

# HP OpenView Select Identity

## Administrator Guide

Software Version: 3.0

UNIX® (Sun Solaris) and Windows®  
Operating Systems



July 2004

© Copyright 2004 Hewlett-Packard Development Company, L.P.

## 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

© Copyright 2002, 2003, 2004 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

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

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils.
- Commons-collections.
- Commons-logging.
- Commons-digester.
- Commons-httpclient.

- Element Construction Set (ecs).
- Jakarta-poi.
- Jakarta-regexp.
- Logging Services (log4j).

Additional third party software used by Select Identity includes:

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

This product includes software developed by Teodor Danciu (<http://jasperreports.sourceforge.net>). Portions Copyright (C) 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. ([www.waveset.com](http://www.waveset.com)). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

## Trademark Notices

Select Identity is a trademark of Hewlett-Packard Development Company, L.P.

Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

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

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

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

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

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

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

## Support

Please visit the HP OpenView web site at:

**<http://openview.hp.com/>**

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the support web site at:

**<http://support.openview.hp.com/>**

The support web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

# contents

<b>Chapter 1</b>	<b>Welcome to Select Identity</b>	12
	System Architecture	14
	Additional Resources	16
<b>Chapter 2</b>	<b>Deployment Overview</b>	17
	Deployment Tasks	17
	Connectors	18
	Resources	18
	Attributes	19
	External Calls	19
	Rules	20
	Notifications	20
	Workflow Studio	21
	Challenge Response	21
	Service	22
	Business Relationships	22
	Context	22
	Administrative Roles	23
	Auto Discovery	23
	Users	24
	Request Status	24
	Configuration and Audit Reporting	25
	Reconciliation	25
	Configurations	25
	Self Service	26

Deployment Order .....	26
Logging In to Select Identity .....	28
<b>Chapter 3 Connectors</b> .....	<b>29</b>
Creating and Installing a Connector .....	30
Managing Connectors .....	31
Deploying a Connector .....	31
Modifying a Connector .....	32
Viewing a Connector .....	32
Deleting a Connector .....	33
<b>Chapter 4 Resources</b> .....	<b>34</b>
Authoritative Sources .....	35
Adding and Managing System Resources .....	36
Access Information .....	36
LDAP for eTrust .....	37
LDAP for Active Directory .....	37
LDAP for iPlanet .....	38
UNIX with SSH .....	39
UNIX with Telnet .....	40
Windows NT Local .....	41
Deploying a Resource .....	42
Modifying a Resource .....	44
Viewing a Resource .....	46
Deleting a Resource .....	46
Viewing Resource Attributes .....	47
<b>Chapter 5 Attributes</b> .....	<b>49</b>
Adding and Mapping an Attribute .....	51
Viewing an Attribute .....	55
Modifying an Attribute .....	56
Deleting an Attribute .....	56
<b>Chapter 6 External Calls</b> .....	<b>57</b>
Creating an External Call For Workflow Templates .....	58
Creating an External Call for Attributes .....	58

	Deploying an External Call . . . . .	59
	Modifying an External Call . . . . .	61
	Viewing an External Call . . . . .	61
	Deleting an External Call . . . . .	62
<b>Chapter 7</b>	<b>Rules . . . . .</b>	<b>63</b>
	Adding a Rule . . . . .	64
	Modifying a Rule . . . . .	64
	Viewing a Rule . . . . .	65
	Deleting a Rule . . . . .	65
<b>Chapter 8</b>	<b>Notifications . . . . .</b>	<b>66</b>
	Pre-defined Variables . . . . .	67
	Creating and Modifying Notification Templates . . . . .	68
	Adding a Notification Template . . . . .	68
	Copying a Notification Template . . . . .	70
	Modifying a Notification Template . . . . .	70
	Viewing a Notification Template . . . . .	71
	Deleting a Notification Template . . . . .	71
<b>Chapter 9</b>	<b>Workflow Studio . . . . .</b>	<b>72</b>
	Workflow Studio Overview . . . . .	73
	Workflow Templates in Select Identity . . . . .	73
<b>Chapter 10</b>	<b>Challenge Response Questions . . . . .</b>	<b>75</b>
<b>Chapter 11</b>	<b>Services . . . . .</b>	<b>77</b>
	Business Relationships . . . . .	78
	Context . . . . .	79
	Creating and Modifying Services . . . . .	79
	Deploying a Service . . . . .	80
	Modifying a Service . . . . .	81
	Deleting a Service . . . . .	82
	Service Views . . . . .	82
	Creating a Service View . . . . .	82
	Modifying a Service View . . . . .	84



Deleting a Service View .....	84
Service Attributes .....	85
Setting Service Attribute Values .....	85
Setting Service Attribute Properties .....	86
Defining Business Relationships and Context .....	88
Creating a Business Relationship .....	88
Modifying a Business Relationship .....	90
Deleting a Business Relationship .....	91
Creating Context .....	91
Modifying Context .....	93
Deleting Context .....	94
<b>Chapter 12 Administrative Roles .....</b>	<b>95</b>
Administrative Capabilities and Actions .....	96
Select Identity Capabilities and Actions .....	96
Select Identity Default Roles .....	99
Creating and Managing Administrative Roles .....	100
Adding an Admin Role .....	101
Modifying a Role .....	102
Viewing a Role .....	102
Deleting a Role .....	103
<b>Chapter 13 Auto Discovery .....</b>	<b>104</b>
Using an SPML Data File .....	104
Scheduling Auto Discovery .....	107
Viewing Discovery Status .....	108
Scheduling Service Assignments .....	109
Viewing Service Assignment Status .....	110
<b>Chapter 14 Users .....</b>	<b>112</b>
Adding a User .....	113
Modifying a User Account .....	115
Adding a Service to a User Account .....	116
Enabling or Disabling Service Membership .....	117
Enabling or Disabling All Services .....	118
Viewing Service Membership .....	118

Resetting a User's Password . . . . .	119
Deleting a Service Membership . . . . .	120
Terminating a User Account . . . . .	120
Viewing Account Attributes . . . . .	121
Managing User Account Expiration . . . . .	122
<b>Chapter 15 Approvals . . . . .</b>	<b>123</b>
<b>Chapter 16 Request Status . . . . .</b>	<b>126</b>
<b>Chapter 17 Account Reconciliation . . . . .</b>	<b>129</b>
Reconciliation Dependencies . . . . .	130
Reconciling with Authoritative Sources . . . . .	130
Reconciling with Non-authoritative Sources . . . . .	131
Reconciling Account Data . . . . .	132
Viewing an Automated Job . . . . .	133
Modifying an Automated Job . . . . .	133
Deleting an Automated Job . . . . .	134
Creating a Job to Run Once . . . . .	134
Viewing Task Status . . . . .	135
<b>Chapter 18 Account Self Service . . . . .</b>	<b>137</b>
Changing a Password and Password Hints . . . . .	137
Delegating or Removing Administrative Roles . . . . .	139
<b>Chapter 19 Configuration and Audit Reports . . . . .</b>	<b>140</b>
Generating Audit Reports . . . . .	140
Generating Configuration Reports . . . . .	143
Saving Report Configurations . . . . .	144
<b>Chapter 20 Configurations . . . . .</b>	<b>146</b>
Exporting a Configuration . . . . .	146
Importing a Configuration . . . . .	148
<b>Appendix A Creating Rules . . . . .</b>	<b>149</b>
Application Server Configuration for Rules . . . . .	149

Rule DTD .....	150
Example: Reconciliation Rule .....	156
<b>Appendix B Creating SPML Files .....</b>	<b>158</b>
Execution Types .....	159
Security .....	160
Example File for Reconciliation.....	161
<b>Appendix C Event Reference.....</b>	<b>164</b>
<b>Glossary.....</b>	<b>165</b>
<b>Index .....</b>	<b>174</b>

# 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:

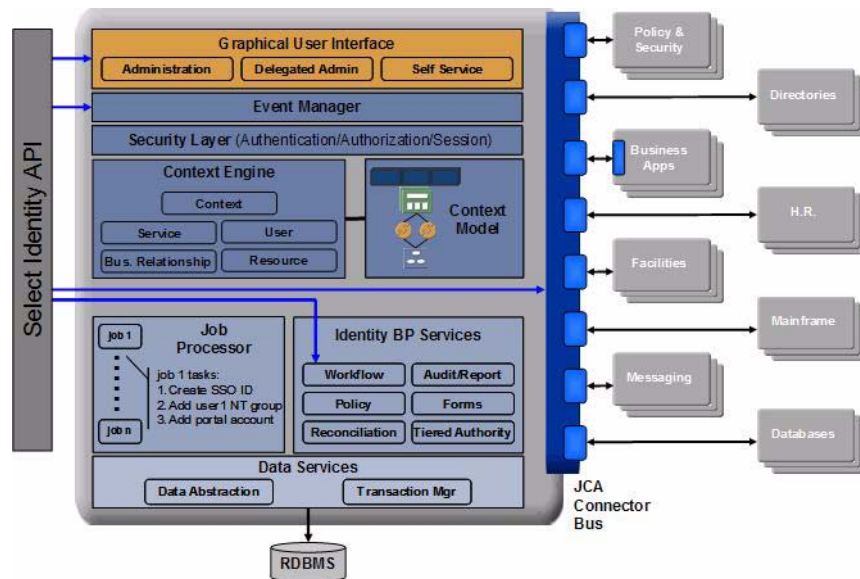
- **Centralized Management** – Provides a single point of control for the management of users and entitlements
- **Provisioning** – Automates the creation, update, and deletion of accounts and entitlements on information systems across the enterprise
- **Administrative Delegation** – Enables administrative 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 security policies that are defined by an administrator 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.

**Business Relationship Management** – Provides granular control over how groups of users access Services.

**Group Management** – Provides an attribute-based model for grouping users in order to simplify their management.

**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.

## Additional Resources

This guide provides information about Select Identity configuration and deployment. Detailed procedures for deployment and system management steps are covered in this guide and in the online help system, which is accessed through the Select Identity client. Actions are grouped by the Select Identity capabilities that govern them. This enables you to delegate specific management actions to internal and partner administrators. The information that they can access in the client pertains to the administrative roles that they have been given.

The Select Identity product documentation also includes the following:

- If you need to develop workflow templates, you can refer to the *HP OpenView Select Identity Installation Guide*. This guide describes installation and configuration information. All installation prerequisites, system requirements, and procedures are covered in detail in this guide. There is also a section that covers the uninstallation procedure for Select Identity. Troubleshooting methods are included in an appendix.
- Each resource connector has an *HP OpenView Connector Installation Guide*. These are located on the Select Identity Connector CD.
- The *HP OpenView Select Identity Workflow Studio Guide* provides detailed information for creating approval processes for managing account provisioning events.
- 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.
- If you need to develop connectors, which enable you to connect to external systems for provisioning, refer to the *HP OpenView Select Identity Connector 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.
- An independent, web-based, API help system is available for integration development and customization tasks. To view this help, double-click the `index.htm` file in the `Docs/API_Help` directory. This directory resides on the HP OpenView Select Identity CD.



# 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.

## Deployment Tasks

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, web single sign-on, 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 29](#).

## 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 may contain information about the user. For example, you may offer a service to your customers that relies on a database, such as Oracle or web single sign-on service, such as

ClearTrust. 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 Oracle system and the ClearTrust 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 34](#).

## 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.

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 49](#).

## 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 57](#).

## Rules

Rules are used by Select Identity to programmatically control processing of an account based on user's attributes when registering for a Service. Rules provide a flexible mechanism for handling exception cases when assigning entitlements, handling exclusions, and monitoring authoritative sources.

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 63](#).

## Notifications

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

You can create templates for the following event types:

### ***Users***

Sends email 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.

***Approval Process***

Sends email to an administrator when an account requires approval, or when an account has not been reviewed within a specified period of time.

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 66](#).

## 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 126](#) for more information.

Creating workflow templates is performed through the Workflow Studio capability. For overview information, see [Workflow Studio on page 72](#). 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 75](#) 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 Business Relationships and Context.

## Business Relationships

A large part of Service creation involves establishing Business Relationships that you want to have with customers and partners. The Business Relationships that you create define how companies, organizations, or divisions access your Services. Business Relationships create a secure context in which partners and users of your Services see only what is relevant to them.

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

## Context

While Business Relationships 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, Business Relationships, 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 Business Relationships
- Create, modify, and delete Context

For more information, see [Services on page 77](#).

## 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 95](#).

Roles are assigned through a user's association with an Admin Service. See [Services on page 77](#) for more information.

## Auto Discovery

The Auto Discovery capability enables you to add multiple users to one or more Services at one time. 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 104](#) 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 Business Relationship 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

For more information, see [Users on page 112](#).

## 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 126](#).



## 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 [Configuration and Audit Reports on page 140](#).

## 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 129](#).

## 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

For more information, see [Account Self Service on page 137](#).

## Deployment Order

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.

After Select Identity is installed, the following items are available for you to begin the deployment process:

An administrative account is created:

Login `sis`

Password `g02sch001`

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 `sis_a` account. This account belongs to the System Administrator role. See [Select Identity Default Roles on page 99](#) for actions.

