = 100`

    Set the Connections capacity in: **JDBC Providers → SI_Oracle_JDBC_Provider → Data Sources → jdbc.TruAccess → Connection Pools**
  - In the WebLogic Console, set

    `Connections: Capacity Increment = 20` and `Maximum Capacity = 100`

    Set the Connections capacity in: **Mydomain → JDBC → Connection Pools → SI Connection Pool → Configuration → Connections**.

➤ Before setting the maximum capacity, check with your database administrator. 100 is acceptable as long as the database is configured to handle over 100 concurrent connections. If this value is too high, setting it to the highest level acceptable for your database will still be beneficial.

- Set logging level = WARNING.

  In the JRE `logging.properties` file, add the following line: **`.level=WARNING`**. See "Logging" in the *HP OpenView Select Identity Installation Guide* for more information about configuring the `logging.properties` file.
- Limit the number of requests that are concurrently processed, using the `truaccess.workflow.thread.poolsize` property in the `TruAccess.properties` file.

  The `truaccess.workflow.thread.poolsize` property specifies the number of workflows to be instantiated at any given time, thereby preventing the system from slowing or locking up because too many requests are being processed simultaneously. The default setting is **`15`**.

On systems where a high volume of requests are expected, this number can be increaded to allow more requests to be processed simultaneously. Consider these two issues when increasing this property:

— The system should have the physical capacity to handle the additional processing

— Related tuning parameters such as the number of database connections should be increased appropriately

The above parameter values are recommendations and may vary depending on your environment. You should carefully examine your specific environment and fine tune settings that affect the Application Server or Database when running Select Identity.

For more details on how to configure these settings and other important settings, see the *HP OpenView Select Identity Installation Guide*.

Customizing the Graphical Interface

You can customize parts of the Select Identity graphical interface to reflect your company information. You do this by editing specific default settings in the `TruAccess.properties` file, which is located in the `%InstallDir%\sysArchive` directory.

You can also change the search criteria setting, which is defined to display a drop-down list if there are less than 50 items in the list. If greater than 50, the search icon 🔍 replaces the drop-down list, in which case, you click 🔍 to search for and select the item. See "Customizing the Graphical Interface " in Chapter 6 of the *HP OpenView Select Identity Installation Guide* for details on how to configure these settings and other important settings.

Support

If you need to call support for help regarding Select Identity deployment or maintenance, please have the version and build numbers available for the representative. You can locate the build number by running the following command from the web server:

```
java -jar connector.jar connector.jar
```

Product Documentation

The Select Identity product documentation includes the following:

- Release notes are provided in the top-level directory of the HP OpenView Select Identity CD. This document provides important information about new features included in this release, known defects and limitations, and special usage information that you should be familiar with before using the product.
- For installation and configuration information, refer to the *HP OpenView Select Identity Installation and Configuration Guide*. All installation prerequisites, system requirements, and procedures are explained in detail in this guide. Specific product configuration and logging settings are included. This guide also includes uninstall and troubleshooting information.
- An *HP OpenView Connector Installation Guide* is provided for each resource connector. These are located on the Select Identity Connector CD.
- Detailed procedures for deployment and system management are documented in the *HP OpenView Select Identity Administrator Guide* and Select Identity online help system. This guide provides detailed concepts and procedures for deploying and configuring the Select Identity system. In the online help system, tasks are grouped by the administrative functions that govern them.
- The *HP OpenView Select Identity Workflow Studio Guide* provides detailed information about using Workflow Studio to create workflow templates. It also describes how to create reports that enable managers and approvers to check the status of account activities.
- The *HP OpenView Select Identity External Call Developer Guide* provides detailed information about creating calls to third-party applications. These calls can then be deployed in Select Identity to constrain attribute values or facilitate workflow processes. In addition, JavaDoc is provided for this API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/external_calls/Javadoc` directory on the HP OpenView Select Identity CD.

- If you need to develop connectors, which enable you to connect to external systems for provisioning, refer to the *HP OpenView Select Identity Connector Developer Guide*. This document provides an overview of the Connector API and the steps required to build a connector. The audience of this guide is developers familiar with Java.

  JavaDoc is also provided for the Connector API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/external_calls/Javadoc` directory on the HP OpenView Select Identity CD.

- The *HP OpenView Select Identity Web Service Developer Guide* describes the Web Service, which enables you to programmatically provision users in Select Identity. This guide provides an overview of the operations you can perform through use of the Web Service, including SPML examples for each operation.

  An independent, web-based help system is available for this API. To view this help, double-click the `index.htm` file in the `docs/api_help/web_service/help` directory on the HP OpenView Select Identity CD.

- The *HP OpenView Select Identity Attribute Mapping Utility User's Guide* describes how to access the Attribute Mapping Utility, provides an overview to the utility's user interface, and describes how to define user and entitlements mappings. This guide is provided on the Select Identity Connector CD and is for use with the SQL and SQL Admin connectors only.

2

Deployment Overview

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, you can 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.

Select Identity Deployment Concepts

This chapter provides an overview of the tasks that are necessary to deploy 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 Select Identity 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 will also expedite the process.

Connectors

Select Identity uses J2EE connectors to communicate with the 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 Select Identity reconciles identity information with your system resources. A connector is needed for each resource type in your environment. For example, if your identity information resides in LDAP, Windows, and UNIX systems, you must deploy a connector for each system type.

Deploying and managing system connectors is performed through the Connectors capability and includes the following actions:

- Deploy, delete, and modify connectors
- View connector settings

For more information, see Connectors on page 35.

Resources

Resources in the Select Identity system represent the applications, databases, and directories that Select Identity provisions. 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 be Windows Server Systems or UNIX. After you deploy connectors for each resource type, you can deploy 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 deploy these resources in the Select Identity system, the end user accessing the service has one logical 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 Select Identity creates the bridge to each data store. Select Identity then uses administrative authority to access each user data repository in each resource as each service requires.

Adding and managing system resources is performed through the Resources capability and includes the following actions:

- Deploy, modify, delete resources
- View resources

For more information, see Resources on page 40.

Attributes

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. You can 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 Select Identity attributes are mapped to each resource or data store.

Adding and managing attributes is performed through the Attributes capability and includes the following actions:

- Deploy, modify, and delete attributes
- View attributes

For more information, see Attributes on page 52.

External Calls

When accounts are added to 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. You can 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 *HP OpenView Select Identity External Call Guide*.

After you create external calls required by your business, you can manage them through the External Calls capability, which includes the following actions:

- Deploy, delete, and modify external call settings
- View external call settings

For more information, see External Calls on page 69.

Rules

Reconciliation rules are executed by Select Identity when a new user is added from an Authoritative resource through the Reconciliation capability. 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 another to assign the user to additional services.

Rules are created outside of Select Identity and are uploaded to the system. Managing rules is performed through the Rules capability of the client and includes the following actions:

- Add, modify, and delete rules
- View rules

For more information, see Rules on page 83.

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 capability and includes the following actions:

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

For more information, see Notifications on page 86.

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 184 for more information.

Creating workflow templates is performed through the Workflow Studio capability. For overview information, see Workflow Studio on page 95. 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 Challenge Response Questions on page 98 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 capability 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.

Service Roles

A large part of Service creation involves establishing Service Roles that you want to have with customers and partners. The Service Roles that 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.

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. Service Roles are then assigned to Context groupings.

Context

While Service Roles define the criteria by which users access Services, Context 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.

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

- Create, modify, and delete Services
- Create, modify, and delete Service Views

- Set Service attribute values and properties
- Create, modify, and delete Service Roles
- Create, modify, and delete Context

For more information, see Services on page 101.

Administrative Roles

After you define Services, you can establish the administrative roles that are relevant for each. Administrative roles determine the capabilities and actions that Select Identity administrators can perform within the system.

Select Identity provides basic roles that reflect the capabilities 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 capability and includes the following actions:

- Add, delete, and modify Admin roles
- View Admin roles

For more information, see Administrative Roles on page 126.

Roles are assigned through a user's association with an Admin Service. See Services on page 101 for more information.

Auto Discovery

The Auto Discovery capability enables you to add multiple users to one or more Services. Auto Discovery 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 Auto Discovery on page 135 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 capability to move a group of users from one Service context to another.

See Bulk Add or Move for Accounts on page 148 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 capability 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
- Reset account passwords
- View user account attributes
- Manage user expiration
- Move user to another Service context
- Move all users to another Service context

For more information, see Users on page 163.

Request Status

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

For more information, see Request Status on page 184.

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.

The following configuration and audit reports are available:

- Service Audit Report
- User Audit Report
- User Audit Summary Report
- User Configuration Report
- User Configuration Summary Report
- User Configuration Detail Report

For more information, see Audit and Configuration Reports on page 232.

Reconciliation

You can synchronize Select Identity account data with the data in an authoritative or other system resource. An authoritative source is one that contains the most recent account information, such as a human resources server or email server. Non-authoritative sources may be used to update less important account data. For more information, see Account Reconciliation on page 188.

Configurations

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 capability and includes the following actions:

- Importing configurations
- Exporting configurations

Self Service

After users are established within Select Identity, they can view and update their passwords and challenge response questions. This reduces the number of required actions in areas such as account updates and password management.

User management of accounts is called Self Service in the Select Identity client and includes the following actions:

- Changing passwords and password hints
- Delegating Admin Roles, if an administrator
- View account profile
- Update own account
- View request status that was made by the Admin or the end-user.

For more information, see Account Self Service on page 217.

Sample Deployment Process

There are several ways to deploy your Select Identity system. The following is a suggestion based on previous Select identity deployments. Chapters in this guide refer to when and how you can change the order to better fit your production process.

Logging In to Select Identity

To log in after the server is installed, you must obtain the host name, login ID, password, and port number. The default login account is

User name: **sisa**

Password: **abc123**

Log in to Select Identity by entering the following URL in the web browser:

If WebLogic is the application server:

http://`WebLogic_hostname`:7001/lmz/control/home

Log in to the system with this account information and create a new Select Identity system administrator based on your company's security policies, and delete the `sisa` account. This account belongs to the System Administrator role. See Select Identity Default Roles on page 131 for actions.

Deployment Steps

The following is a sample deployment process. Though steps can be performed in a different order, certain steps are prerequisites for others. For example, you cannot deploy a resource without deploying a connector for that resource.

1. Log in to the system as the Select Identity system administrator.
2. Open **Connectors** and deploy any connectors that you require for resources to communicate with Select Identity.
3. Open **Resources** and create a resource for each of the systems on which Select Identity will rely for user identity information.
4. Open **Attributes** and define the identity attributes that will determine how accounts are grouped and managed.
5. Open **External Calls** and deploy any programs that you want to call third-party applications during the account approval process.
6. Open **Rules** and deploy rules when you want to programmatically assign new users to a Service based on some qualifying criteria during the reconciliation process.
7. Open **Notifications** and create the templates that the system will use to notify users and administrators when a system event occurs, such as the addition or removal of an account.

8. Open **Workflow Studio** and create templates to define the process by which user accounts are provisioned.
9. Open **Challenge/Response** and define the questions and hints that users can answer to reset their passwords.
10. Open **Services** and create all of the Services, Service Roles, and Context that you plan to offer customers and partners.
11. Open **Admin Roles** and create the administrative roles that will govern your Services.

After completing these tasks, you can add users or enable users to request registration with the system. You can also use the **Auto Discovery** process to add groups of users at one time. You can also use the **Bulk** process to add users or move them from one Service context to another.

After users are established within Select Identity, they can view and update portions of their identity profiles with the **Self Service** pages.

Use the **Approvals** and **Request Status** pages to manage and monitor the addition of accounts to the Select Identity system.

Use **Configurations** to import or export Select Identity configurations from test to production environments.

Audit and **Configuration Reports** can be run at any time to view system configuration and account activity.

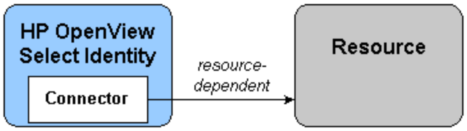
3

Connectors

HP OpenView 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 Select Identity to access a resource is called a **connector**. The connector acts as a gateway between Select Identity and the resource.

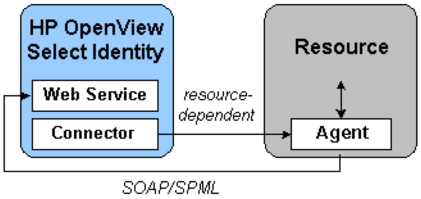
Select Identity supports two types of connectors:

- 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:

  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.

- A two-way connector contains the connector that resides on the Select Identity 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.



The connector must issue a request according to the resource’s specifications. When the agent issues a request to Select Identity’s web service, it must do so through the SOAP protocol with an 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, you must build a resource adapter using the J2EE 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 API to be used in conjunction with JCA to create connectors. After you build the connector, you can install it on the Select Identity server, which enables you to deploy it and create resources in the Select Identity client. Each connector is delivered with an installation guide that contains information about associated connector files and attribute mapping files.

The *HP OpenView Select Identity Connector Guide* provides details about writing code for a connector, 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. Refer to Product Documentation on page 21 for details on accessing the documentation.

Managing Connectors

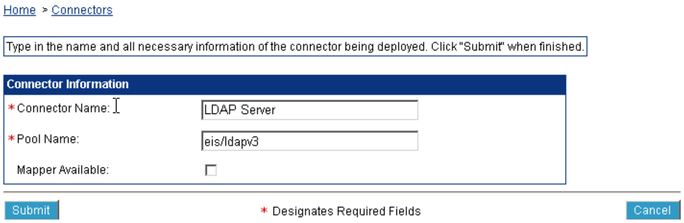
After you create a connector, you can deploy it through the Select Identity Connector pages. You will need one connector for each resource type that you want to support. For example, if you want to connect to three LDAP servers, only one LDAP connector is installed and deployed.

Before connectors can be managed through the Connector pages, the *connector*.rar file must be deployed on the Select Identity application server. See the *HP OpenView Connector Installation Guide*, which is included on the Select Identity Connector CD.

Deploying a Connector

Perform the following to deploy a new connector:

1 From the home page of Connectors, click **Deploy New Connector**. The Connector Information page displays.



Home > Connectors

Type in the name and all necessary information of the connector being deployed. Click "Submit" when finished.

Connector Information

*Connector Name: LDAP Server

*Pool Name: eis/ldapv3

Mapper Available: □

* Designates Required Fields

2 Enter a unique name for this connector in the Connector Name field.

3 Enter the JNDI name for the connector in the Pool Name field. It is always eis/*connector_name*. This JNDI name is specified during the creation of the connector.

4 If you are deploying an SQL Server, Oracle or Sybase connector, you can click the **Mapper Available** check box to access the Attribute Mapper utility. This utility enables you to map user and entitlement attributes to Select Identity attributes. For details on how to use the Attribute Mapper utility, see the *HP OpenView Select Identity Attribute Mapping Utility User's Guide*.

5 Click **Submit**.

The connector is deployed by the system.

Modifying a Connector

If your connector configuration changes, you can update the deployment information.

Perform the following steps to modify a connector:

1. From the home page of Connectors, select a connector from the Connectors drop-down list.
2. Select **Modify Connector** from the Actions drop-down list.
3. Click **Submit**. The Connector Information page displays.
4. You can modify the Pool Name.
5. If you are modifying an SQL Server, Oracle or Sybase connector, you can click the **Mapper Available** check box to access the Attribute Mapper utility to modify any of the mapped user and entitlement attributes. For details on how to use the Attribute Mapper utility, see the *HP OpenView Select Identity Attribute Mapping Utility User's Guide*.
6. When finished, click **Submit**.

Viewing a Connector

You can view resource connectors configured for your system.

Perform the following steps to view a connector:

1. From the home page of Connectors, select a connector from the Connectors drop-down list.
2. Select **View Connector** from the Actions drop-down list.
3. Click **Submit**. The Connector Information page displays.

Deleting a Connector

You can delete a connector from the Select Identity system. Make sure to remove any resource and Service dependencies before deleting the connector.

Perform the following steps to delete a connector:

1. From the home page of Connectors, select a connector from the Connectors drop-down list.
2. Select **Delete Connector** from the Actions drop-down list.
3. Click **Submit**.

   You are prompted to confirm the action. Click **OK** to delete the connector.

4

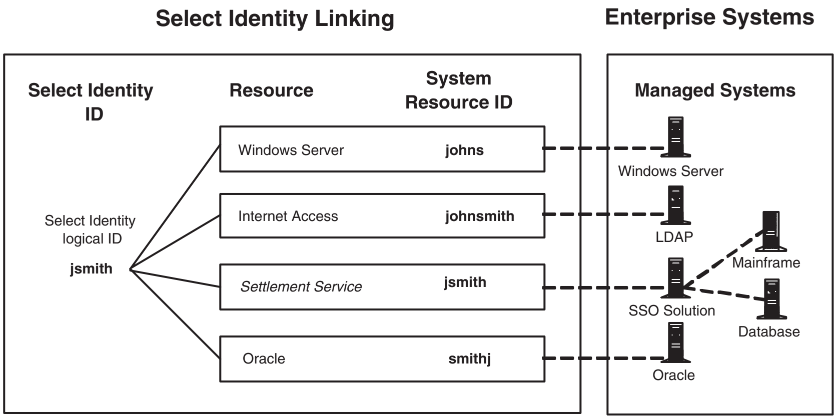
Resources

Resources in the HP OpenView 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, you can deploy, view, 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.

Figure 2 Select Identity 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.

Authoritative Sources

The Authoritative Source setting enables you to establish a resource that is used as the baseline for all accounts within the Select Identity system. For example, your human resources server may contain all of your company's most current identity profile information. If so, you can add this server as a resource and delegate it as an Authoritative Source for user information.

An authoritative resource implies that all the attributes in the resource are also authoritative. However you may mark individual attributes of a non-authoritative resource as authoritative. If an attribute marked as authoritative in a non-authoritative resource also exists in an authoritative resource, changes to that attribute's value in either resource are propagated to all resources in the system.

Once a system is defined as an Authoritative Source, you can add a rule that detects changes within that resource and propagates them to Select Identity. See Rules on page 83 for more information about using rules in Select Identity.

Another advantage of defining an Authoritative Source is that it can be used to add user accounts to the Select Identity system during initial deployment. You can also add accounts from an Authoritative Source after the system is in production.

You can compare resource information to a non-Authoritative Source, but you cannot add accounts from one. See Account Reconciliation on page 188 for information about Reconciliation.

Adding and Managing System Resources

Select Identity is installed with each of the resource connections that 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 SDK. Connectors can be deployed and managed through the Connectors section of the client. See Connectors on page 35 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 Select Identity 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.

Deploying a Resource

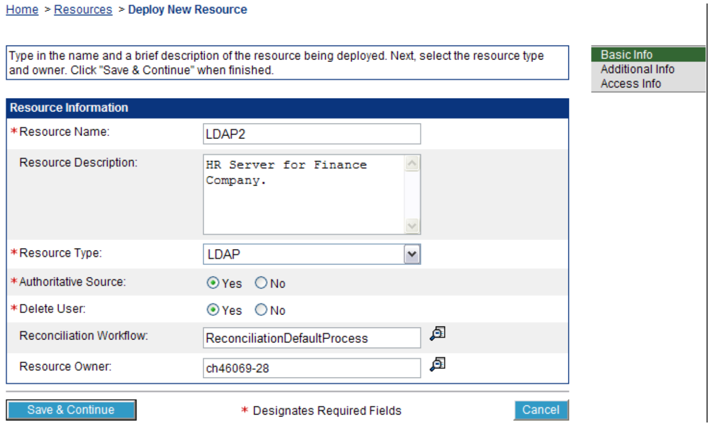
You need to deploy a resource for each system on which users have accounts that relate to the Services you provide. The following procedures use an LDAP system as a resource example.

The information that you will enter 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.

Perform the following steps to deploy a resource:

1. From the home page of Resources, click **Deploy New Resource**.

   The Resource Information page displays.



Type in the name and a brief description of the resource being deployed. Next, select the resource type and owner. Click "Save & Continue" when finished.

Resource Information

*Resource Name:	LDAP2
Resource Description:	HR Server for Finance Company.
*Resource Type:	LDAP
*Authoritative Source:	● Yes ○ No
*Delete User:	● Yes ○ No
Reconciliation Workflow:	ReconciliationDefaultProcess
Resource Owner:	ch46069-28

* Designates Required Fields

2. Enter a name for this resource in the Resource Name field.
3. If you choose, you can add a description for this application in the Resource Description text box.
4. Select a system type from the Resource Type drop-down list. This determines the connector used to access the resource.

5 If this resource provides the most current user data in your environment, select **Yes** from the Authoritative Source options. Select Identity can then rely on this resource to synchronize account data.

> If you make this resource authoritative, the attributes that are mapped to this resource are also authoritative. When attribute data is reconciled, the values for these attributes take precedence over other resource attributes. See Attributes on page 52 for more information about attributes.

6 If you want to delete users from this resource when they are deleted from an associated Service, select **Yes** from the Delete user options.

7 To define a workflow template to be used for reconciliation by resource instead of service, click 🔍 to search for and select a workflow template to assign to this process. See Account Reconciliation on page 188 for more information about the reconciliation process.

Workflow templates define the process by which requests are managed in Select Identity. Select Identity provides several default templates. You can also create templates that are specific to your business needs through the Workflow Studio pages.

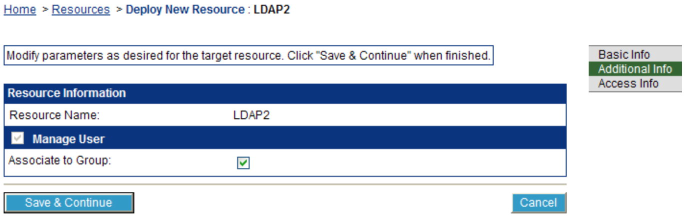
See the *HP OpenView Select Identity Workflow Studio Guide* for an explanation of the default templates and template creation procedures.

8 If there is a resource owner, click 🔍 to search for and select an owner for this resource.

Resource Owner is an informational field to indicate which Select Identity user may be contacted if there is a question about the resource, such as when the resource is down.

9 Click **Save & Continue** to proceed.

The Additional Information page displays.



Home > Resources > Deploy New Resource : LDAP2

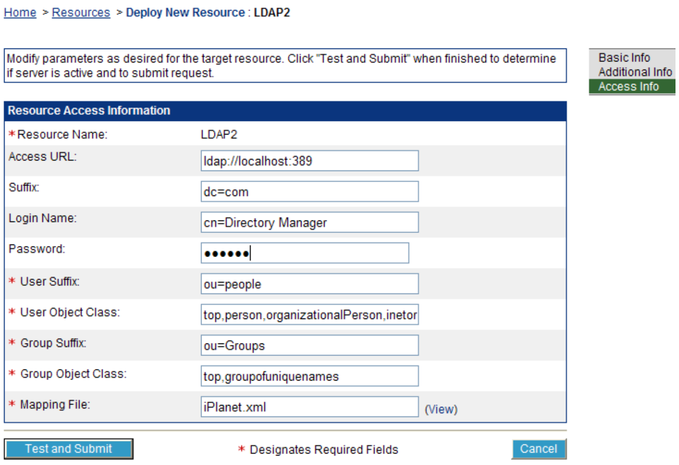
Modify parameters as desired for the target resource. Click "Save & Continue" when finished.

Resource Information	
Resource Name:	LDAP2
☑ Manage User	
Associate to Group:	☑

10 You may be asked to associate this resource with a Manage User, if the system uses the concept of entitlements. Select the check box to create the association.

11 Click **Save & Continue** to proceed.

The Resource Access Information page displays.



Home > Resources > Deploy New Resource : LDAP2

Modify parameters as desired for the target resource. Click "Test and Submit" when finished to determine if server is active and to submit request.

Resource Access Information	
*Resource Name:	LDAP2
Access URL:	ldap://localhost:389
Suffix:	dc=com
Login Name:	cn=Directory Manager
Password:	••••••
* User Suffix:	ou=people
* User Object Class:	top,person,organizationalPerson,inetor
* Group Suffix:	ou=Groups
* Group Object Class:	top,groupofuniquenames
* Mapping File:	iPlanet.xml (View)

* Designates Required Fields

12 Based on the application type that you selected in Step 4, you will be asked to provide the information required to connect to this system, such as machine name and URL. You can also view the mapping file that Select Identity uses to map attributes to this resource.

Enter your system connection information. See the *HP OpenView Connector Installation Guide* for examples.

13 Click **Test and Submit**. Select Identity verifies the connection and adds the new resource to the system.

If the resource deployment fails 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.

Modifying a Resource

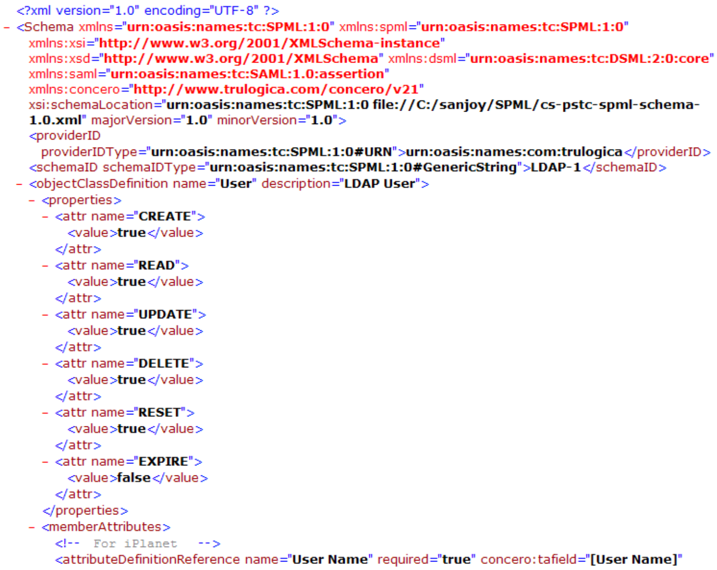
You can modify the system resources on which your products and Services rely. You may need to modify a resource in the following cases:

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

Perform the following steps to modify a resource:

1. From the home page of Resources, select the resource that you want to modify from the Resources drop-down list.
2. Select **Modify Resource** from the Actions drop-down list.
3. Click **Submit**. The Resource Information page displays.
4. You can modify all but the resource name and type.
5. Click **Save & Continue**. The Additional Information page displays.
6. Select or clear the Associate to Group check box.
7. Click **Save & Continue**. The Access Information page displays.
8. If your access to this system changed, you can edit the appropriate fields.
9. If you want to view the mapping file for this resource, click **View** next to the Mapping File field.

The XML file displays.



```
   <?xml version="1.0" encoding="UTF-8" ?>
 - <Schema xmlns="urn:oasis:names:tc:SPML:1:0" xmlns:spml="urn:oasis:names:tc:SPML:1:0"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
     xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
     xmlns:concero="http://www.trulogica.com/concero/v21"
     xsi:schemaLocation="urn:oasis:names:tc:SPML:1:0 file://C:/sanjoy/SPML/cs-pstc-spml-schema-
     1.0.xml" majorVersion="1.0" minorVersion="1.0">
     <providerID
       providerIDType="urn:oasis:names:tc:SPML:1:0#URN">urn:oasis:names:com:trulogica</providerID>
     <schemaID schemaIDType="urn:oasis:names:tc:SPML:1:0#GenericString">LDAP-1</schemaID>
   - <objectClassDefinition name="User" description="LDAP User">
     - <properties>
       - <attr name="CREATE">
           <value>true</value>
         </attr>
       - <attr name="READ">
           <value>true</value>
         </attr>
       - <attr name="UPDATE">
           <value>true</value>
         </attr>
       - <attr name="DELETE">
           <value>true</value>
         </attr>
       - <attr name="RESET">
           <value>true</value>
         </attr>
       - <attr name="EXPIRE">
           <value>false</value>
         </attr>
       </properties>
     - <memberAttributes>
         <!--  For iPlanet   -->
         <attributeDefinitionReference name="User Name" required="true" concero:tafield="[User Name]"
```

10 Click **Test and Submit.**

Select Identity verifies the connection and updates the resource.

Viewing a Resource

You can view system information for resources on which Select Identity and your Services rely.

Perform the following steps to view a system resource:

1. From the home page of Resources, select the resource that you want to view from the Resources drop-down list.
2. Select **View Resource** from the Actions drop-down list.
3. Click **Submit**.

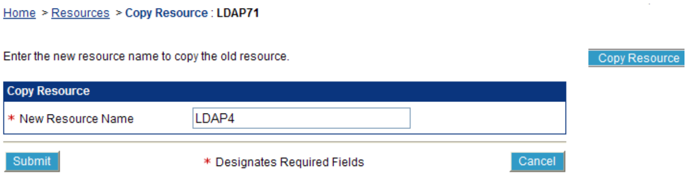
   You can view all configuration information by clicking the available links on the right.

Copying a Resource

If you have multiple, similar resources to add, you can copy an existing resource. All of the connection and configuration information is copied. You can later modify specific fields.

Perform the following steps to copy a system resource:

1. From the home page of Resources, select the resource that you want to copy from the Resources drop-down list.
2. Select **Copy Resource** from the Actions drop-down list.
3. Click **Submit**. The Copy Resource page displays.



Home > Resources > Copy Resource : LDAP71

Enter the new resource name to copy the old resource.

Copy Resource

* New Resource Name: LDAP4

* Designates Required Fields

4. Enter a unique name for this resource in the New Resource Name field.
5. Click **Submit**. The resource is copied.

Deleting a Resource

You can delete a system resource from Select Identity if your Services no longer require access to it.

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

Perform the following steps to delete a resource:

1. From the home page of Resources, select the resource that you want to delete from the Resources drop-down list.
2. Select **Delete Resource** from the Actions drop-down list.
3. Click **Submit**.

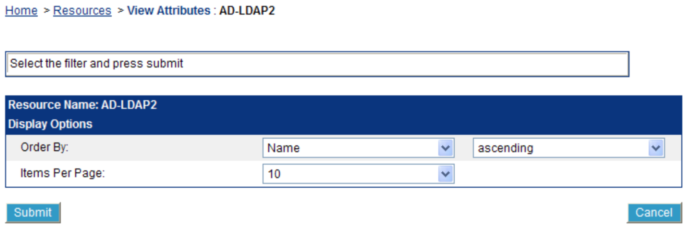
   You are prompted to confirm the action. Click **OK** to delete the resource.

Viewing Resource Attributes

You can view the attributes that are used to provision user information for a given resource.

Perform the following steps to view resource attributes:

1. From the home page of Resources, select a resource from the Resources drop-down list.
2. Select **View Attributes** from the Actions drop-down list.
3. Click **Submit**. The Display Options page displays.



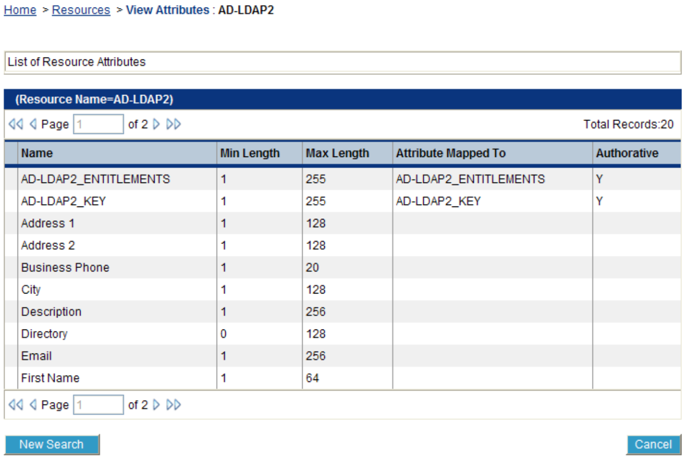
Home > Resources > View Attributes : AD-LDAP2

Select the filter and press submit

Resource Name: AD-LDAP2
Display Options

Order By: Name ascending
Items Per Page: 10

4. Choose the Order By and Items Per Page options that you want.
5. Click **Submit**. The List of Resource Attributes displays.


Home > Resources > View Attributes : AD-LDAP2
List of Resource Attributes
(Resource Name=AD-LDAP2)
Page 1 of 2
Total Records:20
New Search
Cancel

Name	Min Length	Max Length	Attribute Mapped To	Authorative
AD-LDAP2_ENTITLEMENTS	1	255	AD-LDAP2_ENTITLEMENTS	Y
AD-LDAP2_KEY	1	255	AD-LDAP2_KEY	Y
Address 1	1	128		
Address 2	1	128		
Business Phone	1	20		
City	1	128		
Description	1	256		
Directory	0	128		
Email	1	256		
First Name	1	64		

6 You can page through the results to view details for each attribute, such as value constraints, Select Identity mapping, and whether or not the attribute is considered authoritative. See Authoritative Sources on page 41 for more information.

7 You can click **New Search** to change display criteria, or click **Cancel** to return to the Resources home page.

Modifying Resource Attribute Mapping

You can modify the way that attributes are mapped between Select Identity and system resources. Attributes are mapped to enable synchronization and account updates.

See Adding and Mapping an Attribute on page 57 for information on creating and mapping attributes in Select Identity.

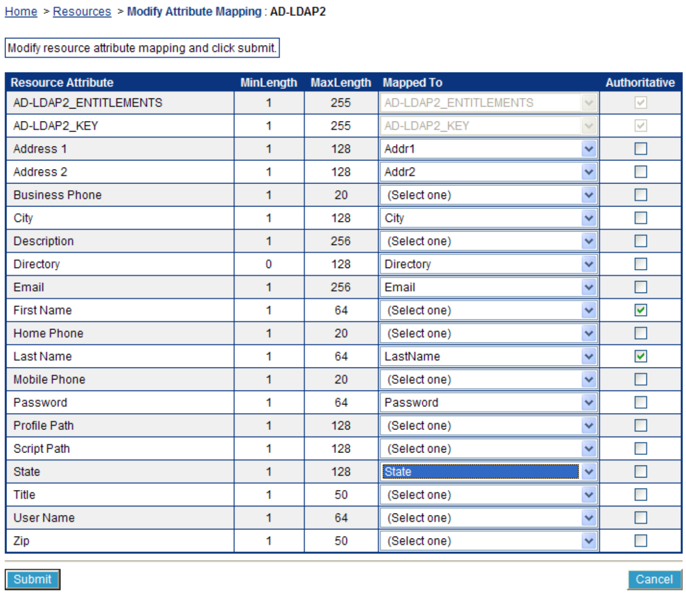
Perform the following to modify attribute mappings:

1 From the home page of Resources, select a resource from the Resources drop-down list.

2 Select **Modify Attribute Mapping** from the Actions drop-down list.

3 Click **Submit**.

The Attribute Mapping page displays.



Home > Resources > Modify Attribute Mapping : AD-LDAP2

Modify resource attribute mapping and click submit.

