

# HP OpenView Select Identity

For IBM WebSphere 6.0.2  
with Oracle 10G  
on Red Hat Enterprise Linux

Software Version: 4.10

---

## Installation Guide

Document Release Date: November 2006  
Software Release Date: November 2006



## 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

© 2006 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.
- BouncyCastle engine for keystore management, bouncycastle.org.

This product includes software developed by Teodor Danciu (<http://jasperreports.sourceforge.net>). Portions Copyright (C) 2001-2005 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2005 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) 2001-2005, Gaudenz Alder. All rights reserved.

## Trademark Notices

UNIX® is a registered trademark of The Open Group.

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

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

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

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

WebSphere Application Server is a trademark of International Business Machines Corporation.

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

You can visit the HP OpenView Support web site at:

**[www.hp.com/managementsoftware/support](http://www.hp.com/managementsoftware/support)**

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

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

To find more information about access levels, go to:

**[www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)**

To register for an HP Passport ID, go to:

**[www.managementsoftware.hp.com/passport-registration.html](http://www.managementsoftware.hp.com/passport-registration.html)**



# Contents

<b>1</b>	<b>Introduction</b> .....	13
	System Architecture .....	13
	Security and Communication .....	15
	Keystores .....	15
	Integration .....	15
	Connectors .....	16
	Internationalization .....	16
	Technical Qualifications for Installing Select Identity .....	16
<b>2</b>	<b>Requirements</b> .....	19
	Installation Process Overview .....	19
	Reviewing Minimum Requirements .....	20
	Supported Configurations .....	20
	Database Server Requirements .....	20
	IBM WebSphere Server Requirements .....	21
	Select Identity Interface Requirements .....	21
	Ports Required for Firewall Configuration .....	21
<b>3</b>	<b>Database Server Configuration</b> .....	23
	Configuring an Oracle Database Server .....	23
<b>4</b>	<b>Installing Select Identity on IBM WebSphere 6.0.225</b>	
	Introduction .....	25
	Prerequisite Configuration .....	25
	Prerequisites for All Installations .....	25
	Prerequisites Specific to Cluster Installations .....	26
	Installation to Directories with Embedded Spaces .....	26
	Preparing to Install Select Identity .....	26
	\$APPSERVER_ROOT/profiles/<profile_name>/logs/<servername>/SystemOut.log . . .	27
	Important Installation Information .....	27
	For all WebSphere 6.0.2 Configurations: .....	27
	For Clusters: .....	27
	Using the Select Identity Installer .....	28
	Auto-Installation Procedure .....	28
	If Auto-Installation is Not Successful .....	36
	Manual Installation Procedures .....	37
	How This Section is Organized .....	37
	Creating Directories and Copying Files .....	37

Configuration Scope .....	39
Creating J2C Authentication Data Entries.....	39
Creating the Oracle JDBC Provider .....	39
Creating the Oracle Data Sources .....	40
Configuring the Select Identity Service Integration Bus .....	41
Adding Bus Members .....	41
Creating Bus Destinations .....	42
Creating JMS Resources .....	43
Creating The Queue and Topic Connection Factories .....	43
Creating the JMS Queues and Topics .....	44
Creating Activation Specifications .....	45
Configuring the Select Identity Mail Provider, Protocol Provider, and Mail Session .....	47
Deploying Select Identity and the Online Help .....	48
Updating The Select Identity Application Settings .....	49
Updating the Server Class Loading Mode.....	50
Configuring the Java Virtual Machine .....	50
Configuring Logging for Select Identity .....	50
Configuring Global Security .....	51
Verifying the Select Identity Installation.....	51
Logging In to Select Identity on IBM WebSphere .....	51
<b>5 Configuring Select Identity.....</b>	<b>53</b>
Configuring Required TruAccess Properties .....	53
How to Set Properties.....	53
Required Settings .....	53
Directory Locations .....	54
Staging Directories for One-Time Reconciliation and Import Jobs.....	54
Email Sender .....	54
Attribute Maximum Length .....	55
Select Identity URL.....	55
Database Settings .....	55
Workflow Settings .....	55
Helpdesk Contact Message.....	55
Optional Settings .....	55
Setting Up the Select Identity Security Framework .....	56
The Bootstrap Keystore .....	56
The Object Migration Keystores .....	56
Setting Up the Bootstrap Keystore .....	56
Setting Up the Bootstrap Keystore on a New Installation or an Installation With Default Keystores	56
HSM Procedure for Bootstrap Keystore Setup.....	56
Non-HSM Procedure for Bootstrap Keystore Setup.....	57
Setting Up the Bootstrap Keystore on an Existing Installation With Custom External Keystores	58
Creating the Object Migration KeyStore.....	58
Creating a Trust Store .....	59
Setting TruAccess Properties for the Security Framework .....	59
Recommended Configuration .....	59
Extending User Searches.....	60



How to Specify Extended User Search Attributes . . . . .	60
Adding Display Columns for Extended Attributes . . . . .	61
Disabling the Extended Search Features . . . . .	62
Custom User Interface Properties . . . . .	63
User Interface Sections . . . . .	63
Customization Properties . . . . .	63
com.hp.ovsi.ui.masthead.fgcolor . . . . .	63
com.hp.ovsi.ui.masthead.bgcolor . . . . .	63
com.hp.ovsi.ui.logo.image.src . . . . .	64
com.hp.ovsi.ui.common.header.image.src . . . . .	64
com.hp.ovsi.ui.landing.named.image.src . . . . .	64
com.hp.ovsi.ui.landing.named-top.image.src . . . . .	64
com.hp.ovsi.ui.landing.named.image.style . . . . .	64
com.hp.ovsi.ui.landing.named-top.image.style . . . . .	64
com.hp.ovsi.ui.landing.common.image.src . . . . .	64
com.hp.ovsi.ui.landing.box.right.bgcolor . . . . .	64
com.hp.ovsi.ui.landing.users.image.src . . . . .	64
com.hp.ovsi.ui.landing.requests.image.src . . . . .	65
com.hp.ovsi.ui.landing.selfservice.image.src . . . . .	65
com.hp.ovsi.ui.landing.servicestudio.image.src . . . . .	65
Default Values for User Interface Properties . . . . .	65
Internationalization and Localization . . . . .	66
Localizing the Date and Time Format . . . . .	66
Functional Overview . . . . .	66
Custom Date and Time Formats . . . . .	67
Setting the Calendar Language . . . . .	67
Setting the Time and Date Default Format in the TruAccess.properties File . . . . .	67
Configuration for Specific Environments or Platforms . . . . .	68
Tuning the Database Server . . . . .	68
UTF-8 Encoding on Oracle 10G . . . . .	68
iPlanet LDAP Configuration . . . . .	69
Set Encoding in Internet Explorer . . . . .	69
Adding Supported Language Fonts . . . . .	70
Additional Configuration Options . . . . .	70
<b>6 Upgrading Select Identity . . . . .</b>	<b>73</b>
Supported Platforms for Upgrading . . . . .	73
Upgrading on Unsupported Platforms . . . . .	73
Upgrade Requirements . . . . .	73
Preparing to Upgrade . . . . .	74
Downloading the Oracle JDBC Driver . . . . .	74
Stopping Select Identity Traffic . . . . .	74
General Web Server Preparation . . . . .	75
Database Upgrade Procedure . . . . .	75
Required Libraries and Files . . . . .	76
Troubleshooting a Database Upgrade . . . . .	76
WebSphere Server Upgrade Procedure . . . . .	77

Synchronizing Resources . . . . .	78
<b>7 Integrating Select Identity With Other OpenView Applications</b>	<b>79</b>
Select Identity–Service Desk Integration . . . . .	79
Required Files . . . . .	79
External Call from Select Identity to Service Desk . . . . .	80
Workflow Template for Integrated Password Management . . . . .	80
Functional Scenarios . . . . .	80
Password Management Request from Select Identity Triggers New Service Call in Service Desk	80
Service Call and Workflow Data Exchange and Interaction . . . . .	80
Accessing the Select Identity Request Status Page from Service Desk . . . . .	81
Configuration Tasks in Service Desk . . . . .	81
Customizing a Number Field for the Request ID . . . . .	81
Customizing a String Field for Request Failure Information . . . . .	82
Activating a String Field for the Request Link . . . . .	82
Customizing a Short String Field for the Request Type . . . . .	82
aCreating a Smart Action . . . . .	85
Linking a Service Calls to Select Identity Password Requests . . . . .	85
OpenView Select Identity Configuration Tasks . . . . .	86
System Context . . . . .	87
Process Flow . . . . .	88
Select Identity-Select Audit Integration . . . . .	89
Requirements and Recommendations . . . . .	89
Setting Up Integration in Select Identity . . . . .	89
The Select Audit Agent . . . . .	89
TruAccess Properties . . . . .	90
Configuring the Select Identity Database . . . . .	90
Setting Up Integration in Select Audit . . . . .	91
Data Filtering and Report Access Matrices . . . . .	91
Report Mapping . . . . .	92
<b>8 Uninstalling Select Identity</b> . . . . .	<b>105</b>
Auto-Uninstalling Select Identity . . . . .	105
Uninstalling Select Identity Manually on IBM WebSphere 6.0.2 . . . . .	105
Undeploying the Online Help or Another Application . . . . .	106
Uninstalling the Select Identity Database . . . . .	106
Uninstalling Oracle . . . . .	106
<b>A TruAccess Properties</b> . . . . .	<b>107</b>
TruAccess Properties Summary . . . . .	107
General Settings . . . . .	107
Asynchronous Provisioning Delay . . . . .	108
Audit Settings . . . . .	108
Authentication Settings . . . . .	109
Auto User Import Settings . . . . .	109
Batch Processing Settings . . . . .	109
Bulk Upload Settings . . . . .	110

Cache Settings	110
Connector Schema Directory	110
Email Settings	110
Execution Retry Settings	111
External Calls Settings	112
JNDI Data Source Settings	112
Localization Settings	112
Notification Event Settings	112
Operations Templates	112
Page Redirect Timeout	113
Reconciliation Settings	113
Report Settings	114
Repository Type Settings	115
Schema Settings	115
Search Settings	115
Security Framework and Keystore Settings	115
Self-Registration Settings	116
Server Management Settings	116
User and Account Settings	116
Web Service Request Settings	117
Workflow Settings	117
XML Mapping File	118
<b>B Auditing XML and Client Sample</b>	<b>119</b>
Processing the Audit XML Stream into a Database	119
Using the Audit Client	119
Configuring Connection Properties	120
Running the Audit Client	120
Using the Audit Client on IBM WebSphere 6.0.2	120
The Select Identity Audit XSD	121
Event Sequences	122
Data Types	123
AttrChangeData	123
auditType and auditSubType	123
ConfigChangeType	124
EntityType	124
EntityListType	124
EventType	124
MembershipType	125
OpType	125
PropertyType	125
requestType	125
SvcConfigChangeType	126
targetType	126
UserType	126
Constraints	126
Element Definitions	127
Event Types	133

Index ..... 143

---

# 1 Introduction

This guide provides instructions for installing HP OpenView Select Identity on a supported Web application server in several supported operating system environments. It also describes how to configure the database server and load the Select Identity schema.

For detailed information about using Select Identity after installation, refer to the *HP OpenView Select Identity Administration and Concepts Guide* and the Select Identity online help.

This section covers the following topics:

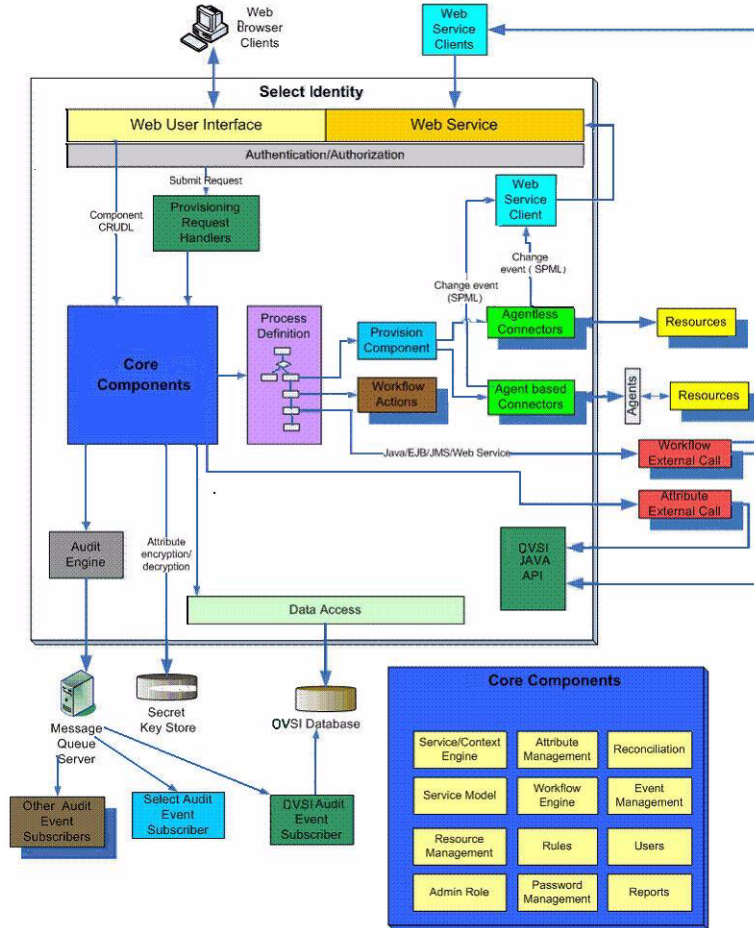
- [System Architecture](#)
- [Security and Communication](#)
- [Connectors](#)
- [Internationalization](#)
- [Technical Qualifications for Installing Select Identity](#)

## System Architecture

All requests to and from the system use the HTTP protocol. Select Identity manages a single *logical identity* for each user and administrator. Each logical identity is mapped to associated user accounts on back-end systems and services. Logical identities, as well as their corresponding accounts and privileges, are governed by Select Identity system functions and permissions. Accounts are also governed by security policies defined by an administrator; policies are based on the access requirements of the company's products and services.

[Figure 1](#) provides a high-level view of the Select Identity system components.

**Figure 1 HP OpenView Select Identity Architecture**



The Context Engine and Identity Business Process Services components of the Select Identity architecture are of particular importance 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 the following:

Function	Description
Context Management	Maintains the Context structure that defines identities and access for all users and resources in the extended enterprise.
Services	Provides a business-centric abstraction over resources, entitlements, and other identity-related entities. Services represent the products and services that you offer to customers, partners, and employees.
Service Roles	Provides granular control over how groups of users access services.
Users	Provides consistent account creation and management across products and services.
Resources	Provides a connection to the physical information systems on which your products and services rely for user account data.

<b>Function</b>	<b>Description</b>
Workflow Studio	Enables the definition of identity-related business processes that can be executed for access to services or any other 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 over user entitlements and system event history.
Forms	Automates the creation of electronic forms used by end users to register for access to services, change their passwords, set password hints, and update personal information.
Tiered Authority	Enables the secure, multi-tiered delegation of administrative tasks, such as management of identity profiles and entitlements, to functional departments, customers, and partners.

## Security and Communication

Select Identity encrypts application data in transit and storage. Data that is in transit is encrypted using SSL. For in-storage encryption, Select Identity uses the standard encryption algorithm, SHA. The algorithm guarantees that the same message (input) will produce the same message digest. Therefore, at any given time, you can verify that the input (such as a password) is the same as the original value by comparing the hash value.

It is recommended nonetheless that you tighten database access control and ensure passwords are complex.

### Keystores

Select Identity provides a security framework that consists of the keystores and secret keys used to encrypt and decrypt application data. This security framework also supports Hardware Security Modules (HSM).

A keystore is a file that contains security information such as public and private keys, and certificates of trusted Certification Authorities. Private keys are associated with a certificate chain, which authenticates the corresponding public key.

By generating the keystore, you add security to data exchange in Select Identity. See [Setting Up the Select Identity Security Framework](#) on page 56 for details.

## Integration

As of version 4.10, Select Identity can exchange data dynamically with two other OpenView applications: Service Desk and Select Audit.

## Connectors

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.

The connectors that enable you to provision users in external resources are built using JCA (J2EE Connector Architecture) and run within the Web application server on which Select Identity is deployed. Communication between Select Identity and the connectors is internal to the Web application server. The connectors then use the appropriate protocol or means of communication for each resource.

The following list provides examples of typical connectors and the protocol used for each resource:

- The LDAP connector uses the JNDI (Java Naming and Directory Interface) API to address the LDAP stores.
- For Active Directory (LDAP-based), the connector uses LDAPS (LDAP over SSL).
- For UNIX-based connectors, provisioning commands are executed through a Telnet session or over SSH.

For agent-based connectors, each agent resides on the resource with which the connector communicates. The messages exchanged between the connector and the agent are based on a non-standard proprietary XML format and encrypted using 128-bit PC1 encryption. The agent communicates internally with the resource application.

For detailed information on installing each resource connector, see the specific connector's *HP OpenView Connector Installation Guide*. These guides are located on the Select Identity Connector CD. If you need to develop connectors, which enable you to connect to external systems for provisioning, refer to the *HP OpenView Select Identity Connector Developer Guide*.

## Internationalization

The Select Identity application is internationalized, and is localized to languages specified on the labeling of the localized HP OpenView Select Identity product CD. The Select Identity server is supported in a non-US environment with internationalization encoding. In addition, the LDAP connectors are internationalization encoded. The LDAP connectors rely on the JNDI resource provider interface to exchange information with the LDAP resources.

For more information about the internationalized Select Identity, see [Internationalization and Localization](#) on page 66.

## Technical Qualifications for Installing Select Identity

If you are installing Select Identity, you need the following qualifications or knowledge:

- System administration for your operating system platform
- Knowledge of the server command line in your operating system



- Database administration skills
- Installation and administration training on your Web application server
- General familiarity with background technology such as HTTP and JCA



## 2 Requirements

This chapter provides an overview of the installation process and describes the required and recommended system configuration for HP OpenView Select Identity.

This chapter covers the following topics:

- [Installation Process Overview](#)
- [Reviewing Minimum Requirements](#)
- [Supported Configurations](#)
- [Database Server Requirements](#)
- [IBM WebSphere Server Requirements](#)
- [Select Identity Interface Requirements](#)
- [Ports Required for Firewall Configuration](#)

### Installation Process Overview

The following is an overview of the complete installation process:

- 1 Review the requirements and recommendations in this section.
- 2 Configure the Web application server for use with Select Identity, as documented in [Prerequisite Configuration](#) on page 25.
- 3 Configure the database and load the Select Identity schema.
- 4 If installing on a cluster, configure a shared Network File System folder where Select Identity will be installed.
- 5 Set up the Select Identity security framework before installing Select Identity, as documented in [Chapter 5, Configuring Select Identity](#).
- 6 Ensure that you have the correct policy files, as documented in the installation section for your Web application server.
- 7 Install Select Identity, as documented in [Chapter 4, Installing Select Identity on IBM WebSphere 6.0.2](#).
- 8 If you are installing a localized version of Select Identity using the Select Identity language media kit, mount the Language Media CD, locate the documentation, and follow the instructions on how to deploy specific languages.
- 9 Configure the `TruAccess.properties` file for your environment, using the information provided in [Chapter 5, Configuring Select Identity](#) and in [Appendix A, TruAccess Properties](#).
- 10 Install and configure the connectors that will be used with your system. Refer to the *Connector Installation Guides* supplied with your connectors for instructions.

## Reviewing Minimum Requirements

The minimum requirements vary in some circumstances. Examine your specific environment and adjust or correct any aspect that could affect the performance of the Web application server or database when running Select Identity.

In addition, requirements vary widely depending on the intended use and throughput in your environment. If additional processing power is required as your system grows, it is recommended that you expand by adding nodes to existing clusters.

## Supported Configurations

Select Identity release 4.10 is supported on the following configurations:

Web Application Server	Platform	Database
IBM WebSphere and IBM WebSphere - ND Version 6.0.2 or later	Red Hat Enterprise Linux v3	Oracle 10G, Release 2

## Database Server Requirements

Hewlett-Packard strongly recommends that you follow these guidelines when configuring your database server:

- Follow a regular maintenance schedule.
- Install the database server on a different system than the Web application server, for optimal performance and ease of management.

The following table provides both the minimum requirements and the recommended configuration for database servers to support Select Identity with Oracle 10G.

<b>Operating System</b>	Red Hat Enterprise Linux v3
<b>Processor</b>	Minimum processor speed: 330 MHz
<b>Memory (RAM)</b>	512 MB of physical RAM 1 GB of swap space (or twice the size of RAM)
<b>Disk space</b>	3.5 GB
<b>JDBC driver</b>	Oracle Thin Driver Version 10.2.0.2.0 (oracle.jdbc.OracleDriver)

# IBM WebSphere Server Requirements

Hewlett-Packard strongly recommends that you follow these guidelines when configuring your WebSphere server:

- Install the WebSphere server on a different system than the database server for optimal performance and ease of management.

The table below provides the minimum and recommended configurations for systems running Select Identity on WebSphere servers.

Operating System	Red Hat Enterprise Linux v3
Processor	Minimum processor speed: 1 GHz
Memory (RAM)	768 MB RAM (minimum) 1 GB RAM (recommended)
Disk space	Approximately 820MB

## Select Identity Interface Requirements

The Select Identity user interface requires Microsoft Internet Explorer (IE), version 5.5 or higher, with JavaScript and cookies enabled.

The optimal screen resolution for viewing the Select Identity user interface is 1024x768.

No installation steps are required to install the Select Identity client user interface. The Web server that is configured for Select Identity serves its interface pages.

## Ports Required for Firewall Configuration

Select Identity uses the following ports for communication by default. You can change some of these settings during installation.

The Web server TCP/IP port for all inbound communication:

- 9001 for WebSphere

If a Web server is configured to redirect requests to the Select Identity server, any other TCP/IP port may be used to mask the server URL, including its port.

The JDBC port, which depends on the database server:

- 1521 for Oracle

If you are installing connectors, additional ports are needed to send requests from the connector to the target resource. For example:

- The LDAP connectors use port 389 (LDAP) or 636 (LDAPS).
- The UNIX connectors port 23 (Telnet) or 22 (SSH).

Refer to the documentation supplied with the target resource to determine what the standard communication port is for each.

If you are installing on a Web server cluster, each node may be using a different HTTP port. This may require a firewall. HP recommends that you configure a Web server to mask the Web container ports.

# 3 Database Server Configuration

This chapter describes how to create the database and set up a user account for Select Identity to access the database server.

It is essential that you load the Select Identity schema onto the chosen database server. Before loading the schema, ensure that the database server meets the minimum requirements as documented in Chapter 2, System Requirements. Oracle Database Configuration.

This chapter contains the following topics:

- [Configuring an Oracle Database Server](#)

## Configuring an Oracle Database Server

You create an Oracle database for use by Select Identity by running SQL scripts. Complete the following procedure to create the database:

- 1 Launch SQL Plus and log in with DBA privileges.



You can perform the following steps from the Oracle Enterprise Manager console. However, the SQL Plus steps in this procedure are based on Linux and Windows.

- 2 Create a tablespace into which you will load the Select Identity tables.

The following command line example creates a tablespace; the size and datafile directory will vary according to your environment.

```
CREATE TABLESPACE <tablespace_name>
DATAFILE <install_dir>/oracle/oradata/<ORACLE_SID>/
<tablespace_name>.dbf
SIZE 10M (or greater) AUTOEXTEND ON NEXT 10M (or greater)
MAXSIZE unlimited;
```

This example creates 10MB of tablespace then automatically extends it as needed. The <tablespace\_name> is your chosen name for the Select Identity tablespace. You reference this name when you create the database user in [step 3](#).

- 3 Create a user account for Select Identity to access the tables, as shown in the following example:

```
CREATE USER <user_name>
IDENTIFIED BY <password>
DEFAULT TABLESPACE <tablespace_name>
TEMPORARY TABLESPACE <temporary tablespace_name>;
GRANT CONNECT TO <user_name>;
```


```
GRANT RESOURCE TO <user_name>;
GRANT CREATE VIEW TO <user_name>;
```

Where:

- <user\_name> is the name of the database user to be created.
- <password> is the user's password.
- <tablespace\_name> is the name of the tablespace to be used, assigned as the user's default tablespace.
- <temporary tablespace\_name> is the default temporary tablespace.

The `oracle_concero_ddl.sql` script, in [step 6](#), creates tables in the user's default tablespace. If you do not assign the Select Identity tablespace as the user's default, you must edit the script to reference the Select Identity tablespace.

- 4 Repeat [step 3](#), creating an additional user account that the Java Messaging Service (JMS) will use to access the Select Identity database. You can also repeat [step 2](#) first if you wish to create a separate tablespace for the JMS user account.

 There are two possible approaches to creating the tables for the JMS user. Either you can grant the JMS user the authority to create the tables automatically, or you can create these tables yourself and assign use-only authority to the JMS user account. For more information, refer to the IBM WebSphere public technical library.

- 5 Change to the first user account you created, by entering the following command:

```
CONNECT user_name/password
```

- 6 Create the schema for the Select Identity database, as follows:

- a Copy the schema creation script from the HP OpenView Select Identity Product CD.

- b Execute the copied script by running the following:

```
<path>/oracle_concero_ddl.sql
```

where <path> is the full path to the file.

- c Verify that no error message results.

- 7 Insert the required default data into the Select Identity database:

- a Copy the data creation script from the HP OpenView Select Identity CD.

- b Execute the copied script by entering the following command:

```
<path>/oracle_concero_dml.sql
```

Where <path> is the full path to the file.

- c Verify that no error message results.



# 4 Installing Select Identity on IBM WebSphere 6.0.2

This chapter describes how to install Select Identity on an IBM WebSphere 6.0.2 application server.

This chapter includes the following topics:

- [Important Installation Information](#)
- [Prerequisite Configuration](#)
- [Using the Select Identity Installer](#)
- [Manual Installation Procedures](#)
- [Logging In to Select Identity on IBM WebSphere](#)

## Introduction

The HP OpenView Select Identity product CD includes an installer that guides you through single or clustered server installation. This method is suitable for most systems. If your environment requires a specialized procedure, this chapter describes manual installation as an alternative.



You must be experienced with WebSphere 6.0.2 to perform a manual installation. The process is complex and consists of many configuration procedures throughout the WebSphere system. It is recommended that you use the Select Identity installer.

## Prerequisite Configuration

This section applies to both standalone and cluster installations, as well as to both installer and manual processes.

Verify that the tasks listed in this section have been performed, or perform them before you begin to install Select Identity.



Select Identity supports clusters through the WebSphere application server layer. See the WebSphere documentation for information on cluster topology.

## Prerequisites for All Installations

The following prerequisites must be complete on all WebSphere installations:

- IBM HTTP Server is configured.
- Host aliases are configured for every server instance.

- The proxy server is configured.
- WebSphere is installed on a system that meets the requirements listed in [Chapter 2, Requirements](#).
- Security is enabled for the WebSphere admin console.
- Two new user accounts have been created on the database (one for Select Identity and one for JMS), and the Select Identity database schema has been loaded, as documented in [Configuring an Oracle Database Server](#) on page 23.
- The security framework has been set up, using the instructions in [Setting Up the Select Identity Security Framework](#) on page 56.

## Prerequisites Specific to Cluster Installations

*On a cluster*, additional prerequisites are as follows:

- Two clusters have been configured, one for Select Identity use, and one for JMS.
- The Network Deployment Manager is configured with appropriate nodes and clusters.
- The Deployment Manager nodes, node agents, and application servers can be started and stopped without errors.

## Installation to Directories with Embedded Spaces

Installation of Select Identity to a directory named with embedded spaces is not recommended. Use directory naming that does not contain spaces; you can use an underscore character in place of a space.

## Preparing to Install Select Identity

To prepare WebSphere for installation, complete the following steps:

- 1 Upgrade the policy files on the WebSphere application server to “unlimited strength” policy files, by downloading the following files from IBM’s Web site:

```
US_export_policy.jar
local_policy.jar
```

- ▶ If you are installing Select Identity in a location other than the United States, you may need location-specific policy files.

- 2 Copy the policy files from [step 1](#) to %WAS\_HOME%/java/jre/lib/security.
- 3 If using Oracle, download the Oracle thin driver `ojdbc14.jar` to the machine running the installer. The installer prompts for the path to this file.

- ▶ The Oracle 10G driver is required.

- 4 On a cluster, configure the shared file system (NFS share on UNIX) for the installation directory.
- 5 For easier access to documentation, copy the product documentation PDF files from the `/docs` directory on the HP OpenView Select Identity product CD, to a directory of your choice on the application server.

