

# HP OpenView Select Identity

For the Red Hat Enterprise Linux,  
HP-UX 11i, and  
Windows 2003 Server Operating Systems

Software Version: 4.01

---

## Installation Guide

May 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

© Copyright 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.

HP OpenView 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 HP OpenView 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.

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

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

## Support

Please visit the HP OpenView support web site at:

**<http://www.hp.com/managementsoftware/support>**

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

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

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

## Preface

Welcome to the *HP OpenView Select Identity Installation Guide*. This guide provides all installation prerequisites, system requirements, and procedures. Specific product configuration and logging settings are included. This guide also includes uninstall and troubleshooting information.

### About This Guide

The *HP OpenView Select Identity Installation Guide* is designed to help you install and manage HP OpenView Select Identity based on your system criteria.

### Audience

This document is intended for system administrators who are installing HP OpenView Select Identity. This guide provides detailed procedures for installing and configuring the Select Identity system.

### Typographical Conventions

This guide uses the following typographical conventions:

Convention	Description
<b>Bold</b>	Used for user interface elements (menus, buttons, and so on), new terms, and URLs.
<i>Italics</i>	Used for variables, book titles, and emphasis.
Monospacing	Used for code examples, directory and file names, commands, and user input.

### Product Documentation

The Select Identity product documentation includes the following:

- Release notes are provided in the top-level directory of the HP OpenView Select Identity CD. This document provides important information about new features included in this release, known defects and limitations, and special usage information that you should be familiar with before using the product.

- Detailed procedures for deployment and system management are documented in the *HP OpenView Select Identity Administrator Guide* and Select Identity online help system. This guide provides detailed concepts and procedures for deploying and configuring the Select Identity system. In the online help system, tasks are grouped by the administrative functions that govern them.
- The *HP OpenView Select Identity My Identity User Guide* provides detailed information for end-users about the My Identity function, which allows users to manage their identity information.
- The *HP OpenView Select Identity Workflow Studio Guide* provides detailed information about using Workflow Studio to create workflow templates. It also describes how to create reports that enable managers and approvers to check the status of account activities.
- An *HP OpenView Connector Installation and Configuration Guide* is provided for each resource connector. These are located on the Select Identity Connector CD.
- The *HP OpenView Select Identity Attribute Mapping Utility User's Guide* describes how to access the Attribute Mapping Utility, provides an overview to the utility's user interface, and describes how to define user and entitlements mappings. This guide is provided on the Select Identity Connector CD and is for use with the SQL and SQL Admin connectors only.
- The *HP OpenView Select Identity External Call Developer Guide* provides detailed information about creating calls to third-party applications. These calls can then be deployed in Select Identity to constrain attribute values or facilitate workflow processes. In addition, JavaDoc is provided for this API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/external_calls/Javadoc` directory on the Select Identity CD.
- If you need to develop connectors, which enable you to connect to external systems for provisioning, refer to the *HP OpenView Select Identity Connector Developer Guide*. This document provides an overview of the Connector API and the steps required to build a connector. This guide also describes the Web Service, which enables you to programmatically provision users in Select Identity, providing an overview of the operations you can perform through use of the Web Service, including SPML examples for each operation. The audience of this guide is developers familiar with Java.

JavaDoc is also provided for the Connector API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/connectors/Javadoc` directory on the Select Identity CD. Also, an independent, web-based help system is available for the Web Service API. To view this help, double-click the `index.htm` file in the `docs/api_help/web_service/help` directory on the Select Identity CD.





---

# Contents

<b>1</b>	<b>Welcome to HP OpenView Select Identity</b> .....	<b>1</b>
	Introduction .....	1
	System Architecture .....	1
	Security and Communication .....	4
	Internationalization .....	5
	Technical Qualifications for Installing Select Identity .....	6
<b>2</b>	<b>System Requirements</b> .....	<b>7</b>
	Installation Process Overview .....	7
	Reviewing Minimum Recommendations .....	8
	Supported Configurations .....	8
	Installation to Directories with Embedded Spaces .....	9
	Database Server Requirements .....	9
	BEA WebLogic Server Requirements .....	10
	IBM WebSphere Server Requirements .....	11
	Select Identity Interface Requirements .....	12
	Ports Required for Firewall Configuration .....	12
<b>3</b>	<b>Configuring the Database Server</b> .....	<b>13</b>
	Oracle Database Configuration .....	13
	Configuring an MS SQL Database Server .....	15
<b>4</b>	<b>Installing Select Identity on BEA WebLogic</b> .....	<b>19</b>
	Introduction .....	19
	Single or Clustered Server Installation .....	20
	Select Identity Installation Requirements .....	20
	Important Installation Information .....	20
	Prerequisite Configuration Procedure .....	21

Editing the Default startWebLogic Script on a Single-Server Installation . . . . .	23
Select Identity Installer Process Summary . . . . .	23
Select Identity Installer Procedure . . . . .	25
Validating the Installation . . . . .	34
Restarting WebLogic After Installing Select Identity . . . . .	35
Select Identity Manual Installation Procedure . . . . .	35
Creating Select Identity Directories and Copying Installation Files . . . . .	36
Creating the myStartWL Script on a Single Server . . . . .	38
Starting WebLogic . . . . .	40
Configuring the Mail Session . . . . .	41
Configuring JMS Settings . . . . .	42
Configuring New JMS Connection Factories . . . . .	43
Configuring a JMS File Store . . . . .	45
Configuring a JMS Server . . . . .	47
Creating the JMS Queues on a Single Server . . . . .	50
Configuring JMS Queues on a Clustered Server . . . . .	53
Configuring the JMS Audit Queues on a Clustered Server . . . . .	56
Configuring JMS Topics on a Clustered Server . . . . .	56
Creating the JMS Topics on a Single Server . . . . .	57
Creating JMS Server Members . . . . .	58
Modifying the JMS Template for JMS Queues and Topics . . . . .	61
Configuring a JDBC Connection Pool . . . . .	63
Configuring the JDBC Data Source . . . . .	67
Modifying the WebLogic Server Class Path . . . . .	69
Configuring the Select Identity Execute Queues . . . . .	72
Enabling Anonymous Admin Lookup . . . . .	74
Starting the WebLogic Server . . . . .	75
Deploying Select Identity on WebLogic . . . . .	75
Additional Configuration . . . . .	79
Configuring the JTA Settings . . . . .	79
Deploying the Select Identity Online Help Files . . . . .	79
<b>5 Installing Select Identity on IBM WebSphere . . . . .</b>	<b>81</b>
Introduction . . . . .	81
Important Installation Information . . . . .	81
Prerequisite Configuration Procedure . . . . .	82

Installation to Directories with Embedded Spaces . . . . .	83
Configuration Steps . . . . .	83
Using the Select Identity Installer . . . . .	84
Installation Wizard Procedure . . . . .	85
For Clustered Servers . . . . .	92
Manual Installation Procedures . . . . .	95
Creating Directories and Copying Files . . . . .	96
Configuration Scope . . . . .	97
Creating a Select Identity Mail Session . . . . .	97
Creating a J2C Authentication Data Entry . . . . .	101
Cluster Configurations . . . . .	101
Standalone Server Configurations . . . . .	103
Deploying the JDBC Provider and Data Source for Oracle . . . . .	104
Configuring Server Components . . . . .	109
Configuring the Generic JVM Arguments . . . . .	111
Configuring a JMS Queue Factory . . . . .	113
Configuring a JMS Topic Factory . . . . .	115
Creating the JMS Queues . . . . .	117
Creating JMS Topics . . . . .	120
Configuring the Application Server . . . . .	122
Configuring the Message Listener Service . . . . .	122
Deploying Select Identity . . . . .	124
Configuring Logging for Select Identity . . . . .	126
Logging In to Select Identity on IBM WebSphere . . . . .	127
<b>6 Configuring HP OpenView Select Identity . . . . .</b>	<b>129</b>
Configuring TruAccess.properties Required Settings . . . . .	129
Setting the Database Repository Property . . . . .	129
Additional Required Settings . . . . .	130
Generating a Custom Keystore . . . . .	131
Creating the Custom Keystore . . . . .	132
Integrating the Keystore with Select Identity . . . . .	133
Recommended Configuration . . . . .	135
Custom User Interface Properties . . . . .	135
How to Set Properties . . . . .	136
User Interface Sections . . . . .	136

Customization Properties . . . . .	137
Default Properties . . . . .	139
Internationalization and Localization . . . . .	140
Configuration for Specific Environments or Platforms . . . . .	141
Tuning the WebLogic Application and Database Servers . . . . .	141
Optimizing JMS Distributed Queues and Weblogic Execute Queues . . . . .	141
Tuning the Database Server . . . . .	143
UTF-8 Encoding on Oracle 10G . . . . .	144
iPlanet LDAP Configuration . . . . .	144
Set Encoding in Internet Explorer . . . . .	145
Adding Supported Language Fonts . . . . .	145
Additional Configuration Options . . . . .	146
<b>7 Upgrading Select Identity . . . . .</b>	<b>149</b>
Upgrading from Versions Prior to 3.3.1 . . . . .	149
Upgrading from Version 3.3.1 to 4.0 . . . . .	149
Preparing to Upgrade . . . . .	150
Downloading the Oracle JDBC driver . . . . .	150
Stopping Select Identity Traffic . . . . .	151
Preparing the WebLogic Server . . . . .	151
Modifying Resources . . . . .	153
Preliminary Migration Steps . . . . .	154
Running the Migration Script . . . . .	155
Troubleshooting . . . . .	155
Command Line Options . . . . .	156
<b>8 Uninstalling HP OpenView Select Identity . . . . .</b>	<b>157</b>
Using the Wizard to Uninstall from the WebLogic Server . . . . .	157
Manually Uninstalling from the WebLogic Server . . . . .	157
Manually Uninstalling WebLogic . . . . .	158
Deleting the EAR File . . . . .	158
Deleting the Connectors . . . . .	158
Deleting the Data Source . . . . .	159
Deleting the Connection Pool . . . . .	159
Deleting the Mail Session . . . . .	159
Uninstalling the Select Identity Database . . . . .	160

<b>A</b>	<b>Logging</b>	161
<b>B</b>	<b>Troubleshooting</b>	165
	General Installation Errors	165
	System Errors on WebLogic	167
	Migration Errors	168
<b>C</b>	<b>Configuring TruAccess.properties</b>	169
	TruAccess.properties Settings	169
	General Settings	169
	Asynchronous Provisioning Delay	171
	Audit Settings	171
	Authentication Settings	171
	Auto User Import Settings	172
	Batch Processing Settings	172
	Bulk Upload Settings	173
	Cache Settings	173
	Connector Schema Directory	174
	Email Settings	174
	Execution Retry Settings	175
	External Calls Settings	176
	JNDI Data Source Settings	176
	Keystore Settings	176
	Localization Settings	176
	Notification Event Settings	177
	Operations Templates	177
	Page Redirect Timeout	177
	Reconciliation Settings	177
	Report Settings	179
	Repository Type Settings	180
	Schema Settings	180
	Search Settings	180
	Self-Registration Settings	181
	Server Management Settings	181
	User and Account Settings	181
	Web Service Request Settings	183

Workflow Settings . . . . .	183
XML Mapping File . . . . .	184
Attribute Mapping for Search Efficiency . . . . .	184
<b>Index</b> . . . . .	<b>187</b>

---

# 1 Welcome to HP OpenView Select Identity

This section covers the following topics:

- Introduction
- System Architecture
- Security and Communication
- Internationalization

## Introduction

HP OpenView Select Identity (OVSI) is the first truly scalable solution for managing identity within and between large enterprises. It is the most comprehensive identity management system available.

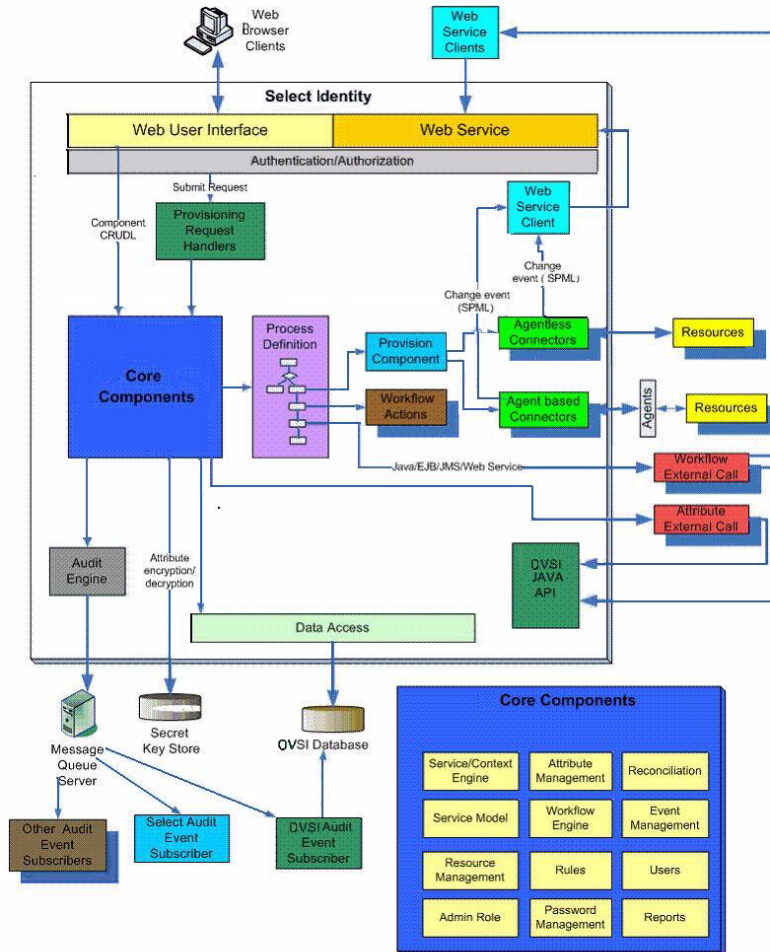
This guide provides instructions for installing Select Identity onto an existing WebLogic or WebSphere application server. It also provides information about how to configure a database server and load the schema used with Select Identity.

For detailed information about using Select Identity, refer to the *HP OpenView Select Identity Administrator's Guide*.

## System Architecture

Figure 1 provides a high-level view of the Select Identity system and its components.

**Figure 1 HP OpenView Select Identity Architecture.**



All requests to and from the system use the HTTP protocol. Select Identity manages a single, logical identity for each user and administrator. These logical identities are mapped to the users' various accounts on back-end systems and services. The 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 that are defined by an administrator based on the access requirements of the company's products and services.



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

- **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.

- **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.

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.

## 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-1 hash. 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.

Select Identity also enables you to generate a keystore, which encrypts and decrypts application data. A keystore is a file that contains security information such as public and private keys, and certificates of trusted Certification Authorities. The private keys are associated with a certificate chain, which authenticates the corresponding public key. By generating the keystore, you add another layer of security to the data that is exchanged in Select Identity. See [Generating a Custom Keystore](#) on page 131 for details.

The connectors that enable you to provision users in external resources are built using JCA (J2EE Connector Architecture) and run within the WebLogic server on which Select Identity relies. Communication between Select Identity and the connectors is internal to the WebLogic 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 and Configuration 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 on WebLogic and Oracle is supported as its database 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 140.

# 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 terminal emulator or other method used to access the server command line
- Database administration skills
- BEA WebLogic or IBM WebSphere Server installation and administration training

---

## 2 System Requirements

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

This chapter covers the following topics:

- [Installation Process Overview](#)
- [Reviewing Minimum Recommendations](#)
- [Installation Process Overview](#)
- [Database Server Requirements](#)
- [BEA WebLogic 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 database and load the Select Identity schema (see [Configuring the Database Server](#) on page 13).
- 3 Configure the Web Application server for use with Select Identity (For BEA WebLogic, see [Prerequisite Configuration Procedure](#) on page 21).
- 4 Install Select Identity (see [Installing Select Identity on BEA WebLogic](#) on page 19).