Resource Attribute	MinLength	MaxLength	Mapped To	Authoritative
AD-LDAP2_ENTITLEMENTS	1	255	AD-LDAP2_ENTITLEMENTS	☑
AD-LDAP2_KEY	1	255	AD-LDAP2_KEY	☑
Address 1	1	128	Addr1	□
Address 2	1	128	Addr2	□
Business Phone	1	20	(Select one)	□
City	1	128	City	□
Description	1	256	(Select one)	□
Directory	0	128	Directory	□
Email	1	256	Email	□
First Name	1	64	(Select one)	☑
Home Phone	1	20	(Select one)	□
Last Name	1	64	LastName	☑
Mobile Phone	1	20	(Select one)	□
Password	1	64	Password	□
Profile Path	1	128	(Select one)	□
Script Path	1	128	(Select one)	□
State	1	128	State	□
Title	1	50	(Select one)	□
User Name	1	64	(Select one)	□
Zip	1	50	(Select one)	□

4 Select the attribute that you want to map from the Mapped To drop-down list.

5 If you want to make this attribute authoritative, click the Authoritative check box.

Making an attribute authoritative ensures that it takes precedence over others when accounts are moved or synchronized.

6 Click **Submit** when finished.

5

Attributes

HP OpenView Select Identity enables you to define the way in which user identities are managed and stored. Each user profile can contain any number of attributes, such as username, first name, last name, and email address. The resources that you deployed contain their own resource attributes based on the operating system or application group's information. Select Identity relies on attributes defined for each resource and resource attributes defined through the Attributes pages to enable access to Services and provision accounts.

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 following is a sample:

```
- <memberAttributes>
- <!--
 For iPlanet
-->
<attributeDefinitionReference name="UserName" required="true" con-
cero:tafield="[UserName]" concero:resfield="uid" concero:is-
Key="true" concero:init="true" />
   <attributeDefinitionReference name="Password" required="false"
   concero:tafield="[Password]" concero:resfield="userpassword"
   concero:init="true" />
```

You can create attributes that are specific to Select Identity through the Attributes pages. These attributes can be used to associate Select Identity user accounts with system resources by mapping them to the connector mapping file. This process becomes necessary because a single attribute “username” can have a different definition on three different resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server.

You also can create attributes that you do not map to a resource. 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 Service Attributes on page 109 for details):

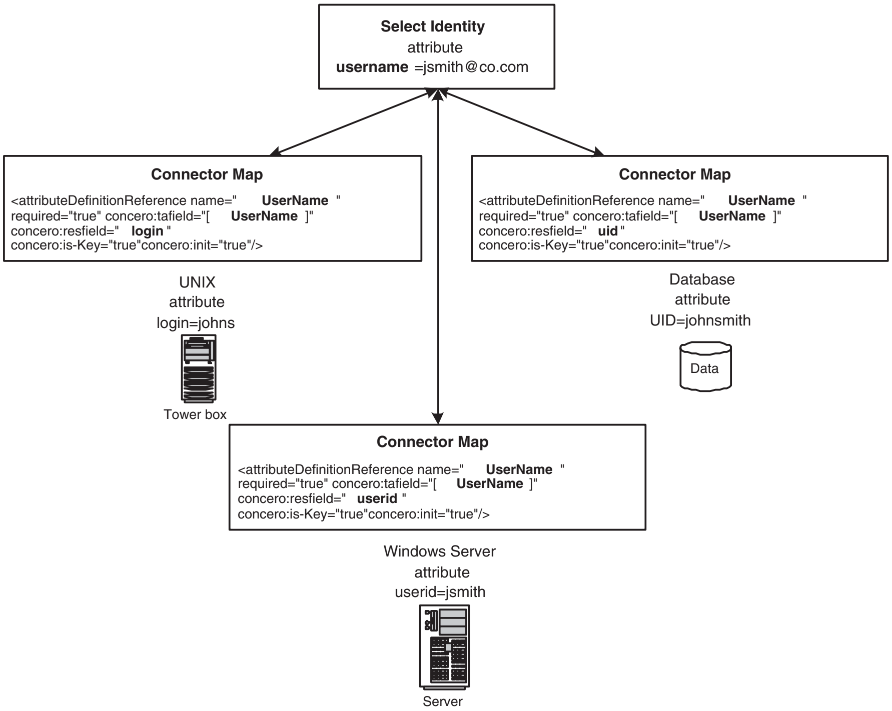
UserName
FirstName
LastName
Email
Password

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 3 Attribute Mapping Example



```
<attributeDefinitionReference name="   UserName  "
required="true" concero:tafield="[   UserName  ]"
concero:resfield="   login "
concero:is-Key="true"concero:init="true"/>
```

```
<attributeDefinitionReference name="   UserName  "
required="true" concero:tafield="[   UserName  ]"
concero:resfield="   uid "
concero:is-Key="true"concero:init="true"/>
```

```
<attributeDefinitionReference name="   UserName  "
required="true" concero:tafield="[   UserName  ]"
concero:resfield="   userid "
concero:is-Key="true"concero:init="true"/>
```

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 resources, regardless of how the attribute is defined on the resource.

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

When defining attributes, you can 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*.

Authoritative Attributes

Just as you can make a resource an authoritative source for user data, you can define specific attributes as authoritative as well. Changes to an authoritative attribute take precedence over non-authoritative attributes.

An authoritative resource implies that all the attributes in the resource are authoritative. However you can mark individual attributes of a non-authoritative resource as authoritative. If an attribute marked as authortiative in a non-authoritative resource also exists in an authoritative resource, changes to that attribute's value in either resource are propagated to all resources in the system.

Managing Multiple Passwords

Select Identity manages and synchronizes multiple passwords used throughout an enterprise. Typically, legacy systems, client-server, and newer technology systems are managed by different IT staffs and require different password formats, strengths, and policy. Select Identity uses the Attributes function to manage all password specifications. An administrator 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 Select Identity, which can be pushed to the resource during account creation and reset activities.

Select Identity has one default password attribute called *password*. This attribute cannot be removed as it is used for Select Identity system authentication. This attribute can be used to push the same password to any number of resources, thus synchronizing Select Identity with the resources.

Multiple password attributes can be created to address differing password policies and requirements. Each password attribute must have a unique text name and contain a unique password policy, such as minimum and maximum characters allowed during registration, or whether the password should be auto-generated to meet a corporate standard.

Once a password attribute is used to provision a user with Select Identity, that password is tracked by Select Identity for the life of the user's existence in the system. 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 attributes to resources can be 1:1 or 1: many.

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 certain attributes on which you want to search, you can perform the following:

- Identify the key attributes, such as SSN, EmployeeId, or email. You will need to make sure that these are defined within Select Identity and within the mapping file used for each system resource in which data is stored.
- Add corresponding columns to the `TAUser` table in the database.
- Add entries in the `TruAccess.properties` file.

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

Adding and Mapping an Attribute

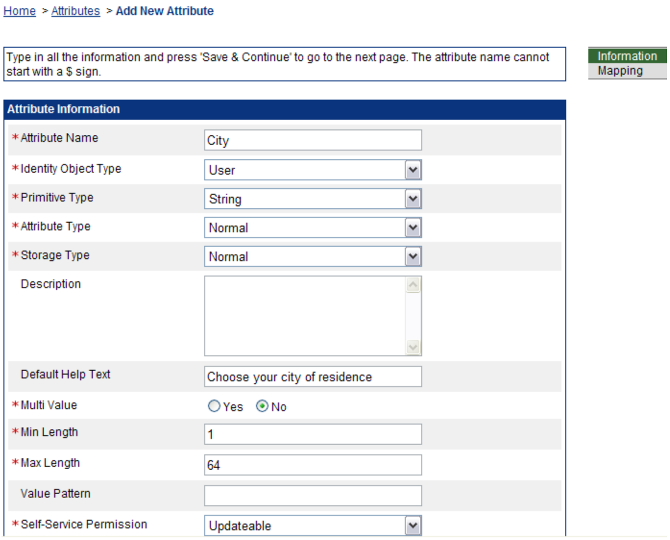
You can add any number of attributes to manage identity information. The attribute can then be mapped to resource attributes during account addition and updates.

When adding a user in Select Identity, 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.

Perform the following steps to add and map an attribute:

1 From the home page of Attributes, click **Add New Attribute**.

The Attribute Information page displays. The following is the first half of the page.



Home > Attributes > Add New Attribute

Type in all the information and press 'Save & Continue' to go to the next page. The attribute name cannot start with a $ sign.

Attribute Information

*Attribute Name	City
*Identity Object Type	User
*Primitive Type	String
*Attribute Type	Normal
*Storage Type	Normal
Description	
Default Help Text	Choose your city of residence
*Multi Value	○ Yes ● No
*Min Length	1
*Max Length	64
Value Pattern	
*Self-Service Permission	Updateable

2 Enter a name for the attribute in the Attribute Name field.

3 Choose the object type for this attribute from the Identity Object Type drop-down list. Choose **User** if the attribute will define user profile information.

4. Choose the type of value that you want the attribute to have from the Primitive Type drop-down menu. Choices include **String** and **Date**.

5. Choose the attribute type. Choices are **Password** for those attributes that define password requirements, and **Normal** for all others.

   If you choose the **Password** attribute type, the storage type option must be **OneWay**.

6. Choose the storage type for the attribute from the Storage Type drop-down menu. 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.

7. If you choose, you can enter a description for the attribute in the Description text box.

8. Enter text to help the user understand what is required from this field in the Default Help text box.

9. If this attribute can have multiple values, Select the **Yes** Multi Value option.

10. Enter a minimum length for the attribute value in the Min Length field.

11. Enter a maximum length for the attribute value in the Max Length field.

12. You can enter a regular expression for the attribute value in the Value Pattern field. Select Identity supports the Jakarta style of regular expressions. The following is an email example:

    ```
    ^([a-zA-Z]+)([a-zA-Z0-9_'\\.|\\-])*@((([a-zA-Z]+)\.))*([a-zA-Z]
    {2,4})$
    ```

13. Self-Service Permission allows an Administrator to set the permission of the field or attribute which determines how the field appears on the form in Self Service. Following are the settings that affect what a user can do when view profile or modify profile is performed from self-service:

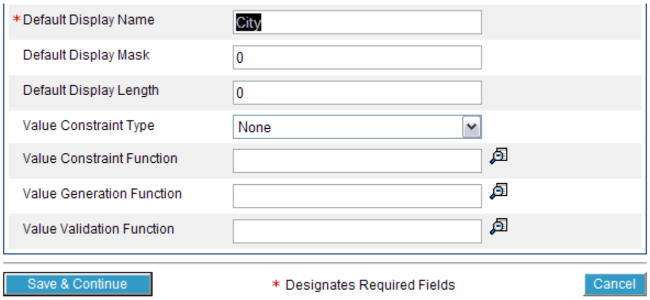
    Hidden — Ensures the attribute cannot be seen when a user performs a view or modify profile in Self Service.

    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.

The following is the second half of the page.



*Default Display Name	City	
Default Display Mask	0	
Default Display Length	0	
Value Constraint Type	None	
Value Constraint Function		🔍
Value Generation Function		🔍
Value Validation Function		🔍

14 Enter the Default Display Name for the attribute. This is the name that users see when registering for a Service.

15 If you want to mask a portion or all of the attribute’s value when entered, enter a number in the Default Display Mask field. You can use this option to mask password entries.

16 Enter the number of characters that you want displayed for the attribute value in the Default Display Length field.

17 Choose a type from the Value Constraint Type drop-down list.

None enables a user to enter a value.

Specified enables you to specify values that a user can select for this attribute. If you choose this option, an additional page is displayed enabling you to specify name and value pairs.

Dynamic specifies a search for values through the use of an external call.

18 If you want to call a function to constrain the value of the attribute, click 🔍 to search for and specify the program. Programs are registered through the External Calls capability.

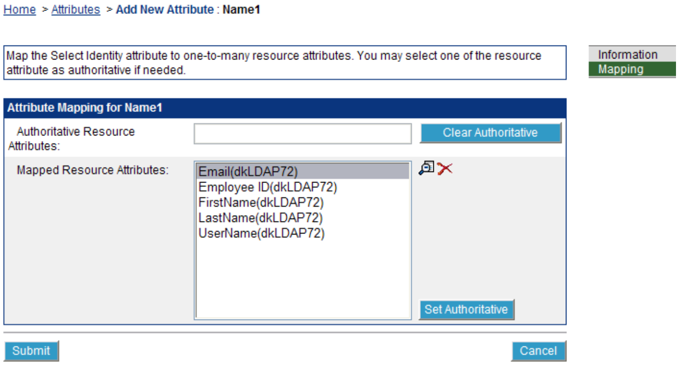
If you specified **Dynamic** for the Value Constraint Type, you must choose a program to search for a value. An additional page displays enabling you to specify arguments.

19 If you want to call a function to generate the value of the attribute, click 🔍 next to the Value Generation function to search for and specify the function.

20 If you want to call a program to validate the value of the attribute, click 🔍 to search for and specify the program.

21 Click **Save & Continue** to proceed.

The Attribute Mapping page displays.



Home > Attributes > **Add New Attribute** : **Name1**

Map the Select Identity attribute to one-to-many resource attributes. You may select one of the resource attribute as authoritative if needed.

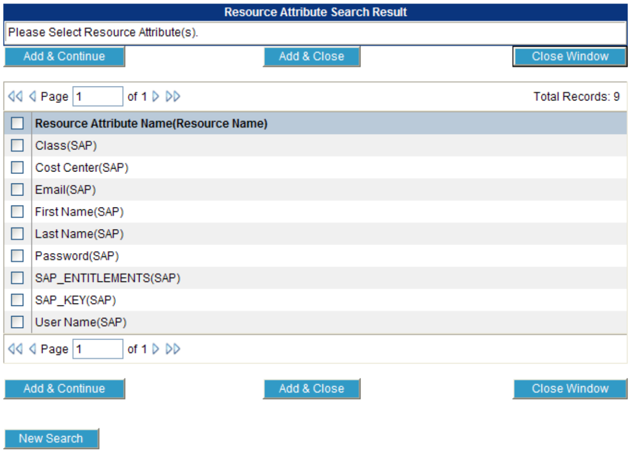
Attribute Mapping for Name1

Authoritative Resource Attributes:		Clear Authoritative

Mapped Resource Attributes:	Email(dkLDAP72)
	Employee ID(dkLDAP72)
	FirstName(dkLDAP72)
	LastName(dkLDAP72)
	UserName(dkLDAP72)
		Set Authoritative

22 Click 🔍 to search for the resource and attributes that you want to map.

After you locate the resource, the available attributes are listed.



Resource Attribute Search Result

Please Select Resource Attribute(s).

Page 1 of 1 Total Records: 9

□	Resource Attribute Name(Resource Name)
□	Class(SAP)
□	Cost Center(SAP)
□	Email(SAP)
□	First Name(SAP)
□	Last Name(SAP)
□	Password(SAP)
□	SAP_ENTITLEMENTS(SAP)
□	SAP_KEY(SAP)
□	User Name(SAP)

Page 1 of 1

23 Choose the attribute or attributes that you want to map and click **Add & Continue** to choose more options or **Add & Close** to add your choices and close the window. When you are finished click **Close Window**.

The Attribute Mapping page displays.

To remove attributes from the Mapped Resource Attributes list, select the attribute and click the trash icon.

24 If you want an attribute mapped to the authoritative resource, select it and click **Set Authoritative**. The attribute is mapped to the resource that you define as the authoritative source. See Authoritative Sources on page 41 for more information.

25 When finished, click **Submit**.

You can modify the mapping of attributes through the Resources pages. See Modifying Resource Attribute Mapping on page 50 for more information.

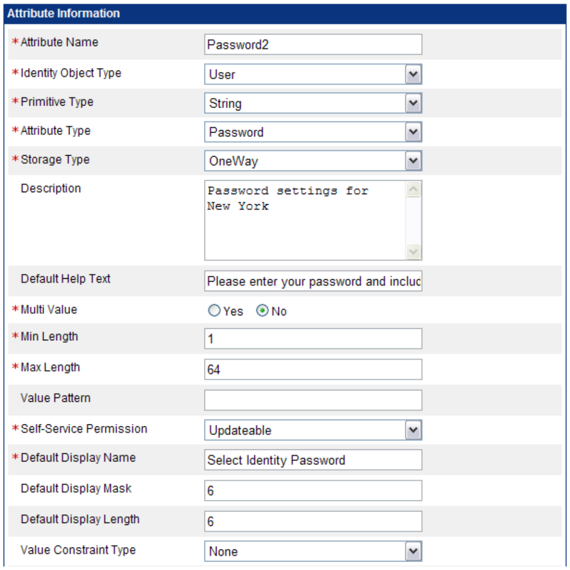
Creating a Password Attribute

You can create a password attribute that determines the policy and characteristics of Select Identity passwords. Password attributes require one-way storage.

Perform the following to create a password attribute:

1 From the home page of Attributes, click **Add New Attribute**.

The Attribute Information page displays.



Attribute Information

*Attribute Name	Password2
*Identity Object Type	User
*Primitive Type	String
*Attribute Type	Password
*Storage Type	OneWay
Description	Password settings for New York
Default Help Text	Please enter your password and incluc
*Multi Value	○ Yes ● No
*Min Length	1
*Max Length	64
Value Pattern	
*Self-Service Permission	Updateable
*Default Display Name	Select Identity Password
Default Display Mask	6
Default Display Length	6
Value Constraint Type	None

2 Enter a name for the attribute in the Attribute Name field.

3 Choose the object type for this attribute from the Identity Object Type drop-down list. Choose **User** if the attribute will define user profile information.

4 Choose the type of value that you want the attribute to have from the Primitive Type drop-down menu. Choices include **String** and **Date**.

5 Choose the **Password** attribute type.

6 Choose the **OneWay** storage type for the attribute from the Storage Type drop-down menu. The password is only stored with one-way encryption.

7 If you choose, you can enter a description for the attribute in the Description text box.

8 Enter text to help the user understand what is required from this field in the Default Help text box.

9 Typical passwords are single-value entries. Select the **No** Multi Value option.

10 Enter a minimum length for the attribute value in the Min Length field.

11 Enter a maximum length for the attribute value in the Max Length field.

12 You can enter a regular expression for the attribute value in the Value Pattern field. Select Identity supports the Jakarta style of regular expressions.

13 Self-Service Permission allows an Administrator to set the permission of the field or attribute which determines how the field appears on the form in Self Service. Following are the settings that affect what a user can do when view profile or modify profile is performed from self-service:

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.

14 Enter the Default Display Name for the attribute. This is the name that users see when registering for a Service.

15 If you want to mask a portion or all of the attribute's value when entered, enter a number in the Default Display Mask field. The masked characters are applied from the beginning of the line. You can use this option to mask any attribute such as password, Social Security number, credit card number, and so on.

➤ If you want to modify the attribute and set the Default Display Mask, see Modifying an Attribute on page 67 for instructions.

16 Enter the number of characters that you want displayed for the attribute value in the Default Display Length field.

17 Choose a type from the Value Constraint Type drop-down list.

None enables a user to enter a value.

Specified enables you to specify values that a user can select for this attribute. If you choose this option, an additional page is displayed enabling you to specify name and value pairs.

Dynamic specifies a search for values through the use of an external call.

18 If you want to call a function to constrain the value of the attribute, click 🔍 to search for and specify the program. Programs are registered through the External Calls capability.

If you specified **Dynamic** for the Value Constraint Type, you must choose a program to search for a value. An additional page displays enabling you to specify arguments.

19 If you want to call a function to generate the value of the attribute, click 🔍 next to the Value Generation function to search for and specify the function.

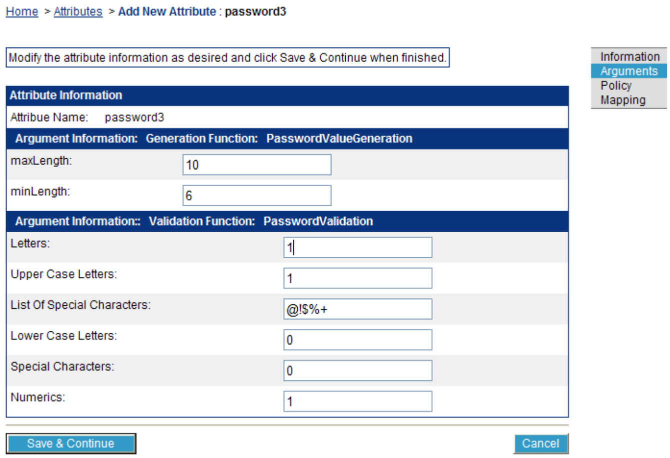
If you want the system to automatically generate password values, select the **PasswordValueGeneration** function.

20 If you want to call a program to validate the value of the attribute, click 🔍 to search for and specify the program.

If you want the system to validate password values, select the **PasswordValidation** function.

21 Click **Save & Continue** to proceed.

If you selected the password generation and validation functions, the Arguments page displays.



Home > Attributes > **Add New Attribute** : **password3**

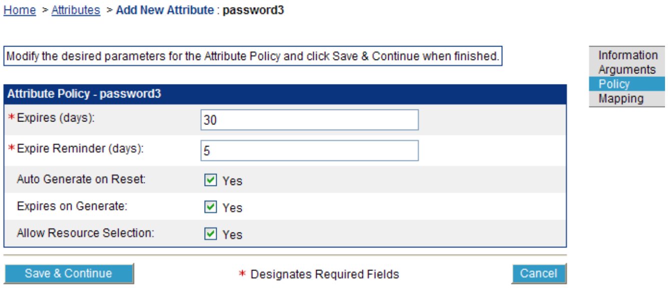
Modify the attribute information as desired and click Save & Continue when finished.

Attribute Information	
Attribue Name: password3	
Argument Information: Generation Function: PasswordValueGeneration	
maxLength:	10
minLength:	6
Argument Information:: Validation Function: PasswordValidation	
Letters:	1
Upper Case Letters:	1
List Of Special Characters:	@!$%+
Lower Case Letters:	0
Special Characters:	0
Numerics:	1

22 If you selected the **PasswordValueGeneration** function, enter the maximum and minimum length of the password value.

23 If you selected the **PasswordValidation** function, Enter the characteristics that you want to define the password value.

24 Click **Save & Continue**. The Attribute Policy page displays.



Modify the desired parameters for the Attribute Policy and click Save & Continue when finished.

Attribute Policy - password3

* Expires (days):	30
* Expire Reminder (days):	5
Auto Generate on Reset:	☑ Yes
Expires on Generate:	☑ Yes
Allow Resource Selection:	☑ Yes

* Designates Required Fields

25 Enter an expiration value in days in the Expires field.

26 Enter a reminder value in days in the Expire Reminder field.

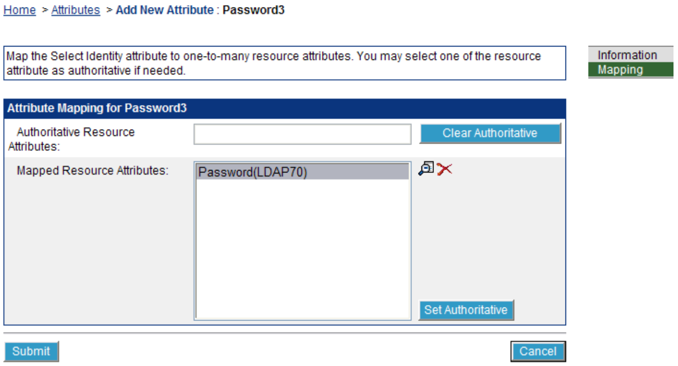
27 If you want the system to automatically generate a password when a password reset is requested, select the Auto Generate on Reset check box.

28 If you want the old password on the resource to expire when a new one is generated, click the Expires on Generate check box.

29 If you want the user to be able to choose the resources that will be updated with the new password, click the Allow Resource Selection check box.

> The options provided by the **PasswordValueGeneration** function may not apply to all connectors and resources. You can create your own function and upload it through External Calls to ensure that the options that you need for each connector apply.

30 Click **Save & Continue**. The Attribute Mapping page displays.



Home > Attributes > Add New Attribute : Password3

Map the Select Identity attribute to one-to-many resource attributes. You may select one of the resource attribute as authoritative if needed.

Attribute Mapping for Password3

Authoritative Resource Attributes:

Mapped Resource Attributes: Password(LDAP70)

31 If you want to map this attribute to an attribute in an existing resource, click 🔍 to select the resource and choose the attribute or attributes that you want to map.

32 Click **Submit**. The attribute is saved.

See Changing Passwords on page 218 for details on how these options and settings affect the user's view of the password reset action.

Viewing an Attribute

You can view an attribute and its mapping information.

Perform the following steps to view an attribute:

1 From the home page of Attributes, click 🔍 to search for the attribute that you want to view.

2 Select **View Attribute** from the Actions menu.

3 Click **Submit**. The Attribute Information page displays.

4 Click the tabs to the right of the page to view attribute mapping information.

5 When finished, click **Attributes** in the cookie trail at the top of the page to return to the home page.

Modifying an Attribute

You can modify attributes and mapping information. See Adding and Mapping an Attribute on page 57 for details about each field. When modifying an attribute, there are custom properties of Select Identity attributes that may not be reflected at the Service level.

Perform the following to modify an attribute:

1. From the home page of Attributes, click 🔍 to search for the attribute that you want to modify.
2. Select **Modify Attribute** from the Actions menu.

   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:

     Modify the attribute to set the Default Display Mask, delete the attribute from the existing service, and Submit. Now modify the service and add that attribute back.

3. Click **Submit**. The Attribute Information page displays.
4. Modify any available fields.
5. Click **Save & Continue**. The Attribute Mapping page displays.
6. You can add, edit, or delete attribute mapping values.
7. When finished, click **Submit** to save your settings.

Deleting an Attribute

You can delete an attribute from the Select Identity system. Remove any Service or Service Role dependencies before deleting the attribute.

Perform the following steps to delete an attribute:

1. From the home page of Attributes, click 🔍 to search for the attribute that you want to delete.
2. Select **Delete Attribute** from the Actions menu.
3. Click **Submit**.
4. You are prompted to confirm the action. Click **OK** to delete the attribute.

6

External Calls

HP OpenView Select Identity workflow processes and profile attributes support the ability to perform actions on external systems. This capability, 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 profile attributes.

Select Identity supports the ability to invoke calls to external systems. You can use external calls to perform the following:

- 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 that the value is what was previously saved. This is used to verify passwords.
- Workflow action — performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems
- Approver Selection — searches an external program for a workflow step approval
- Certification management — enables you to retrieve a certificate from an external system

You must code the classes that are 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 *HP OpenView 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 that indicates 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 for Workflow Steps and Approver Lookups. Each external call is within one of the following call types:

- 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
- Approver selection — searches an external system for a list of users who can approve provisioning requests during a workflow
- Workflow action — performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems
- Certification management — enables you to retrieve a certificate from an external system

Most external calls have predefined parameters that you can modify. The following sections list and describe the functions of the external calls and their parameters, by call type.

Attribute Value Generation

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

IDValueGeneration External Call

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 External Call

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 External Call

Generates a UserID based on another attribute.

Parameters:

Parameter Name	Parameter Value Description
MaxRetryAttempts	Maximum number of attempts that can be tried to create a unique ID
Length	Length of the generated ID
AttributeName	Attribute name from which the UserID is generated (such as from email)

Attribute Value Constraint

Provides a list of possible values for an attribute. Following are the Attribute Value Constraint external calls:

Search Connector
Search Table

Search Connector External Call

Constrains attribute based on the resource_name specified.

Parameters:

Parameter Name	Parameter Value Description
resource_name	Select Identity resource name

Search Table External Call

Constrains attributes based on the specified query and valuefield. The query is executed using the specified poolname.

Parameters:

Parameter Name	**Parameter Value Description**
valuefield	Value from the query to use for constraining the attribute
query	Query invoked to dynamically lookup valid values from the database
poolname	JNDI name for the data source and poolname for which the query is to be executed

Attribute Value Validation

Validates the value of an attribute. Following are the Attribute Value Validation external calls:

IsAlphaNumeric
ManageExpireValidation
PasswordValidation

IsAlphaNumeric External Call

Validates if the attribute is alphanumeric — no parameters.

ManageExpireValidation External Call

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 displays.

PasswordValidation External Call

Validates that the password contains at least the number of each type of characters specified.

Parameters:

Parameter Name	**Parameter Value Description**
Special Characters	Number of required special characters
List of Special Characters	Comma delimited list of valid special characters
Lower Case Letters	Number of required lowercase letters
Upper Case Letters	Number of required uppercase letters
Numerics	Number of required numeric values
Letters	Number of required letters

Attribute Value Verification External Call

Verifies the value of an attribute — no editable parameters.

Approver Selection

Searches an external system for a list of users who can approve provisioning requests during a workflow. The Attribute Value Generation external call is WFGetApproverSampleExtCall.

WFGetApproverSampleExtCall External Call

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

Workflow External Call

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:

LoadUserServices
UserEnableDisableWFExtCall
WorkflowCertificateRequest

LoadUserServices External Call

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 External Call

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

Parameter Name	**Parameter Value Description**
UserName	Admin with authority to modify users that will be using this external call
Password	Admin's password
url	Webservices URL

WorkflowCertificateRequest External Call

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**
DN_FieldName	Attribute name that stores the user’s distinguished name (DN) from the certificate.
CertificateFieldName	Challenge password assigned at the time of user registration.
EmailTemplateName	Default email template from Select Identity, to send email to the user.
CertificateProviderName	Certificate provider name. In the case of Verisign, the name must be “Verisign.” In all other cases, the administrator can assign the name.
ExternalCallName	Name of the CA-specific Java class that implements validation and generation functions for the certificate.

Certification Management Function

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*.

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 that exists 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 is terminated and an error is sent.

After you create the call, copy the source file(s) to a directory on the Select Identity server. Copying the files to a directory in the Select Identity installation path will save 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*.

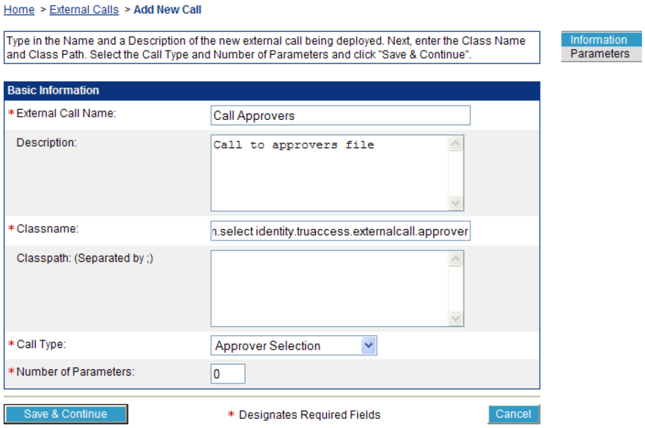
Deploying an External Call

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 profile attribute creation management.

Perform the following steps to deploy an external call:

1. From the home page of External Calls, click **Add New Call**.

   The Basic Information page displays.



Home > External Calls > Add New Call

Type in the Name and a Description of the new external call being deployed. Next, enter the Class Name and Class Path. Select the Call Type and Number of Parameters and click "Save & Continue".

Basic Information

* External Call Name:	Call Approvers
Description:	Call to approvers file
* Classname:	ı.select identity.truaccess.externalcall.approver
Classpath: (Separated by ;)	
* Call Type:	Approver Selection
* Number of Parameters:	0

* Designates Required Fields

2 Enter a unique name for the new call in the External Call Name field.

3 If you choose, enter a description in the Description text box.

4 Enter the name of the class that implements the Java interface in the Classname field.

5 Enter the fully qualified path to the interface in the Classpath field. The class path entries cannot contain directories. 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.

6 Select the type of call you are adding from the Call Type drop-down list. Choices for a workflow process are as follows:

WorkFlow External Call – calls an external program or system during a workflow process.

Approver Selection – searches an external program for a workflow step approval.

Attribute Value Generation – generates the value of an attribute.

Certificate Management Function – implements validation and generation functions for the certificate.

Attribute Value Constraint – restricts the value of an attribute.

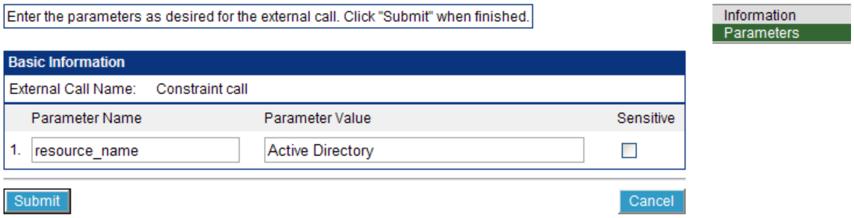
Attribute Value Verification – verifies that the value is what was previously saved. This is used to verify passwords.

Attribute Value Validation – validates an attribute value.

7 Enter the number of parameters required by the external call in the Number of Parameters field.

8 Click **Save & Continue**.

If you specified parameters for this call, the Parameters page displays.



Enter the parameters as desired for the external call. Click "Submit" when finished.

Basic Information

External Call Name: Constraint call

	Parameter Name	Parameter Value	Sensitive
1.	resource_name	Active Directory	□

9 Enter the name and value for each parameter that you want to pass to the external system. See Default External Calls on page 70 for descriptions of the parameters for each external call by call type.

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 **Submit**. The new call is registered with Select Identity.

Modifying an External Call

If you need to change the external call classname, path, or the parameters that are passed from Select Identity, you can modify this information in the Select Identity client.

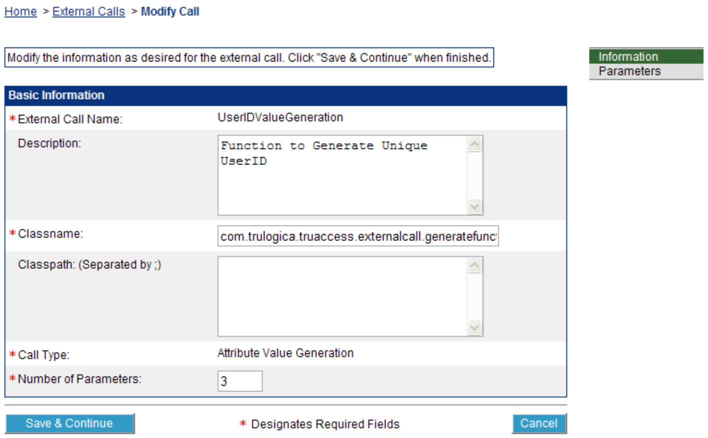
Perform the following steps to modify an external call:

1 From the home page of External Calls, click 🔍 to search for and select an external call. The Search Information page displays. 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 **Submit** and selecting the external call.

2 Select **Modify Call** from the Actions drop-down list.

3 Click **Submit**. The Basic Information page displays.



Home > External Calls > Modify Call

Modify the information as desired for the external call. Click "Save & Continue" when finished.

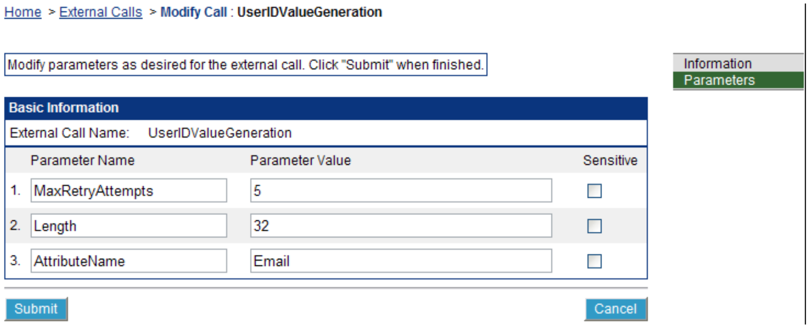
Basic Information	
* External Call Name:	UserIDValueGeneration
Description:	Function to Generate Unique UserID
* Classname:	com.trulogica.truaccess.externalcall.generatefunc
Classpath: (Separated by ;)	
* Call Type:	Attribute Value Generation
* Number of Parameters:	3

* Designates Required Fields

4 Change any information but the call name and type.

5 Click **Save & Continue**. The Parameter Information page displays.

> You must proceed through each page or your changes will not take effect.