You deploy the online help as a Web Application Archive (a .war file) after you have installed Select Identity.

- 6 Ensure that your Select Identity database is configured as described in [Configuring an Oracle Database Server](#) on page 23.
- 7 Configure the custom external keystores and encryption keys, as described in [Setting Up the Select Identity Security Framework](#) on page 56.



Do not attempt to launch Select Identity until the security framework has been completely set up.

- 8 On a standalone installation, start the WebSphere Application Server. On a cluster, start the Deployment Manager and all node agents in the cluster.
- 9 If using the installer process, tail the following log files before starting the installer and monitor the output closely during installation:

```
$USER_INSTALL_DIR/log/install_trace.log
```

```
$APPSERVER_ROOT/profiles/<profile_name>/logs/<servername>/SystemOut.log
```

## Important Installation Information

Before you begin, ensure that you have available the information listed below.

### For all WebSphere 6.0.2 Configurations:

You will need the following information for installation on any configuration topology:

- The SMTP email host to be used by Select Identity
- The database server host name and IP address
- The operating system login ID used when installing WebSphere
- The login ID and password for the Select Identity and JMS database user accounts created in [Chapter 3, Database Server Configuration](#).
- The IP address and host name of the WebSphere admin server
- The login ID and password for the user account with which WebSphere was installed
- The location of the keystore parameter file
- The location of the Oracle thin driver archive file

### For Clusters:

Select Identity installation on a cluster in WebSphere 6.0.2 requires the use of two clusters, one for Select Identity, and one for JMS. You will need the following information for Select Identity installation on a WebSphere cluster topology:

- The directory location on the Network File System where Select Identity shared files will be stored.
- The name of the cluster on which you are installing the Select Identity application.
- The name of the cluster that provides JMS clustering.
- The IP address and host name of every server in both clusters.

- The directory locations of any processes that you will need to start or stop, such as the WebSphere console or node managers.

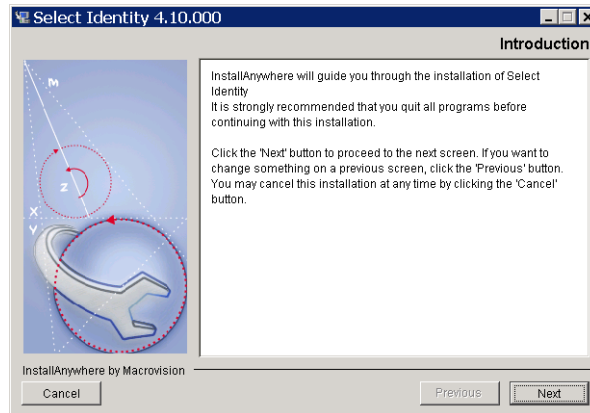
## Using the Select Identity Installer

This section describes how to install Select Identity using the installer. Before starting this procedure, you must complete the [Prerequisite Configuration](#) on page 25.

### Auto-Installation Procedure

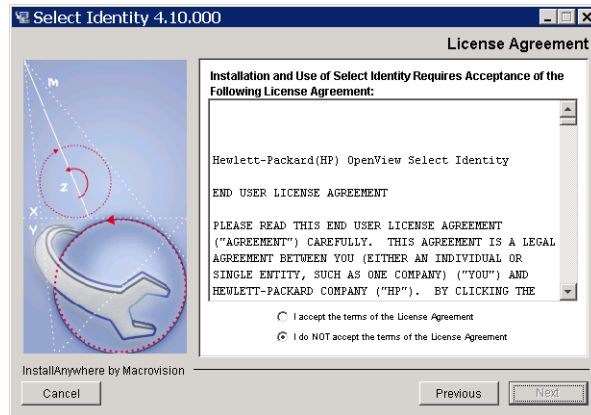
- 1 Log on to the operating system as the same user that was used to install WebSphere.  
You must copy and run the installer directly on the application server's local machine, or the Deployment Manager node in a cluster. Do not try to run the installer remotely.
- 2 Mount the Select Identity CD and navigate to the installation directory.
- 3 Run the `install.bin` executable to open the **Introduction** page of the InstallAnywhere installer.

**Figure 2 The InstallAnywhere Introduction page**



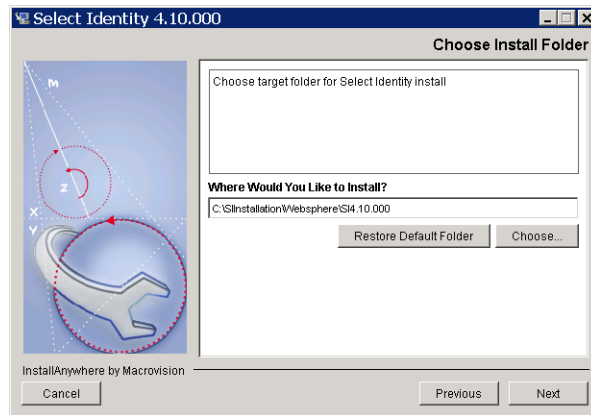
- 4 Click **Next** to review the license agreement.

**Figure 3 The License Agreement page**



- 5 Click the radio button labeled **I Accept the License Agreement** and click **Next** to proceed to the **Choose Install Folder** page.

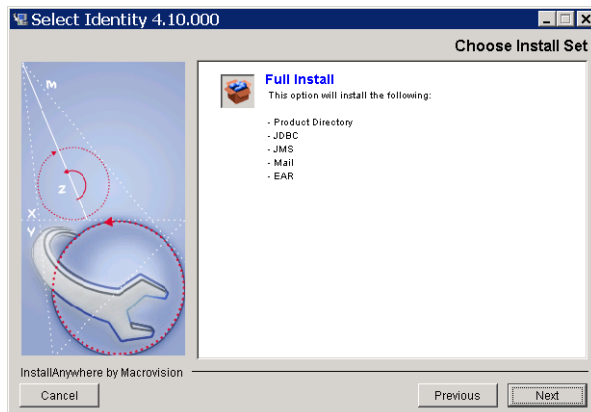
**Figure 4 The Choose Install Folder page**



- 6 Enter or browse to the path for the intended Select Identity home directory and click **Next** to proceed to the **Choose Install Set** page.

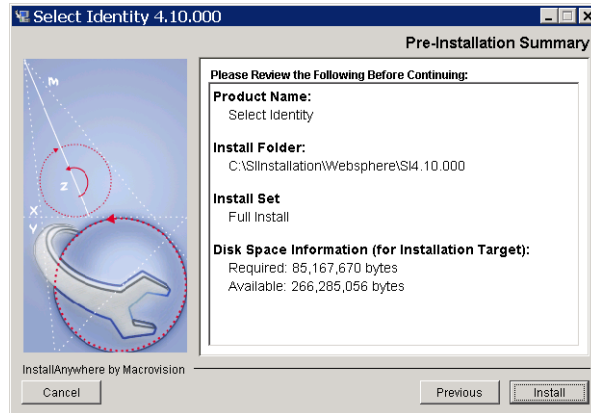
On a cluster, ensure that the installation directory is a shared file system directory.

**Figure 5 The Choose Install Set page**



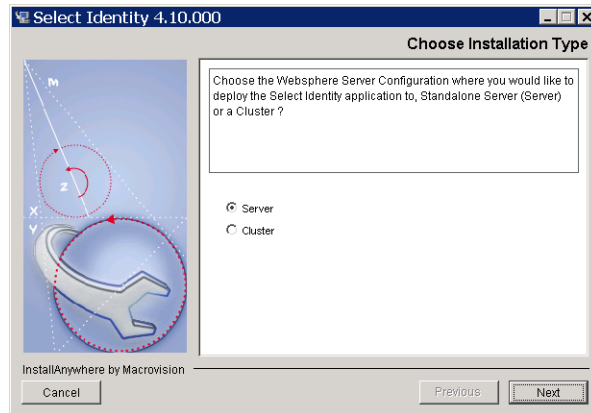
- 7 **Full Install** is the only option on this page; you do not need to select it. Click **Next** to proceed to the **Pre-Installation Summary** page.
- 8 Review the summary information before you click **Install** to continue.

**Figure 6 The Pre-Installation Summary page**



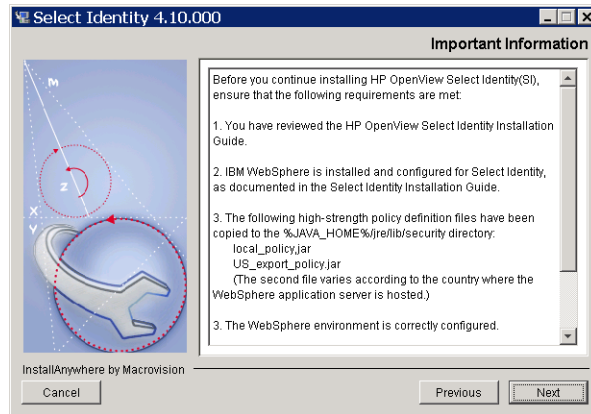
The wizard installs the files according to your settings. A progress bar indicates that the installation is in progress. When installation is complete, the installer displays the **Choose Installation Type** page.

**Figure 7 Choose Installation Type page**



- 9 Select **Server** or **Cluster** according to your WebSphere configuration.
- 10 Click **Next** to proceed to the **Important Information** page.

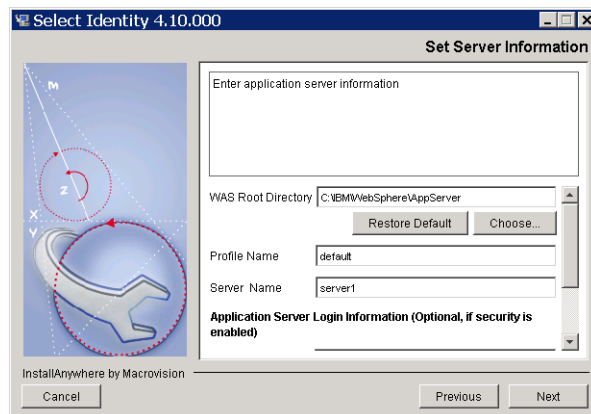
**Figure 8 The Important Information page**



11 Review and follow the instructions on this page, then click **Next**.

- If you are performing a standalone installation, the installer proceeds to the **Set Server Information** page (Figure 9).
- If you are performing a cluster installation, the installer proceeds to the **Set Cluster Information** page (Figure 10).

**Figure 9 The Set Server Information page (standalone installation)**

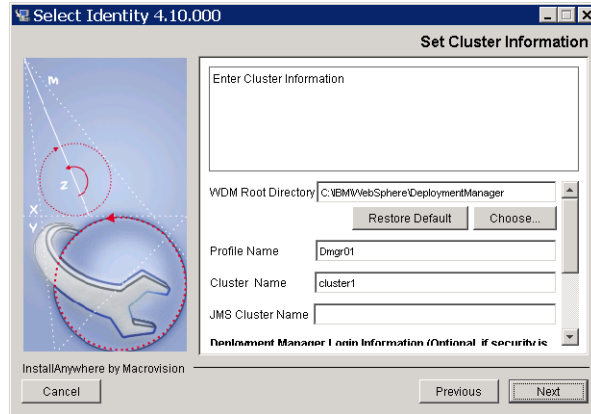


12 If installing on a cluster, skip to [step 13](#). On a standalone installation, specify settings for the Websphere application server, as follows:

- **WAS Root Directory** — The directory where the WebSphere application server is installed.
- **Profile Name** — The profile on which you are installing Select Identity.
- **Server Name** — The server on which you are installing Select Identity
- **Login Name** — The user name for logging in to the WebSphere admin console.
- **Password** and **Confirm Password**— The password for the admin console account. Confirm the password in the **Confirm Password** field.

▶ You do not need to enter login info if security is not enabled. Leave these fields empty if security is not enabled.

**Figure 10 The Set Cluster Information page (cluster installation)**



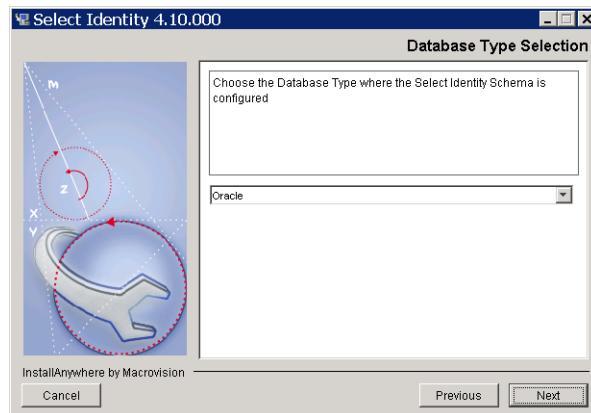
13 Specify cluster settings, as follows:

- **WDM Root Directory** — The directory where the WebSphere application server Network Deployment is installed.
- **Profile Name** — The profile on which you are installing Select Identity.
- **Login Name** — The user name for logging in to the WebSphere admin console.
- **Password** and **Confirm Password**— The password of the admin console account. Confirm the password in the **Confirm Password** field.
  - ▶ You do not need to enter login info if security is not enabled. Leave these fields empty if security is not enabled.
- **Cluster Name** – The name of the cluster on which you are installing the Select Identity application.
- **JMS Cluster Name** – The name of the cluster on which JMS messaging will run.

14 After making the settings, click **Next**.

15 When WebSphere checking is complete, the installer displays the **Database Type Selection** page.

**Figure 11 The Database Type Selection page**

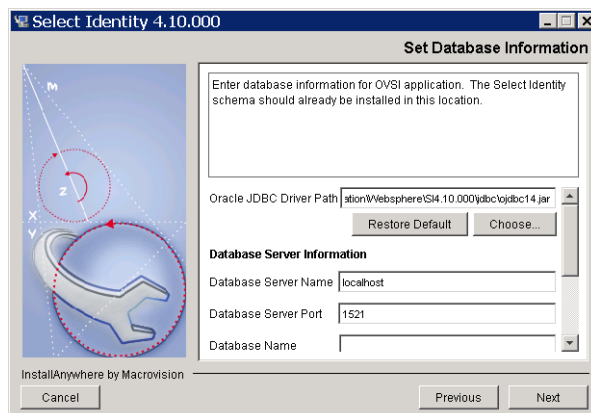


Select your database type and click **Next** to proceed to the **Set Database Information** page for Select Identity.



The instructions and illustrations that describe the database settings are based on Oracle 10g.

**Figure 12 The Set Database Information page (Select Identity)**

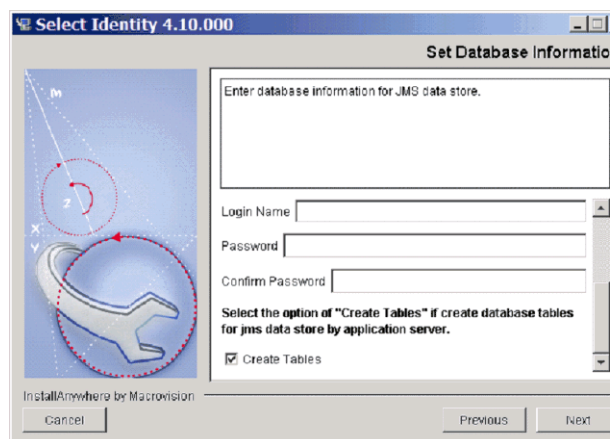


16 Complete the fields with the appropriate information about the Select Identity database user account:

- **Database Server Name** — The hostname or IP address of the database server.
- **Database Server Port** — The port on which the database server communicates with Select Identity.
- **Database Name** — The name of the Select Identity database.
- **Database Login** — The Select Identity database user name.
- **Database Password and Confirm Database Password** — The password for logging in to the database.
- **Oracle JDBC Driver Path** — The full path to the Oracle JDBC driver file (including the actual file name: `ojdbc.jar`).

17 After making the settings, click **Next** to proceed to the **Set Database Information** page for JMS.

**Figure 13 The Set Database Information page (JMS)**



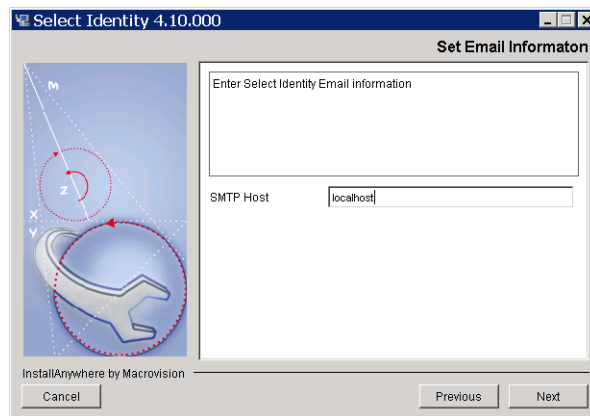
18 Complete the fields with the appropriate information about the JMS database user account:

- **Database Server Name** — The hostname or IP address of the database server.
- **Database Server Port** — The port on which the database server communicates with Select Identity.
- **Database Name** — The name of the Select Identity database.
- **Database Login** — The JMS database user name.
- **Database Password and Confirm Database Password** — The password for logging in to the database.
- **Create Tables** — Check this option if the JMS database user creates the database tables for the messaging engine data store the first time Select Identity starts up. Leave this option unchecked if your database administrator creates the messaging engine database tables beforehand.

► It is recommended that you check the **Create Tables** option in most cases. You can use `sibDDLGenerator.bat` (available under `WAS_INSTALL_ROOT\bin`), to create the JMS data tables. Information is available about the technical background to this setting at IBM's public WebSphere technical library on the Internet.

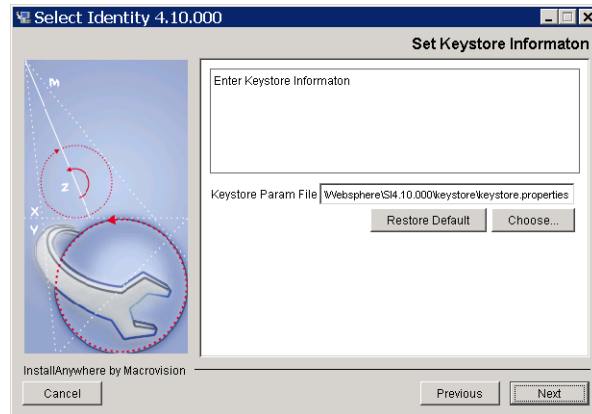
19 After making the settings, click **Next** to proceed to the **Email Information** page.

**Figure 14 The Email Information page**



20 Specify the name of the SMTP host Select Identity uses when sending email, then click **Next** to proceed to the **Keystore Information** page.

**Figure 15 The Set Keystore Information page**



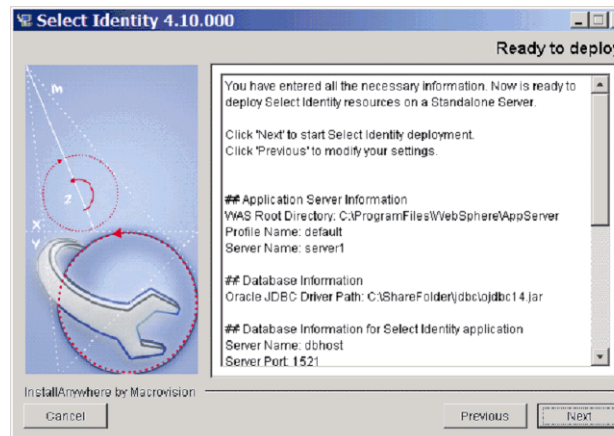
- 21 Click **Choose** and browse to the file system location of the keystore parameters file (keystore.properties).

▶ The correct directory location of the keystore.properties file is documented in [Setting Up the Select Identity Security Framework](#) on page 56.

Complete this task at part of the [Prerequisite Configuration](#) on page 25.

- 22 Click **Next** to proceed to the **Ready to Deploy** page.

**Figure 16 The Ready to Deploy page**



- 23 Click **Next** to deploy Select Identity.

When Select Identity is installed and deployed, the installer displays the **Installation Complete** page.

- 24 Click **Done** to close the installer.

- 25 For standalone and every server in a cluster, copy the following files from the Select Identity product CD to the \$WEBSHERE\_HOME/lib/ext directory:

- sysArchive/connector.jar
- sysArchive/ovsii18n.jar

- 26 Stop and restart the server or the Select Identity cluster (as applicable), so that WebSphere loads the `.jar` files that you copied in [step 25](#).
- 27 Refer to [Chapter 5, Configuring Select Identity](#), and [Appendix B, Configuring TruAccess.properties](#) for information about configuring the `TruAccess.properties` file for your environment.
- 28 Deploy the online help, as documented in [Deploying Select Identity and the Online Help](#) on page 48.
- 29 Configure the WebSphere logging features for Select Identity, as documented in [Configuring Logging for Select Identity](#) on page 50.
- 30 Stop and restart the WebSphere application server.  
On a cluster, stop and restart all Node Agents and Deployment Manager.
- 31 If using global security, refer to [Configuring Global Security](#) on page 51.
- 32 You can now log in to Select Identity, as documented in [Logging In to Select Identity on IBM WebSphere](#) on page 51.

## If Auto-Installation is Not Successful

If you are unable to launch Select Identity after running the installer, or if the installer returns any errors, it is recommended that you uninstall by running the auto-uninstaller, using the instructions provided in [Auto-Uninstalling Select Identity](#) on page 105. This procedure removes any installed components even if the installation is incomplete.

After uninstalling, investigate any error messages and check your database and Web application server to ensure these systems are correctly configured for Select Identity.

When re-installing, double-check the information you provide in each field of the installer. In many instances, small errors such as incorrect paths can cause installation to fail.

# Manual Installation Procedures

This section covers the following topics:

- [How This Section is Organized](#)
- [Creating Directories and Copying Files](#)
- [Configuration Scope](#)
- [Creating J2C Authentication Data Entries](#)
- [Creating the Oracle JDBC Provider](#)
- [Creating the Oracle Data Sources](#)
- [Configuring the Select Identity Service Integration Bus](#)
- [Creating JMS Resources](#)
- [Configuring the Select Identity Mail Provider, Protocol Provider, and Mail Session](#)
- [Deploying Select Identity and the Online Help](#)
- [Updating The Select Identity Application Settings](#)
- [Updating the Server Class Loading Mode](#)
- [Configuring Logging for Select Identity](#)

## How This Section is Organized

This section does not provide detailed instructions about how to navigate in IBM WebSphere 6.0.2; you must be familiar with the Web application server platform in order to perform Select Identity manual installation. Ensure that you have the appropriate WebSphere documentation available before you begin.

Each procedure provides a suggested navigation route to the configuration pages concerned. However, in many instances it is possible to reach the same page by more than one route. As the navigational information is primarily for guidance, use the route you prefer where alternatives exist.

The procedures document only settings you must change, or items that you must add. If a field, setting, or item is not mentioned, leave the default unchanged.

## Creating Directories and Copying Files

The following steps prepare the Select Identity directories on the WebSphere server before you configure it and deploy Select Identity.

- 1 Create a shared directory on the application server that will serve as the Select Identity home directory. The product and connector installations will reference this directory.

For example, create the `/opt/<OVSI_INSTALL_DIR>` directory.

On a cluster, this directory must be in the network file system, accessible by all servers in the cluster.

Refer to the WebSphere installation documentation for more information.

- 2 Create the following subdirectories in the <OVSI\_INSTALL\_DIR> directory:
  - <OVSI\_INSTALL\_DIR>/deploy
  - <OVSI\_INSTALL\_DIR>/email
  - <OVSI\_INSTALL\_DIR>/lib
  - <OVSI\_INSTALL\_DIR>/recon
  - <OVSI\_INSTALL\_DIR>/recon/reconroot
  - <OVSI\_INSTALL\_DIR>/recon/reconbackup
  - <OVSI\_INSTALL\_DIR>/recon/reconstaging
  - <OVSI\_INSTALL\_DIR>/reports
  - <OVSI\_INSTALL\_DIR>/sysArchive
  - <OVSI\_INSTALL\_DIR>/temp
  - <OVSI\_INSTALL\_DIR>/upload
  - <OVSI\_INSTALL\_DIR>/userimport
  - <OVSI\_INSTALL\_DIR>/userimport/adbackup
  - <OVSI\_INSTALL\_DIR>/userimport/adroot
  - <OVSI\_INSTALL\_DIR>/userimport/adstaging
- 3 Copy the following files from the Select Identity product CD to the <OVSI\_INSTALL\_DIR>/deploy directory:
  - application/WAS6\_lmz.ear
  - application/ovsil10n\_help\_en\_US.war
- 4 Copy the following file from the Select Identity product CD to <OVSI\_INSTALL\_DIR>/sysArchive.
  - properties/TruAccess.properties
- 5 Create a directory for each connector type that you install; install connector-specific information only into its respective directory.
- 6 On the WebSphere application server, or on every node if installing on a cluster, copy the following files to the \$WAS\_HOME/lib/ext directory from the Select Identity Product CD:
  - sysArchive/connector.jar
  - sysArchive/ovsil18n.jar

Make sure that these files reside in this directory when starting the WebSphere application server.
- 7 Stop and restart the WebSphere server or Select Identity cluster (whichever applies).
- 8 For easier access to documentation, copy the product documentation PDF files from the docs directory on the HP OpenView Select Identity product CD to a directory of your choice on the application server.
 

You deploy the online help separately as a Web Application Repository (.war), after you have deployed the Select Identity application.
- 9 Ensure that the system where WebSphere is installed meets the *minimum* requirements, documented in [System Requirements](#) on page 9.
- 10 Log on to the WebSphere Administrative Console as **admin**.

## Configuration Scope

The scope selection is crucial to many of the manual installation procedures in both standalone and cluster configurations. Use the following table for reference regarding the correct scope selection for the configuration items listed:

	<b>Mail</b>	<b>J2C Auth</b>	<b>JDBC Prov</b>	<b>JMS Queue Factory</b>	<b>JMS Topic Factory</b>	<b>JMS Queue</b>	<b>JMS Topic</b>	<b>Activ. Spec</b>	<b>EAR File</b>
Standalone	Server	Cell	Server	Server	Server	Server	Server	Server	Server
Cluster (Select Identity and JMS)	Cluster	Cell	Cluster	Cluster	Cluster	Cluster	Cluster	Cluster	Cluster

## Creating J2C Authentication Data Entries

- 1 In the left panel of the console, navigate to **Security** → **Global Security**.
- 2 Expand **JAAS Configuration**, located on the bottom right of the page.
- 3 Click **J2C Authentication Data Entries**, at the bottom of this group.
- 4 Click **New**.
- 5 Create a data entry for Select Identity, with the listed fields set as follows:
  - **Alias:** OVSI Oracle10g
  - **User ID:** <DB\_LOGIN>
  - **Password:** <DB\_PASSWORD>
- 6 Click **Apply**.
- 7 Create an additional authentication data entry for the JMS datastore, with the listed fields set as follows:
  - **Alias:** OVSI Oracle10g\_JMS
  - **User ID:** <JMS\_DB\_LOGIN>
  - **Password:** <JMS\_DB\_PASSWORD>
- 8 Click **Apply**.
- 9 Save your changes to the master configuration.

## Creating the Oracle JDBC Provider

*On a cluster,* create two JDBC providers, one on the Select Identity cluster, and one on the JMS cluster, by performing the following steps.

*On a standalone installation,* create a single JDBC Provider, named OVSI Oracle JDBC Provider.

- 1 In the left panel of the console, navigate to **Resources** → **JDBC Providers**.
- 2 Set cluster **Scope** (the Select Identity cluster).
- 3 Click **New**.

- 4 Make the following selections:
  - **Database Type:** Oracle
  - **Provider Type:** Oracle JDBC Driver
  - **Implementation:** XA data source.
- 5 Click **Next**.
- 6 Enter or select the following items:
  - **Name:** OVSI Oracle JDBC Provider
  - **Class Path:** Enter the path to the Oracle 10g JDBC driver.
- 7 Click **Apply**.
- 8 Save your changes to the master configuration.
- 9 Repeat [step 1](#) through [step 8](#) to create a second JDBC provider, with the **Scope** set to the JMS cluster, and the **Name** set to **OVSI Oracle10g JMS JDBC Provider**.

## Creating the Oracle Data Sources

Select Identity requires two Oracle data sources, one for Select Identity and one for the JMS data store.

*On a cluster,* locate the OVSI DataSource under the Select Identity JDBC Provider, on the Select Identity cluster. Locate the OVSI JMS DataSource under the Select Identity JMS JDBC Provider, on the JMS cluster.