- 5 Generate a keystore and configure the Select Identity server; perform this optional procedure if you wish to encrypt and decrypt two-way data in Select Identity using your keystore (see [Generating a Custom Keystore](#) on page 131).
- 6 Configure the `TruAccess.properties` file for your environment (see [Configuring HP OpenView Select Identity](#) on page 129 for required and recommended `TruAccess.properties` settings).

## Reviewing Minimum Recommendations

The minimum recommendations vary in some circumstances. Examine your specific environment and adjust or correct any aspect that could affect the performance of the WebLogic 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 4.01 is supported on the following configurations:

<b>Web Server</b>	<b>Platform</b>	<b>Database</b>
BEA WebLogic Server 8.1.5	Red Hat Enterprise Linux v3	Oracle 10G
BEA WebLogic Server 8.1.5	Windows 2003 Server	Oracle 9i
BEA WebLogic Server 8.1.5	Windows 2003 Server	MS-SQL 2000
IBM WebSphere 5.1.1.7	Windows 2003 Server	Oracle 9i
IBM WebSphere 5.1.1.7	HP-UX 11i	Oracle 9i

## Installation to Directories with Embedded Spaces

Installation of Select Identity to a directory with embedded spaces is not recommended.

## 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 server, for optimal performance and ease of management.

The following table provides the *minimum* requirements for database servers to support Select Identity, and the recommended configuration for target systems.

<b>Oracle 10g</b>	
Version	Oracle Database, version 10g
Operating System	Red Hat Enterprise Linux v3
Processor	Minimal Processor: 330 MHz
Memory (RAM)	512 MB of physical RAM 1 GB of swap space (or twice the size of RAM)
Disk space	3.5 GB
JDBC driver*	Oracle Thin Driver Version 10.1.0.4 (oracle.jdbc.OracleDriver)

<b>Oracle 9i</b>	
Version	Oracle Database, version 9i
Operating System	Microsoft Windows 2003
Processor	Minimal Processor: 330 MHz

<b>Oracle 9i</b>	
Memory (RAM)	512 MB of physical RAM 1 GB of swap space (or twice the size of RAM)
Disk space	3.5 GB
JDBC driver*	Oracle Thin Driver Version 10.1.0.4 (oracle.jdbc.OracleDriver)

<b>MS-SQL</b>	
Version	MS-SQL Server 2000, Enterprise Edition
Operating System	Windows Server 2000 with service pack 3 Windows Server 2003, Standard Edition SP3 Windows Server 2003, Enterprise Edition SP3 Windows Server 2003, Datacenter Edition SP3
Processor	Intel Pentium or compatible, 166 megahertz (MHz) or higher processor
Memory (RAM)	Enterprise Edition: 512MB RAM; 1024MB recommended
Disk space	95 - 270 MB of available hard disk space for the server; 250 MB for a typical installation
JDBC driver*	BEA MS SQL Server Type 4 driver, class name: weblogic.jdbc.sqlserver.SQLServerDriver

## BEA WebLogic Server Requirements

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

- Install the WebLogic 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



<b>BEA WebLogic</b>	
<b>Version</b>	BEA WebLogic Server, v8.1, sp5
<b>Operating System</b>	Red Hat Enterprise Linux v3
<b>Processor</b>	1 GHz CPU
<b>Memory (RAM)</b>	512 MB RAM (minimum) 1 GB RAM (recommended)
<b>Disk space</b>	Approximately 820MB of disk space

## 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.

<b>IBM WebSphere</b>	
<b>Version</b>	IBM WebSphere 5.1.1.7
<b>Operating System</b>	Windows 2003 Server (Standard, Enterprise, and DataCenter editions) HP-UX 11i V1 (PA-RISC)
<b>Processor</b>	1 GHz CPU
<b>Memory (RAM)</b>	768 MB RAM (minimum) 1 GB RAM (recommended)
<b>Disk space</b>	Approximately 820MB of disk space

# Select Identity Interface Requirements

The Select Identity user interface requires Microsoft Internet Explorer (IE), version 5.5 or higher, with JavaScript and cookies enabled. No installation steps are required to install the Select Identity 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:
  - 7001 for WebLogic

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
  - 1433 for MS-SQL 2000

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 for the target resource to determine what the standard communication port is for each.



If you are installing on a server cluster, each of the servers in the cluster may use different HTTP ports. This may require a firewall. HP recommends that you configure a web server to mask the web container ports.

# 3 Configuring the Database Server

This chapter describes how to create a database and user account that Select Identity uses 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

You create a 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 is an example command to create 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;
```

Where <tablespace\_name> is the chosen name for the Select Identity tablespace. You reference this name when creating the database user.

This creates 10MB of tablespace then automatically extends the tablespace as needed.

3 Create a user for Select Identity to access the tables:


```
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>;
```

If you are installing on an Oracle 10G database, add the following command after you create the user:

```
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, [Step 5](#), 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 Change to the new user by entering the following command:

```
CONNECT user_name/password
```

5 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.

- 6 Insert the required default data into the Select Identity database:
  - a Copy the data creation script from the HP OpenView Select Identity Product 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.

## Configuring an MS SQL Database Server

Create a database for use by Select Identity by running SQL scripts.



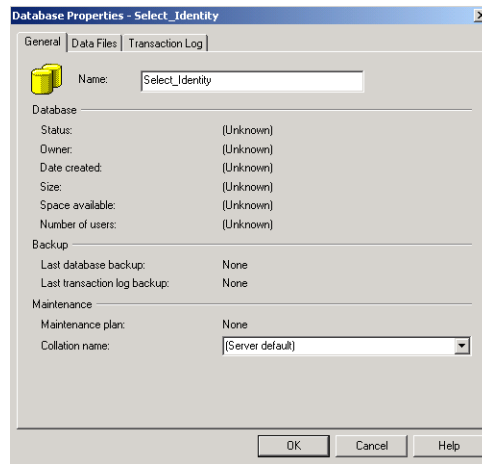
Ensure that your MS SQL Database is configured to be case-insensitive, and that it is configured in Mixed-Authentication mode.

Complete the following to create a SQL Server database:

- 1 Create a directory on the server that will serve as the Select Identity Database home directory on the SQL Server system, such as `C:\Select_Identity` (on Windows). Do *not* put spaces into the directory name.
- 2 Copy the `concero_ddl.sql` and `concero_dml.sql` files from the Database directory on the Select Identity CD to the Select Identity home directory on the SQL Server system.
- 3 Log in to the Microsoft SQL Server Enterprise Manager interface.
- 4 In Enterprise Manager, expand **Microsoft SQL Server** → **SQL Server Group** → **server**, where **server** is the name of the SQL Server instance.

- 5 Right-click **Databases**, and select **New Database....**

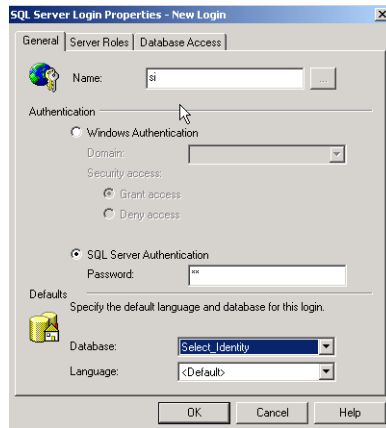
**Figure 2 Database Properties**



- 6 Enter a name for the database, such as **Select\_Identity**. Click **OK** to finish creating the database.
- 7 Create a database user to manage the Select Identity database by completing the following steps:
  - a Select the **Microsoft SQL Server** → **SQL Server Group** → **server** → **Security** folder in the Enterprise Manager tree.

- b Create a new login for the new database by right-clicking **Logins** and selecting **New Login**. The **SQL Server Login Properties** dialog opens.

**Figure 3 SQL Server Login Properties**



- c On the **General** tab, enter a user name such as **SI**, enter a password, and select **SQL Server Authentication** as the authentication type.
  - d Select the new database (Select\_Identity) from the Database list. Keep the remaining default settings.
  - e Click **OK**.
  - f Confirm your password when prompted.
  - g Click the **Database Access** tab.
  - h Check the **Permit** box next to the Select Identity database user.
  - i Assign the **db\_owner** and **public** permissions to the new user.
  - j Click **OK** to save your settings.
- 8 Create the Select Identity database schema by performing the following steps:
- a Launch the SQL Query Analyzer by selecting **Tools** -> **SQL Query Analyzer**.
  - b Select the new database (SI) from the DB list.
  - c Load the `concerro_ddl.sql` script from the Select Identity home directory you created in [Step 2](#) on page 15.
    - Click the **Open** icon.

- Locate the Select Identity home directory.
  - Select the `concero_ddl.sql` file.
  - Click **Open**.
- d Run the script by clicking the **Execute Script** or **Play** button.
- e Verify that no error message is displayed.
- 9 Insert the required default data into the Select Identity database by performing the following:
  - a Clear the previous script by clicking the **Clear Query Window** button.
  - b Load the `concero_dml.sql` script from the directory you created in [Step 2](#) on page 15.
  - c Click the **Execute Script** button. Messages in the console indicate that rows are being created.
  - d Verify that no error message is displayed.
  - e Close the SQL Query Analyzer and the Microsoft SQL Server Enterprise Manager.



After you have installed Select Identity, you will need to modify database and other settings in the `TruAccess.properties` file, which is installed with the product.



---

# 4 Installing Select Identity on BEA WebLogic

This chapter describes how to install and configure Select Identity on a WebSphere application server.

The following sections provide procedures for configuring and installing Select Identity on a WebLogic server or server cluster:

- [Prerequisite Configuration Procedure](#)
- [Select Identity Installer Procedure](#)
- [Select Identity Manual Installation Procedure](#)

## Introduction

Select Identity relies on the web application server to serve its interface pages, communicate with the database server to store and retrieve data, and send email based on actions performed through the Select Identity interface.

The HP Openview Select Identity product CD provides 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 a manual installation process as an alternative.

This chapter applies whether you are installing Select Identity on a Windows or a Linux system. Specific directory locations and pathing information should be adjusted according to your operating system platform and the configuration of your individual servers.

# Single or Clustered Server Installation

Select Identity supports WebLogic clusters through the WebLogic Server layer. See the WebLogic Server documentation for more information on clustered servers.

The installation procedures that follow combine single and clustered server installation. Where the steps for either differ, the procedure describes the difference.

## Select Identity Installation Requirements

The installation environment must meet the following requirements before you begin. These apply to both the installer and manual processes:

Single and clustered servers:

- The database is configured with the Select Identity schema.
- The database server is running.
- The WebLogic and database servers are able to communicate with each other.

Clustered servers:

- The WebLogic Admin Server is running.
- The WebLogic Node Manager is running on every node.
- The managed servers are stopped.
- The cluster has a shared file system for storing application files (properties files, input/output directories for reconciliation, user import jobs, and so on).

## Important Installation Information

Ensure that you have the following information available before you begin installing Select Identity using either the Installer or the manual process:

For single and clustered servers:

- The SMTP email host to be used by Select Identity
- The login ID used when installing WebLogic
- The login ID for the database server admin user
- The IP address and hostname of the WebLogic admin server
- The directory location of the Java Development Kit on the WebLogic server or servers.

This varies depending on the type of environment in place (eg. Sun or Jrockit)

- The directory location of the WebLogic home directory
- Weblogic Application domain directory for the Select Identity application

For clusters:

- The directory location on the Network File System where Select Identity shared files will be stored.

By default installer configures JMS file stores under the shared file system directory. However, for performance reasons, you may move these files to a private drive. See [Chapter 6, Configuring HP OpenView Select Identity](#) for more information.

- The cluster name and the names of all servers in the cluster
- The IP address and hostname of every server in the cluster
- The directory locations of any processes that you will need to start or stop, such as the WebLogic console or node managers.

## Prerequisite Configuration Procedure

Perform this procedure before you begin to install Select Identity using either the installer or the manual installation process.

- 1 Verify that the correct policy files are present on the WebLogic server and determine if the system needs to be upgraded to the “unlimited strength” policy files.

On a cluster, perform [Step 1](#) on the admin server.

▶ Directory locations may differ on your system.

a For Linux systems, change directories to:

```
<BEA_HOME>/jrockit81sp5_142_08/jre/lib/security
```

For Windows systems, change directories to:

```
<BEA_HOME>\jdk142_08\jre\lib\security
```

b Locate the following files:

— local\_policy.jar

— US\_export\_policy.jar

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

- 2 If the policy files on the WebLogic server are correct, skip to [Editing the Default startWebLogic Script on a Single-Server Installation](#). Otherwise, proceed to [Step 3](#).
- 3 Open a Web browser on the WebLogic server and go to the following URL:  
**<http://java.sun.com/j2se/1.4.2/download.html>**
- 4 On the Java Downloads Web page, locate the download link for the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2**. This is located under **Other Downloads**.
- 5 Download the files and save them to a convenient location. To confirm which files you need to replace, refer to the `readme` file that comes with the downloaded policy files.

If you are installing on a cluster, perform this step on every server in the cluster.

## Editing the Default startWebLogic Script on a Single-Server Installation

If you are installing Select Identity on a standalone WebLogic server, you must modify the default WebLogic startup script, which is named `startWebLogic.sh` (Linux) or `startWebLogic.cmd` (Windows). This script is located in the WebLogic installation directory.

Using a text editor such as Vi (Linux) or Notepad (Windows), add the path to `qname.jar` to the beginning of the WebLogic classpath. Add the following line to the script in between where the `SERVER_NAME` is set and the `CLASSPATH` is set.

- On Windows:

```
set
WEBLOGIC_CLASSPATH=C:\si4.0\weblogic\lib\qname.jar;%WEBLOGIC_CLASSPATH%
```

- On Linux:

```
WEBLOGIC_CLASSPATH=/opt/si4.0/weblogic/lib/
qname.jar:$WEBLOGIC_CLASSPATH
```

## Select Identity Installer Process Summary

This section summarizes the tasks that the Select Identity installer performs and lists several important tasks that you must perform yourself before running the installer. This information applies on both single and clustered servers.

Before starting the installation procedure, you must complete the tasks in [Prerequisite Configuration Procedure](#) on page 21 to avoid errors.

The installer performs the following tasks by default:

- Copies the Select Identity files into the Network File System
- Creates a Select Identity JDBC connection pool
- Creates a Select Identity data source
- Creates a Select Identity mail session

- Creates HTTP, SOAP, and EJB execute queues
- Deploys the EAR file
- Configures the Select Identity server with your specified settings
- Configures the Select Identity JMS

The installer does *not* perform the following tasks:

- Validate all preconditions; for example, it does not verify installation of the Select Identity schema.
- Install Weblogic Domain, servers, and clusters; WebLogic must be installed before you begin installing Select Identity.
- Verify the existence of JAVA\_HOME, WL\_HOME, or application domain directories. You must have these directories in place before you begin, and you must enter pathnames accurately into the installer fields.

# Select Identity Installer Procedure

Complete the following steps to install Select Identity:

- 1 Perform the installation on the machine where the Weblogic Admin server is started.
- 2 Log on to the server with the user account that was used to install WebLogic.

If you log on with a different user ID, you will not have the permissions or access needed to install and run Select Identity.