Follow the sample deployment process.

- 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 for any special cases where Services or entitlements need to be added or excluded.
- 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, Business Relationships, 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. 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.

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

## 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. Record the information here for future reference.

Host name: \_\_\_\_\_

Login ID: \_\_\_\_\_

Port number: \_\_\_\_\_

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

If WebLogic is the application server:

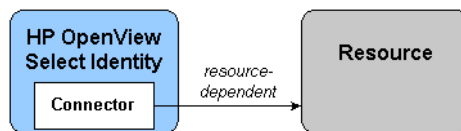
**`http://WebLogic_hostname:7001/lmz/control/home`**

## 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.

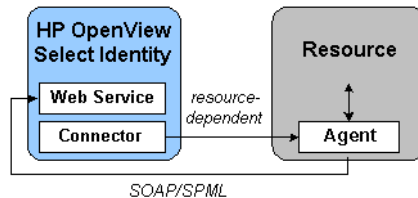
Select Identity supports two types of connectors:

- A one-way connector initiates communication with a resource. If a resource is supported through the use of a one-way connector, user data must be updated in Select Identity and the changes are sent to the resource, to synchronize the resource with Select Identity. 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. This enables the resource to issue a request to Select Identity, and also results in Select Identity issuing a request to the resource. 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 resource issues a request to Select Identity's web service, it must do so over the SOAP protocol and it must send an SPML payload.

## Creating and Installing a Connector

To create a connector that enables Select Identity to connect to a back-end system 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.

Because you must code Java files to build a connector, and you must install the connector by copying its files and configuring Select Identity's supporting application server, the *HP OpenView Select Identity Connector Guide* is provided to explain this information at length. 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 [Additional Resources on page 16](#) 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.

Admin Roles | **Connectors** | Resources | Services | Notifications | Users  
 Request Status | Audit Reports | Configuration Reports | Challenge / Response | WorkFlow Studio | Attributes  
 Auto Discovery | Reconciliation | External Calls | Approvals | Configurations | Rules

Home > Connectors Thursday, July 29, 2004

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

**Connector Information**

\* Connector Name:

\* Pool Name:

\* 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 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.  
Basic connection information is listed, including the connector name and pool name.
- 4 Modify any of the available fields and 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.  
Basic connection information is listed, including the connector name and pool name.



## 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.

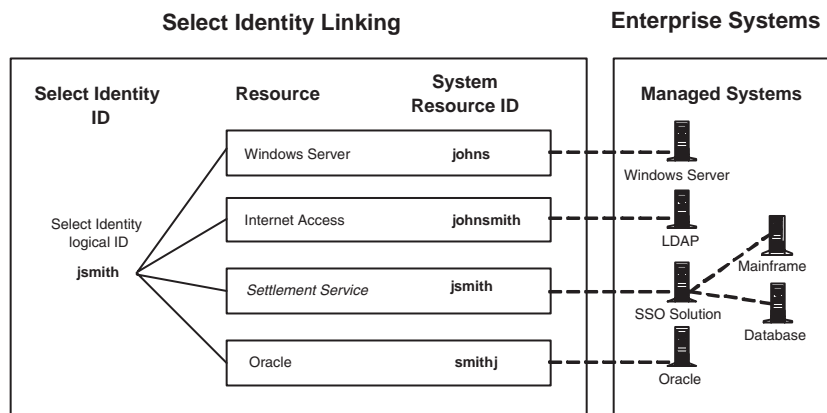
## Resources

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.

Within the Resources section of the client, you can deploy, view, modify, and delete the resources to which Select Identity maps its user IDs. 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, such as ClearTrust. 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.

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 63](#) 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 129](#) for information about Resource 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 29](#) 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.

### Access Information

Make sure that all of your system and connection information is available before adding resources to the Select Identity system. You will be prompted for network connection information and system account access information during the deployment process.

You will need the following access information for each resource that you deploy.

## LDAP for eTrust

Field Name	Sample Values	Description
Resource Name	ETrust	Name of the target resource.
Access URL	ldap://136.168.1.20:389	URL access to the resource.
Suffix	c=AU	Root distinguished name suffix.
Login Name	admin	Name required to log in to the resource.
Password	Password123	Password corresponding to the login account.
User Suffix	ou=ADMINISTRATION, ou=CORPORATE, ou=DEMOCORP	Suffix part of user's distinguished name.
User Object Class	inetorgperson	Object class of users.
Group Suffix	ou=ADMINISTRATION, ou=CORPORATE, ou=DEMOCORP	Suffix part of group's distinguished name.
Group Object Class	OrganizationalUnit	Object class of user groups.
Mapping File	CAEtrust.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

## LDAP for Active Directory

Field Name	Sample Values	Description
Resource Name	ActiveDirectory	Name of the target resource.
Access URL	ldap://136.168.1.20:389	URL access to the resource.
Suffix	dc=qa,dc=hp,dc=com	Root suffix.
Login Name	cn=Directory Manager	Name required to log in to the resource.

Field Name	Sample Values	Description
Password	Password123	Password corresponding to the login account.
User Suffix	cn=users	Suffix of user's distinguished name.
User Object Class	top, person, organizationalPerson,user	Object class of users.
Group Suffix	cn=users	Suffix part of group's distinguished name.
Group Object Class	top,group	Object class of user groups.
Mapping File	ActiveDir.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

## LDAP for iPlanet

Field Name	Sample Values	Description
Resource Name	local_iplanet	Name of the target resource.
Access URL	ldap://localhost:389	URL access to the resource.
Suffix	dc=india, dc=hp	Root suffix.
Login Name	cn=Directory Manager	Name required to log in to the resource.
Password	Password123	Password corresponding to the login account.
User Suffix	ou=people	Suffix of user's distinguished name.
User Object Class	top, person, organizationalPerson,interorgPerson	Object class of users.
Group Suffix	ou=groups	Suffix part of group's distinguished name.

Field Name	Sample Values	Description
Group Object Class	top,groupofuniquenames	Object class of user groups.
Mapping File	iplanet.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

## UNIX with SSH

Field Name	Sample Values	Description
UserName	accountadmin	Login account on the UNIX machine.
UserPassword	Password123	Password for the UserName account.
HostName	Users.mydomain.com	The hostname or ip address of the unix machine to perform user account provisioning.
AdminPassword	rootPassword	Password to gain administrator privileges.
UnixType	Solaris	Type of UNIX operating system that HostName is running.
Ssh	True	Encrypted connection to hostname using the Secure Shell protocol.
sshKnownHosts	knownHosts	The file that contains the list of known hosts for SSH connections. If a connection is made to HostName and its id does not match the id stored in sshKnownHosts, then the connection is denied. This parameter is optional but highly recommended.

Field Name	Sample Values	Description
Port	22	Port to use when connecting to HostName. The default for ssh is 22 and non-ssh is 23. This parameter is optional.
scriptLocation	C:/connectorScripts/	Location for the Bean Shell scripts that are used by the connector.
mappingFile	UnixConnector.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

## UNIX with Telnet

Field Name	Sample Values	Description
Resource Name	Unix-53	Name given to the resource.
Host Name	192.168.1.53	IP Address of the UNIX machine.
UserName	accountadmin	Login account on the UNIX machine.
UserPassword	Password123	Password for the UserName account.
AdminPassword	rootPassword	The password to gain administrator privileges.
Executable	C:/tools/expect-5.21/expect.exe	Path name of the expect executable, required to run scripts.



Field Name	Sample Values	Description
scriptLocation	C:/connectorScripts/ expect/Solaris	Location of the expect scripts that are used by the connector.
mappingFile	UnixConnector-tel.xml	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

### Windows NT Local

Field Name	Sample Values	Description
UserName	Administrator	Administrative account on the target resource.
Password	Password123	Password corresponding to the administrative account.
Server	Myserver	Target resource NETBIOS name or IP address.
ServerPort	5001	Forward connector server port, as configured on the resource agent.

## 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.

Perform the following steps to deploy a resource:

- 1 From the home page of Resources, click **Deploy New Resource**. The Resource Information page displays.

Thursday, July 29, 2004

Home > Resources > Deploy New Resource

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.

Basic Info  
Additional Info  
Access Info

**Resource Information**

\* Resource Name:

Resource Description:

\* Resource Type:

\* Authoritative Source:  Yes  No

\* Delete User:  Yes  No

\* 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.
- 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 Click **Save & Continue** to proceed.

The Additional Information page displays.

Thursday, July 29, 2004

Home > Resources > Deploy New Resource

LDAP

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

Basic Info  
Additional Info  
Access Info

**Resource Information**

Resource Name: LDAP

Manage User

Associate to Group:

Save & Continue Cancel

- 8 You may be asked to associate this resource with a Managed Group, if the system uses the concept of entitlements. Select the check box to create the association.
- 9 Click **Save & Continue** to proceed.

The Resource Access Information page displays.

Home > Resources > Deploy New Resource

LDAP

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

Basic Info  
Additional Info  
Access Info

**Resource Access Information**

\* Resource Name: LDAP

Access URL: ldap://localhost:389

Suffix: dc=com

Login Name: cn=Directory Manager

Password:

\* User Suffix: ou=people

\* User Object Class: top, person, organizationalPerson, in

\* Group Suffix: ou=Groups

\* Group Object Class: top, groupofuniqueNames

\* Mapping File: iPlanet.xml (view)

Test and Submit \* Designates Required Fields Cancel

- 10 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 [Access Information on page 36](#) for examples.


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

## 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 a resource from the Resources drop-down list, or click  to use the search function.
- 2 Select **Modify Resource** from the Actions drop-down list.
- 3 Click **Submit**. The Resource Information page displays.
- 4 You can modify the following information:
  - If you want a description for this resource, you can add or edit one in the Resource Description text box.
  - You can also change the Authoritative Source for this resource.
- 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:conceroc="http://www.trulogica.com/conceroc/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" conceroc:tafield="[User Name]"
```

## 10 Click **Test and Submit**.

Select Identity verifies the connection and updates the resource.




Changing the configuration of a resource can have serious consequences. Select Identity may display a warning and ask you to confirm the action in any of the following cases:

- If you change the URL or IP of the resource
- If there is a filter present and you change it
- If the Select Identity database is not synchronized with 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 a resource from the Resources drop-down list, or click  to use the search function.
- 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.


## 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 a resource from the Resources drop-down list, or click  to use the search function.
- 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, or click  to use the search function.
- 2 Select **View Attributes** from the Actions drop-down list.
- 3 Click **Submit**. The Display Options page displays.

Admin Roles	Connectors	<b>Resources</b>	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Thursday, July 29, 2004

Home > Resources > View Attributes

Select the filter and press submit

Resource Name: ActiveDir

**Display Options**

Order By:

Items Per Page:

- 4 Choose the Order By and Items Per Page options that you want.
- 5 Click **Submit**.

The Search Results page displays.

Admin Roles	Connectors	<b>Resources</b>	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Thursday, July 29, 2004

[Home](#) > [Resources](#) > [View Attributes](#)

List of Resource Attributes (Resource Name=ActiveDir)				
<< < Page 1 of 2 >>				Total Records: 20
Name	Min Length	Max Length	Attribute Mapped To	Authoritative
ActiveDir_ENTITLEMENTS	1	255	ActiveDir_ENTITLEMENTS	Y
ActiveDir_KEY	1	255	ActiveDir_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		

<< < Page 1 of 2 >>

- 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 35](#) for more information.
- 7 You can click **New Search** to change display criteria, or click **Cancel** to return to the Resources home page.



## 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 attributes based on the operating system or application group's information. Select Identity relies on attributes defined for each resource and 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:

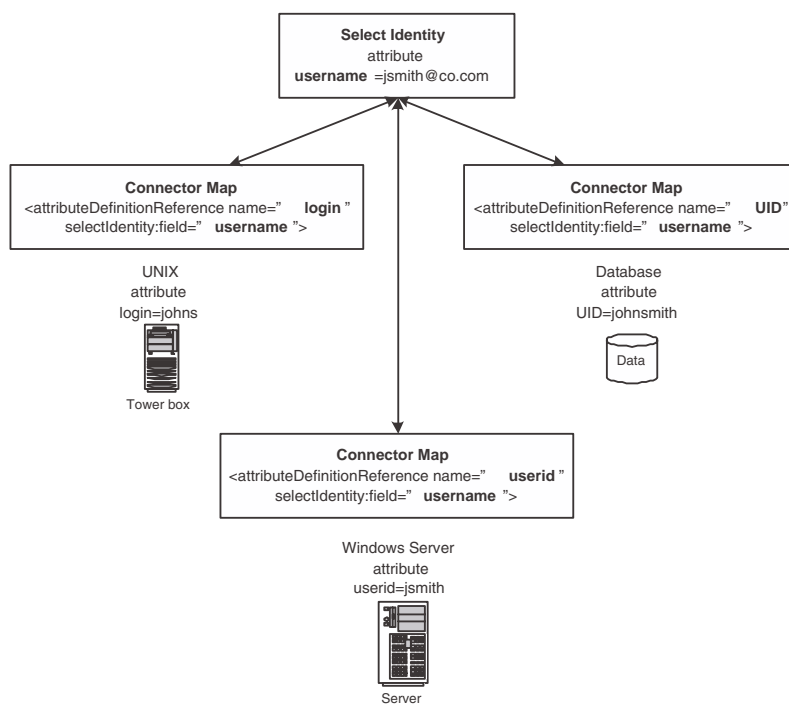
```
- <memberAttributes>
- <!--
  For iPlanet
-->
<attributeDefinitionReference name="UserName" required="true" concero:tafield="[UserName]" concero:resfield="uid" concero:isKey="true" concero:init="true" />
  <attributeDefinitionReference name="Password" required="false"
    concero:tafield="[Password]"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

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.