*On a standalone installation,* Locate both data sources under the JDBC Provider (OVSI Oracle JDBC Provider).

To create the data sources, perform the following steps:

- 1 Navigate to the JDBC Provider named OVSI Oracle 10G JDBC Provider, that you created in [Creating the Oracle JDBC Provider](#) on page 39.
- 2 Click **Data Source**, under **Additional Properties**.
- 3 Click **New**, and create a data source for **Select Identity**:
  - a Set the following fields, as listed:
    - **Name:** OVSI DataSource
    - **JNDI Name:** jdbc/TruAccess
    - **Data Store Helper Class Name:** Oracle10g data store helper
    - **Component-managed Authentication Alias:** OVSI Oracle10g
    - **Url:** jdbc:oracle:thin:@<DBSERVER\_NAME>:<DBSERVER\_PORT>:<DB\_NAME>
  - b Click the link to **Connection Pools**, at the bottom of the page.
  - c Make the following settings:
    - **Maximum Connections:** 100
  - d Click the link to **WebSphere Application Server Data Source Properties**, under **Additional Properties**.
  - e Set the following value:
    - **Statement Cache Size:** 50



- f Return to the Select Identity data source page.
- g Apply the Select Identity data source.

Create a data source for the JDBC Provider for JMS by performing the following steps:

- 1 Navigate to the JDBC Provider named OVSI Oracle 10G JMS JDBC Provider, that you created in [Creating the Oracle JDBC Provider](#) on page 39.
- 2 Click **Data Source**, under **Additional Properties**.
  - a Click **New**, and create a data source for **JMS**:
  - b Set the following fields, as listed:
    - **Name:** OVSI JMS DataSource
    - **JNDI Name:** jdbc/TruAccess\_JMS
    - **Data Store Helper Class Name:** Oracle10g data store helper
    - **Component-managed Authentication Alias:** OVSI Oracle10g\_JMS.
    - **Url:** jdbc:oracle:thin:@<DBSERVER\_NAME>:<DBSERVER\_PORT>:<DB\_NAME>
  - c Click the link to **Connection Pool Properties**, on the top right under **Additional Properties**.
  - d Make the following settings:
    - **Maximum Connections:** 100
  - e Return to the **JMS Data Source** page.
  - f Apply the JMS data source.
  - g Save your changes to the master configuration.

## Configuring the Select Identity Service Integration Bus

To configure the Select Identity integration bus, perform each of the procedures in this section.

To create the integration bus, perform the following steps:

- 1 In the left panel of the console, navigate to **Service Integration** → **Buses**.
- 2 Click **New**.
- 3 Name the bus **OVSIBus**.
- 4 Set the **High Message Threshold** to 500,000.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration using the **Message** link at the top of the page.

### Adding Bus Members

To add bus members, perform the following steps:

- 1 Follow the link to **Bus Members**, under **Topology**, in the top right of the page.
- 2 Add the member appropriate to your WebSphere configuration:
  - *For standalone servers*, add the WebSphere server as a bus member.
  - *For clusters*, add your JMS cluster as a bus member.

- 3 Set the **Data Source JNDI Name** field for the new member to `jdbc/TruAccess_JMS`.
- 4 Under **Data Store**, deselect **Default**.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration using the **Message** link at the top of the page.

## Creating Bus Destinations

To create bus destinations (JMS queues and topics), perform the following steps:

- 1 Follow the link to **Destinations**, under **Destination Resources**, in the top right of the page.
- 2 Create the JMS destination queues listed in the table below.
  - Assign each to the bus member you created earlier (this should be the default selection).
  - Ensure that you enter each **Name** and **JNDI Name** *exactly* as listed below:
    - `jms.OVSIAuditProcQ`
    - `jms.OVSIBulkQueue`
    - `jms.OVSIChangeReconProcessorQueue`
    - `jms.OVSIEntCacheQueue`
    - `jms.OVSIMessageAckQueue`
    - `jms.OVSIReconQueue`
    - `jms.OVSIResReconDispatcherQ`
    - `jms.OVSIResReconQ`
    - `jms.OVSI SaudQ`
    - `jms.OVSI SchedulerQueue`
    - `jms.OVSI ServiceAssignQueue`
    - `jms.OVSI UserImportPQueue`
    - `jms.OVSI WorkflowQueue`
    - `jms.OVSI WfRequestExpireQueue`
- 3 Click **Finish** after entering the settings for each destination, before creating the next.
- 4 Return to the **Destinations page** and click **Topics**.
- 5 Create the topic spaces listed in the following table.
  - Assign each topic to the bus member you created earlier (this should be the default selection).
  - Ensure that you enter each **Name** *exactly* as listed below:
    - `jms.OVSI AuditBroadcast`
    - `jms.OVSI CacheTopic`
- 6 Click **Apply** after you create each topic destination.
- 7 Navigate to **OVSIBus** → **Messaging Engines** → `<your_messaging_engine>` → **Data Store**.

- 8 Set the **Schema Name** to <JMSDB\_LOGIN\_USER> (in Oracle, the schema name is the same as the user name).
- 9 Select the JMS data store **Authentication Alias** (OVSI Oracle10g\_JMS) that you created in [Creating J2C Authentication Data Entries](#) on page 39.
- 10 When you have created all the queue and topic destinations, save your changes to the master configuration using the **Message** link at the top of the page.

## Creating JMS Resources

Creating the JMS resources consists of creating the following components:

- One queue connection factory
- One topic connection factory
- Fourteen JMS queues
- Two JMS topics
- One activation specification for each JMS queue and topic

Each JMS queue and topic, together with its corresponding activation specification, also maps to the bus destinations created in [Creating Bus Destinations](#) on page 42.

## Creating The Queue and Topic Connection Factories

Perform the following steps to create the JMS queue connection factory:

- 1 In the left panel of the console, navigate to **Resources** → **JMS Providers** → **Default Messaging**.
- 2 Select the **Scope** appropriate to your configuration, as follows:
  - *For standalone servers*, select **Server** scope.
  - *For clusters*, select **Cluster** scope (the JMS cluster).
- 3 Under **Connection Factories** in the bottom right of the page, click **JMS Queue Connection Factory**.
- 4 Click **New**.
- 5 Set the listed queue connection factory fields as follows:
  - **Name:** jms.OVSIQCF
  - **JNDI Name:** jms/OVSIQCF
  - **Bus Name:** OVSIBus
- 6 Click **Apply**.
- 7 Click the link to **Advanced Connection Pool Properties**, under **Additional Properties** on the top right of the page.
- 8 Set the **Max Connections** field to 100.
- 9 Click **Apply**.
- 10 Save your changes to the master configuration using the **Message** link at the top of the page.
- 11 Return to the **Default Messaging** page.

Perform the following steps to create the topic connection factory:

- 1 Under **Connection Factories** in the bottom right of the page, click **JMS Topic Connection Factory**.
- 2 Click **New**.
- 3 Set the listed topic connection factory fields as follows:
  - **Name:** `jms.OVSITCF`
  - **JNDI Name:** `jms/OVSITCF`
  - **Bus Name:** `OVSIBus`
- 4 Click **Apply**.
- 5 Click the link to **Connection Pool Properties**, under **Additional Properties** on the top right of the page.
- 6 Set the **Max Connections** field to 100.
- 7 Click **Apply**.
- 8 Save your changes to the master configuration using the **Message** link at the top of the page.
- 9 Return to the **Default Messaging** page.

## Creating the JMS Queues and Topics

Perform the following steps to create the JMS queues:

- 1 In the left panel of the console, navigate to **Resources** → **JMS Providers** → **Default Messaging**.
- 2 Select the **Scope** appropriate to your configuration, as follows:
  - For *standalone servers*, select **Server** scope.
  - For *clusters*, select **Cluster** scope (the JMS cluster).
- 3 Click **JMS Queues**, in the bottom right of the page.
- 4 On the **JMS Queues** page, click **New**.
- 5 Name the JMS queues as listed in the table below.
  - Ensure that you enter each **Name** and **JNDI Name** *exactly* as shown.

Name	JNDI Name
<b>jms.OVSIAuditProcQ</b>	<code>jms/OVSIAuditProcQ</code>
<b>jms.OVSIBulkQueue</b>	<code>jms/OVSIBulkQueue</code>
<b>jms.OVSIChangeReconProcessorQueue</b>	<code>jms/OVSIChangeReconProcessorQueue</code>
<b>jms.OVSIEntCacheQueue</b>	<code>jms/OVSIEntCacheQueue</code>
<b>jms.OVSIMessageAckQueue</b>	<code>jms/OVSIMessageAckQueue</code>
<b>jms.OVSIReconQueue</b>	<code>jms/OVSIReconQueue</code>
<b>jms.OVSIResReconDispatcherQ</b>	<code>jms/OVSIResReconDispatcherQ</code>
<b>jms.OVSIResReconQ</b>	<code>jms/OVSIResReconQ</code>

Name	JNDI Name
jms.OVSIaudQ	jms/OVSIaudQ
jms.OVSI SchedulerQueue	jms/OVSI SchedulerQueue
jms.OVSI ServiceAssignQueue	jms/OVSI ServiceAssignQueue
jms.OVSI UserImportPQueue	jms/OVSI UserImportPQueue
jms.OVSI WorkflowQueue	jms/OVSI WorkflowQueue
jms.OVSI WfRequestExpireQueue	jms/OVSI WfRequestExpireQueue

- 6 For each queue, set the following fields as listed under **Connection**:
  - **Bus Name**: Select **OVSIBus**. This populates the **Queue Name** field.
  - **Queue Name**: Select the name corresponding to the queue.
- 7 Click **OK** after entering the settings for each queue, before creating the next:
- 8 When you have completed the queues listed, save your changes to the master configuration using the **Message** link at the top of the page.

Perform the following steps to create the JMS topics:

- 1 Return to the **Default Messaging** page.
- 2 Click **JMS Topics**, in the bottom right of the page.
- 3 On the **JMS Topics** page, click **New**.
- 4 Name the JMS topics as listed in the table below.

Ensure that you enter each **Name** and **JNDI Name** exactly as shown:

Name	JNDI Name	Topic Space
jms.OVSI AuditBroadcast	jms/OVSI AuditBroadcast	jms.OVSI AuditBroadcast
jms.OVSI CacheTopic	jms/OVSI CacheTopic	jms.OVSI CacheTopic

- 5 For each topic, set the following fields as listed under **Connection**:
  - **Bus Name**: Select **OVSIBus**. This populates the **Topic Name** field.
  - **Topic Name**: Select the name corresponding to the topic.
- 6 Click **OK** after entering the settings for each topic, before creating the next:
- 7 When you have created all fourteen queues and two topics, save your changes to the master configuration using the **Message** link at the top of the page.

## Creating Activation Specifications

To create the activation specifications, perform the following steps from the **Default Messaging** page:

- 1 Under **Activation Specifications** in the bottom right of the page select **JMS Activation Specification**.

The following steps document the creation of an activation specification for each Select Identity JMS queue and topic.

- 2 Click **New**.
- 3 Set the fields *exactly* as listed for each activation specification in the following tables:
  - a For the entries in the table below, select **Queue** as the **Destination Type**, and **OVSIBus** as the **Bus Name**:

<b>Name</b>	<b>JNDI Name</b>	<b>Destination JNDI Name</b>	<b>Maximum Concurrent Endpoints</b>
eis.OVSIAuditProcQ	eis/OVSIAuditProcQ	jms/OVSIAuditProcQ	10
eis.OVSIBulkQueue	eis/OVSIBulkQueue	jms/OVSIBulkQueue	10
eis.OVSIChangeReconProcessorQueue	eis/OVSIChangeReconProcessorQueue	jms/OVSIChangeReconProcessorQueue	10
eis.OVSIEntCacheQueue	eis/OVSIEntCacheQueue	jms/OVSIEntCacheQueue	10
eis.OVSIMessageAckQueue	eis/OVSIMessageAckQueue	jms/OVSIMessageAckQueue	1
eis.OVSIReconQueue	eis/OVSIReconQueue	jms/OVSIReconQueue	2
eis.OVSIResReconDispatcherQ	eis/OVSIResReconDispatcherQ	jms/OVSIResReconDispatcherQ	10
eis.OVSIResReconQ	eis/OVSIResReconQ	jms/OVSIResReconQ	10
eis.OVSIISaudQ	eis/OVSIISaudQ	jms/OVSIISaudQ	10
eis.OVSIISchedulerQueue	eis/OVSIISchedulerQueue	jms/OVSIISchedulerQueue	5
eis.OVSIServiceAssignQueue	eis/OVSIServiceAssignQueue	jms/OVSIServiceAssignQueue	10
eis.OVSIUserImportPQueue	eis/OVSIUserImportPQueue	jms/OVSIUserImportPQueue	2
eis.OVSIWorkflowQueue	eis/OVSIWorkflowQueue	jms/OVSIWorkflowQueue	10
eis.OVSIWfRequestExpireQueue	eis/OVSIWfRequestExpireQueue	jms/OVSIWfRequestExpireQueue	3

- b For the entries in the table below, select **Topic** as the **Destination Type**, and **OVSIBus** as the **Bus Name**.

<b>Name</b>	<b>JNDI Name</b>	<b>Destination JNDI Name</b>	<b>Maximum Concurrent Endpoints</b>
eis.OVSIAuditBroadcast	eis/OVSIAuditBroadcast	jms/OVSIAuditBroadcast	1
eis.OVSIICacheTopic	eis/OVSIICacheTopic	jms/OVSIICacheTopic	10

- 4 Click **Apply** after entering each activation specification.

- 5 When you have entered and applied all the activation specifications, save the changes to the master configuration using the **Message** link at the top of the page.

## Configuring the Select Identity Mail Provider, Protocol Provider, and Mail Session

To configure the Select Identity mail provider and session, perform the following steps:

- 1 Create a Select Identity mail provider by completing the following steps:
  - a In the left panel of the console, navigate to **Resources** → **Mail Providers**.
  - b Set the appropriate **Scope** as specified in [Configuration Scope](#) on page 39:
    - *For standalone servers*, select **Server** scope.
    - *For clusters*, select **Cluster** scope (the Select Identity cluster).
  - c Set the following mail provider fields:
 

**Name:** OVSI Mail Provider.

**Description:** Enter an appropriate description.
  - d Click **Apply**.
- 2 Perform the following steps to create an SMTP protocol provider:
  - a On the **Mail Providers** page, click the link to the **OVSI Mail Provider**.
  - b On the configuration page for the **OVSI Mail Provider**, select **Protocol Providers** under **Additional Properties**, in the top right of the page.
  - c Click **New**.
  - d Set the listed fields as follows:
 

**Protocol:** smtp

**Class name:** com.sun.mail.smtp.SMTPTransport

**Type:** TRANSPORT
  - e Click **Apply**.
- 3 Create a Select Identity mail session in the **OVSI Mail Provider** by completing the following steps:
  - a Return to the **OVSI Mail Provider** configuration page.
  - b Follow the link to **Mail Sessions**, under **Additional Properties**, in the top right of the page.
  - c Click **New**.
  - d Set the mail session fields as listed in the following table:

Field	Value
<b>Name</b>	<b>OVSI Mail Session</b>
<b>JNDI Name</b>	<b>mail/TruAccess</b>
<b>Mail Transport Host</b>	The IP address of the server to which to connect when sending mail.
<b>Mail Transport Protocol</b>	<b>smtp</b>

- e Click **Apply**.
- f Save your changes to the master configuration using the **Message** link at the top of the page.

## Deploying Select Identity and the Online Help

Select Identity is provided as an Enterprise Application Repository (.ear) file, for deployment via the WebSphere **Install New Application** page.

The online help is a .war (Web Application Repository) file, located in the same directory as the .ear file deployed to activate Select Identity. This is the only .war file in that directory location. The precise file name varies according to the localized version of Select Identity that you are using.

To deploy the Select Identity .ear file and the help .war file, perform the following steps:

- 1 In the left panel of the console, navigate to **Applications** → **Install New Application**.
- 2 Under **Path to the New Application**, click **Browse for Remote File System**, then browse to the Select Identity home directory created in [Creating Directories and Copying Files](#) on page 37.
- 3 Open the \deploy directory, select WAS6\_lmz.ear, and click **OK**.
- 4 If you are installing the online help, provide the **Context Root** value for the help file:  
`ovsi_help_en_US`  
This value should be adjusted for localized versions of the help.
- 5 On the **Install New Application** page, click **Next**.
- 6 Accept the defaults on the **Bindings and Mappings** page, and click **Next**.
- 7 On the **Select Installation Options** page, enter OVSIApplication as the **Application Name**.
- 8 Accept all other defaults on the **Select Installation Options** page and click **Next**.
- 9 Click **Next** on the **Map Modules to Servers** page.
- 10 Click **Next** on the **Provide Listener Bindings for Message-Driven Beans** page.
- 11 If installing on a standalone server, click **Next** on the **Map Modules to Servers** page. If installing on a cluster, target all application modules to the Select Identity cluster.
- 12 Click **Next** on the **Provide JNDI Names for Beans** page.
- 13 Click **Next** on the **Map EJB references to beans** page.
- 14 Click **Next** on the **Map Resource References to Resources** page.
- 15 Click **Next** on the **Map resource env entry references to resources** page.
- 16 Click **Next** on the **Map Virtual Hosts for Web modules** page.
- 17 Click **Next** on the **Ensure all unprotected 2.x methods have the correct level of protection** page.
- 18 On the **Summary** page, review the settings and correct as needed.



For the WAS6\_LMZ.ear deployment, you should see the following settings on this page:

Option	Value
Use Binary Configuration	No
Create MBeans for resources	Yes
Cell/Node/Server	<a href="#">Click here</a>
Reload interval in seconds	
Enable class reloading	No
Process embedded configuration	No
Application name	OVSIAApplication
Validate Input off/warn/fail	warn
Directory to install application	\opt\<<OVSI_INSTALL>
Distribute application	Yes
Deploy Web services	No
Pre-compile JSP	No
Deploy enterprise beans	No

- 19 Click **Finish** after you have reviewed the installation options.
- 20 Deploy the online help by repeating this procedure from [step 1](#), selecting the help .war file in place of the Select Identity .ear file.

## Updating The Select Identity Application Settings

Set the Class Loader Mode and WAR Class Loader Policy by performing the following steps:

- 1 In the left panel of the console, navigate to **Applications** → **Enterprise Applications**.
- 2 Click the link to the **Configuration** page for the Select Identity application.
- 3 In the center left of the page, under **Class Loading and File Update Detection**, make the following selections:
  - **Class loader mode:** Parent Last
  - **WAR class loader policy:** Module
- 4 Click **Apply**.
- 5 Save your changes to the master configuration.

Set the Transaction Timeout by performing the following steps. Perform this procedure on every server if you are installing on a cluster:

- 1 In the left panel of the console, navigate to **Servers** → **Application Servers**.
- 2 Select the server from the list in the main area of the page.
- 3 Expand the item labeled **Container Services** in the top center of the page, and click the link to **Transaction Service**.

- 4 Set the field labeled **Total transaction lifetime timeout** to 300.
- 5 Apply and then save your settings to the master configuration.

## Updating the Server Class Loading Mode

To update the server class loading mode, perform the following steps:

- 1 In the left panel of the console, navigate to **Servers** → **Application Servers**.
- 2 *For cluster installations*, navigate to the **Configuration** page for each server in the Select Identity cluster, and perform the remainder of this procedure on each one.  
*For standalone installations*, navigate to the **Configuration** page for the WebSphere server.
- 3 Under **Server-specific Application Settings**, on the left of the **Configuration** page, select **Parent Last** for the **Class Loading Mode**.
- 4 Click **Apply**.
- 5 Repeat this procedure for each server if you are installing on a cluster.
- 6 Save your changes to the master configuration.

## Configuring the Java Virtual Machine

- 1 In the left panel of the console, navigate to **Resources** → **Application Servers**.
- 2 *For cluster installations*, navigate to the **Configuration** page for each server in the Select Identity cluster, and perform the remainder of this procedure on each one.  
*For standalone installations*, navigate to the **Configuration** page for the WebSphere server.
- 3 Under **Server Infrastructure**, in the center right of the page, expand the **Java and Process Management** item, and click **Process Definition**.
- 4 On the **Process Definition** page, under **Additional Properties** in the top right, click **Java Virtual Machine**.
- 5 On the **Java Virtual Machine** page, set the listed fields as follows:
  - **Generic JVM arguments:**  
"-Dcom.truologica.truaccess.property.file=<OVSI\_INSTALL\_DIR>/sysArchive/TruAccess.properties -Djava.awt.headless=true".
  - **Initial Heap Size:** 256
  - **Maximum Heap Size:** 1024
- 6 Click **Apply**.
- 7 Save your changes to the master configuration.

## Configuring Logging for Select Identity

Configure logging for Select Identity, if desired, by setting the logging file location.

This procedure is not essential, but it is strongly recommended.

On a cluster, perform the following steps on every server:

- 1 In the left panel of the console, navigate to **Troubleshooting** → **Logging and Tracing**.

- 2 Click the link to the application server, or each cluster node in turn.
- 3 Click **JVM Logs**.
- 4 Change the content of the **file name** field to reflect the directory location of the Select Identity log file.
- 5 Click **Apply** after changing this setting on each node in a cluster.
- 6 Save your changes to the master configuration.

## Configuring Global Security

Configure Global Security, if your system uses it, by performing the following steps:

- 1 In the left panel of the console, navigate to **Security** → **Global Security**.
- 2 Disable the setting labeled **Enforce Java 2 Security**.
- 3 Apply the changes and then save to the master configuration.
- 4 In the left panel of the console, navigate to **Environment** → **Naming** → **CORBA Naming Service Groups** → **Everyone**.
- 5 Enable **Read** and **Write** permissions for this group.
- 6 Apply and then save the change to the master configuration.

You must also disable security on the OVSI bus if you are using Global Security.

To disable security for the OVSI bus, perform the following steps:

- 1 In the left panel of the console, navigate to **Service integration** → **Buses** → **OVSIBus**.
- 2 Uncheck the box labeled **Secure** in **Security settings**.
- 3 Apply and then save the change to the master configuration.

## Verifying the Select Identity Installation

From the WebSphere admin console, verify deployment as summarized in this section:

- *On a cluster*, use **Cluster** scope (for the OVSI cluster) to view JDBC providers, JMS providers and Mail providers.
- *On a standalone installation*, use **Server** scope to verify the items listed for the cluster verification above.

There are additional configuration steps for WebSphere installations. See [Configuring Select Identity](#) on page 53 to finish the process.



Do not launch the Select Identity application until you have set up the security framework as described in [Setting Up the Select Identity Security Framework](#) on page 56. This is a critical step.

## Logging In to Select Identity on IBM WebSphere

To log in to Select Identity on WebSphere, enter a URL similar to the example below:

**http://app\_svr\_host IP:port/lmz/signin.do**

The port used in the login URL depends on the configuration of virtual hosts in your WebSphere environment. Host aliases must be defined for each HTTP transport port in the Web container within a cluster. If the virtual host uses the default port (80), an entry for port 80 should be specified in the host alias.

Refer to the documentation supplied with WebSphere, such as the Network Deployment Edition manual, for information about virtual host configuration.

# 5 Configuring Select Identity

This chapter provides important information and procedures for required and recommended configuration of Select Identity after installation.

This chapter contains the following topics:

- [Configuring Required TruAccess Properties](#)
- [Setting Up the Select Identity Security Framework](#)
- [Recommended Configuration](#)
- [Default Values for User Interface Properties](#)
- [Custom User Interface Properties](#)
- [Internationalization and Localization](#)
- [Configuration for Specific Environments or Platforms](#)



If you are installing on a cluster, you must perform these configuration steps on every node in the cluster.

## Configuring Required TruAccess Properties

Many configuration settings are made by modifying the content of a file named `TruAccess.properties`. This file is located in the `<OVSI_INSTALL_DIR>\sysArchive` directory. Many settings are optional, such as those that determine defaults for the Select Identity client.

For a complete listing and description of all settings in the `TruAccess.properties` file, see [TruAccess Properties](#) on page 107.

### How to Set Properties

To change the default value of any property in the `TruAccess.properties` file, use a text editor such as Vi or Notepad to open the file, make the change, and save it. It is recommended that you back up the original before making any change.

### Required Settings

The `TruAccess.properties` settings documented in this section are required. Ensure they are set correctly before starting Select Identity for the first time.

## Directory Locations

Modify the following settings in the `TruAccess.properties` file to point to the actual directories in your Select Identity. These are essential system directories, and must be accurately specified:

- `ovsi.ad.rootdir=<OVSI_INSTALL_DIR>/userimport/adroot`
- `ovsi.ad.backupdir=<OVSI_INSTALL_DIR>/userimport/adbackup`
- `ovsi.ad.stagingdir=<OVSI_INSTALL_DIR>/userimport/adstaging`
- `truaccess.recon.rootdir=<OVSI_INSTALL_DIR>/recon/reconroot`
- `truaccess.recon.stagingdir=<OVSI_INSTALL_DIR>/recon/reconstaging`
- `truaccess.recon.backupdir=<OVSI_INSTALL_DIR>/recon/reconbackup`
- `truaccess.batch.reportdir=<OVSI_INSTALL_DIR>/reports`
- `=truaccess.upload.filedir=<OVSI_INSTALL_DIR>/upload`

### Staging Directories for One-Time Reconciliation and Import Jobs

One-time jobs for reconciliation, user import, and bulk add operations upload the files under a common root directory specified by the property below:

```
truaccess.upload.filedir=<common root directory>
```

The system creates unique subdirectories for each job, as follows:

```
<truaccess.upload.filedir>/FileUpload_UI/<adminID>_<jobName>/  
<userimport_file>
```

```
<truaccess.upload.filedir>/FileUpload_RC/<adminID>_<jobName>/  
<reconciliation_file>
```

```
<truaccess.upload.filedir>/FileUpload_BK/<adminID>_<jobName>/  
<bulkadd_file>
```

Once the job file is moved from the upload to the staging directory, the system deletes the parent directory, so that the file is also removed (the file named `<adminID>_<jobName>/<file>`).

If you delete any of the contents of an upload directory, first ensure all outstanding jobs are finished.

## Email Sender

Specify a general email address that will be used as the sender's address for email sent by Select Identity. This address must exist on the SMTP server configured for use by the Select Identity application server.

The following property controls this setting:

```
truaccess.sender.email
```

The following example illustrates how this setting should be formatted:

```
truaccess.sender.email=si_admin@your_company.com
```

You can also specify a value for the `truaccess.sender.name` property, to coincide with this setting. This corresponds to the displayed sender name, as opposed to the originating email address, in an email message, as shown in the following example:

```
truaccess.sender.name=si_admin
```

## Attribute Maximum Length

Specify the Attribute Maximum Length default value (kilobyte). The following example illustrates how this setting should be formatted:

```
com.hp.si.user.attributes.maxlength=10
```

## Select Identity URL

Provide values for the following settings that make up the URL for accessing Select Identity. Specify the protocol, host name or IP address, and port, such as **http://localhost:7001/**.

```
truaccess.method  
truaccess.host  
truaccess.port
```

## Database Settings

Set the `truaccess.repository.type` property to the type of database server you are using:

- Possible values are `oracle` for Oracle.
- Enter the value in lowercase.
- The default setting is `oracle`.

Specify a valid location on the Select Identity server that can be used as temporary storage while Select Identity uploads files to the database. Use the following property for this setting:

```
truaccess.upload.filedir
```

## Workflow Settings

Specify the **SI Provisioning Password Change** workflow template for password reset operations. Use the following property for this setting:

```
truaccess.fixedtemplate.passwordreset=SI\ Password\ Change\  
Provisioning
```

## Helpdesk Contact Message

Provide the error message that the system displays if the user cannot log on to the Select Identity client.

```
contact_helpdesk=Please contact the helpdesk
```

## Optional Settings

Configure settings in the `TruAccess.properties` file to perform the following optional functions:

- Customize the graphical interface - see [Custom User Interface Properties](#) on page 63.
- Optimize Select Identity - see [Recommended Configuration](#) on page 59.

# Setting Up the Select Identity Security Framework

A new security framework has been introduced in Select Identity 4.10. You must set this up before you run Select Identity for the first time, so that the security framework is properly initialized in the database.



Failure to set up and initialize the security framework correctly may cause data corruption. This is a critical procedure.

## The Bootstrap Keystore

Select Identity 4.10 requires an external keystore in which to store the keys used to encrypt data in the database. Select Identity cannot initialize without this external keystore. This keystore is therefore known as the *bootstrap keystore*.