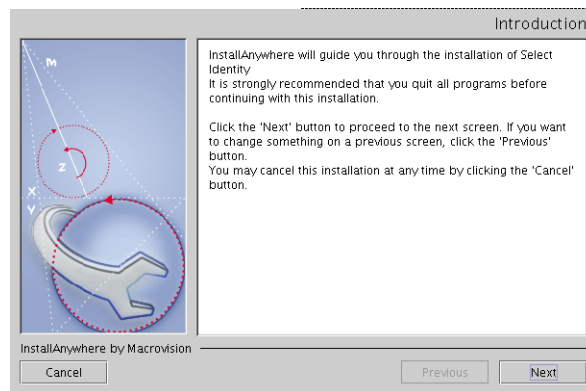
- 3 Mount the HP OpenView Select Identity product CD.
- 4 We recommend using the `install.exe` or `install.bin` file located under the VM directories.
- 5 Copy the following files into a convenient location on the Admin server from the HP OpenView Select Identity product CD:

Linux: `installer.bin`

Windows: `installer.exe`

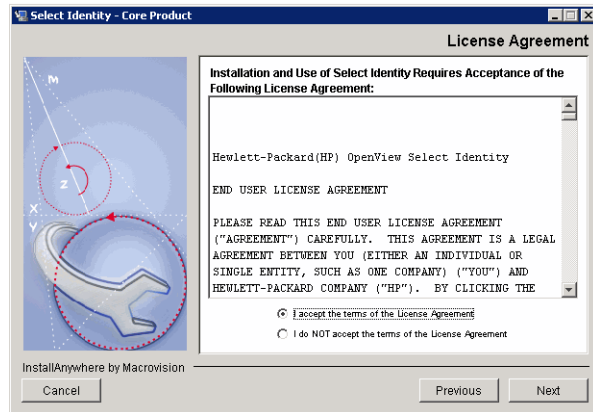
- 6 Run the executable named `install.bin` (Linux) or `install.exe` (Windows) to open the HP OpenView Select Identity Installer, as shown in Figure 4.

**Figure 4 The HP OpenView Select Identity Installer Introduction**



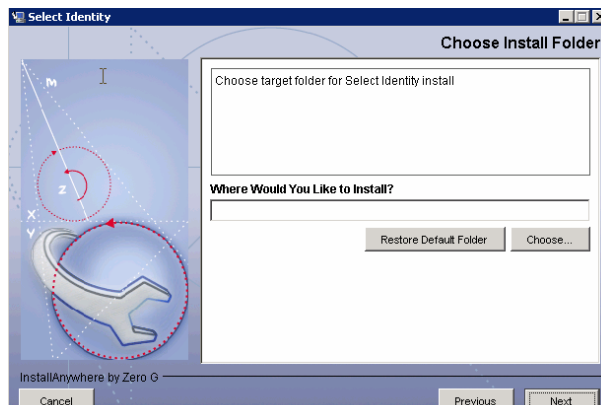
- 7 Click **Next** to proceed to the **License Agreement** page.

**Figure 5 The License Agreement page**




- 8 Click the radio button to **Accept the license agreement** and click **Next** to proceed to the **Choose Install Folder** page.

**Figure 6 The Choose Install Folder page**



- 9 This page includes a field labeled **Where Would You Like to Install**, which is populated with a default installation path appropriate to your operating system.

To use a path other than the default, click **Choose** to browse the file system, or delete the default and enter the path manually.

 If you are installing on a clustered server, ensure that your chosen installation location is in the shared file system.



10 Click **Next** to proceed to the **Pre-Installation Summary** page.

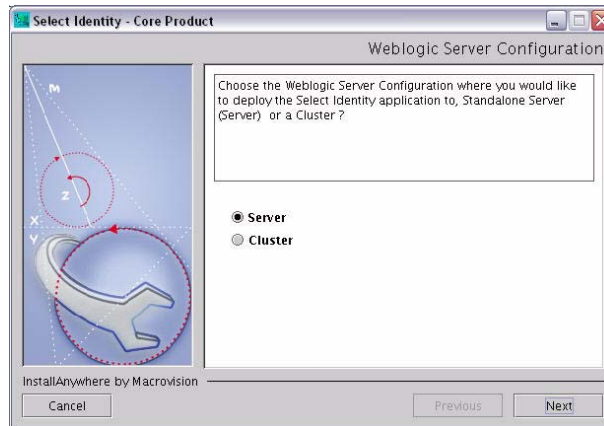
**Figure 7 The Pre-Installation Summary page**



11 Verify the information in the Pre-Installation Summary and ensure that you have completed all required steps.

12 Click **Install** to proceed to the **Server Configuration** page.

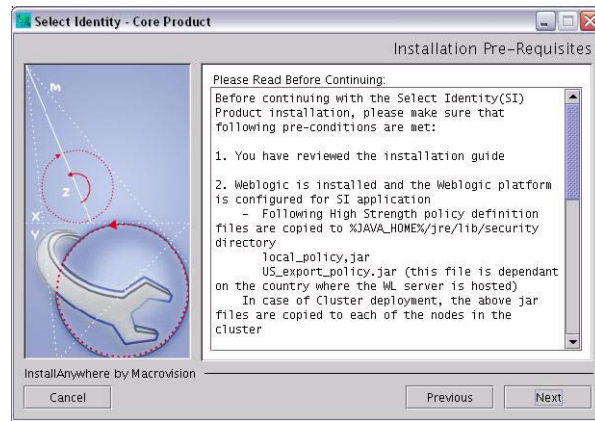
**Figure 8 The Server Configuration Page**



13 If you are installing on a cluster, select **Cluster**; if you are installing on a single server, select **Server**.

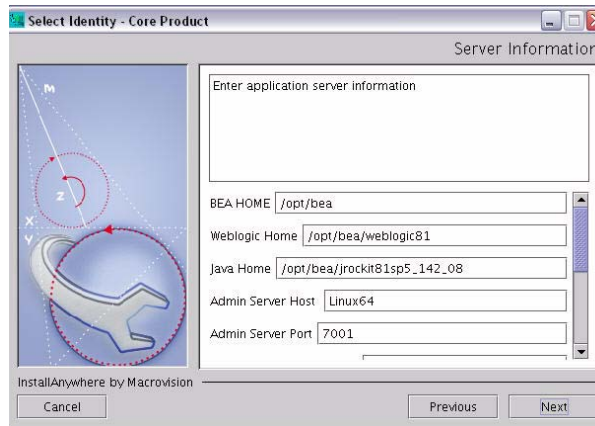
14 Click **Next** to proceed to the **Installation Prerequisites** page.

**Figure 9 Installation Prerequisites page**



- 15 Review the information and verify that all prerequisites are met before you continue.
- 16 Click **Next** to proceed to the **Server Information** page.

**Figure 10 The Server Information page, showing paths for a Linux system**



- 17 Complete each field with the appropriate information, as follows:
  - **BEA Home** — The directory where WebLogic is installed
  - **Java Home** — The directory where the JDK is installed
  - **Server Host** — The hostname of the WebLogic Admin server

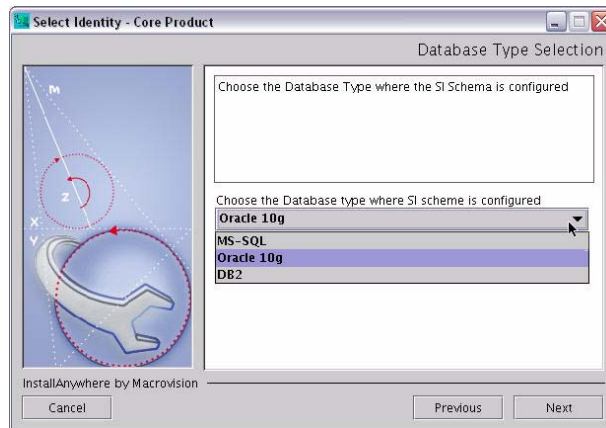
- **Server Port** — The port used by Select Identity
- **Domain Name** — The application domain of the installation
- **Admin Server Login Name** — The WebLogic Admin user name
- **Admin Server Password** — The password for the WebLogic Admin user
- **Cluster Name** — The name of the cluster or server, depending on whether you are installing on a single server or clustered server.

18 Click **Next** to proceed to the **Database Type Selection** page.

19 Use the list box to select the database for Select Identity (Oracle 10g for Linux systems, and Oracle 9i or MS-SQL for Windows systems).

20 See [Configuring the Database Server](#) on page 13 for more information.

**Figure 11 The Database Type Selection page, on a Linux system**



21 Click **Next** to proceed to the **Database Information** page.

**Figure 12 Database Information Page**

Database Information

Enter database information. The Select Identity schema should already be installed in this location.

Database Server Name | QALNX1.americas.hpqcorp.net

Database Server Port | 1521

Database Name | ora65

Database Login | dvs1

Database Password | \*\*\*\*

InstallAnywhere by Macrovision

Cancel Previous Next

22 Specify the settings for the database where Select Identity stores its data.

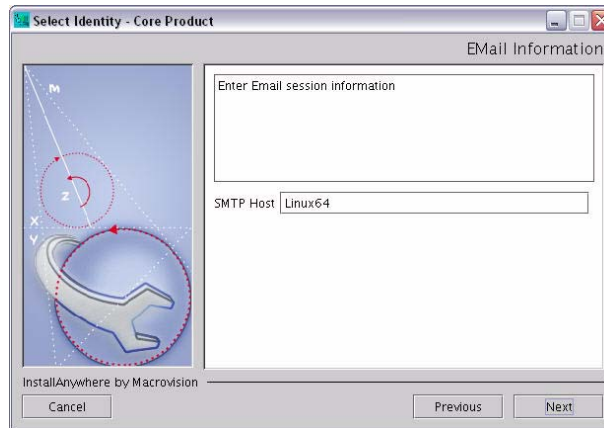
The installer prepopulates the fields based on previous selections.

Settings are as follows:

- **Database Server Name** — The hostname of the database server
- **Database Server Port** — The database server port
- **Database Name** — The name of the database created for Select Identity
- **Database Login** — The user name Select Identity uses to access the database
- **Database Password** — The password for the database user name

23 Click **Next** to proceed to the **Email Information** page.

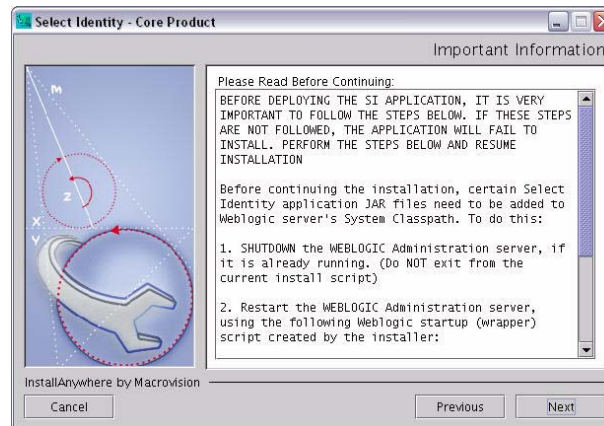
**Figure 13 The Email Information page**



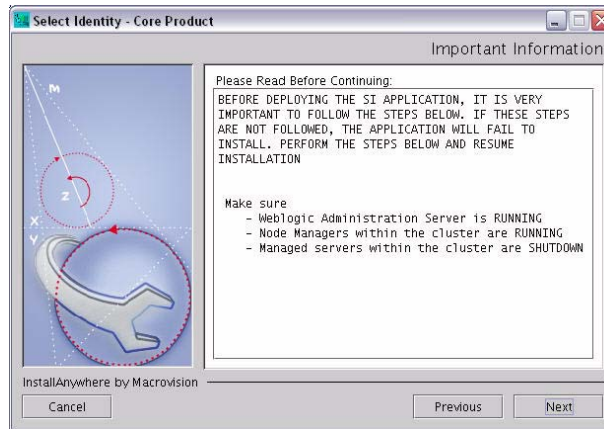
- 24 Specify the name of the SMTP host through which Select Identity sends email.
- 25 Click **Next** to proceed to the **Important Information** page.

This page varies depending upon whether you are installing on a single or clustered server environment.

**Figure 14 Important Information page for single servers**



**Figure 15 Important information page for clustered servers**



- 26 Review and follow the directions on the page. If the WebLogic processes are not running as directed, Select Identity installation will fail.
- 27 Click **Next**.

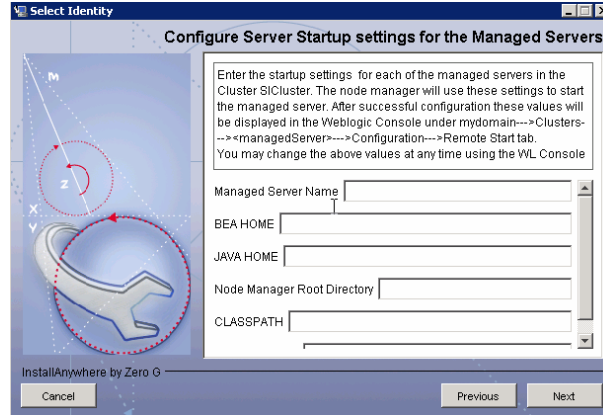
The installer verifies the WebLogic Admin server configuration information and begins to install Select Identity.



It is very important that the Weblogic server is started using the installer-generated script because this updates the class path entry correctly.

- 28 If you are installing on a single server, skip to [Validating the Installation](#) on page 34.
- 29 If you are installing on a cluster, click **Next** to proceed to the **Managed Server Configuration** page.

**Figure 16 The Managed Server Configuration page for a WebLogic cluster**



30 If you are installing on a cluster, specify the settings on the **Managed Server Configuration** page for each of the managed servers in the Cluster.

If you are installing on a single server, you make these settings once only.

Settings are as follows:

- **Managed Server Name** — Name of the managed server on which you are installing Select Identity
- **BEA Home** — Directory where WebLogic is installed
- **Java Home** — Directory where the JDK is installed
- **Node Manager Root Directory** — Location of the node manager root directory
- **Class Path** — Class paths used by the servers in a cluster when starting up, to locate the following files:
  - connector.jar
  - ovsi18n.jar
  - commons-logging.jar
  - qname.jar
- **JVM Arguments** — Directory path of the `TruAccess.properties` and `logging.properties` files

31 When you have completed the settings, click **Next**.

The installer verifies the information, performs the configuration, and creates the JMS settings.

- 32 When prompted, click **Yes** if you have additional managed server to configure. Click **No** when you have configured all managed servers
- 33 Perform [Step 30](#) and [Step 31](#) for each node until all servers have been configured. Then proceed to [Step 34](#).
- 34 The installer presents the managed server settings for review. You may make any changes necessary to the settings.

The installer performs the following functions:

- Deploys the connection pool
- Deploys the data source
- Configures JMS
- Deploys mail
- Deploys the EAR file

## Validating the Installation



If the installer displays the following message, it is recommended that you uninstall and reinstall Select Identity after correcting the problem.

**The installation of SI is finished, but some errors occurred during the install.**

Follow the steps below to validate the installation:

- 1 Wait for the installer to finish, then close it by clicking **Done**.
- 2 Verify the values that you just defined through the remote start setting for each server from the **Administrative Console** on WebLogic.


In the WebLogic Admin Console, use the navigation icons on the left to select **Clusters>Configurations**.

- 3 Verify that the `TruAccess.properties` file contains the correct database type, and that any paths it contains match your specific system environment.

For more information about the TruAccess properties, see [Appendix B, Configuring TruAccess.properties](#).




- 4 If you installed Select Identity on a WebLogic cluster, start all of the managed servers in the cluster from the WebLogic Administrative Server console.

 You must start the cluster from the console to apply the classpath for the managed servers correctly.

- 5 Refer to [Appendix a, Logging](#) for instructions on configuring the `logging.properties` file. By default, a `logging.properties` file is provided by the WebLogic server's JVM.