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

**Figure 3 Attribute Mapping Example**



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

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.
- 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.

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*.

## 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.

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.

Attribute Information	
* Attribute Name	City
* Identity Object Type	User
* Primitive Type	String
* Attribute Type	Normal
* Storage Type	Normal
Description	Specifies the city in which the user resides.
Default Help Text	Enter your city
* Multi Value	<input type="radio"/> Yes <input checked="" type="radio"/> No
* Min Length	1
* Max Length	64
Value Pattern	
* Required	<input type="radio"/> Yes <input checked="" type="radio"/> No
* Default Display Name	City
Default Display Mask	0
Default Display Length	0
Value Constraint Type	None
Value Constraint Function	Search Connector
Value Generation Function	
Value Validation Function	

- 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.
- 6 Choose the storage type for the attribute from the Storage Type drop-down menu. This option determines if the attribute is stored in Select Identity, in a resource, or both.
- 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.
- 13 If you want this attribute to be required, select the **Yes** Required option.
- 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.
- 18 If you want to call a program to constrain the value of the attribute, click  to search for and specify the program. Programs are created in External Calls.
- 19 If you want to call a program to generate the value of the attribute, click  to search for and specify the program.
- 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](#)

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


[Information Mapping](#)

### Attribute Mapping for USCity

Authoritative Resource Attributes:  [Clear Auth](#)

Mapped Resource Attributes:  [Set Auth](#)  
[Remove](#)

[Submit](#) [Cancel](#)

- 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: 20

<input type="checkbox"/> Resource Attribute Name(Resource Name)
<input type="checkbox"/> ActiveDir_ENTITLEMENTS(ActiveDir)
<input type="checkbox"/> ActiveDir_KEY(ActiveDir)
<input type="checkbox"/> Address 1(ActiveDir)
<input type="checkbox"/> Address 2(ActiveDir)
<input type="checkbox"/> Business Phone(ActiveDir)
<input checked="" type="checkbox"/> City(ActiveDir)
<input type="checkbox"/> Description(ActiveDir)
<input type="checkbox"/> Directory(ActiveDir)
<input type="checkbox"/> Email(ActiveDir)
<input type="checkbox"/> First Name(ActiveDir)
<input type="checkbox"/> Home Phone(ActiveDir)
<input type="checkbox"/> Last Name(ActiveDir)
<input type="checkbox"/> Mobile Phone(ActiveDir)
<input type="checkbox"/> Password(ActiveDir)
<input type="checkbox"/> Profile Path(ActiveDir)
<input type="checkbox"/> Script Path(ActiveDir)
<input type="checkbox"/> State(ActiveDir)
<input type="checkbox"/> Title(ActiveDir)
<input type="checkbox"/> User Name(ActiveDir)
<input type="checkbox"/> Zip(ActiveDir)

<< < Page 1 of 1 > >>

[Add](#) [Close Window](#)

- 23 Choose the attribute or attributes that you want to map and click **Add**. When you are finished click **Close Window**.

The Attribute Mapping page displays.

[Home](#) > [Attributes](#) > Add New Attribute

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

Information Mapping

Attribute Mapping for USCity

Authoritative Resource Attributes:  [Clear Auth](#)

Mapped Resource Attributes: City(ActiveDir) [🔍](#)

[Set Auth](#)  
[Remove](#)

[Submit](#) [Cancel](#)

To remove attributes from the Mapped Resource Attributes list, select the attribute and click **Remove**.

- 24 If you want an attribute mapped to the authoritative resource, select it and click **Set Auth**. The attribute is mapped to the resource that you define as the authoritative source. See [Authoritative Sources on page 35](#) for more information.
- 25 When finished, click **Submit**.

## 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 **Mapping** 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 51](#) for details about each field.


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.
- 3 Click **Submit**. The Attribute Information page displays.
- 4 Modify any information you want, except the attribute name.
- 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 Business Relationship 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.



## 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 validate, constrain, or verify the value of identity profile attributes.

Select Identity supports the ability to invoke calls to external systems 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
- Workflow action — performs a task as part of a workflow, enabling you to integrate approval processes with external processes and systems

You must code the classes 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.

## Creating an External Call For Workflow Templates

Select Identity enables you to interact with external systems for Workflow Steps and Approver Lookups. 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.

These functions are created and made available in the Select Identity system through the External Calls pages. For an example, 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 create an external call:

- 1 From the home page of External Calls, click **Add New Call**. The Basic Information page displays.

The screenshot shows the 'Add New Call' form in the Select Identity client. The form is titled 'Basic Information' and contains several fields: 'External Call Name' (text box with 'Constrain Value'), 'Description' (text area), 'Classname' (text box with 'n.selectidentity.truaccess.externalcall.constrain'), 'Classpath: (Separated by:)' (text area), 'Call Type' (dropdown menu with 'Attribute Value Constraint'), and 'Number of Parameters' (text box with '0'). There are also buttons for 'Save & Continue' and 'Cancel', and a note '\* 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.  
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

**Attribute Value Generation** – generates the value of an attribute

**Attribute Value Constraint** – restricts the value of an attribute

**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.

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

Information  
Parameters

Basic Information	
External Call Name:	Search Connector
Parameter Name	Parameter Value
1. resource_name	Active Directory



Submit
Cancel

- 9 Enter the name and value for each parameter that you want to pass to the external system.
- 10 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.
- 2 Select **Modify Call** from the Actions drop-down list.
- 3 Click **Submit**. The Basic Information page displays.
- 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.
- 6 If you have any parameters set, you can modify them here.
- 7 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.
- 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.
- 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.

# Rules

Rules are used by HP OpenView Select Identity to programmatically control processing based on a user's attributes when registering for a Service. Although Select Identity's management model greatly reduces the number of rules required for most deployments, exceptions are sometimes required for complex environments. Rules provide a flexible mechanism for handling exception cases in the assignment of entitlements, exclusion handling, and change monitoring of authoritative sources. Select Identity supports the following types of rules.

Select Identity supports the monitoring, detection, and propagation of data changes within Authoritative Sources. Change monitoring rules define the data attributes that Select Identity considers important when a change occurs. These are the attributes that, if changed, could result in adding, modifying, or deleting one or more users' entitlements or Service access. Change monitoring rules are defined per Service so that a single data change in an authoritative source can be updated across multiple Select Identity Services. See [Authoritative Sources on page 35](#) for more information.

You can create a change detection rule and upload it through the Rules pages.

## Adding a Rule

Rules are used to programmatically assign entitlements to a user who is registering for a Service. Conditions for the rules are based on user attributes fields for a particular Service, such as Address1, Business Phone, Title, or State. The entitlements that are assigned by rules are in addition to the entitlements already selected for this Service.

This procedure requires you to create an XML file that defines the actions to be performed. See [Creating Rules on page 149](#) for details.

Perform the following to define a rule:

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

- 2 Click the **RuleTemplate.xml** link to view or edit the template file, or click **Browse** to select a rule.
- 3 Click **Save Rule** 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 Information page displays.
- 4 Click the **RuleTemplate.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 **Save Rule**.

## 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.

# Notifications

The Notifications section of the client enables you to define the content of email notices that are sent to users and administrators 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.

You can create templates for each of the following event types within the Select Identity system:

## **Users**

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

## **Approval Process**

Sends email to an administrator when an account requires approval or when an account has not been reviewed within a specified period of time.

## Pre-defined Variables

When creating notification templates, you can use variables for administrator names, user names, and email addresses. These variables enable the system to supply the appropriate information based on the action and the user performing the action. The following are available variables:

Variable Type	Description	Variable
Request	Variables for the Request Object. The REQ variable supports two objects: ServiceName RequestId Example: [REQ:RequestId]	<b>REQ:</b>
RequestTarget	Variables for the userID that is being created. All variables from the TAAtrDef table can be used. Example: [RQT:UserName]	<b>RQT:</b>
Requester	Variables for the administrator making the request. All variables from the TAAtrDef table can be used. Example: [RQSTR:UserName]	<b>RQSTR:</b>
Workflow	Variables defined in the workflow template. Workflow variables show workflow information. Currently, the only workflow variable is Approvers Comments. Example: [WF:\$ApproverComments]	<b>WF:</b>
Environment	Variables defined for the environment within properties file. Environment variables provide information such as host or port. Any value that you can perform a System.getProperty() on can be used for this variable.	<b>ENV:</b>

# 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 164](#) 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.

Admin Roles | Connectors | Resources | Services | **Notifications** | Users

Request Status | Audit Reports | Configuration Reports | Challenge / Response | Workflow Studio | Attributes

Auto Discovery | Reconciliation | External Calls | Approvals | Configurations | Rules

Home > Notifications > Add New Notification Template Thursday, July 29, 2004

Add template name, description and select other parameters for new notification template. Click "Save & Continue" when finished. Information Content

**Template Information**

\* Template Name:

Template Description:

\* Category:

\* 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.
  - Select **Approval Process** to define a template that administrators will see when an account needs approval.

## 5 Click **Save & Continue**.

The Content page displays.

Admin Roles	Connectors	Resources	Services	<b>Notifications</b>	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Thursday, July 29, 2004

Home > Notifications > Add New Notification Template

► Add User

Enter the required information for the notification template and click "Submit" when finished.

Information	<b>Content</b>
-------------	----------------

Template Information	
* Template Name:	Add User
Sender Name:	<input type="text" value="admin_a"/>
Sender Email:	<input type="text" value="admin@company.com"/>
To Email:	<input type="text" value="user@company.com"/>
CC Email:	<input type="text"/>
BCC Email:	<input type="text"/>
* Subject:	<input type="text" value="Access to Service"/>
* Body:	<input type="text" value="Welcome to ABC Service!&lt;br/&gt;Please login and change your password."/>

\* Designates Required Fields


- 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 [Pre-defined Variables on page 67](#) 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](#).
- 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 68](#).
- 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 68](#).

- 5 Click **Save & Continue** after completing your changes on each page.
- 6 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.

## 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 57](#) 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 Business Relationship. (A Business Relationship is created as part of a Service.) 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 95](#) for more information.
- Sending email using one of the email templates created on the Notifications home page. See [Notifications on page 66](#) for more information.
- Calling external systems registered with Select Identity on the External Calls home page. See [External Calls on page 57](#) 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.

## 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 password hints for the system.

The Select Identity challenge and response policy governs the password hints for the system. You can also restrict login attempts with this 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. Hint

**Your Password Hints**

Existing Challenge(s):

What is your pet's name?	<input type="checkbox"/> Delete
What is your favorite color?	<input type="checkbox"/> Delete
What is your least favorite animal?	<input type="checkbox"/> Delete
Do you LOVE Select Identity?	<input checked="" type="checkbox"/> Delete

New Challenge(s):

To change password, user required to answer  challenge(s)

Account will be locked after:  incorrect Challenge/Response submission(s)

Modify Cancel

- 2 Modify any of the fields. You can
  - 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**.

## 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 things 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, policies, 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 Business Relationships, which provide a secure management structure and view for your partners and customers. Business Relationships are hierarchical and management can be delegated to any level.

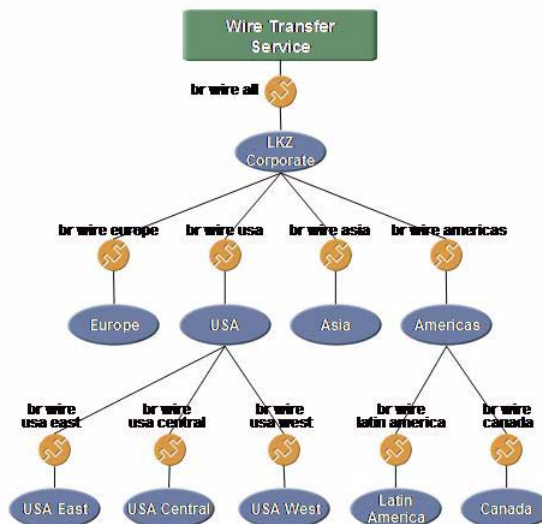
This chapter provides details for all of the actions that you can perform within the Services pages. Access to each of these functional areas is determined by the administrative roles assigned to your account by the Select Identity system administrator.

## Business Relationships

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

The following example illustrates a simple structure as defined by a Business Relationship hierarchy.

**Figure 4 Business Relationship Hierarchy**



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

Attributes defined at the Business Relationship 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 Business Relationship 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 Business Relationship (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 Business Relationships and Context on page 88](#) for detailed procedures.