Home > External Calls > Modify Call : UserIDValueGeneration

Modify parameters as desired for the external call. Click "Submit" when finished.

Basic Information

External Call Name: UserIDValueGeneration

	Parameter Name	Parameter Value	Sensitive
1.	MaxRetryAttempts	5	☐
2.	Length	32	☐
3.	AttributeName	Email	☐

6 If you have any parameters set, you can modify them. See Default External Calls on page 70 for descriptions of the parameters for each external call by call type.

7 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.

8 Click **Submit** to save your settings.

Viewing an External Call

Perform the following steps to view external call settings:

1. From the home page of External Calls, click 🔍 to search for and select an external call. The Search Information page displays. 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 **Submit** and selecting the external call.
2. Select **View Call** from the Actions drop-down list.
3. Click **Submit**. The Basic Information page displays.
4. Click the tabs to the right to view configuration information.

Deleting an External Call

Perform the following steps to delete an external call:

1. From the home page of External Calls, click 🔍 to search for and select an external call. The Search Information page displays. 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 **Submit** and selecting the external call.
2. Select **Delete Call** from the Actions drop-down list.
3. Click **Submit**.
4. You are prompted to confirm the action. Click **OK** to delete the call from Select Identity.

7

Rules

Reconciliation Rules are used to control how new users are assigned and provisioned in HP OpenView Select Identity for reconciliation requests. When a reconciliation add request is received by Select Identity for an authoritative resource, the rule is applied to the new user. If the user meets the criteria specified in the rule and qualifies for a Service, the user can be added to that Service based on criteria specified in the rule. In addition, a Rule can be used to assign additional services to a user during Move User. This is done using an external call to read the rule from a workflow. Once a rule is created, you can 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 or SPML file that adheres to the rules DTD. Inside the rule file, the RuleID must be named ResourceName_ReconRule for an authoritative resource rule. 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.

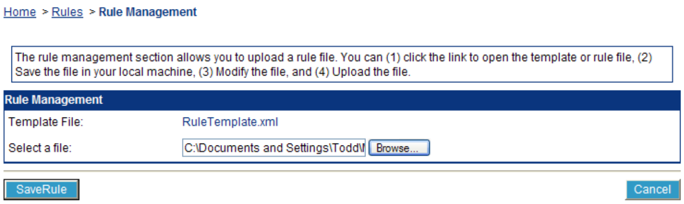
To see SPML file examples, refer to the `\SampleXML\Reconciliation` directory on Select Identity product CD. A sample rule and overview of the DTD are available in Creating Reconciliation Rules on page 245.

Adding a Rule

This procedure requires you to create an XML or SPML file that defines the actions to be performed. See Creating Reconciliation Rules on page 245 for details.

Perform the following to define a rule:

1 From the home page of Rules, click **Add New Rule**. The Rule Management page displays.



Home > Rules > Rule Management

The rule management section allows you to upload a rule file. You can (1) click the link to open the template or rule file, (2) Save the file in your local machine, (3) Modify the file, and (4) Upload the file.

Rule Management

Template File:	RuleTemplate.xml
Select a file:	C:\Documents and Settings\Todd\

2 Click the **RuleTemplate.xml** link to view or edit the template file, or click **Browse** to select a rule.

3 Click **SaveRule** to make the file available within Select Identity.

Modifying a Rule

After a rule is added to the system, you can modify it on your system and update it through the Rules pages.

Perform the following steps to modify a rule:

1 From the home page of Rules, select the rule that you want to modify from the Available Rules drop-down list.

2 Select **Modify Rule** from the Actions list.

3 Click **Submit**. The Rule Management page displays.

4. Click the **.xml** link to edit the template file and save it, or click **Browse** to select a rule that you modified on your system.
5. Click **SaveRule**.

Viewing a Rule

Perform the following steps to view a rule:

1. From the home page of Rules, select the rule that you want to view from the Available Rules drop-down menu.
2. Select **View Rule** from the Actions list.
3. Click **Submit**. The rule's XML displays.

Deleting a Rule

Perform the following steps to delete a rule:

1. From the home page of Rules, select the rule that you want to delete from the Available Rules drop-down menu.
2. Select **Delete Rule** from the Actions list.
3. Click **Submit**.
4. You are prompted to confirm the action. Click **OK** to delete the rule.

8

Notifications

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.

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.

Notification Variables

When creating notification templates, you can 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. There are several types of variables that can be referenced in an email notification template.

The following table contains the types of variables available in email notifications:

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:**

➤ 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 Select Identity database. For example, use `<ovsi-encrypt>[RQT:Password]</ovsi-encrypt>` for a “New Account Password” notification.

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 Select Identity used to approve the request.	**USERDEF:**

Variable Type	**Description**	**Variable**
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:**
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 SI database, even when a workflow instance ends. You can 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:**

Variable Type	Description	Variable
Environment	Variables defined for the environment within the properties file. The Environment variable provides the ability to reference variables defined for the JVM environment. By default, Select Identity adds all properties from the `truaccess.properties` file to the JVM Environment. Any value that you can perform a `System.getProperty()` on 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

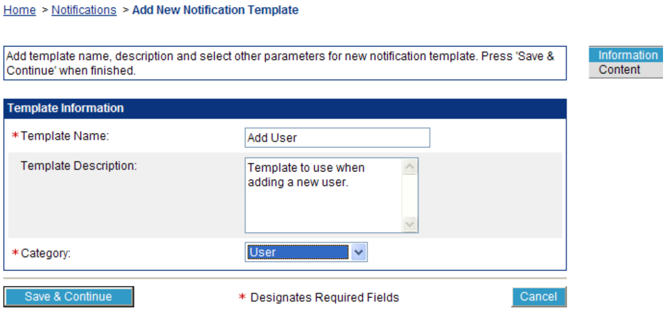
The Notifications capability enables you to define the content of email notices that are sent to users and administrators during the account creation, modification, or removal process. See Event Reference on page 254 to review the actions for which you can create notification templates.

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

Adding a Notification Template

Perform the following steps to add a new notification template:

1. From the home page of Notifications, click **Add New Notification Template**. The Information page displays.



Home > Notifications > Add New Notification Template

Add template name, description and select other parameters for new notification template. Press 'Save & Continue' when finished.

Template Information

*Template Name:	Add User
Template Description:	Template to use when adding a new user.
*Category:	User

* Designates Required Fields

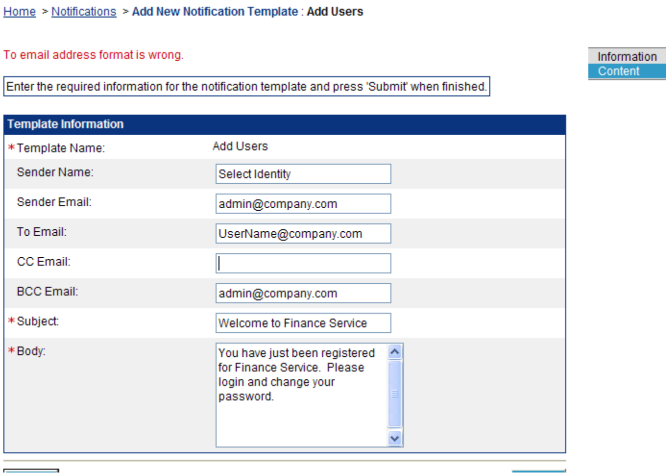
2 Enter a name for this template in the Template Name field.

3 Enter a description for this template in the Template Description field.

4 Select the category, or type of template, that you want to create from the Category drop-down list.

Select **User** to define a notification template that users will see when their accounts are created or modified.

5 Click **Save & Continue**.The Content page displays.



Home > Notifications > Add New Notification Template : Add Users

To email address format is wrong.

Enter the required information for the notification template and press 'Submit' when finished.

Template Information

*Template Name:	Add Users
Sender Name:	Select Identity
Sender Email:	admin@company.com
To Email:	UserName@company.com
CC Email:	
BCC Email:	admin@company.com
*Subject:	Welcome to Finance Service
*Body:	You have just been registered for Finance Service. Please login and change your password.

6 Enter a name or value in the Sender Name field. You can use predefined variables, such as [RQSTR:UserName], and the system will enter the name of the administrator sending the request. See Notification Variables on page 86 for more information.

7. Enter an address in the Sender Email field. You can use the predefined variables and the system will enter the address of the administrator that is sending the request.
8. If you want the email to be sent to another recipient, enter the address in the CC Email or BCC Email fields.
9. Enter a subject for this email in the Subject field.
10. Enter the text for this email response in the Body text box. The text should reflect the meaning of the category that you selected in Step 4.

➤ 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

11. Click **Submit** to save your settings.

    The new template is added to the template list on the Notifications home 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.

Perform the following steps to copy a notification template:

1. From the home page of Notifications, click 🔍 to search for and select the template that you want to copy.
2. Select **Copy Notification Template** from the Actions drop-down list.
3. Click **Submit**. The Information page displays.

4. Enter a unique name for this template in the Template Name field. This is the only field that you are required to change.
5. You can modify any of the information on this and the next configuration page. The pages and fields are the same as in the Add New Notification Template procedure on page 90.
6. Click **Save & Continue** after completing your changes on each page.

   The copied template is added to the system.

Modifying a Notification Template

You can change any of the template fields. Users and administrators will see the new messages the next time an action prompts the system to send one.

Perform the following steps to modify a template:

1. From the home page of Notifications, click 🔍 to search for and select the template that you want to copy.
2. Select **Modify Notification Template** from the Actions drop-down list.
3. Click **Submit**.
4. You can modify any of the information on the rest of the configuration pages. The pages and fields are the same as in the Add New Notification Template procedure on page 90. Click **Save & Continue** after completing your changes on each page.
5. Click **Submit** to save your settings.

Viewing a Notification Template

Perform the following steps to view a template:

1. From the home page of Notifications, click 🔍 to search for and select the template that you want to copy.
2. Select **View Notification Template** from the Actions drop-down list.
3. Click **Submit**.
4. Select the type of information that you want to view from the topics on the right.

- **Information** provides basic information about the template.
- **Contents** provides the content variables that are sent in the email.

Deleting a Notification Template

To delete a notification template, perform the following steps:

1. From the home page of Notifications, click 🔍 to search for and select the template that you want to copy.
2. Select **Delete Notification Template** from the Actions drop-down list.
3. Click **Submit**.
4. You will be prompted to confirm the action. Click **OK** to delete the template.

9

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 multiple Select Identity administrators' approval. The approval process can also rely on external calls to third-party systems or databases.

For example, when an employee is promoted to manager, he needs access to the company's HCM system to manage other employees. To support these newly-acquired responsibilities, the employee must be granted new entitlements and access privileges. Before giving him access to these systems, upper-level management needs to 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 him that he is now authorized to manage others.

Workflow Studio Overview

Workflow Studio enables you to create the workflow templates that represent the provisioning process. A workflow template models this process in order to automate the actions that 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 External Calls on page 69 for more information.

An administrator with Workflow Studio actions defines the workflow templates and processes by which users are added to, updated, or removed from the system. A workflow can require one or more steps before completion. Each approver can be notified by email when a new account needs to be reviewed. That administrator can then log in and access the Approvals section of the Select Identity client, where a Pending Tasks notification displays at the top of the home page.

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. All of the concepts and procedures for the Workflow Studio capability 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 Service Roles on page 102.) For example, you can assign a simple provisioning template to an add request for self-registration. This template might perform user provisioning and request a single approval. Then, when a new user requests access to the service, 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 home page. See Administrative Roles on page 126 for more information.
- Sending email using one of the email templates created on the Notifications home page. See Notifications on page 86 for more information.
- Calling external systems registered with Select Identity on the External Calls home page. See External Calls on page 69 for more information.

You can generate reports to track the status of request events and the workflows that support them. To view reports, specify parameters on the Request Status home page of the Select Identity client. See the *HP OpenView Select Identity Workflow Studio Guide* for more information.

10

Challenge Response Questions

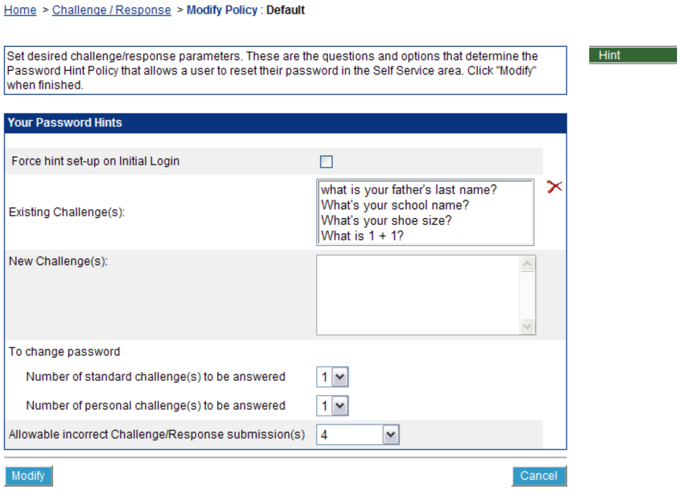
Secure access to the Services that your company offers is defined through the use of attributes and challenge and response policies. The HP OpenView Select Identity Challenge/Response capability determines the generic security policy for the system.

The Select Identity challenge and response policy governs the password hints for the system. You can restrict login attempts with this policy and force hint configuration on initial login.

Modifying the Challenge and Response Policy

Perform the following steps to modify the Select Identity challenge and response policy:

1 From the home page of Challenge/Response, the Password Hints page displays.



Home > Challenge / Response > Modify Policy : Default

Set desired challenge/response parameters. These are the questions and options that determine the Password Hint Policy that allows a user to reset their password in the Self Service area. Click "Modify" when finished.

Your Password Hints

Force hint set-up on Initial Login	□
Existing Challenge(s):	what is your father's last name? What's your school name? What's your shoe size? What is 1 + 1?
New Challenge(s):	
To change password	
Number of standard challenge(s) to be answered	1
Number of personal challenge(s) to be answered	1
Allowable incorrect Challenge/Response submission(s)	4

2 Modify any of the fields. You can

- force the user to set hints at initial login
- delete the existing hints
- create new hints
- determine the number of hints a user must answer to change a password
- lock the account after a number of incorrect attempts

3 Click **Modify.**

Modifying the Forget Password Setting

You can determine whether Select Identity or the user will reset a password when the user selects the Forget Password link. You do this by editing the following setting in the `TruAccess.properties` file, which is located in the `%InstallDir%\sysArchive` directory:

```
com.hp.ovsi.forgetpassword.autogenerate=true
```

- If `com.hp.ovsi.forgetpassword.autogenerate=true` (the default), Select Identity will automatically generate the password and provide the correct answers to the Challenge/Response questions. In this case, the notification email that is sent out to the user will have the new password shown in clear text.
- If `com.hp.ovsi.forgetpassword.autogenerate=false`, the user will enter a new password, which will be accepted by Select Identity. The notification email sent out in this case will show ******* as the new password, since the user already knows the new password.

11

Services

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.

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

There are three types of Services.

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

Admin Services – Provide a means of associating administrative roles to user accounts.

Composite Services – Enable Service grouping. Users registering for a composite Service can have access to multiple Services.

The Services capability also enables you to set and view Service Roles, which provide a secure management structure and view for your partners and customers. Service Roles are hierarchical and management can be delegated to any level.

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 Service attribute values and properties, which determine the attribute characteristics that are acceptable for this Service.
- Creating Service views, 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, which defines a logical grouping of users accessing the Service.

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

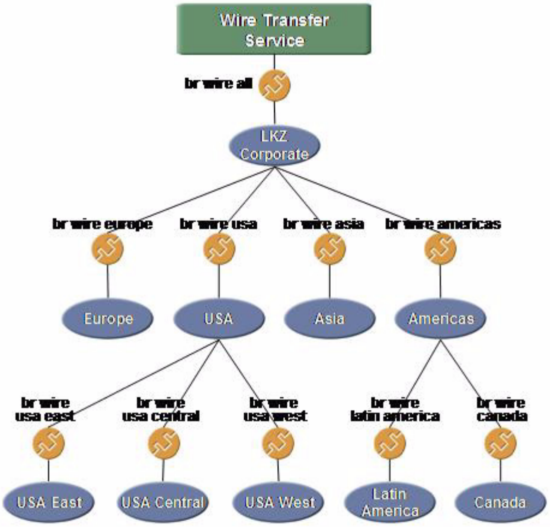
➤ When possible, it is recommended that you use constraints when configuring the Service attribute values. By using constraints, you may improve performance within Select Identity. See Setting Service Attribute Values on page 110 for details.

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.

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

Figure 4 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 and protects the privacy and security of those Service Roles.

Attributes defined at the Service Role level take precedence over those set at the Service level. For example, if a Service is defined to require a one-stage approval process for new account registration and a Service Role is assigned to a partner that requires a two-step process, the partner is required to follow the two-step process to register for that Service.

Context

Context defines the rights and permissions that a group of users receives based on the defined Service Role (such as Gold, Silver, and Platinum). Users are added to a context grouping according to the attributes and values that you select. For example, you may want to group users by location. You would then create a context with attribute “Country” and values “USA,” “India,” and “France” defined. Users are sorted according to the value they select when registering for a Service. See Defining Service Roles and Context on page 117 for detailed procedures.

Fixed and Optional Entitlements

The Select Identity Service-oriented management structure enables you to offer sets of entitlements based on the Service Role. Entitlements can either be fixed (required) or optional. The entitlements that are available at the Service Role level are defined by the parent Service. Service Roles that are created from a parent Service Role inherit from the parent’s entitlement lists. Entitlements that are fixed at the Service level will be required throughout the Service Role hierarchy.

You can define constraint values for multi-valued attributes at the Service Role level so that users associated with different Service Role can be assigned different values based on the hierarchy. See Creating a Service Role on page 117 for more detailed information.

Creating and Modifying Services

The Services capability enables you to add, modify, and delete the Services that are accessed by your customers and business partners. 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 contexts from the Services pages. Services are made available to your customers and partners by setting a Service Role in Select Identity.

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

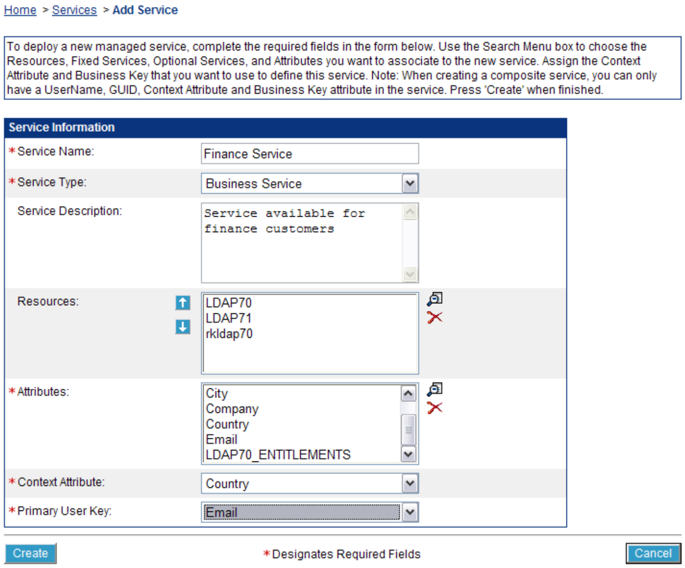
  Do not include the password attribute for modifying users. The password will not be pushed to any resource. Passwords should only be set when adding a user, or reset using the Reset Password action from the Users home page (see Resetting a User's Password on page 173).

Deploying a Service

You can provide many Services to your customers. Make sure that the resources required to support each Service are already configured. Perform the following steps to add a Service:

1 From the home page of Services, click **Deploy New Service**.

The Service Information page displays.



Home > Services > **Add Service**

To deploy a new managed service, complete the required fields in the form below. Use the Search Menu box to choose the Resources, Fixed Services, Optional Services, and Attributes you want to associate to the new service. Assign the Context Attribute and Business Key that you want to use to define this service. Note: When creating a composite service, you can only have a UserName, GUID, Context Attribute and Business Key attribute in the service. Press 'Create' when finished.

Service Information

*Service Name:	Finance Service
*Service Type:	Business Service
Service Description:	Service available for finance customers
Resources:	LDAP70 LDAP71 rkldap70
*Attributes:	City Company Country Email LDAP70_ENTITLEMENTS
*Context Attribute:	Country
*Primary User Key:	Email

2 Enter a name for the Service in the Service Name field.

3 Select a Service type 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.

Composite Service – a grouping of Services. Services must be created before they can be grouped into a composite Service.

4 Enter a description for the Service in the Service Description field.

5 Click 🔍 to locate and add resources to support the Service. You can add multiple resources at one time from the Search Results page.

After you add resources, you can change their order with the up and down arrows. This determines the order to which resources are provisioned.

6 Click 🔍 to locate and add attributes to support the Service. You can add multiple attributes at one time from the Search Results page.

7. Select an attribute for which 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, you can use the “Country” attribute and users will be grouped by the value, such as “USA,” “India,” or “France.”
8. 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.
9. Click **Create**.

   The Service remains in **Pending** state until attributes, Service Roles, and context are defined.

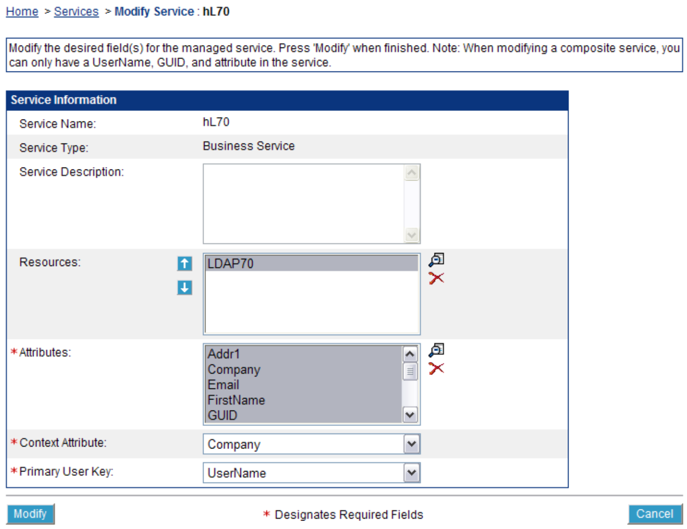
Modifying a Service

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.

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

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Modify Service** from the Actions drop-down list.
3. Click **Submit**.

   The Service Information page displays.



Home > Services > **Modify Service** : **hL70**

Modify the desired field(s) for the managed service. Press 'Modify' when finished. Note: When modifying a composite service, you can only have a UserName, GUID, and attribute in the service.

Service Information

Service Name: hL70

Service Type: Business Service

Service Description:

Resources: LDAP70

* Attributes: Addr1, Company, Email, FirstName, GUID

* Context Attribute: Company

* Primary User Key: UserName

4 Modify the information that is available to you. You can

- add, modify or delete the service description
- add resources.
- change the order of supporting resources.
- delete resources.
- add attributes.
- delete attributes.
- change the context attribute.
- change the primary user key.

5 Click **Modify** after completing your changes.

Copying a Service

If you need to copy a Service, perform the following:

1 From the home page of Services, select a Service from the Service drop-down list.

2 Select **Copy Service** from the Actions drop-down list.

3. Click **Submit**. The Copy Service dialog displays.
4. Enter a unique name for this Service in the **Service Name** field.
5. Click **Submit**. The Service is copied.

Deleting a Service

You can delete a Service from the Select Identity system. Make sure that no users are associated with the Service.

Perform the following steps to delete a Service:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Delete Service** from the Actions drop-down list.
3. Click **Submit**.
4. You will be prompted to confirm the action. Click **OK**.

Service Attributes

You can 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 Select Identity 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

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

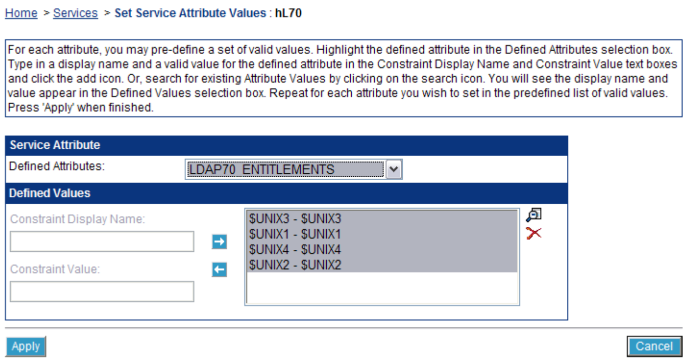
Setting Service Attribute Values

You can 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.

Perform the following steps to set Service attribute values:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Set Service Attribute Values** from the Actions drop-down list.
3. Click **Submit**.

   The Attribute Selection page displays.
4. Select the attribute for which you want to restrict values from the Defined Attributes list. If the attribute that you selected has predefined values, the search icon displays.



Home > Services > Set Service Attribute Values : hL70

For each attribute, you may pre-define a set of valid values. Highlight the defined attribute in the Defined Attributes selection box. Type in a display name and a valid value for the defined attribute in the Constraint Display Name and Constraint Value text boxes and click the add icon. Or, search for existing Attribute Values by clicking on the search icon. You will see the display name and value appear in the Defined Values selection box. Repeat for each attribute you wish to set in the predefined list of valid values. Press 'Apply' when finished.

Service Attribute

Defined Attributes: LDAP70_ENTITLEMENTS

Defined Values

Constraint Display Name:

Constraint Value:

$UNIX3 - $UNIX3
$UNIX1 - $UNIX1
$UNIX4 - $UNIX4
$UNIX2 - $UNIX2

5 Enter a display name and values for the selected attribute, or, if available, click 🔍 to search for and select the values that you want to set for this attribute.

6 If you entered values in the fields provided, click the right arrow icon to move the value pair to the right.

7 When finished, click **Apply**.

Setting Service Attribute Properties

You can require 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.

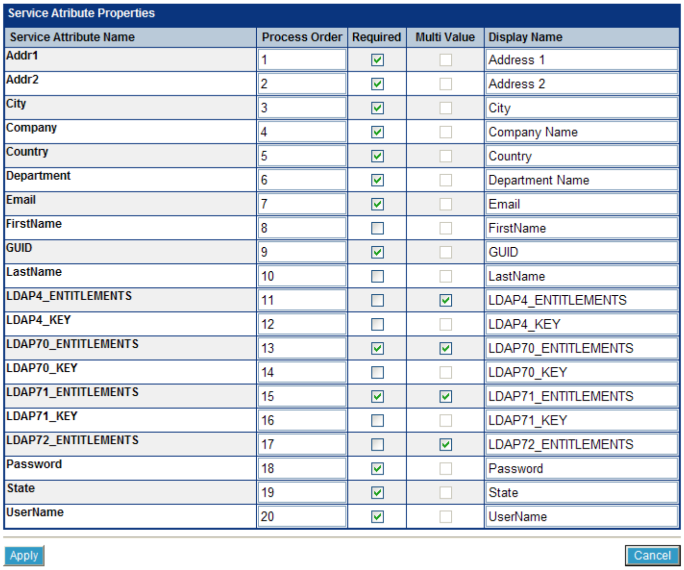
Perform the following steps to set attributes properties for a Service:

1 From the home page of Services, select a Service from the Service drop-down list.

2 Select **Set Service Attribute Properties** from the Actions drop-down list.

3 Click **Submit**.

The Attribute Selection page displays.



Service Atribute Properties

Service Attribute Name	Process Order	Required	Multi Value	Display Name
Addr1	1	☑	□	Address 1
Addr2	2	☑	□	Address 2
City	3	☑	□	City
Company	4	☑	□	Company Name
Country	5	☑	□	Country
Department	6	☑	□	Department Name
Email	7	☑	□	Email
FirstName	8	□	□	FirstName
GUID	9	☑	□	GUID
LastName	10	□	□	LastName
LDAP4_ENTITLEMENTS	11	□	☑	LDAP4_ENTITLEMENTS
LDAP4_KEY	12	□	□	LDAP4_KEY
LDAP70_ENTITLEMENTS	13	☑	☑	LDAP70_ENTITLEMENTS
LDAP70_KEY	14	□	□	LDAP70_KEY
LDAP71_ENTITLEMENTS	15	☑	☑	LDAP71_ENTITLEMENTS
LDAP71_KEY	16	□	□	LDAP71_KEY
LDAP72_ENTITLEMENTS	17	□	☑	LDAP72_ENTITLEMENTS
Password	18	☑	□	Password
State	19	☑	□	State
UserName	20	☑	□	UserName

4 Select the check boxes to the left of the fields that you want displayed for this view. The fields are displayed for users registering for this Service.

5 Order the fields that you want displayed by entering 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.

6 If you want to require a field, select its check box 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.

7 If an attribute can have multiple values, the Multi Value check box is selected. Deselect the check box if you want to restrict the user to one value.

8 Edit the name that is displayed to users in the Display Name fields.

9 Click **Apply** to save your settings.

Service Views

After you create a Service, you can create views 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, you can define a view that makes only those fields available.

You can also use these views to determine what information approvers see when requests are processed through workflow steps. Each approval block within a workflow can have a different Service view associated with it. See Creating a Service Role on page 117 for information on configuring views for workflow approval blocks.

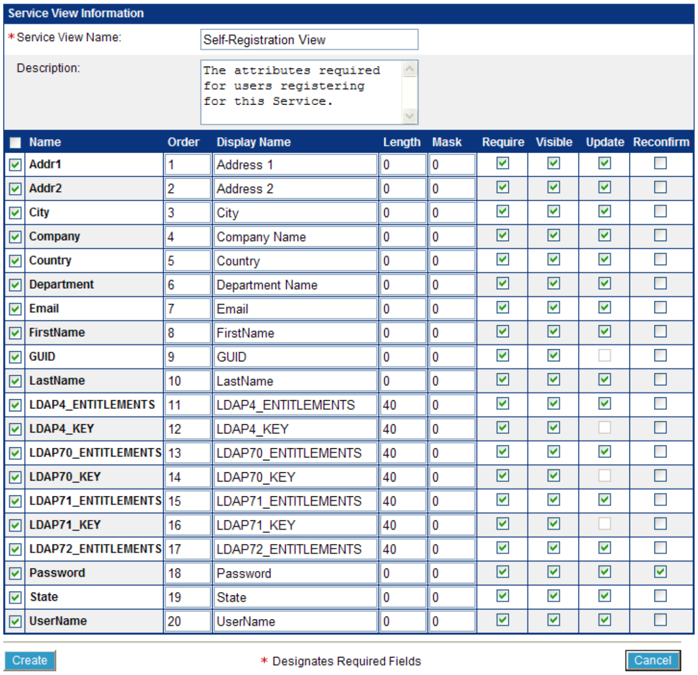
Service views can also be used to create a multi-page view. A multi-page view can be used in delegated user management, self service, self registration, and the approval pages to determine what users see for each action. The display of the views can be ordered.

Creating a Service View

Perform the following steps to create a Service view:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Create View** from the Actions drop-down list.
3. Click **Submit**.

The Service View Information page displays.



Service View Information

*Service View Name: Self-Registration View

Description: The attributes required for users registering for this Service.

□ Name	Order	Display Name	Length	Mask	Require	Visible	Update	Reconfirm
☑ Addr1	1	Address 1	0	0	☑	☑	☑	□
☑ Addr2	2	Address 2	0	0	☑	☑	☑	□
☑ City	3	City	0	0	☑	☑	☑	□
☑ Company	4	Company Name	0	0	☑	☑	☑	□
☑ Country	5	Country	0	0	☑	☑	☑	□
☑ Department	6	Department Name	0	0	☑	☑	☑	□
☑ Email	7	Email	0	0	☑	☑	☑	□
☑ FirstName	8	FirstName	0	0	☑	☑	☑	□
☑ GUID	9	GUID	0	0	☑	☑	□	□
☑ LastName	10	LastName	0	0	☑	☑	☑	□
☑ LDAP4_ENTITLEMENTS	11	LDAP4_ENTITLEMENTS	40	0	☑	☑	☑	□
☑ LDAP4_KEY	12	LDAP4_KEY	40	0	☑	☑	□	□
☑ LDAP70_ENTITLEMENTS	13	LDAP70_ENTITLEMENTS	40	0	☑	☑	☑	□
☑ LDAP70_KEY	14	LDAP70_KEY	40	0	☑	☑	□	□
☑ LDAP71_ENTITLEMENTS	15	LDAP71_ENTITLEMENTS	40	0	☑	☑	☑	□
☑ LDAP71_KEY	16	LDAP71_KEY	40	0	☑	☑	□	□
☑ LDAP72_ENTITLEMENTS	17	LDAP72_ENTITLEMENTS	40	0	☑	☑	☑	□
☑ Password	18	Password	0	0	☑	☑	☑	☑
☑ State	19	State	0	0	☑	☑	☑	□
☑ UserName	20	UserName	0	0	☑	☑	☑	□

* Designates Required Fields

4 Enter a name for this view in the Service View Name field.

5 If you choose, enter a description to this view in the Description field.

6 Select the check boxes to the left of the fields that you want available for this view.

7 Order the fields that you want displayed by entering numbers in the Order column.

8 You can edit the name that is displayed to users in the Display Name fields.

9 Define or change the maximum length of each value in the Length column.

10 If you want all or a portion of the value masked, enter that number of characters in the Mask column.

11 If you want to require a field, select its check box in the Require column.

12 If you want a field to be visible on the registration page, select its check box in the Visible column.

13 If you want to give users permission to update a field value, select its check box in the Update column.

14 If you want the user to reconfirm a value for validation purposes, select its check box in the Reconfirm column.

15 Click **Create**.

Creating a Multi-Page View

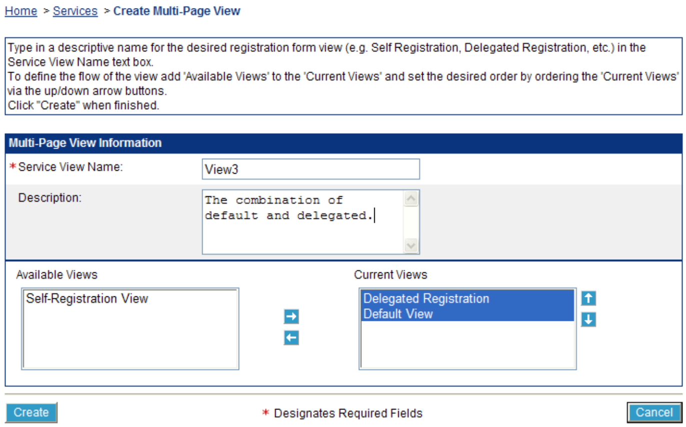
You may want to create a view that consists of other views.