On WebLogic, this file resides in the `$BEA_HOME/jrockit81sp5_142_08/jre/lib` directory on Linux systems, and `%BEA_Home%\jdk142_08\jre\lib` on Windows systems.

 Configuring logging is crucial. Select Identity may not function properly if you do not configure the `logging.properties` file for each node.

- 6 Follow the instructions in [Additional Configuration](#) on page 79 to set the JTA timeout and deploy the online help into the Select Identity Help menu.

## Restarting WebLogic After Installing Select Identity

- 1 After successful installation of SI on single server, you must restart the WebLogic admin server using the installer-generated script file.
- 2 After successful installation of SI on cluster server, restart the WebLogic admin server using Weblogic's startup script. When WebLogic has started up, log into the Administration Console and start the cluster.
- 3 Failure to start the WebLogic server according to these instructions will result in JMS exceptions and Select Identity login failure.

# Select Identity Manual Installation Procedure

This section provides procedures for installing Select Identity using the manual installation process for single and clustered servers.

Complete the following procedures to install Select Identity manually:

- Check to make sure your system meets the [Select Identity Installation Requirements](#) on page 20.
- [Creating Select Identity Directories and Copying Installation Files](#)
- [Starting WebLogic](#)
- [Configuring the Mail Session](#)
- [Configuring JMS Settings](#)
- [Configuring the JTA Settings](#)
- [Configuring a JDBC Connection Pool](#)
- [Configuring the JDBC Data Source](#)
- [Modifying the WebLogic Server Class Path](#)
- [Configuring the Select Identity Execute Queues](#)
- [Enable Anonymous Admin Lookup by performing the following steps:](#)



The left pane of the WebLogic console is updated each time you add a new configuration. You can save your settings and log out of the WebLogic console and log in later to continue the installation process.

## Creating Select Identity Directories and Copying Installation Files

Create the directories and copy the files listed in this section before you begin installing Select Identity.

- 1 Create the Select Identity home directory on the WebLogic Administration server. This will contain all files and subdirectories in the finished installation.

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

- 2 Create the following subdirectories in the `<OVSI_INSTALL_DIR>` directory:
  - `<OVSI_INSTALL_DIR>/deploy`
  - `<OVSI_INSTALL_DIR>/sysArchive`
  - `<OVSI_INSTALL_DIR>/lib`
  - `<OVSI_INSTALL_DIR>/temp`
  - `<OVSI_INSTALL_DIR>/reconroot`


- <OVSI\_INSTALL\_DIR>/reconstaging
  - <OVSI\_INSTALL\_DIR>/reconbackup
  - <OVSI\_INSTALL\_DIR>/reports
  - <OVSI\_INSTALL\_DIR>/adroot
  - <OVSI\_INSTALL\_DIR>/adbackup
  - <OVSI\_INSTALL\_DIR>/adstaging
  - <OVSI\_INSTALL\_DIR>/jmsstore<Server1>
    - For clustered installations, the JMS file and paging stores for a cluster can be moved to a private drive on each server in the cluster.
- 3 For standalone manual installations, create the following directory to store the myStartWL script:
    - <OVSI\_INSTALL\_DIR>/scripts
  - 4 Copy the application/lmz.ear file from the Select Identity product CD to the <OVSI\_INSTALL\_DIR>/deploy directory.
 

As explained in [Step 2](#), since you do not need to create the deploy subdirectory on cluster nodes, this also applies to the lmz.ear file.
  - 5 Copy the following files into the <OVSI\_INSTALL\_DIR>/sysArchive directory:
    - properties/TruAccess.properties
    - lib/ovsii18n.jar
    - connector/connector.jar


Copy the following files into the <OVSI\_INSTALL\_DIR>/lib directory:

    - lib/commons-logging.jar
    - lib/qname.jar
  - 6 Ensure the following settings in the TruAccess.properties file are set so that the database initializes correctly:
    - For the Thin Driver for Oracle 9i and 10G:
      - truaccess.repository.type=<oracle10>
      - truaccess.repository.oracle.driver.bea=no
    - For Microsoft SQL Server:


```
truaccess.repository.type=mssql
truaccess.repository.oracle.driver.bea=no
```

 If you attempt to start Select Identity without completing this step, you will initialize the database improperly.

- 7 Determine your method of encryption and make sure that the correct encryption method is valid in the `TruAccess.properties` file.

 See [Configuring TruAccess.properties Required Settings](#) on page 129 for more details.

- 8 Copy a `logging.properties` file from the default location in the WebLogic Server JVM into the `sysArchive` directory.
  - For clusters: Copy the `logging.properties` file to every node on a clustered server installation. Give each copy a name that makes it easy to identify within the cluster.

 By default, a `logging.properties` file is provided by the WebLogic server JVM. This file resides in the `$BEA_HOME/jrockit81sp5_142_08/jre/lib` directory for Linux systems.

Do not copy the `logging.properties` file to the default directory. That instance is for WebLogic messages. Instead, copy `logging.properties` to a subdirectory in the `<OVSI_INSTALL_DIR>` directory, such as `sysArchive`.

- 9 Copy the product documentation from the `docs` directory on the HP OpenView Select Identity Product CD to the WebLogic server.

## Creating the myStartWL Script on a Single Server

When installing on a standalone server, you must set the JVM arguments by editing the `myStartWL` script. The following is an example of what should be added to the `myStartWL` file:

This example includes the following:

- Setting the memory
- Location of `TruAccess.properties`
- Location of `logging.properties`
- `Headless=true` setting for Linux

- Adding the connector.jar and ovsii18n.jar to the classpath

**Figure 17 Example myStartWL script for Windows systems**

```

set JAVA_OPTIONS=-server -Xms256m -Xmx1024m
-XX:MaxPermSize=256m
-Dcom.trulogica.truaccess.property.file="C:\si4.0\weblogi
c\sysArchive\TruAccess.properties"
-Djava.util.logging.config.file="C:\si4.0\weblogic\sysArc
hive\logging.properties"

set
CLASSPATH=C:\si4.0\weblogic\sysArchive\connector.jar;C:\s
i4.0\weblogic\sysArchive\ovsii18n.jar;C:\si4.0\weblogic\s
ysArchive;C:\si4.0\weblogic\lib\commons-logging.jar;%CLAS
SPATH%

cd "c:\bea\user_projects\domains\mydomain"

call startweblogic.cmd

```

**Figure 18 Example myStartWL script for Linux systems**

```

#!/bin/sh

JAVA_OPTIONS="-server -Xms256m -Xmx1024m
-Dcom.trulogica.truaccess.property.file=/opt/si4.0/
weblogic/sysArchive/TruAccess.properties
-Djava.awt.headless=true
-Djava.util.logging.config.file=/opt/si4.0/weblogic/
sysArchive/logging.properties
-Dweblogic.management.anonymousAdminLookupEnabled=true"

export JAVA_OPTIONS

CLASSPATH=/opt/si4.0/weblogic/sysArchive:/opt/si4.0/
weblogic/sysArchive/connector.jar:/opt/si4.0/weblogic/
sysArchive/schema.jar:/opt/si4.0/weblogic/sysArchive/
ovsii18n.jar:/opt/si4.0/weblogic/lib/
commons-logging.jar:$CLASSPATH

export CLASSPATH

cd /opt/bea/user_projects/domains/mydomain

/opt/bea/user_projects/domains/mydomain/startWebLogic.sh

```

# Starting WebLogic

Complete the following steps to start WebLogic:

- 1 For *standalone* installations, start WebLogic by executing the following command from the WebLogic server command line.

Choose the correct script according to your operating system (Linux or Windows):

```
<OVSI_INSTALL_DIR>/scripts/myStartWL.sh
```

```
<OVSI_INSTALL_DIR>\scripts\myStartWL.cmd
```

For *clustered* server installations, start the Admin server by executing the following command from the WebLogic Admin server's command line.

Choose the correct script according to your operating system (Linux or Windows):

```
<WEBLOGIC_INSTALL_DIR>/user_projects/domains/
```

```
<YOUR_DOMAIN>/startWebLogic.sh
```

```
<WEBLOGIC_INSTALL_DIR>\user_projects\domains\<YOUR_DOMAIN>\startWebLogic.cmd
```

- 2 Open a browser and log in to the WebLogic Server Console to open the WebLogic Server Home page.

**Figure 19 WebLogic Server Home Page**



## Configuring the Mail Session

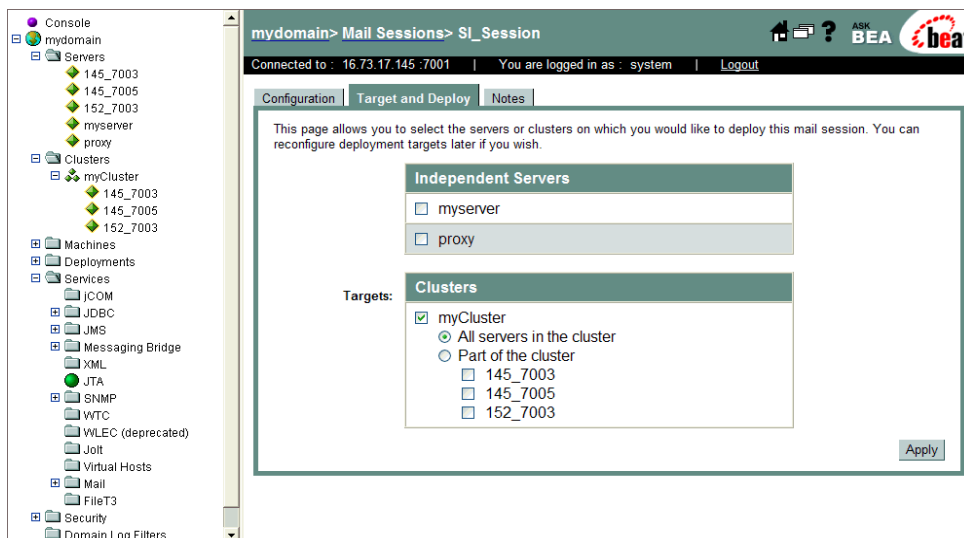
Configure the mail session for Select Identity, as follows:

- 1 Open the **Mail Services** page by navigating to `<domain_name>` → **Services** → **Mail** using the tree view in the left panel. `<domain_name>` is the domain created during the WebLogic installation.
- 2 Click the link to **Configure a New Mail Session** at the bottom of the page.
- 3 Provide the following information on the **Configure a New Mail Session** page:

Field	Value
<b>Name</b>	Enter a name for the mail session.
<b>JNDIName</b>	Enter <code>mail/TruAccess</code>
<b>Properties</b>	Enter the IP address of the mail server. For example: <code>mail.smtp.host=192.168.1.52</code> .

Click **Create** to save these settings and proceed to the **Target and Deploy** page. The illustration in [Figure 20](#) shows an example for a clustered server. If you are installing on a single server, only independent (single) servers are available for deployment.

**Figure 20 Target and Deploy Page for clustered servers**



- 4 Select the cluster or server designated for Select Identity use.
- 5 Click **Apply** to finish the mail session configuration. The console remains on the **Target and Deploy** page.

## Configuring JMS Settings

Complete the following required procedures to configure the JMS settings for each server in a cluster:

- [Configuring New JMS Connection Factories](#)
- [Configuring a JMS File Store](#)
- [Configuring a JMS Server](#)
- [Creating the JMS Queues on a Single Server](#)
- [Configuring JMS Queues on a Clustered Server](#)
- [Configuring JMS Topics on a Clustered Server](#)
- [Creating JMS Server Members](#)
- [Modifying the JMS Template for JMS Queues and Topics](#)



## Configuring New JMS Connection Factories

Select identity requires two JMS connection factories. To create and configure these, perform the following steps:

- 1 Open the **JMS Connection Factories** page by navigating to `<domain_name>` → **Services** → **JMS** → **Connection Factories**.
- 2 Click the link at the bottom of the page to **Configure a New JMS Connection Factory**.
- 3 On the new connection factory page, enter the recommended Connection Factory name and the required JNDI name listed below into the appropriate fields.

Purpose	Recommended Name	Required JNDI Name
Select Identity Queue Connection Factory	<code>jms.OVSIQCF</code>	<code>jms/OVSIQCF</code>
Select Identity Topic Connection Factory	<code>jms.OVSITCF</code>	<code>jms/OVSITCF</code>

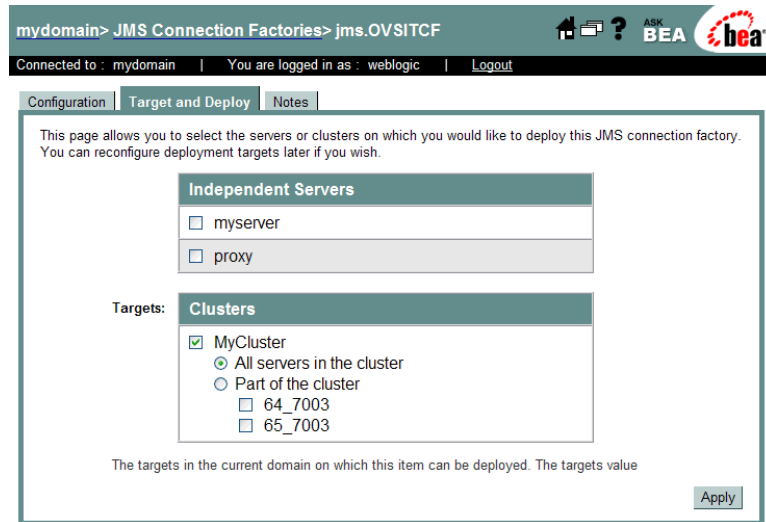
- 4 Tab from field to field to enter the information listed below.

Field	Action
Server Affinity Enabled	<b>Clustered servers:</b> — Uncheck to indicate <b>False</b> . <b>Single servers:</b> — Check to indicate <b>True</b> (default).
Message Maximum	10

- 5 When configuring the `OVSITCF` topic connection factory, ensure that the default delivery mode is set to **non-Persistent**.
- 6 When configuring the `OVSIQCF` queue connection factory, set the **Default Redeliver Delay** option to 30000 (30 seconds), and the **Default Delivery Mode** to **Persistent**. Both of these settings are on the **General** tab.

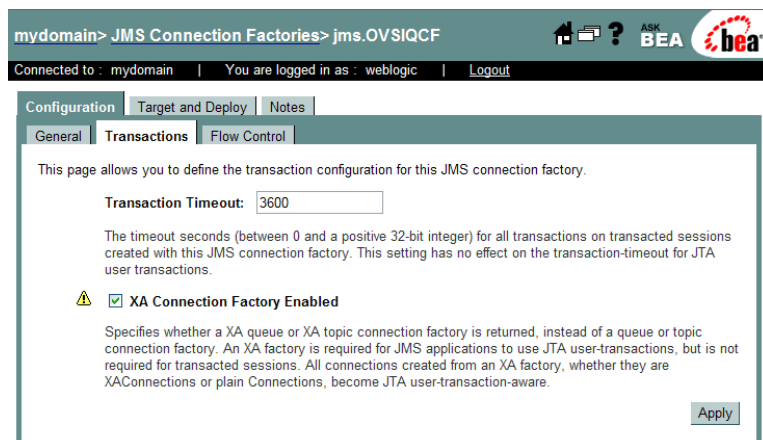
- 7 Accept all other defaults and click **Create** to proceed to the **Target and Deploy** page.

**Figure 21 JMS Connection Factory Target and Deploy Page**



- 8 Select **All servers in the cluster** to deploy the Connection Factory to each node. On a single server, select the name of the independent server.  
Your cluster name is automatically selected.
- 9 Click **Apply** to save the selection.
- 10 Click the **Configuration** tab, then the **Transactions** tab to proceed to the **Transactions** page.