## Creating and Modifying Services

The Services section enables you to add, modify, and delete the Services that are accessed by your customers and business partners. These Services, in addition to the Business Relationship structure that you establish, form a management structure for users of the Select Identity system.

You can also set Business Relationships and context from the Services pages. Services are made available to your customers and partners by setting a Business Relationship in Select Identity.



Some of the steps in the following procedures reference other capabilities and actions within Select Identity. Cross references are provided where appropriate. Because there are many ways to deploy the Select Identity system, review these sections to determine the order that is right for you.

## 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 Basic Info page displays.

Home > Services > Add Service Thursday, July 29, 2004


To deploy a new managed service, complete the required fields in the form below. Use the Search Menu box to choose the Resources 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. Click 'Create' when finished

Service Information	
* Service Name:	ABC Service
* Service Type:	Business Service
Resources:	ActiveDir
* Attributes:	ActiveDir_ENTITLEMENTS Addr1 Addr2 City Company
* Context Attribute:	ActiveDir_ENTITLEMENTS
* Primary User Key:	ActiveDir_ENTITLEMENTS

\* Designates Required Fields

- 2 Enter a name for the Service in the Service Name field.
- 3 Click  to locate and add resources to support the Service. You can add multiple resources at one time from the Search Results page.




- 4 Click  to locate and add attributes to support the Service. You can add multiple attributes at one time from the Search Results page.
- 5 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.”
- 6 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.
- 7 Click **Create**.

If this Service requires the configuration of Business Relationships, it will remain in the Pending state until activated by the association of Business Relationships and Context.

## Modifying a 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. The pages that are displayed are the same as the pages in the previous procedure.

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Modify Service** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Modify the information that is available to you.  
The pages and fields are the same as in the Deploy New Service procedure on [page 80](#).
- 5 Click **Modify** after completing your changes.

## Deleting a Service

You can delete a Service from the Select Identity system. Make sure to notify your customers and users before doing so.

Perform the following steps to delete a Service:


- 1 From the home page of Services, click  to search for and select a Service.
- 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 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.

## Creating a Service View

Perform the following steps to create a Service view:

- 1 From the home page of Services, click  to search for and select a Service.
- 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: <input type="text" value="Finance A"/>								
<input type="checkbox"/>	Name	Order	Display Name	Length	Mask	Require	Visible	Update
<input checked="" type="checkbox"/>	City	5	City	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Control_SA_KEY	0	Control SA_KEY	40	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	UserName	1	UserName	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	GUID	2	GUID	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Control_SA_ENTITLEMENTS	4	Control SA_ENTITLEMENT	40	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Email	3	Email	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="button" value="Create"/>		* Designates Required Fields					<input type="button" value="Cancel"/>	

- 4 Enter a name for this view in the Service View Name field.
- 5 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.
- 6 Order the fields that you want displayed by entering numbers in the Order column.
- 7 You can edit the name that is displayed to users in the Display Name fields.
- 8 Define or change the maximum length of each value in the Length column.
- 9 If you want all or a portion of the value masked, enter that number of characters in the Mask column.
- 10 If you want to require a field, select its check box in the Require column.
- 11 If you want a field to be visible on the registration page, select its check box in the Visible column.
- 12 If you want to give users permission to update a field value, select its check box in the Update column.
- 13 Click **Create**.

## Modifying a Service View


Perform the following steps to modify a Service view:

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Modify View** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Click  to search for and select a Service view. 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, click  to search for and select a Service.
- 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**.


# 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 super-set for Business Relationship and context creation.

## Setting Service Attribute Values

You can restrict the values that a user can select from when registering for a Service. 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, click  to search for and select a Service.
- 2 Select **Set Service Attribute Values** from the Actions drop-down list.
- 3 Click **Submit**. The Attribute Selection page displays.

Admin Roles	Connectors	Resources	<b>Services</b>	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Thursday, July 29, 2004

[Home](#) > [Services](#) > [Set Service Attribute Values](#)

For each attribute, you may pre-define a set of valid values. Highlight the defined attribute in the left hand side Defined Attributes selection box. Type in a valid value for the defined attribute in the Attribute Values text box and click 'Add'. Or, search for existing Attribute Values by clicking on the search icon. You will see the value appear in the Defined Attribute Values selection box. Repeat for each attribute you wish to set in the predefined list of valid values. Click 'Apply' when finished.

**Service Attribute**

Defined Attributes:

**Defined Values**

Constraint Display Name:

Constraint Value:

Mississippi - MS


Kansas - KS

Texas - TX

Illinois - IL

Ohio - OH


\* Designates Required Fields

- 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 **Add** button and search icon display.
- 5 Click  to search for and select the values that you want to set for this attribute.
- 6 After values are selected, click **Add**.
- 7 If you want to constrain the display name and value for this attribute, enter the name and value pair in the constrain fields.
- 8 Click **Apply**.

## Setting Service Attribute Properties

You can require a set of attributes or set properties that are specific for a Service.

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

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Set Service Attribute Properties** from the Actions drop-down list.
- 3 Click **Submit**.

## The Attribute Selection page displays.

[Home](#) > [Services](#) > [Set Service Attribute Properties](#)

Choose the order in which the function associated to the attributes will be processed. Not all attributes have a function associated to them, and therefore, not all attributes require an Process Order number. To make an attribute required during registration, check the box in the Required column. To allow an attribute to contain more than one value, check the box in the Multi Value column. Provide a user friendly name that will appear on the registration screen by filling in the text box under Display Name. Click "Apply" when finished.

Service Attribute Name	Process Order	Required	Multi Value	Display Name
Consolidated Directory_ENTITLEMENTS	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Consolidated Directory_ENTITL
Consolidated Directory_KEY	12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Consolidated Directory_KEY
Country	3	<input type="checkbox"/>	<input type="checkbox"/>	Country
Department	8	<input type="checkbox"/>	<input type="checkbox"/>	Department Name
Email	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Email
FirstName	9	<input type="checkbox"/>	<input type="checkbox"/>	First Name
GUID	5	<input type="checkbox"/>	<input type="checkbox"/>	GUID
Hierarchy	13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Hierarchy
LastName	4	<input type="checkbox"/>	<input type="checkbox"/>	Last Name
Password	10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Password
Person Number	3	<input type="checkbox"/>	<input type="checkbox"/>	Person Number
SSN	11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SSN
Standard ID	14	<input type="checkbox"/>	<input type="checkbox"/>	Standard ID (H)
State	6	<input type="checkbox"/>	<input type="checkbox"/>	State
UserName	2	<input type="checkbox"/>	<input type="checkbox"/>	Standard ID

[Apply](#)

[Cancel](#)

- 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.

# Defining Business Relationships and Context

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

Defining a Business Relationships 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.


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

The following procedures enable you to set and view Business Relationships and define context for each of your Services.

## Creating a Business Relationship

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

Perform the following steps to set a Business Relationship:

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Create Business Relationship** from the Actions drop-down list.
- 3 Click **Submit**.










The Business Relationship Information page displays.

The screenshot shows the 'Business Relationship Information' page. At the top, there is a field for 'Business Relationship Name' with the value 'Online Banking'. Below this, the page is divided into several sections:

- Notification Events:** This section contains two tables. The first table, 'Notification Events', lists 'Add User - Success' and 'Approve'. The second table, 'Notifications', lists 'Email Verification'.
- Event Handlers:** This section contains two tables. The first table, 'Request Events', lists 'DELEGATED:add operation'. The second table, 'Workflow Template', lists 'single\_approval\_workflow'.
- Fixed Attributes:** This section contains a 'Name' field with a dropdown menu showing 'Control\_SA\_ENTITLEMEN' and a 'Value' field with a dropdown menu showing 'Control\_SA\_ENTITLEMENTS - ""'.

At the bottom of the page, there are 'Create' and 'Cancel' buttons, and a note that '\* Designates Required Fields'.



- 4 Enter a name for the new Business Relationship in the Business Relationship Name field.
- 5 Click  to search for and select the Notification events that you want available for this relationship.
  - 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 66](#) for information about notification policies.
- 6 Click  to search for and select the Request events and that you want set for this relationship. See [Event Reference on page 164](#) for a list of events and actions within Select Identity.
  - 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 72](#) 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 event.
- 7 Select the fixed attributes that you want assigned to users enabled for this Business Relationship. You can select multiple attributes. See [Attributes on page 49](#) for information about attributes and values.
    - a Choose an attribute from the Name drop-down list. This list is provided by the parent Business Relationship.
    - 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 .
  - 8 Click **Create**.

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

## Modifying a Business Relationship



Perform the following steps to modify a Business Relationship:

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Modify Business Relationship** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Click  to search for and select the Business Relationship that you want to modify.
- 5 Modify any of the available fields.
- 6 Click **Modify**.

## Deleting a Business Relationship

Before you delete a Business Relationship, make sure that the Context settings for this relationship have been deleted.


Perform the following steps to delete a Business Relationship:

- 1 From the home page of Services, click  to search for and select a Service.
- 2 Select **Delete Business Relationship** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Click  to search for and select the Business Relationship that you want to modify. The Business Relationship Information page displays.
- 5 Click **Delete**.

## Creating Context




Context enables you to assign a Business Relationship 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 business relationship:



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



The Service Context Information page displays.

The screenshot shows a web form titled "Service Context Information". It contains three required text input fields: "Service Context Name" (containing "New York"), "Business Relationship" (containing "Online Banking"), and "City" (containing "New York"). Each field has a search icon to its right. Below these fields are two main sections: "Notification Event Handlers" and "Event Handlers". The "Notification Event Handlers" section contains two empty tables: "Notification Events" and "Notifications". The "Event Handlers" section contains two empty tables: "Request Events" and "Workflow Template". At the bottom of the form, there is a "Create" button on the left, a "Cancel" button on the right, and a note in the center: "\* 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 Business Relationship. The Business Relationship provides a superset of attributes, workflow processes, and policies that you can choose from.
- 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 “Country” as the context attribute for this Service, you would select a value such as “India” to create this context.

When you choose the parent Business Relationship, other options display.



- 8 Click  to search for and select the Notification events that you want available for this relationship. If the Business Relationship 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 66](#) for information about notification policies.

- 9 Click  to search for and select the Request events and that you want set for this relationship. If the Business Relationship 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 72](#) 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, click  to search for and select a Service.
- 2 Select **Modify Context** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Click  to search for and select the context that you want to modify. The Service Context Information page displays.
- 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, click  to search for and select a Service.
- 2 Select **Delete Context** from the Actions drop-down list.
- 3 Click **Submit**.
- 4 Click  to search for and select the context that you want to delete.
- 5 Click **Delete**.

## 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.

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 by registering for a Service or 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.

[Admin Function Management](#) | [Connector Management](#) | [Resource Management](#) | [TA Service Management](#) |  
[Notification Policy](#) | [User Management](#) | [WorkFlow Studio](#) | [Attribute Management](#) | [External Call Management](#) |



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	<div data-bbox="706 338 975 451"> <p><b>Admin Roles</b> <span style="float: right;">select all</span></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Admin Role</li> <li><input checked="" type="checkbox"/> Add Admin Role</li> <li><input checked="" type="checkbox"/> Modify Admin Role</li> <li><input checked="" type="checkbox"/> Delete Admin Role</li> </ul> </div>
Connectors	<div data-bbox="706 494 975 607"> <p><b>Connectors</b> <span style="float: right;">select all</span></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Connector</li> <li><input checked="" type="checkbox"/> Deploy Connector</li> <li><input checked="" type="checkbox"/> Modify Connector</li> <li><input checked="" type="checkbox"/> Delete Connector</li> </ul> </div>
Resources	<div data-bbox="706 651 975 781"> <p><b>Resources</b> <span style="float: right;">select all</span></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Resource</li> <li><input checked="" type="checkbox"/> Deploy Resource</li> <li><input checked="" type="checkbox"/> Modify Resource</li> <li><input checked="" type="checkbox"/> Delete Resource</li> <li><input checked="" type="checkbox"/> View Resource Attributes</li> </ul> </div>
Services	<div data-bbox="706 824 975 1189"> <p><b>Services</b> <span style="float: right;">select all</span></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Add Service</li> <li><input checked="" type="checkbox"/> View Service</li> <li><input checked="" type="checkbox"/> Modify Service</li> <li><input checked="" type="checkbox"/> Delete Service</li> <li><input checked="" type="checkbox"/> Set Service Attribute Values</li> <li><input checked="" type="checkbox"/> Set Service Attribute Properties</li> <li><input checked="" type="checkbox"/> Create View</li> <li><input checked="" type="checkbox"/> Modify View</li> <li><input checked="" type="checkbox"/> Delete View</li> <li><input checked="" type="checkbox"/> Create Business Relationship</li> <li><input checked="" type="checkbox"/> Modify Business Relationship</li> <li><input checked="" type="checkbox"/> Delete Business Relationship</li> <li><input checked="" type="checkbox"/> Create Context</li> <li><input checked="" type="checkbox"/> Modify Context</li> <li><input checked="" type="checkbox"/> Delete Context</li> </ul> </div>
Notifications	<div data-bbox="706 1232 975 1362"> <p><b>Notifications</b> <span style="float: right;">select all</span></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Notification Template</li> <li><input checked="" type="checkbox"/> Add Notification Template</li> <li><input checked="" type="checkbox"/> Copy Notification Template</li> <li><input checked="" type="checkbox"/> Modify Notification Template</li> <li><input checked="" type="checkbox"/> Delete Notification Template</li> </ul> </div>