The bootstrap keystore stores the following keys:

- The database key, a secret key for encrypting data in the database.
- A second secret key that is used internally by the security framework.

## The Object Migration Keystores

The object migration feature requires the following keystores:

- The object migration keystore, which stores the signing and encryption key pairs.
- The truststore, which stores the trusted source and destination certificates for secure object migration.

## Setting Up the Bootstrap Keystore

There are two possible scenarios in which you set up the bootstrap keystore:

- You are performing a new installation, or upgrading over an existing installation that uses the internal default encryption keys.
- You are upgrading an existing installation configured to use a custom external keystore.

Determine which scenario applies to your installation and perform the procedure indicated using the instructions in this section.

### Setting Up the Bootstrap Keystore on a New Installation or an Installation With Default Keystores

This procedure varies depending on whether or not you are using HSM. Perform the procedure appropriate to your situation.

#### HSM Procedure for Bootstrap Keystore Setup

If you are using HSM, perform the following procedure to create a custom keystore:

- 1 Configure HSM, if applicable, by performing the following steps:



- a Use the HSM utilities to create two secret keys for use with the AES encryption algorithm.
  - b For both keys, use the same password as the keystore.
- 2 Create a keystore property file by performing the following steps:
- a Run the prepackaged utility `genprop.sh` (Linux/UNIX) or `genprop.bat` (Windows), using the command line examples below for reference:
    - For HSM keystores: `./genprop.sh`
    - for HSM (nCipher): `./genprop.sh ncipher nocheck`
  - b Select option 1 to create a bootstrap keystore.
  - c When prompted, enter the full path to the property file.
  - d Make a separate record of the path to the property file.
 

You must enter this path when running the Select Identity installer. If installing manually, you must enter this path as the value for the `si.keystore.paramfile` property in the `TruAccess.properties` file before you launch Select Identity for the first time.
- 3 Perform this step if you are using **nCipher HSM** for the bootstrap keystore. Skip this step if you are *not* using nCipher HSM:
- a Modify the `java.security` file, `<WAS_INSTALL_DIR>\java\jre\lib\security` by adding the following to the **Provider** list:
 

```
security.provider.2=com.ncipher.provider.km.nCipherKM
```
  - b Perform this step on every server if you are installing on a cluster.

### Non-HSM Procedure for Bootstrap Keystore Setup

If you are *not* using HSM, perform the following steps to set up the bootstrap keystore:

- 1 Create a Java keystore by performing the following steps:
- a Use the `keytool` command, as shown in the command line example below, to create a JCEKS keystore in sequence. This will serve as the bootstrap keystore.
  - b After entering the command, enter the keystore and key passwords when prompted (the keystore and both keys must all use the same password).
 

Use the command line example below when creating a keystore:

```
keytool -keystore myKeystore.jceks -genkey -alias myTempKeyAlias
-storetype JCEKS -keyalg RSA -dname
CN=ownerName,O=orgName,OU=unitName,ST=state,L=city,C=country
```

Use the command line example below when deleting a keystore:

```
keytool -keystore myKeystore.jceks -delete -alias myTempKeyAlias
-storetype JCEKS
```
- 2 Perform this step *twice* to create two secret keys in the JCEKS keystore that you created in [step 1](#), as follows:
- a Execute the packaged tool `genkey.sh` (Linux/UNIX) or `genkey.bat` (Windows) to create each key in the keystore.
  - b Enter the requested information when prompted.

- c Make sure at least one of the keys is using the keystore password. The security framework encryption key must use the keystore password.
- 3 Create a keystore property file by performing the following steps:
  - a Run the prepackaged utility `genprop.sh` (Linux/UNIX) or `genprop.bat` (Windows).
  - b Select option 1 to create a bootstrap keystore.
  - c When prompted, enter the full path to the property file.
  - d Make a separate record of the path to the property file.

You must enter this path when running the Select Identity installer. If installing manually, you must enter this path as the value for the `si.keystore.paramfile` property in the `TruAccess.properties` file before you launch Select Identity for the first time.

## Setting Up the Bootstrap Keystore on an Existing Installation With Custom External Keystores

The following procedure describes how to set up the bootstrap keystore on Select Identity versions prior to 4.10.

- 1 Create a key in the external keystore, by running the `genkey.sh` or `genkey.bat` utility.
- 2 Assign this key a key password that is identical to the keystore password. This key is used as the security framework encryption key.
- 3 Enter the following information in the old keystore property file:
 

```
si.keystore.keypass.alias=<key alias>
```
- 4 If you are using AES keys on a pre-4.10 system, ensure that the `TruAccess.properties` file contains the following setting:
 

```
si.keystore.<key alias>.keyalg = AES
```

## Creating the Object Migration KeyStore

This keystore is used to store the signing and encryption key pairs requires two certificates: encryption certificates for a server. You register this keystore using the GUI.

Select Identity requires two keypairs: one for signing and one for encryption.

- 1 Run the `keytool` utility to create a keystore and two keypairs.
- 2 Generate a certificate request file, as shown in the command line example below, which creates an X509 certificate request file at `./req/myReq.csr` for a certificate at `myKeyAlias` in the keystore:
 

```
keytool -certreq -keyalg RSA -alias myKeyAlias -file ./req/myReq.csr-keystore ./ks/myKeyStore -storetype JKS
```
- 3 You can either send the new request file to your certificate authority for digital signing, or use the following certificate signing commands to sign this certificate locally.
- 4 Import the signed certificate back to the key store from which you generated the certificate request.

You may also want to import the certificate to a trust keystore, which can be deployed to a site where the certificate is verified.

The following command imports the signed certificate file `./signed/signedCert.pem` to `ks/myKeystore` at the key alias named `myKeyAlias`.

```
keytool -import -trustcacerts -alias myKeyAlias -file ./signed/signedCert.pem -keystore ./ks/myKeystore -storetype JKS
```

- 5 Import the certificate into the truststore by performing the following steps:
  - a Execute `genprop.sh/genprop.bat` to create a property file (select option 2 when prompted).
  - b Use the Select Identity browser interface to register the property file, under **Security Setup**.

## Creating a Trust Store

Create a trust store to hold certificates to verify signatures, and to hold the destination encryption key:

- 1 Run `keytool` to create a JKS keystore.
- 2 Import the signed certificates.
- 3 Execute `genprop.sh/genprop.bat` to create a property file.
- 4 Use the Select Identity browser interface to register the property file.

## Setting TruAccess Properties for the Security Framework

After successful installation, add or modify the following entries, as appropriate, in the `TruAccess.properties` file, then restart the server or cluster to make the settings take effect.

```
si.keystore.paramfile=<location_to_bootstrap_keystore_property_file>
```

For Linux/Windows on WebSphere, add the following:

```
com.ibm.crypto.provider.IBMJCE
```

For all other configurations, add the following:

```
com.sun.crypto.provider.SunJCE
```

If using nCipher HSM, add the following to specify provider details:

```
com.hp.ovsi.encryptionkey.provider.classname=com.ncipher.provider.km.nCipherKM
```

```
com.hp.ovsi.encryptionkey.provider.position=2
```

```
com.hp.ovsi.encryptionkey.keystoretype=nCipher.sworld
```

For all configurations, add the following to specify use of the IBM Crypto Provider:

```
com.hp.ovsi.keypair.provider.classname=com.ibm.crypto.provider.IBMJCE
```

## Recommended Configuration

Before you start using Select Identity, it is strongly recommended that you customize it for optimal performance. You may also want to customize the graphical interface to reflect your company information, as well as changing some of the interface default settings.

The following general settings are recommended:

- When creating the Oracle database connection, always enter the user name in uppercase. This prevents logging errors associated with converting the name to uppercase.
- Set the maximum JVM heap size as **1024** Megabytes or higher.
- Set logging level to `WARNING`. See [Configuring Logging for Select Identity](#) on page 50 for more information.



The above parameter values are recommendations and may vary for individual systems. Examine your specific environment and tune settings that affect the application server or database when running Select Identity.

## Extending User Searches

User accounts can consist of a large number of attributes. Typically, user search criteria contain key attributes, such as the last name, email, or user name.

Several user profile attributes can be added to the `TruAccess.properties` file and used to extend the range of possible search requests.

If you specify user search attributes in the `TruAccess.properties` file, you must also extend the **TAUser** database table by adding extra columns. The added columns must be named so that they map to the selected attributes.

### How to Specify Extended User Search Attributes

To specify extended search attributes, you perform the following tasks:

- Identify the attributes you want to use, for example job title or employee ID.
- Ensure the selected attributes are defined in Select Identity and in the attribute mapping file used for each system resource where data is stored.
- Add corresponding columns to the **TAUser** table in the Select Identity database.
- Add corresponding entries to the `TruAccess.properties` file.
- Recreate all Select Identity database views to refresh them and propagate the changes (this is an essential step).

The following procedure describes how to set extended user search attributes by configuring the `TruAccess.properties` file and adding columns to the **TAUser** table:

- 1 Add the following settings to the `TruAccess.properties` file:

- `truaccess.user.extra=Addr1, PhBus`

This property lists the Select Identity attributes to be added, separated by commas.

- `truaccess.user.extra.Addr1.column=Address1`
- `truaccess.user.extra.PhBus.column=Phone`

The `truaccess.user.extra` property maps the name of an attribute to its corresponding column name in the **TAUser** table. Include one instance of this property for each column you are adding to the **TAUser** table.

The format for the `truaccess.user.extra` property is as follows:

```
truaccess.user.extra.<Attr>.column=<TAUser Column Name>
```

- The **TAUser** column names cannot contain spaces, but the Select Identity attribute names can. This is so that escape sequence can be used when updating the `TruAccess.properties`.

For example, if the Select Identity attribute `Home Phone` is mapped to the **TAUser** table column labeled **Phone**, the `TruAccess.properties` for this mapping can be formatted as follows:

```
truaccess.user.extra=Addr1,Home\ Phone
truaccess.user.extra.Addr1.column=Address1
truaccess.user.extra.Home\ Phone.column=PhoneMiscellaneous
Settings
```

To configure the **TAUser** table with extra columns for the extended search attributes and then refresh the views in the Select Identity database, perform the following steps:

- 1 Use the following SQL scripts to add a column to the **TAUser** table for each extended search attribute that you added to the `TruAccess.properties` file:

```
ALTER TABLE TAUser ADD Address1 VARCHAR(128) NULL
ALTER TABLE TAUser ADD Phone VARCHAR(30) NULL
```

- 2 Locate the Select Identity database script named `oracle_concero_ddl.sql`.

This is the script that installs the Select Identity database, as documented in in [Chapter 3, Database Server Configuration](#). You can copy it from the product CD.

- 3 Open the `oracle_concero_ddl.sql` script using the database tool or text editor of your choice.
- 4 Locate and copy every `CREATE VIEW` statement to another, empty, file.
- 5 Replace every instance of `CREATE VIEW` with `CREATE OR REPLACE VIEW`, and save the resultant script in a new file.
- 6 Run the new script against the Select Identity database to refresh the views.

## Adding Display Columns for Extended Attributes

This procedure enables the extra **TAUser** table columns to be updated when a user is added or modified.

The extra columns can also be used as the **Search** column. For example, to add **PhBus** as the search and display column, perform the following steps:

- 1 Add the following setting to the `TruAccess.properties` file:

- User Search Criteria Names, comma separated (use `_Status` for **User State Status**):

```
#com.hp.si.usersearch.criteria.names.default =
UserName,Email,FirstName,LastName,_Status,UserType
```

```
com.hp.si.usersearch.criteria.names.default =
UserName,Email,FirstName,LastName,_Status,UserType,PhBus
```

- User Search Column Return Names, comma separated, `UserName` required:

```
#com.hp.si.usersearch.result.columns =
UserName,FirstName,LastName,Email,UserType
```

```
com.hp.si.usersearch.result.columns =
UserName,FirstName,LastName,Email,UserType,PhBus
```

## Disabling the Extended Search Features

To disable the extended search feature, perform the following steps:

- 1 Remove the properties containing extended search attributes from the `TruAccess.properties` file.

- 2 Use the following SQL scripts to remove the **TAUser** table columns:

```
ALTER TABLE TAUser DROP COLUMN Phone
```

```
ALTER TABLE TAUser DROP COLUMN Address1
```

- 3 Refresh the views as documented on [page 61](#).

# Custom User Interface Properties

Minimal customization to the user interface can be performed by setting certain properties in the `TruAccess.Properties` file.

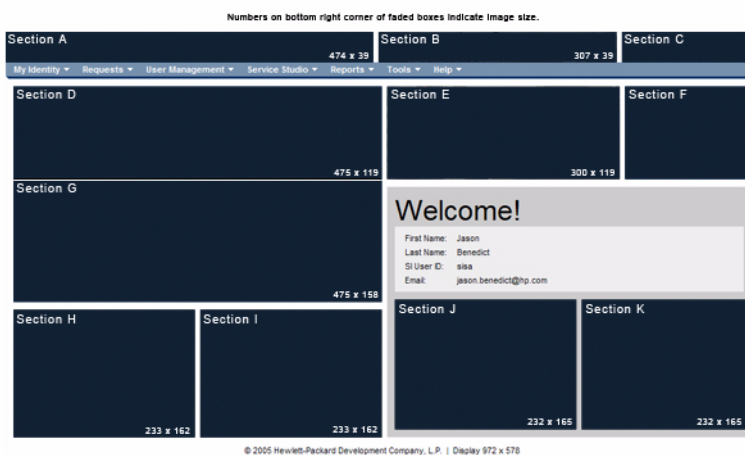
These user interface properties are not required, but they must be present in the `TruAccess.Properties` file and set to the default, if they are not customized.

This section lists these properties and explains their use and possible range of values for each.

## User Interface Sections

The user interface is divided into sections, which are identified in [Figure 17](#). The descriptions of the properties that follow use this diagram for reference.

**Figure 17 User Interface Sections**



## Customization Properties

The customization properties are listed in this section. All properties that specify colors use a three-digit or six-digit hexadecimal code for the RGB value of the desired color. The value range is from 000000 (black) to FFFFFFFF (white).

`com.hp.ovsi.ui.masthead.fgcolor`

This property sets the main foreground color of the masthead, also known as font color. This affects only the username, home, and logout links located in the masthead (Section C).

`com.hp.ovsi.ui.masthead.bgcolor`

This property sets the main background color of the masthead. This does not affect the white backgrounds on either side of the masthead common image in Section B (Sections A and C).

[com.hp.ovsi.ui.logo.image.src](#)

This property sets the URL of the image file for the main logo in Section A. The maximum image size is 474 x 39 pixels, rendered as a background in the table cell. The style on the table cell background is set to no-repeat and the table cell is resized when the browser is resized. If the table cell becomes wider than the image, the background color fills the extended space.

[com.hp.ovsi.ui.common.header.image.src](#)

This property sets the URL of the image file for the center image in Section B. The size of the image is 307 x 39 pixels. This image will expand or contract to the set size. The table cell that contains this image does not resize.

[com.hp.ovsi.ui.landing.named.image.src](#)

This property sets the URL of the image file in Section G. The maximum size of the image is 475 x 119 pixels. The table cell is resized when the browser is resized. If the table cell becomes wider than the image, the background color fills the extended space.

[com.hp.ovsi.ui.landing.named-top.image.src](#)

This property sets the image in Section D. The maximum size of the image is 475 x 158 pixels. The table cell is resized when the browser is resized. In the event that the table cell becomes wider than the image, the background color fills the extended space.

[com.hp.ovsi.ui.landing.named.image.style](#)

This property sets the table cell CSS style for Section G. Use this style to manipulate the positioning of the image set in Section G. The background color can also be set using this style property.

[com.hp.ovsi.ui.landing.named-top.image.style](#)

This property will set the table cell CSS style for Section D. Use this style to manipulate the placement of the image set in Section D. The background color can also be set using this style property.

[com.hp.ovsi.ui.landing.common.image.src](#)

This property sets the center image in Section E. The set size of the image is 300 x 119 pixels. This image will expand or contract to the set size. The table cell this image is in does not resize.

[com.hp.ovsi.ui.landing.box.right.bgcolor](#)

This property will set the background color of Section F.

[com.hp.ovsi.ui.landing.users.image.src](#)

This property sets the image in Section H that is shown when User Administration permissions are not granted. The size of the image is 233 x 162 pixels. The table cell this image is in does not resize. This image will be a background in the table cell. The style on the table cell background is set to repeat.



[com.hp.ovsi.ui.landing.requests.image.src](#)

This property sets the image in Section I that is shown when Approval Administration permissions are not granted. The size of the image is 233 x 162 pixels. The table cell this image is in does not resize. This image will be a background in the table cell. The style on the table cell background is set to repeat.

[com.hp.ovsi.ui.landing.selfservice.image.src](#)

This property sets the image in Section J that is shown when Self Service Administration permissions are not granted. The size of the image is 232 x 165 pixels. The table cell this image is in does not resize. This image will be a background in the table cell. The style on the table cell background is set to repeat.

[com.hp.ovsi.ui.landing.servicestudio.image.src](#)

This property sets the image in Section K that is shown when Service Studio Administration permissions are not granted. The size of the image is 232 x 165 pixels. The table cell this image is in does not resize. This image will be a background in the table cell. The style on the table cell background is set to repeat.

## Default Values for User Interface Properties

Default values for these properties are as set below.

```
com.hp.ovsi.ui.masthead.fgcolor=#FFF
```

```
com.hp.ovsi.ui.masthead.bgcolor=#036
```

```
com.hp.ovsi.ui.logo.image.src=/images/themes/blue/  
logo_hp_smallmasthead.gif
```

```
com.hp.ovsi.ui.common.header.image.src=/images/masthead_photo_small.jpg
```

```
com.hp.ovsi.ui.landing.named.image.src=/images/selectidentity.gif
```

```
com.hp.ovsi.ui.landing.named-top.image.src=/images/space.gif
```

```
com.hp.ovsi.ui.landing.named.image.style=padding: 20px 10px 98px 10px;  
background-color: #036
```

```
com.hp.ovsi.ui.landing.named-top.image.style=padding: 20px 10px 98px  
10px; background-color: #036
```

```
com.hp.ovsi.ui.landing.common.image.src=/images/landing-photo-misc.jpg
```

```
com.hp.ovsi.ui.landing.box.right.bgcolor=#036
```

```
com.hp.ovsi.ui.landing.users.image.src=/images/landing-photo-user.jpg
```

```
com.hp.ovsi.ui.landing.requests.image.src=/images/  
landing-photo-approval.jpg
```

```
com.hp.ovsi.ui.landing.selfservice.image.src=/images/  
landing-photo-selfserv.jpg
```

```
com.hp.ovsi.ui.landing.servicestudio.image.src=/images/  
landing-photo-shortcuts.jpg
```

## Internationalization and Localization

Select Identity is internationalized and is able to operate with languages that are supported by the Java Unicode specification. Internationalization support in Select Identity includes the following capabilities:

- The user can enter the local language characters as input data. The display text provided by Select Identity, such as labels, help text, and other static display strings are shown in English or in the languages supported on the localized HP OpenView Select Identity product CD.

XML files used for Select Identity Web services, user import, and rules can take foreign characters as tag or attribute values. The exported XML files through Configuration pages allow foreign characters as well. You can enter foreign characters directly into the XML files as long as they are entered in an editor with UTF-8 encoding enabled. In general, any UTF-8 supported editors can be used for this purpose. However, some editors could store additional hidden characters while saving the file. To ensure that the XML files containing foreign characters are stored correctly, Select Identity recommends using XML editors such as XMLSpy.

- The date and time are displayed in the local format.
- Linguistic sorting is not supported.

Internationalization is supported for Select Identity on the following platforms:

- Application server – WebSphere 6.0.2
- Database – Oracle 10G
- Connectors – LDAP/UTF-8



Make sure that your database supports the language characters that you want to use.

### Localizing the Date and Time Format

In Select Identity Version 4.10, using Internet Explorer's **Internet Options** to set language preference affects the text and format of dates. In previous versions, specifying language preference affected the field names and messages in the system, but did not affect the date. The underlying date format is not changed, so each user sees the date in their preferred format.

#### Functional Overview

Select Identity 4.10 provides calendar text for 27 languages. Field names and messages are also available for languages such as Korean and Chinese.

The time format set by the system administrator applies to all users on the server. Individual Internet Options language settings may override the default text display.

The calendar wizard in Version 4.10 uses a clickable calendar for selecting dates, as did previous versions of Select Identity. However, in Version 4.10, the calendar text uses the language that you select in **Internet Options**. Thus, if your preferred language is Japanese, the calendar text displays in Japanese.

The default language setting is U.S. English. If the character set for a given language selection is not available, the system substitutes U.S. English.

## Custom Date and Time Formats

The system administrator can override the default date and time formats by specifying custom formats in the `TruAccess.properties` file. This does not change the language displayed. Only the date and time formats used by the current language are affected.

Administrators can also select either twelve- or twenty-four hour clock for time display and entry.

## Setting the Calendar Language

- 1 In Internet Explorer, open the **Tools** menu and select **Internet Options**.
- 2 Click the **General** tab.
- 3 Open the **Languages** preference page by clicking **Languages**.
- 4 Click **Add** to open the **Add Languages** page.
- 5 Select the language(s) you prefer and click **OK** to open the **Language Preferences** page with the selected languages listed.
- 6 Arrange the list in order of preference. The language at the top of the list is used first. If there is no matching character set, the system substitutes the next language in the list, and so on.
- 7 Click **OK** to close the **Language Preferences** page, and again to close the **Internet Options** page.



This setting affects all pages displayed in Internet Explorer, not just Select Identity.

## Setting the Time and Date Default Format in the `TruAccess.properties` File

The system administrator can configure the default format of times and dates within Select Identity. The `TruAccess.properties` file establishes several settings to enable date and time display:

- `ui.locale.date.format=MM/dd/yyyy` for date-only fields, such as dates selected from a calendar.
- `ui.locale.datetime.format=MM/dd/yyyy hh.mm aa` for date- and time-only fields, such as the status time for jobs submitted through reconciliation.
- `ui.locale.time.format=hh.mm aa` for time only fields, such as list boxes with hours and minutes for scheduling a batch job through reconciliation or bulk add.

To display 24 hour times in place of 12 hour times, modify the time patterns in the following ways

- Replace `hh` with `HH` in the pattern.
- Drop `aa` from the pattern.

For example, this will display 13:00 instead of 1:00 PM.



All three settings must be updated to reflect your users' preferences. The syntax must follow the guidelines for Java Class SimpleDateFormat.

Refer to [Appendix A, TruAccess Properties](#) for more information.

## Configuration for Specific Environments or Platforms

The following sections provide platform and environment-specific configurations.

- [Tuning the Database Server](#)
- [UTF-8 Encoding on Oracle 10G](#)
- [iPlanet LDAP Configuration](#)
- [Set Encoding in Internet Explorer](#)
- [Adding Supported Language Fonts](#)

### Tuning the Database Server

The maximum capacity of the JDBC connection pool for each Select Identity node should be set to at least 100.

When Select Identity deployment descriptors are modified to increase the pools of any Select Identity MDB, the JDBC pool should be increased accordingly.

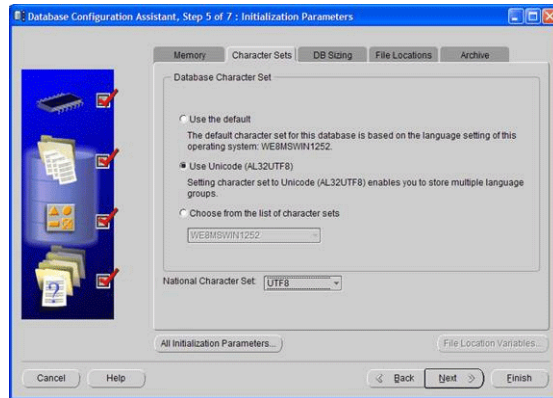
Some servers, such as Oracle, have the parameters controlling the maximum number of concurrent sessions that can be established at the same time from any client application.

Increasing the number of nodes in the cluster also increases the number of concurrent sessions from Select Identity instances to the database server. The limit of concurrent sessions in the database server should be increased accordingly.

### UTF-8 Encoding on Oracle 10G

Perform the following to set UTF-8 encoding for Oracle at database creation:

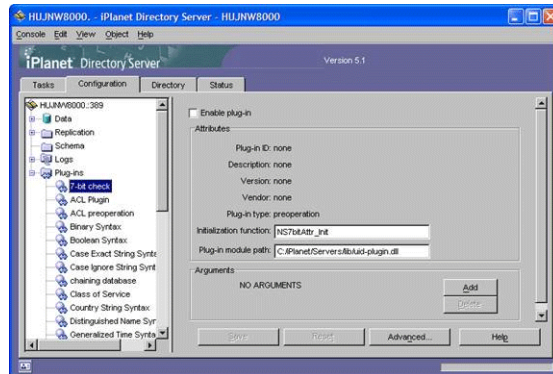
- 1 For Oracle 10g, open the Initialization Parameters window and select the **Character Set** tab.
- 2 Select the **Use Unicode (AL32UTF8)** radio button as shown.



## iPlanet LDAP Configuration

Perform the following to disable 7-bit ASCII:

- 1 In iPlanet's Configuration window, expand the plug-ins node and select the **7-bit** check box.
- 2 Deselect **Enable plug-in**, which is selected by default.



## Set Encoding in Internet Explorer

Perform the following procedure to set encoding in Internet Explorer to UTF-8 and define a language:

- 1 From the main menu, select **View** → **Encoding** → **UTF-8**.
- 2 Select **Tools** → **Internet Options**.
- 3 Click the **Languages** button.
- 4 Click **Add**.
- 5 Select the desired locale from the Language list and click **OK**.
- 6 Select the language and move it to the top of the list.

## Adding Supported Language Fonts

The JDK font properties file ships with most languages. Perform the following to add language fonts that do not exist in the file:

In `<JAVA_HOME>/jre/lib/font.properties`, add font entries for supported languages.

For example, to add Chinese GB2312 for normal and bold face fonts, add the following lines near font definition lines with similar names:

```
dialog.3=\u5b8b\u4f53,GB2312_CHARSET
dialog.bold.3=\u5b8b\u4f53,GB2312_CHARSET
```

## Additional Configuration Options

You can perform the following configuration to customize the behavior of Select Identity:

- HP OpenView Select Identity login page — You can specify whether or not this page displays.

The following default setting indicates that the login page will display.

```
truaccess.authentication=on
truaccess.sso.token.name=ct_remote_user
truaccess.loginURL=https://localhost:port/lmz/signin.do
truaccess.logoutPage=https://localhost:port/lmz/logout.do
```

If `truaccess.authentication=on` then the three settings that follow are ignored.

If `truaccess.authentication=off` then the three settings that follow are used for logging in to specify the single sign-on token name, the login URL and the logout URL for cleaning up the session.

- Self-Registration
  - Change the default text that appears on the HP OpenView Select Identity Home page by setting the following property:

```
com.hp.si.selfreg.instruct = Welcome and thank you for accessing
Self-Registration. After completing this page, press '{0}'. You will
then be asked for additional information. Once you have completed all
pages, your request will be submitted for processing.
```

- Schedule field visibility in the Self-Registration form — You can specify whether or not the **Time** field is displayed. The default is displayed. A false setting hides the field.

```
com.hp.si.selfreg.schedule = true
```

- Specify the first page that displays when Self-Registration is opened — You can specify that the first page will be the defined Service View name (`selfregview`) with pre-defined attributes and context. If this setting is not defined, the first page that displays is the Service View defined for the Service Role.

```
com.hp.ovsi.commonattributesview.name=selfregview
```

- Emailed report format — You can specify which columns display and in which order, in the User Configuration Detail Report that is emailed. The default is all columns separated by commas.

```
truaccess.userdetailconfigrpt.sortattributes=UserName,
FirstName,LastName,Email,Company,Department,CostCenter
```

- **Support contact** — You can set your own company support contact information. The default is the Select Identity contact number.

```
contact_helpdesk=Please contact the helpdesk
```

- You can set the following user search criteria:

- **User name fields in the User Search Information dialog** — You can specify how many fields are displayed. The default is all fields separated by commas. Note that the status field must be entered as `_Status`.


```
com.hp.si.usersearch.criteria.names.default =
UserName,Email,FirstName,LastName,_Status
```

- **Columns in the User Search Results page** — You can specify which columns will be displayed and in which order in the User Search Results page. `UserName` is required.

```
com.hp.si.usersearch.result.columns =
UserName,FirstName,LastName,Email
```

- **Maximum number of user records in the User Search Results page** — You can specify the maximum number of records that can be returned in a user search. The default is 300.

```
com.hp.si.usersearch.result.max = 300
```

- **Search criteria drop-down list** — You can specify the maximum number of items that can be in a drop-down list. If the number is exceeded, then the drop-down list is replaced with the search icon. 