**Figure 22 Transactions Page**



- 11 Check the box labeled **XA Connection Factory** to enable the XA Connection Factory.
- 12 Repeat this procedure for the second connection factory.
- 13 Navigate to **<domain\_name> → Services → JMS → Connection Factories** again to check that all Connection Factories have been configured.

## Configuring a JMS File Store

The JMS settings define the File Store that the JMS Queue writes to for each server. One File Store and one Paging Store must be set up for each node within a cluster. Only a single instance of each is needed on a single server installation.

Each JMS server must have a unique Persistent File Store, which corresponds to that JMS server. The same File Store cannot be used by another JMS server. A new File Store must be created for each new JMS server.

Repeat this procedure for each node if you are installing on a clustered server.

Perform the following steps to configure the JMS Stores for clustered servers:

- 1 Open the **JMS Stores** page by navigating to **<domain\_name> → Services → JMS → Stores**.

## Figure 23 JMS Stores Page

mydomain > JMS Stores

Connected to : mydomain | You are logged in as : weblogic | Logout

A persistent JMS store is a physical repository for storing persistent message data and durable subscribers. A JMS store can also be used for the paging of messages to disk when memory has been exhausted. It can be either a JDBC-accessible database or a disk-based file.

This JMS Stores page displays key information about each JMS store that has been configured in the current WebLogic Server domain.

[Configure a new JMS JDBC Store...](#)  
[Configure a new JMS File Store...](#)

[Customize this view...](#)

Name	Type		
<a href="#">FileStore</a>	JMSFileStore		

- 2 Click the **Configure a new JMS File Store** link to open the **JMS Store** page.

## Figure 24 JMS Store Page

mydomain > JMS File Stores > Create a new JMSFileStore...

Connected to : mydomain | You are logged in as : weblogic | Logout

Configuration Notes

This page allows you to define a disk-based JMS file store for storing persistent messages and durable subscribers. A dedicated JMS file store can also be defined to temporarily store non-persistent messages that are paged out from memory when message loads reach a specified threshold.

**Name:**

The name of this disk-based file store. This name must be unique within the WebLogic Server instance or its cluster.

**Synchronous Write Policy:**

A policy that determines how this JMS file store writes data to disk. This policy also affects the JMS file store's performance, scalability, and reliability. **Disabled** means that transactions complete as soon as file store writes are cached in memory, instead of waiting for the writes to successfully reach the disk. **Cache-Flush** means that transactions cannot complete until all of their writes have been flushed down to disk. **Direct-Write** means that all file store writes are written directly to disk. (The **Direct-Write** policy may not be transactionally safe on some Windows systems. See the online help for more information.)

**Directory:**

The pathname to the directory on the file system where the JMS file store is kept. (This directory must exist on your system, so be sure to create it before completing this tab.)

- 3 Click the **Name** field and enter the appropriate name.

Create the File Store and repeat this procedure to create the Paging Store.

Purpose	Name
Persistent Select Identity Audit and Workflow JMS messages	OVSI File Store Server1 <b>Server1</b> is the server ID in the cluster.
Temporarily store the Select Identity Service Assignment, Reconciliation, and Cache cleanup JMS messages	OVSI Paging Store Server1 <b>Server1</b> is the server ID in the cluster.

- 4 Tab to the **Directory** field and enter the path to the File and Paging Store.  
For example: <OVSI\_INSTALL\_DIR>/jmsstore<Server1>  
<Server1> is the server ID in the cluster.
- 5 Accept the default for the **Synchronous Write Policy**.
- 6 Click **Create**, then **Apply** to save your work.
- 7 Repeat this procedure for each node.

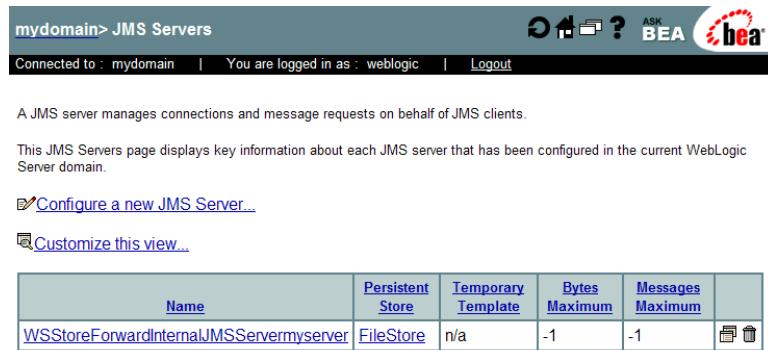
## Configuring a JMS Server

Each JMS server must have a unique persistent File Store and Paging Store, which corresponds to that JMS server.

Repeat this procedure for each node to create the JMS server:

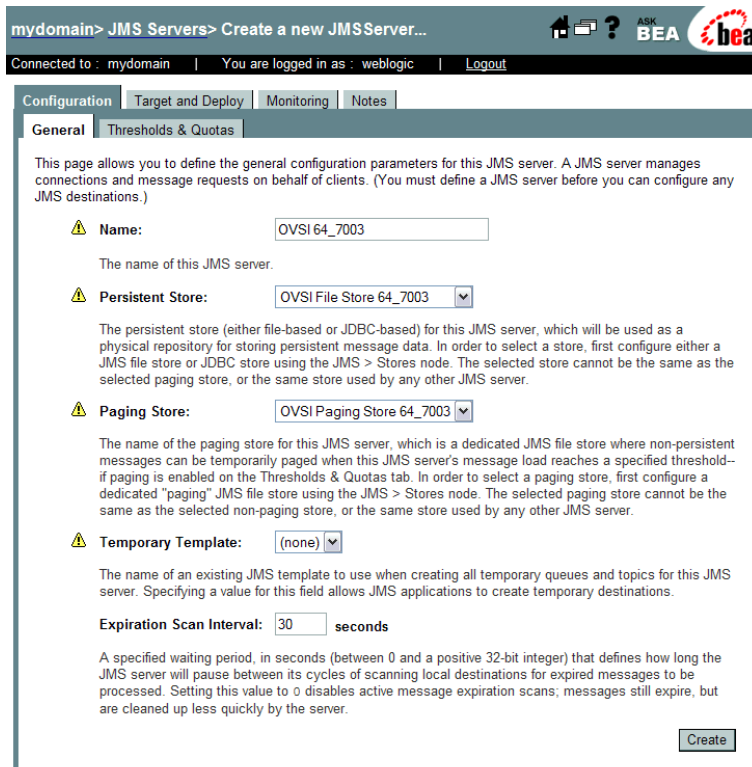
- 1 Open the **JMS Servers** page by navigating to <domain\_name> → **Services** → **JMS** → **Servers**.

**Figure 25 JMS Servers Page**



2 Click the **Configure a new JMS Server** link.

**Figure 26 Create a new JMS Server Page**

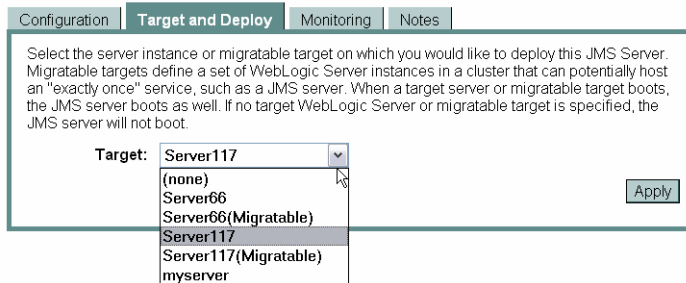


- 3 Tab from field to field and enter the required information.

Field	Action
Name	Enter OVSI <Server1> <Server1> is the server ID in the cluster.
Persistent Store	Enter OVSI File Store <Server1> <Server1> is the server ID in the cluster.
Paging Store	Enter OVSI Paging Store <Server1> <Server1> is the server ID in the cluster.

- 4 Accept all other defaults.
- 5 Click **Create** to proceed to the **Target and Deploy** page.

**Figure 27 JMS Server Target and Deploy Page**



- 6 Select the target on which to deploy this JMS server. Do not select the migratable target.
- 7 Click **Apply** to save this setting.
- 8 Click the **Configurations** tab, then the **Thresholds & Quotas** tab to view the **Thresholds & Quotas** page.

- 9 Tab to the fields listed below and enter the correct information.

Field	Action
Bytes Maximum	Set this to -1 for an unlimited quota. The JMS server limit must be higher than the limit for queues.
Bytes Paging Enabled	Insert a check to indicate <b>True</b> .
Bytes Threshold High	100000000 (100MB)
Bytes Threshold Low	10000000 (10MB)
Messages Paging Disabled	Ensure this option is disabled (unchecked).
Blocking Send Policy	FIFO

- 10 Accept all other defaults.
- 11 Click the **Apply** button to save these settings.
- 12 Repeat this procedure for each server until all servers are set up.

## Creating the JMS Queues on a Single Server

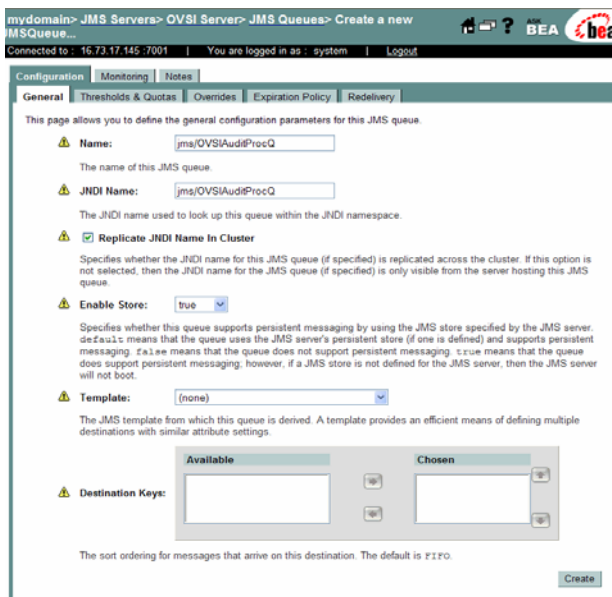
You must configure each JMS Queue listed in this procedure. If you are installing on a clustered server, skip this procedure and proceed to [Configuring JMS Queues on a Clustered Server](#) on page 53.

Perform the following steps to create the JMS Queues for a single server:

- 1 Open the **<your\_OVSI\_Server>** page by navigating to **<domain\_name>** → **Services** → **JMS** → **<your\_OVSI\_Server>** → **Destinations**.
- 2 Click the link to the **Configure a new JMS Queue** page.



**Figure 28 Configure a New JMS Queue Page**




- 3 Click the **Recommended Name** and **JNDI Name** field and enter the name. Use the exact JNDI names shown in the table.

Repeat [Step 1](#) through [Step 3](#) for each JMS Queue in the following table.

Purpose	Recommended Name	Required Name
Select Identity Audit Process	jms.OVSIAuditProcQ	jms/OVSIAuditProcQ
Batch Processing for Bulk Operations	jms.OVSIBulkQueue	jms/OVSIBulkQueue
ServiceRecon Process	jms.OVSIChangeReconProcessorQueue	jms/OVSIChangeReconProcessorQueue
Entitlement Cache Processing	jms.OVSIEntCacheQueue	jms/OVSIEntCacheQueue
ServiceRecon Flow Control	jms.OVSIMessageAckQueue	jms/OVSIMessageAckQueue

<b>Purpose</b>	<b>Recommended Name</b>	<b>Required Name</b>
<b>UserRecon Process</b>	jms.OVSIReconQueue	jms/OVSIReconQueue
<b>Resource Reconciliation Flow Control</b>	jms.OVSIResReconDispatcherQ	jms/OVSIResReconDispatcherQ
<b>Resource Reconciliation Processing</b>	jms.OVSIResReconQ	jms/OVSIResReconQ
<b>SA Integration</b>	jms.OVSI SaudQ	jms/OVSI SaudQ
<b>Batch Handling</b>	jms.OVSI Scheduler Queue	jms/OVSI Scheduler Queue
<b>Service Assignment</b>	jms.OVSI ServiceAssign Queue	jms/OVSI ServiceAssign Queue
<b>Request Expiration</b>	jms.OVSIwfRequestExpireQueue	jms/OVSIwfRequestExpireQueue
<b>Workflow Process</b>	jms.OVSIWorkflow Queue	jms/OVSIWorkflow Queue

- 4 Accept all defaults, with the following exceptions:
  - Tab to the **Enable Store** field and select **True** for each JMS Queue.
- 5 Click **Create** to save your settings.
- 6 When creating the OVSIWorkflowQueue set the following settings:
  - Click the **Redelivery** tab and set the **Error Destination** to `jms.OVSIwfRequestExpireQueue`.
  - Click the **Expiration Policy** tab and set the **Expiration Policy** to **Redirect**.
  - Click the **Overrides** tab and set the **Delivery Mode Override** to **Persistent**.
- 7 Repeat these steps for each JMS Queue.
  -  You must create *all* of the listed JMS Queues for your installation to be succesful. Check carefully before you continue.
- 8 Proceed to [Configuring the JTA Settings](#) on page 79.

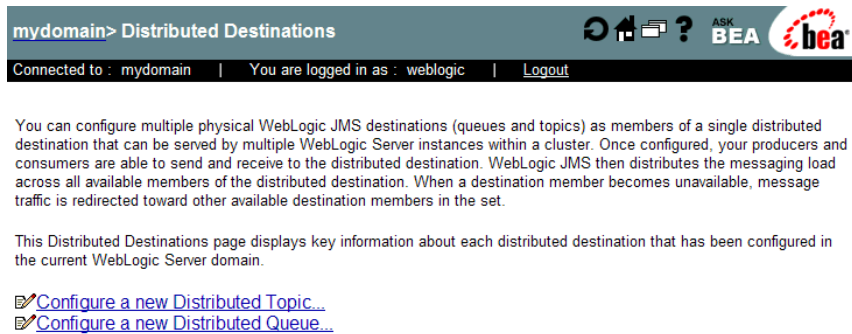
## Configuring JMS Queues on a Clustered Server

You must create and configure every JMS Queue listed in this procedure, but you do not need to repeat the procedure for the individual nodes because the queues are deployed to the nodes automatically.

Perform the following steps to configure the JMS Queues:

- 1 Open the **Distributed Destinations** page by navigating to `<domain_name>` → **Services** → **JMS** → **Distributed Destinations**.

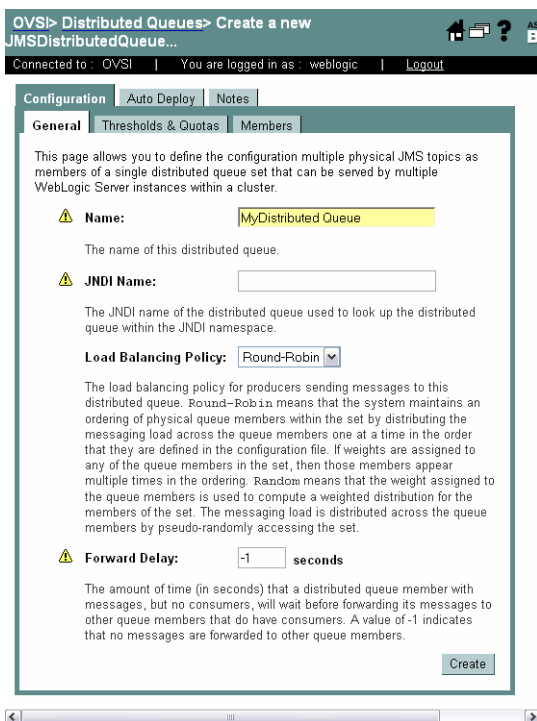
**Figure 29 Distributed Destinations Page**



The screenshot shows the 'mydomain> Distributed Destinations' page. The top navigation bar includes icons for home, search, and help, along with the BEA logo. Below the navigation bar, a status bar indicates 'Connected to : mydomain | You are logged in as : weblogic | Logout'. The main content area contains a paragraph explaining that multiple physical WebLogic JMS destinations (queues and topics) can be configured as members of a single distributed destination. It also notes that once configured, producers and consumers can send and receive to the distributed destination, and the messaging load is distributed across all available members. When a member becomes unavailable, message traffic is redirected to other available members. Below this text are two links: 'Configure a new Distributed Topic...' and 'Configure a new Distributed Queue...'.