Capability	Actions
Users	<p><b>Users</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Service Membership</li> <li><input checked="" type="checkbox"/> Add New User</li> <li><input checked="" type="checkbox"/> Modify User</li> <li><input checked="" type="checkbox"/> Enable Service Membership</li> <li><input checked="" type="checkbox"/> Disable Service Membership</li> <li><input checked="" type="checkbox"/> Delete Service Membership</li> <li><input checked="" type="checkbox"/> Enable All Services</li> <li><input checked="" type="checkbox"/> Disable All Services</li> <li><input checked="" type="checkbox"/> Reset Password</li> <li><input checked="" type="checkbox"/> Terminate User</li> <li><input checked="" type="checkbox"/> Add Service</li> <li><input checked="" type="checkbox"/> View User Attributes</li> <li><input checked="" type="checkbox"/> Manage User Expiration</li> </ul>
Request Status	<p><b>Request Status</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User Request</li> </ul>
Audit Reports	<p><b>Audit Reports</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Service Audit Report</li> <li><input checked="" type="checkbox"/> User Audit Report</li> <li><input checked="" type="checkbox"/> User Audit Summary Report</li> </ul>
Configuration Reports	<p><b>Configuration Reports</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> User Configuration Report</li> <li><input checked="" type="checkbox"/> User Configuration Summary Report</li> </ul>
Challenge/ Response	<p><b>Challenge / Response</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Modify Challenge / Response</li> </ul>
Workflow Studio	<p><b>Workflow Studio</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Add Workflow Template</li> <li><input checked="" type="checkbox"/> Modify Workflow Template</li> <li><input checked="" type="checkbox"/> Delete Workflow Template</li> </ul>
Attributes	<p><b>Attributes</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Add Attribute</li> <li><input checked="" type="checkbox"/> View Attribute</li> <li><input checked="" type="checkbox"/> Modify Attribute</li> <li><input checked="" type="checkbox"/> Delete Attribute</li> </ul>
Auto Discovery	<p><b>Auto Discovery</b> <a href="#">select all</a></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Schedule User Discovery</li> <li><input checked="" type="checkbox"/> View User Discovery Status</li> <li><input checked="" type="checkbox"/> Schedule Services Assignment</li> <li><input checked="" type="checkbox"/> View Assignment Status</li> </ul>

Capability	Actions
Reconciliation	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px;"><b>Reconciliation</b> <span style="float: right; font-weight: normal; color: white;">select all</span></div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Add New Automated Job</li> <li><input checked="" type="checkbox"/> View Automated Job</li> <li><input checked="" type="checkbox"/> Modify Automated Job</li> <li><input checked="" type="checkbox"/> Delete Automated Job</li> <li><input checked="" type="checkbox"/> One Time Task</li> <li><input checked="" type="checkbox"/> View Task Status</li> </ul> </div>
External Calls	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px;"><b>External Calls</b> <span style="float: right; font-weight: normal; color: white;">select all</span></div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> View Call</li> <li><input checked="" type="checkbox"/> Add New Call</li> <li><input checked="" type="checkbox"/> Modify Call</li> <li><input checked="" type="checkbox"/> Delete Call</li> </ul> </div>
Approvals	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px;"><b>Approvals</b> <span style="float: right; font-weight: normal; color: white;">select all</span></div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Approval</li> </ul> </div>
Rules	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px;"><b>Rules</b> <span style="float: right; font-weight: normal; color: white;">select all</span></div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Add Rule</li> <li><input checked="" type="checkbox"/> Modify Rule</li> <li><input checked="" type="checkbox"/> View Rule</li> <li><input checked="" type="checkbox"/> Delete Rule</li> </ul> </div>
Configurations	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px;"><b>Configurations</b> <span style="float: right; font-weight: normal; color: white;">select all</span></div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Export configuration</li> <li><input checked="" type="checkbox"/> Import Configuration</li> </ul> </div>

## Select Identity Default Roles

Select Identity offers several default roles that you can use “as-is” or modify to better match your business requirements. All roles have access to Self Service, which enables administrators to view account profiles.

The following roles are available by default:

***End User***

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.

***Approver***

An Approver can perform account provisioning actions. An administrator 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.

## 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.



Part of the administrator management process is granting roles to new and existing administrator accounts. Defining roles before adding administrators expedites the process.

## 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 Under Root**. The Role Definition page displays.

Home > Admin Roles > Add New Role

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

**Function Name:** Service Admin

**Function Description:** Performs administrative tasks for a given Service.

Admin Roles	select all
<input checked="" type="checkbox"/> View Admin Role	
<input checked="" type="checkbox"/> Add Admin Role	
<input checked="" type="checkbox"/> Modify Admin Role	
<input checked="" type="checkbox"/> Delete Admin Role	

Challenge / Response	select all
<input checked="" type="checkbox"/> Modify Challenge / Response	

Workflow Studio	select all
<input checked="" type="checkbox"/> Add Workflow Template	
<input checked="" type="checkbox"/> Modify Workflow Template	
<input checked="" type="checkbox"/> Delete Workflow Template	

Connectors	select all
<input checked="" type="checkbox"/> View Connector	
<input checked="" type="checkbox"/> Deploy Connector	
<input checked="" type="checkbox"/> Modify Connector	
<input checked="" type="checkbox"/> Delete Connector	

Attributes	select all
<input checked="" type="checkbox"/> Add Attribute	
<input checked="" type="checkbox"/> View Attribute	
<input checked="" type="checkbox"/> Modify Attribute	
<input checked="" type="checkbox"/> Delete Attribute	

Resources	select all
<input checked="" type="checkbox"/> View Resource	
<input checked="" type="checkbox"/> Deploy Resource	

Auto Discovery	select all
----------------	------------

- 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 96](#).


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, click  to search for and select the role that you want to modify.
- 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 96](#).
  - 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, click  to search for and select the role that you want to modify.
- 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, click  to search for and select the role that you want to modify.
- 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 add user accounts to HP OpenView Select Identity and system resources. You can create an XML file with account data and upload it through the Auto Discovery pages.

## Using an SPML Data File

User accounts are uploaded into the Select Identity system using an SPML data file. After the job created to run this file completes, a “results” file is sent to the administrator who scheduled the upload process. The results file is also an XML file.

Have the resources and variable entitlements that you want to assign to each account available. You can specify them in the data file. All other fixed entitlements and entitlements granted through rules are automatically assigned.

Each account that is added must have a unique user ID within Select Identity. If an account exists within the Select Identity system, the information in this file is not added and an exception displays in the results file.



The following is an excerpt of the file:

```

<?xml version="1.0" encoding="ISO-8859-1" ?>
- <batchRequest xmlns:countries="countries.uri"
  xmlns:cities="cities.uri"
  xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
  xmlns:spml="urn:oasis:names:tc:SPML:1:0"
  xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
- <operationalAttributes xmlns="">
  - <attr name="urn:trulogica:conceroc:2.0#keyFields">
    <value>Person Number</value>
  </attr>
</operationalAttributes>
- <addRequest requestID="1">
  - <operationalAttributes xmlns="">
    - <attr name="urn:trulogica:conceroc:2.0#taUserName">
      <value>JUN214</value>
    </attr>
    - <attr name="urn:trulogica:conceroc:2.0#taResourceKey">
      <value>61260214</value>
    </attr>
  </operationalAttributes>
- <attributes xmlns="">
  - <attr name="Client Type">
    <value>1</value>
  </attr>
  - <attr name="Hierarchy Code">
    <value>HC</value>
  </attr>
  - <attr name="Hierarchy">
    <value>HP</value>
  </attr>
  - <attr name="Department Name">
    <value>MATCH***</value>
  </attr>
  ...

```

The file must begin and end with `<batchRequest></batchRequest>`.

The first operational attribute defines the key attribute that is used to search for accounts in the Select Identity database.

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.

All other attributes listed for each account are the required fields that are defined in the delegated registration section for this particular Service. The attribute name must match the field name exactly. If a required field is missing, an exception is listed in the results file.

The following is an example of the results that are sent to the administrator after this job completes:

```
<?xml version="1.0" ?>
- <batchResponse xmlns="urn:oasis:names:tc:SPML:1:0"
xmlns:dsm1="urn:oasis:names:tc:DSML:2:0:core"
xmlns:Select Identity="http://www.hp.com/Select Identity/2.0"
processing="urn:oasis:names:tc:SPML:1:0#sequential"
onError="urn:oasis:names:tc:SPML:1:0#resume">
    result="failed" job="jj107" admin="16103" service="Finance -
latest" totalInputRecord="8" success="4" fail="4">
    <addResponse requestID="ab@company.com" result="submitted" />
    <addResponse requestID="cd@company.com" result="submitted" />
    <addResponse requestID="ef@company.com" result="submitted" />
    <addResponse requestID="sup@company.com" result="submitted" />
    <addResponse requestID="financeadmin@company.com"
result="failed">
        <errorMessage>Finance -latest: Wrong Group Name FINANCE ADMIN
is missing or contains invalid characters.
</errorMessage>
    - <attributes>
        - <attr name="First Name">
            <value>John</value>
        </attr>
        - <attr name="Middle Name">
            <value>H</value>
        </attr>
```

The errors are listed at the beginning of the file so that you can view them quickly. 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.

For more information about SPML files, see [Creating SPML Files on page 158](#).

# Scheduling Auto Discovery

You can configure Select Identity to add user accounts at regular intervals. This process enables Select Identity to add account data to the system from a data file that you create. See [Using an SPML Data File on page 104](#) 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.


Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

Home > Auto Discovery > Schedule Discovery

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'.

Auto Discovery Upload Configuration	
* Select a Resource	LDAP71 
* Job Name	Auto Discovery 1
* Upload File Path	C:\Documents and Settings\Todd\ 
Email CC:	<input type="text"/>
* Job Execution Date	2004-7-31 

- 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 [Using an SPML Data File on page 104](#) 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.

- 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.

- Click **Submit**.

The job is added and will run when scheduled.

## Viewing Discovery Status

You can view the status of previously scheduled jobs.

Perform the following steps to view job status:

- From the home page of Auto Discovery, select **View User Discovery Status** from the Actions drop-down list.
- Click **Submit**.

The Search Information page displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Home > Auto Discovery > View Discovery Status Friday, July 30, 2004

Choose the Job Name, Resource Name and Scheduled Date search criteria, enter or select the search string in the Job Name, Resource Name and Scheduled Date box and choose the desired display options. Leave the Job Name text box empty to display all records. Click "Submit" when finished.

Search Information	
Job Name:	Begins with <input type="text" value="LDAP"/>
Resource Name:	Exact <input type="text" value="LDAP177"/> 🔍
Scheduled Date:	Exact <input type="text"/>
Display Options	
Items Per Page:	20

- Enter search values for the job name.
- Enter search values or click 🔍 to locate the resource name.
- Enter search values for the schedule date.
- Define how you want to view search results.
- Click **Submit**.

The Search Results page displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Home > Auto Discovery > View Discovery Status Friday, July 30, 2004

**List of Auto Discovery Jobs**

<<< Page 1 of 1 >>> Total Records: 2

Job ID	Job Name	Resource Name	Scheduled Date	Status	User ID
1022	au1	LDAP177	2004-07-30	Complete	1006
1107	AU1b	LDAP177	2004-07-30	Complete	1006

<<< Page 1 of 1 >>>

The jobs that match your search criteria are listed.

## Scheduling Service Assignments

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.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Home > Auto Discovery > Schedule Service Assignment Friday, July 30, 2004

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

Email CC

\* Job Execution Date

Select Services

- 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 Service 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.


Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Home > Auto Discovery > View Assignment Status Friday, July 30, 2004

Select the filter and press submit

<b>Search Information</b>		
Job Name:	Begins with	<input type="text"/>
Scheduled Date:	Exact	<input type="text"/>
<b>Display Options</b>		
Order By:	Job ID	ascending
Items Per Page:	20	

- 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.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
<b>Auto Discovery</b>	Reconciliation	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

[Home](#) > [Auto Discovery](#) > [View Assignment Status](#)

List of Service Assignment Jobs				
<< < Page 1 of 1 > >>				Total Records: 4
Job ID	Job Name	Scheduled Date	Status	User ID
1108	ServAS1	2004-07-30	Completed	1006
1113	ServAssing2	2004-07-30	Completed	1006
1209	svass3	2004-07-30	Completed	1006
1210	All Serv	2004-07-30	Completed	1006

<< < Page 1 of 1 > >>

The jobs that match your search criteria are listed.

# 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 77](#) for information about Services and context. See [Attributes on page 49](#) for information about attributes.

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.

- 2 Click  to search for and select the Services that you want to associate to the user.
- 3 Click **Continue** to proceed.

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

- 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 Business Relationships and Context on page 88](#) for information about context and context attributes.