- Click this icon to view the **Search Information** page where you can filter the search to select an item, or click **Submit** to select from all available items. The default is 50.

```
com.hp.si.user.attributes.dropdown.constraint.count=50s
```





# 6 Upgrading Select Identity

This chapter describes how to upgrade an existing Select Identity system. Read these instructions carefully *before* attempting to upgrade.

This section covers the following topics:

- [Supported Platforms for Upgrading](#)
- [Upgrade Requirements](#)
- [Preparing to Upgrade](#)
- [Database Upgrade Procedure](#)

## Supported Platforms for Upgrading

The Select Identity upgrade script supports upgrading from 4.0 or 4.01 on any Web application server, with an Oracle 10g database, to Select Identity version 4.10 on the WebSphere 6.0.2 Web application server.

### Upgrading on Unsupported Platforms

If you are upgrading in any of the following circumstances, contact Hewlett-Packard Technical Support for individual assistance:

- Upgrading from Select Identity versions prior to 4.0



Select Identity versions 4.0 and 4.01 both include scripts for upgrading from earlier versions on certain platforms.

## Upgrade Requirements

Your Web application server and Select Identity must meet the following requirements to be suitable for upgrading to Select Identity Version 4.10 using this procedure:

- Select Identity version 4.0 or 4.01
- Unix-based operating system platform
- Oracle Client version 10g installed, with SQLplus in the system path
- Oracle 10.1.0.4 or later



Ensure that your Web application server and database server meet the minimum requirements specified in [Chapter 2, Requirements](#).

# Preparing to Upgrade

The procedures in this section prepare the Web application server and Select Identity database for upgrading to version 4.10. Follow the instructions corresponding to your system environment.

## Downloading the Oracle JDBC Driver

If you are running a version of Oracle earlier than 10.1.0.4, you must download and install the Oracle JDBC driver before you can run the upgrade script. In Oracle 10.1.0.4 installations, the appropriate version of the JDBC driver file `ojdbc14.jar` is located in the Oracle home directory under `jdbc\lib`.



This procedure directs you to the Oracle Web site. Oracle may change the layout of the site at any time, without notice. In addition, you must register as a member of the Oracle Technology Network. There is no charge for membership.

- 1 Open a browser window and navigate to **www.oracle.com**.
- 2 Follow the link to **Technology Network** at the top of the page.
- 3 Under the **Technologies, Utilities and Drivers** section, follow the link to **Oracle JDBC Drivers**.
- 4 Follow the link to **Oracle Database 10G (10.1.0.4)(10.1.0.2) drivers**.
- 5 Agree to the license terms and export restrictions.
- 6 Click the filename `ojdbc14.jar` under the heading **Oracle Database 10g 10.1.0.4 JDBC Drivers**.
- 7 When prompted, log in to an existing Oracle Technology Network account, or create an account and then log in.
- 8 After you log in, the driver is downloaded to the file system location of your choice.

## Stopping Select Identity Traffic

Perform the following procedure to stop all Select Identity traffic on your Web application server:

- 1 Ensure that no other users are connected to the Web application server or to Select Identity. No requests should be initiated until the upgrade is complete.
- 2 Access the Select Identity 4.0x client.
- 3 On the login page, verify the installed Select Identity version by checking the version number located under the login fields, at the bottom of the page.



Do not proceed if Select Identity is earlier than version 4.0x.

- 4 Log in to the Select Identity 4.0x client.
- 5 Approve any “pending” workflow tasks.
- 6 Verify that any pending or in-process requests or reconciliations are complete by viewing the status reports.
- 7 Log out of Select Identity.

## General Web Server Preparation

Perform the following tasks regardless of the Web application server on which you are upgrading Select Identity:

- 1 Log in to the Web application server administrative or management console.
- 2 Navigate to the deployed Select Identity `lmz.ear` application and undeploy it.
- 3 Shut down the Web application server process and any managed servers/node processes.
- 4 Log in to the Administrative server at the command line, using an appropriate user ID.
- 5 Back up the existing 4.0x Select Identity directories and files.
- 6 Back up the existing `TruAccess.properties` file in an accessible location. You may need to refer to it when configuring the `TruAccess.Properties` file after upgrading.
- 7 Uninstall the old version of Select Identity (4.0x) using the manual uninstallation instructions provided with that version.

## Database Upgrade Procedure

The upgrade script, `migrator.sh` calls another script, `setUserEnv.sh`, that contains several environment variables. Modify the values assigned to these variables, if desired, to enable the script to run automatically without prompting you to enter the information needed to target the upgrade process. If you choose not to set these variables within the subscript, the upgrade script prompts you to enter the information each time.

Running the upgrade script from start to finish takes a variable amount of time depending on the size of the Select Identity database and the performance of your database and Web application servers. It is not unusual for the complete process to take more than an hour.

Perform the following steps to upgrade Select Identity from version 4.0 or 4.01 to 4.10.

- 1 Unzip the upgrade files.
- 2 Copy `ojdbc14.jar` to the `lib` directory under the `Migrator` directory. or edit the `JDBC_CLASSPATH` in the file named `oracle_run_migrate.sh` so that the path points to the location of `ojdbc14.jar`.
- 3 Locate the file named `setUserEnv.sh` and edit the following environment variables:
  - `TRUACCESS_HOME`: The location of the `TruAccess.properties` file in your existing 4.0.x Select Identity installation. It is critical that this be set correctly.
  - `DB_VENDOR`: The manufacturer of your database, such as Oracle, all in lowercase characters. Currently only Oracle is supported.
  - `J2EE_JARS`: The path to the `ojdbc14.jar` file. It is critical that this be set correctly.
  - `DB_USER`: The user name for connecting to the Oracle database and accessing the Select Identity schema, typically the same user name that was entered for the database connection when installing the old version of Select Identity.
  - `DB_PASS`: The password for the above user account.
  - `ORASERVER`: The IP address or domain name of the Oracle database server.
  - `ORAPORT`: The database port on which the Oracle database listens for connections, usually 1521.

- `ORACLE_SID`: The connection identifier (from the `tnsnames.ora` file) for the database server where the Select Identity database is running. This is only used by SQLPlus, not by Java.
- 4 Edit the entry named `java.util.logging.FileHandler.pattern` in the `Logging.properties` file, so that it points to a valid directory entry where the Java log files will be written.

A sample `Logging.properties` file is provided in the `\samples` directory. Copy this file into the same directory as `migrator.sh` so that it logs the behavior of the script. Failure to perform this step correctly may result in missing on-screen status and log message display during parts of the upgrade process.

- 5 Change directories to the main directory for the upgrade files.
- 6 Execute the following command:

```
./migrator.sh
```

The `migrator.sh` script has the following command line options:

- `-j`: Run a single step. For example, `migrate.sh -j 6` runs Step 6 and then stops.
- `-r`: Resume execution at the specified step. For example, `migrator.sh -r 12` resumes the upgrade by running step 12 and then continuing to the end of the process.

## Required Libraries and Files

The following libraries and files are required to complete the upgrade after running the database upgrade script:

- Database JDBC `.jar` files
- `TruAccess.properties` file from the old Select Identity installation

## Troubleshooting a Database Upgrade

Refer to the readme or any release notes supplied with Select Identity, particularly those that accompany the upgrade files, for information about known problems as of the time of release.

If you encounter a problem running the upgrade script, the following steps may assist in tracing it and completing the upgrade successfully:

- 1 The `migrator.sh` script runs each step in numerical order. If a failure occurs during any step, the failure is logged and the script stops. Review the entries in the `migrationlog` table under the Select Identity schema.
- 2 Log on to SQLplus as the Select Identity owner and run the `oracle_migration_report.sql` script. This shows the status of each step.
- 3 If the failure occurs during one of the Java upgrade steps, review the screen output or log files in the directory specified by the `java.util.logging.FileHandler.pattern` entry in the `logging.properties` file.
- 4 After resolving the problem, resume the script from the last completed step using the `-r` option.

# WebSphere Server Upgrade Procedure

You must perform several tasks to upgrade Select Identity on a WebSphere 6.0.2 server, in addition to the [Database Upgrade Procedure](#) on page 75:

- 1 Create an Oracle user ID for use by the JMS datastore. Refer to [Configuring an Oracle Database Server](#) on page 23 for instructions. You do not need to create a new database when upgrading; only the additional user account is needed.
- 2 Create or configure the Select Identity bootstrap keystore.

You must use a custom keystore; you cannot use the default keystore. If the old environment does *not* have a custom keystore, you must create one for database encryption *before* running the upgraded Select Identity system.

If the old environment already has a custom keystore, you can modify the existing keystore to be compatible with Select Identity 4.10.

Create the keystore with a keypair. Refer to [Setting Up the Select Identity Security Framework](#) on page 56, for instructions.
- 3 Install the new release of Select Identity (4.10) using the instructions in the Select Identity installation procedure for your Web application server. It is recommended that you use the installer procedure.
- 4 Add any custom settings that were in the old `TruAccess.properties` file to the new `TruAccess.properties` file.
- 5 Import Select Identity 4.10 configuration files, as follows:
  - a Log in to the Select Identity client.
  - b Open the **Tools** menu, select **Import / Export Configurations**, and then select **Import Configuration**.
  - c On the **Import Configuration** page, select **Workflow Application Definition** from the **Configuration Type** list box.
  - d Tab to the **File Name** field and browse for the `Workflow Application Definition.xml` file, which is located in the `\Migration` folder on the HP OpenView Select Identity Product CD.
  - e Click **Import Configuration** to import the selected file.
  - f Select the **Request Instance Report** configuration type and import the `Request Instance Report.xml` file located in the `\Migration` folder on the HP OpenView Select Identity Product CD.
  - g Click **Import Configuration** to import the selected file.
- 6 Verify that the resource passwords are still synchronized.

<b>If the Resource Passwords</b>	<b>Then</b>
Are still synchronized	Continue.
Are not synchronized	Follow the steps in <a href="#">Synchronizing Resources</a> on page 78.

- 7 Restart the Web application server. If you are upgrading on a cluster, restart each of the managed servers to ensure that the changes are propagated across the entire cluster.

## Synchronizing Resources

Perform the following procedure if you upgrade Select Identity and resource passwords need to be synchronized so that all resources can be accessed:

- 1 Open the Select Identity client.
- 2 Select **Service Studio** → **Resources** to open the **Resource List** page.
- 3 Select the first resource in the list.
- 4 Click **Modify** to open the **Modify Resource** page.
- 5 Click **Apply** to resynchronize the resource.
- 6 Click **OK** to save your work and return to the **Resource List** page.
- 7 Repeat the process until all resources have been resynchronized.
- 8 Restart the Web application server. If you are upgrading on a cluster, restart each of the managed servers to ensure that the changes are propagated across the entire cluster.

# 7 Integrating Select Identity With Other OpenView Applications

This chapter describes integration and interoperability support between Select Identity and other OpenView applications, namely Service Desk and Select Audit as of Release 4.10.

Select Identity can be configured alongside Service Desk and Select Audit so that each product is enhanced by exchanging data with the other. This chapter explains how to set up integration in Select Identity and discusses what to expect when integration is functioning.

- ▶ Detailed configuration steps for Service Desk are not included in this section. A general summary of the steps is provided. Refer to the Service Desk documentation as necessary.

This chapter covers the following topics:

- [Select Identity–Service Desk Integration](#)
- [Select Identity-Select Audit Integration](#)

## Select Identity–Service Desk Integration

This section provides information about how to integrate Select Identity 4.10 with Service Desk 4.5, service pack 13.

Integration of Select Identity password management with Service Desk enables Service Call tickets in Service Desk to be automatically updated by Select Identity. This provides tracking of issues and enforcement of Service Level Agreements (SLAs) in Service Desk.

If the two applications are not integrated, a **Password Management** Service Call opened in Service Desk must be handled by manually activating the password management process using Select Identity. Select Identity password management is not controlled by Service Desk for enforcing Service Level Agreements (SLAs).

- ▶ Hewlett-Packard recommends that in a non-cluster environment, Select Identity be installed on its own server for best performance and compliance. Therefore, Hewlett-Packard does not test the coexistence of Select Identity with other HP products, such as Service Desk, when running on the same server.

### Required Files

A file named `ovsd_web_api.jar` is included on the HP OpenView Select Identity product CD, and must be in the Select Identity class path for the integration to work.

## External Call from Select Identity to Service Desk

When opening and updating Service Calls in Service Desk, Select Identity uses an external call to connect to the Service Desk server and invoke the Web API. Parameters required for communication with Service Desk are configured when setting up the Service Desk external call (**SDIntegrator**) in Select Identity.

## Workflow Template for Integrated Password Management

Service Desk Integration includes a special-purpose Workflow Studio default template, Password Management With OVSD. This template is documented in *Select Identity Workflow Studio Online help*. This uses the Service Desk external call to communicate with Service Desk throughout workflow execution. Fields to be updated in the Service Call are determined by the workflow variables set for the workflow activity to update them.

## Functional Scenarios

This section provides use-case scenarios for Select Identity-Service Desk integration. In essence, password management requests can be initiated either from Select Identity or Service Desk.

The password management functions are listed below for reference:

- **Change password:** The user changes his/her password.
- **Reset password:** An administrator performs a delegated password change on the user's behalf.
- **Forget password:** Either the system resets the password with an auto-generated password, or the user is able to enter a new password. This depends on the value assigned to the TruAccess property named `com.hp.ovsi.forgetpassword.autogenerate` (if set to `true`, the system auto-generates the password).

## Password Management Request from Select Identity Triggers New Service Call in Service Desk

When a Select Identity end user or administrator submits a password management request (reset or change password, or retrieve forgotten password), this automatically opens a new Service Call in Service Desk, and updates the Service Desk workflow in Select Identity throughout the request process. By default, the Service Call is updated with **Closed** status at the end of the workflow. This can be set to a different status value by configuring the appropriate workflow variable.

## Service Call and Workflow Data Exchange and Interaction

When a Service Desk Customer Service Representative (CSR) opens or updates a new Service Call for password management, the Select Identity **Password Management** page opens and the CSR performs the request directly in Select Identity. Service Call status is updated at various stages of the Service Desk workflow in Select Identity. The Service Call is updated with **Closed** status at the end of the workflow. This can be set to a different status value by configuring the appropriate workflow variable.



## Accessing the Select Identity Request Status Page from Service Desk

A Service Desk CSR can access the **Request Status** page in Select Identity, to check the status of the request corresponding to a Service Call for password resets.

## Configuration Tasks in Service Desk

Perform the following configuration tasks in Service Desk:

- **Task 1:** Activate custom fields on the Service Call form.
- **Task 2:** Modify the **Service Call Category** and **Service Call Status** fields.
- **Task 3:** Create a service call template, or update an existing template.
- **Task 4:** Edit the default form to display the custom fields added in **Task 1**.
- **Task 5:** Create two database rules.
- **Task 6:** Create one smart action.
- **Task 7:** Set the service pages to use the template that you created or updated in **Task 3**.

### Task 1: Activating Custom Fields

Configure the following custom Service Desk fields for integrated operations with Select Identity:

- **Request ID** contains the Select Identity request ID, which is used to view request status.
- **Request Failure Description** provides information in case of failure.
- **Request Link** contains a direct link to the request in Select Identity.
- **Request Type** indicates whether the request is self-service or delegated.

Service Desk provides predefined custom fields that can be directly activated. For integration with Select Identity, two of these custom fields can be activated and renamed. Customize these fields in the Administrator Console, via the **Custom Fields** feature.



You must use the custom field names specified in the field customization procedures, because these names are coded into the integration software.

### Customizing a Number Field for the Request ID

To activate a custom service call number field for the request ID, perform the following steps:

- 1 In the left panel, navigate to **Data** and select **Custom Fields**.
- 2 In the right panel, double-click **Service Call** and select **Sc. Number 10** from the **Field** menu.
- 3 Change the field name to **Request ID**.
- 4 Select **1234567** as the **Display Format**.
- 5 Check the **Activate** box.
- 6 Click the radio button labeled **All Categories**.
- 7 Click **OK**.

### Customizing a String Field for Request Failure Information

To activate a custom service call string field for request failure information, perform the following steps:

- 1 In the left panel, navigate to **Data** and select **Custom Fields**.
- 2 In the right panel, double-click **Service Call** and select **Sc. Text 1** from the **Field** menu.
- 3 Change the field name to **Request Failure Description**.
- 4 Check the **Activate** box.
- 5 Click the radio button labeled **All Categories**.
- 6 Click **OK**.

### Activating a String Field for the Request Link

To activate a custom service call string field for the request link, perform the following steps:

- 1 In the left panel, navigate to **Data** and select **Custom Fields**.
- 2 In the right panel, double-click **Service Call** and select **Sc. Text 2** from the **Field** menu.
- 3 Change the field name to **Request Link**.
- 4 Check the **Activate** box.
- 5 Click the radio button labeled **All Categories**.

### Customizing a Short String Field for the Request Type

To activate a custom service call short string field for the request type, perform the following steps:

- 1 In the left panel, navigate to **Data** and select **Custom Fields**.
- 2 In the right panel, double-click **Service Call** and select **Ser. ShortText 1** from the **Field** menu.
- 3 Change the field name to **Request Type**.
- 4 Check the **Activate** box.
- 5 Click the radio button labeled **All Categories**.

## Task 2: Modifying the Service Call Category and Service Call Status Fields

Modify the **Service Call Category** field by adding categories for the user to select. You must name the added categories exactly as follows:

- **Forget Password**
- **Change/Reset Password**

- 1 In the left panel, navigate to **Data** → **Codes** → **Service Call** → **Service Call Category**.
- 2 Right-click and select **New Service Call Category**.
- 3 Enter **Forget Password** in the **Text** field.
- 4 If the **Parent** field contains any value, clear it by selecting the empty line from the list box.
- 5 Save and Close.
- 6 Repeat [step 1](#) through [step 5](#) to create another category named **Change/Reset Password**.

Modify the **Service Call Status** field by performing the following steps:

- 1 In the left panel, navigate to **Data** → **Codes** → **Service Call** → **Service Call Status**.

- 2 In the right panel, right-click and select **New Service Call Status**.
- 3 Enter **Failed** in the **Text** field.
- 4 Select **Accountable** for the **State** field.
- 5 Repeat [step 1](#) through [step 4](#) to create additional **Status** values if desired.

If you create different status values than those documented here, set the corresponding value in the OVSI Password Integration with OVSD template in Workflow Studio. Refer to the *Select Identity Online help for Workflow Studio* for details.

- 6 Save and close.

### Task 3: [Creating/Updating a Service Call Template for Select Identity Calls](#)

The purpose of a Service Desk template is to set default values. For Select Identity-Service Desk integration, initial values for some fields must be specified in the template.

To create or update a Service Desk template, perform the following steps:

- 1 In the left panel, navigate to **Data** → **Templates** → **Service Call**.
- 2 Create a new template by right-clicking in the right panel, or double-click an existing template to update it.
- 3 Name the template **OVSD-OVSI integration Template**.
- 4 Set the following fields to the specified default values:
  - **Status:** Registered
  - **Caller:** Current Person
  - **Description:** Enter an appropriate description.
  - **Information:** Enter any appropriate information.
  - **Source ID:** Enter an appropriate ID.

### Task 4: [Editing the Default Form to Display the Added Fields](#)

Add the activated custom fields from [Task 1](#) to the default form, so that the fields are displayed when creating a service call.

- 1 In the left panel, navigate to **Presentation** → **Forms** → **Service Call**.
- 2 In the right pane, double-click the default form.



Be sure that you are editing the *default form*, which is typically the **Service Call** form. If the default form is different on your system, use that form instead.

- 3 Drag the **Request ID**, **Request Failure Description**, **Request Link**, and **Request Type** from the **Attributes** area onto the form.
- 4 Save and close.

### Task 5: [Creating Database Rules to Send Emails Containing Select Identity URLs](#)

Create two database rules to send emails and update the **Request Link** field the Select Identity URLs for Forgotten and Change/Reset password respectively.

Each database rule contains two actions:

**Send E-mail Message:** This should include the Select Identity request link in the email body, as follows:

```
<http://<host>:<port>/lmz/ovsdintg/
forgetpassword.do?username=[Caller;Account;Login
name]&serviceCallId=[ID]>
```

**Update Data:** This should compose the following expression to set into the **Request Link** field:

```
(CONCATENATE http://<host>:<port>/lmz/ovsdintg/
pwdchangereset.do?userName= With (CONCATENATE [Caller Account Login
name] With (CONCATENATE &serviceCallId= With [ID])))
```

To create the database rules, perform the following steps:

- 1 Navigate to **Business Logic → Database Rules → Service Call**.
- 2 In the right pane, right-click and select **New Database Rule**.
- 3 Create the rules using the example rules below for reference.  
For **Condition**, specify the exact service call template name, from [Task 3](#).  
For the **URLs**, specify the actual <host> and <port> of your Select Identity system .

### Figure 18 Forgotten Password Database Rule

```
When service call is created
where Template;Name (*) is (exactly) Template for OVSD-OVSI integration
AND NOT (Caller;Account (*) is empty)
AND Category (*) equals Forget Password
Rule for OVSD-OVSI integration (Send e-mail message), Send to: [Caller;E-mail], Subject:
Select the link for password management, Message: Dear [Caller;Name],
You've made a request to reset a Forgotten Password. Please click the links below to
continue the procedure.
<http://<host>:<port>/lmz/ovsdintg/forgetpassword.do?username=[Caller;Account;Login
name]&serviceCallId=[ID]>

Regards
,Help Desk, Attachment Classification: <Unclassified>
Set a value (Update Data) Request Link set to (Concatenate http://<host>:<port>/lmz/
ovsdintg/forgetpassword.do?username= With (Concatenate [Caller Account Login name] With
(Concatenate &serviceCallId= With [ID])))
```

### Figure 19 Change Password Database Rule

```
When service call is created
where Template;Name (*) is (exactly) Template for OVSD-OVSI integration
AND NOT (Caller;Account (*) is empty)
AND Category (*) equals Change/Reset Password
Send email for Change/Reset Password (Send e-mail message), Send to: [Caller;E-mail],
Subject: Change/Reset Password, Message: Dear [Caller;Name],

You've made a request to Change or Reset your Password. Please click the links below to
continue the procedure.
<http://<host>:<port>/lmz/ovsdintg/pwdchangereset.do?userName=[Caller;Account;Login
name]&serviceCallId=[ID] >

Regards,
Help Desk
, Attachment Classification: <Unclassified>
Set a value (Update Data) Request Link set to (Concatenate http://<host>:<port>/lmz/
ovsdintg/pwdchangereset.do?userName= With (Concatenate [Caller Account Login name] With
(Concatenate &serviceCallId= With [ID])))
```

## aCreating a Smart Action

Create a smart action for the Service Desk CSR to view the request status in Select Identity.

- 1 Navigate to **Business Logic** → **Actions** → **Smart Actions** → **Service Call**.
- 2 In the right pane, right-click and select **New Smart Action**.
- 3 Enter the action name in the **Text** field.
- 4 Select **Internet Explorer** in the **Application** field.
- 5 Enter the following URL in the **Parameters** field, using the actual host name and port number for your Select Identity system:

```
http://<host>:<port>/lmz/ovsdintg/  
requeststatus.do?userName=[Caller;Account;Login  
name]&serviceCallId=[ID]&listObjectId=[Request ID]
```

### Task 6: Setting the Service Pages to Use the Select Identity Calls Template

Set the **Service** pages to use the template created in [Task 3](#), so the system will use this template when CSRs create new service calls.

- 1 In the administrator console, navigate to **Service Pages** → **Data** → **Template Settings**.
- 2 In the right pane, double-click **Service Call**.
- 3 Change both template settings to the name of the Select Identity calls template ([Task 3](#)).

## Linking a Service Calls to Select Identity Password Requests

Place a link from a service call to open the resultant password management request in Select Identity. This section describes how to configure the link into the service call template.

- 1 In the administrator console, navigate to **Service Pages** → **Data** → **Custom Fields**.
- 2 In the right pane, locate and open the **Service Call** item.
- 3 Make the following changes:
  - Locate one of the fields labeled **Sc. Text n**. Rename the field to **Request Link**.
  - Check the box labeled **Activate**.
  - Click the radio button labeled **All Categories**.
  - Click **OK**.
- 4 Edit the default form that you edited in [Task 4](#), to display the **Request Link** field:
  - a Navigate to **Presentation** → **Forms** → **Service Call**.
  - b Open the **Service Call** form and drag the **Request Link** from the **Attributes** to the form.
  - c Save and close the form.
- 5 Modify the database rules that you created in [Task 5](#) to target the link at the **Request Link** field.

Perform these steps carefully. They include the creation of dynamic variables.

- a Open the **Change/Reset Password** rule in the **Rule Editor**.
- b Click **Next** twice to locate the field labeled **Which actions do you want to be performed**.
- c Click **Add** and select **Update Data**.

- d Enter a **Name**, at the top of the dialog.
- e Select **Request Link** from the **Fields** list, and click the icon to the far right of the **Value** field.
- f In the dialog labeled **Set Value For Set To Request Link**, select **Concatenate** from the **Function** list, then click the icon at the right of the **Value** field under the list.
- g In the dialog labeled **Set Value for Concatenate**, select the **Fixed Value** and set the value to the following:  

```
http://<host>:<port>/lmz/ovsdintg/pwdchangereset.do?userName=
```
- h Click **OK** to return to the dialog labeled **Set Value for Set To Request Link**.  
 Notice that the **Value** field contains the URL from [step g](#).
- i Click the icon to the right of the field labeled **With**, which opens a dialog labeled **Set Value for Concatenate (With)**
- j Select **Concatenate** from the Function list again, then click the icon to the right of the **Value** field.
- k In the dialog labeled **Set Value For Concatenate**, select **Attribute** and click the icon at the right, so that you can select **Caller Account Login Name** from the menu.
- l Click **OK**.
- m Click the icon at the right of **With**.
- n Select the **Concatenate** function again.
- o Click the icon to the right of **Value**.
- p Enter `&serviceCallId=` in the **Fixed Value** field, then click **OK**.
- q Click the icon to the right of **With**. Select **Attribute**, and click the icon at the right
- r Enter `ID` into the field and click **OK**.
- s Click **OK** three more times, click **Add To List**, then Click **OK**.
- t In the Database Rule wizard, proceed through the remaining pages and save the rule.
- u Perform the same steps again for the **Forget Password** rule. for this rule, use the following value for the URL:  

```
http://<host>:<port>/lmz/ovsdintg/forgetpassword.do?username=
```

## OpenView Select Identity Configuration Tasks

In Select Identity, perform the following steps to configure Service Desk integration. Refer to the *Select Identity Online Help for Administrators* if you need additional information:

**Task 1:** Set the integration workflow in the `TruAccess.properties` file.

**Task 2:** Set parameters in the **SDIntegrator** external call.

### Task 1: Setting the Service Desk Workflow in the `TruAccess.properties` File

In the `TruAccess.properties` file, change the `truaccess.fixedtemplate.passwordreset` property to the following:

```
truaccess.fixedtemplate.passwordreset=OVSI\ Password\ Management\ with\
OVSD
```

## Task 2: Setting the External Call Parameters

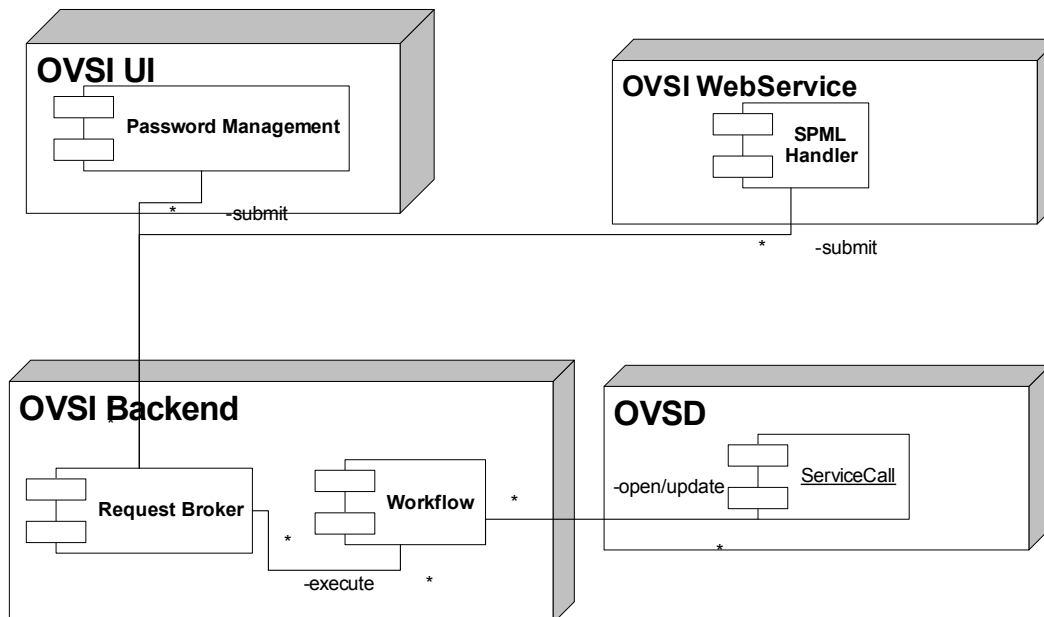
The **OVS** Password Management with **OVS** workflow invokes an external call when processing. Set its invocation parameters as follows:

- 1 Open the Select Identity **Service Studio** menu and select **External Calls**.
- 2 Locate and select the **SDIntegrator** external call.
- 3 Click **Modify** to change the parameter values.
- 4 Make the following changes to the parameters below:
  - **URL:** The hostname or IP address of the Service Desk server (the port is not needed).
  - **Login ID:** The Service Desk administrator. Set this to **system**.
  - **Password:** The password for the **System** Login ID. The default password for **System** is `servicedesk`.
  - **Template name:** The service call template name used for the integration. Enter the template name from Service Desk configuration [Task 3](#).