- 2 Click the **Configure a new Distributed JMS Queue** link to open the **Create a New JMS Distributed Queue** page.

**Figure 30 Create a New JMS Distributed Queue Page**



- 3 Click the **Recommended Name** and **JNDI Name** field and enter the name. Use the exact JNDI names shown in the table.

Repeat [Step 1](#) through [Step 3](#) for each JMS Queue recommended name in the following table

Process	Recommended Name	Required JNDI Name
<b>Batch Processing for Bulk Operations</b>	jms.OVSIBulkQueue	jms/OVSIBulkQueue
<b>Service Recon Process</b>	jms.OVSIChangeReconProcessorQueue	jms/OVSIChangeReconProcessorQueue
<b>Entitlement Cache Processing</b>	jms.OVSIEntCacheQueue	jms/OVSIEntCacheQueue
<b>Service Recon Flow Control</b>	jms.OVSIMessageAckQueue	jms/OVSIMessageAckQueue

<b>Process</b>	<b>Recommended Name</b>	<b>Required JNDI Name</b>
<b>User Recon Process</b>	jms.OVSIReconQueue	jms/OVSIReconQueue
<b>Resource Reconciliation Dispatch</b>	jms.OVSIResReconDispatcherQ	jms/OVSIWfResReconDispatcherQ
<b>Resource Reconciliation Processing</b>	jms.OVSIResReconQ	jms/OVSIResReconQ
<b>SA Integration</b>	jms.OVSIISaudQ	jms/OVSIISaudQ
<b>Batch Handling</b>	jms.OVSIISchedulerQueue	jms/OVSIISchedulerQueue
<b>Service Assignment</b>	jms.OVSIServiceAssignQueue	jms/OVSIServiceAssignQueue
<b>Workflow Process</b>	jms.OVSIWorkflowQueue	jms/OVSIWorkflowQueue
<b>Request Expire</b>	jms.OVSIWfRequestExpireQueue	jms/OVSIWfRequestExpireQueue

- 4 Tab to the **Load Balancing Policy** field and enter **Round Robin**.
- 5 Tab to the **Forward Delay** field and enter **0**.
- 6 Select the **Replicate JNDI Name in Cluster** check box for all JMS Queues except `jms/OVSIResReconDispatcherQ`. Accept all other defaults.
- 7 Click **Create** to create the JMS Queue.
- 8 Click the **Thresholds & Quotas** tab to view the **Thresholds & Quotas** page.
- 9 Tab from field to field and enter the required information.

<b>Field</b>	<b>Action</b>
<b>Bytes Maximum</b>	Enter <b>-1</b> .
<b>Bytes Threshold High</b>	100000000 (100MB)
<b>Bytes Threshold Low</b>	10000000 (10MB)
<b>Bytes Paging Enabled</b>	Set to <b>True</b> .

- 10 Accept all other defaults.
- 11 Click **Apply** to save these settings.
- 12 Repeat this procedure until all of the JMS Queues are complete.

## Configuring the JMS Audit Queues on a Clustered Server

The JMS Audit queue requires special configuration on a clustered server. This is because Select Identity requires a local audit queue on each node in place of a distributed queue.

Do not build a distributed audit queue on a cluster.

Perform the JMS queue creation procedure documented in [Creating the JMS Queues on a Single Server](#) on page 50 for each node, using the queue settings as documented in that procedure. Use the notes below for guidance:

- Name this queue **jms.OVSIAuditProcQ**. (required JNDI name `.jms/OVSIAuditProcQ`).
- Ensure that the setting to **Replicate JNDI Name in Cluster** is unchecked.

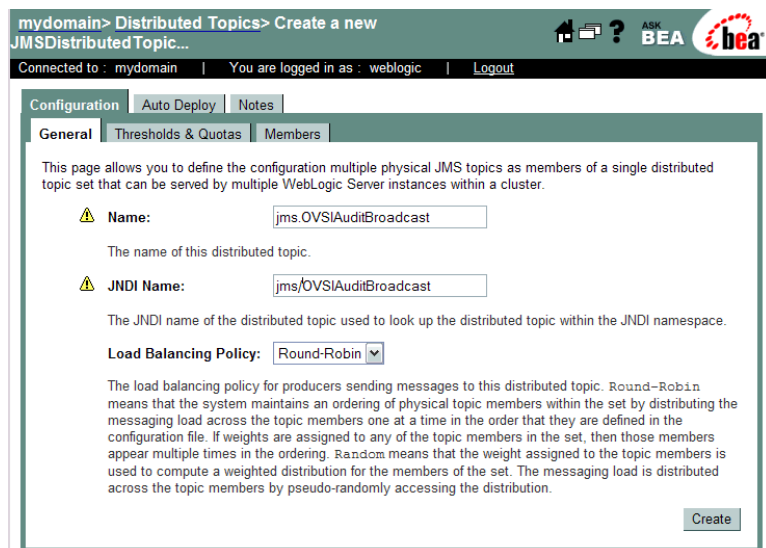
## Configuring JMS Topics on a Clustered Server

You must configure each JMS Topic listed in this procedure, but you do not need to repeat the procedure for the individual nodes because the JMS Topics are deployed to the nodes automatically.

Perform the following steps to configure the JMS Topics:

- 1 Open the **Distributed Destinations** page by navigating to `<domain_name> → Services → JMS → Distributed Destinations`.
- 2 Select the **Configure a new JMS Topic** link to open the **Create a new JMS Distributed Topic** page.

**Figure 31 Create a new JMS Topic Page**



- 3 Enter the **Name** and **JNDI Name** in the appropriate fields, using the table below for reference:

Purpose	Recommended Name	Required JNDI Name
Select Identity Audit Process	jms.OVSIAuditBroadcast	jms/OVSIAuditBroadcast
Select Identity Cache Cleanup	jms.OVSI_CACHE_TOPIC	jms/OVSI_CACHE_TOPIC

- 4 Click the **Load Balance Policy** field and select **Round Robin**.
- 5 Click **Create** to create the JMS topic.
- 6 Repeat this procedure until all topics are set up.

### Creating the JMS Topics on a Single Server

You must configure each JMS Topic listed in this procedure. If you are installing on a clustered server, skip this procedure and instead use [Configuring JMS Topics on a Clustered Server](#) on page 56.

Perform the following steps to create the JMS Topics for a single server:

- 1 Open the **<your\_OVSI\_Server>** page by navigating to **<domain\_name>** → **Services** → **JMS** → **Destinations** → **<your\_OVSI\_Server>**.
- 2 Click the link to the **Configure a new JMS Topic** page.
- 3 Enter the **Name** and **JNDI Name** in the appropriate fields, using the table below for reference:

Purpose	Recommended Name	Required JNDI Name
Select Identity Audit Process	jms.OVSIAuditBroadcast	jms/OVSIAuditBroadcast
Select Identity Cache Cleanup	jms.OVSI_CACHE_TOPIC	jms/OVSI_CACHE_TOPIC

Repeat [Step 1](#) through [Step 3](#) for each JMS Topic in the table:

 You must use the exact JNDI names shown in the table.

- 4 Accept all defaults, with the following exceptions:
  - Tab to the **Enable Store** field and select **True** for each JMS Queue.
- 5 Click **Create** to save your settings.
- 6 Proceed to [Configuring the JTA Settings](#) on page 79.

## Creating JMS Server Members

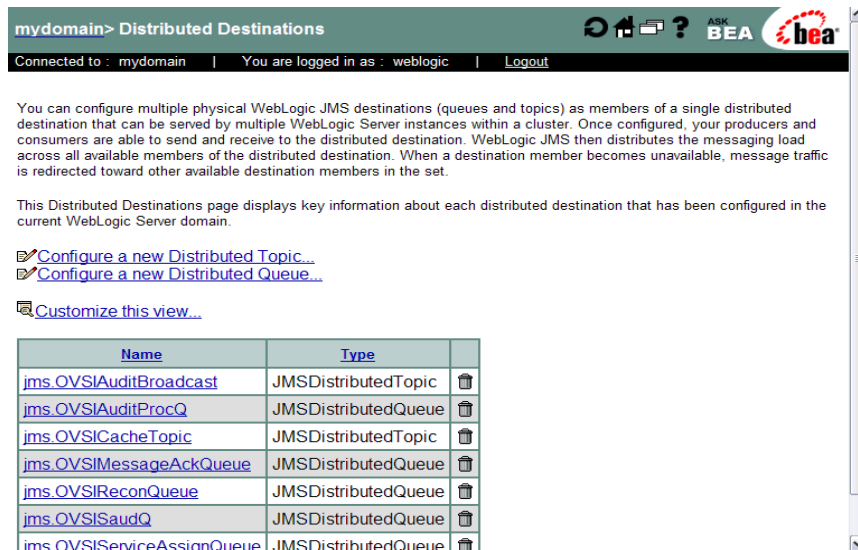
You can configure multiple WebLogic JMS destinations (for both Queues and Topics) as server members of a single distributed destination. The server members can be served by multiple WebLogic server instances within a cluster.

Perform the following steps to create a JMS Server Member for each Queue and Topic.

- 1 Open the **Distributed Destinations** page by navigating to **<domain\_name>** → **Services** → **JMS** → **Distributed Destinations**.



**Figure 32 Distributed Topic Page**



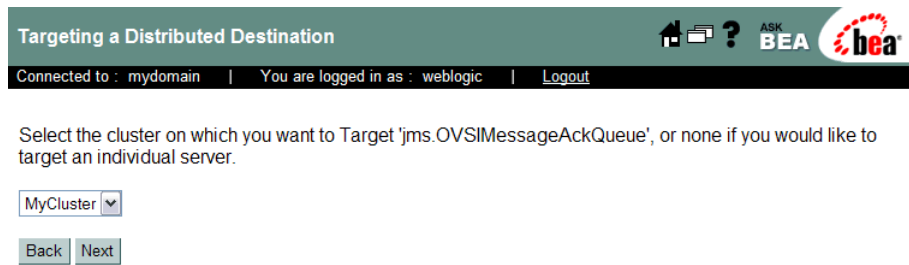
- 2 Select an existing JMS Queue or JMS Topic link in the **Name** column.  
The **Distributed Destinations** page opens, showing the last tab that was saved for the selected JMS Queue or Topic.
- 3 Click the **Auto Deploy** tab to view the **Auto Deploy** page.

**Figure 33 Auto Deploy Page**



- 4 Click the **Create members on the selected Servers (and JMS Servers)** link to proceed to the **Targeting a Distributed Destination** page.

**Figure 34 Targeting a Distributed Destination Page**

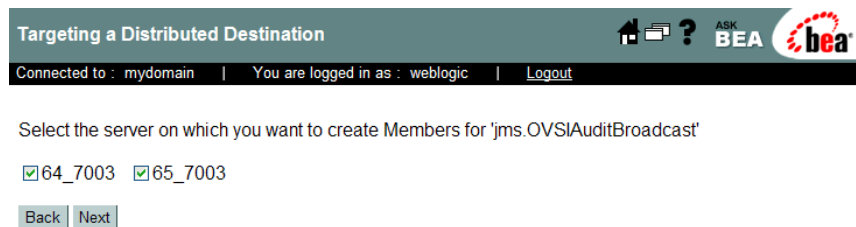


- 1 Make the correct entry

Server Type	Action
Single Server	Select <b>None</b> in the field displayed.
Clustered Server	Select your cluster in the field displayed.

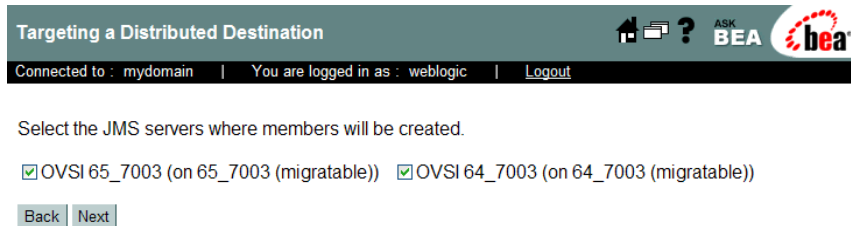
- 5 Click **Next** to proceed to the next **Targeting a Distributed Destination** page, in which you select the servers.

**Figure 35 Targeting a Distributed Destination Page to Select Servers**



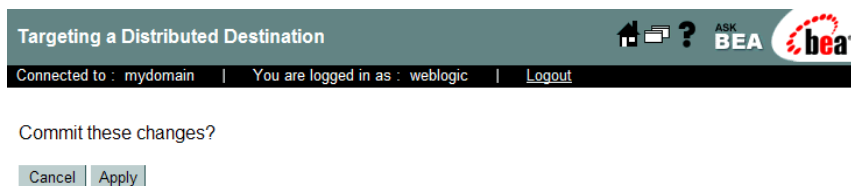
- 6 Select each server on which you want to create members for the JMS Queue or Topic.
- 7 Click **Next** to proceed to the next **Targeting a Distributed Destination** page and select servers.

**Figure 36 Targeting a Distributed Destination Page: Selecting Servers**



- 8 Select each JMS server on which members are to be created.
- 9 Click **Next** to proceed to the next **Targeting a Distributed Destination** page and commit the changes for the JMS Queue or Topic.

**Figure 37 Targeting Distributed Destination Page: Committing Changes**



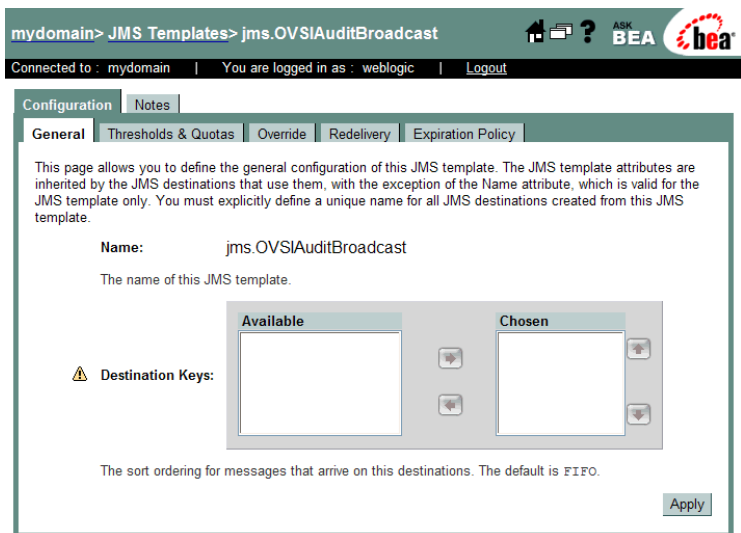
- 10 Click the **Apply** button to commit the changes.
- 11 Repeat this procedure for all JMS Queues and Topics in the Distributed Destinations tree.

## Modifying the JMS Template for JMS Queues and Topics

Perform the following steps to modify the JMS Template for the JMS Queue:

- 1 Open the **JMS Templates** list by navigating to `<domain_name>` → **Services** → **JMS** → **Templates**.
- 2 Open the **JMS Templates General** page for each queue or topic by clicking the link in the **Name** column.