5 Click **Continue**. The Service Display page displays.

Admin Roles Connectors Resources Services Notifications **Users**

Request Status Audit Reports Configuration Reports Challenge / Response WorkFlow Studio Attributes

Auto Discovery Reconciliation External Calls Approvals Configurations Rules

Friday, July 30, 2004

Home > Users > Add New User

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. Click "Submit" when finished.

Service	Reviewed
atbs1 (Business Service)	NO
atbe1 (Business Service)	NO

Provisioning Schedule Information

Schedule Time:

Service  
Context Attribute  
**Service Display**  
Attributes

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

Home > Users > Add New User

Insert the required attributes for the user and click "Save & Continue" when finished.

Attribute Information	
Password:	<input type="password"/> Password
* City:	<input type="text" value="Austin"/> City
* LastName:	<input type="text" value="Middlebrook"/> LastName
Email:	<input type="text"/> Email
* State:	<input type="text" value="Texas"/> State
* FirstName:	<input type="text" value="K"/> FirstName
* UserName:	<input type="text" value="kmiddlebrook"/> UserName
Title:	<input type="text"/>

\* Designates Required Fields

Service  
Context Attribute  
Service Display  
**Attributes**

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

If this is an Admin Service, 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 this 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:	<input type="text" value="AEAA"/> <span>🔍 🗑️</span> <input type="checkbox"/> All
Context Attribute Information For Service: atb2LDAP70	
* Hierarchy:	<input type="text"/> <span>🔍 🗑️</span> <input checked="" type="checkbox"/> All

\* Designates Required Fields

Service  
 Context Attribute  
 Service Display  
 Attributes  
 Admin Service  
 Contexts

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

- 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.

## 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.

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 Click  to search for and select the Services for which you want to modify this user's information.
- 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.
- 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.
- 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 Business Relationships and Context on page 88](#) 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. If you would like to delete a user account from a Service, see [Deleting a Service Membership on page 120](#).

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 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 120](#).

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.

[Home](#) > [Users](#) > [View Service Membership](#)  
 ▶ [GregVgv@tl.com](#)

Review the information for the user. If you need to make any modifications, you must select the [Modify User Account](#) Management main page.


User Information	
User Name:	GregVgv@tl.com
Email:	gv@tl.com
Status:	Created
User Information For Service: \$UNIX-TESTJOBCODE <span style="float: right;">Status: Enabled</span>	
SSN:	*****6789
W2K Domain:	CORP
Client Type:	1
Client Status:	A
GUID:	1EABCF3A-E4E2-035E-89E2-2774BD3E9DA6
Title:	
City:	
Telephone Number:	
Personnel Source:	
Date of Birth:	1975-6-11
Company Number:	110
Middle Name:	C
Last Name:	V

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. 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.

## 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 120](#).

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 from 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-1D5E38A568F1
LDAP211_ENTITLEMENTS	CD Group2 QA Managers
Company Name	HP
UserName	jen211
LDAP177_ENTITLEMENTS	USA Central
LDAP211_KEY	jen211
Email	tvo@trulogica.com

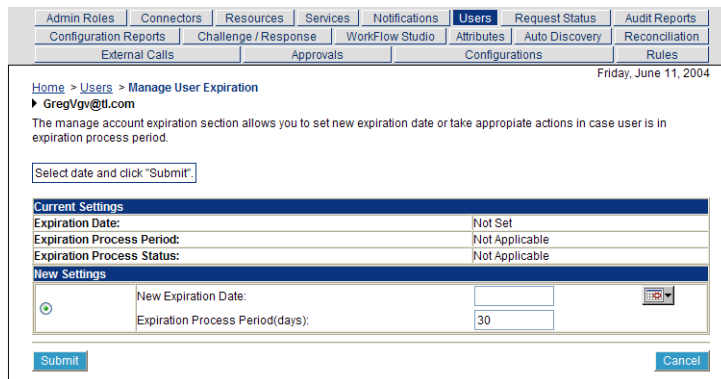
# Managing User Account Expiration

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.



Admin Roles | Connectors | Resources | Services | Notifications | **Users** | Request Status | Audit Reports

Configuration Reports | Challenge / Response | WorkFlow Studio | Attributes | Auto Discovery | Reconciliation

External Calls | Approvals | Configurations | Rules


Home > Users > Manage User Expiration Friday, June 11, 2004

▶ GregVgv@tl.com

The manage account expiration section allows you to set new expiration date or take appropriate actions in case user is in expiration process period.

Select date and click "Submit".

Current Settings	
Expiration Date:	Not Set
Expiration Process Period:	Not Applicable
Expiration Process Status:	Not Applicable

New Settings	
<input type="radio"/>	New Expiration Date: <input type="text"/> 
<input type="radio"/>	Expiration Process Period(days): <input type="text" value="30"/>

Submit Cancel

- 4 Click the calendar icon to select a new date for account expiration, or enter a range of days.
- 5 Click **Submit**.

# 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 accounts that are pending. You will receive email notification when an account is pending your approval.

Perform the following steps to approve or reject an account:

- 1 From the home page of Approvals, choose a date range from the Period options and account status (**All**, **Pending**, **Approved**, **Rejected**) from the Display Options fields.

The screenshot shows the 'Approvals' page interface. At the top, there is a blue header bar with the word 'Approvals' in white. Below the header, the breadcrumb 'Home > Approvals' is visible on the left, and the date 'Friday, July 30, 2004' is on the right. A message box states: 'To display your workflow approvals, select a timeframe and the desired Display Options. Click 'Display' when finished.' Below this is the 'Workflow Approval' form. The form is divided into two columns: 'Period' and 'Display Options'. Under 'Period', there are two date pickers: 'From: 2004-7-1' and 'Through: 2004-7-30'. Under 'Display Options', there are two dropdown menus: 'Status: All' and 'Items Per Page: 20'. At the bottom left of the form is a blue 'Display' button.





- 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.

Approval Process List						Status: all
	Category	Action	Target	Service	Request ↓	Close / How Long
	USER	Add New User	NNTESTA	TestGroup13	07-30-2004 16:50	44 MM
	USER	Add New User	NBTESTE	TestGroup13	07-30-2004 16:21	07-30-2004 16:22
	USER	Add New User	NBKTESTD	TestGroup13	07-30-2004 16:19	07-30-2004 16:19
	USER	Add New User	NBTESTC	TestGroup13	07-30-2004 16:01	01:33 HHMM
	USER	Add New User	NBTESTB	TestGroup13	07-30-2004 15:56	01:38 HHMM
	USER	Add New User	NBTESTA	TestGroup13	07-30-2004 15:48	01:46 HHMM
	USER	Add New User	NBTEST	TestGroup13	07-30-2004 15:46	01:48 HHMM
	USER	Add New User	DTTEST7	TestGroup13	07-30-2004 15:15	07-30-2004 15:16
	USER	Add New User	NBKTEST6	TestGroup15	07-30-2004 15:09	07-30-2004 15:10
	USER	Add New User	NBTEST4	TestGroup13	07-30-2004 14:57	07-30-2004 14:58
	USER	Add New User	NBTEST14	TestGroup13	07-30-2004 14:48	07-30-2004 14:48
	USER	Add New User	NBTEST3	TestGroup13	07-30-2004 14:41	07-30-2004 14:41
	USER	Add New User	NBTEST2	TestGroup12	07-30-2004 14:17	07-30-2004 14:18
	USER	Add New User	NBTEST2	TestGroup14	07-30-2004 14:16	07-30-2004 14:16
	USER	Add New User	test45	j28	07-30-2004 14:13	07-30-2004 14:15
	USER	Add New User	NBTEST2	TestGroup13	07-30-2004 14:12	07-30-2004 14:16
	USER	Add New User	NBTEST2	TestGroup14	07-30-2004 14:12	07-30-2004 14:16
	USER	Add New User	j30u1	j28	07-30-2004 12:30	07-30-2004 12:30

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** 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 account is modified.
-  indicates that the account is added.
-  indicates that the account is deleted.
-  indicates that there are more approvers needed.

- 4 To review a user account, click the target account name.

## The Service Attribute Edit page display.

Approvals Friday, July 30, 2004

[Home](#) > Approvals

Click on service name to edit that service attributes. Click "Approve" or "Reject" when all the services edit status is "YES". Search List

Service	Reviewed
TestGroup13 (Business Service)	NO

Information

Comment:

Approval Status Summary

Approvals required:	1	Checked out:	0	<a href="#">Status Details</a>
Approved:	0	Rejected:	0	<a href="#">Checkout</a>

[Approve](#) [Reject](#) [Cancel](#)

- Click the Service name to review the account details. Account details display.

Approvals Friday, July 30, 2004

[Home](#) > Approvals

Review/Edit attribute information. Press "Submit" when done.

Attribute Name	Value	Label
*UserName:	NBTEST	UserName
*FirstName:	Davidson	FirstName
*LastName:	Tomlin	LastName
*Email:	dtomlin@trulogica.com	Email
*Password:	*****	Password

LDAP71\_ENTITLEMENTS:

[Submit](#) [Cancel](#)

- Some values may be editable. These values are defined in the Service view. Click **Submit**.
- You are returned to the Service Attribute Edit page.
- Click **Approve** to approve the account, or **Reject** to reject it.

## 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 in a Request Status report.

Perform the following steps to request account status:

- 1 From the home page of Request Status, choose a date range from the Period options and account status (**All**, **Completed**, **In Process**) from the Display Options fields.
- 2 If you want status for a single request and know the request number, enter the number in the Request Number field.

Admin Roles	Connectors	Resources	Services	Notifications	Users
<b>Request Status</b>	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

[Home](#) > [Request Status](#)

The Request Status section allows you to check the status of any user request. You can search by a particular Request Number or by the Status of the request (All, Completed, Opened, Failed).

Request Status Report			
Request Number:	<input type="text"/>		
Period	Display Options		
From:	2004-7-1	Status:	All
Through:	2004-7-30	Items Per Page:	20
<input type="button" value="Submit"/>			

- 3 Select the number of items per page that you want to view from the Items Per Page drop-down list.
- 4 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	Start	Close / How Long
1263	j30u1	Closed	07-30-04 17:57	07-30-04 17:57
1261	j30u1	Closed	07-30-04 17:56	07-30-04 17:56
1259	BBB500	Closed	07-30-04 17:55	07-30-04 17:56
1257	BBB100	Closed	07-30-04 17:55	07-30-04 17:55
1255	j30u1	Closed	07-30-04 17:54	07-30-04 17:55
1253	BBB200	Closed	07-30-04 17:42	07-30-04 17:43
1251	BBB100	Closed	07-30-04 17:42	07-30-04 17:42
1248	kmiddlebrook	Closed	07-30-04 17:30	07-30-04 17:30
1246	BBB500	Closed	07-30-04 17:26	07-30-04 17:26
1244	BBB500	Closed	07-30-04 17:26	07-30-04 17:26
1242	BBB400	Closed	07-30-04 17:26	07-30-04 17:26
1240	BBB300	Closed	07-30-04 17:26	07-30-04 17:26
1238	BBB200	Closed	07-30-04 17:25	07-30-04 17:26
1236	BBB100	Closed	07-30-04 17:25	07-30-04 17:26
1234	AAA600	Closed	07-30-04 17:14	07-30-04 17:15
1232	AAA500	Closed	07-30-04 17:14	07-30-04 17:15
1230	AAA400	Closed	07-30-04 17:14	07-30-04 17:15
1228	AAA300	Closed	07-30-04 17:14	07-30-04 17:15
1226	AAA200	Closed	07-30-04 17:14	07-30-04 17:15
1224	AAA100	Closed	07-30-04 17:14	07-30-04 17:15

<< Page 1 of 3 >>

- 5 Click on a request number to view request status.

Status for that request displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
<b>Request Status</b>	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	Reconciliation	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

[Home](#) > [Request Status](#)

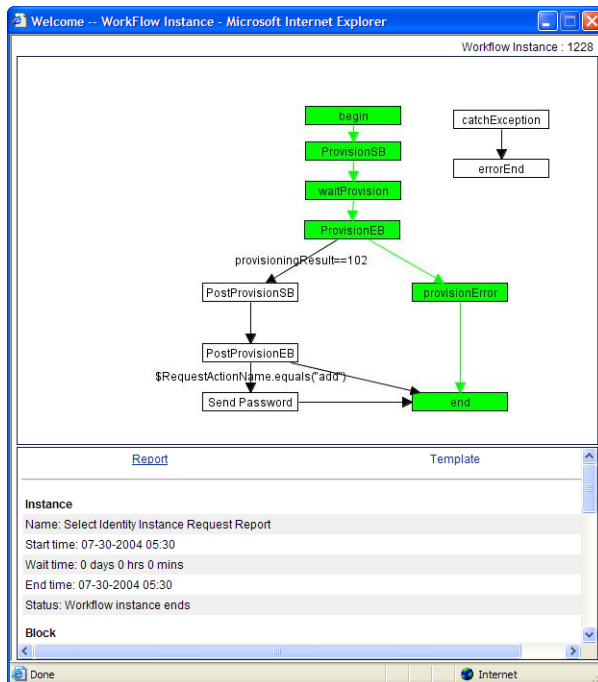
To view the details of a specific user request, click on the corresponding Workflow Instance.