## System Context

[Figure 20](#) shows integration in its architectural context. The Select Identity user interface and back-end component dependencies with Service Desk are displayed as well as the communication between the components.

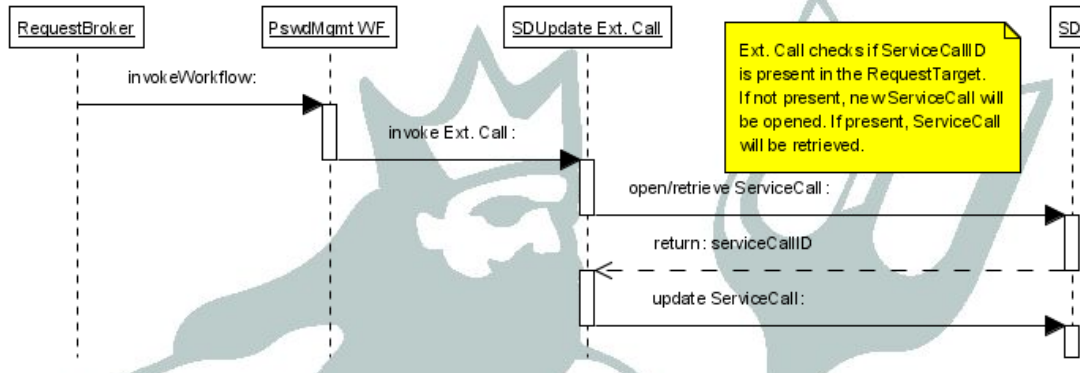
**Figure 20 Select Identity-Service Desk integration context**



## Process Flow

The diagram below shows the interactions when invoking or updating a Service Call from Service Desk.

**Figure 21 Service Call process flow**





## Select Identity-Select Audit Integration

Select Identity can be configured with Select Audit so that the two applications are able to perform the following:

- Pass Select Identity request, transaction, configuration, and maintenance data into Select Audit for compliance auditing in Sarbanes-Oxley, HIPAA, and other regulatory settings.
- Incorporate data from the Select Identity XML audit data stream into a wide range of reports.
- Allow Select Identity administrators to view configuration reports in Select Audit, depending on the access rights they have for Select Identity configuration reports. The Select Audit reports filter by the managed service and the context of the Select Identity administrator; you can only see reports for users and services you manage.

➤ Refer to the Select Audit documentation for detailed instructions on how to perform configuration steps in Select Audit. This documentation provides summary information only about how to set up integration from the Select Audit side.

### Requirements and Recommendations

The following guidelines apply to integrated Select Identity-Select Audit systems:

- Select Identity and Select Audit should be installed in separate Web Application Server domains.
- Select Audit must be able to connect to the Select Identity database.
- Select Identity must be able to send data to Select Audit via the port on which the Select Audit agent listens.

### Setting Up Integration in Select Identity

Select Identity configuration steps are minimal:

- 1 Install the Select Audit agent.
- 2 Configure the TruAccess properties that relate to the integration.
- 3 Insert a row into the database by editing the `dml` file.

### The Select Audit Agent

To set up the connection between Select Identity and Select Audit, you must install a standalone agent, known as the Select Audit connector, in Select Identity.

Refer to the installation guide provided with this agent for full instructions.

➤ No external call is needed for interoperability with Select Audit.

## TruAccess Properties

Several settings in the `TruAccess.properties` file relate to Select Audit integration. Set each one with the appropriate contents and save the file.

The following properties specify the host and port where the agent is running:

- `com.hp.ovsi.audit.saud.connector.host=localhost`
- `com.hp.ovsi.audit.saud.connector.port=9979`

This property defines what will be listed as the source application for Select Identity audit entries in Select Audit. Change this to something like Select Identity:

- `com.hp.ovsi.audit.saud.connector.client_id=unknown`

The following properties control performance aspects of the Select Audit agent.

- `com.hp.ovsi.audit.saud.connector.retries=1`
- `com.hp.ovsi.audit.saud.connector.pool_size=1`
- `com.hp.ovsi.audit.saud.connector.intervals=500`

## Configuring the Select Identity Database

You must modify the Select Identity database by adding an `insert` statement to the Oracle file. This statement inserts a row into the `AuditCfgEntry` table.

This operation can be performed in two ways:

- Remove the comment marks (indicated by the `--` character) from the line at installation time, so that the row will be inserted when the `dml` is run. If you do not invoke this line at installation time, you must run it manually using a tool such as SQLPlus.
- Insert the following fields manually into the `AuditCfgEntry` table:

```
— auditCfgEntryId
— eventType
— status
— namingFactory
— namingProvider
— connectionFactoryName
— destinationName
— destIsTopic
— auditCfgId
— disPosition
— values(2, 0, 1, null, 't3://localhost:7001', 'java:comp/env/jms/auditProcessorQCF', 'java:comp/env/jms/auditSelectAuditQueue', 0, 1, 1);
```

## Setting Up Integration in Select Audit

The Select Audit *Installation Guide* contains a section that specifically covers Select Identity integration. Technicians working on each side should be familiar with the other's documentation in addition to their own.

Integration can be set up in the following scenarios:

- During Select Audit installation, using the Select Identity configuration options that are built into the Select Audit installer.
- On an established system. In this case, Select Identity integration configuration resides in the Select Audit user interface.



Ensure that there are pre-existing Select Audit user accounts corresponding to those with access from Select Identity; you must create these on the Web application Server.

## Data Filtering and Report Access Matrices

The tables in this section provide details of the reports available to Select Identity users, and the report types to which users must have access in Select Identity to be able to access corresponding report types in Select Audit.

In general, if your role and context permits you to view audit and configuration reports in Select Identity, you can view the corresponding types in Select Audit.

Report Name	SI User	Non-SI User	SI Not Available	Administrators	Auditors
Account Change	If allowed in SI on certain report types (see table below), will have these permissions on related reports: <ul style="list-style-type: none"> <li>• Read,</li> <li>• Execute,</li> <li>• Schedule,</li> <li>• Adhoc</li> </ul>	Denied	Denied	Full permissions including: <ul style="list-style-type: none"> <li>• Read,</li> <li>• Write,</li> <li>• Delete,</li> <li>• Execute,</li> <li>• Schedule,</li> <li>• Adhoc,</li> <li>• View</li> <li>• Grant</li> <li>• Revoke</li> </ul>	<ul style="list-style-type: none"> <li>• Read</li> <li>• Execute</li> <li>• Schedule</li> <li>• Adhoc</li> </ul>
Account Events					
Administrator					
Change History					
Configuration					
Password Management					
Security Events					
Service					
System Activity					
User Activity					
User Summary					
Workflow Events					
Attestation	Read, Execute, Schedule, Adhoc				
Data Integrity	Read, Execute, Schedule, Adhoc				
Raw Message	Denied				

## Report Mapping

The following table shows which Select Identity report types are required in order for users to access each Select Audit report:

<b>To be seen in this report in Select Audit</b>	<b>Users need <i>any</i> of these report types in Select Identity.</b>
Account Change Report	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Account Events Report	AuditUser
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
Administrator Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserHint
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Change History Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination

Configuration Report	AdminConfiguration
Password Management Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Security Events Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Service Report	AuditService
System Activity Report	Any report types
User Activity Report	Any report types
User Summary Report	AuditUserSummary
Workflow Events Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination

The following table shows the relationship between Select Identity report types and Select Audit events.

If you have this report type assigned in SI	You will be able to see these events in Select Audit		
	AUDITEVENTNAME	APPLICATION	COMPONENTEVENTNAME
Audit User	Sent Login request	SelectFederation	SF Protocol Sent Login Request
Audit User	Sent Logout request	SelectFederation	SF Protocol Sent Logout Request
Audit User	Received Login request	SelectFederation	SF Protocol Received Login Request
Audit User	Received Login request	SelectFederation	SF Protocol Received Logout Request
Audit User	Received Logout request	SelectFederation	SF API Received logout request
Audit User	Logged In	SelectAccess	Login
Audit User	Logged In	SelectIdentity	SI login
Audit User	Logged In	SelectFederation	SF Internal Logged In

<b>Audit User</b>	Logged Out	SelectAccess	Logout
<b>Audit User</b>	Logged Out	SelectIdentity	SI logout
<b>Audit User</b>	Logged Out	SelectFederation	SF Internal Logged Out
<b>Audit User</b>	Login Error	SelectAccess	Login error
<b>Audit User</b>	Login Error	SelectFederation	SF Internal Login Error
<b>Audit User</b>	Admin Logged in	SelectAccess	Admin Login
<b>Audit User</b>	Admin Logged in	SelectAccess	Delegate Admin Login
<b>Audit User</b>	Admin Logged in	SelectFederation	SF Admin Logged In
<b>Audit User</b>	Admin Logged Out	SelectAccess	Admin Logout
<b>Audit User</b>	Admin Logged Out	SelectAccess	Delegate Admin Logout
<b>Audit User</b>	Admin Logged Out	SelectFederation	SF Admin Logged Out
<b>Audit User</b>	Admin Login Error	SelectAccess	Admin Login error
<b>Audit User</b>	Admin Login Error	SelectAccess	Delegate Admin Login error
<b>Audit User</b>	Admin Login Error	SelectFederation	SF Admin Login Error
<b>Audit User</b>	Credential expire	SelectAccess	Credential expire
<b>Audit User</b>	User Authenticated	SelectFederation	SF Internal User Authenticated
<b>Audit User</b>	User Authentication Error	SelectFederation	SF Internal User Authentication Error
<b>Audit User</b>	Access Allow	SelectAccess	Allow
<b>Audit User</b>	Access Deny	SelectAccess	Deny
<b>Audit User</b>	Reset Password	SelectIdentity	SI Reset Password
<b>Audit User</b>	Change Password	SelectIdentity	SI Change Password
<b>Audit User</b>	Change Password	SelectFederation	SF AdminAdm Password Changed
<b>Audit User</b>	Error Changing Password	SelectFederation	SF AdminAdm Error Changing Password
<b>Audit User</b>	Forget Password	SelectIdentity	SI Forget Password
<b>Audit User</b>	Expire Password Notification	SelectIdentity	SI Expire Password Notification
<b>Audit User</b>	Expire Password	SelectIdentity	SI Expire Password
<b>Audit User</b>	Hint Setup	SelectIdentity	SI Hint Setup
<b>Audit User</b>	Password Policy change	SelectAccess	passwordPolicyChange
<b>Audit User</b>	Password Reset Config Change	SelectAccess	password Reset Config Change
<b>Audit User</b>	User Add	SelectAccess	UserAdd
<b>Audit User</b>	User Add	SelectIdentity	SI Add NewUser
<b>Audit User</b>	User Delete	SelectAccess	UserDelete

<b>Audit User</b>	User Change	SelectAccess	UserChange
<b>Audit User</b>	User Change	SelectIdentity	SI Modify user
<b>Audit User</b>	Terminate User	SelectIdentity	SI Terminate User
<b>Audit User</b>	Modify Profile	SelectIdentity	SI Modify Profile
<b>Audit User</b>	Manage User Expiration	SelectIdentity	SI Manage User Expiration
<b>Audit User</b>	Move User	SelectIdentity	SI Move User
<b>Audit User</b>	disable before terminate	SelectIdentity	SI disable before terminate
<b>Audit User</b>	Added Admin	SelectFederation	SF AdminAdm Added Admin
<b>Audit User</b>	Deleted Admin	SelectFederation	SF AdminAdm Deleted Admin
<b>Audit User</b>	User Consented	SelectFederation	SF User Consented
<b>Audit User</b>	Copy User	SelectIdentity	SI Copy User
<b>Audit User</b>	User Source Add	SelectAccess	userSourceAdd
<b>Audit User</b>	User Source Delete	SelectAccess	userSourceDelete
<b>Audit User</b>	User Source Change	SelectAccess	userSourceChange
<b>Audit User</b>	Security Violation	SelectIdentity	SI Security Violation
<b>Audit User</b>	Group Add	SelectAccess	GroupAdd
<b>Audit User</b>	Group Delete	SelectAccess	GroupDelete
<b>Audit User</b>	Group Change	SelectAccess	GroupChange
<b>Audit User</b>	User Role Add	SelectAccess	UserRoleAdd
<b>Audit User</b>	User Role Delete	SelectAccess	UserRoleDelete
<b>Audit User</b>	User Role Change	SelectAccess	UserRoleChange
<b>Audit User</b>	Admin Role Add	SelectIdentity	SI Admin role create
<b>Audit User</b>	Admin Role Delete	SelectIdentity	SI Admin role delete
<b>Audit User</b>	Admin Role Change	SelectIdentity	SI Admin role modify
<b>Audit User</b>	User role delegation Activate	SelectIdentity	SI User Role Delegation Activate
<b>Audit User</b>	User role delegation Deactivate	SelectIdentity	SI User Role Delegation Deactivate
<b>Audit User</b>	Folder Add	SelectAccess	FolderAdd
<b>Audit User</b>	Folder Delete	SelectAccess	FolderDelete
<b>Audit User</b>	Folder Change	SelectAccess	FolderChange
<b>Audit User</b>	Authn Add	SelectAccess	authnAdd
<b>Audit User</b>	Authn Delete	SelectAccess	authnDelete
<b>Audit User</b>	Authn Change	SelectAccess	authnChange
<b>Audit User</b>	Delegate delegated	SelectAccess	delegate delegate

<b>Audit User</b>	Delegate undelegate	SelectAccess	delegate undelegate
<b>Audit User</b>	Delegate inherit	SelectAccess	delegate inherit
<b>Audit User</b>	Delegate Change	SelectAccess	delegateChange
<b>Audit User</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User</b>			
<b>Audit User</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit User</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit User</b>	Enable Service Membership	SelectIdentity	SI Enable Service Membership
<b>Audit User</b>	Disable Service Membership	SelectIdentity	SI Disable Service Membership
<b>Audit User</b>	Enable All Services	SelectIdentity	SI Enable All Services
<b>Audit User</b>	View resource attribute	SelectIdentity	SI View resource attribute
<b>Audit User</b>	View attribute	SelectIdentity	SI View attribute
<b>Audit User</b>	activeAttributes	SelectAccess	activeAttributes
<b>Audit User</b>	User Federated	SelectFederation	SF Internal User Federated
<b>Audit User</b>	User Federation Error	SelectFederation	SF Internal User Federation Error
<b>Audit User</b>	View Service Membership	SelectIdentity	SI View Service Membership
<b>Audit User</b>	Ignore Add	SelectIdentity	SI Ignore Add
<b>Audit User</b>	Ignore Modify	SelectIdentity	SI Ignore Modify
<b>Audit User</b>	Ignore Delete	SelectIdentity	SI Ignore Delete
<b>Audit Service</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit Service</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted



<b>Audit Service</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit Service</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit Service</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit Service</b>			
<b>Audit Service</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit Service</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit Service</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit Service</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit Service</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit Service</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit Service</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit Service</b>	Add Service	SelectIdentity	SI Add Service
<b>Audit Service</b>	Create service	SelectIdentity	SI Create service
<b>Audit Service</b>	Delete service	SelectIdentity	SI Delete service
<b>Audit Service</b>	Modify service	SelectIdentity	SI Modify service
<b>Audit Service</b>	Copy service	SelectIdentity	SI Copy service
<b>Audit Service</b>	Set service attribute values	SelectIdentity	SI Set service attribute values
<b>Audit Service</b>	Set service attribute properties	SelectIdentity	SI Set service attribute properties
<b>Audit Service</b>	Create service view	SelectIdentity	SI Create service view
<b>Audit Service</b>	Delete service view	SelectIdentity	SI Delete service view
<b>Audit Service</b>	Modify service view	SelectIdentity	SI Modify service view
<b>Audit Service</b>	Create service role	SelectIdentity	SI Create service role
<b>Audit Service</b>	Delete service role	SelectIdentity	SI Delete service role
<b>Audit Service</b>	Create service context	SelectIdentity	SI Create service context
<b>Audit Service</b>	Delete service context	SelectIdentity	SI Delete service context
<b>Audit Service</b>	Modify service context	SelectIdentity	SI Modify service context
<b>Audit Service</b>	Import service	SelectIdentity	SI Import service
<b>Audit Service</b>	Modify service role	SelectIdentity	SI Modify service role
<b>Audit Service</b>	Svc Change Recon Modify User	SelectIdentity	SI Svc Change Recon Modify User
<b>Audit Service</b>	Svc Change Recon Add resource	SelectIdentity	SI Svc Change Recon Add resource

<b>Audit Service</b>	Svc Change Recon Delete resource	SelectIdentity	SI Svc Change Recon Delete resource
<b>Audit Service</b>	Service Export	SelectIdentity	SI Service Export
<b>Audit Service</b>	Create attribute	SelectIdentity	SI Create attribute
<b>Audit Service</b>	Delete attribute	SelectIdentity	SI Delete attribute
<b>Audit Service</b>	Modify attribute	SelectIdentity	SI Modify attribute
<b>Audit Service</b>	View attribute	SelectIdentity	SI View attribute
<b>Audit Service</b>	Copy attribute	SelectIdentity	SI Copy attribute
<b>Audit Service</b>	Attribute import	SelectIdentity	SI attribute export
<b>Audit User Creation</b>	User Add	SelectAccess	UserAdd
<b>Audit User Creation</b>	User Add	SelectIdentity	SI Add NewUser
<b>Audit User Creation</b>	Move User	SelectIdentity	SI Move User
<b>Audit User Creation</b>	Added Admin	SelectFederation	SF AdminAdm Added Admin
<b>Audit User Creation</b>	Copy User	SelectIdentity	SI Copy User
<b>Audit User Creation</b>	User Source Add	SelectAccess	userSourceAdd
<b>Audit User Creation</b>	Group Add	SelectAccess	GroupAdd
<b>Audit User Creation</b>	User Role Add	SelectAccess	UserRoleAdd
<b>Audit User Creation</b>	Admin Role Add	SelectIdentity	SI Admin role create
<b>Audit User Creation</b>	Folder Add	SelectAccess	FolderAdd
<b>Audit User Creation</b>	Authn Add	SelectAccess	authnAdd
<b>Audit User Creation</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User Creation</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User Creation</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User Creation</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User Creation</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User Creation</b>			
<b>Audit User Creation</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User Creation</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User Creation</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User Creation</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User Creation</b>	Workflow copy	SelectIdentity	SI workflow copy

<b>Audit User Creation</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User Creation</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit User Creation</b>	Enable Service Membership	SelectIdentity	SI Enable Service Membership
<b>Audit User Creation</b>	Enable All Services	SelectIdentity	SI Enable All Services
<b>Audit User Deletion</b>	User Delete	SelectAccess	UserDelete
<b>Audit User Deletion</b>	Move User	SelectIdentity	SI Move User
<b>Audit User Deletion</b>	Deleted Admin	SelectFederation	SF AdminAdm Deleted Admin
<b>Audit User Deletion</b>	User Source Delete	SelectAccess	userSourceDelete
<b>Audit User Deletion</b>	Group Delete	SelectAccess	GroupDelete
<b>Audit User Deletion</b>	User Role Delete	SelectAccess	UserRoleDelete
<b>Audit User Deletion</b>	Admin Role Delete	SelectIdentity	SI Admin role delete
<b>Audit User Deletion</b>	Folder Delete	SelectAccess	FolderDelete
<b>Audit User Deletion</b>	Authn Delete	SelectAccess	authnDelete
<b>Audit User Deletion</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User Deletion</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User Deletion</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User Deletion</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User Deletion</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User Deletion</b>			
<b>Audit User Deletion</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User Deletion</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User Deletion</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User Deletion</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User Deletion</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit User Deletion</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User Deletion</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit User Deletion</b>	Disable Service Membership	SelectIdentity	SI Disable Service Membership
<b>Audit User Termination</b>	Terminate User	SelectIdentity	SI Terminate User
<b>Audit User Termination</b>	disable before terminate	SelectIdentity	SI disable before terminate

<b>Audit User Termination</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User Termination</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User Termination</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User Termination</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User Termination</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User Termination</b>			
<b>Audit User Termination</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User Termination</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User Termination</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User Termination</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User Termination</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit User Termination</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User Termination</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit User Password</b>	Reset Password	SelectIdentity	SI Reset Password
<b>Audit User Password</b>	Change Password	SelectIdentity	SI Change Password
<b>Audit User Password</b>	Change Password	SelectFederation	SF AdminAdm Password Changed
<b>Audit User Password</b>	Error Changing Password	SelectFederation	SF AdminAdm Error Changing Password
<b>Audit User Password</b>	Forget Password	SelectIdentity	SI Forget Password
<b>Audit User Password</b>	Expire Password Notification	SelectIdentity	SI Expire Password Notification
<b>Audit User Password</b>	Expire Password	SelectIdentity	SI Expire Password
<b>Audit User Password</b>	Password Policy change	SelectAccess	passwordPolicyChange

<b>Audit User Password</b>	Password Reset Config Change	SelectAccess	password Reset Config Change
<b>Audit User Password</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User Password</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User Password</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User Password</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User Password</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User Password</b>			
<b>Audit User Password</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User Password</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User Password</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User Password</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User Password</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit User Password</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User Password</b>	Workflow export	SelectIdentity	SI workflow export
<b>Audit User Hint</b>	Hint Setup	SelectIdentity	SI Hint Setup
<b>Audit User Login</b>	Sent Login request	SelectFederation	SF Protocol Sent Login Request
<b>Audit User Login</b>	Sent Logout request	SelectFederation	SF Protocol Sent Logout Request
<b>Audit User Login</b>	Received Login request	SelectFederation	SF Protocol Received Login Request
<b>Audit User Login</b>	Received Login request	SelectFederation	SF Protocol Received Logout Request
<b>Audit User Login</b>	Received Logout request	SelectFederation	SF API Received logout request
<b>Audit User Login</b>	Logged In	SelectAccess	Login
<b>Audit User Login</b>	Logged In	SelectIdentity	SI login
<b>Audit User Login</b>	Logged In	SelectFederation	SF Internal Logged In
<b>Audit User Login</b>	Logged Out	SelectAccess	Logout
<b>Audit User Login</b>	Logged Out	SelectIdentity	SI logout

<b>Audit User Login</b>	Logged Out	SelectFederation	SF Internal Logged Out
<b>Audit User Login</b>	Login Error	SelectAccess	Login error
<b>Audit User Login</b>	Login Error	SelectFederation	SF Internal Login Error
<b>Audit User Login</b>	Admin Logged in	SelectAccess	Admin Login
<b>Audit User Login</b>	Admin Logged in	SelectAccess	Delegate Admin Login
<b>Audit User Login</b>	Admin Logged in	SelectFederation	SF Admin Logged In
<b>Audit User Login</b>	Admin Logged Out	SelectAccess	Admin Logout
<b>Audit User Login</b>	Admin Logged Out	SelectAccess	Delegate Admin Logout
<b>Audit User Login</b>	Admin Logged Out	SelectFederation	SF Admin Logged Out
<b>Audit User Login</b>	Admin Login Error	SelectAccess	Admin Login error
<b>Audit User Login</b>	Admin Login Error	SelectAccess	Delegate Admin Login error
<b>Audit User Login</b>	Admin Login Error	SelectFederation	SF Admin Login Error
<b>Audit User Login</b>	Credential expire	SelectAccess	Credential expire
<b>Audit User Login</b>	Reset Password	SelectIdentity	SI Reset Password
<b>Audit User Login</b>	Password Reset Config Change	SelectAccess	password Reset Config Change
<b>Audit User Login</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
<b>Audit User Login</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Audit User Login</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Audit User Login</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Audit User Login</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Audit User Login</b>			
<b>Audit User Login</b>	Workflow create	SelectIdentity	SI workflow create
<b>Audit User Login</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Audit User Login</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Audit User Login</b>	Workflow view	SelectIdentity	SI workflow view
<b>Audit User Login</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Audit User Login</b>	Workflow import	SelectIdentity	SI workflow import
<b>Audit User Login</b>	Workflow export	SelectIdentity	SI workflow export
<b>Admin Configuration</b>	WorkflowConfigChange	SelectAccess	WorkflowConfigChange

<b>Admin Configuration</b>	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
<b>Admin Configuration</b>	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
<b>Admin Configuration</b>	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
<b>Admin Configuration</b>	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
<b>Admin Configuration</b>			
<b>Admin Configuration</b>	Workflow create	SelectIdentity	SI workflow create
<b>Admin Configuration</b>	Workflow delete	SelectIdentity	SI workflow delete
<b>Admin Configuration</b>	Workflow modify	SelectIdentity	SI workflow modify
<b>Admin Configuration</b>	Workflow view	SelectIdentity	SI workflow view
<b>Admin Configuration</b>	Workflow copy	SelectIdentity	SI workflow copy
<b>Admin Configuration</b>	Workflow import	SelectIdentity	SI workflow import
<b>Admin Configuration</b>	Workflow export	SelectIdentity	SI workflow export
<b>Admin Configuration</b>	Logging Config Change	SelectAccess	loggingConfigChange
<b>Admin Configuration</b>	Select Audit Report Config	SelectAudit	





# 8 Uninstalling Select Identity

This section covers the following topics:

- [Auto-Uninstalling Select Identity](#)
- [Uninstalling Select Identity Manually on IBM WebSphere 6.0.2](#)
- [Uninstalling the Select Identity Database](#)

## Auto-Uninstalling Select Identity

If you installed Select Identity using the InstallAnywhere installer, you can also uninstall it using the auto-uninstaller.

Uninstalling a manual Select Identity installation may not be successful because manual installations are likely to vary from the settings expected by the uninstaller.

- To uninstall using the auto-uninstaller, locate and run the `uninstall` executable, which the installer places into `<OVSI_install_dir>/`. This removes all deployed resources.

## Uninstalling Select Identity Manually on IBM WebSphere 6.0.2

To uninstall Select Identity manually, log on to the WebSphere console and perform the following steps:

- 1 Undeploy the Select Identity `was6_lmz.ear` application from the **Enterprise Applications** page. See [Undeploying the Online Help or Another Application](#) on page 106.
- 2 Delete the following items. Delete only those instances of each item that are specific to Select Identity:
  - The mail provider and session
  - JDBC provider
  - JMS queue connection factory
  - JMS topic connection factory
  - JMS queues
  - JMS topics
  - JMS activation specifications
  - Service integration bus (OVSIbus)
  - Bus destinations

## Undeploying the Online Help or Another Application

Perform the following steps to remove the online help or any other deployed application from the WebSphere server.

- 1 Locate the application that you want to remove on the **Enterprise Applications** page.
- 2 If the application **Status** is **Started** (green arrow), click **Stop** to shut it down; if **Stopped**, skip this step.
- 3 Confirm that the application status is **Stopped**.
  - Select the application that you just stopped, and click **Uninstall** to remove the application from the WebSphere server.

## Uninstalling the Select Identity Database

This section describes how to uninstall an Oracle Select Identity database.