Perform the following steps to create a multi-page view:

1 From the home page of Services, select a Service from the Service drop-down list.

2 Select **Create View (Multi-Page)** from the Actions drop-down list.

3 Click **Submit**. The Multi-Page View Information page displays.



Home > Services > Create Multi-Page View

Type in a descriptive name for the desired registration form view (e.g. Self Registration, Delegated Registration, etc.) in the Service View Name text box.
To define the flow of the view add 'Available Views' to the 'Current Views' and set the desired order by ordering the 'Current Views' via the up/down arrow buttons.
Click "Create" when finished.

Multi-Page View Information

*Service View Name: View3

Description: The combination of default and delegated.

Available Views: Self-Registration View

Current Views: Delegated Registration, Default View

4 Enter a unique name for this view in the Service View Name field.

5 If you choose, enter a description for this view in the Description field.

6. Choose the views that you want to group from the Available Views list and click the right arrow to move them to the Current Views list. You can change the display order of the views with the up and down arrows.
7. Click **Create** to create the view.

Modifying a Service View

Perform the following steps to modify a Service view:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Modify View** from the Actions drop-down list.
3. Click **Submit**.
4. Select a Service view from the drop-down list. The Service View Information page displays.
5. Modify any of the field definitions.
6. Click **Modify.**

Deleting a Service View

Before deleting a Service view, make sure that all dependencies have been removed.

Perform the following steps to delete a Service view:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Delete View** from the Actions drop-down list.
3. Click **Submit**.
4. Select a Service view from the Service View Name drop-down list.
5. Click **Delete**.

Defining Service Roles and Context

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 view to be used in that block. The initial delegated or self add/modify form will always use the default view defined, but any views defined in the block view are used in place of the default view 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 view Service Roles and define a context for each of your Services.

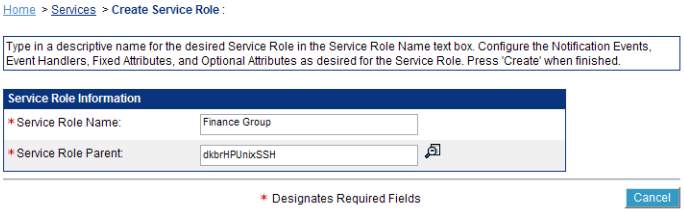
Creating a Service Role

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.

Perform the following steps to set a Service Role:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Create Service Role** from the Actions drop-down list.
3. Click **Submit**.

   The Service Role Information page displays.



Home > Services > Create Service Role :

Type in a descriptive name for the desired Service Role in the Service Role Name text box. Configure the Notification Events, Event Handlers, Fixed Attributes, and Optional Attributes as desired for the Service Role. Press 'Create' when finished.

Service Role Information

*Service Role Name: Finance Group

*Service Role Parent: dkbrHPUnixSSH

* Designates Required Fields

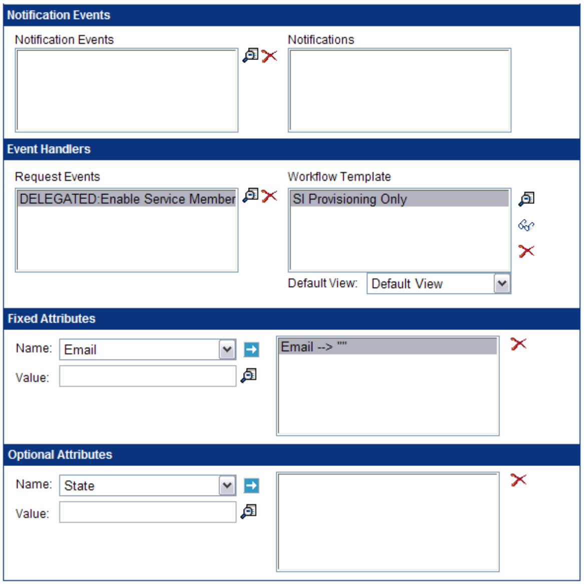
If this is the first Service Role that you are creating for this Service, you will not see the parent option.

➤ 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.

4 Enter a name for the new Service Role in the Service Role Name field.

5 Click 🔍 to search for and select a parent for this Service Role.

The Service Role Information page is populated with options determined by the parent selection.



Notification Events

- Notification Events:
- Notifications:

Event Handlers

- Request Events: DELEGATED:Enable Service Member
- Workflow Template: SI Provisioning Only
- Default View: Default View

Fixed Attributes

- Name: Email
- Value:
- Email --> ""

Optional Attributes

- Name: State
- Value:

6 Click 🔍 to search for and select the Notification events that you want available for this Service Role.

  a After you choose the events, select an event in the list.

  b Click 🔍 next to the Notifications table to search for and select the notification policies that you want to assign for each event. See Notifications on page 86 for information about notification policies.

7 Click 🔍 to search for and select the Request events that you want set for this Service Role.

  See Event Reference on page 254 for a list of events and actions within Select Identity.

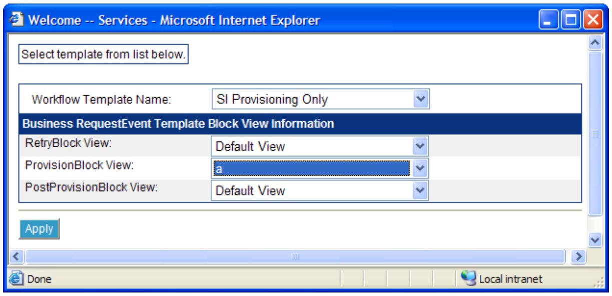
  > ➤ It is recommended that you select a view that does not include the password for the DELEGATED Modify User action. This password will not be pushed to any resource.

  a After you choose the events, select an event in the list.

b Click 🔍 next to the Workflow Template table to search for and select the workflow templates that you want to assign for each event. See Workflow Studio on page 95 for information about workflow templates.

c With the template still selected, click 🔍 next to the Default View field to search for and select the Service view that you want assigned to each workflow template.

d You can select Service views at the approval block level within the workflow process. Select the workflow template and click ⚯ to view workflow block details.



Welcome -- Services - Microsoft Internet Explorer

Select template from list below.

Workflow Template Name: SI Provisioning Only

Business RequestEvent Template Block View Information

RetryBlock View:	Default View
ProvisionBlock View:	a
PostProvisionBlock View:	Default View

e For each approval block, select the Service view that you want approvers to see when reviewing this request event. If you do not specify a view, the Default view is selected.

8 Select the fixed attributes that you want assigned to users enabled for this Service Role. You can select multiple attributes. See Attributes on page 52 for information about attributes and values.

a Choose an attribute from the Name drop-down list. This list is provided by the parent Service Role.

b After the attribute is selected, search for or enter a value in the Value field.

If you are creating an administrative Service, this is where you select roles.

c Click ▷ to move the attribute and value to the entry table. To delete an attribute, select it and click ✕.

9. Select the optional attributes that you want assigned to users enabled for this Service Role. You can select multiple attributes. See Attributes on page 52 for information about attributes and values.
   a. Choose an attribute from the Name drop-down list. This list is provided by the parent Service Role.
   b. After the attribute is selected, search for or enter a value in the Value field.
   c. Click ▷ to move the attribute and value to the entry table. To delete an attribute, select it and click ✕.
10. Click **Create**.

The Service Role is now active. However, the Service remains in a Pending state until the Context is set.

Modifying a Service Role

Perform the following steps to modify a Service Role:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Modify Service Role** from the Actions drop-down list.
3. Click **Submit**.
4. Select the Service Role that you want to modify from the Service Role name drop-down list. The Service Role parameters display.
5. Modify any of the available fields.
6. Click **Modify**.

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. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Delete Service Role** from the Actions drop-down list.
3. Click **Submit**.
4. Click 🔍 to search for and select the Service Role that you want to delete.
5. Click **Delete**.

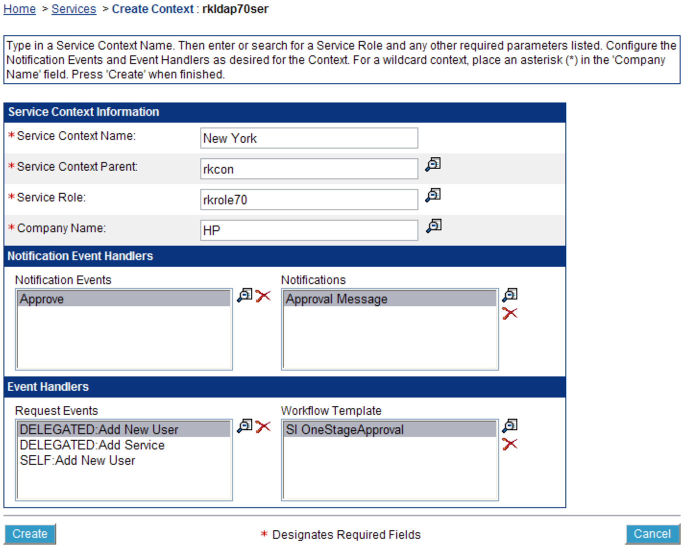
Creating Context

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. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Create Context** from the Actions drop-down list.
3. Click **Submit**.

   The Service Context Information page displays.



Home > Services > Create Context : rkldap70ser

Type in a Service Context Name. Then enter or search for a Service Role and any other required parameters listed. Configure the Notification Events and Event Handlers as desired for the Context. For a wildcard context, place an asterisk (*) in the 'Company Name' field. Press 'Create' when finished.

Service Context Information

* Service Context Name:	New York
* Service Context Parent:	rkcon
* Service Role:	rkrole70
* Company Name:	HP

Notification Event Handlers

Notification Events	Notifications
Approve	Approval Message

Event Handlers

Request Events	Workflow Template
DELEGATED:Add New User DELEGATED:Add Service SELF:Add New User	SI OneStageApproval

* Designates Required Fields

4 Enter a name for the context in the Service Context Name field.

5 If available, click 🔍 to search for and select a parent context. The parent provides a superset of attributes, workflow processes, and policies that you can choose from.

6 Click 🔍 to search for and select a parent Service Role. The parent Service Role provides a superset of attributes, workflow processes, and policies that you can choose from.

When you choose the parent Service Role, the rest of the form is displayed.

7 Click 🔍 to search for and select a value for the context attribute that you defined when creating the Service. For example, if you defined “Company Name” as the context attribute for this Service, you would select a value such as “HP” to create this context.

8 Click 🔍 to search for and select the Notification events that you want available for this Service Role. If the Service Role has only one Notification event selected, these steps are not necessary.

a After you choose the events, select an event in the list.

   b Click 🔍 next to the Notifications table to search for and select the notification policies that you want to assign for each event. See Notifications on page 86 for information about notification policies.

9. Click 🔍 to search for and select the Request events and that you want set for this Service Role. If the Service Role has only one Request event selected, these steps are not necessary.

   a After you choose the events, select an event in the list.

   b Click 🔍 next to the Workflow Template table to search for and select the workflow templates that you want to assign for each event. See Workflow Studio on page 95 for information about workflow templates.

10. Click **Create**. The context is created for the Service and the Service is now enabled.

Modifying Context

You can modify the context relationship of users assigned to a Service.

Perform the following steps to modify context:

1. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Modify Context** from the Actions drop-down list.
3. Click **Submit**.
4. Select the context that you want to modify from the Service Context Name drop-down list. The Service Context parameters display.
5. Modify any of the available fields.
6. When finished, click **Modify**.

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. From the home page of Services, select a Service from the Service drop-down list.
2. Select **Delete Context** from the Actions drop-down list.
3. Click **Submit**.
4. Select the context that you want to delete from the Service Context Name drop-down list.
5. Click **Delete**.

12

Administrative Roles

You can create administrative roles to govern the actions that each administrator can perform within the HP OpenView Select Identity system. There are predefined roles that you can view and modify. If your environment requires more granular roles, you can create your own.

Administrative roles are made available through Services that are designed specifically for management. When you create a Service, you have the option to define it as an Administrative Service. You can then add users to this Service to assign administrative roles. See Creating and Modifying Services on page 104 for information about creating a Service.

When creating administrative roles, remember that Select Identity provides n-tier delegation of management tasks. Your organization can delegate any range of management tasks to customers and partners as needed.

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

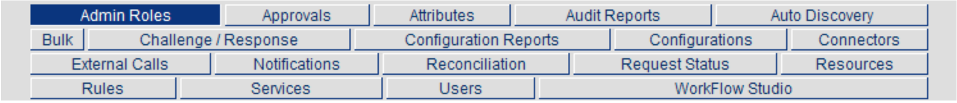
Administrative Capabilities and Actions

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

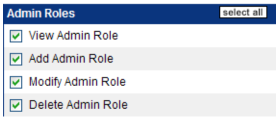
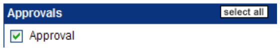
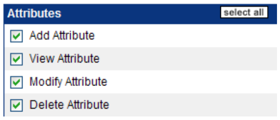
Select Identity Capabilities and Actions

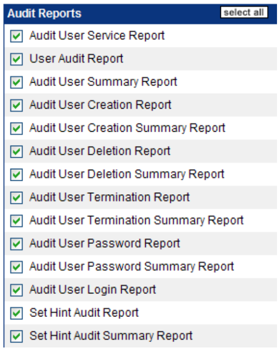
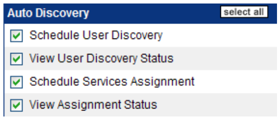
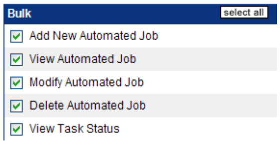
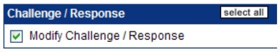
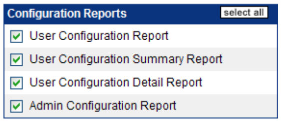
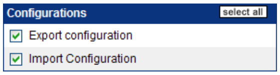
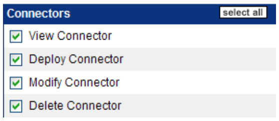
Roles represent a group of actions that a Select Identity administrator can perform within each management capability (link) in the client. The actions that are assigned to each administrator help form a view of the system. You can assign any number of management capabilities to each administrative role.

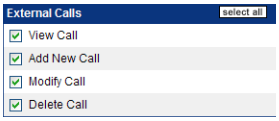
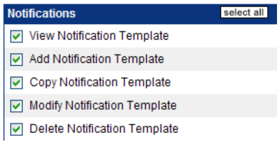
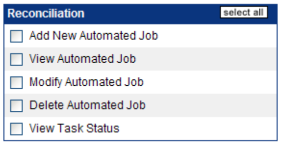
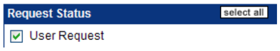
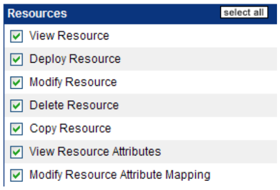
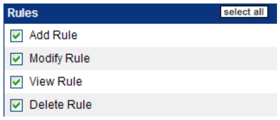
When an administrator with that role logs in to Select Identity, a list of roles associated with the account is listed at the bottom of the home page.

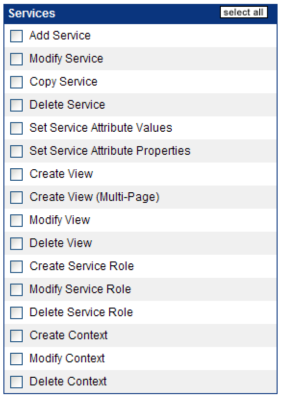
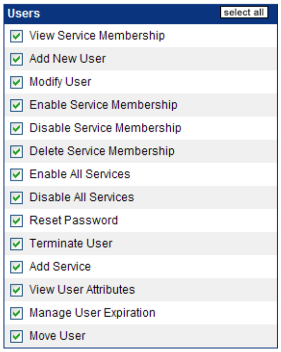
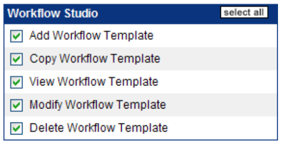


The following are all of the actions organized by Select Identity capability. All are accessed through the Admin Roles section of the client.

Capability	Actions
Admin Roles	 Admin Roles select all ☑ View Admin Role ☑ Add Admin Role ☑ Modify Admin Role ☑ Delete Admin Role
Approvals	 Approvals select all ☑ Approval
Attributes	 Attributes select all ☑ Add Attribute ☑ View Attribute ☑ Modify Attribute ☑ Delete Attribute

Capability	Actions
Audit Reports	 Audit Reports select all ☑ Audit User Service Report ☑ User Audit Report ☑ Audit User Summary Report ☑ Audit User Creation Report ☑ Audit User Creation Summary Report ☑ Audit User Deletion Report ☑ Audit User Deletion Summary Report ☑ Audit User Termination Report ☑ Audit User Termination Summary Report ☑ Audit User Password Report ☑ Audit User Password Summary Report ☑ Audit User Login Report ☑ Set Hint Audit Report ☑ Set Hint Audit Summary Report
Auto Discovery	 Auto Discovery select all ☑ Schedule User Discovery ☑ View User Discovery Status ☑ Schedule Services Assignment ☑ View Assignment Status
Bulk	 Bulk select all ☑ Add New Automated Job ☑ View Automated Job ☑ Modify Automated Job ☑ Delete Automated Job ☑ View Task Status
Challenge/ Response	 Challenge / Response select all ☑ Modify Challenge / Response
Configuration Reports	 Configuration Reports select all ☑ User Configuration Report ☑ User Configuration Summary Report ☑ User Configuration Detail Report ☑ Admin Configuration Report
Configurations	 Configurations select all ☑ Export configuration ☑ Import Configuration
Connectors	 Connectors select all ☑ View Connector ☑ Deploy Connector ☑ Modify Connector ☑ Delete Connector

Capability	Actions
External Calls	 External Calls ☑ View Call ☑ Add New Call ☑ Modify Call ☑ Delete Call
Notifications	 Notifications ☑ View Notification Template ☑ Add Notification Template ☑ Copy Notification Template ☑ Modify Notification Template ☑ Delete Notification Template
Reconciliation	 Reconciliation □ Add New Automated Job □ View Automated Job □ Modify Automated Job □ Delete Automated Job □ View Task Status
Request Status	 Request Status ☑ User Request
Resources	 Resources ☑ View Resource ☑ Deploy Resource ☑ Modify Resource ☑ Delete Resource ☑ Copy Resource ☑ View Resource Attributes ☑ Modify Resource Attribute Mapping
Rules	 Rules ☑ Add Rule ☑ Modify Rule ☑ View Rule ☑ Delete Rule

Capability	Actions
Services	 Services select all □ Add Service □ Modify Service □ Copy Service □ Delete Service □ Set Service Attribute Values □ Set Service Attribute Properties □ Create View □ Create View (Multi-Page) □ Modify View □ Delete View □ Create Service Role □ Modify Service Role □ Delete Service Role □ Create Context □ Modify Context □ Delete Context
Users	 Users select all ☑ View Service Membership ☑ Add New User ☑ Modify User ☑ Enable Service Membership ☑ Disable Service Membership ☑ Delete Service Membership ☑ Enable All Services ☑ Disable All Services ☑ Reset Password ☑ Terminate User ☑ Add Service ☑ View User Attributes ☑ Manage User Expiration ☑ Move User
Workflow Studio	 Workflow Studio select all ☑ Add Workflow Template ☑ Copy Workflow Template ☑ View Workflow Template ☑ Modify Workflow Template ☑ Delete Workflow Template

Select Identity Default Roles

Select Identity offers default roles that you can use “as-is” or modify to better match your business requirements.

The following roles are available by default:

End User
All users added to Select identity are granted this role. Users added through Auto Discovery are granted this role on initial login.

An end user is simply a user of Select Identity Services. Accounts with this role have only the entitlements that are granted through registration of a Service. You can change the permissions that all end users have by modifying this role.

This role determines what a user can do through the Self Service pages. See Account Self Service on page 217 for a list of actions.

Approver
An Approver can perform account provisioning actions. This role is automatically granted to users who are assigned an approval task. A user with this role can approve user account additions, removals, or changes.

Select Identity System Administrator
A Select Identity System Administrator has all 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 section of the client enables you to create, modify, and manage the roles that define administrator’s access to the Select Identity system.

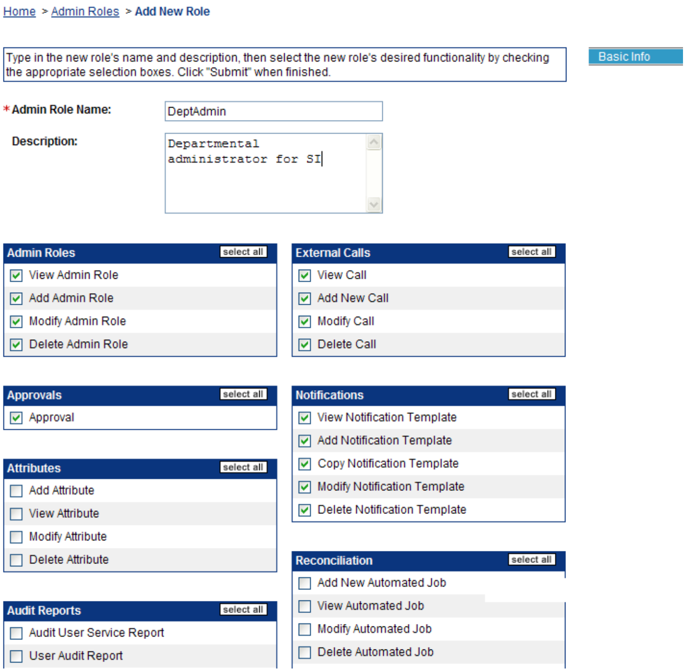
Adding an Admin Role

You can add any number of roles to meet your management needs. Roles are later assigned to users through administrative Services.

Perform the following steps to add a role:

1. From the home page of Admin Roles, click **Add New Admin Role**.

   The Role Definition page displays.



Home > Admin Roles > **Add New Role**

Type in the new role's name and description, then select the new role's desired functionality by checking the appropriate selection boxes. Click "Submit" when finished.

Basic Info

***Admin Role Name:** DeptAdmin

Description: Departmental administrator for SI

Admin Roles select all
- ☑ View Admin Role
- ☑ Add Admin Role
- ☑ Modify Admin Role
- ☑ Delete Admin Role

External Calls select all
- ☑ View Call
- ☑ Add New Call
- ☑ Modify Call
- ☑ Delete Call

Approvals select all
- ☑ Approval

Attributes select all
- □ Add Attribute
- □ View Attribute
- □ Modify Attribute
- □ Delete Attribute

Audit Reports select all
- □ Audit User Service Report
- □ User Audit Report

Notifications select all
- ☑ View Notification Template
- ☑ Add Notification Template
- ☑ Copy Notification Template
- ☑ Modify Notification Template
- ☑ Delete Notification Template

Reconciliation select all
- □ Add New Automated Job
- □ View Automated Job
- □ Modify Automated Job
- □ Delete Automated Job

2. Enter a name for this role in the Role Name field.
3. Enter a description for the role in the Role Description field.
4. Select the actions that you want an administrator with this role to perform by checking the appropriate check boxes. To review each category and its purpose in the system, see Select Identity Capabilities and Actions on page 127.

   If you want to enable all actions within a given category, click **select all**.
5. Click **Submit** to save your settings.

Modifying a Role

If you have permission to do so, you can modify Select Identity administrative roles.

Perform the following steps to modify an administrative role:

1. From the home page of Admin Roles, select the role that you want to modify from the Admin Role drop-down list.
2. Select **Modify Admin Role** from the Actions drop-down list.
3. Click **Submit**. The Role Definition page displays.
   - You can edit the description for this role in the Role Description field.
   - By checking the appropriate check boxes, you can define the actions that you want an administrator with this role to perform. You can deselect the actions that you do not want associated with this role. To review each category and its purpose in the system, see Select Identity Capabilities and Actions on page 127.
   - If you want to enable all actions within a given category, click **select all**.
4. Click **Submit** to save your settings.

Viewing a Role

You can view the actions for a given role.

Perform the following steps to view an administrative role:

1. From the home page of Admin Roles, select the role that you want to view from the Admin Role drop-down list.
2. Select **View Admin Role** from the Actions drop-down list.
3. Click **Submit**. The following information displays:
   - The name for this role
   - A description for the role
   - The actions associated with this role

Deleting a Role

You can delete any administrative role, except the Select Identity System Administrator role. Before deleting a role, make sure that the administrators who were assigned this role are notified.

Perform the following to delete an administrative role:

1. From the home page of Admin Roles, select the role that you want to delete from the Admin Role drop-down list.
2. Select **Delete Admin Role** from the Actions drop-down list.
3. Click **Submit**.
4. You are prompted to confirm the action. Click **OK** to delete the role.

Auto Discovery

The Auto Discovery capability enables you to easily add a large group of your organization's existing users to HP OpenView Select Identity. 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 Discovery** action.

After users are added to Select Identity, entitlements associated with the users are discovered by specifying the resource 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 associated the users to the proper Services. By associating users to Services, you've created an account which can now be maintained through Select Identity's contextual model.

Before you start the Auto Discovery process, it is strongly recommended that you optimize Select Identity for best performance. See Optimizing Select Identity on page 18 for a list of specific optimization settings. For details on configuring these settings and other important settings, see “Optimizing Select Identity” in Chapter 6 of the *HP OpenView Select Identity Installation Guide*.

Auto Discovery Procedure Overview

This chapter describe the process of 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 to perform Auto Discovery tasks.

Define Users and Attributes from an Authoritative Resource

Typically, businesses have an existing authoritative resource that contains account information and attributes for each account. 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). Before building your SPML file, identify your main source of user data and determine your list of attributes to be loaded to Select Identity.

Create 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. To create the SPML format needed for Auto Discovery, 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.
- Programmatically build the file by reading through your resource and writing out a data record for each user.

To see an example of an auto discovery file after the LDIF format to SPML conversion, view the sample files located in the `\SampleXML\Auto-Discovery` directory on the Select Identity product CD.

When creating the input file containing the user attributes, specify the 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>
```

In addition to specifying the operational attribute in the header of the file, you will need to specify two operational attribute values for each add user request. The following sample of the SPML file:

```
<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.

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.

If the UserName attribute is set up with a value generation function, and an Auto Discovery 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.

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>
```

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 Attributes on page 52.

To see an example of an add user request file, refer to the Select Identity product CD in the `\SampleXML` directory.

Create an SPML file Containing Entitlements

After building the SPML file containing your list of users and associated attributes, you will now need to review the resources containing the entitlements associated with your users. User's may have entitlements from multiple resources. To upload these entitlements, a separate SPML file containing the entitlements must be created for each resource. You will need to use one of the methods described in Create an SPML file Containing Users and Attributes on page 136 to create this SPML file.

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. In addition, you will 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>AEE20
0</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 directory.

Check for Service Membership Requirements

Once a user is added, the user can be assigned Service memberships. Based on the user's attributes, a Service membership may be assigned to the user. 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.
- 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.
- a matching attribute value for any attributes in the Service that have a constraint list.

Check the TruAccess.properties File

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.

- `truaccess.batch.inprogresstimeout=18000000`
  `truaccess.batch.ownerkey=0`

  Specifies the attributes for batch processing for the Auto Discovery and Reconciliation functions. Ownerkey defines the ID of the Server from which Select Identity picks up the data file. If you have multiple servers in a cluster and want to dedicate a unique server for reconciliation, enter the unique ID here. If Select Identity can pick up files from multiple servers, use **0**.

- `truaccess.batch.pickuppolicy=1`
  `truaccess.batch.reportdir=c:/temp/reports`

  Specifies the policy to pick up the batch files for the Auto Discovery facility. Values are:

  1: if the `ownerKey` is **0**, which is a generic server ID, Select Identity can pick up the file from any server in the cluster with this ID.

2: If you have a designated server, you can assign a unique server ID (such as ownerKey=999) and have Select Identity pick up data files from that server only.

3: Files are picked up from all servers in the cluster.

-
  ```
  ovsi.ad.rootdir=/opt/si3.3.1/websphere/adroot
  ovsi.ad.backupdir=/opt/si3.3.1/websphere/adbackup
  ovsi.ad.stagingdir=/opt/si3.3.1/websphere/adstaging
  #ovsi.ad.subdir=subdir
  ovsi.ad.userid=2
  ovsi.ad.file.threshold=2
  ```

  These properties specify automatic pickup of Auto Discovery files. If rootdir and backupdir are not provided in the property file, no user-discovery will be scheduled.

  The format of the input batch file is:

  ```
  <resourceName>_<datetime><randomNumber>
  ```

  Please note that the first underscore "_" from the end will be used as a delimeter to identify the resourceName. That is, the resourceName can have embedded underscores as in LDAP_71_<datetime><randomNumber>. Therefore, do not use an underscore "_" in <datetime><randomNumber>.

  Following are descriptions of each property:

  – ovsi.ad.rootdir=/opt/si3.3.1/websphere/adroot

    Specifies the location of Auto Discovery input batch files.

  — ovsi.ad.backupdir=/opt/si3.3.1/websphere/adbackup

    Specifies the location of processed Auto-Discovery batch files.

  — ovsi.ad.stagingdir=/opt/si3.3.1/websphere/adstaging

    Specifies the location of the working directory used for processing the file.

  – #ovsi.ad.subdir=subdir

    Specifies the location of the subdirectory off /opt/si3.3.1/websphere/adroot where the files will be retrieved. This property is optional.

  — ovsi.ad.userid=2

    Specifies sisa (userid 2) as the user running the Auto Discovery job. Defaults to sisa if a number is not provided.

— `ovsi.ad.file.threshold=2`

Indicates the number of Auto Discovery files that will be simultaneously uploaded. The maximum recommendation is two 10K simultaneous files. Defaults to 3 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 will facilitate the Auto Discovery process.

The `TruAccess.properties` file is described in detail in the *HP OpenView Select Identity Installation Guide*.

Upload User Accounts, Attributes, and Entitlements

You can now upload the user accounts, attributes, and entitlements through the Auto Discovery pages. See Scheduling User Discovery on page 144 for a complete procedure.

➤ You can improve the performance of Auto Discovery tasks by breaking large files into smaller ones and running the files in parallel. Performance is significantly improved when running on a multi-CPU server. It is strongly recommended that you run multiple files in parallel when uploading files for Auto Discovery. When doing this, only run files associated with one resource at a time.

Schedule Services Assignment

The **Schedule Services Assignment** action associates newly discovered users with existing Services in Select Identity. To take advantage of Select Identity's Contextual 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 Auto Discovery process. Service assignment should only be done after all user accounts and entitlements have been loaded into Select Identity. All Services should be created before performing this action.

All user accounts that qualify for an existing Service are automatically assigned to the Service. Qualification is based on attribute and entitlement match for each account. An administrator can assign newly created accounts to all or a subset of existing Services. Once Services are assigned, user accounts are maintained using Select Identity's Users capability.

The system goes through each user account and evaluates whether that user is provisioned to the specified Service's resources. The user must be provisioned 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.

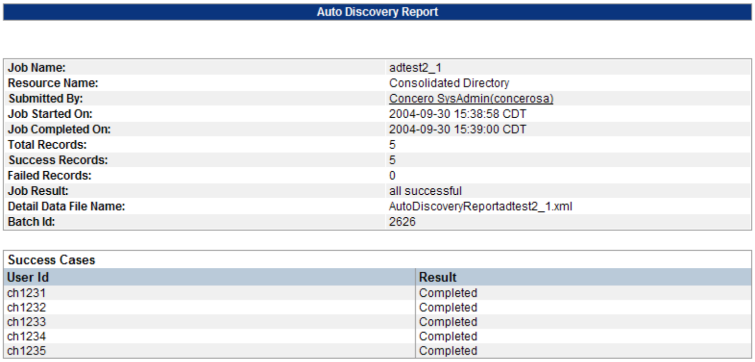
Therefore, Auto Discovery of each resource must be 100% completed before Service Assignment starts.

See Scheduling Services Assignment on page 146 for a complete procedure.

Job Results

After each of the Auto Discovery jobs completes, the creator of the job receives an HTML report. The report lists users that were successfully created and those that failed.

The following is a sample report:



Auto Discovery Report

Job Name:	adtest2_1
Resource Name:	Consolidated Directory
Submitted By:	Concero SysAdmin(concerosa)
Job Started On:	2004-09-30 15:38:58 CDT
Job Completed On:	2004-09-30 15:39:00 CDT
Total Records:	5
Success Records:	5
Failed Records:	0
Job Result:	all successful
Detail Data File Name:	AutoDiscoveryReportadtest2_1.xml
Batch Id:	2626

Success Cases

User Id	Result
ch1231	Completed
ch1232	Completed
ch1233	Completed
ch1234	Completed
ch1235	Completed

You can make any needed corrections and resubmit the file with only those accounts that failed. You will need to create a new job to upload this file in the Select Identity client.

➤ If you are the creator of the job that ran initially, you cannot give the new job the same name. Each job that you create as an administrator must be assigned a unique name.

Scheduling User Discovery

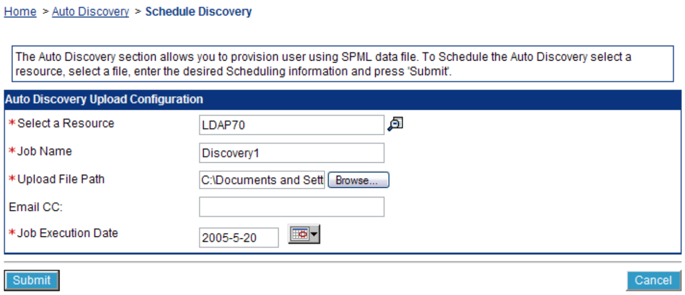
You can configure Select Identity to add user accounts on a specified date. This process enables Select Identity to add account data to the system from a data file that you create. See Create an SPML file Containing Users and Attributes on page 136 for information about creating a data file.

Perform the following steps to schedule user account discovery:

1 From the home page of Auto Discovery, select **Schedule User Discovery** from the Actions drop-down list.

2 Click **Submit**.

The Auto Discovery Configuration page displays.


Home > Auto Discovery > Schedule Discovery
Auto Discovery Upload Configuration
Browse...
Submit
Cancel

The Auto Discovery section allows you to provision user using SPML data file. To Schedule the Auto Discovery select a resource, select a file, enter the desired Scheduling information and press 'Submit'.

*Select a Resource: LDAP70
*Job Name: Discovery1
*Upload File Path: C:\Documents and Sett
Email CC:
*Job Execution Date: 2005-5-20

3 Click 🔍 to search for and select the resource in which you want to locate user accounts.

4 Enter a name for this job in the Job Name field.

5. Click **Browse** to locate and select the data file that you want to upload. See Create an SPML file Containing Users and Attributes on page 136 for information about data files.
6. 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.
7. Click the **Calendar** icon to choose a date for this job to run. The job runs at 12:00 AM on the scheduled day. If you select the current day from the calendar, the job runs immediately.
8. Click **Submit**.

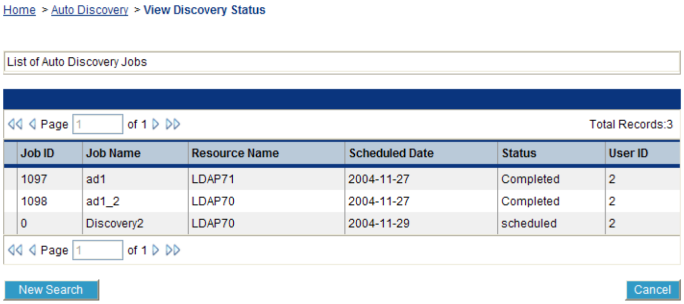
   The job is added and will run when scheduled.

Viewing User Discovery Status

You can view the status of previously scheduled jobs.

Perform the following steps to view job status:

1. From the home page of Auto Discovery, select **View User Discovery Status** from the Actions drop-down list.
2. Click **Submit**. The Search Information page displays.
3. Enter search values for the job name.
4. Enter search values or click 🔍 to locate the resource name.
5. Enter search values for the schedule date.
6. Define how you want to view search results.
7. Click **Submit**. The Search Results page displays.



Home > Auto Discovery > View Discovery Status

List of Auto Discovery Jobs

Page 1 of 1 Total Records:3

Job ID	Job Name	Resource Name	Scheduled Date	Status	User ID
1097	ad1	LDAP71	2004-11-27	Completed	2
1098	ad1_2	LDAP70	2004-11-27	Completed	2
0	Discovery2	LDAP70	2004-11-29	scheduled	2

The jobs that match your search criteria are listed.

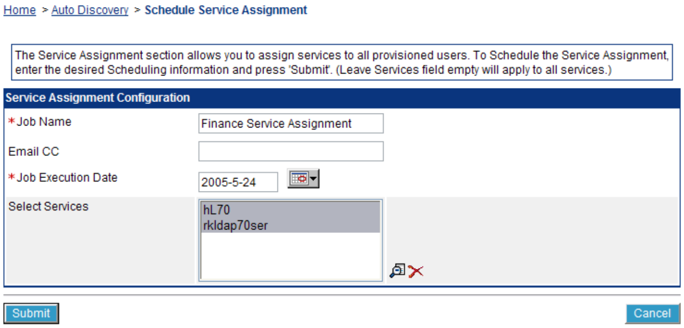
Scheduling Services Assignment

As users are added to the system, you can schedule Service access.

Perform the following steps to schedule Service assignments:

1. From the home page of Auto Discovery, select **Schedule Services Assignment** from the Actions drop-down list.
2. Click **Submit**.

   The Service Assignment Configuration page displays.



Home > Auto Discovery > Schedule Service Assignment

The Service Assignment section allows you to assign services to all provisioned users. To Schedule the Service Assignment, enter the desired Scheduling information and press 'Submit'. (Leave Services field empty will apply to all services.)

Service Assignment Configuration

*Job Name	Finance Service Assignment
Email CC	
*Job Execution Date	2005-5-24
Select Services	hL70 rkldap70ser

3. Enter a name for the job in the Job Name field.
4. 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.

5. Click the **Calendar** icon to choose a date for this job to run. The job runs at 12:00 AM on the scheduled day. If you select the current day from the calendar, the job runs immediately.

6. Click 🔍 to locate and select the Services that you want to assign.

7. Click **Submit**.

   The job is added and will run when scheduled.

Viewing Assignment Status

You can view status for jobs scheduled to assign Services to provisioned users.

Perform the following steps to view Service assignment status:

1. From the home page of Auto Discovery, select **View Assignment Status** from the Actions drop-down list.

2. Click **Submit**. The Search Information page displays.

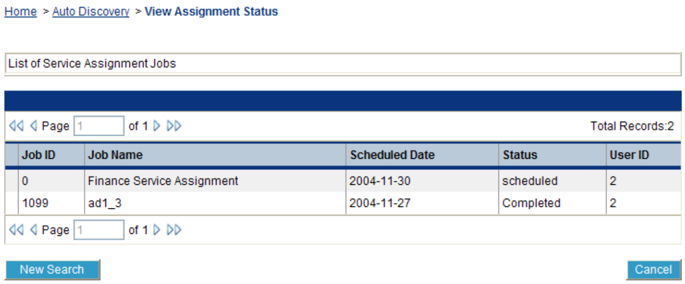
3. Enter search values for the job name.

4. Enter search values for the schedule date.

5. Define how you want to view search results.

6. Click **Submit**.

   The Search Results page displays.



Home > Auto Discovery > **View Assignment Status**

List of Service Assignment Jobs

Page 1 of 1 Total Records:2

Job ID	Job Name	Scheduled Date	Status	User ID
0	Finance Service Assignment	2004-11-30	scheduled	2
1099	ad1_3	2004-11-27	Completed	2

Page 1 of 1

The jobs that match your search criteria are listed.

14

Bulk Add or Move for Accounts

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.

User accounts are uploaded to the system using an SPML data file. The data file maps all Select Identity attributes that you define for a Service to the new accounts. All other fixed entitlements and entitlements granted through rules are automatically assigned.

Bulk Dependencies

Before running a bulk job, ensure that the following dependencies are met:

- Connectors and resources are deployed for systems with which you want to reconcile or upload data.
- All necessary resource and Select Identity attributes are mapped within the connector mapping files and Select Identity Attributes capability.

- One or more Services are created to use the resources with which you want to reconcile data and the default workflow template for bulk jobs (SIBulkOneStageApproval) is associated in the TruAccess.properties file. You can also create and assign a custom template. See the *HP OpenView Select Identity Workflow Studio Guide* for information about workflow templates.

Make sure the following are in place when creating the SPML data file:

- The file name must begin with an underscore (_) if it is used by an automated job. It should be 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 it is used for a one-time task, there are no naming restrictions.
- You can specify the Services to which you want to add users through the job creation pages or in the data file. All of the attributes that are 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.
- 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 that have multiple resources with different resource key fields.
- If you are adding accounts to multiple Services with differing sets of entitlements, create a separate add request for each of the Services.

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 136. 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.

During Select Identity installation, several settings were established in the `TruAccess.properties` file to enable bulk jobs. See the *HP OpenView Select Identity Installation and Configuration Guide* for details about this file and its settings.

➤ You must have the Select Identity system administrator role to perform bulk tasks.

You may need to increase the JTA time-out seconds on WebLogic for bulk jobs to work properly.

Check the Application Server Properties

Set up the necessary parameters in the `TruAccess.properties` file and create relative directories on the application server host.

The following are key properties that you can set in the `TruAccess.properties` file to facilitate the upload process.