Request Items for Request Number: 1248					
Workflow Instance	Action	Type	Target	Service	Status
1228	Add New User	Delegated Request	kmiddlebrook	atbs1	Closed
1229	Add New User	Delegated Request	kmiddlebrook	atbs1	Closed

NA - Not Available Cancel

- Click on the workflow instance to view the approval process for the request.

The workflow template displays.





## Account Reconciliation

Dynamically changing environments may need to update account information periodically. This process is called **reconciliation**. If you have a resource that is considered the authoritative source for user data in your environment, you can reconcile HP OpenView Select Identity data with that resource. For example, your human resources server may be the first to receive changes regarding users in your environment. Select Identity can reconcile account data with that resource on a regular basis.

Select Identity Reconciliation uses the same SPML data file type as discussed in [Using an SPML Data File on page 104](#). This file should reflect changes from a specified resource, including entitlement and attribute changes. The file is then uploaded to Select Identity. All Services that rely on the specified resource are checked for account changes and updated accordingly.

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

## Reconciliation Dependencies

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.
- All necessary resource and Select Identity attributes are mapped within the connector mapping files and Attributes capability.
- All SPML data files for automated jobs follow the *ResourceName\_file.xml* or *ResourceName\_file.spml* naming convention and are stored in the reconciliation root directory as specified in the `TruAccess.properties` file. See the *HP OpenView Select Identity Installation Guide* for information about this properties file.
- One or more Services is created to use the resources with which you want to reconcile data and the default workflow template for reconciliation (`ReconciliationDefaultProcess`) is associated. See the *HP OpenView Select Identity Workflow Studio Guide* for information about this template.
- User accounts added to a Service through reconciliation must
  - have access to all resources that the Service requires.
  - have all valid, required Service attribute values, a matching Service context value, and fixed attribute values. Values must match the constraints set by the field definition.

## Reconciling with Authoritative Sources

When resources are created, they can be designated as authoritative sources. These resources have the most up-to-date account information in your environment. Reconciling with an authoritative source enables Select Identity to

- Create accounts that are not already in Select Identity and assign all relevant attributes, values, and entitlements.

- Update existing account attributes, values, and entitlements. If the account is disabled, Select Identity begins the assigned workflow process to enable the account.
- Check any existing rules associated with the resource to provide Service access. Each resource can have one defined reconciliation rule for this purpose and the rule must be named *ResourceName\_ReconRule*.
  - The rule affects new users only.
  - If this rule exists, the new user is added to Services as specified by the rule.
  - If the rule does not exist, the workflow process is started to add all new accounts to Services associated with the resource, if the user is qualified.
- Check for accounts that are deleted from the resource and enables them.

## Reconciling with Non-authoritative Sources

Reconciliation with non-authoritative sources requires that accounts be present in the resource and in Select Identity. If accounts are not present, no add or modify actions are performed. If the account exists in Select Identity, all add, modify, and delete actions can be performed.

## Reconciling Account Data

You can schedule a job to reconcile data with a specified resource.

Perform the following steps to schedule reconciliation:

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

Admin Roles | Connectors | Resources | Services | Notifications | Users  
 Request Status | Audit Reports | Configuration Reports | Challenge / Response | Workflow Studio | Attributes  
 Auto Discovery | **Reconciliation** | External Calls | Approvals | Configurations | Rules

Home > Reconciliation > Add New Automated Job Saturday, June 12, 2004

**Job Information**

\* Job Name

\* Resource Name

Server File Sub Directory

CC Email

Start Date


\* Frequency

\* Designates Required Fields

- 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.
- 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.
- 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.
- 2 Select **View Automated Job** from the Actions drop-down list.
- 3 Click **Submit**. The Job Information page displays.


Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	<b>Reconciliation</b>	External Calls	Approvals	Configurations	Rules

Home > [Reconciliation](#) > View Automated Job Friday, July 30, 2004

Job Information	
* Job Name	Auto-LDAP71
* Resource Name	LDAP71
Server File Sub Directory	
CC Email	atb2@test.trulogica.com
Start Date	2004-07-30
* Frequency	1 Min


## 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.
- 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.
- 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.

## Creating a Job to Run Once

Perform the following steps to run a reconciliation job once:


- 1 From the home page of Reconciliation, click  to search for and select the job that you want to delete.
- 2 Select **One Time Job** from the Actions drop-down list.
- 3 Click **Submit**. The Job Configuration page displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	<b>Reconciliation</b>	External Calls	Approvals	Configurations	Rules


Friday, July 30, 2004

[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	<input type="text" value="reconcile"/>
* Resource Name	<input type="text" value="LDAP177"/> 
* Upload File Path	C:\Documents and Sett <input type="button" value="Browse..."/>
CC Email	<input type="text"/>
* Start Date	<input type="text" value="2004-7-30"/> <input type="button" value="Calendar"/>

\* Designates Required Fields

- 4 Enter a name for the job in the Job Name field.
- 5 Click  to search for and select the resource from which you want to update.

- 6 Click **Browse** to select the directory from which you want Select Identity to upload the data file.
- 7 The system sends email to the creator of the job when the job completes. If you want to send a copy of the email to another user, enter the address in the Email CC field.
- 8 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.
- 9 Click **Submit**.

The job is created and runs when scheduled.

## Viewing Task Status

Perform the following steps to view task status:

- 1 From the home page of Reconciliation, select **View Task Status** from the Actions drop-down list.
- 2 Click **Submit**. The Search page displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	<b>Reconciliation</b>	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

[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	<input type="text" value="reconcile"/>
* Resource Name	<input type="text" value="LDAP177"/>
* Upload File Path	C:\Documents and Sett <input type="button" value="Browse..."/>
CC Email	<input type="text"/>
* Start Date	<input type="text" value="2004-7-30"/>

\* Designates Required Fields

- 3 Enter your search criteria.
- 4 Click **Submit**.

The Results page displays.

Admin Roles	Connectors	Resources	Services	Notifications	Users
Request Status	Audit Reports	Configuration Reports	Challenge / Response	WorkFlow Studio	Attributes
Auto Discovery	<b>Reconciliation</b>	External Calls	Approvals	Configurations	Rules

Friday, July 30, 2004

[Home](#) > [Reconciliation](#) > [View Task Status](#)

**List of Reconciliation Task**

Page 1 of 1 Total Records: 6

Task ID	Job Name	Resource Name	Start Time	End Time	Status	User ID
1002	Auto-Auth	LDAP177	2004-07-30 17:03:49.0	2004-07-30 17:04:00.0	Completed	1006
1003	Auto-LDAP71	LDAP71	2004-07-30 17:14:19.0	2004-07-30 17:14:41.0	Completed	1006
1004	Auto-LDAP71	LDAP71	2004-07-30 17:25:49.0	2004-07-30 17:26:09.0	Completed	1006
1005	ModManualEnts	LDAP71	2004-07-30 17:42:21.0	2004-07-30 17:42:31.0	Completed	1006
1006	Auto-LDAP71	LDAP71	2004-07-30 17:55:19.0	2004-07-30 17:55:33.0	Completed	1006
1007	Auto-Auth	LDAP177	2004-07-30 18:03:49.0	2004-07-30 18:03:53.0	Completed	1006

Page 1 of 1

[New Search](#) [Cancel](#)

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



## Account 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.

### Changing a Password and Password Hints

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.

Perform the following steps to change your account password:

- 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.

Please input your old password and new password

**Password Input**

\* Current password:

\* Password

\* Confirm Password

\* Designates Required Fields

- 3 Enter your current password in the Current Password field.
- 4 Enter a new password.
- 5 Confirm the new password.
- 6 Click **Submit**.

When the change is approved, Select Identity sends email confirmation based on the notification policy associated with the action.

Perform the following to change your password reset questions:

- 1 From the home page of Self Service, select **Change Password Reset Questions** from the Actions drop-down list.
- 2 Click **Submit**.

The Your Password Reset Questions page displays.

[Home](#) > [Self Service](#) > [Password Reset Questions](#)

To set your answers for the password reset questions, please fill out the form below and press submit. If you lose or forget your password, you will be prompted to re-enter these answers to reset your password. All answers are case sensitive.

**Your Password Reset Questions (All answers are case sensitive)**

\* Current Password:

Challenge: What is your high school's name?


\* Answer:

\* Confirm Answer:

\* Designates Required Fields

- 3 Enter your password in the Current Password field.
- 4 Enter an answer for this question in the Answer field.
- 5 Confirm the answer.

- If available, select another question from the second Challenge drop-down list.

 This action is dependent on the Select Identity challenge and response policy.

- Enter an answer for this question in the Answer field.
- Confirm the answer.
- 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:


- From the home page of Self Service, select **Delegate Admin Roles** from the Actions drop-down list.
- Click **Submit**. The User Selection page displays.

[Home](#) > [Self Service](#) > [Delegation](#)

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:  

- Click the search icon  to search for a name. The user must be a member of your Service context.
- Click **Activate** to delegate roles, or click **Deactivate** to remove roles.

When the change is approved, Select Identity sends email confirmation based on the notification policy associated with the action.

# Configuration and Audit 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 Configuration Report and Audit 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.

## Generating Audit Reports

Select Identity provides audit reports for all Select Identity system functions. Audit reports provide the history of activities within the system. You can generate a single report or create a report template, which can be accessed each time you click **Audit Reports**.

### **User Audit Reports**

Generate a User Audit report to view configuration activities for specific user accounts over a period of time.

## Service Audit Report

Generate a Service Audit report to view configuration activities for a Service over a period of time.

The configuration procedure for each report is similar. The available audit data will change to suit the report type. The following procedure uses the Service Audit report as an example.


Perform the following steps to generate an audit report:

- 1 From the Audit Reporting home page, select **Service Audit Report** from the Report Type Selection drop-down list.
- 2 Click **Submit**. The Report Configuration page displays.

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.
  - Select a report type.
  - Choose the **Generate Report Now** option, or schedule to report to run at a later date.
- 5 Select the audit data that you want to display. You can use the **CTRL** and **SHIFT** keys to select multiple options.
  - 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 144](#) for information about saving reports.

The following is an example report.

Home > Audit Reports > Service Audit Rpt

<< Page 1 of 1 >>

Audit Service Report								
Num	Time Stamp	Requestor	Service Name	Action	Component	Component Name	Status	
1	2004-07-13 17:28:59.0	concerosa	alan	modify	Biz Relation	atb70bra	success	
2	2004-07-13 16:53:24.0	concerosa	alan	modify	service	alan	success	
3	2004-07-13 16:53:05.0	concerosa	alan	modify	service	alan	success	
4	2004-07-13 16:52:17.0	concerosa	alan	modify	service	alan	success	
5	2004-07-13 16:50:39.0	concerosa	alan	modify	service	alan	success	
6	2004-07-13 13:21:13.0	concerosa	alan	modify	Biz Relation	atb70bra	success	
7	2004-07-07 18:32:22.0	concerosa	alan	modify	Biz Relation	atb70bra	success	

<< Page 1 of 1 >>

Printer View      Configure New Report

Click on a requestor name to view profile information for a user.

Click **Printer View** to print the report, or you can configure a new report.

# Generating Configuration Reports

Select Identity provides configuration reports for user, administrator, and Service management activities. Configuration reports provide current system information. You can generate a single report or create a report template that can be accessed each time you click **Configuration Reports**.

## User Configuration Reports

Generate a User Configuration report to view active user accounts within a Group over a period of time.


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.


Perform the following steps to generate a configuration report:

- 1 From the Configuration Reporting home page, select **User Configuration Summary Report** from the Report Type Selection drop-down list.
- 2 Click **Submit**.

The Report Configuration page displays.

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, or schedule to report to run at a later date.
  - Click  to search for and select the Service that you want to audit.

- Click  to search for and select the Service that you want to audit.
- 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 144](#) for information about saving reports.

The following is a sample.

[Home](#) > [Configuration Reporting](#) > [User Configuration Summary Rpt](#)

User Configuration Summary		
Total User Accounts:		2
User Accounts by Specific Services		
Service Name	Context	Count
j2Adm-AP	HP	2

[Printer View](#) [Configure New Report](#)

After the report displays, you can click **Printer View** and print the report, or configure a new report.

## 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:

[Submit](#) [Cancel](#)

- 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 edit 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:

Report Configuration Action:

# Configurations


HP OpenView Select Identity provides a configuration management capability that enables you import and export Service, workflow, request, notice, attribute, and resource data from one environment to another. 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.

- 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="identityObjectId"> <int>1</int> </void> <void
property="identityObjectName"> <string>USER</string> </void>
</object> </void> <void property="TAResultAction"> <object
class="com.trulogica.truaccess.request.model.TAResultAction"> <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="TAResultType"> <object id="TAResultType0"
class="com.trulogica.truaccess.request.model.TAResultType"> <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.

- 4 Click **Browse** to locate the file that you want to import.
- 5 Click **Submit** to import the file.

The Configuration list page displays.