After you uninstall Select Identity from the Web application server, back up and remove the data and tables from the database.

### Uninstalling Oracle

Perform the following steps to uninstall the Select Identity database from Oracle:

- 1 From a SQL Plus command prompt, log in to Oracle as a user with system permissions.
- 2 Enter the following command:

```
drop user Select_Identity_database_username cascade
```

# A TruAccess Properties

Configure general settings for the HP OpenView Select Identity server and user interface by using a text editor to modify the `TruAccess.properties` file. This file contains important settings for triggers that determine the way that Select Identity operates. Consider each with great care.

Some of these settings specify directories used by Select Identity. Ensure that you specify these accurately if you modify them.

To disable individual properties, comment them out. In a few instances, a property is commented out by default. This may be for several reasons; for example, properties intended for a future release may be put into place in advance using this method.

## TruAccess Properties Summary

This section summarizes each TruAccess property. The description indicates if a property should not be edited.

For information about TruAccess properties that you use to customize the Select Identity user interface, see [Custom User Interface Properties](#) on page 63.

For information about TruAccess properties that you use to customize the Select Identity date and time format, see [Localizing the Date and Time Format](#) on page 66.

### General Settings

- **`truaccess.dateformat=yyyy-MM-dd`**  
Specifies the date format throughout the Select Identity system.
- **`truaccess.timestampformat=yyyy-MM-dd hh:mm:ss a`**  
Specifies the time stamp format throughout the Select Identity system.
- **`truaccess.version=<version number>`**  
Specifies the Select Identity version number. *Do not change this value.*
- **`truaccess.hibernate.config=/com/tru logica/truaccess/util/persistence/mssqlserver.hibernate.cfg.xml`**  
Specifies the hibernate property file. *Leave this property commented.*
- **`truaccess.policy.id=1`**  
Specifies the default Select Identity policy identifier.
- **`truaccess.expirationProcessPeriod=30`**  
Specifies the time interval prior to automatic account expiration (in days). The default is 30days. At this point, a designated manager is sent a reminder notification.

- **truaccess.expire.administrator.userId=sis**  
**truaccess.expire.administrator.adminFunc=Concero Sys Admin**  
Specifies the default Select Identity system administrator user ID and administrative role.
- **contact\_helpdesk=Please contact the helpdesk.**  
Provides the text for an error message that displays if the user cannot log on to the Select Identity client.
- **com.hp.ovsi.help.web = http://support.hp.com**  
The URL for external Web help
- **truaccess.homepage=http://www.hp.com**  
**com.hp.si.clientName=HP**  
Client Name. Specifies your home page and your company name when uncommented.
- **com.hp.ovsi.i18n.labels.debug = false**  
Debug resource bundle strings
- **ui.locale.date.format=MM/dd/yyyy**  
Defines the preferred date format in the user interface. This is specified as a date pattern described in java.text.SimpleDateFormat. This value can be left empty in order to use the default format.
- **com.hp.si.user.attributes.maxlength=10**  
Attribute Max Length default value in KB.
- **si.autodiscovery.audit=false (hidden, default to false)**  
Whether to audit user import
- **si.serviceassignment.server.num = X**  
Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.

## Asynchronous Provisioning Delay

- **truaccess.provisioning.delay=2**  
Specifies the delay (in seconds) for asynchronous provisioning.

## Audit Settings

These include settings for exchanging data with HP OpenView Select Audit.

- **truaccess.audit.detail=off**  
Specifies whether to increase the level of detail stored for audit history reports. If set to **on**, performance may be affected.
- **com.hp.ovsi.audit.saud.connector.host=localhost**  
**com.hp.ovsi.audit.saud.connector.port=9979**  
**com.hp.ovsi.audit.saud.connector.client\_id=unknown**  
**com.hp.ovsi.audit.saud.connector.retries=1**  
**com.hp.ovsi.audit.saud.connector.pool\_size=1**  
**com.hp.ovsi.audit.saud.connector.intervals=500**

Select Audit configuration settings. By default the connector is installed on the localhost. Refer to the Select Audit documentation about these values, and remove the **prefix com.hp.ovsi.audit.saud.connector**. The resulting property is the same property used by HP OpenView Select Audit.

## Authentication Settings

- **truaccess.authentication=on**  
**truaccess.sso.token.name=ct\_remote\_user.do**  
**truaccess.loginURL=https://localhost:7001/lmz/control/signin**  
**truaccess.logoutPage=https://localhost:7001/lmz/control/logoff.do**

Specifies authentication settings. If `truaccess.authentication` is set to **on**, the next three attributes are ignored. If it is set to **off**, you must specify the single sign-on token name, the logon URL, and the logout URL for cleaning up the session.

## Auto User Import Settings

- **ovsi.ad.rootdir=/opt/si4.0/websphere/adroot**  
**ovsi.ad.backupdir=/opt/si4.0/websphere/adbackup**  
**ovsi.ad.stagingdir=/opt/si4.0/websphere/adstaging**  
**ovsi.ad.subdir=subdir**  
**ovsi.ad.userid=2**  
**ovsi.ad.file.threshold=2**

Specifies the default values for properties for an Auto User Import. If automatic pickup of user import files. If `rootdir` and `backupdir` are not provided in the `TruAccess.properties` file, no user import will be scheduled.

## Batch Processing Settings

- **truaccess.batch.inprogresstimeout=1800000**  
Specifies the time-out and owner for batch processing for the User Discovery facility. To specify common batch processing, set `truaccess.batch.ownerkey` to **0**, or you can specify a specific WebLogic server.
- **truaccess.batch.reportdir=c:/temp/reports**  
Specifies the policy to pick up the batch files for the User Import facility and the directory to which reports are written.
- **truaccess.batch.report.file.maxsize =1000000**  
Determines the maximum batch generated file size (in bytes) to be sent as attachment by Select Identity.
- **truaccess.batch.reportdir=c:/temp/reports**  
**truaccess.reports.printView.maxRecords = 1000**  
Specifies the location to save a batch generated file if its size exceeds maximum size limit defined by `truaccess.batch.report.file.maxsize` and the maximum number of records that can be stored by Select Identity.
- **truaccess.sqlQueryInListSize=200**  
Specifies the maximum number of positional parameters to be used in a SQL query “in” list or array as in the query `select ... where a in (?, ?, ?, ?...)`

- **truaccess.batchQuerySize=500**  
Specifies the maximum number of queries to be executed in a single batch insert or update statement.
- **si.serviceassignment.batchsize=xx (hidden, default to 20)**  
Number of users to process in one JMS message

## Bulk Upload Settings

- **truaccess.upload.filedir=c:/temp**  
**truaccess.upload.maxfilesize=10485760**  
Specifies a temporary directory that the Bulk Upload process uses. It specifies the maximum upload file size (in bytes) as well.

## Cache Settings

- **si.cache.service.local=true**  
Determines whether or not to turn the resource cache on (hidden and default to true)
- **si.cache.resource.localmax=50**  
Maximum entries in service cache (hidden and default to 50)
- **si.cache.service.local=true (hidden and default to true)**  
Whether to turn the service cache on.  
**si.cache.service.localmax=100 (hidden and default to 100)**  
Max entries in service cache
- **si.cache.service.local.checkdb=false (hidden and default to false)**  
Whether the cached entry should be compared against database.
- **si.cache.taattrdef.local=true (hidden and default to true)**  
Whether to turn attribute definition cache on.
- **si.cache.taattrdef.localmax=300 (hidden and default to 100)**  
Max entries in service cache.
- **si.cache.taattrdef.local.checkdb=false (hidden and default to false)**  
Whether the cached entry should be compared against database

## Connector Schema Directory

- **com.hp.ovsi.connector.schema.dir=C:/si4.0/schema**  
Determines the connector schema directory.

## Email Settings

- **truaccess.email.new.timeinterval=120**  
Specifies the time interval (in seconds) that the email daemon uses to send new email.

- **truaccess.email.retry.timeinterval=900**  
Specifies the time interval (in seconds) that the email daemon uses for sending new email if initial attempts were unsuccessful.
- **truaccess.email.retry.maximum=3**  
Specifies the maximum number of retry attempts for sending email. Setting this to **0** causes Select Identity to retry indefinitely.
- **truaccess.email.to.empty=off**  
Specifies whether to send email if the “to” email address cannot be determined. Specify **on** if you want to send email to the administrator in this event. Specify **off** if you do not want email sent.
- **truaccess.email.userinfochange=off**  
*Do not change the value of this property.*
- **truaccess.email.redirect=off**  
**truaccess.email.redirect.dir=C:/temp/email**  
Specifies if and where email should be written if a mail server is not available. In general, this is for testing purposes only.
- **truaccess.email=on**  
**truaccess.email.inprogresstimeout=600000**  
**truaccess.email.batchcount=50**  
**truaccess.email.authetication=sntp**  
Determines whether Select Identity sends email. If `truaccess.email` is set to **off**, no email is sent.
- **truaccess.sender.name=SelectIdentity**  
**truaccess.sender.email=selectidentity@hp.com**  
Specifies a default name and email address to use if the sender’s information cannot be determined.
- **truaccess.method=http**  
**truaccess.host=localhost**  
**truaccess.port=7001**  
Specifies the URL construction to the Select Identity system within email notifications.
- **ovsi.ad.emailCC=your.email@yourdomain.com**  
Specifies the email address pattern used by Select Identity to validate email addresses.
- **si.email.attachment.size=500**  
Defines the maximum size of an email attachment if component limit size option is on (hidden default set to 500K).

## Execution Retry Settings

- **truaccess.job.retry.timeinterval=600**  
**truaccess.job.retry.maximum=3**  
Specifies the time interval (in seconds) that Select Identity will wait between attempts to execute a function, such as deleting a user, and the maximum number of retries allowed before the request fails.

- **truaccess.postprovision.retry.timeinterval=5000**  
**truaccess.postprovision.retry.maximum=20**

Specifies the time (in milliseconds) to sleep before retrying a post-provisioning attempt (to add an account to the Select Identity database) and the number of retry events required before the request fails.

- **com.ovsi.passwordoperation.retrydelay=100**  
**com.ovsi.passwordoperation.retrycount=3**

Specifies the retry time (in milliseconds) to perform a password operation during provisioning and the number of retry events required before the request fails.

- **truaccess.entcache.retry.timeinterval=5000**  
**truaccess.entcache.retry.maximum=3**

Specifies the time (in milliseconds) to get an entitlement from the entitlement cache before retrying and the number of retry events required before the request fails.

## External Calls Settings

- **personId.attributes=FirstName,LastName**  
**standardId.attributes=personId,Email**  
**\_\_managerEmailLookup.attributes=Email**

Specifies the attributes for external calls.

## JNDI Data Source Settings

- **truaccess.dataSource=jdbc/TruAccess**

Specifies the JNDI name of the data source. You should not need to modify this setting.

- **truaccess.mailSession=mail/TruAccess**

Specifies the JNDI name for the mail session ID. You should not need to modify this setting.

## Localization Settings

- **com.hp.si.locales=en,en\_US,zh\_CN,ko**

Supported locales (US English is the default).

## Notification Event Settings

- **com.hp.ovsi.default.notification.approve=Add\ User**

The default email template for Approve Notification Event

## Operations Templates

- **truaccess.fixedtemplate.passwordreset=SI\ Password\ Change\Provisioning**  
**truaccess.fixedtemplate.terminate=SI\ Provisioning\ Only**  
**truaccess.fixedtemplate.disable=SI\ Provisioning\ Only**  
**truaccess.fixedtemplate.enable=SI\ Provisioning\ Only**



**truaccess.fixedtemplate.expiration=UserAccountExpirationWF**  
**truaccess.fixedtemplate.securityviolation=SI\ Email\ Only**  
**truaccess.fixedtemplate.modifyprofile=SI Provisioning Only**  
**truaccess.fixedtemplate.passwordexpirenot=SI\ PasswordExpire\Email**  
**truaccess.fixedtemplate.passwordexpire=SI\ Provisioning\ Only**  
**truaccess.fixedtemplate.disable.terminate=SI\ Provisioning\Only**  
**truaccess.fixedtemplate.reconciliation=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.recon\_enable=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.recon\_terminate=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.recon\_disable=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.recon\_disable\_terminate=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.bulk\_default=ReconciliationDefaultProcess**  
**truaccess.fixedtemplate.bulk\_move=SI Provisioning Only Bulk**

Specifies workflow template for certain Select Identity operations. The fixedtemplate workflows are used by operations NOT controlled by Service Role events; there is no Password Reset Request Event on the service, the template to be used has to be defined in the properties file.

## Page Redirect Timeout

- **truaccess.pageredirect.timeout=10**  
Specifies the timeout (in seconds) for page redirects.

## Reconciliation Settings

- **truaccess.resource.record.max=1000**  
Specifies the maximum number of users updated during reconciliation.

- **truaccess.recon.rootdir=c:/temp/reconroot**  
**truaccess.recon.stagingdir=c:/temp/reconstaging**  
**truaccess.recon.backupdir=c:/temp/reconbackup**  
**truaccess.recon.filename.timeformat=yyyy\_MM\_dd\_H\_mm**  
**truaccess.recon.task.check.threshold=3**

Specifies the attributes for account reconciliation. The `TruAccess.recon.task.check.threshold` property specifies the number of times that a task is checked (in 30-second intervals) before it is put to process. There is a limit to the number of simultaneous tasks that can be processed in Select Identity. If the limit is exceeded, a new task must wait for its turn. This parameter is used to prevent blocking of further processing if some tasks become suspended in an error and incomplete state.

The following reconciliation properties are obsolete in release 4.0 and later:

**truaccess.recon.check\_serviceassignment\_authadd=false**  
**truaccess.recontimer.startdelay=30**  
**truaccess.recontimer.timeinterval=30**

- **truaccess.reconciliation.postprovpolicy=1**  
Specifies when Select Identity performs post-provisioning reconciliation. Specify one of the following values:

**Perform SI Update if:**

- 1 — if all provisioning activities were successful**
- 2 — if the corresponding provisioning activity was successful**
- 3 — always**

- **si.recon.policybased=true (hidden, default to true)**  
Policy Based Recon Switch
- **si.recon.server.num = X**  
Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.
- **si.recon.processor.num = X**  
Hidden, default set to 8.
- **truaccess.bulk.postprovpolicy=2**  
Specifies when Select Identity performs post-provisioning after a bulk upload. Specify one of the following values:  
**Perform SI Update if:**  
1 — if all provisioning activities were successful  
2 — if the corresponding provisioning activity was successful  
3 — always
- **com.jp.ovsi.spml.resourcename.separator=+**  
Select Identity reads data files from the `reconroot` directory. The file name should begin with an underscore ( `_` ). If the property above is set as shown, then the file placed on `reconroot` will begin with a “+.”

## Report Settings

- **com.hp.ovsi.volumedata.report.compressed = true**  
Controls whether reports are compressed before being emailed to recipients.  
`true` = reports are compressed  
`false` = reports are not compressed
- **truaccess.generatedFileSizeLimit=2000000**  
Indicates the size of the files (in bytes) that are generated by the reporting subsystem. This is a soft limit; the actual file size may exceed this by a small amount.
- **truaccess.userdetailconfigrpt.sortattributes=UserName, FirstName, LastName, Email, Company, Department, CostCenter**  
Indicates the column(s) on which sorting takes place in the user detail configuration report and the order of the sort.
- **truaccess.batch.report.file.maxsize = 1000000**  
Specifies the maximum email size of a batch report.
- **com.hp.si.request.report.day=14**  
Specifies the number of days for which request status is retrieved by default in the **From** field of the **Request Status** page. If this property is not specified, the value defaults to **14**.
- **si.volumedata.report.email.limitsize=true**  
Indicates whether or not report size should be limited (hidden, default set to true, limit the report).

## Repository Type Settings

- **truaccess.repository.type=oracle**
- **truaccess.repository.oracle.driver.bea=no**

If you are running Select Identity on WebLogic, connecting to an Oracle database, and using the Thin driver for Oracle 10G (which provides internationalization support), you must set this property to **no**.

## Schema Settings

- **truaccess.AZN.schema.owner=db2inst1.**

Specifies the schema owner for AZN DB Stored Procedures. This value should end with a period (.).

- **truaccess.NEWCO.schema.owner=db2inst1.**

Specifies the schema owner for NEWCO DB Stored Procedures. This value must end with a period (.).

## Search Settings

- **com.hp.si.usersearch.criteria.names.default = UserName,Email,FirstName,LastName,\_status**

Specifies the user search criteria fields. The fields are separated by commas. Use “\_Status” to search for the user state status.

- **com.hp.si.usersearch.criteria.names.additional = \_Status,ServiceName,ResourceName**  
**com.hp.si.usersearch.criteria.names.additional =**  
**City,State,Zip,Country,\_Status,ServiceName,ResourceName**

Determines additional user search criteria fields.

- **com.hp.si.usersearch.result.columns = UserName,FirstName,LastName,Email**

Specifies the order in which the attribute columns display in the search results page. The names are separated by commas. The **UserName** is required.

- **com.hp.si.usersearch.result.max = 300**

Specifies the maximum number of users that can display in a user search.

## Security Framework and Keystore Settings

- **si.keystore.paramfile=C:/Temp/SI40/keystore/keystore.properties**

Set this property to the location of the `keystore.properties` file in the security framework.

- **com.hp.ovsi.encryptdecrypt.algorithm=AES/ECB/PKCS5Padding**

Cipher Algorithm setting, used if the bootstrap keystore has AES keys.

- **com.hp.ovsi.securityfw.repository.type=1**

Security framework repository type: `database=1, XML=0`. Sets the repository type used by the security framework. Currently only 1 (database) is supported.

## Self-Registration Settings

- **com.hp.si.selfreg.schedule=true**  
Specifies whether the **Schedule Time** field in the self-registration form will be visible.
- **com.hp.si.selfreg.instruct = Welcome and thank you for accessing Self-Registration. After completing this page, press "{0}". You will then be asked for additional information. Once you have completed all of the pages, your request will be submitted for processing.**  
Determines the text seen in self-registration instructions.
- **com.hp.ovsi.selfreg.cancel.action.url = http://www.hp.com**  
Specifies the URL used when self-registration is cancelled.

## Server Management Settings

- **server.manager.enable=true**  
Allows you to set the server management properties when set to the default (true).

## User and Account Settings

- **truaccess.disable=true**  
**truaccess.disabledays=1**  
**truaccess.system.terminate.administrator.userId=sisa**  
**truaccess.system.expire\_notification.administrator.userId=sisa**  
Specifies the account disable period before the account is terminated. Set the `truaccess.disable` property to **true** if the user needs to be disabled before termination occurs.
- **si.serviceassign.evaluation=1**  
Specifies whether to evaluate user attributes or service assignments. Specify one of the following values (1 is the default).  
**0— Evaluate all (attributes and service assignments)**  
**1— Skip services previously assigned to users**
- **truaccess.singlevalue.attribute.delete=false**  
Specifies whether a user's single value attributes should be deleted.  
If this is set to `true`, an error will result during a terminate user operation unless the following properties are all set to `false` as shown below:  
**truaccess.singlevalue.attribute.delete.FirstName=false**  
**truaccess.singlevalue.attribute.delete.LastName=false**  
**truaccess.singlevalue.attribute.delete.Email=false**  
**truaccess.singlevalue.attribute.delete.Password=false**
- **truaccess.user.extra=PhBus, PhHome, PhMobile, Company,Department, DOB, Addr1, Addr2, City, State, Zip, Country, CostCenter, ExpirationDate, UserDescription, \_Status**  
**truaccess.user.extra.State.column=State**  
**truaccess.user.extra.City.column=City**  
**truaccess.user.extra.Country.column=Country**  
**truaccess.user.extra.Zip.column=Zip**  
Use the automatic matching feature for PersonNumber  
**truaccess.user.extra.PersonNumber.column=PersonNumber**

Extra attributes associated with users. These settings support null values.

- **com.hp.ovsi.forgetpassword.autogenerate=true**  
Determines if a password is automatically generated for the user if the user indicates the password has been forgotten. If `forgetpassword` is set to true, Select Identity automatically generates a password when the user forgets the password, and provides the correct answers to the Challenge/Response question. If set to false, users must reset their own password.
- **com.hp.ovsi.modify.disableduser=false**  
Select Identity allows modification of a disabled user by default. Set this property to **false** if this should not be allowed.
- **com.hp.si.user.attributes.dropdown.constraint.count=10**  
User Attribute drop-down value count. This property determines if a drop-down list displays or a search is used when a user selects an attribute which contains a constraint list. If the number of constraint values for the attribute is below the property value (such as 50 in the example), a drop-down list will appear on the registration or approval form. If the number of constraint values is equal to or greater than the property value, a search will be required for selecting values from the list.
- **com.hp.ovsi.parentrequestlist.contextcheck=False**  
Returns only those requests that the admin is authorized to view on the Request Status page by default. This is set to false for performance reasons. Change the value to true to enable this behavior.

## Web Service Request Settings

- **com.hp.si.webservice.auth.resource=ldap**  
**com.hp.si.webservice.auth.ldap.accessurl=ldap://localhost:389**  
**com.hp.si.webservice.auth.ldap.uidattr=uid**  
**com.hp.si.webservice.auth.ldap.suffix=ou=People,dc=trulogica,dc=com**  
**com.hp.si.webservice.auth.ldap.needssl=false**  
Specifies external authentication for Web Service requests when uncommented
- **si.recon.webservice.report.generate=2**  
Whether to generate and send report for Web Service reconciliation:
  - 0 - Never
  - 1 - Only Initial Report when no request is processed
  - 2 - always

## Workflow Settings

- **com.hp.ovsi.default.workflowtemplate.bulk.addnewuser**  
**=SIBulkOneStageApproval**  
**com.hp.ovsi.default.workflowtemplate.bulk.addservice**  
**=SIBulkOneStageApproval**  
**com.hp.ovsi.default.workflowtemplate.delegated.addnewuser**  
**=S\ OneStageApproval**  
**com.hp.ovsi.default.workflowtemplate.delegated.addservice=S\ OneStageApproval**  
**com.hp.ovsi.default.workflowtemplate.delegated.modifyuser**  
**=S\ Provisioning\ Only**

```

com.hp.ovsi.default.workflowtemplate.delegated.deleteservice
=SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.disable-service
=SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.enable-service
=SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.moveuser
=SIBulkOneStageApproval
com.hp.ovsi.default.workflowtemplate.delegated.viewservice
=SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.recon.addservice
=ReconciliationDefaultProcess
com.hp.ovsi.default.workflowtemplate.recon.deleteservice
=ReconciliationDefaultProcess
com.hp.ovsi.default.workflowtemplate.self.addnewuser=SI\ OneStageApproval
com.hp.ovsi.default.workflowtemplate.self.addservice=SI\ OneStageApproval
com.hp.ovsi.default.workflowtemplate.self.modifyprofile=SI\ Provisioning\ Only
com.hp.ovsi.default.workflowtemplate.self.viewprofile=SI\ Provisioning\ Only
com.hp.ovsi.default.workflowtemplate.service.change.recon
=SI\ Provisioning\ Only

```

The default workflow templates for User Request Events

The **default.workflowtemplates** are used when you create a new service on the service role page. When a new Service Role is created, all the Request Events have a default Workflow Template, which is derived from the **default.workflowtemplates** settings. The default templates can be deleted on the Service Role and other templates selected, but this setting allows services to be set up with standard defaults.

## XML Mapping File

- **truaccess.userdiscovery.mapping.file=C:/temp/AttributeMapping.xml**

Specifies the location of the XML attribute mapping file for user import.

## B Auditing XML and Client Sample

HP OpenView Select Identity can pass event auditing data to third-party auditing tools (such as HP OpenView Select Audit) as an XML stream. An extensible schema definition (XSD) and a sample Audit Client are packaged with Select Identity.

This appendix describes how to run the Audit Client and provides details of the sequences, types, and elements that are defined in the Select Identity Audit XSD.

This appendix covers the following topics:

- [Processing the Audit XML Stream into a Database](#)
- [Using the Audit Client](#)
- [The Select Identity Audit XSD](#)

The Audit Client is an example program that illustrates how to connect to an application server via JMS and subscribe to the audit XML stream.

The audit XML schema provided can be used to develop an application that interprets the Audit XML stream and presents it in a user-readable format such as a report. The XML stream can be processed into a database, for example, and analyzed using a reporting tool.

The XML stream can also be translated into a Java Object Hierarchy, which must be undertaken using a third party tool. Appropriate development tools are available from several sources, such as Sun Microsystems and Apache.

### Processing the Audit XML Stream into a Database

The steps below provide a brief high-level outline of the process that must be used to translate the Audit XML stream into a format that can be used to build reports in a database:

- 1 Determine in advance how the database schema and tables will be set up and create these so that they are compatible with the converted Java objects.
- 2 Select a third-party tool to map XML to a java object hierarchy and insert the result into the database.
- 3 Map the java objects to the database schema.

### Using the Audit Client

The Audit Client displays the audit stream in a terminal window in real-time. It is located in the `/utilities/auditclient` subdirectory.

The Audit Client consists of the component files listed in the table below:

File or Directory	Purpose
/doc	Contains API documentation in HTML format.
runclient.bat	The batch file used to run the Audit Client
jndi.properties	Connection properties for interfacing with WebLogic
readme.txt	Release notes and other information
auditbroadcastlistener.java	Sample code demonstrating how to connect to the application server and subscribe to the audit stream
auditbroadcastlistener.class	compiled version of the AuditBroadcastListener class
new-audit.xsd	The XML schema definition for Select Identity audit XML
weblogic.jar	The Audit Client Java executable

## Configuring Connection Properties

The Audit Client is configured by default to connect to Select Identity on localhost to receive the audit stream. If you need to connect to a different host, edit the host name in the `jndi.properties` file before running the Audit Client.

## Running the Audit Client

To run the Audit Client, perform the following steps:

- 1 Copy the entire contents of the following directory from the HP OpenView Select Identity product CD into an appropriate subdirectory in your Select Identity install directory:

```
/utilities/auditclient/WebLogic_client
```

- 2 Ensure that WebLogic and HP OpenView Select Identity are running.
- 3 Run the Audit Client batch file by entering the following command at the WebLogic admin server command line:

```
./runclient.bat
```

## Using the Audit Client on IBM WebSphere 6.0.2

For Audit Client to communicate with the Select Identity JMS topic deployed on Websphere 6.0.2, the following requirements must be met:

- The Websphere Application client must be installed on the host where the Audit Client is run.
- The version of the Websphere Application client must match that of the Websphere Application server, as specified below:



- WebSphere Application client 6.0.0.1 works well with WebSphere Application server 6.0.0.1
- WebSphere Application client 6.0.2.x works well with WebSphere Application server 6.0.2.x
- WebSphere Application client 6.0.0.1 does *not* work with WebSphere Application server 6.0.2.x.
- The provider endpoint must be correctly configured for the Select Identity Topic Connection Factory.

Perform the following steps to install and run the Audit Client on IBM Websphere 6.x:

- 1 Install Websphere Application Client 6.0.0.1 on the host where the Select Identity Audit Client will run.
- 2 The WebSphere Application client is bundled with WebSphere Application server 6.0 ND or WebSphere Application server 6.0 base software CD or e-assembly software image. If you have a CD or image, execute the script `launchpad.bat` and click the link to **Launch Installation Wizard for WebSphere Application Clients** to install the Application client.
- 3 Update the Websphere Application Client from 6.0.0.1 to 6.0.2.0.  
This step is essential if the WebSphere Application Server is of version 6.0.2.X. For WebSphere Application Server 6.0.0.1, it is optional.
- 4 Download and unzip the fix pack, which will generate the `updateinstaller` directory.
- 5 Copy the `updateinstaller` into WAS APP client folder and run `update.exe` under `updateinstaller` folder to upgrade WAS App client to 6.0.2.0.
- 6 It is suggested by IBM, though not required for the Audit Client to run, that WebSphere Application client 6.0.2.0 should be updated to 6.0.2.15.
- 7 Set up the provider endpoint for the Select Identity Topic Connection Factory, as follows:
  - a Determine the `SIB_ENDPOINT_ADDRESS` port in Websphere, by navigating to **Servers** → **Application Servers** from the left panel. Click any server on the **OVSIBus**, then click **Ports** under **Communications**.
  - b On the Select Identity Topic Connection Factory **Configuration** page, enter the following value in **Provider Endpoints**:  

```
<host name or IP >:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging
```

 Where:  

```
<host name or IP >
```

 is the name of the host on which the bootstrap server runs.  

```
<SIB_ENDPOINT_ADDRESS>
```

 is the port you found in previous step.  
 Do not specify `localhost` or `127.0.0.1` for `<host name or IP>`.
- 8 Run the Audit Client using the following command:  

```
<from audit_client_dir>\websphere_client\runclient.bat
```

## The Select Identity Audit XSD

Select Identity Auditing data is output in XML form as set out in the Audit XML Schema Definition, named `Audit.xsd`. This file is located on the HP OpenView Select Identity Product CD, under `\utilities\auditClient`.