**Figure 38 JMS Templates General Page**



- 3 Click the **Thresholds and Quotas** tab to open the **Thresholds and Quotas** page.
- 4 Tab from field to field and enter the required information.

Field	Action
Bytes Maximum	Enter -1.
Bytes Threshold High	100000000 (100MB)
Bytes Threshold Low	10000000 (10MB)
Bytes Paging Enabled	Enter a check to indicate <b>True</b> .

- 5 Click the **Apply** button to save the settings.
- 6 Click the **Redelivery** tab to view the **Redelivery** page.
- 7 Click the **Redeliver Delay Override** field and enter -1.
- 8 Tab to the **Redelivery Limit** and enter -1.
- 9 Accept all other defaults.
- 10 Click **Apply** to save the settings.

- 11 When configuring the template for the OVSIWorkflowQueue, click the **Override** tab and set the **Delivery Mode Override** to **Persistent**.
- 12 Repeat the procedure until all of the existing JMS Queue and Topic templates have been set up.

## Configuring a JDBC Connection Pool

Configure a JDBC connection pool to enable WebLogic to communicate with the database server by performing the following steps:

- 1 Open the **JDBC Connection** page by navigating to `<domain_name>` → **Services** → **JDBC** → **Connection Pools**.
- 2 Open the **Configure a JDBC Connection Pool** page by clicking the link to **Configure a new JDBC Connection Pool**.

**Figure 39 Configure a JDBC Connection Pool Page**

The screenshot shows the 'Configure a JDBC Connection Pool' page. At the top, there is a breadcrumb trail: 'mydomain> JDBC Connection Pools> Configure'. Below this, there is a navigation bar with 'Connected to : mydomain', 'You are logged in as : weblogic', and a 'Logout' link. The main content area is titled 'Configure a JDBC Connection Pool' and has a sub-section 'Choose database'. A text block explains that the following steps will help create and deploy a connection pool. Below this, there are two dropdown menus: 'Database Type' (set to 'Oracle') and 'Database Driver'. The 'Database Driver' list contains several entries, with '\*Oracle's Driver (Thin) Versions:9.0.1,9.2.0,10' selected. A note at the bottom states: 'Note: Not all drivers in the list are installed. You may need to install the driver you select before you can use it. If your driver is not listed, select Other.' A 'Continue' button is located at the bottom right of the form.

- 3 Select the database type that corresponds to your database from the **Database Type** list box.
- 4 Choose the correct database driver from the **Database Driver** list:
  - For Oracle, select the Oracle Thin Driver, versions 9.0.1, 9.2.0, 10.

- For MS-SQL, select BEA's MS-SQL Server Driver (Type 4) versions 7.0, 2000

5 Click **Continue** to proceed to the **Define Connection Properties** page.

**Figure 40 Define Connection Properties Page**

mydomain> JDBC Connection Pools> Configure

Connected to : mydomain | You are logged in as : weblogic | Logout

Configure a JDBC Connection Pool

**Define connection properties**

Name your new connection pool and provide additional information to connect to your database.

**Name:**

The name of this JDBC connection pool.

**Connection Properties**

**Database Name:**

The name of the database to connect to.

**Host Name:**

The name or IP address of the database server.

**Port:**

The port on the database server used to connect to the database.

**Database User Name:**

The database account user name used in the physical database connection.

**Password:**

**Confirm Password:**

The database account password used in the physical database connection.

6 Tab from field to field and enter the following information:

Field	Value
<b>Name</b>	Enter a name for the connection pool.
<b>Database Name</b>	Enter the name of the database created on the database server for use by Select Identity. For example, Select_Identity.
<b>Host Name</b>	Enter the IP address or host name of the database server.

Field	Value
Port	Enter the database port. The default port for Oracle is 1521.
Database User Name	Enter the Select Identity database admin user name.
Password and Confirm Password	Enter the database user password.

- 7 Click **Continue**.

WebLogic displays the **Test database connection** page and constructs the values displayed in the fields on the page.

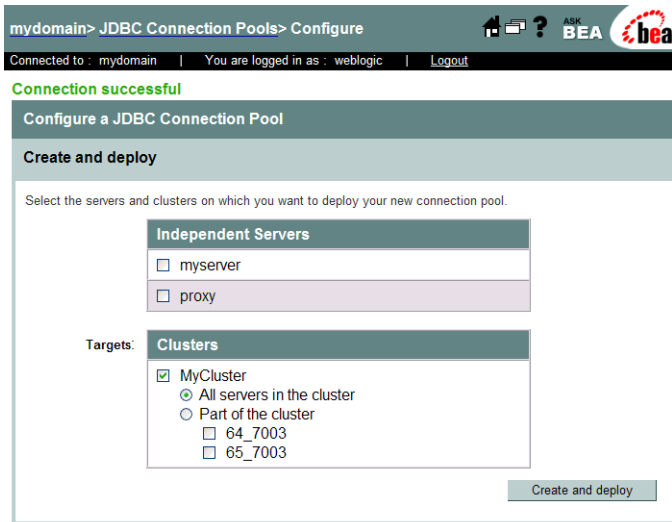
- 8 If you are installing Select Identity with Oracle 9i or 10g, add the following to the **Properties** field. Enter the value on a separate line from any pre-existing content in that field:

```
SetBigStringTryClob=true
```

- 9 Click **Test Driver Configuration** to validate the driver configuration.

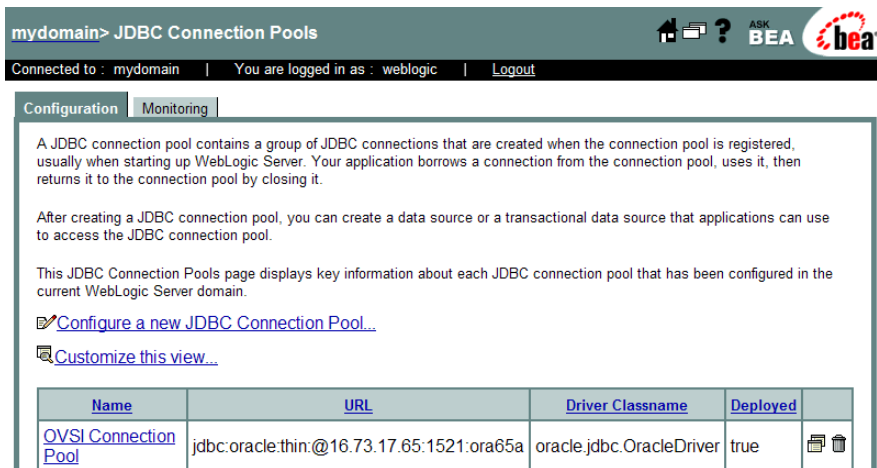
This step verifies that WebLogic can connect to the database. If the connection is successful, the **Configure a JDBC Connection Pool** page opens with a message in the top left corner to indicate that connection was successful.

**Figure 41 Configure a JDBC Connection Pool Page**



- 10 Check the box corresponding to the cluster designated for Select Identity.
- 11 Click **Create and Deploy** to deploy the connection pool and return to the **JDBC Connection Pools Configuration** page.

**Figure 42 JDBC Connection Pools Configuration Page**





- 12 In the list of connection pools, click the link to the new connection pool in the **Name** column.
- 13 Click the **Target and Deploy** tab to verify that your server is selected.
- 14 Click the **Connections** tab to view the **Connections** page.
- 15 Set the following properties:
  - Initial Capacity = 15
  - Capacity Increment = 5
  - Maximum Capacity =100
- ▶ **Maximum Capacity** defines the maximum number of connections per server. If you set the maximum capacity to 100 on a cluster with three servers, you can open maximum of 300 connections. Check with your database administrator to determine the best setting for your database environment.
- 16 Select the Statement Cache Type: **LRU** or **Fixed**.
- 17 Enter the appropriate **Statement Cache Size**.

Server Type	Statement Cache Size
Single server	Statement Cache Size = 20
Clustered servers	Statement Cache Size = 20

- 18 Scroll to the bottom of the page and click the link to show **Advanced Options**.
- 19 Check the box labeled **Test Reserved Connections**.
- 20 Click **Apply** to save your settings.

## Configuring the JDBC Data Source

Perform the following steps to configure a JDBC Data Source. For clustered servers, repeat these steps for each server in the cluster:

- 1 Open the **Data Sources Configuration** page by navigating to **<domain\_name> → Services → JDBC → Data Sources**.

- Open the **Configure a JDBC Data Source** page by clicking the link to **Configure a new JDBC Data Source**.

**Figure 43 Configure a JDBC Data Source Page**

mydomain> JDBC Data Sources> Configure

Connected to : 16.73.17.145 :7001 | You are logged in as : system | Logout

**Configure a JDBC Data Source**

**Configure the data source**

Define your new JDBC data source.

**Name:**

The name of this JDBC data source.

**JNDI Name:**

The JNDI path to where this JDBC data source is bound.

**Honor Global Transactions**

Specifies whether this data source will participate in existing global (XA) transactions. Unchecking this option while creating the data source should be done rarely and with care. This option can not be changed once the data source is created.

**Emulate Two-Phase Commit for non-XA Driver**

Specifies whether the JDBC resource will emulate participation in a global transaction. This option is only applicable when the associated connection pool uses a non-XA JDBC driver and when global transactions are honored in the data source.

- Enter the following information:

Field	Action
<b>Name</b>	Enter a name for the new data source.
<b>JNDI Name</b>	Enter <code>jdbc/TruAccess</code> .
<b>Honor Global Transactions</b>	Click the checkbox to enable this setting.
<b>Emulate Two-Phase Commit for non-XA Driver</b>	Click the checkbox to enable this setting.

- Click **Continue** to proceed to the **Connect to connection pool** page.

**Figure 44 Connect to Connection Pool Page**

Configure a JDBC Data Source

Connect to connection pool

Associate your newly created JDBC data source with a connection pool.

Pool Name:

The JDBC connection pool associated with this data source. The connection pool you select is used to supply database connections to client applications that request a connection from this data source.

Continue

- 5 Select the connection pool from the **Pool Name** list box that was created in [Configuring a JDBC Connection Pool](#) on page 63.
- 6 Click **Continue**.
- 7 Ensure your server is selected on the **Target Data Source** page and click **Create**.

## Modifying the WebLogic Server Class Path

Class paths are critical to a successful installation and must be placed in the correct order.

Perform the following steps to modify the WebLogic Server Class Path. If installing on a cluster, perform this procedure for every server in the cluster.

- 1 On a single server, stop the WebLogic server process at the command line by entering:

```
./stopWebLogic.sh (Linux)
```

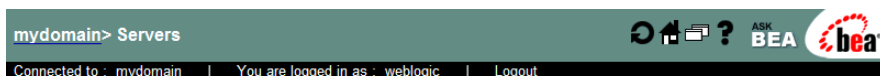
```
stopWebLogic.cmd (Windows)
```

On a cluster, use the following step to stop the servers via the WebLogic console:

- In the left pane of the console, right-click the cluster and select **Start/Stop this Cluster**.
- 2 After stopping the servers, view the **Servers** page by navigating to `<domain_name>` → **Servers**.

Verify that the servers are stopped by viewing the **State** column.

**Figure 45 Servers Page With Running Servers**



A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration. Each WebLogic Server domain must have one server that acts as the Administration Server. In a typical production environment, the Administration Server is where the Administration Console is run and used to perform administrative tasks. By default, the Administration Server is called `myserver`. A typical production environment may also have one or more Managed Servers, which are instances of WebLogic Server used to host enterprise applications.

This Servers page displays key information about each server that has been configured in the current WebLogic Server domain.

[Configure a new Server...](#)

[Customize this view...](#)

Name	Listen Port	Listen Port Enabled	State	
<a href="#">64_7003</a>	7003	true	RUNNING	
<a href="#">65_7003</a>	7003	true	RUNNING	
<a href="#">myserver</a>	7001	true	RUNNING	
<a href="#">proxy</a>	80	true	RUNNING	

- 3 Click the name of the server you want to modify, to open the **Servers General** page.
- 4 Click the **Remote Start** tab, at the top of the main area of the page, to open the **Remote Start** page.
- 5 Tab from field to field and enter the required information as follows. Specific paths may vary on your system:

Field	Action
<b>Java Home</b>	<p>&lt;BEA_HOME&gt;/jrockit81sp5_142_08 (Linux)                      &lt;BEA_HOME&gt;\JDK142_08\ (Windows)</p> <p><b>For single servers:</b>                      You do not need to make this setting.</p>
<b>BEA Home</b>	<p>&lt;BEA_HOME&gt;</p> <p>The actual path to the WebLogic home directory, for example:                      /opt/bea</p> <p><b>For single servers:</b>                      You do not need to make this setting.</p>

Field	Action
<b>Root Directory</b>	<p data-bbox="508 222 939 248">&lt;BEA_HOME&gt;/common/nodemanager</p> <p data-bbox="508 256 1068 282">The path to the Node Manager for the cluster.</p> <p data-bbox="508 296 722 322"><b>For single servers:</b></p> <p data-bbox="508 336 959 362">You do not need to make this setting.</p>
<b>Class Path</b>	<p data-bbox="508 388 1258 480">Class paths are the directory locations of critical system files, and they must be provided in the correct order. Use the examples below for reference.</p> <p data-bbox="508 494 629 520"><b>Windows:</b></p> <p data-bbox="508 534 1273 725">C:\si4.0\weblogic\lib\qname.jar;C:\bea\jdk142_08\lib\tools.jar;c:\bea\weblogic81\server\lib\weblogic_sp.jar;c:\bea\weblogic81\server\lib\weblogic.jar;C:\si4.0\weblogic\sysArchive\connector.jar;C:\si4.0\weblogic\sysArchive\ovsii18n.jar;C:\si4.0\weblogic\lib\commons-logging.jar</p> <p data-bbox="508 734 591 760"><b>Linux:</b></p> <p data-bbox="508 774 1253 996">/opt/si4.0/weblogic/lib/qname.jar:/opt/bea/jrockit81sp5_142_08/lib/tools.jar:/opt/bea/weblogic81/server/lib/weblogic_sp.jar:/opt/bea/weblogic81/server/lib/weblogic.jar:/opt/si4.0/weblogic/sysArchive/connector.jar:/opt/si4.0/weblogic/sysArchive/ovsii18n.jar:/opt/si4.0/weblogic/lib/commons-logging.jar</p> <p data-bbox="508 1008 722 1034"><b>For single servers:</b></p> <p data-bbox="508 1048 1280 1140">You set the class path by editing the <code>myStartWL.sh</code> or <code>myStartWL.cmd</code> script in the WebLogic domain directory where you will be running Select Identity.</p>

Field	Action
<b>Arguments</b>	<pre data-bbox="511 222 899 246">-server -Xms256m -Xmx1024m</pre> <p data-bbox="511 260 1213 284">In Windows, add the argument <code>-XX:MaxPermSize=256M</code></p> <pre data-bbox="511 302 1063 392">-Dcom.truologica.truaccess.property. file=/&lt;OVSI_INSTALL_DIR&gt;/sysArchive/ TruAccess.properties</pre> <p data-bbox="511 437 1021 461">On Linux systems only, add the argument</p> <pre data-bbox="511 475 863 499">-Djava.awt.headless=true</pre> <p data-bbox="511 552 1270 638">Add the argument that specifies the location and name of the logging.properties file for that server, using the example below for reference:</p> <pre data-bbox="511 656 1128 746">-Djava.util.logging.config.file= &lt;OVSI_INSTALL_DIR&gt;/ sysArchive.myServer1_logging.properties</pre> <p data-bbox="511 798 721 822"><b>For single servers:</b></p> <p data-bbox="511 836 1278 923">You must set these arguments by editing the <code>myStartWL.sh</code> or <code>myStartWL.cmd</code> script in the WebLogic domain directory where you will be running Select Identity.</p>

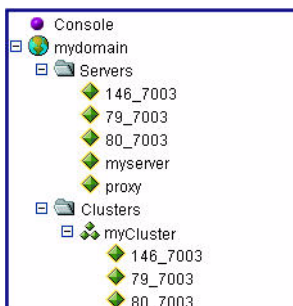
- 6 Click **Apply**.
- 7 On a Weblogic cluster, repeat the process until you have updated each server in the cluster.