## Creating Rules

Select Identity enables you to create rules to facilitate the account reconciliation process. Each authoritative resource can have one reconciliation rule to add Service access to new user accounts. Services are added based on a specified attribute and value.

You must create an XML file that adheres to the rules DTD. You can save the XML file in any directory on the Select Identity server; when you create the rule in the Rules capability, the XML rule file is uploaded to the Select Identity database through the Rules capability.

## Application Server Configuration for Rules

There are three `.jar` files packaged with the Select Identity installation CD that must be placed in a specific directory on the WebLogic web server. The files are `xml-apis.jar`, `xercesImpl.jar`, and `xalan.jar`. They must be copied to `jdk141_05\jre\endorsed` within the BEA home directory.

## 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: <b>&amp;lt;</b> for <, <b>&amp;gt;</b> for >, <b>&amp;amp;</b> for &, <b>&amp;quot;</b> for ", and <b>&amp;apos;</b> 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>
</ul>
```

contains is a special operation. It can be applied to String, Map and Collection types.

```
-->
<!ATTLIST Relation
  op ( eq | ne | gt | lt | ge | le | contains ) #REQUIRED>
<!--
  TrueAction 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 Arithmetic 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 concatenation 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.truologica.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>
        </AndCondition>
      </Condition>
    </ConditionScript>
  </Script>
</Rule>
```

```

        <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>

```

## Creating SPML Files

HP OpenView Select Identity has implemented the Web Service API according to the OASIS SPML (Service Provisioning Markup Language) specification, which defines the concepts, operations, and XML schema for an XML-based provisioning request and response protocol. This means that Select Identity extended the SPML schema, thereby defining how Select Identity will manage users in external systems, such as databases and servers.

Information regarding the APIs mentioned in this chapter is available in the API directory packaged with the Select Identity product CD.

The Web Service API enforces all business processes on operations based on the context of each operation. Context is derived from the Requesting Authority (RA) that has initiated the request using the Select Identity API and the Provisioning Service Target (PST) on which the action will take place. When Select Identity receives a request (via an SPML-compliant message), the context of the request is determined as follows:

- If the request contains caller information, the caller information is verified. If the caller information is not verified, the request is considered anonymous. For anonymous requests, the only operations that are allowed are **<addRequest>** and **<schemaRequest>**, which are treated as self-registration requests.

Validated users can request self-registration for a new service, registration of another user (delegated registration), profile updates, password change, deletion of user, stage completion in an approval process, and so on.

- The context of the PST is obtained from the `urn:trulogica:concerto:2.0#serviceName` attribute in the request.

In addition, SPML mandates the use of the `requestID` attribute in requests and responses so that each response can be matched with the corresponding request in asynchronous requests. This ID must be client-generated and globally unique.

If the `requestID` attribute is not present, Select Identity will generate a globally unique ID and communicate it back to the caller in the response. If the requested parameter is present but not globally unique, an error is generated. The size of the requested parameter is restricted to 128 characters.

## Execution Types

As described in the SPML specification, requests can be issued synchronously or asynchronously. The following table outlines Select Identity's execution model based on the request type:

<b>Request</b>	<b>Synchronous</b>	<b>Asynchronous</b>
<code>&lt;addRequest&gt;</code>		X
<code>&lt;modifyRequest&gt;</code>		X
<code>&lt;deleteRequest&gt;</code>		X
<code>&lt;searchRequest&gt;</code>	X	
<code>&lt;statusRequest&gt;</code>	X	
<code>&lt;batchRequest&gt;</code>		X
<code>&lt;extendedRequest&gt;</code>	X	
<code>&lt;schemaRequest&gt;</code>	X	

# Security

Select Identity provides the same level of security for the User Provisioning API as a web-based browser interface. That is, Select Identity supports HTTP through SSL 3.0 or TLS 1.0.

Operations that require user authentication must pass the username and password in an **<operationalAttributes>** element. Before any operation is complete, the username and password is verified against an authoritative source.

In the case of a modification request, you can add an optional resource identifier to indicate the origin of the request. This is primarily used by agent software to indicate changes in attribute values in a resource. If the resource identifier is specified, an additional check is made to verify that the security principal is associated with the resource identified by the resource ID.

The following is an example:

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
  <soap:Body>
    <modifyRequest requestID="1234567890-0987654321"
      execution="urn:oasis:names:tc:SPML:1:0#asynchronous">
      <operationalAttributes>
        <attr name="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomain-
Name">
          <value>john.doe123@thecompany.com</value>
        </attr>
        <attr name="urn:trulogica:conceroc:2.0#password">
          <value>kroywen!</value>
        </attr>
        <attr name="urn:trulogica:conceroc:2.0#resourceId">
          <value>R123534</value>
        </attr>
        <attr name="urn:trulogica:conceroc:2.0#serviceName">
          <value>urn:acme:com:Conceroc:ITService</value>
        </attr>
      </operationalAttributes>
      <identifier type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDo-
mainName">
        <id>john.doe123@thecompany.com</id>
      </identifier>
      <modifications>
        <modification name="city" operation="replace">
          <value>New York</value>
        </modification>
        <modification name="NTGroups" operation="replace" >
          <value>IT Admin</value>
          <value>IT HelpDesk</value>
        </modification>
      </modifications>
    </modifyRequest>
  </soap:Body>
</soap:Envelope>
```



```

        </modification>
    </modifications>
</modifyRequest>
</soap:Body>
</soap:Envelope>

```

## Example File for Reconciliation

The following sample is a modify user request for an ETrust system. The resource is considered an authoritative source.

```

<?xml version="1.0" encoding="ISO-8859-1" ?>
- <batchRequest xmlns:countries="countries.uri"
xmlns:cities="cities.uri"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0"
xmlns="urn:oasis:names:tc:SPML:1:0" requestID="1085774668899">
  - <operationalAttributes xmlns="">
    - <attr name="urn:trologica:concero:2.0#keyFields">
      <value>employee Number</value>
    </attr>
  </operationalAttributes>
  - <modifyRequest requestID="1">
    - <identifier xmlns=""
type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName">
      <id>000006</id>
    </identifier>
    - <modifications xmlns="">
      - <modification name="LastName" operation="replace">
        <value>Jones</value>
      </modification>
      - <modification name="FirstName" operation="replace">
        <value>Mark</value>
      </modification>
    </modifications>
  </modifyRequest>
</batchRequest>

```

The following example is an add request for a non-authoritative LDAP resource.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
-<batchRequest xmlns="urn:oasis:names:tc:SPML:1:0"
requestID="101">
  -<operationalAttributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#keyFields">
      <value>Employee Number</value>
    </attr>
  </operationalAttributes>
-<addRequest requestID="1">
  -<operationalAttributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#taResourceKey">
      <value>30150026</value>
    </attr>
  </operationalAttributes>
  -<identifier xmlns=""
    type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName">
    <id>30150026</id>
  </identifier>
  -<attributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#groups">
      <value>HR-Manager</value>
      <value>Network-All</value>
    </attr>
  </attributes>
</addRequest>

-<addRequest requestID="2">
  -<operationalAttributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#taResourceKey">
      <value>30150027</value>
    </attr>
  </operationalAttributes>
  -<identifier xmlns=""
    type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName">
    <id>30150027</id>
  </identifier>
  -<attributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#groups">
      <value>CD Group1</value>
    </attr>
  </attributes>
</addRequest>
```

```
-<addRequest requestID="3">
  -<operationalAttributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#taResourceKey">
      <value>30150028</value>
    </attr>
  </operationalAttributes>
  -<identifier xmlns=""
type="urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName">
    <id>30150028</id>
  </identifier>
  -<attributes xmlns="">
    -<attr name="urn:trulogica:concerro:2.0#groups">
      <value>$UNIX-TESTJOBBCODE</value>
      <value>PD Managers</value>
    </attr>
  </attributes>
</addRequest>

</batchRequest>
```



# Event Reference

The following tables lists the request events to which you can assign a workflow template when creating Business Relationships:

## Delegated-registration Request Events

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

## Reconciliation Request Events

- Adding a service to a user
- Deleting a service membership
- Disabling all services

## 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

An action represents a task that can be performed within each Select Identity capability.

See also: *capability*

### 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 attribute is 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****Business Relationship**

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.

## Business Service

A business service is 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

The Configurations capability enables you to import and export Select Identity settings and configurations. This is useful when moving from a test to a production environment.

### Configuration Reports

Configuration reports provide 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 Business Relationships.

**Credentials**

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.

**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.

**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.

**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.

### 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.

### 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: *administrative 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.

### 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: *Attributes*

### 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

A file that is used to add and provision accounts within Select Identity.

See also: *Data File*

## U

### Users

The Select Identity capability that provides consistent account creation and management across Services.

## W

### Workflow

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 Engine

A system component that executes workflows and advances them through their flow steps.

### Workflow Studio

The Select Identity capability that enables you to create and manage workflow templates.

# index

## A

- account reconciliation, 129
- actions, 96
- administrative roles, 95
  - adding a role, 101
  - capabilities and actions, 96
  - deleting a role, 103
  - list of interface actions, 96
  - modifying a role, 102
  - tasks overview, 23
  - viewing a role, 102
- approvals, 123
- approve or reject account requests, 123
- approver role, 100
- architecture diagram, 14
- attributes, 19, 49
  - adding and mapping, 51
  - deleting, 56
  - modifying, 56
  - precedence in business relationships, 79
  - viewing, 55
  - XML mapping file, 49
- audit reports, 140
- authoritative sources, 35

- auto discovery, 104
  - results file example, 106
  - scheduling a job, 107
  - scheduling service assignments, 109
  - spml data file use, 104
  - tasks overview, 23
  - viewing job status, 108
  - viewing service assignment status, 110

## B

- business relationships, 22, 78, 88
  - creating, 88
  - deleting, 91
  - hierarchy, 78
  - modifying, 90

## C

- capabilities, 96
- challenge/response questions, 75
- challenge response, 21
- configuration reports, 143
- configurations, 146
  - exporting, 146
  - importing, 148
  - tasks overview, 25

connectors, 29  
  connector API, 18, 30  
  creating, 30  
  deleting, 33  
  deploying, 31  
  modifying, 32  
  one-way communication, 29  
  tasks overview, 18  
  two-way communication, 30  
  viewing, 32

context, 22, 79, 88  
  creating, 91  
  deleting, 94  
  modifying, 93

context engine, 14

## D

data file, 104

deployment  
  example order, 26  
  tasks, 17

## E

end user role, 100

event reference, workflow-related events,  
  164

external calls, 57  
  deleting, 62  
  deploying, 59  
  modifying, 61  
  tasks overview, 19  
  types, 60  
  viewing, 61

## I

interface actions, 96

## J

J2EE Connector Architecture, 30

## N

notification policy  
  approval process, 66  
  users, 66  
  viewing a policy, 71

notifications, 66  
  copying a policy, 70  
  deleting a policy, 71  
  modifying a policy, 70  
  predefined variables, 67  
  tasks overview, 20  
  viewing a policy, 71

## O

online help, 16

## P

predefined variables, 67

product documentation, 16

## R

reconciliation, 129  
  adding new job, 132  
  creating a one-time job, 134  
  deleting an automated job, 134  
  modifying an automated job, 133  
  tasks overview, 25  
  viewing an automated job, 133  
  viewing job status, 135  
  with authoritative sources, 130  
  with non-authoritative sources, 131

reporting  
  tasks overview, 25

reports, 140  
    saving report configuration, 144

request ID number, 127

request status, 126  
    tasks overview, 24

resources, 34  
    attribute mapping file, 45  
    deleting, 46  
    deploying, 42  
    modifying, 44  
    tasks overview, 18  
    viewing, 46  
    viewing attributes, 47

rules, 63  
    adding, 64  
    creating rules, 149  
    deleting, 65  
    DTD overview, 150  
    modifying, 64  
    tasks overview, 20  
    viewing, 65

## S

Select Identity  
    default roles, 99  
    logging in to, 28

Select Identity features, 13

Select Identity ID example, 35

self service, 137  
    changing passwords and hints, 137  
    delegating roles, 139  
    tasks overview, 26

service attributes, 85  
    setting attribute properties, 86  
    setting attribute values, 85

service management  
    modifying a service, 81

services, 77  
    deleting, 82  
    deploying, 80  
    tasks overview, 22

service views, 82  
    creating, 82  
    deleting, 84  
    modifying, 84

spml data file, 104  
    creating, 158  
    example, 105

system administrator role, 100

system architecture, 14

## U

user provisioning API, 158

users, 112  
    adding a service to an account, 116  
    adding a user, 113  
    deleting a service membership, 120  
    enabling or disabling all services for an account, 118  
    enabling or disabling service membership, 117  
    managing user expiration, 122  
    modifying a user, 115  
    resetting a password, 119  
    tasks overview, 24  
    terminating an account, 120  
    viewing account attributes, 121  
    viewing service membership, 118

## W

workflow approval, 123

workflow studio, 21, 72  
    overview, 73



workflow templates  
  integration with Select Identity, 73  
  overview, 73

## **X**

XML attribute mapping example, 49