The sections and tables that follow define the XML elements in the Audit XSD, grouped to show their hierarchical relationships. The Element Reference table provides detailed information about each individual element, since some can belong to more than one complex.

## Event Sequences

Event sequences allow related audit event data elements to be processed as a group. Some elements are optional and others are required.

Sequences can reference one another as element types. Thus, `configChangeSeq` and other sequence names appear in some of the elements as the element type in the same way as integer or string types. For complete detail about the possible contents of event sequences or any other auditing element, refer to the XSD (`audit.xsd`).

The sequences used in Select Identity audit data are listed below, together with the possible child elements:

**configChangeSeq:** Configuration changes

`OVSIAuditConfigChange`

**EntityChangeSeq:** Changes to entities

`entity`

**EventSeq:** The beginning of an event sequence of any type defined in the XSD.

**MembershipSeq:** Changes to service or resource membership

`MembershipType`

**OVSIAuditAttrChangeDataSeq:** Changes to attribute data

`OVSIAuditAttrChangeData`

**PropertySeq:** Changes to properties

`property`

**PropertyValueSeq:** Changes to property values

`entity`

`value`

`name`

`key`

**SvcConfigChangeSeq:** Service configuration changes

`OVSIAuditConfigChange`

**TargetSeq:** The target of the event

`OVSIAuditTarget`

**UserSeq:** User-related changes

`OVSIAuditUser`

**ValueSeq:** Changes to values

value

## Data Types

Child elements of each event sequence are structured according to the types listed in this section. Some of these are simple elements consisting of a single value or string, while others contain multiple child elements.

### AttrChangeData

attrId  
attrName  
oldValue  
newValue  
opType  
sensitiveLevel

### auditType and auditSubType

These are simple type elements that contain a single value indicating the audit type or subtype.

## ConfigChangeType

type  
fieldId  
fieldName  
properties

## EntityType

PropertySeq

## EntityListType

property  
entity

## EventType

adminRole  
auditType  
auditSubType  
adminId  
adminName  
requestMethod  
requestType  
requestId  
parentRequestId  
causeByRequestId  
status  
timestamp  
serviceName  
ctxVarName  
ctxVarValue  
ctxVarId  
auditTargets  
auditUsers  
auditResourceChanges  
auditServiceChanges  
auditAttrs  
auditAdminRoles

auditConnectors  
auditNotifications  
auditExtCalls  
auditRules  
auditWorkflows

## MembershipType

userId  
membershipId  
membershipOperation  
membershipType

## OpType

This is a simple type element that contains a single value indicating the type of operation performed in an audit event.

## PropertyType

delete  
add  
entityChanges

## requestType

This is a simple type element that contains a single value indicating the request type.

## SvcConfigChangeType

type  
serviceId  
serviceName  
fieldId  
fieldName  
properties

## targetType

targetId  
targetName  
targetType

## UserType

primaryId  
primaryName  
userId  
name  
attrChangeDatas  
memberships

## Constraints

The `minoccurs` and `maxoccurs` attributes define the value range for each element:

**MinOccurs=1:** the element is required in an event sequence.

**MinOccurs=0:** the element is optional in an event sequence.

**MaxOccurs=unbounded:** the element can occur any number of times in an event sequence.

**MaxOccurs=1:** the element can occur once only if it is present in an event sequence.

## Element Definitions

The table below provides detailed information about each element.

Element Name	Type	Constraints	Definition
(ConfigChange) Type	Integer		The type of configuration change: TYPE_RESOURCE = 1 TYPE_ADMIN_ROLE = 4 TYPE_EXT_CALL = 5 TYPE_SERVICE = 6 TYPE_SERVICE_CTX = 7 TYPE_SERVICE_ROLE = 8 TYPE_SERVICE_VIEW = 9 TYPE_ATTRIBUTE = 10 TYPE_WORKFLOW = 11 TYPE_RULE = 12 TYPE_NOTIFICATION = 13 TYPE_CONNECTOR = 14
add	PropertyValueSeq	Optional	A property that was added
adminID	String	Required, once per event	The Admin account ID requesting the operation
adminName	String	Optional, once per event	The name of the administrator requesting the operation
adminRole	String	Required, once per event	The role name that authorized the operation
attrChangeData	OVSIAuditAttr ChangeDataSeq	Optional	Affected user attributes/ properties
attrId	Integer	Required, once per event	Attribute ID affected
attrName	String	Required, once per event	Attribute name affected
auditAdminRoles	ConfigChangeSeq	Optional, once per event	Any changes to admin roles
auditAttrs	ConfigChangeSeq	Optional, once per event	Any attribute changes

<b>Element Name</b>	<b>Type</b>	<b>Constraints</b>	<b>Definition</b>
auditConnectors	ConfigChangeSeq	Optional, once per event	Any changes to connectors
auditExtCalls	ConfigChangeSeq	Optional, once per event	Any changes to external calls
auditNotifications	ConfigChangeSeq	Optional, once per event	Any changes to email templates
auditResourceChanges	ConfigchangeSeq	Optional, once per event	Any resource changes
auditRules	ConfigChangeSeq	Optional, once per event	Any changes to rules
auditServiceChanges	SvcConfigChangeSeq	Optional, once per event	Any service changes
auditTargets	Targetseq	Optional, once per event	The target of the request (eg. a user, service, or resource)
auditType	Integer	Required, once per event	UNKNOWN_VAL = 0 APPROVAL_VAL = 1 PROVISIONING_VAL = 2 POST_PROVISIONING_VAL = 3 EXTERNAL_CALL_VAL = 4 RESERVED_1_VAL = 5 RESERVED_2_VAL = 6 RESERVED_3_VAL = 7 RESERVED_4_VAL = 8 RESERVED_5_VAL = 9
auditUsers	UserSeq	Optional, once per event	Users affected by the request
auditWorkflows	ConfigChangeSeq	Optional, once per event	Any changes to workflows
causeByRequestId	Integer	Optional, once per event	If an event was triggered by another event, the ID of the triggering event.
ConfigChangeType	Complex		Details of a configuration change



<b>Element Name</b>	<b>Type</b>	<b>Constraints</b>	<b>Definition</b>
ctxVarId	String	Optional, once per event	For service-specific requests, the context variable ID
ctxVarName	String	Optional, once per event	For service-specific requests, the context variable name
ctxVarValue	String	Optional, once per event	For service-specific requests, the context variable value
delete	PropertyValueSeq	Optional	A property that was deleted
entity		Optional, unbounded	When this change is relative to an entity change the entity for this property
entityChanges	EntityChangeSeq	Optional	A collection of changed items. If you change a resource attribute mapping, each attribute of the resource that change will be included in the entity changes for the property "attrs." Each entity change is similar to a property change.
EntityListType	Complex	Optional	A Group of changed entities
fieldId	Integer	Required	ID of configuration item that changed. i.e. ServiceRole ID, Context ID
fieldName	String	Required	The name of the configuration item that changed, i.e. resource name, service name, rule name
key	String		The key name of the entity
membershipId	Integer	Required, once per event	Affected service or resource IDs
membershipName	String	Required	The name of the service or resource in a membership operation
membershipOperation	Integer	Required	Whether the membership was added or deleted: ADD_VAL = 1 DEL_VAL = 2
memberships	MembershipSeq	Optional	Affected memberships

<b>Element Name</b>	<b>Type</b>	<b>Constraints</b>	<b>Definition</b>
membershipType	Integer	Required	Whether the membership was to a service or resource: RESOURCE_VAL = 1 SERVICE_VAL = 2
name	String	Required	Affected user name
name	String	Required	The name of a changed property
newValue	String	Required	The value to which the attribute was changed.
oldValue	String	Optional	The value that was changed.
opType	Integer	Required	A simple type that contains a value indicating the type of operation: Add_VAL = 1 Change_VAL = 2 Delete_VAL = 3
OVSIAuditAttrChange Data	Complex		Attribute change details.
OVSIAuditUser	UserType	Optional, unbounded	Represents the user affected by the event.
parentRequestId	Integer	Optional, once per event	The ID number assigned to a parent request.
primaryId	Integer	Optional	Primary affected user ID (if affected user ID is secondary).
primaryName	String	Optional	Primary affected user name (if affected user name is secondary).
properties	PropertySeq	Required	The Properties that changed as a result of an operation.
property	propertyType	Required	An individual property that changed as a result of an operation.
PropertyType	Complex	Optional	Property change type
requestID	Integer	Optional, once per event	The ID number assigned to a request

Element Name	Type	Constraints	Definition
requestMethod	Integer	Optional, once per event	The method via which the operation was performed, e.g. API, Web, WebService, File: DELEGATED_API = 1 all requests from UI have value. DELEGATED_WEB whether delegated or self service, name is not precise. DELEGATED_WEB = 2 all requests from web service have value. DELEGATED_WEBSERVICE no matter delegated or self service, name is not precise DELEGATED_WEBSERVICE = 3 RECONCILIATION_FILEUPLOAD = 10 RECONCILIATION_WEBSERVICE = 11 BULK_FILEUPLOAD = 12 BULK_WEBSERVICE = 13; BULK_MOVEUSER = 14; RECONCILIATION_POLLING = 15
requestType	Integer	Optional, once per event	The type of request DELEGATED_REGISTRATION = 1 SELF_REGISTRATION = 2 AUTO_DISCOVERY = 3 RECONCILIATION = 4 SYSTEM = 5 BULK_UPLOAD = 6 PROVISION = 7 SERVICECHANGE_RECONCILIATION = 8
sensitiveLevel	Integer	Optional	Indicates a field that is marked "sensitive."
serviceId	Integer	Required	Service ID of the item that changed
serviceName	String	Optional, once per event	For service-specific requests, the service that initiated the request
serviceName	String	Required	Service name of the item that changed

<b>Element Name</b>	<b>Type</b>	<b>Constraints</b>	<b>Definition</b>
status	Integer	Required, once per event	PENDING_VAL = 1 SUCCESS_VAL = 2 FAILURE_VAL = 3 PARTIAL_SUCCESS_VAL = 4 APPROVED_VAL = 5 APPROVED_CHANGES_VAL = 6 REJECTED_VAL = 7
SvcConfigChangeType	Complex		Specialized form of ConfigChangeType
targetId	Integer	Required	The ID of the target
targetName	String	Required	The name of the target
targetType	Integer	Required	The type of target: USER_NORMAL_VAL = 1 USER_PRIMARY_VAL = 2 USER_SECONDARY_VAL = 3 USER_CLUSTER_VAL = 4 RESOURCE_VAL = 5 SERVICE_VAL = 6 SERVICE_CONTEXT_VAL = 7 SERVICE_ROLE_VAL = 8 SERVICE_VIEW_VAL = 9 ATTRIBUTE_VAL = 10 WORKFLOW_VAL = 11 RULE_VAL = 12; NOTIFICATION_VAL = 13 CONNECTOR_VAL = 14 EXTERNAL_CALL_VAL = 15 ADMIN_ROLE_VAL = 16
TargetType	Complex		Audit operation target details
timestamp	Long Integer	Required, once per event	The time at which the event occurred, relative to server time, expressed as the number of milliseconds since January 1st, 1970.
type	Integer	Required	As for ConfigChangeType
userId	Integer	Required	Affected user ID

## Event Types

Event Type elements indicate the action that occurred in an audit event. The table below lists the possible event types.

<b>Action Type</b>	<b>Action</b>
Service Change Reconciliation	SVCCHG_RECON_MODIFY_USER = 51 SVCCHG_RECON_ADD_RESOURCE = 52 SVCCHG_RECON_DELETE_RESOURCE = 53
Resource Reconciliation	RESOURCE_RECONCILIATION_DELETE = 56 RESOURCE_RECONCILIATION_MODIFY = 57 RESOURCE_RECONCILIATION_REPLACE = 58
User Role Delegation	USER_ROLE_DELEGATION_ACTIVATE = 54 USER_ROLE_DELEGATION_DEACTIVATE = 55

<b>Action Type</b>	<b>Action</b>
User Request	ADD_NEW_USER = 1 MODIFY_USER = 2 DELETE_SERVICE_MEMBERSHIP = 3 ENABLE_ALL_SERVICES = 4 DISABLE_ALL_SERVICES = 5 RESET_PASSWORD = 6 COPY_USER = 7 ADD_SERVICE = 8 CHANGE_PASSWORD = 9 FORGET_PASSWORD = 10 ENABLE_SERVICE_MEMBERSHIP = 11 VIEW_SERVICE_MEMBERSHIP = 12 TERMINATE_USER = 13 MANAGE_USER_EXPIRATION = 14 DISABLE_SERVICE_MEMBERSHIP = 15 SECURITY_VIOLATION = 16 MODIFY_PROFILE = 17 PASSWORD_EXPIRE_NOT = 18 MOVE_USER = 19 LOGIN = 20 LOGOUT = 21 IMPORT = 22 EXPIRE_PASSWORD = 24 HINTSETUP = 30 DISABLE_TERMINATE = 31 REVERT_MODIFY = 32 REVERT_ADD = 33 REVERT_DELETE = 34 IGNORE_ADD = 35 IGNORE_MODIFY = 36 IGNORE_DELETE = 37
Cluster Operations	CREATE_CLUSTER = 40 MODIFY_CLUSTER = 41 DELETE_CLUSTER = 42 ADD_SECONDARY = 43 REMOVE_SECONDARY = 44

<b>Action Type</b>	<b>Action</b>
Service	SERVICE_CREATE = 2000 SERVICE_DELETE = 2001 SERVICE_MODIFY = 2002 SERVICE_COPY = 2003 SERVICE_SET_ATTR_VALUES = 2004 SERVICE_SET_ATTR_PROPS = 2005 SERVICE_VIEW_CREATE = 2006 SERVICE_VIEW_DELETE = 2007 SERVICE_VIEW_MODIFY = 2008 SERVICE_ROLE_CREATE = 2009 SERVICE_ROLE_DELETE = 2010 SERVICE_CONTEXT_CREATE = 2011 SERVICE_CONTEXT_DELETE = 2012 SERVICE_CONTEXT_MODIFY = 2013 SERVICE_IMPORT = 2014 SERVICE_ROLE_MODIFY = 2015 SERVICE_EXPORT = 2016
Resource	RESOURCE_CREATE = 3000 RESOURCE_DELETE = 3001 RESOURCE_MODIFY = 3002 RESOURCE_VIEW = 3003 RESOURCE_COPY = 3004 RESOURCE_ATTR_VIEW = 3005 RESOURCE_ATTR_MODIFY = 3006 RESOURCE_IMPORT = 3007 RESOURCE_EXPORT = 3008
Attribute	ATTRIBUTE_CREATE = 4000 ATTRIBUTE_DELETE = 4001 ATTRIBUTE_MODIFY = 4002 ATTRIBUTE_VIEW = 4003 ATTRIBUTE_COPY = 4004 ATTRIBUTE_IMPORT = 4005 ATTRIBUTE_EXPORT = 4006
Workflow	WORKFLOW_CREATE = 5000 WORKFLOW_DELETE = 5001 WORKFLOW_MODIFY = 5002 WORKFLOW_VIEW = 5003 WORKFLOW_COPY = 5004 WORKFLOW_IMPORT = 5005 WORKFLOW_EXPORT = 5006

<b>Action Type</b>	<b>Action</b>
External Call	EXT_CALL_CREATE = 6000 EXT_CALL_DELETE = 6001 EXT_CALL_MODIFY = 6002 EXT_CALL_VIEW = 6003 EXT_CALL_COPY = 6004
Notification	NOTIFICATION_CREATE = 7000 NOTIFICATION_DELETE = 7001 NOTIFICATION_MODIFY = 7002 NOTIFICATION_VIEW = 7003 NOTIFICATION_COPY = 7004 NOTIFICATION_IMPORT = 7005 NOTIFICATION_EXPORT = 7006
Connectors	CONNECTOR_CREATE = 8000 CONNECTOR_DELETE = 8001 CONNECTOR_MODIFY = 8002
Rules	RULE_CREATE = 9000 RULE_DELETE = 9001 RULE_MODIFY = 9002
Admin Roles	ADMINROLE_CREATE = 10000 ADMINROLE_DELETE = 10001 ADMINROLE_MODIFY = 10002















# Index

## A

- Account Change Report, 92
- Account Events Report, 92
- activation specifications, 46
- Admin Configuration, 103
- administrator, 13
- Administrator Report, 92
- Admin Logged Out, 102
- Admin Login Error, 102
- agent
  - Select Audit, 89
- agent-based connectors, 16
- API, Service Desk, 80
- application
  - status, 106
  - undeploying, 106
- application settings, WebSphere, 49
- approvals, 119
- Architecture, 14
- Audit
  - Data Types, 123
  - event sequences, 122
- audit and configuration reports, 91
- AuditCfgEntry table, 90
- Audit Client, 119
  - jndi.properties file, 120
  - using, 119
  - XSD, 122
- Audit data
  - Java Object Hierarchy, 119
- audit data stream, 89
- audit events, 93
- auditing, 15
- Audit User Hint, 101
- Audit User Login, 102
- Audit User Password, 101
- authentication, 15

- Authority, tiered, 15

## B

- bootstrap keystore, 56
- browser version, 21
- bus destinations, 42
- Business Process Services, 14

## C

- Caller field, 83
- category
  - service call, 82
- Certification Authorities, 15
- Change/Reset Password, 82
- Change History Report, 92
- Change Password, 100
- Class Loading Mode, 50
- clusters
  - required for WebSphere, 27
- compliance auditing, 89
- configuration reports, 89
- configuring
  - recommended, 59
  - TruAccess.properties, 53, 107
  - TruAccess.properties required settings, 53
- connection factory
  - queue, 43
  - topic, 44
- connection pool, 41
- connectors, 16
- context, 89, 91
- Context Engine, 14
- context management, 14
- cookies, 21
- CORBA Naming Service Groups, 51
- Customer Service Representative, 80
- custom external keystores, 27

- custom field, 82
- custom fields
  - Service Desk, 83
- D**
- database, 13, 89
  - and Select Audit, 90
  - configuring, 27
  - user accounts, 26
- database access control, 15
- database rules
  - Service Desk, 84
- database rules, Service Desk, 81
- database server, 27
- database user login, 27
- data filtering, 91
- data sources, 40
- data store
  - helper class, 41
- delegated password change, 80
- delegated request, 81
- delegation, 15
- Description field, 83
- Destination JNDI Name, 46
- destinations, 42
- Destination Type, 46
- directory naming, 26
- Display Format, 81
- dml file, 89
- documentation, 26
- domains
  - Select Identity and Select Audit, 89

- E**
- EAR file, 49
- Emailed report format, 70
- embedded spaces, 26
- encryption, 15
  - PC1, 16
  - SHA, 15
- encryption keys, 27
- Endpoints, 46
- entitlements, 14, 15
- Error Changing Password, 100

- event auditing data, 119
- event history, 15
- events
  - audit, 93
- Expire Password Notification, 100
- extensible schema definition
  - XSD, 119

- F**
- firewall ports, 21
- form,default, 83
- Forms, 15

- G**
- general settings, 53
- generic JVM Arguments, 50

- H**
- Hardware Security Modules, 15
- high message threshold, 41
- Hint Setup, 101
- Host aliases, 25, 52
- HSM, 15
- HTTP, 13
- HTTP transport port, 52

- I**
- IBM HTTP Server, 25
- IBM WebSphere - ND, 20
- Information, 83
- install.bin, 28
- install\_trace.log, 27
- InstallAnywhere installer, 28
- installation
  - logging, 27
  - remote, 28
- installation process summary, 19
- installer
  - Select Audit, 91
- installing:WebSphere installation wizard for standalone server, 28
- interface settings, 53
- internationalization, 16, 66
  - UTF-8 encoding on Oracle10G, 68



interoperation, 89

IP address, 27

## J

J2EE Connector Architecture, 16

JAAS Configuration, 39

Java

Object Hierarchy, 119

Java 2 security, 51

Java Messaging Service. *See*

Java Naming and Directory Interface, 16

javascript, 21

JCA, 16

JDBC driver, 20, 40

JDBC port, 21

JDBC Provider, 40, 41

JMS

Activation Specification, 45

and Audit Client, 119

database user, 27

database user account, 26

data source, 41

data store, 42

default messaging, 45

queue, 43

queue connection factory, 43

queues, 44

resources, 43

topic, 43

topic connection factory, 44

topics, 45

JMS cluster, 41, 43

JMS clustering, 27

JMSDB\_LOGIN\_USER, 43

JMS user, 24

JNDI, 16

JNDI Name, 42

JNDI resource provider interface, 16

JVM arguments, 50

JVM Logs, 51

## K

keystore, 56

keystore parameter file, 27

keystores, 15

## L

language fonts, 70

language media kit, 19

LDAP, 16

LDAPS, 16

local\_policy.jar, 26

localization, 66

localized version, 19

log files

tail, 27

logging

WebSphere, 50

Logging and Tracing, 50

Logging Config Change, 103

logging in

WebSphere, 51

logical identity, 13

login page, 70

## M

Mail Provider, 47

mail session, 47

Mail Sessions, 47

managed service, 89

Max Connections field, 44

maximum connections, 41

Microsoft Internet Explorer, 21

migration, 73

minimum requirements, 20

## N

Network Deployment Manager, 26

Network File System, 27

installation directory, 26

NFS, 26

Notepad, 53

Number Field, 81

## O

ojdbc14.jar, 26

online help, 27

deployment, 49

operating system login, 28

- operating system login ID, 27
- Oracle
  - internationalization encoding, 68
  - uninstalling, 106
- Oracle10g data store helper, 41
- Oracle 10g JDBC driver, 40
- Oracle 10g requirements, 20
- oracle\_concero\_ddl.sql, 24
- Oracle data sources, 40
- Oracle Technology Network, 74
- Oracle thin driver, 26
- Oracle thin driver archive, 27
- Oracle Thin Driver Version, 20
- OVSD-OVSI integration Template, 83
- OVSIAApplication, 48
- OVSIAuditBroadcast, 42, 45
- OVSIAuditProcQ, 42, 44, 46
- OVSIBulkQueue, 42, 44, 46
- OVSIBus, 43, 44, 45, 46
- OVSibus
  - security setting, 51
- OVSICacheTopic, 42, 45
- OVSICChangeReconProcessorQueue, 42, 44, 46
- OVSI cluster, 44
- OVSI DataSource, 40
- OVSIEntCacheQueue, 42, 44, 46
- OVSI Mail Session, 47
- OVSIMessageAckQueue, 42, 44, 46
- OVSI Oracle10g, 40
- OVSI Oracle10g\_JMS, 41
- OVSI Password Management with OVSD, 87
- OVSIREconQueue, 42, 44, 46
- OVSIResReconDispatcherQ, 42, 44, 46
- OVSIResReconQ, 42, 44, 46
- OVSISaudQ, 42, 45, 46
- OVSISchedulerQueue, 42, 45, 46
- OVSIServiceAssignQueue, 42, 45, 46
- OVSITCF, 44
- OVS IUserImportPQueue, 42, 45, 46
- OVS IWfRequestExpireQueue, 42, 45, 46
- OVS IWorkflowQueue, 42, 45, 46

## P

- Parent field, 82
- Parent Last, 50
- Password, 100
- Password Management Report, 93
- password management request, 80
- Password Policy change, 100
- password request, link, 85
- Password Reset Config Change, 101
- policy files, 26
- ports
  - firewall, 21
- private key, 15
- privileges, 13
- processes
  - starting and stopping, 28
- profiles, 15
- protocol providers, mail, 47
- provisioning workflow, 15
- proxy server, 26
- public key, 15

## Q

- qualifications for installing, 16
- queue connection factory, 43

## R

- Received Login request, 101
- Received Logout request, 101
- reconciliation, 15
- Red Hat Enterprise Linux v3, 20
- report access
  - Select Audit, 91
- reporting, 15
- report mapping, 92
- report type, 93
- Request Failure Description, 83
- Request Failure Description field, 82
- Request ID, 83
- request ID, 81
- Request ID, 81
- request link, 84, 85
- Request Link,, 83

- Request Link field, 82
- request status, 81, 85
- Request Status Page, 81
- Request Status page, 81
- Request Type, 83
- Request Type field, 82
- Reset Password, 100
- Reset Password Service Call, 79
- resource connector, 16
- Resources, 14
- role, 91
- roles
  - service, 14

**S**

- Sc. Text 1 field, 82
- Sc. Text 2 field, 82
- schema, 13, 19
  - XML, 119
- schema, Select Identity, 24
- schema name, 43
- scope, 47
  - cluster, 43, 44
  - server, 43, 44
- SDIntegrator external call, 80, 86
- SDK, 16
- security, 15
  - Java 2, 51
  - WebSphere console, 26
- Security Events Report, 93
- Security Framework, 27
- security framework, 26, 51
- SelectAccess, 102
- Select Audit, 92, 103
  - data filtering, 91
  - viewing configuration reports, 89
- Select Audit connector,, 89
- Select Audit Report Config, 103
- SelectFederation, 102
- Select Identity
  - launching, 51
- Select Identity schema, 19
- Self-Registration, 70
- self-service request, 81

- Sent Login request, 101
- Sent Logout request, 101
- Ser. ShortText 1 field, 82
- sers, 14
- server settings, 53
- Service Call, 81
- service call, 79
- service call,category, 82
- service call, link, 85
- Service Call Category, 82
- Service Call Category field, 81
- service call status, 83
- service call template, 81
- Service Desk
  - database rules, 84
  - smart action, 81
- Service Desk integration
  - configuring in Select Identity, 86
- Service Desk Integration, context, 87
- Service Desk Integration, process flow, 87
- Service Level Agreements, 79
- Service Report, 93
- Service Roles, 14
- services, 14, 89
- SF Admin Logged Out, 102
- SHA, 15
- short string field, 82
- SLAs, 79
- smart action, 85
- SMTP email host, 27
- SMTP protocol provider, 47
- Source ID field, 83
- SQL Plus, 23
- SSH, 16
- SSL, 15, 16
- State field, 83
- Status field, 83
- string field, 82
- System Activity Report, 93
- SystemOut.log, 27

**T**

- tablespace, 24

- TAUser table, 60
- Telnet, 16
- template
  - service call, 83, 87
- Terminate User, 99
- Text field, 82, 83
- tickets, Service Desk, 79
- topic connection factory, 44
- topics, 45
- topology, 25
  - bus members, 41
- TruAccess.properties, 53, 86
  - configuring, 107
  - configuring required settings, 53
  - Select Audit, 90
  - settings, 107
- TruAccess\_JMS, 42

## U

- Uninstalling, 105
- unlimited strength policy files, 26
- upgrade Select Identity, 73
- URL
  - login, 51
- US\_export\_policy.jar, 26
- user account, 27
  - JMS, 24
  - Select Identity, 23
- user accounts, 13
  - Select Audit, 91
- User Activity Report, 93
- users, 89
- User Search criteria, 71
- User Summary Report, 93
- UTF-8 encoding, 69

## V

- Vi, 53

## W

- WAR class loader policy, 49
- WAR file, 27, 49
- WAS6\_LMZ.ear, 49
- webapi.jar, 79
- Web Application Archive, 27

- Web application server
  - performance, 20
  - upgrade requirements, 73
- web application server, configuring WebLogic, 26
- WebSphere, 24
  - preparing to install SI, 26
  - starting, 27
- WebSphere admin server
  - IP and host name, 27
- WebSphere install:installation wizard, 28
- Workflow, 102
- workflow, 80, 87
- WorkflowChangeRequest approved, 101, 103
- WorkflowChangeRequest rejected, 101
- WorkflowChangeRequest reverted, 101, 103
- WorkflowChangeRequest submitted, 101, 102, 103
- WorkflowConfigChange, 101, 102
- Workflow copy, 101, 103
- Workflow create, 101, 103
- Workflow delete, 101, 103
- Workflow Events Report, 93
- Workflow export, 101, 103
- Workflow import, 100, 101, 103
- Workflow modify, 101, 103
- Workflow Studio, 15, 83
- Workflow Studio online help, 80
- Workflow Studio Service Desk Template, 80
- Workflow view, 101, 103

## X

- XML, 16, 89
- XML stream, 119