```
truaccess.batch.inprogresstimeout=18000000
truaccess.batch.ownerkey=0
```

Specifies the attributes for batch processing for the Auto Discovery, Bulk, and Reconciliation functions. Common batch processing is 0, or you can specify an identifier for a specific application server.

```
truaccess.batch.pickuppolicy=1
truaccess.batch.reportdir=c:/temp/reports
```

Specifies the policy to pick up the batch files. Values are:

1 - common batch only (`truaccess.batch.ownerkey` property is set to 0)
2 - own batch only (must have a unique owner key ID specified in the `truaccess.batch.ownerkey` property)
3 - common and own batch

This file is described in detail in the *HP OpenView Select Identity Installation and Configuration Guide*. See Checking the Application Server Properties on page 201 for more information about bulk and reconciliation-specific property settings.

Create 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. To create the SPML format needed for bulk jobs, 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.
- programmatically build the file by reading through your resource and writing out a data record for each user.

To see an example of using an LDIF format to SPML conversion, view the sample files located in the `\SampleXML\` directory on the Select Identity product CD.

All attributes specified in this file are Select Identity attributes, not resource attributes. The `requestID` for each request should be unique so that it is properly reflected 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 identifier is specified in the `<operationalAttributes xmlns=>` header 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>
```

The“urn:trulogica:concero:2.0#keyFields” operational attributes specify the field in an individual request that should be used to check for the existence of a user in Select Identity. If this field is not provided, no check is performed and the job will generate 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 that you want assigned for each add user request:

```
- <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>
```

If you can specify the Services that you want assigned to users in the following ways:

- Specify the Services in the header section of the file and they will be added to all add requests in the file.
- Specify a group of common Services in the header section of the file and add others that are specific to accounts within the account’s add request (as displayed above). Lower level Services take precedence over those at the header level.
- Do not specify Services in the SPML file and choose them through the job creation pages. You can choose Services for scheduled jobs. See Scheduled Job on page 156 for details.
- If you do not specify Services in the SPML file or through the job creation pages, all accounts in the file are added to all Select Identity Services.

The attributes listed for each account are the required fields that are defined for this particular Service through the Services pages. The attribute name must match the field name exactly. If a required field is missing, an exception is listed in the results file. See Deploying a Service on page 105 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 attributes that are listed are required for access to the Services.

```
- <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>UserName</value>
    </attr>
  </operationalAttributes>
  - <addRequest requestID="1">
    - <operationalAttributes xmlns="">
      - <attr name="urn:trulogica:concero:2.0#serviceName">
          <value>FinanceService</value>
        </attr>
      </operationalAttributes>
    - <attributes xmlns="">
      - <attr name="UserName">
          <value>jimA</value>
        </attr>
      - <attr name="Password">
          <value>abc123</value>
        </attr>
      - <attr name="Email">
          <value>jimA@company.com</value>
        </attr>
      </attributes>
    </addRequest>
  - <addRequest requestID="2">
    - <operationalAttributes xmlns="">
      - <attr name="urn:trulogica:concero:2.0#serviceName">
          <value>FinanceService</value>
          <value>MarketService</value>
        </attr>
      </operationalAttributes>
    - <attributes xmlns="">
      - <attr name="UserName">
          <value>saraH</value>
        </attr>
      - <attr name="Password">
          <value>abc123</value>
        </attr>
      - <attr name="Email">
          <value>saraH@company.com</value>
        </attr>
      </attributes>
    </addRequest>
  </batchRequest>
```

Example: Adding Users to Services with Specified Entitlements

The same user can be added to different Services that rely on common resources. In order for this operation to be successful, the entitlements that you want the user to have across shared resources should be specified within the add request. If this feature is used, the Service name specified in the bulk task can not have '#' as part of its name. In this example, the user name is generated. The following is an example:

```
  <?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

You can now upload the data files including user accounts, attributes, and entitlements through the Bulk pages. See Creating a Bulk Upload Job on page 156 for a complete procedure.

Job Results

After each of the jobs completes, the creator of the job receives an HTML report. The report lists users that were successfully created and those that failed. 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.

➤ If you are the creator of the job that ran initially, you cannot give the new job the same name. Each job that you create as an administrator must be assigned a unique name.

Creating a Bulk Upload Job

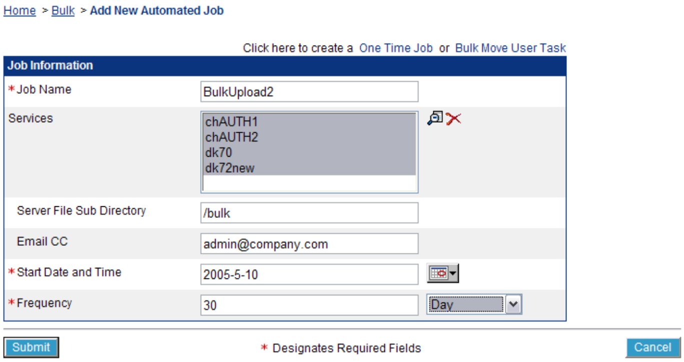
You can create and schedule a job to reconcile data or move users from one context to another. Create an SPML file with the necessary data before performing the following procedures.

Scheduled Job

Perform the following steps to schedule a bulk upload of user accounts to one or more Services:

1 From the home page of Bulk, click **Add New Job**.

The Job Information page displays.



Home > Bulk > Add New Automated Job

Click here to create a One Time Job or Bulk Move User Task

Job Information

*Job Name	BulkUpload2
Services	chAUTH1 chAUTH2 dk70 dk72new
Server File Sub Directory	/bulk
Email CC	admin@company.com
*Start Date and Time	2005-5-10
*Frequency	30 Day

Submit | * Designates Required Fields | Cancel

2 Enter a name for the job in the Job Name field.

3 Click 🔍 to search for and select the Services to which you want to upload users.

4 Select Identity reads data files from the `reconroot` directory. You may have multiple files and multiple jobs to run. If so, enter a subdirectory for this job to reference in the Server File Sub Directory field. This is the directory in which the SPML data file is stored.

If you add a sub directory under `reconroot`, you must also add the same sub directory under the `reconstaging` directory.

5 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 Email CC field.

6 Click the calendar icon to choose a day for the job to start running. If you select today's date, the job runs immediately. The job runs at 12:00 A.M. on all other dates.

7 Enter a value in the Frequency field and select an increment of time from the drop-down list. The frequency determines when Select Identity will pick up the data file from the specified directory.

For example, if you specified a date of 12-15-04 and a frequency of 3 hours, the job will pick up the file and run at 3:00 A.M on December 15.

8 Click **Submit**.

The job is created and runs when scheduled.

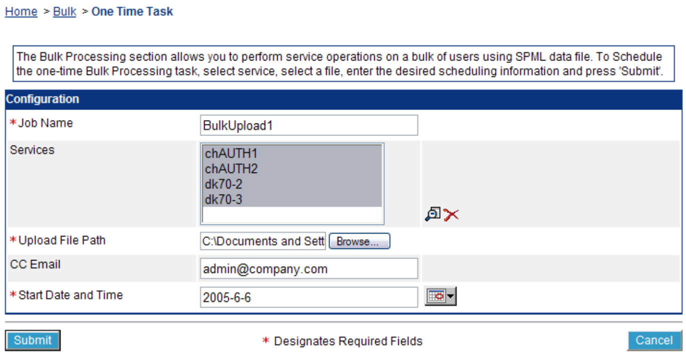
One Time Job

Perform the following steps to run a job once:

1 From the home page of Bulk, click **Add New Job**. The Job Information page displays.

2 At the top of the page, click the **One Time Job** link.

The Job Configuration page displays.



Home > Bulk > One Time Task

The Bulk Processing section allows you to perform service operations on a bulk of users using SPML data file. To Schedule the one-time Bulk Processing task, select service, select a file, enter the desired scheduling information and press 'Submit'.

Configuration

*Job Name	BulkUpload1
Services	chAUTH1 chAUTH2 dk70-2 dk70-3
*Upload File Path	C:\Documents and Sett Browse...
CC Email	admin@company.com
*Start Date and Time	2005-6-6

Submit * Designates Required Fields Cancel

3 Enter a name for the job in the Job Name field.

4 Click 🔍 to search for and select the Services to which you want to upload users.

5 Click **Browse** to select the directory from which you want Select Identity to upload the data file.

6 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 Email CC field.

7 Click the calendar icon 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.

8 Click **Submit**.

The job is created and runs when scheduled.

Bulk Move User Task

Perform the following steps to create a job that moves 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 capability.

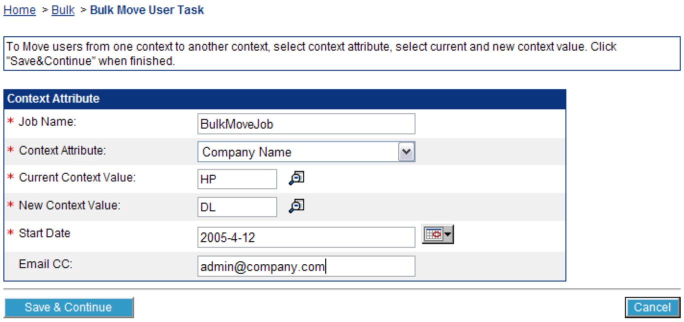
Changing a user's context may remove access to a Service or modify the entitlements that are granted within the Service. A user cannot be added to a Service with this function. A user is added to services as the External call, Rules, and workflow are defined.

➤ To perform this task, you must have administrative rights to the Services that are affected by the context change.

Perform the following steps to create and run the job.

1 From the home page of Bulk, click **Add New Job**. The Job Information page displays.

2 At the top of the page, click the **Bulk Move User Task** link. The Context Attribute page displays.



Home > Bulk > **Bulk Move User Task**

To Move users from one context to another context, select context attribute, select current and new context value. Click "Save&Continue" when finished.

Context Attribute

* Job Name:	BulkMoveJob
* Context Attribute:	Company Name
* Current Context Value:	HP
* New Context Value:	DL
* Start Date	2005-4-12
Email CC:	admin@company.com

3 Enter a name for the job in the Job Name field.

4 Choose the context attribute that you want to change for this group of users from the Context Attribute drop-down list.

5 Click 🔍 to search for and select the the current value for this group of users in the Current Context Value field.

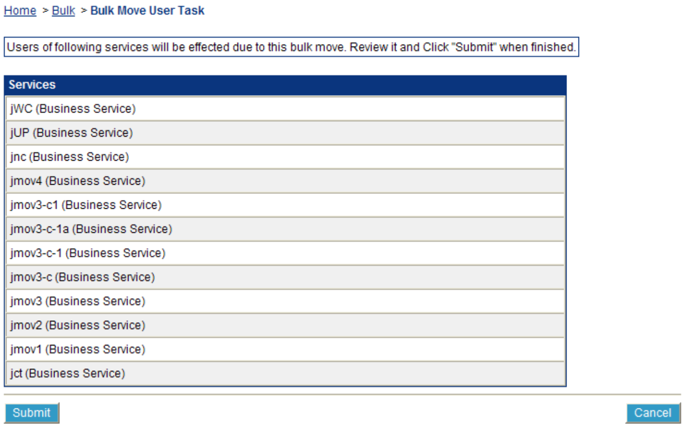
6 Click 🔍 to search for and select the new value in for this group of users in the New Context Value field.

7 Click the calendar icon 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.

8 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 Email CC field.

9 Click **Save & Continue**.

The Services that are affected by the move are displayed.



Home > Bulk > Bulk Move User Task

Users of following services will be effected due to this bulk move. Review it and Click "Submit" when finished.

Services
jWC (Business Service)
jUP (Business Service)
jnc (Business Service)
jmov4 (Business Service)
jmov3-c1 (Business Service)
jmov3-c-1a (Business Service)
jmov3-c-1 (Business Service)
jmov3-c (Business Service)
jmov3 (Business Service)
jmov2 (Business Service)
jmov1 (Business Service)
jct (Business Service)

10 Review the Services and click **Submit**.

The job is created and runs when scheduled.

Viewing an Automated Job

Perform the following steps to view a bulk job:

1 From the home page of Bulk, click 🔍 to search for the job that you want to view. In the Bulk Job Search page, select **Automated** for the Job Type and click **Submit** to select an automated job. Then click **Select**.

2 Select **View Automated Job** from the Actions drop-down list.

3 Click **Submit**. The Job Information page displays.

Modifying an Automated Job

Perform the following steps to modify a bulk job:

1. From the home page of Bulk, click 🔍 to search for the job that you want to modify. In the Bulk Job Search page, select **Automated** for the Job Type and click **Submit** to select an automated job. Then click **Select**.
2. Select **Modify Automated Job** from the Actions drop-down list.
3. Click **Submit**. The Job Information page displays.
4. Change any property, but the job name.
5. Click **Submit**.

Deleting an Automated Job

Perform the following steps to delete a job:

1. From the home page of Bulk, click 🔍 to search for the job that you want to delete. In the Bulk Job Search page, select **Automated** for the Job Type and click **Submit** to select an automated job. Then click **Select**.
2. Select **Delete Automated Job** from the Actions drop-down list.
3. Click **Submit**.
4. You are prompted to confirm the action. Click **OK** to delete the job.

Viewing Task Status

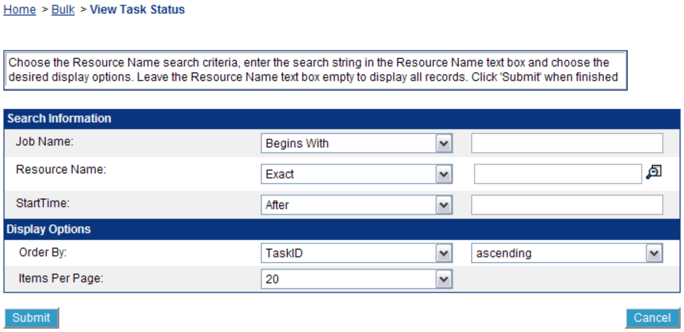
You may have several jobs scheduled and running. Use the View Task Status action to display status for each. Status includes task ID, job name, resource name, start time, end time, status (complete, scheduled, or failed), and the user ID of the person who created the job.

Perform the following steps to view task status:

1 From the home page of Bulk, select **View Task Status** from the Actions drop-down list.

2 Click **Submit**.

The Search page displays.



Home > Bulk > **View Task Status**

Choose the Resource Name search criteria, enter the search string in the Resource Name text box and choose the desired display options. Leave the Resource Name text box empty to display all records. Click 'Submit' when finished

Search Information

Job Name:	Begins With	
Resource Name:	Exact	
StartTime:	After	

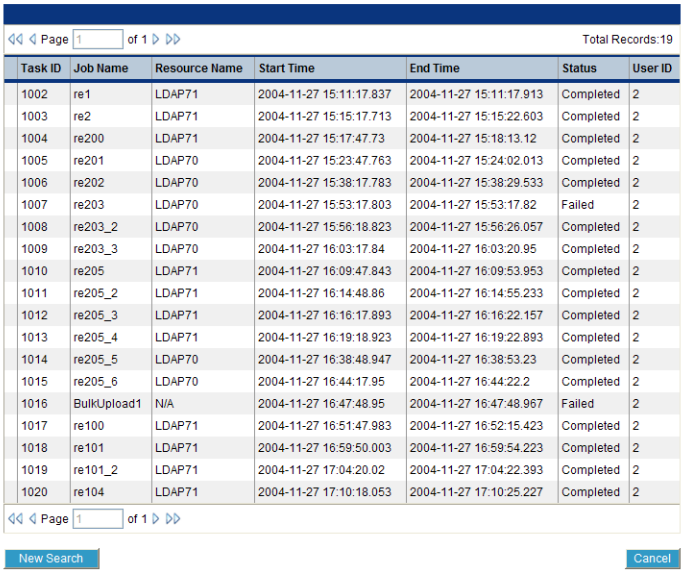
Display Options

Order By:	TaskID	ascending
Items Per Page:	20	

3 Enter your search criteria.

4 Click **Submit**.

The Results page displays.



Page 1 of 1 Total Records:19

Task ID	Job Name	Resource Name	Start Time	End Time	Status	User ID
1002	re1	LDAP71	2004-11-27 15:11:17.837	2004-11-27 15:11:17.913	Completed	2
1003	re2	LDAP71	2004-11-27 15:15:17.713	2004-11-27 15:15:22.603	Completed	2
1004	re200	LDAP71	2004-11-27 15:17:47.73	2004-11-27 15:18:13.12	Completed	2
1005	re201	LDAP70	2004-11-27 15:23:47.763	2004-11-27 15:24:02.013	Completed	2
1006	re202	LDAP70	2004-11-27 15:38:17.783	2004-11-27 15:38:29.533	Completed	2
1007	re203	LDAP70	2004-11-27 15:53:17.803	2004-11-27 15:53:17.82	Failed	2
1008	re203_2	LDAP70	2004-11-27 15:56:18.823	2004-11-27 15:56:26.057	Completed	2
1009	re203_3	LDAP70	2004-11-27 16:03:17.84	2004-11-27 16:03:20.95	Completed	2
1010	re205	LDAP71	2004-11-27 16:09:47.843	2004-11-27 16:09:53.953	Completed	2
1011	re205_2	LDAP71	2004-11-27 16:14:48.86	2004-11-27 16:14:55.233	Completed	2
1012	re205_3	LDAP71	2004-11-27 16:16:17.893	2004-11-27 16:16:22.157	Completed	2
1013	re205_4	LDAP71	2004-11-27 16:19:18.923	2004-11-27 16:19:22.893	Completed	2
1014	re205_5	LDAP70	2004-11-27 16:38:48.947	2004-11-27 16:38:53.23	Completed	2
1015	re205_6	LDAP70	2004-11-27 16:44:17.95	2004-11-27 16:44:22.2	Completed	2
1016	BulkUpload1	N/A	2004-11-27 16:47:48.95	2004-11-27 16:47:48.967	Failed	2
1017	re100	LDAP71	2004-11-27 16:51:47.983	2004-11-27 16:52:15.423	Completed	2
1018	re101	LDAP71	2004-11-27 16:59:50.003	2004-11-27 16:59:54.223	Completed	2
1019	re101_2	LDAP71	2004-11-27 17:04:20.02	2004-11-27 17:04:22.393	Completed	2
1020	re104	LDAP71	2004-11-27 17:10:18.053	2004-11-27 17:10:25.227	Completed	2

Page 1 of 1

If your job is not listed, click **New Search** to refine your search criteria.

15

Users

The Users capability enables you to manage user accounts within your organization. You determine the Services that are made available to each account and the attributes that are relevant. As new users log in to access Services, workflow templates define the process by which user requests are approved and provisioned by Select Identity.

You should be familiar with your company's Service structure. Many of the actions that you perform in the Users section are dependant upon Service, context, and profile attribute information. See Services on page 101 for information about Services and context. See Attributes on page 52 for information about attributes.

You can search for users throughout Select Identity's other functional capabilities. User searches are based on the attributes that make up the user account profile. You can add addtional attributes by which to search for users through the `TruAccess.properties` file. See the *HP OpenView Select Identity Installation and Configuration Guide* for information about the `TruAccess.properties` file

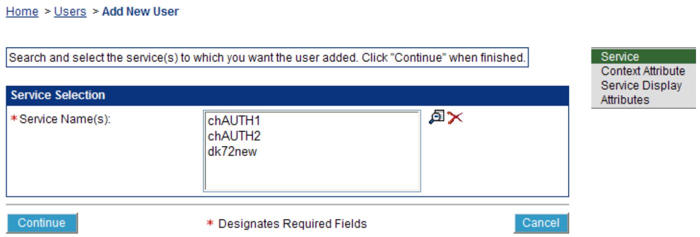
This chapter provides details for all of the actions that you can perform within the Users pages. Access to each of these functional areas is determined by the administrative roles assigned to your account.

Adding a User

To enable access to Services managed by Select Identity, add accounts for users in your customers' organizations.

Perform the following steps to add a new user account:

1 From the home page of Users, click **Add New User**. The Service Selection page displays.



Home > Users > Add New User

Search and select the service(s) to which you want the user added. Click "Continue" when finished.

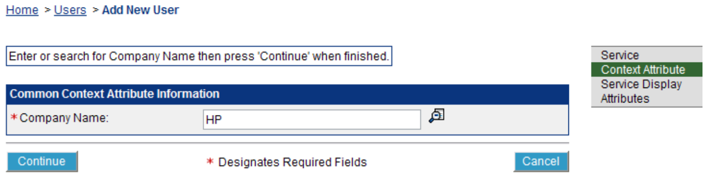
Service Selection

*Service Name(s): chAUTH1
chAUTH2
dk72new

2 Click 🔍 to search for and select the Services that you want to associate to the user. Only 15 Services can be added at one time.

3 Click **Continue** to proceed.

The Common Context Attribute Information page displays. This page may vary based on the Services that you select.



Home > Users > Add New User

Enter or search for Company Name then press 'Continue' when finished.

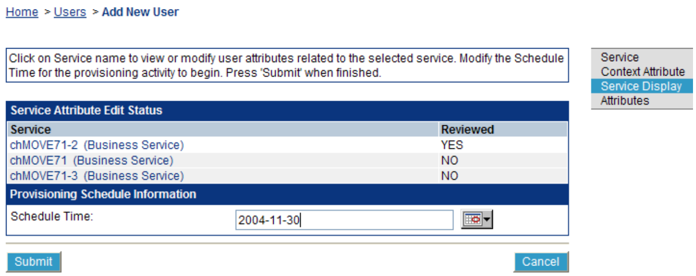
Common Context Attribute Information

*Company Name: HP

4 The context attributes that were defined for each selected Service display to the left. Click 🔍 to search for and select the values that you want to assign to this user. This determines the context grouping in which the account is managed. See Defining Service Roles and Context on page 117 for information about context and context attributes.

5 Click **Continue**.

The Service Display page displays.



Click on Service name to view or modify user attributes related to the selected service. Modify the Schedule Time for the provisioning activity to begin. Press 'Submit' when finished.

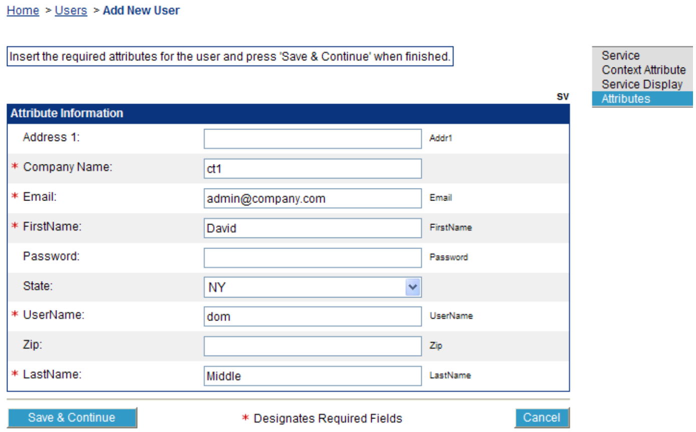
Service Attribute Edit Status

Service	Reviewed
chMOVE71-2 (Business Service)	YES
chMOVE71 (Business Service)	NO
chMOVE71-3 (Business Service)	NO

Provisioning Schedule Information

Schedule Time: 2004-11-30

6 Click a Service link. The attributes required for the Service view display.



Insert the required attributes for the user and press 'Save & Continue' when finished.

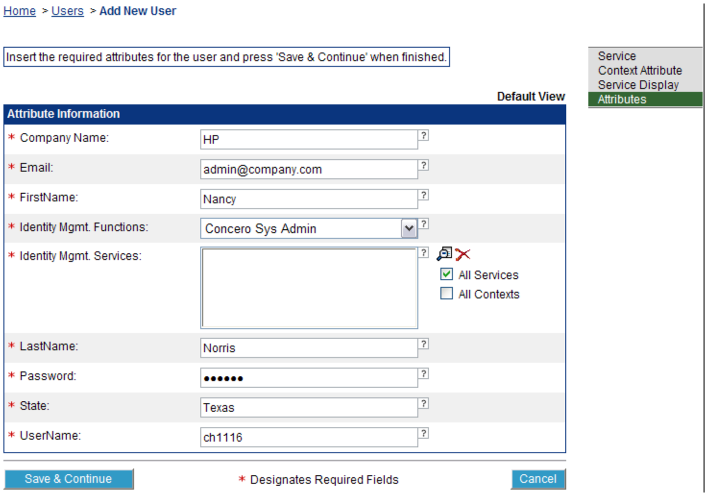
Attribute Information

Address 1:		Addr1
* Company Name:	ct1	
* Email:	admin@company.com	Email
* FirstName:	David	FirstName
Password:		Password
State:	NY	
* UserName:	dom	UserName
Zip:		Zip
* LastName:	Middle	LastName

* Designates Required Fields

7 Enter or choose values for this user account and click **Save & Continue** to proceed.

If this is an Admin Service, the Attribute Information page displays like this:



Home > Users > Add New User

Insert the required attributes for the user and press 'Save & Continue' when finished.

Default View

Attribute Information

* Company Name:	HP
* Email:	admin@company.com
* FirstName:	Nancy
* Identity Mgmt. Functions:	Concero Sys Admin
* Identity Mgmt. Services:	☑ All Services □ All Contexts
* LastName:	Norris
* Password:	••••••
* State:	Texas
* UserName:	ch1116

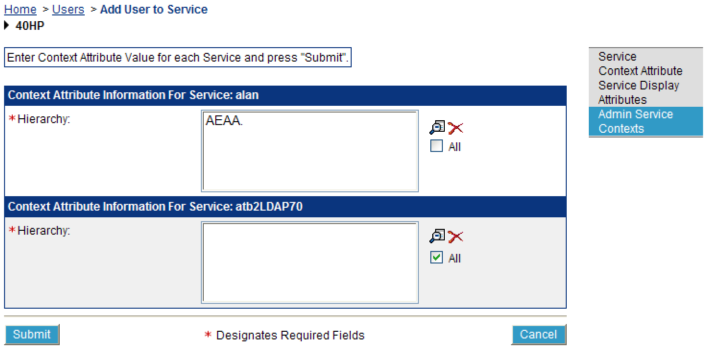
Select the Administrative Roles that you want the user to have. You will also select the Services that this user will manage or you can select:

All Services – which enables the user to manage all Services

All Contexts – which enables the user to manage all contexts defined for each selected Service.

If **All Services** is selected, the Default Context Attribute Information page displays.

If a service or services are selected and the **All Contexts** option is not selected, the Admin Service Contexts page displays.



Home > Users > Add User to Service
40HP

Enter Context Attribute Value for each Service and press "Submit".

Context Attribute Information For Service: alan

*Hierarchy:	AEAA. □ All

Context Attribute Information For Service: atb2LDAP70

*Hierarchy:	☑ All

Click 🔍 to search for and select values for each context attribute or select **All** to manage all contexts for a Service.

> ➤ Selecting the Domain Users entitlement when adding a user to a Service that relies on an Active Directory resource will result in a failed request. The Domain Users entitlement is automatically added by default during provisioning.

8. Click **Submit**. You are returned to the Service Display page.

   If you are assigning multiple Services, you must perform Step 6 through Step 8 for each one.

9. When finished assigning values for each Service, you can schedule the addition of the user or click **Submit** to immediately add the user.

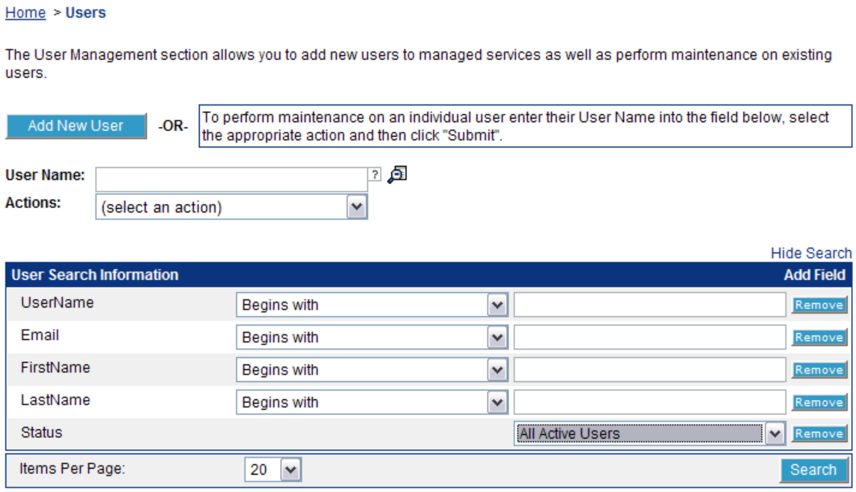
   If you selected an Administrative Service, additional information may be required.

   If you schedule the account addition, the account is added at 12:00 A.M. on the day you select.

The user account remains in the Pending state until it is approved according to the workflow template associated with each Service. The new user will receive email notification with a password when approved.

Searching for a User

The User Search allows you to search for Users within Select Identity based on different criteria. Click 🔍 to display the User Search Information dialog at the bottom of the page.



Home > Users

The User Management section allows you to add new users to managed services as well as perform maintenance on existing users.

To perform maintenance on an individual user enter their User Name into the field below, select the appropriate action and then click "Submit".

User Name:

Actions: (select an action)

User Search Information			Add Field
UserName	Begins with		Remove
Email	Begins with		Remove
FirstName	Begins with		Remove
LastName	Begins with		Remove
Status		All Active Users	Remove

Items Per Page: 20

You can search for users in one of two ways:

- Click the **Search** button without entering any values in the fields to see all available users.
- Enter specific values in one or more fields to filter the amount of users returned. For example, you can search for all users whose User Name begins with “D” AND whose Last Name begins with “A.” An “AND” is always performed on fields that contain values.

  The Status field is selected by default with **All Active Users**, which returns all users with an enabled or disabled status (but not users with a terminated status). You can also select:

  - **Enabled** — Returns only users that are enabled.
  - **Disabled** — Returns only users that are disabled.
  - **Terminated** — Returns only users that have been terminated and no longer exist on Select Identity. You cannot perform any actions with these users.

➤ When entering values in multiple search fields, users are only returned when all criteria is met.

Once you select a row from the results screen (the filtered results), the User Name field is automatically populated so that you can perform an action on the specified user.

The **Add Field** link allows you to add additional fields to the search dialog if fields have been configured to be searchable. See Using Attributes to Facilitate User Searches on page 56 if you wish to add fields other than the default fields as search criteria.

The **Remove** button removes fields from the Search. If you do not wish to use specific fields for searching, you can remove these fields from the screen. If you wish to add a removed field back, click on the **Add Field** link and select the removed field.

The **Hide Search** link removes the User Search Information dialog from the default Users page. To return the Search dialog to the screen, click 🔍 .

Modifying a User Account

You can modify account information for the users in your Service context. You cannot, however, modify the Select Identity user ID or Context value. To move users from one Service context to another, see Moving a User from one Context to Another on page 177 for instructions.

Select Identity allows you to modify a disabled user, by default. A `TruAccess.property` file property, `com.hp.ovsi.modify.disableduser=true`, specifies whether a disabled user can be modified or not. If you do not want to allow disabled users to be modified, you can set the property to `false` or comment this property out.

Perform the following steps to modify a user account:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Modify User** from the Actions drop-down list.
3. Click **Submit**.
4. Select the Service or Services in the Available Service(s) box, for which you want to modify this user's information. Click the right arrow to place the selected Service in the Selected Service(s) box, or select a Service in the Selected Service(s) box you do not want and click the left arrow.

   Only 15 Services can be modified at one time.
5. Click **Continue** to proceed. The Service Display page displays.

6 Click a Service link. The attributes and values for the Service context display.

7 You can modify any available fields.

> It is recommended that you select a view that does not include the password for the DELEGATED Modify User action. This password will not be pushed to any resource.

8 Click **Save & Continue**. The Context Attribute Information page displays if the selected Service is an Admin Service.

9 Select the appropriate value for the context attribute.

10 Click **Submit**.

You are returned to the Service Display page. Select any other Services for which you want to make account modifications and repeat Step 6 through Step 10.

11 When you are finished assigning values for each Service, you can schedule the modification of the account, or click **Submit** for changes to occur immediately.

If you schedule the modification, the account is changed at 12:00 A.M. on the day you select.

Adding a Service to a User Account

You can add Service access to an existing account.

Perform the following steps to add Service access:

1 From the home page of Users, click 🔍 to search for and select a user ID.

2 Select **Add Service** from the Actions drop-down list.

3 Click **Submit**. The Service Selection page displays.

4 Click 🔍 to search for and select the Services to which you want to grant access. Only 15 Services can be added at one time.

5 Click **Continue**. The Context Attribute Information page displays.

6. The context attributes that were defined for each selected Service that you selected display to the left. Click 🔍 to search for and select the values that you want to assign to this user. This determines the context grouping in which the account is managed. See Defining Service Roles and Context on page 117 for information about context and context attributes.
7. Click **Continue**. The Service Display page displays.
8. Click a Service link. The attributes and values for the Service context display.
9. The user profile information populates the available fields for this Service. If necessary, enter attribute values and add Service-specific information.

   You are returned to the Service Display page. Select any other Services for which you want to make account modifications and repeat this process.
10. When finished assigning values for each Service, you can schedule the Service addition, or click **Submit** to immediately add the Service.

    If you schedule the addition, the Service is added at 12:00 A.M. on the day you select.

Enabling or Disabling Service Membership

You can enable or disable Service membership for any user account based on the following requirements:

- You can enable a user on a resource if the resource only belongs to one Service.
- You can disable a user on a resource if the resource does not belong to this user's other existing Services.

If you would like to delete a user account from a Service, see Deleting a Service Membership on page 174.

Perform the following steps to disable or enable Service membership for a user account:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Enable Service Membership** or **Disable Service Membership** from the Actions drop-down list.

3. Click **Submit**.
4. Select the Services for which you want the account enabled or disabled.
5. The request to enable or disable the account is made.

The workflow process assigned to each Service in which the account is managed must be completed before the account is enabled or disabled.

Enabling or Disabling All Services

You can enable or disable all Services for any user account. If you would like to delete a user account from the system, see Terminating a User Account on page 174.

Perform the following steps to disable or enable a user account:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Enable All Services** or **Disable All Services** from the Actions drop-down list.
3. Click **Submit**.
4. The request to enable or disable the account is made.

The workflow process assigned to each Service in which the account is managed must be completed before the account is enabled or disabled.

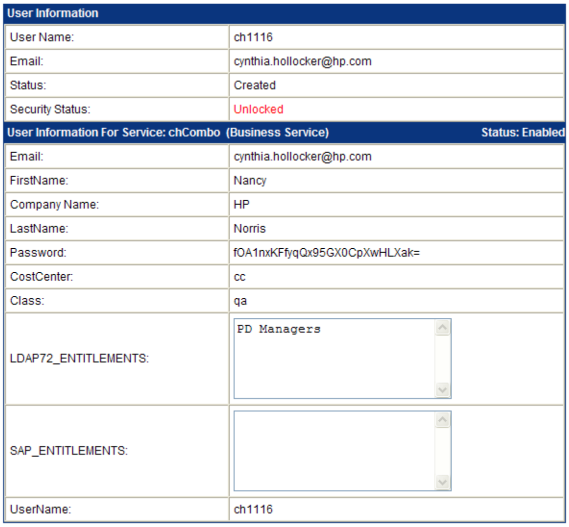
Viewing Service Membership

You can view the attributes and values that make up a user account.

Perform the following steps to view a user account:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **View Service Membership** from the Actions drop-down list.
3. Click **Submit**.

   The User Information page displays.



User Information	
User Name:	ch1116
Email:	cynthia.hollocker@hp.com
Status:	Created
Security Status:	Unlocked
User Information For Service: chCombo (Business Service)	**Status: Enabled**
Email:	cynthia.hollocker@hp.com
FirstName:	Nancy
Company Name:	HP
LastName:	Norris
Password:	fOA1nxKFfyqQx95GX0CpXwHLXak=
CostCenter:	cc
Class:	qa
LDAP72_ENTITLEMENTS:	PD Managers
SAP_ENTITLEMENTS:	
UserName:	ch1116

User profile information for each Service and context is listed for the specified user.

Resetting a User's Password

If a user needs a password reset, you can assign one or have the system generate a new one. The options are dependent on the security policy associated with each Service (see Challenge Response Questions on page 98 for information on specifying the security policy). When this action is complete or approved, the user is sent an email notification.

Perform the following steps to reset an account password:

1. From the home page of User Management, click 🔍 to search for and select a user ID.
2. Select **Reset Password** from the Actions drop-down list.
3. Click **Submit**. The Password Input page displays.
4. Enter a new password in the Password field.
5. Confirm the password.

6. Click **Submit**.
7. The request to change the account password is made.

The workflow process assigned to each Service in which the account is managed must be completed before the account password is changed. The new password will be updated in the Select Identity database and will be pushed to the resources on which the same password is used .

Only reset the user's password using this Reset Password action. If you reset the password using the Modify User action, the password will not be pushed to any resource.

Deleting a Service Membership

To disable an account that might be reinstated later, choose the Disable All Services option. To remove an account from Select Identity and all associated resources, see Terminating a User Account on page 174.

Perform the following steps to delete a user from a Service:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Delete Service Membership** from the Actions drop-down list.
3. Click **Submit**.
4. Select the Services in which you want the account deleted.
5. The request to delete the account is made.

The workflow process assigned to each Service in which the account is managed must be completed before the account is deleted.

Terminating a User Account

Terminating an account removes it from the Select Identity system and all resources associated with the account. The account is disabled for 24 hours before it is removed form the system. If needed, you can enable the account during this time period.

After an account is terminated, it cannot be retrieved. If you want to remove an account from the system but have the account ID available, choose the Delete User action.

Perform the following steps to delete a user from the Select Identity system:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Terminate User** from the Actions drop-down list.
3. Click **Submit**.
4. The request to terminate the account is made.

The account is disabled for a 24-hour period before it is removed from Select Identity and associated resources. This value is configurable through the `TruAccess.properties` file, which is described in the *HP OpenView Select Identity Installation Guide*.

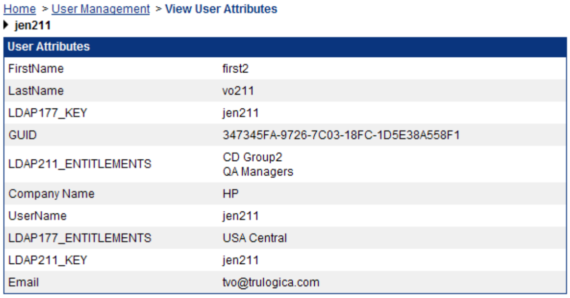
Viewing Account Attributes

You can view the attributes and values associated with an account.

Perform the following steps to view account attributes:

1. From the home page of Users, click 🔍 to search for an select a user ID.
2. Select **View User Attributes** from the Actions drop-down list.
3. Click **Submit**.

   The Attribute Information page displays.



Home > User Management > View User Attributes

▸ jen211

User Attributes	
FirstName	first2
LastName	vo211
LDAP177_KEY	jen211
GUID	347345FA-9726-7C03-18FC-1D5E38A558F1
LDAP211_ENTITLEMENTS	CD Group2 QA Managers
Company Name	HP
UserName	jen211
LDAP177_ENTITLEMENTS	USA Central
LDAP211_KEY	jen211
Email	tvo@trulogica.com

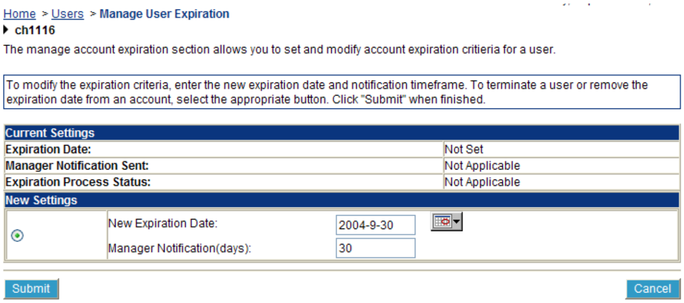
Managing User Account Expiration

You can change the schedule for the expiration of user accounts once the termination process starts.

Perform the following steps to manage the expiration of a user account:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Manage User Expiration** from the Actions drop-down list.
3. Click **Submit**.

   The Expiration Settings page displays.



Home > Users > **Manage User Expiration**

▸ **ch1116**

The manage account expiration section allows you to set and modify account expiration critieria for a user.

To modify the expiration criteria, enter the new expiration date and notification timeframe. To terminate a user or remove the expiration date from an account, select the appropriate button. Click "Submit" when finished.

Current Settings	
Expiration Date:	Not Set
Manager Notification Sent:	Not Applicable
Expiration Process Status:	Not Applicable

New Settings

●	New Expiration Date:	2004-9-30
	Manager Notification(days):	30

4. Click the calendar icon to select a new date for account expiration, or enter a date in the form of yyyy-mm-dd.
5. If you wish to change the number of days a manager is notified before the account expires, replace the default 30 days with the new number.

   The minimum number of days allowed to notify a manager is 1 day.

When the expiration date arrives, the user is terminated from both Select Identity and the resource (if the flag for truaccess.disabled=FALSE in the TruAccess.properties file — see “Configuring TruAccess.properties” in the *HP OpenView Select Identity Installation Guide* for more information). Otherwise, the user is first disabled on the expiration date and then terminated the next day.

6. Click **Submit**.

You can change or remove the expiration date or terminate the user immediately, by opening the Expiration Settings page again (repeat Steps 1 - 3) and changing the settings.

Moving a User from one Context to Another

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 Move User Task on page 158 for details.

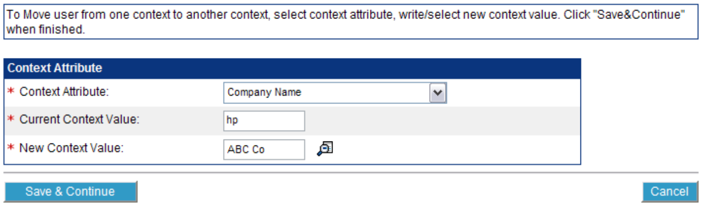
Move User automatically adds entitlements and other attributes to a user when the context value is changed. Existing Services for the user are evaluated to determine what new entitlements or attributes are given to the the user.

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 easily 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.

Perform the following to move a user:

1. From the home page of Users, click 🔍 to search for and select a user ID.
2. Select **Move User** from the Actions drop-down list.
3. Click **Submit**.

   The Context Attribute page displays.



To Move user from one context to another context, select context attribute, write/select new context value. Click "Save&Continue" when finished.

Context Attribute

* Context Attribute:	Company Name
* Current Context Value:	hp
* New Context Value:	ABC Co

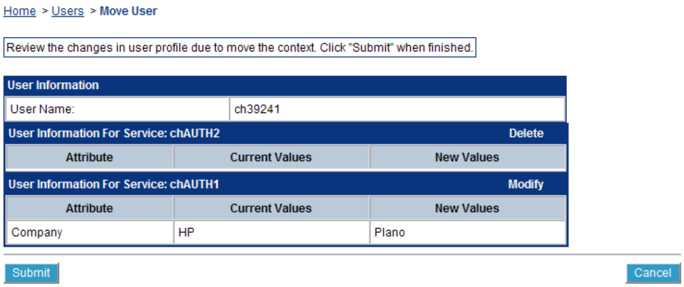
4 Choose the context attribute that you want to change from the Context Attribute drop-down list.

The current context attribute displays in the Current Context Attribute field.

5 Enter the current context value in the Current Context Value field.

6 Enter the new context value in the New Context Value field or click 🔍 to search for and select the value.

7 Click **Submit**. The User Information page displays.



Home > Users > **Move User**

Review the changes in user profile due to move the context. Click "Submit" when finished.

User Information		
User Name:	ch39241	
User Information For Service: chAUTH2		**Delete**
Attribute	**Current Values**	**New Values**
User Information For Service: chAUTH1		**Modify**
Attribute	**Current Values**	**New Values**
Company	HP	Plano

This page displays the following information:

- Delete — New context value is not in the service context. 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 matched with the service context. In this case, the user is modified in the service — all the user's information remains the same except for the context attribute value.

8 Review the information and click **Submit** when finished. The request is processed.

Managing User's Entitlements through Rules

You can associate entitlements and attributes to a user when adding the user to a Service. The entitlements are usually associated to the Service Role in the Service, and the user is given entitlements based on his or her context.

However, you may want to enforce a rule which changes the user's entitlements based on an event such as the addition or modification of an account.

Select Identity enables you to implement a specific rule based on changes made to a user's attribute. For example, if a user's job code is changed through a modification action, entitlement rules can be implemented to change the user's entitlements based on the new job code. The old entitlement associated with the previous job code can be deleted and the user receives a new entitlement based on the new job code. Entitlement rules are enforced through external calls using Select Identity's Workflow Engine.

See a complete example of this scenario and how to implement an entitlement rule using workflow in the *HP OpenView Select Identity Workflow Studio Guide*.

16

Approvals

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. The approval process for account requests or account changes can require multiple administrators or a single administrator, depending on your business and security requirements.

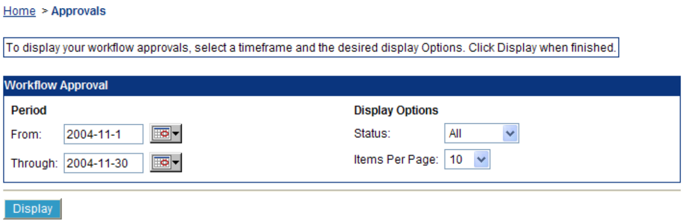
The Approvals capability enables you to approve or reject requests that are pending. You will receive email notification when a request is pending your approval.

➤ An approver added to the system after a set of requests are made will not have access to the existing requests. The new approver will have access to any requests made after his or her account is enabled within Select Identity.

Perform the following steps to approve or reject a request:

1 From the home page of Approvals, choose a date range from the Period options and one of the following account status options from the Display Options fields:

   All
   Pending
   Approved - Any Admin
   Approved - Self Only
   Rejected - Any Admin
   Rejected - Self Only



Home > Approvals

To display your workflow approvals, select a timeframe and the desired display Options. Click Display when finished.

Workflow Approval

Period

From: 2004-11-1

Through: 2004-11-30

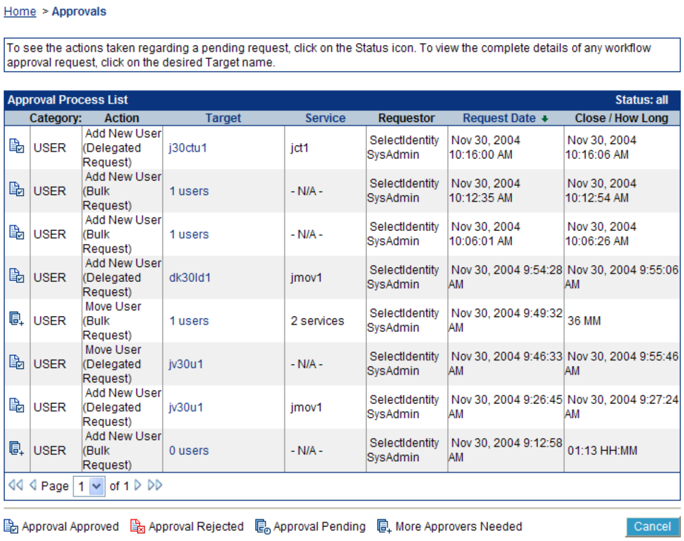
Display Options

Status: All

Items Per Page: 10

2 Select the number of items per page that you want to view from the Items Per Page drop-down list.

3 Click **Display.** The Approval Process List displays.



Home > Approvals

To see the actions taken regarding a pending request, click on the Status icon. To view the complete details of any workflow approval request, click on the desired Target name.

Approval Process List Status: all

	Category:	Action	Target	Service	Requestor	Request Date	Close / How Long
✓	USER	Add New User (Delegated Request)	j30ctu1	jct1	SelectIdentity SysAdmin	Nov 30, 2004 10:16:00 AM	Nov 30, 2004 10:16:06 AM
✓	USER	Add New User (Bulk Request)	1 users	- N/A -	SelectIdentity SysAdmin	Nov 30, 2004 10:12:35 AM	Nov 30, 2004 10:12:54 AM
✓	USER	Add New User (Bulk Request)	1 users	- N/A -	SelectIdentity SysAdmin	Nov 30, 2004 10:06:01 AM	Nov 30, 2004 10:06:26 AM
✓	USER	Add New User (Delegated Request)	dk30ld1	jmov1	SelectIdentity SysAdmin	Nov 30, 2004 9:54:28 AM	Nov 30, 2004 9:55:06 AM
+	USER	Move User (Bulk Request)	1 users	2 services	SelectIdentity SysAdmin	Nov 30, 2004 9:49:32 AM	36 MM
✓	USER	Move User (Delegated Request)	jv30u1	- N/A -	SelectIdentity SysAdmin	Nov 30, 2004 9:46:33 AM	Nov 30, 2004 9:55:46 AM
✓	USER	Add New User (Delegated Request)	jv30u1	jmov1	SelectIdentity SysAdmin	Nov 30, 2004 9:26:45 AM	Nov 30, 2004 9:27:24 AM
+	USER	Add New User (Bulk Request)	0 users	- N/A -	SelectIdentity SysAdmin	Nov 30, 2004 9:12:58 AM	01:13 HH:MM

✓ Approval Approved ✗ Approval Rejected ◷ Approval Pending + More Approvers Needed

You can sort information by user name, Service, or request.

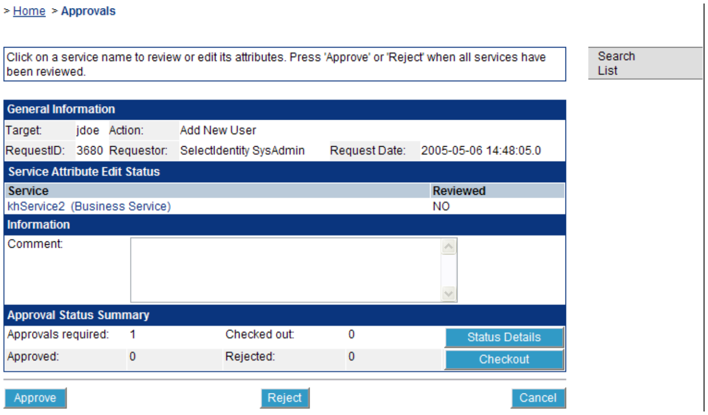
- Click the **Target** heading at the top of the table to sort by user name.
- Click the **Service** heading at the top of the table to sort by Service.
- Click the **Request Date** heading at the top of the table to sort by workflow dates.

The icons to the left show the status of the account.

- ✓ indicates that the request is approved.
- ✗ indicates that the request is rejected.

- 📄 indicates that the request is pending.
- 📄 indicates that there are more approvers needed.

4 To review a user account, click the target account name. If the user you selected is Pending, the following Service Attribute Edit page displays.



> Home > Approvals

Click on a service name to review or edit its attributes. Press 'Approve' or 'Reject' when all services have been reviewed.

Search List

General Information

Target: jdoe Action: Add New User

RequestID: 3680 Requestor: SelectIdentity SysAdmin Request Date: 2005-05-06 14:48:05.0

Service Attribute Edit Status

Service	Reviewed
khService2 (Business Service)	NO

Information

Comment:

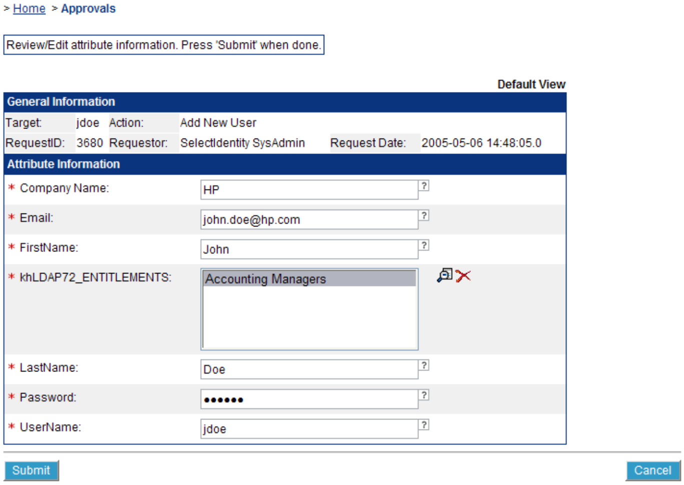
Approval Status Summary

Approvals required:	1	Checked out:	0	Status Details
Approved:	0	Rejected:	0	Checkout

5 You can add text in the Comment box, which will display on the Request Status page. The text can also be sent in emails.

If the user is approved, continue to the next step.

6 Click the Service name to review the account details. The account details page displays.



> Home > Approvals

Review/Edit attribute information. Press 'Submit' when done.

Default View

General Information

Target: jdoe Action: Add New User

RequestID: 3680 Requestor: SelectIdentity SysAdmin Request Date: 2005-05-06 14:48:05.0

Attribute Information

* Company Name:	HP
* Email:	john.doe@hp.com
* FirstName:	John
* khLDAP72_ENTITLEMENTS:	Accounting Managers
* LastName:	Doe
* Password:	••••••
* UserName:	jdoe

7 Some values may be editable. These values are defined in the Service view. Click **Submit**.

8 You are returned to the Service Attribute Edit page.

9 Click **Approve** to approve the account, or **Reject** to reject it.

17

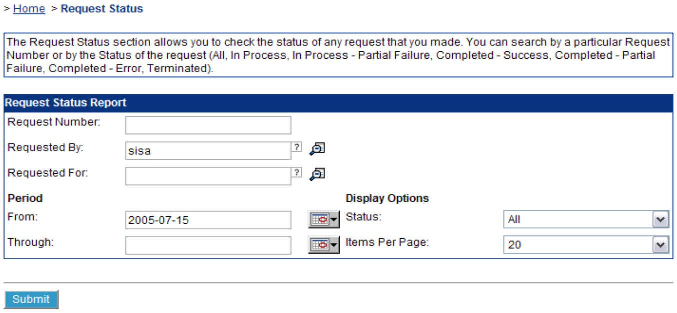
Request Status

The Request Status capability enables you to view the complete transaction status for account events within HP OpenView Select Identity. Account additions, changes, or removals must have a workflow template attached. The workflow process must complete before the request is approved by the system.

Request Status enables you to view the status of account events based on the assigned workflow process. If the workflow template has multiple activities that are grouped into a block, the status of those activities can be viewed.

By default, only requests that the admin is authorized to view are returned. This default is set using the `com.hp.ovsi.parentrequestlist.contextcheck=true property` in the `TruAccess.properties` file.

Perform the following steps to request account status:



> Home > Request Status

The Request Status section allows you to check the status of any request that you made. You can search by a particular Request Number or by the Status of the request (All, In Process, In Process - Partial Failure, Completed - Success, Completed - Partial Failure, Completed - Error, Terminated).

Request Status Report

Request Number:			
Requested By:	sisa		
Requested For:			
Period		**Display Options**	
From:	2005-07-15	Status:	All
Through:		Items Per Page:	20

Submit

1 From the home page of Request Status, choose a date range from the Period options. The From: date is filled in by default.

The default value is 7 days prior to the current date. For example, if today is 2005-07-14, the From: field will display 2005-07-07.

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 will attempt to retrieve all the requests.

2 Choose an account status (**All**, **In Process**, **In Process-Partial Failure**, **Completed-Success**, **Completed-Partial Success**, **Completed-Error**, **Terminated**) from the Display Options fields.

3 If you want the status for a single request and know the request number, enter the number in the Request Number field.

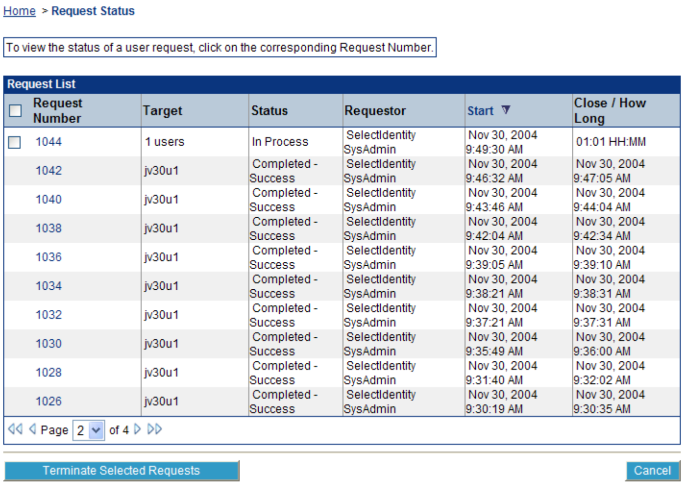
4 If you want the status for requests by a specific Requestor (**Requested By**), and/or by a specific user the request is for (**Requested For**), enter the UserName code if you know it, or click 🔍 to search for and select the user name.

The Requested For search does not include users submitted in a Bulk Request. This search is also not applicable for a Deleted User, a Deleted Admin or a User who has not been created in Select Identity.

5 Select the number of items per page that you want to view from the Items Per Page drop-down list.

6 Click **Submit**.

The Request Status results are displayed.



Home > **Request Status**

To view the status of a user request, click on the corresponding Request Number.

Request List

□ Request Number	Target	Status	Requestor	Start ▼	Close / How Long
□ 1044	1 users	In Process	SelectIdentity SysAdmin	Nov 30, 2004 9:49:30 AM	01:01 HH:MM
1042	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:46:32 AM	Nov 30, 2004 9:47:05 AM
1040	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:43:46 AM	Nov 30, 2004 9:44:04 AM
1038	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:42:04 AM	Nov 30, 2004 9:42:34 AM
1036	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:39:05 AM	Nov 30, 2004 9:39:10 AM
1034	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:38:21 AM	Nov 30, 2004 9:38:31 AM
1032	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:37:21 AM	Nov 30, 2004 9:37:31 AM
1030	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:35:49 AM	Nov 30, 2004 9:36:00 AM
1028	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:31:40 AM	Nov 30, 2004 9:32:02 AM
1026	jv30u1	Completed - Success	SelectIdentity SysAdmin	Nov 30, 2004 9:30:19 AM	Nov 30, 2004 9:30:35 AM

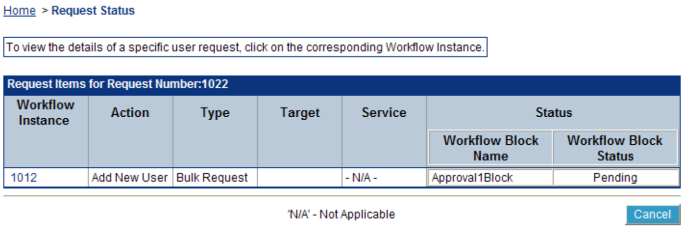
7 You can mouse over a requestor to view the user name and email.

If you want to terminate an open request, select the box next to the request number and click the **Terminate Selected Requests** button.

If a request has failed, you can click the **Manual Retry** button to resubmit the request.

You can sort requests by start date or click on a request number to view request status.

Status for that request displays.



Home > **Request Status**

To view the details of a specific user request, click on the corresponding Workflow Instance.

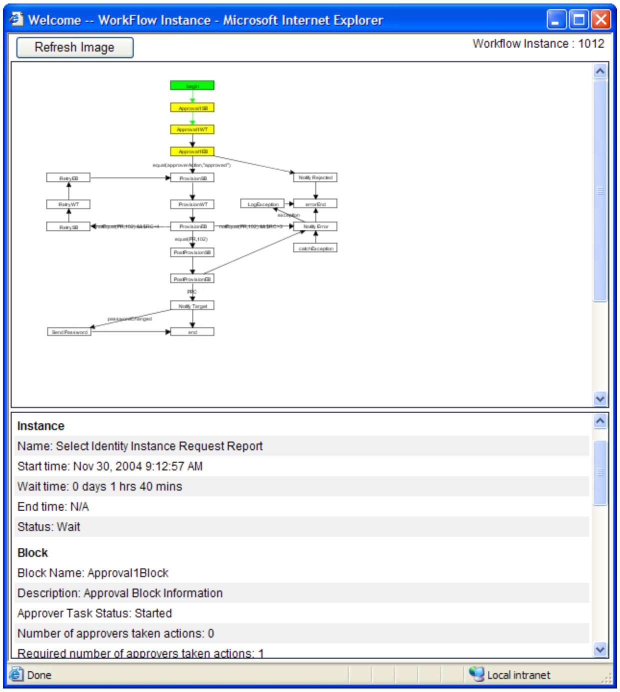
Request Items for Request Number:1022

Workflow Instance	Action	Type	Target	Service	Status	
					Workflow Block Name	Workflow Block Status
1012	Add New User	Bulk Request		- N/A -	Approval1Block	Pending

'N/A' - Not Applicable

8 Click on the workflow instance to view the approval process for the request.

The workflow template displays.



Workflow Instance : 1012

Instance

Name: Select Identity Instance Request Report

Start time: Nov 30, 2004 9:12:57 AM

Wait time: 0 days 1 hrs 40 mins

End time: N/A

Status: Wait

Block

Block Name: Approval1Block

Description: Approval Block Information

Approver Task Status: Started

Number of approvers taken actions: 0

Required number of approvers taken actions: 1

18

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 capability, changes may occur outside of Select Identity. When this occurs, you can configure 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, you may want to ensure that an attribute, such as Last Name, is changed in Select Identity only if the change occurs in a human resources application (an 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 to perform Reconciliation tasks..

Reconciliation Procedure Overview

Before you start the Reconciliation process, it is strongly recommended that you optimize Select Identity for best performance. See Optimizing Select Identity on page 18 for a list of specific optimization settings. For details on configuring these settings and other important settings, see "Optimizing Select Identity" in Chapter 6 of the *HP OpenView Select Identity Installation Guide*.

To perform reconciliation tasks, you need to determine the method that will be 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.

Regardless of the method you use, you follow the same sequence of steps to perform reconciliation. You will want to identify the following before starting the reconciliation process:

1. The authoritative and non-authoritative resources used in reconciliation.
2. The user's unique id and attributes from a resource participating in reconciliation.
3. The entitlements from a resource associated with each user account involved in reconciliation.
4. The attributes to be synchronized across various resources.
5. Any reconciliation rules associated with the addition of accounts from authoritative resources.

Using the Interface Reconciliation Capability

If you are planning to use reconciliation through the Select Identity interface, you will need to perform the following:

- Add all resources and specify an authoritative resource. See Deploying a Resource on page 43 for details.

- Identify and map the attributes to be updated in Select Identity accounts by mapping specific Select Identity attributes to resource attributes in the Authoritative Resource. This can be done by using the Modify Resource Attributes Mapping feature in the Resources capability or by using the Attributes capability. See Modifying Resource Attribute Mapping on page 50 and Adding and Mapping an Attribute on page 57 for details.
- Map any attributes from non-authoritative resources that need to be maintained in Select Identity. If you want an attribute to be added from a non-authoritative resource, that attribute must be identified as authoritative through the Attributes capability. See Adding and Mapping an Attribute on page 57 for details.
- 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 too will contain add, modify, and delete requests.

Using an Agent or Web Service Interface

You may want to programmatically run the reconciliation function. 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:

- Create resources and attributes as described inUsing the Interface Reconciliation Capability.
- 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 CD for examples of Web Services requests.
- Invoke the Web Service from an agent, utility, or another web service.

See the *HP OpenView Select Identity Web Service Developer Guide* for 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 with which you want to reconcile data.
- All necessary resource and Select Identity attributes are mapped within the connector mapping file, which is designated when adding a resource.
- All Select Identity attributes that will be updated are mapped to the appropriate resource attributes using the Attributes capability or the Modify Resource Attributes Mapping feature in the Resources capability.
- 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 *HP OpenView Select Identity Workflow Studio Guide* for information about workflow templates.
- Reconciliation events must be in the Service.
- 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.

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 Adding and Managing System Resources on page 42 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 are checked to determine if Service access should be given. See Using Reconciliation Rules on page 194 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 authoritative on a non-authoritative resource. By doing this, you are telling Select Identity to synchronize with the changes to that attribute on the non-authoritative resource. In this scenario, the authoritative attribute will always be maintained in Select Identity when changes are made to the attribute on the non-authoritative resource.

If, however, the attribute changed on the non-authoritative resource and the attribute was not designated as authoritative, the following two options are available:

- Use the resynchronization feature, which is set in the `TruAccess.properties` file. In this case:

  a Select Identity will reject the attribute change. SI and any other resources will not be updated with the attribute value.

  b Select Identity will then push the correct value back to the resource where the non-authoratative change was received from. Select Identity and all resources will be synchronized.

  c Set the `TruAccess.properties` settings as follows:

  ```
  si.reconciliation.resync.LDAP70=true
  ```

  The reconciliation provisioning back feature is enabled for resource LDAP70.

  ```
  truaccess.fixedtemplate.recon.resync.LDAP70=Reconciliation
  DefaultProcess
  ```

  Default Workflow used for reconciliation provisioning back feature.

  ```
  truaccess.fixedtemplate.recon.resync=ReconciliationDefault
  Process
  ```

  Workflow used for reconciliation provisioning back feature of resource LDAP70.

- If you do not activate this feature, the following will happen when a non authoritative attribute is received from a non authoritative resource:

  a SI will reject the attribute change. SI and any other resources will not be updated with the attribute value.

  b However, now SI and all other resources will be out of sync with the Non Authoritative Resource the change was received from.

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's 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 authoritative to enable an override of an existing value. Authoritative attributes can be set using the Modify Resource Attributes Mapping feature in the Resources capability.
- Attributes that are mapped to multiple resources will automatically be synchronized 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.

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. For example, you may have a business rule stating that all employees hired into the IT department are added to Active Directory. In this case, you can create a 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 would create a Service that contains the Active Directory resource and assign the user to the Service inside the rule based on an attribute value and a conditional parameter, such as `equal`.

Rules are defined in XML and are uploaded to Select Identity through the Rules capability. Each resource can have one defined reconciliation rule for this purpose and the rule ID in the file must be named *`ResourceName`*`_ReconRule`. Reconciliation Rules are only evaluated when an add user account request comes in from an authoritative resource. 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 Service for which they are qualified. For more information about Rules, see Rules on page 83.

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 Creating Reconciliation Rules on page 245.

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.

Service Membership Requirements

Once a user is added or modified through reconciliation, the user's Service memberships are evaluated as a result of the change. Based on the changes to the user's attributes, a Service membership may be assigned to or removed from the user. 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.
- 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.
- a matching attribute value for any attributes in the Service that have a constraint list.

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.

Changes to a user's attributes during reconciliation do not cause provisioning in the resource to occur unless

- 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.

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 Checking the Application Server Properties on page 201 for reconciliation specific settings.

Jobs that are not automated can use any naming convention.

Create 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. 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.

- 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 Select Identity product CD.

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 will need to 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.

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.

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>
```

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 example below, `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>
```

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.

If you need to have multiple values for an attribute within Select Identity, you can use the following syntax:

```
<attr name="name">
    <value>value1</value>
    <value>value2</value>
</attr>
```

Where “name” is mapped to the Select Identity attribute.

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 Attributes on page 52.

To see sample request files, refer to the Select Identity product CD in the `\SampleXML\Reconciliation` directory.

Create 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. In addition, you will 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.

Checking the Application Server Properties

Reconciliation relies on settings that are 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
truaccess.recontimer.startdelay=30
truaccess.recontimer.timeinterval=30
truaccess.recon.task.check.threshold=3
truaccess.recon.check_serviceassignment_authadd=false

#The attributes for batch processing
truaccess.batch.inprogresstimeout=18000000
truaccess.batch.ownerkey=0

#Policy to pick up the batch
#1 - common batch only, 2 - own batch only, 3 - common and own batch
truaccess.batch.pickuppolicy=1
truaccess.batch.reportdir=c:/temp/reports

#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=ReconciliationDefaultProcess

truaccess.fixedtemplate.recon_enable=ReconciliationDefaultProcess
truaccess.fixedtemplate.recon_terminate=ReconciliationDefaultPocess
truaccess.fixedtemplate.recon_disable=ReconciliationDefaultProcess
truaccess.fixedtemplate.recon_disable_terminate=ReconciliationDefaultProcess

  # Perform SI Update if
  # 1 -- all provisioning activities are successful
  # 2 -- corresponding provisioning activity is successful
  # 3 -- always

  truaccess.reconcliation.postprovpolicy=2
  # Perform SI Update if
  # 1 -- all provisioning activities are successful
  # 2 -- corresponding provisioning activity is successful
  # 3 -- always

  #The reconciliation provisioning back feature is enabled for
  #resource LDAP70.
  si.reconciliation.resync.LDAP70=true

  #Default Workflow used for reconciliation provisioning back
  #feature.
  truaccess.fixedtemplate.recon.resync.LDAP70=ReconciliationDefaultProcess

  #Workflow used for reconciliation provisioning back feature of
  #resource LDAP70.
  truaccess.fixedtemplate.recon.resync=ReconciliationDefaultProcess
```

The following table explains each property in the file.

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.recontimer.startdelay`	Yes	Default = 30. No less than **30** seconds recommended	The initial delay to start the reconciliation task timer.
`truaccess.recontimer.timeinterval`	Yes	Default = 30. No less than **30** seconds recommended	The interval for next scan of reconciliation timer.
`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.

Property	**Required**	**Default**	**Description**

`truaccess.recon.`
`check_service`
`assignment_authadd`
	No	**False**	Determines if a Service assignment check should be performed when adding users from an authoritative resource.

`truaccess.batch.` `inprogresstimeout`	Yes	**18000000** seconds	The time-out for when an in-progress batch can be processed again.
`truaccess.batch.` `ownerkey`	Yes	Default = 0	Defines the ID of the Server from which Select Identity picks up the data file. If you have multiple servers in a cluster and want to dedicate a unique server for reconciliation, enter the unique ID here. If Select Identity can pick up files from multiple servers, use **0**.
`truaccess.batch.pick` `uppolicy`	Yes	Default = 1. Used with the `ownerKey` property for clustered environments.	**1**: if the `ownerKey` is 0, which is a generic server ID, Select Identity can pick up the file from any server in the cluster with this ID. **2**: If you have a designated reconciliation server, you can assign a unique server ID (such as `ownerKey=999`) and have Select Identity pick up data files from that server only. **3**: Files are picked up from all servers in the cluster.

Property	Required	Default	Description
`truaccess.batch.reportdir`	No	None	The directory to store report XML for reconciliation, auto discovery, and Service assignment. This report is sent to the administrator who created the job.
`truaccess.fixedtemplate.reconciliation`	Yes	None	The default workflow for reconciliation add, modify, and delete actions.
`truaccess.fixedtemplate.recon_add`	No	**truaccess.fixedtemplate.reconciliation**	The workflow for reconciliation add tasks.
`truaccess.fixedtemplate.recon_modify`	No	**truaccess.fixedtemplate.reconciliation**	The workflow for reconciliation modify tasks.
`truaccess.fixedtemplate.recon_delete`	No	**truaccess.fixedtemplate.reconciliation**	The workflow for reconciliation delete tasks.
`truaccess.fixedtemplate.recon_enable`	Yes	None	The workflow for reconciliation enable tasks.
`truaccess.fixedtemplate.recon_disable`	Yes	None	The workflow for reconciliation disable tasks.
`truaccess.fixedtemplate.recon_terminate`	Yes	None	The workflow for reconciliation terminate tasks.
`truaccess.fixedtemplate.reconcliation.postprovpolicy`	No	**1**	The workflow for reconciliation post provisioning policy.

Property	Required	Default	Description
`si.reconciliation.resync.LDAP70=true`	No	true	The reconciliation provisioning back feature is enabled for resource LDAP70
`truaccess.fixedtemplate.recon.resync.LDAP70=ReconciliationDefaultProcess`	No	None	Default workflow used for reconciliation provisioning back feature.
`truaccess.fixedtemplate.recon.resync=ReconciliationDefaultProcess`	No	None	Workflow used for reconciliation provisioning back feature of resource LDAP70.

By using the `truaccess.fixedtemplate.recon_*` properties, you can have more control over which workflow templates are picked up for a reconciliation request in Select Identity.

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 that is defined in the Resources page of Select Identity. (You can see this by navigating to Resources → View Resources and selecting the resource.) If defined, this template is picked up.
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.

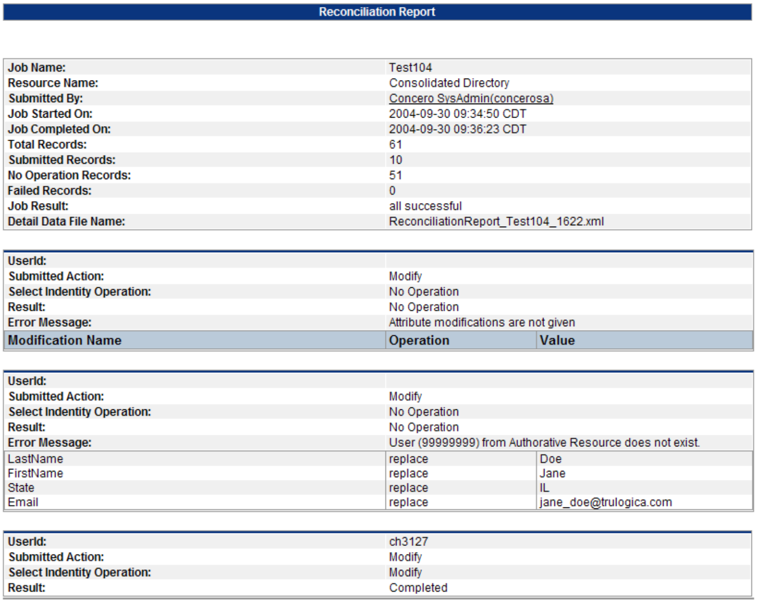
Job Results

After each of the reconciliation jobs completes, the creator of the job receives an HTML report. The report lists users that were successfully created and those that failed.

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.

If you are the creator of the job that ran initially, you cannot give the new job the same name. Each job that you create as an administrator must be assigned a unique name.

The following is a 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

Authoritative Results

You can expect the following results for each action.

- Action = **add**

- — 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 and the rule Id must be *ResourceName_ReconRule*. 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.
- — Service assignments are checked if this line appears in the `TruAccess.properties` file: `truaccess.recon.check_serviceassignment_authadd=true` or if a rule is specified.
- — 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 Create an SPML file Containing Users and Attributes on page 196. 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**
  - — 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**
  - 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**
  - 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.
  - 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.

Creating a Reconciliation Job

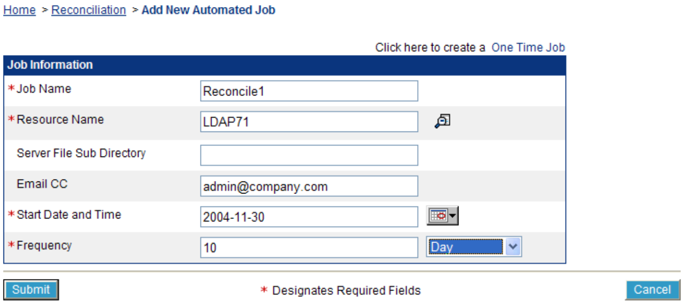
You can create and schedule a job to reconcile data or move users from one context to another. Create an SPML file with the necessary data before performing the following procedures.

Automated Reconciliation Job

Perform the following steps to schedule reconciliation with a specified resource:

1. From the home page of Reconciliation, select the **Reconciliation** option and click **Add New Job**.

   The Job Information page displays.



Home > Reconciliation > Add New Automated Job

Click here to create a One Time Job

Job Information		
*Job Name	Reconcile1	
*Resource Name	LDAP71	🔍
Server File Sub Directory		
Email CC	admin@company.com	
*Start Date and Time	2004-11-30	📅
*Frequency	10	Day

Submit   * Designates Required Fields   Cancel

2 Enter a name for the job in the Job Name field.

3 Click 🔍 to search for and select the resource from which you want to update.

4 Select Identity reads data files from the `reconroot` directory. You may have multiple files and multiple jobs to run. If so, enter a subdirectory for this job to reference in the Server File Sub Directory field. This is the directory in which the SPML data file is stored.

You can change the default `reconroot` directory to another directory. This location is set in the `TruAccess.properties` file. See the *HP OpenView Select Identity Installation and Configuration Guide* for details.

5 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 Email CC field.

6 Click the calendar icon to choose a day for the job to start running. If you select today’s date, the job runs immediately. The job runs at 12:00 A.M. on all other dates. You can also enter a time for the job to run. Enter the time in military format: 9:30, 15:45, 23:59:59.

7 Enter a value in the Frequency field and select an increment of time from the drop-down list. The frequency determines when Select Identity will pick up the data file from the specified directory.

For example, if you specified a date of 12-15-04 and a frequency of 3 hours, the job will pick up the file and run at 3:00 A.M on December 15.

8 Click **Submit**.

The job is created and runs when scheduled.

One-Time Reconciliation Job

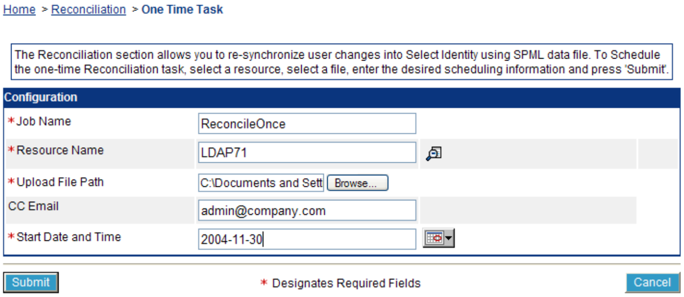
Perform the following steps to run a reconciliation job once:

1 From the home page of Reconciliation, click **Add New Job**.

The Job Information page displays.

2 Click the **One Time Job** link at the top of the page.

The Configuration page displays.



Home > Reconciliation > One Time Task

The Reconciliation section allows you to re-synchronize user changes into Select Identity using SPML data file. To Schedule the one-time Reconciliation task, select a resource, select a file, enter the desired scheduling information and press 'Submit'.

Configuration

*Job Name	ReconcileOnce
*Resource Name	LDAP71
*Upload File Path	C:\Documents and Sett Browse...
CC Email	admin@company.com
*Start Date and Time	2004-11-30

3 Enter a name for the job in the Job Name field.

4 Click 🔍 to search for and select the resource from which you want to update.

5 Click **Browse** to select the directory from which you want Select Identity to upload the data file.

6 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 Email CC field.

7 Click the calendar icon 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.

8 Click **Submit**.

The job is created and runs when scheduled.

Viewing an Automated Job

Perform the following steps to view a reconciliation job:

1. From the home page of Reconciliation, click 🔍 to search for and select the job that you want to view. In the Reconciliation Job Search page, select **Automated** for the Job Type, and click **Submit**. Select the job and click **Select**.
2. Select **View Automated Job** from the Actions drop-down list.
3. Click **Submit**. The Job Information page displays.

Modifying an Automated Job

Perform the following steps to modify a reconciliation job:

1. From the home page of Reconciliation, click 🔍 to search for and select the job that you want to modify. In the Reconciliation Job Search page, select **Automated** for the Job Type, and click **Submit**. Select the job and click **Select**.
2. Select **Modify Automated Job** from the Actions drop-down list.
3. Click **Submit**. The Job Information page displays.
4. Change any property, but the job name.
5. Click **Submit**.

Deleting an Automated Job

Perform the following steps to delete a reconciliation job:

1. From the home page of Reconciliation, click 🔍 to search for and select the job that you want to delete. In the Reconciliation Job Search page, select **Automated** for the Job Type, and click **Submit**. Select the job and click **Select**.

2 Select **Delete Automated Job** from the Actions drop-down list.

3 Click **Submit**.

4 You are prompted to confirm the action. Click **OK** to delete the job.

Viewing Task Status

You can view the task status of a specified job and then manually generate a Reconciliation report of a specific task by running a reconciliation One Time Job.

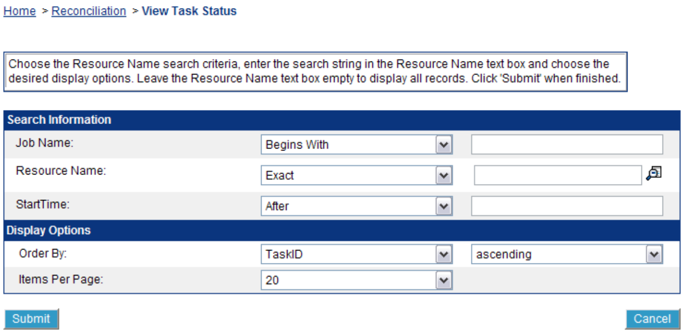
View the Task Status

Perform the following steps to view the task status:

1 From the home page of Reconciliation, click 🔍 to search for and select the job for which you want to view the task status.

2 Select **View Task Status** from the Actions drop-down list.

3 Click **Submit**. The Search page displays.



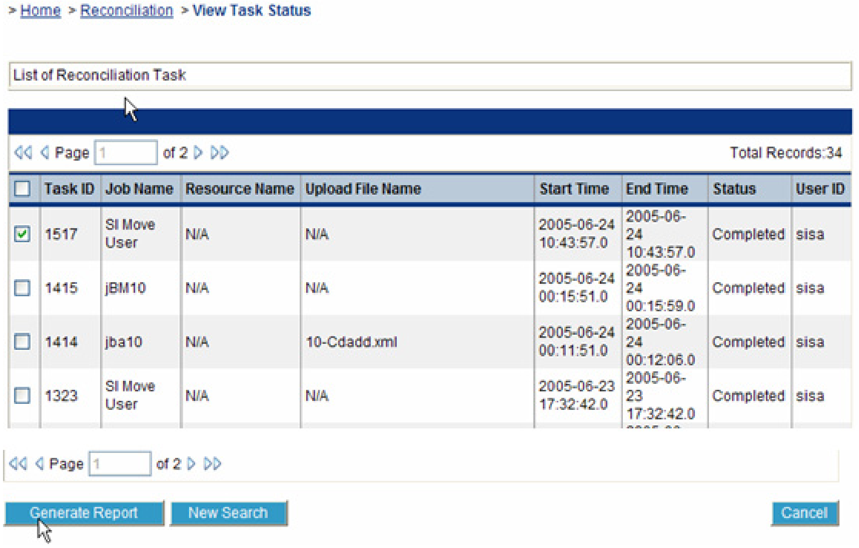
Home > Reconciliation > **View Task Status**

Choose the Resource Name search criteria, enter the search string in the Resource Name text box and choose the desired display options. Leave the Resource Name text box empty to display all records. Click 'Submit' when finished.

Search Information		
Job Name:	Begins With	
Resource Name:	Exact	
StartTime:	After	
Display Options		
Order By:	TaskID	ascending
Items Per Page:	20	

4 Enter your search criteria.

5 Click **Submit**. The Results page displays.



> Home > Reconciliation > View Task Status

List of Reconciliation Task

Total Records:34

□	Task ID	Job Name	Resource Name	Upload File Name	Start Time	End Time	Status	User ID
☑	1517	SI Move User	N/A	N/A	2005-06-24 10:43:57.0	2005-06-24 10:43:57.0	Completed	sisa
□	1415	jBM10	N/A	N/A	2005-06-24 00:15:51.0	2005-06-24 00:15:59.0	Completed	sisa
□	1414	jba10	N/A	10-Cdadd.xml	2005-06-24 00:11:51.0	2005-06-24 00:12:06.0	Completed	sisa
□	1323	SI Move User	N/A	N/A	2005-06-23 17:32:42.0	2005-06-23 17:32:42.0	Completed	sisa

If your job is not listed, click **New Search** to refine your search criteria.

Generate a Reconciliation Report

Perform the following to manually generate a Reconciliation report.

1. From the Results page, select the Task ID of the report you want to generate.
2. Select **Generate Report** at the bottom of the page. You are returned to the Reconciliation home page.

19

Account Self Service

This chapter describes the following functions for users:

- Self Service, which lets users manage their own profiles
- Self-Registration, which lets users add themselves to a Service through an external URL, sent through a notification email from a workflow template.

Self Service

After users are added to the Select Identity system, they can change their passwords, and create password hints through the Self Service pages. Administrators can grant their roles to another administrator within their Service context. This alleviates the burden of some of the most common administrative tasks from your IT or support staff.

Resource attributes that are mapped within Select Identity are updated when user profile information is updated. The context attribute for Services and the Select Identity unique ID cannot be modified.

Changing Passwords

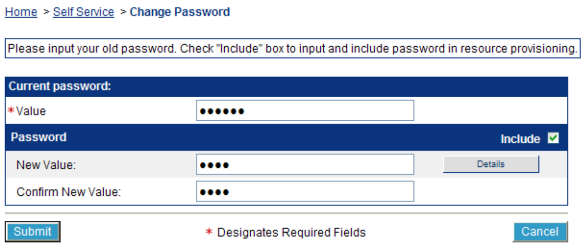
One of the most common user management tasks is changing or updating passwords. Through Self Service, Select Identity enables administrators to pass this task on to users. If given the permission to do so, users can change their password for each Service to which they have access. Users can also set or change password hints.

The following steps show how users change their account passwords:

1 From the home page of Self Service, select **Change Password** from the Actions drop-down list.

2 Click **Submit**.

The Password Information page displays.



Home > Self Service > Change Password

Please input your old password. Check "Include" box to input and include password in resource provisioning.

Current password:

*Value ●●●●●●

Password Include ☑

New Value: ●●●●

Confirm New Value: ●●●●

* Designates Required Fields

3 Enter your current password in the Value field.

The Include check box is selected by default.

4 Enter a new password. Click **Details** to view the policy requirements for this password.

5 If the password policy enables you to choose the resources that will be updated, choose the resources from the drop-down list.

6 Confirm the new password.

7 Click **Submit**.

When the change is approved, Select Identity sends email confirmation based on the notification policy associated with the action.

Changing Password Hints

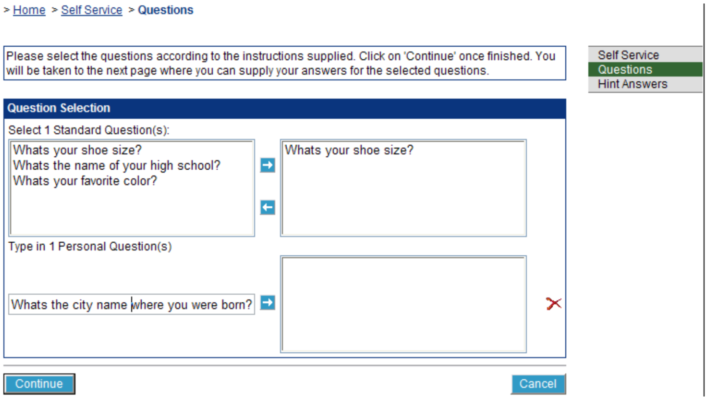
The following steps show how users change their password reset questions (hints), if given permission to do so.

➤ You need to specify the password hints that users first see through the Challenge/Response page (see Challenge Response Questions on page 98).

1 From the home page of Self Service, select **Change Password Reset Questions** from the Actions drop-down list.

2 Click **Submit**.

The Question Selection page displays.



> Home > Self Service > Questions

Please select the questions according to the instructions supplied. Click on 'Continue' once finished. You will be taken to the next page where you can supply your answers for the selected questions.

Question Selection

Select 1 Standard Question(s):

Whats your shoe size?
Whats the name of your high school?
Whats your favorite color?

Whats your shoe size?

Type in 1 Personal Question(s)

Whats the city name where you were born?

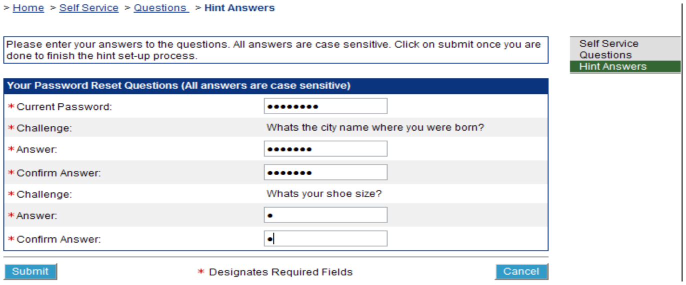
3 Provide one or more password hints. You can:

a Select a question or questions to be your password hint or hints.

b Type a question in the text box and click the right arrow.

4 Click **Continue**.

The Hint Answers page displays.



> Home > Self Service > Questions > Hint Answers

Please enter your answers to the questions. All answers are case sensitive. Click on submit once you are done to finish the hint set-up process.

Your Password Reset Questions (All answers are case sensitive)	
* Current Password:	••••••••
* Challenge:	Whats the city name where you were born?
* Answer:	•••••••
* Confirm Answer:	•••••••
* Challenge:	Whats your shoe size?
* Answer:	•
* Confirm Answer:	•

5 Enter your current password in the Current Password field.

6 Enter an answer for each question in the Answer field.

7 Confirm the answer..

> This action is dependent on the Select Identity challenge and response policy. See Challenge Response Questions on page 98 for details on modifying the challenge and response policy.

8 Click **Submit** to save your changes.

When the change is approved, Select Identity sends email confirmation based on the notification policy associated with the action.

Resetting Your Forgotten Password

When users select the Forget Password link, they can reset their password if you give them permission to do so. You do this by setting the following `TruAccess.properties` setting to false:

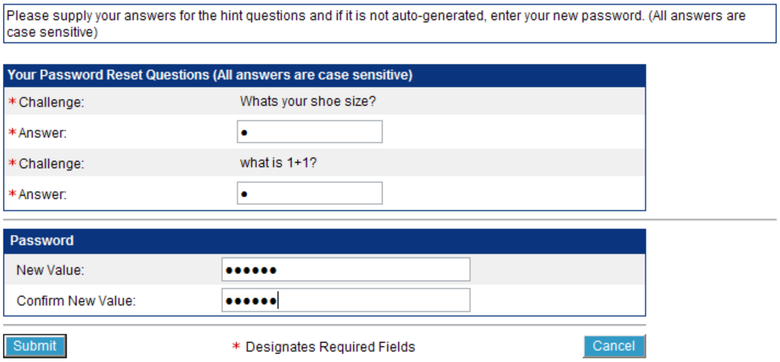
```
com.hp.ovsi.forgetpassword.autogenerate=false.
```

When this setting is set to true (the default), Select Identity automatically generates the password and provides the correct answers to the Challenge/ Response questions. See Modifying the Forget Password Setting on page 99 for more information.

The following steps show how a user resets the password if the forget password setting is set to false:

1 From the login page, click the link for Forget Password. The User Information page displays.

2 Enter your username. The Password Reset Questions page displays.



Please supply your answers for the hint questions and if it is not auto-generated, enter your new password. (All answers are case sensitive)

Your Password Reset Questions (All answers are case sensitive)	
* Challenge:	Whats your shoe size?
* Answer:	•
* Challenge:	what is 1+1?
* Answer:	•

Password	
New Value:	••••••
Confirm New Value:	••••••

3 Enter the answer or answers to the challenge questions.

4 Enter a new password in the New Value text box.

5 Re-enter the new password in the Confirm New Value text box.

6 Click **Submit**.

When the change is approved, Select Identity sends an email confirmation to the user.

Viewing Your Profile

Users can view their account profile if you give them permission to do so.

The following steps show how users can view their profile:

1 From the home page of Self Service, select **View My Profile** from the Actions drop-down list.

2 Click **Submit**. The User Attributes page displays.

3 Click **Self Service** in the cookie trail to return to the Self Service home page.

If your personal information changes, you can change designated profile attributes.

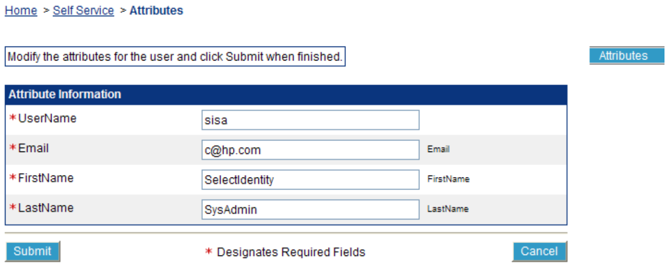
Modifying Your Profile

Users can modify their account profile if you give them permission to do so. The user name, password, and Service context attribute cannot be modified.

Perform the following steps to modify your profile:

1 From the home page of Self Service, select **Modify My Profile** from the Actions drop-down list.

2 Click **Submit**. The Attribute Information page is displayed.



Home > Self Service > Attributes

Modify the attributes for the user and click Submit when finished.

Attribute Information		
*UserName	sisa	
*Email	c@hp.com	Email
*FirstName	SelectIdentity	FirstName
*LastName	SysAdmin	LastName

* Designates Required Fields

3 You can edit any of the available fields.

4 Click **Submit**. Your change request is submitted for processing.

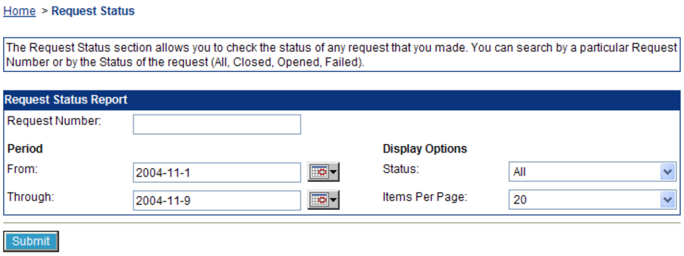
Viewing Request Status

You can view the status of requests that you make including account changes and Service additions.

Perform the following steps to view request status:

1 From the home page of Self Service, select **View Request Status** from the Actions drop-down list.

2 Click **Submit**. The Search page displays.



Home > **Request Status**

The Request Status section allows you to check the status of any request that you made. You can search by a particular Request Number or by the Status of the request (All, Closed, Opened, Failed).

Request Status Report

Request Number:

Period

From: 2004-11-1

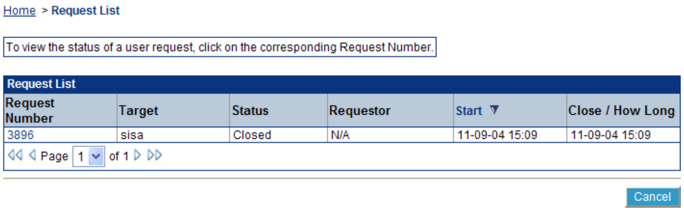
Through: 2004-11-9

Display Options

Status: All

Items Per Page: 20

3 Enter your search criteria and click **Submit**. The results display.



Home > **Request List**

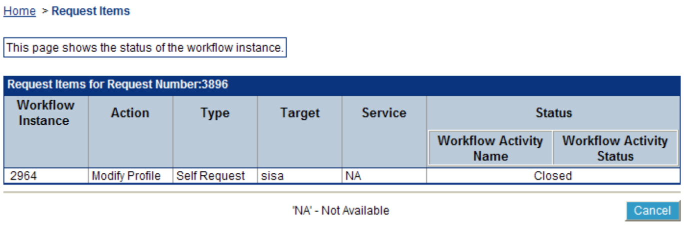
To view the status of a user request, click on the corresponding Request Number.

Request List

Request Number	Target	Status	Requestor	Start	Close / How Long
3896	sisa	Closed	N/A	11-09-04 15:09	11-09-04 15:09

Page 1 of 1

4 Click a Request Number for workflow details. The following displays.



Home > **Request Items**

This page shows the status of the workflow instance.

Request Items for Request Number:3896

Workflow Instance	Action	Type	Target	Service	Status	
					Workflow Activity Name	Workflow Activity Status
2964	Modify Profile	Self Request	sisa	NA	Closed	

'NA' - Not Available

5 Click **Cancel** to return to the Self Service home page.

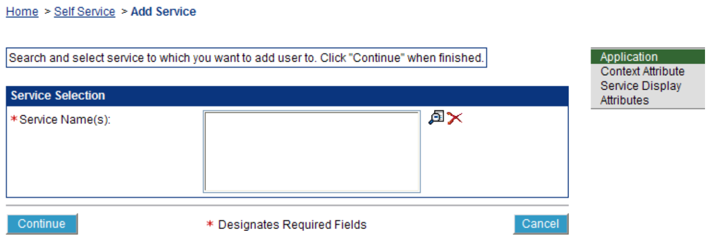
Adding a Service

You can add Service access to your account. Services must have been previously created to be added through the Self Service pages. See Creating and Modifying Services on page 104 for more information.

Perform the following steps to add a Service:

1 From the home page of Self Service, select **Add Service** from the Actions drop-down list.

2 Click **Submit**. The Service Selection page displays.



Home > Self Service > Add Service

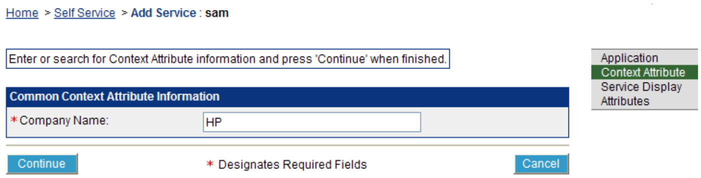
Search and select service to which you want to add user to. Click "Continue" when finished.

Service Selection

*Service Name(s):

3 Click 🔍 to search for and select the Services that you want to access.

4 Click **Continue**. The Context Attribute page displays.



Home > Self Service > Add Service : sam

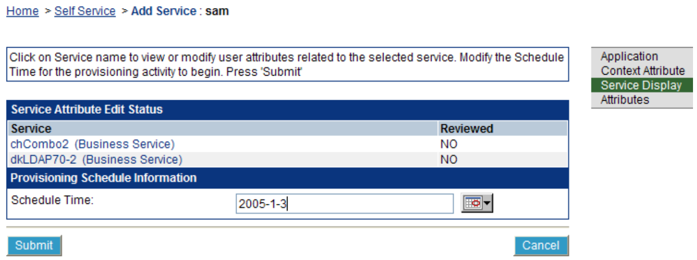
Enter or search for Context Attribute information and press 'Continue' when finished.

Common Context Attribute Information

*Company Name: HP

5 A common attribute for the Services that you selected displays. Review the value and click **Continue**.

The Service Attribute page displays.



Home > Self Service > Add Service : sam

Click on Service name to view or modify user attributes related to the selected service. Modify the Schedule Time for the provisioning activity to begin. Press 'Submit'

Service Attribute Edit Status

Service	Reviewed
chCombo2 (Business Service)	NO
dkLDAP70-2 (Business Service)	NO

Provisioning Schedule Information

Schedule Time: 2005-1-3

6 For each Service, click the Service name to review the attributes and values associated. Enter or choose values for the attributes listed and click **Save & Continue** to proceed. You are returned to the Service Attribute page.

After reviewing each Service, click the calendar icon to schedule the Service addition. The request is submitted at 12:00 A.M. on the day you select. If you select the current day, the request is submitted immediately.

7 Click **Submit**.

When the change is approved, Select Identity sends email confirmation based on the notification policy associated with the action.

Delegating or Removing Administrative Roles

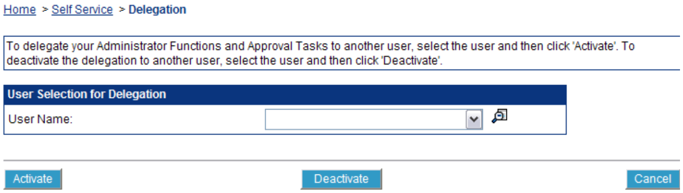
You can delegate your administrative roles to another Select Identity administrator within your Service context or remove roles that were delegated. This action is for administrators only.

Perform the following steps to delegate or remove roles:

1 From the home page of Self Service, select **Delegate Admin Roles** from the Actions drop-down list.

2 Click **Submit**.

The User Selection page displays.



To delegate your Administrator Functions and Approval Tasks to another user, select the user and then click 'Activate'. To deactivate the delegation to another user, select the user and then click 'Deactivate'.

User Selection for Delegation

User Name:

3 Click the search icon 🔍 to search for a name. The user must be a member of your Service context.

4 Click **Activate** to delegate the role to the specific user, or click **Deactivate** to remove functions from the user.

5 Click **Cancel** to return to the Self Service home page without performing an action.

When the change is approved, Select Identity sends an email confirmation based on the notification policy associated with the action.

Self-Registration

Users can add themselves to a Service through the Self-Registration process. Self-Registration is set up through a workflow template, which is assigned to an Add New User event request. (For a general description of workflow templates, see Workflow Templates in Select Identity on page 96, and for detailed information and examples, see the *HP OpenView Select Identity Workflow Studio Guide*.)

For a Service, the Self-Registration Add New User event must be defined with a workflow and view in the Service Role. In the workflow, when the Add New User event request is made, a specified URL is sent to the user to open the Self-Registration page. The Self-Registration page opens differently based on how you configure it.

Configuring the Self-Registration Page

You configure how the Self-Registration page displays based on the following settings 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.ovsi.commonattributesview.name=selfregview`

  Specifies that the first Self-Registration page that displays will be the defined Service View, named `selfregview`, with pre-defined attributes and context. If this setting is not defined, the first page that displays is the Service View defined for the Service Role. To use this setting, the Service View name must be `selfregview`.

➤ When you change this setting, it may be necessary to reboot the server to remove the cache.

- `com.hp.si.selfreg.schedule = true`

  Specifies whether the Schedule time field in the Self-Registration form is displayed. `true` is the default, which displays the Schedule time field. If set to `false`, the Schedule time field is not displayed.

Setting the Self-Registration URL

When you create the Self-Registration notification email in a workflow, you send a specific URL to access the Self-Registration page. (For information about creating notifications, see Notifications on page 86.) The URL you use, and whether you use the `selfregview` Service View, determine which Self-Registration page opens first.

You can use one of the following URLs:

- Service Name URL:

  `http://localhost:port/lmz/control/selfregistration/<SERVICE_NAME>`

  `localhost` is the application server (WebLogic or WebSphere)

  `<SERVICE_NAME>` is the name of a Service that was specified in the workflow.

  For example, if you replace `<SERVICE_NAME>` with **LDAP70**, the URL will be:

  `http://localhost:port/lmz/control/selfregistration/LDAP70`

  The Service Name URL works for any service type (business, admin, composite) as long as the event is defined. When this URL is used, there are two possible cases:

  1. If `selfregview` is defined in the `TruAccess.properties` file, when the user goes to the URL, the first page will be that `selfregview` Service View. Since the context was not defined in the URL, the user must add the context and context value.
  2. If `selfregview` is not defined, when the user goes to the URL, the first page is the Context page, and then the Service View defined in the Service Role for that event handler displays.

- Context URL:

  `http://localhost:port/lmz/control/selfreg/servicename?<contextattr>=<value>`

  `localhost` is the application server (WebLogic or WebSphere)

  `<contextattr>` is the context and `<value>` is the context value

  For example, if you replace `<contextattr>` with **Company**, and `<value>` with **GLOBAL**, the URL will be:

```
http://localhost:port/lmz/control/selfreg/servicename?Company=GLOBAL
```

The Context URL only works for business services, not composite or admin services.

When this URL is used, the first Self-Registration page opens to the Service View defined in the Service Role, whether or not `selfregview` is defined. The context and context value are already filled in.

Self-Registration Procedures

The following sections provide procedures users would use to self-register to a Service, depending on the URL received and whether or not `selfregview` is defined.

- Self-Registration using the Service Name URL with `selfregview` defined
- Self-Registration using the Service Name URL without `selfregview` defined
- Self-Registration using the Context URL

Self-Registration Using the Service Name URL With selfregview Defined

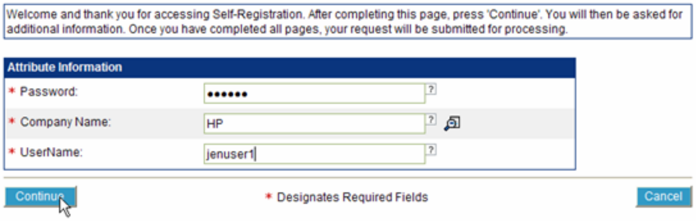
In this procedure, the user will receive a URL by email to self-register in the form of:

```
http://localhost:port/lmz/control/selfreg/<SERVICE_NAME>
```

The first page will be the view defined by `selfregview`.

Perform the following steps to add yourself to the Service:

1 Click on the URL you received by email to self-register. The Attribute Information page displays.



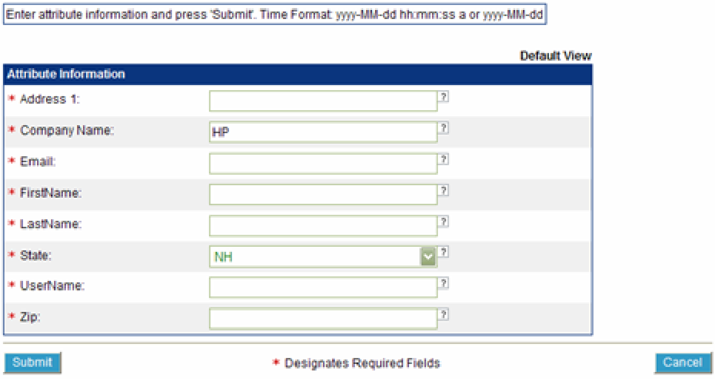
Welcome and thank you for accessing Self-Registration. After completing this page, press 'Continue'. You will then be asked for additional information. Once you have completed all pages, your request will be submitted for processing.

Attribute Information

* Password:	••••••
* Company Name:	HP
* UserName:	jenuser1

2 Enter the required fields.

3 Click **Continue**. The additional information Attribute Information page displays.



Enter attribute information and press 'Submit'. Time Format: yyyy-MM-dd hh:mm:ss a or yyyy-MM-dd

Default View

Attribute Information

* Address 1:	
* Company Name:	HP
* Email:	
* FirstName:	
* LastName:	
* State:	NH
* UserName:	
* Zip:	

* Designates Required Fields

The Service View name appears at the top of the Attribute Information form.

4 Enter the required information that has not been filled in.

5 Click **Submit**.

The add user request is created for you to be added to the Service. You will receive a brief message confirming this action.

Self-Registration Using the Service Name URL Without selfregview Defined

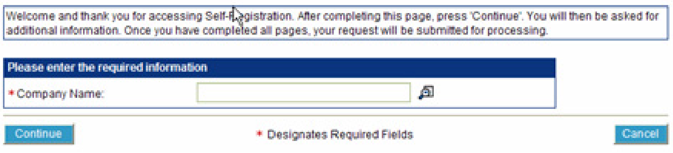
In this procedure, the user will receive a URL by email to self-register in the form of:

```
http://localhost:port/lmz/control/selfreg/<SERVICE_NAME>
```

Since `selfregview` is not defined, the first page will be the Context page.

Perform the following steps to add yourself to the Service:

1 Click on the URL you received by email to self-register. The Context Information page displays.



Welcome and thank you for accessing Self-Registration. After completing this page, press 'Continue'. You will then be asked for additional information. Once you have completed all pages, your request will be submitted for processing.

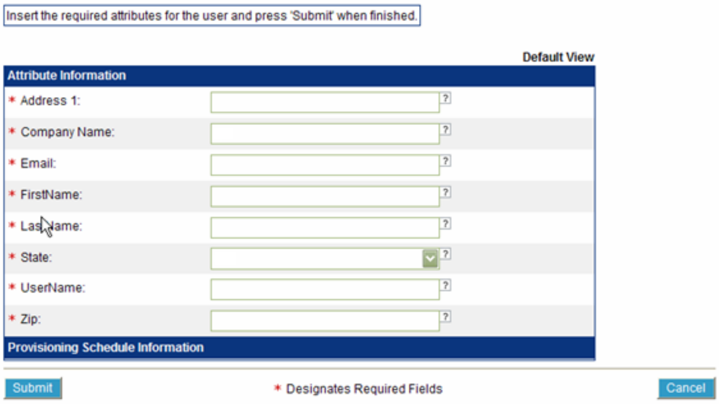
Please enter the required information

* Company Name: ____ 🔎

Continue | * Designates Required Fields | Cancel

2 Click 🔎 to search for and select a common context attribute for the Service to which you will be added.

3 Click **Continue** and the Attribute Information page displays. The attributes that appear on this page were defined in the Service Role.



Insert the required attributes for the user and press 'Submit' when finished.

Default View

Attribute Information

* Address 1: ____ ?

* Company Name: ____ ?

* Email: ____ ?

* FirstName: ____ ?

* LastName: ____ ?

* State: ____ ?

* UserName: ____ ?

* Zip: ____ ?

Provisioning Schedule Information

Submit | * Designates Required Fields | Cancel

The Service View name appears at the top of the Attribute Information form. In the example above, the name is “Default View” which is the default name if no Service View was specified when the Service Role was created. See Creating a Service Role on page 117 for more information.

4 Enter the required information that has not been filled in.

5 Click **Submit**.

The add user request is created for you to be added to the Service. You will receive a brief message confirming this action.

Self-Registration Using the Context URL

In this procedure, the user will receive a URL by email to self-register in the form of:

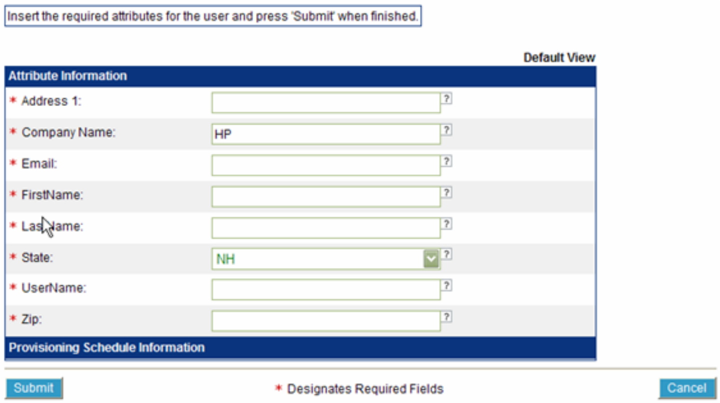
```
http://localhost:port/lmz/control/selfreg/servicename?<contextattr>=<value>
```

The first page will be the Service View defined in the Service Role, with the context and context value filled in.

Perform the following steps to add yourself to the Service:

1. Click on the URL you received by email to self-register. The Attribute Information page displays.

   The attributes that appear on this page were defined in the Service Role.



Insert the required attributes for the user and press 'Submit' when finished.

Default View

Attribute Information

* Address 1:	
* Company Name:	HP
* Email:	
* FirstName:	
* LastName:	
* State:	NH
* UserName:	
* Zip:	

Provisioning Schedule Information

Submit

* Designates Required Fields

Cancel

   The Service View name appears at the top of the Attribute Information form.

2. Enter the required information that has not been filled in.

3. Click **Submit**.

The add user request is created for you to be added to the Service. You will receive a brief message confirming this action.

20

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.

Audit Reports

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. You can generate a single report or create a report template, which can be accessed each time you click **Audit Reports**.

Available Audit Reports

User Audit Reports

Generate a User Audit report to view configuration activities for specific user accounts over a period of time. These reports detail all actions related to any user within 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 the following columns: Time Stamp, Requestor, User Name, Action, Service and Status.

User Audit reports include:

- Audit User Creation
- Audit User Deletion
- Audit User Termination
- Audit User Password
- Audit User Login
- Set Hint Audit

Audit User Summary Reports

Summarize all user account actions within Select Identity and provide a count for each action per Service and context. 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
- Set Hint Audit Summary

Audit User Service Report
Generate an Audit User Service report to view configuration activities for a Service over a period of time. This report details all actions related to one or multiple Services within Select Identity.

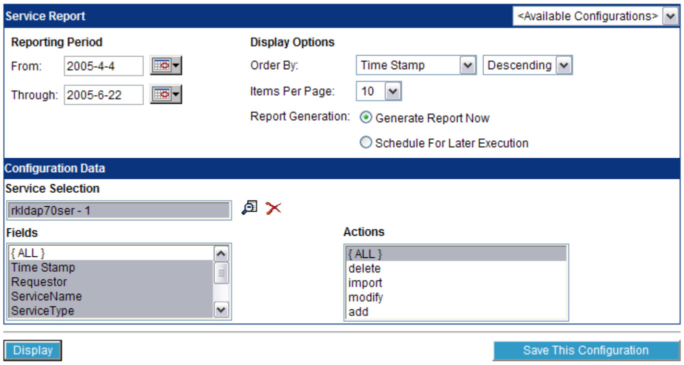
Generating Audit Reports

Reports are generated based on specific actions including delete, modify, import and add. The type of data displayed for each report is configurable and may include the following columns: Time Stamp, Requestor, Service Name, Service Type, Action, Component, Component Name, and Status. See the online Help for specific procedures for each Audit Report.

Perform the following steps to generate an audit report. This procedure uses the Audit User Service report as an example.

1. From the Audit Reporting home page, select **Audit Service Report** from the Audit Report Selection drop-down list.
2. Click **Generate**.

   The Report Configuration page displays.



Service Report

<Available Configurations>

Reporting Period

From: 2005-4-4

Through: 2005-6-22

Display Options

Order By: Time Stamp, Descending

Items Per Page: 10

Report Generation: ● Generate Report Now ○ Schedule For Later Execution

Configuration Data

Service Selection

rkldap70ser - 1

Fields

{ ALL }
Time Stamp
Requestor
ServiceName
ServiceType

Actions

{ ALL }
delete
import
modify
add

To use an existing report template, choose it from the Available Configurations drop-down list at the top of the page. If not, follow the rest of this procedure.

3. Choose a range of days or months and enter them in the From and Through fields. Select from the calendar views or enter dates using the following format (specifying the time is optional):

   yyyy-mm-dd [hh:mm]

4. Choose the display options for this report.

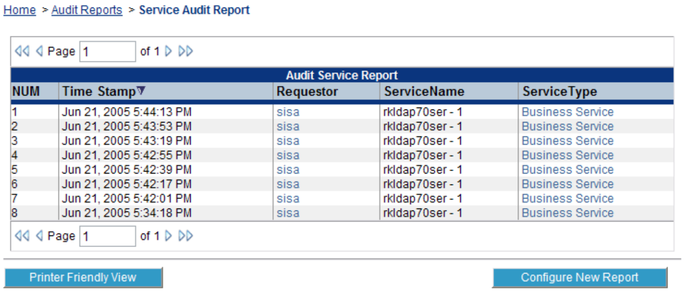
   - Choose the category by which you want to see data ordered from the Order By drop-down list.
   - Choose the field type by which you want information ordered and select **Ascending** or **Descending** from the drop-down lists.
   - Select an option from the Items Per Page list.
   - Choose one of the following options:
     - — **Generate Report Now** radio button to view the report when you click **Display**. This option is chosen for this example.
     - — **Schedule For Later Execution** radio button to schedule and save your batch report. If you choose this option, select the configuration data and then click **Display**. The Batch Report Job Configuration page displays. See Scheduling a Batch Report on page 239 for details on how to schedule your batch report.

5. Select the audit data that you want to display.

   - Click 🔍 to search for and select the Service that you want to audit.
   - Choose the categories of information that you want to view from the Fields list.
   - Select the actions that you want to audit from the Actions list.

6. Click **Display** to view the report, or **Save This Configuration** to have these report settings available for future use. See Saving Report Configurations on page 240 for information about saving reports.

   The following is an example report.



Audit Service Report

NUM	Time Stamp	Requestor	ServiceName	ServiceType
1	Jun 21, 2005 5:44:13 PM	sisa	rkldap70ser - 1	Business Service
2	Jun 21, 2005 5:43:53 PM	sisa	rkldap70ser - 1	Business Service
3	Jun 21, 2005 5:43:19 PM	sisa	rkldap70ser - 1	Business Service
4	Jun 21, 2005 5:42:55 PM	sisa	rkldap70ser - 1	Business Service
5	Jun 21, 2005 5:42:39 PM	sisa	rkldap70ser - 1	Business Service
6	Jun 21, 2005 5:42:17 PM	sisa	rkldap70ser - 1	Business Service
7	Jun 21, 2005 5:42:01 PM	sisa	rkldap70ser - 1	Business Service
8	Jun 21, 2005 5:34:18 PM	sisa	rkldap70ser - 1	Business Service

Click on a requestor name to view profile information for a user.

Click **Printer Friendly View** to print the report, or you can configure a new report.

Configuration Reports

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**.

For most reports, you can choose to generate the report now, or schedule the report for later execution, which is sent to a specified email address using a specified schedule. For the User Configuration Summary Report, you can only generate the report now. For the User Configuration Detail Report, you can only schedule the report for later execution.

Available Configuration Reports

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.

User 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 different between Select Identity and the Resource. You can choose to display:

- All users/entitlements that are different between Select Identity and the Resource.
- Only users/entitlements that are in Select Identity, but are not provisioned to a Resource.
- Only users/entitlements in a specified Resource that are not in Select Identity.

Generating Configuration Reports

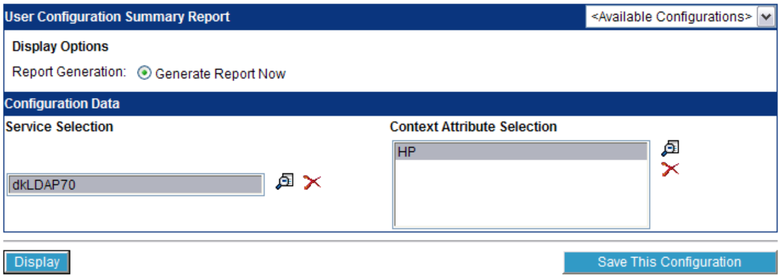
The configuration procedure for each report is similar. The available configuration data will change to suit the report type. The following procedure uses the User Configuration Summary report as an example. See the online help for specific procedures for each Configuration Report.

Perform the following steps to generate a configuration report.

1 From the Configuration Reports home page, select **User Configuration Summary Report** from the Configuration Report Selection drop-down list.

2 Click **Generate Report**.

The Report Configuration page displays.



User Configuration Summary Report

<Available Configurations> ▾

Display Options

Report Generation: ● Generate Report Now

Configuration Data

Service Selection: dkLDAP70

Context Attribute Selection: HP

Display

Save This Configuration

If you want to use an existing report template, choose it from the Available Configurations drop-down list at the top of the page. If not, follow the rest of this procedure.

3 Select the display options for this report.

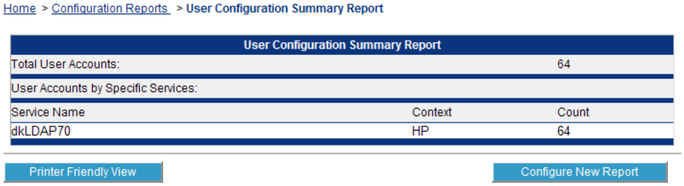
- Choose the **Generate Report Now** option.

> ➤ Some reports have the **Schedule Report For Later Execution** option, which lets you schedule and save a batch report to be run later at regular intervals. If you choose this option, select the configuration data and then click **Display**. The Batch Report Job Configuration page displays. See Scheduling a Batch Report on page 239 for details on how to schedule a batch report.

- Click 🔍 to search for and select the Service.
- Click 🔍 to search for and select the Context attribute.

4 Click **Display** to view the report, or **Save This Configuration** to have these report settings available for future use. See Saving Report Configurations on page 240 for information about saving reports.

The following is a sample.



Home > Configuration Reports > User Configuration Summary Report

User Configuration Summary Report		
Total User Accounts:		64
User Accounts by Specific Services:		
Service Name	Context	Count
dkLDAP70	HP	64

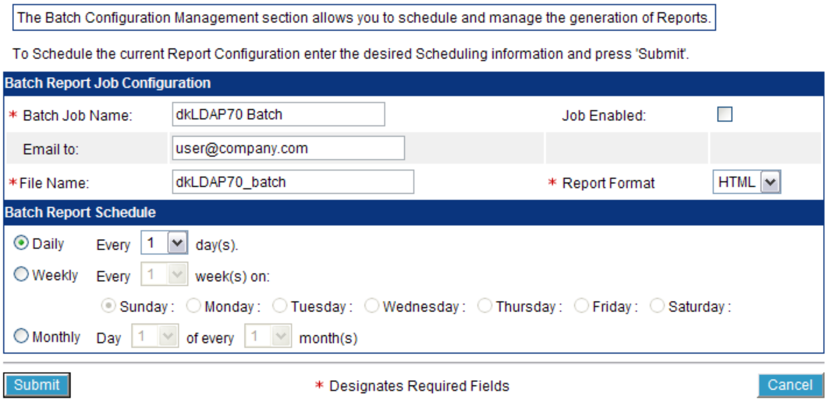
After the report displays, you can click **Printer Friendly View** and print the report, or configure a new report.

Scheduling a Batch Report

If you selected the **Schedule For Later Execution** option from one of the Report Configuration pages, you can schedule a batch report job that can be run at regular intervals.

Perform the following to schedule a batch report:

1 From a Report Configuration page, enter your report criteria and select the **Schedule For Later Execution** option, then click **Display**. The Batch Report Job Configuration page displays.



The Batch Configuration Management section allows you to schedule and manage the generation of Reports.

To Schedule the current Report Configuration enter the desired Scheduling information and press 'Submit'.

Batch Report Job Configuration

* Batch Job Name:	dkLDAP70 Batch	Job Enabled:	□
Email to:	user@company.com		
* File Name:	dkLDAP70_batch	* Report Format	HTML

Batch Report Schedule

● Daily Every 1 day(s).

○ Weekly Every 1 week(s) on:

● Sunday : ○ Monday : ○ Tuesday : ○ Wednesday : ○ Thursday : ○ Friday : ○ Saturday :

○ Monthly Day 1 of every 1 month(s)

2 Enter a unique name for the report job in the Batch Job Name field.

3 Email is automatically sent to the creator of this job. If you want others to receive email, click 🔍 to search for and select additional users.

4. Enter a file name for the report file. If the report is very large, you will receive an email notifying you that this file is saved on a hard drive.

➤ The report size is configurable through the `TruAccess.properties` file, which is described in the *HP OpenView Select Identity Installation Guide*.

5. If you want to enable this job, select the **Job Enabled** check box. You can create the job and enable it later, if you choose.
6. Choose which format you want the report formatted in: HTML or CSV.
7. Define the interval of time that you want the job to run. Select **Daily, Weekly**, or **Monthly** and choose schedule options.
8. Click **Submit**. You are returned to the Report Configuration page.
9. If you want, click **Display** to run the report.

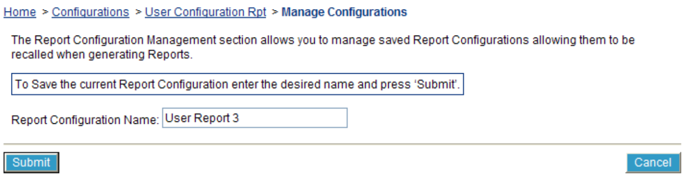
You can access the scheduled report by clicking **Manage Schedules** from the Audit Report home page.

Saving Report Configurations

You can save your report definitions and schedule them to run at regular intervals. This enables you to easily track changes and updates within the Select Identity system.

Perform the following steps to save a report definition:

1. From one of the Report Definition pages, click **Save This Configuration**. The Manage Configurations page displays.


Home > Configurations > User Configuration Rpt > Manage Configurations

The Report Configuration Management section allows you to manage saved Report Configurations allowing them to be recalled when generating Reports.

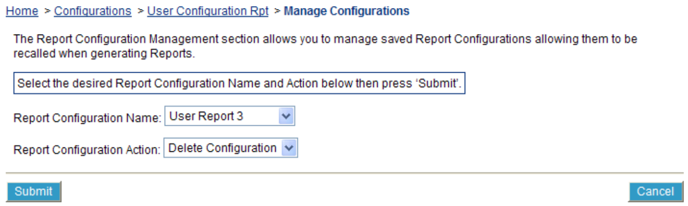
To Save the current Report Configuration enter the desired name and press 'Submit'.

Report Configuration Name: User Report 3

2. Enter a name for the report definition and click **Submit**.

   The report is saved. The definition page displays so that you can run the report. You can later access the report from the Available Configurations drop-down list.

Click **Manage Configurations** from the home page of the reporting section to delete this report definition. The following displays.



Home > Configurations > User Configuration Rpt > **Manage Configurations**

The Report Configuration Management section allows you to manage saved Report Configurations allowing them to be recalled when generating Reports.

Select the desired Report Configuration Name and Action below then press 'Submit'.

Report Configuration Name: User Report 3

Report Configuration Action: Delete Configuration

21

Configurations

HP OpenView Select Identity provides a configuration management capability that enables you to import and export the following from one environment to another:

Service
Workflow template
Workflow application definition
Request instance report
Resource
Notification
Attribute

For example, you may have set up your Select Identity system in a test environment and want to export your configuration to a production environment. All data is imported and exported through XML files.

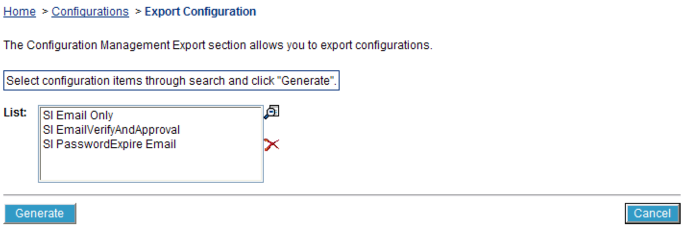
Exporting a Configuration

Perform the following steps to export configuration information:

1. From the home page of Configurations, select the item type that you want to want to export from the Configuration drop-down list.

2 Select **Export Configuration** form the Actions list.

3 Click **Submit**. The Configuration list page displays.



Home > Configurations > Export Configuration

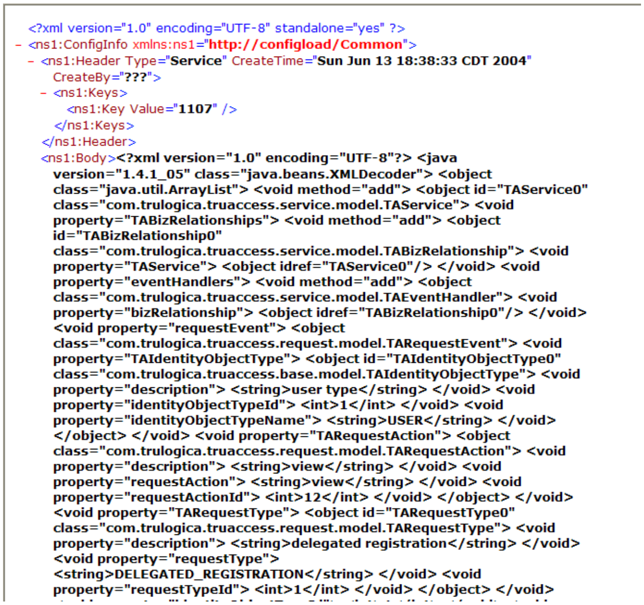
The Configuration Management Export section allows you to export configurations.

Select configuration items through search and click "Generate".

List: SI Email Only
SI EmailVerifyAndApproval
SI PasswordExpire Email

4 Click 🔍 to search for and select the items that you want to export.

5 Click **Generate** to create the XML data file.



```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <ns1:ConfigInfo xmlns:ns1="http://configload/Common">
  - <ns1:Header Type="Service" CreateTime="Sun Jun 13 18:38:33 CDT 2004"
      CreateBy="???">
    - <ns1:Keys>
        <ns1:Key Value="1107" />
      </ns1:Keys>
    </ns1:Header>
    <ns1:Body><?xml version="1.0" encoding="UTF-8"?> <java
      version="1.4.1_05" class="java.beans.XMLDecoder"> <object
      class="java.util.ArrayList"> <void method="add"> <object id="TAService0"
      class="com.trulogica.truaccess.service.model.TAService"> <void
      property="TABizRelationships"> <void method="add"> <object
      id="TABizRelationship0"
      class="com.trulogica.truaccess.service.model.TABizRelationship"> <void
      property="TAService"> <object idref="TAService0"/> </void> <void
      property="eventHandlers"> <void method="add"> <object
      class="com.trulogica.truaccess.service.model.TAEventHandler"> <void
      property="bizRelationship"> <object idref="TABizRelationship0"/> </void>
      <void property="requestEvent"> <object
      class="com.trulogica.truaccess.request.model.TARequestEvent"> <void
      property="TAIdentityObjectType"> <object id="TAIdentityObjectType0"
      class="com.trulogica.truaccess.base.model.TAIdentityObjectType"> <void
      property="description"> <string>user type</string> </void> <void
      property="identityObjectTypeId"> <int>1</int> </void> <void
      property="identityObjectTypeName"> <string>USER</string> </void>
      </object> </void> <void property="TARequestAction"> <object
      class="com.trulogica.truaccess.request.model.TARequestAction"> <void
      property="description"> <string>view</string> </void> <void
      property="requestAction"> <string>view</string> </void> <void
      property="requestActionId"> <int>12</int> </void> </object> </void>
      <void property="TARequestType"> <object id="TARequestType0"
      class="com.trulogica.truaccess.request.model.TARequestType"> <void
      property="description"> <string>delegated registration</string> </void>
      <void property="requestType">
      <string>DELEGATED_REGISTRATION</string> </void> <void
      property="requestTypeId"> <int>1</int> </void> </object> </void>
```

6 Save the file to any location.

Importing a Configuration

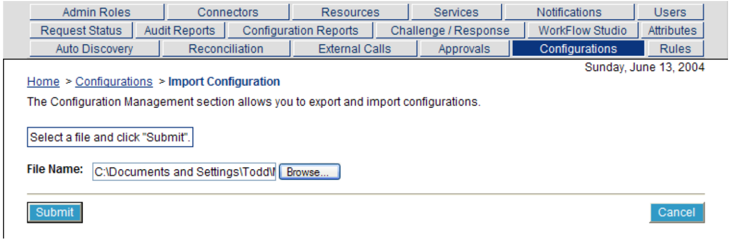
Perform the following steps to import a configuration file:

1 From the home page of Configurations, select the item type that you want to want to import from the Configuration drop-down list.

2 Select **Import Configuration** form the Actions list.

3 Click **Submit**.

The Configuration list page displays.



Sunday, June 13, 2004

Home > Configurations > Import Configuration

The Configuration Management section allows you to export and import configurations.

Select a file and click "Submit".

File Name: C:\Documents and Settings\Todd\

4 Click **Browse** to locate the file that you want to import.

5 Click **Submit** to import the file.

The Configuration list page displays.

A

Creating Reconciliation Rules

Reconciliation rules are only executed by HP OpenView Select Identity when a new user is added from an Authoritative resource through the Reconciliation capability. You must create an XML or SPML file that adheres to the rules DTD. You can save the file in any directory on the Select Identity server. When you add the rule in theRules capability, the rule file is uploaded to the Select Identity database.

Application Server Configuration for Rules

Rule DTD

All rule files must adhere to the rule DTD. All XML documents are made up of the following simple building blocks:

`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: **&lt;** for **<**, **&gt;** for **>**, **&amp;** for **&**, **&quot;** for **“**, and **&apos;** for '.

`PCDATA` Text that is parsed by a parser. Tags inside the text will be treated as markup and entities will be expanded.

`CDATA` Text that is not parsed by a parser. Tags inside the text are not treated as markup and entities are not expanded.

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`. For a DTD tutorial, refer to `http://www.w3schools.com/dtd/default.asp`.

The Select Identity rule DTD is provided in full below. 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)>
```

Example: Reconciliation Rule

The following is a sample of an XML rule used for reconciliation. This sample checks if the resource name is “LDAPv3_Auth,” user attribute “Company,” with a value of “ABCCorp.” The rule then adds new users 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
Authorative 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>&quot;LDAPv3_Auth&quot;</FixedValue>
              </Expression>
            </Relation>
          </UnitCondition>
          <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;ABCCorp&quot;</FixedValue>
              </Expression>
            </Relation>
          </UnitCondition>
        </AndCondition>
      </Condition>
      <TrueAction>
        <ActionScript Comment="Assign Services">
           <AssignStmt>
              <Field name="ServiceNameMap" type="java.util.Map"
fieldKey="&quot;reconSvc1&quot;"/>
                <Expression>
                  <FixedValue>&quot;+OK&quot;</FixedValue>
                </Expression>
            </AssignStmt>
            <AssignStmt>
              <Field name="ServiceNameMap" type="java.util.Map"
fieldKey="&quot;reconSvc2&quot;"/>
                <Expression>
                  <FixedValue>&quot;+OK&quot;</FixedValue>
                </Expression>
           </AssignStmt>
         </ActionScript>
      </TrueAction>
    </ConditionScript>
  </Script>
</Rule>
```

B

Event Reference

The following tables lists 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

glossary

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

A task that can be performed within each Select Identity capability.

In Workflow Studio, an action invokes functions provided by the workflow engine or external applications within an activity. For example, you can log information to a file, set a property to be used later in the workflow, call an external process, provision a user in Select Identity, or store data in a database.

See also: Capability

Activity

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.

Admin Role

A template that defines the administrative actions that can be performed by a user. An Administrative Service is created to provide access to roles. Users are then given access to the Service. Users with administrative roles can also grant their set of roles to another administrator within their Service context.

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.

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.”

Audit Report

A report that provides regular account interaction information within the Select Identity system.

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.

Authorization

Real-time enforcement of an identity’s entitlements. Authentication is a prerequisite for authorization.

Auto Discovery

The process of adding user accounts to the Select Identity system for a specified Service through the use of a data file.

B

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 that is 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.

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

C

Capability

Actions that can be performed within the Select Identity client are grouped by capability, or link, in the interface.

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, 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.

Configurations

A capability that enables you to import and export Select Identity settings and configurations. This is useful when moving from a test to a production environment.

Configuration Report

A report that provides current system information for user, administrator, and Service management activities.

Connector

A J2EE connector that communicates with the system resources that contain your identity profile information.

Context

A Select Identity concept that defines a logical grouping of users that can access a Service.

Contextual Identity Management (CIM)

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 Select Identity Services and Service Roles.

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.

D

Data File

An SPML file that enables you to define user accounts to be added to Select Identity through Auto Discovery or Reconciliation.

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

E

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.

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.

External Call

A programmatic call to a third-party application or system for the purpose of validating accounts or constraining attribute values.

F

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.

I

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.

Instance

See: Workflow Instance

M

Management

The ongoing maintenance of an object or set of objects, including creating, modifying, deleting, organizing, auditing, and reporting.

N

Notifications

The capability that enables you to create and manage templates that define the messages that are sent when a system event occurs.

P

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.

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 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

T

Template

See: Workflow Template

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

Users

The Select Identity capability that provides consistent account creation and management across Services.

V

Variable

See: Workflow Variable

Variable Expression

See: Expression

W

Workflow Engine

A system component that executes workflows and advances them through their flow steps.

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 Select Identity capability 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

index