## Configuring the Select Identity Execute Queues

Create and configure three execute queues on the WebLogic server and on all servers if you are installing Select Identity on a cluster:

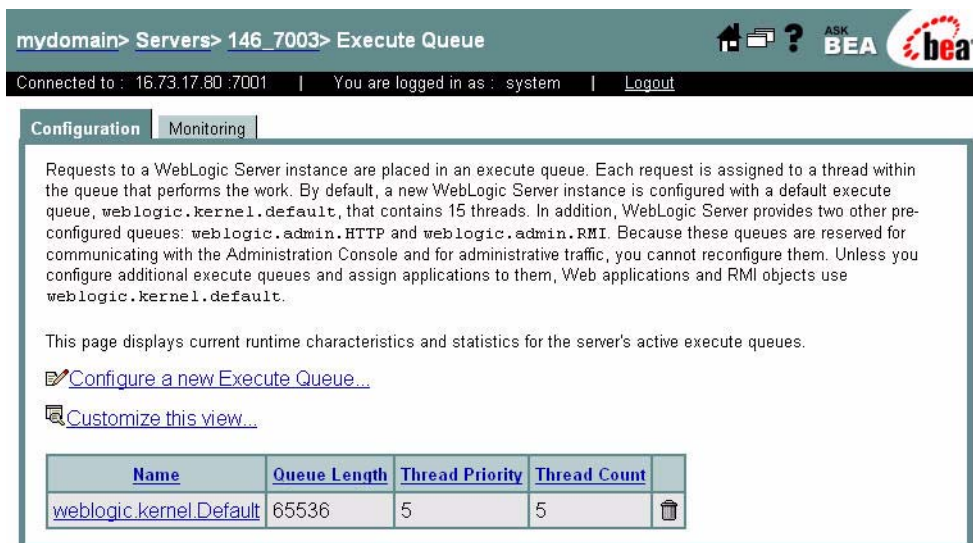
- 1 In the WebLogic console, use the left pane to select a cluster or server. Click the server name to open the server page.

**Figure 46 Selecting the server for Execute Queue Configuration**



- 2 On the server page, scroll down to locate the **Advanced Options**.
- 3 Click **Show** to view the advanced options.
- 4 When the advanced options are visible, scroll down to locate the **Configure Execute Queues** link, at the bottom left of the page.
- 5 Click the **Configure Execute Queues** link to open the **Execute Queues** page. This may only contain the default execute queue as shown in [Figure 47](#).

**Figure 47 Execute Queues Configuration Page**



- 6 Click the link to **Configure a New Execute Queue**.

From this page, you create three queues, named as follows:

- 7 On the new execute queue page, complete the fields for each queue. Use the table below for reference.

Field	hp.ovsi.ejb	hp.ovsi.http	hp.ovsi.soap
Queue Length	65536	65536	65536
Queue Length Threshold Percentage	90	90	90
Thread Count	24	15 (development mode) 25 (production mode)	3
Threads Increase	1	1	0
Thread Maximum	400	400	400
Thread Minimum	5	5	5
Thread Priority	5	10	5

- 8 When you have completed the fields for each queue, click **Apply**.
- 9 When the the **Execute Queues** page reopens, return to [Step 6](#) and repeat until all three queues are created.

## Enabling Anonymous Admin Lookup

Enable Anonymous Admin Lookup by performing the following steps:

- 1 Navigate to the domain where you are installing Select Identity using the left-pane navigation links.
- 2 On the domain page, scroll down and click the link to **Domain-Wide Security Settings**.
- 3 Locate the setting to **Enable Anonymous Admin Lookup**.
- 4 Check the box, if necessary, to enable this setting.
- 5 Click **Apply**.



## Starting the WebLogic Server

*On a single server*, start the WebLogic server process at the command line by entering the following, according to your operating system (Linux or Windows):

```
./myStartWL.sh  
myStartWL.cmd
```

*On a cluster*, use the following step to start the servers via the WebLogic console:

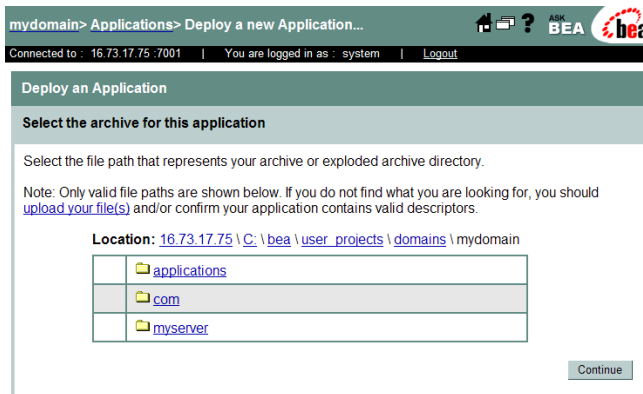
- In the left pane of the console, right-click the cluster and select **Start/ Stop this Cluster**.

## Deploying Select Identity on WebLogic

Deploy Select Identity on the WebLogic Server as follows:

- 1 Log in to the **WebLogic Server Console**.
- 2 Navigate to **<domain\_name> → Deployments → Applications**.  
The Applications page displays.
- 3 Select the **Deploy a new Application** link.  
The **Deploy an Application** page displays.

**Figure 48 Deploy an Application Page**

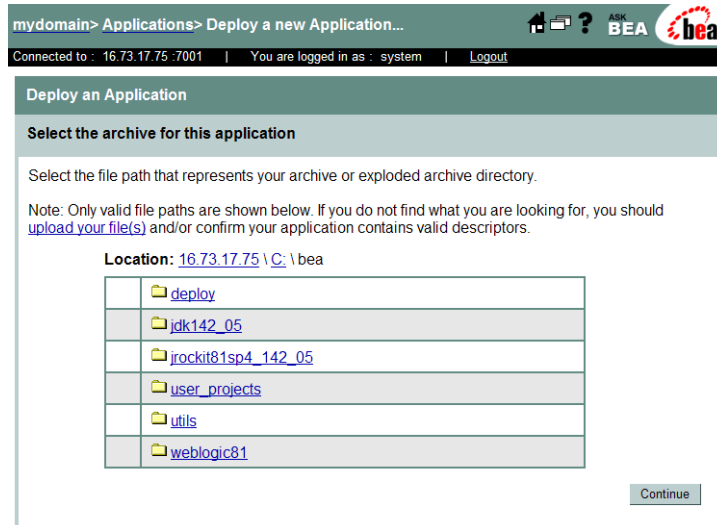


- 4 Locate and select the `1mz.ear` file, which resides in the `<OVSI_INSTALL_DIR>/deploy` directory created in [Creating Select Identity Directories and Copying Installation Files](#) on page 36.

In the figure above, you would click the `bea` directory to open the next page with the `deploy` directory.

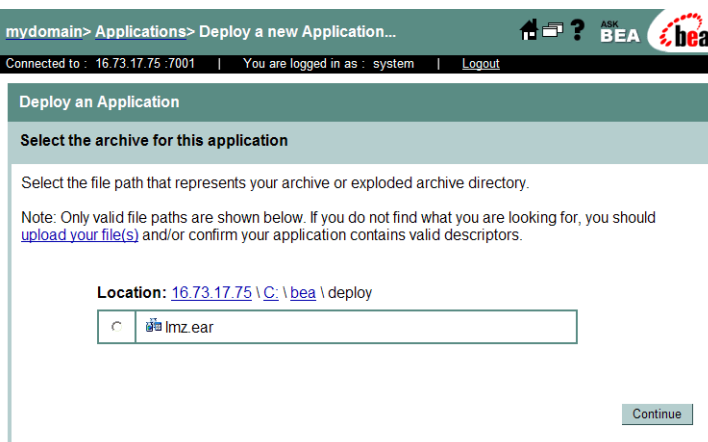
The second **Deploy an Application** page displays with the `bea` subdirectories.

**Figure 49 Second Deploy an Application Page**



- 5 Open the `deploy` folder to proceed to the third **Deploy an Application** page.

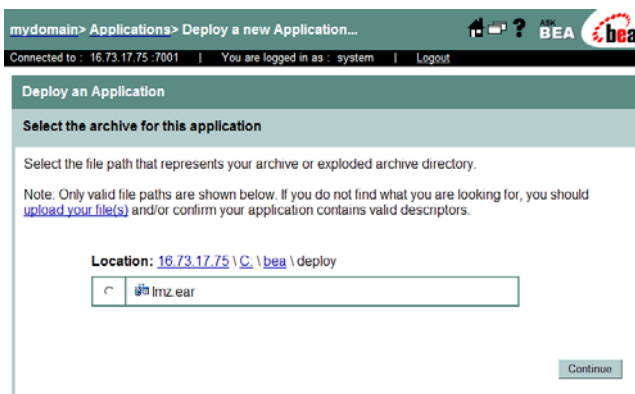
**Figure 50 Third Deploy an Application Page**



- 6 Click the radio button next to the `lmz.ear` file.
- 7 Click **Continue**.

The fourth **Deploy an Application** page displays for you to review your choices and deploy Select Identity.

**Figure 51 Fourth Deploy an Application Page**



- 8 Click **Continue**.
- 9 Select the deployment target (select the cluster if you are installing on a WebLogic cluster) and click **Deploy**. This deploys the `lmz.ear` file module by module onto the selected target. Deployment may take a few minutes to complete.

- 10 Validate deployment by clicking the **Deploy** tab to view the list of deployed applications.
- 11 Locate the newly deployed files in the list to ensure that they have deployed.

**Figure 52 Deploy Page to Validate Select Identity Deployment**

mydomain> Applications> lmz

Configuration | Targets | **Deploy** | Notes

This page allows you to view the deployment status of each module in the application. You may also choose to stop and redeploy all modules within the application using the buttons at the bottom of the page. (To configure additional deployment targets for this application, click the Targets tab.)

Deployment status for EJB Modules

Module	Target	Target Type	Deployment Status	Status of Last Action
usermgrntEjb.jar	myCluster	Cluster	Available	Success
workflowmgrEjb.jar	myCluster	Cluster	Available	Success
resourceEjb.jar	myCluster	Cluster	Available	Success
cdmgrntEjb.jar	myCluster	Cluster	Available	Success
apptntEjb.jar	myCluster	Cluster	Available	Success
idgenEjb.jar	myCluster	Cluster	Available	Success
mailEjb.jar	myCluster	Cluster	Available	Success
attributeEjb.jar	myCluster	Cluster	Available	Success
identityobjEjb.jar	myCluster	Cluster	Available	Success
systemroleEjb.jar	myCluster	Cluster	Available	Success
sysmgrntEjb.jar	myCluster	Cluster	Available	Success
approvalEjb.jar	myCluster	Cluster	Available	Success
reportingEjb.jar	myCluster	Cluster	Available	Success
policyEjb.jar	myCluster	Cluster	Available	Success
provisioningEjb.jar	myCluster	Cluster	Available	Success
applicationEjb.jar	myCluster	Cluster	Available	Success
emailtemplateEjb.jar	myCluster	Cluster	Available	Success
apiEjb.jar	myCluster	Cluster	Available	Success
ruleEjb.jar	myCluster	Cluster	Available	Success
requestBrokerEjb.jar	myCluster	Cluster	Available	Success
externalcallEjb.jar	myCluster	Cluster	Available	Success
provisionconcerEjb.jar	myCluster	Cluster	Available	Success
taserviceessionEjb.jar	myCluster	Cluster	Available	Success
wfengineEjb.jar	myCluster	Cluster	Available	Success
transportEjb.jar	myCluster	Cluster	Available	Success
servermanagerEjb.jar	myCluster	Cluster	Available	Success
emailverificationEjb.jar	myCluster	Cluster	Available	Success
taserviceEjb.jar	myCluster	Cluster	Available	Success
batchBrokerEjb.jar	myCluster	Cluster	Available	Success
autodiscoverEjb.jar	myCluster	Cluster	Available	Success
serviceassignmentEjb.jar	myCluster	Cluster	Available	Success
reconciliationEjb.jar	myCluster	Cluster	Available	Success
auditEjb.jar	myCluster	Cluster	Available	Success
managepasswordEjb.jar	myCluster	Cluster	Available	Success
replacementEjb.jar	myCluster	Cluster	Available	Success
securityEjb.jar	myCluster	Cluster	Available	Success
wfextcallEjb.jar	myCluster	Cluster	Available	Success
changereconEjb.jar	myCluster	Cluster	Available	Success

Deployment Status for Web Application Modules

Module	Target	Target Type	Deployment Status	Status of Last Action
lmz	myCluster	Cluster	Available	Success
attributemappper	myCluster	Cluster	Available	Success

Stop Application    Redeploy Application

- 12 Review the list to make sure all files deployed successfully.

13 Verify that the JMS Settings are correct.



If a setting is not specified, accept the WebLogic default. Refer to [Configuring JMS Settings](#) on page 42 and [Configuring JMS Settings](#) on page 42.

14 After installing Select Identity, refer to [Appendix a, Logging](#) for instructions on configuring the `logging.properties` file.



Configuring logging is crucial. Select Identity may not function properly if you do not configure the `logging.properties` file.

## Additional Configuration

Perform the additional configuration steps documented in this section after you have installed Select Identity using the manual or installer processes. Then see [Configuring HP OpenView Select Identity](#) on page 129 to finish configuring Select Identity.

### Configuring the JTA Settings

Follow the steps below to configure the JTA settings for the server or cluster. You must perform this procedure as part of both the manual and installer procedures:

- 1 Open the **JTA** page by navigating to `<domain_name>` → **Services** → **JTA**.
- 2 Set the timeout to **300** seconds in the **Timeout Seconds** field.
- 3 Click **Apply**.

### Deploying the Select Identity Online Help Files

Select Identity includes an online help module that you must deploy manually after completing either the installer or manual installation processes.

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

To deploy this file, perform the following steps:

- 1 Locate the OVSI `.war` file, which is stored on the HP OpenView Select Identity product CD, in the `application` directory with the `lmz.ear` application file.
- 2 Copy the `.war` file into the `<OVSI_INSTALL_DIR>/deploy` directory.
- 3 Use the instructions provided in [Deploying Select Identity on WebLogic](#) on page 75 to locate and deploy the help files in the same way as you did for `lmz.ear`. On this occasion, however, you must deploy the help files as a Web Application module, by first navigating to **Yourdomain>Deployments>Web Application Modules**.

In addition, other product documentation is provided in PDF format in the `docs` directory on the HP OpenView Select Identity Product CD. Copy these to the directory location of your choice.

---

# 5 Installing Select Identity on IBM WebSphere

This chapter describes how to install and configure Select Identity on a WebSphere application server.

This chapter includes the following topics:

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

## Introduction

The HP OpenView Select Identity product CD provides 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.

Select Identity relies on the Web application server to serve its interface pages, communicate with the database server to store and retrieve data, and send email.

## Important Installation Information

Ensure that you have the information in this topic available before you begin.

For single and clustered servers:

- The SMTP email host to be used by Select Identity

- The login ID used when installing WebSphere
- The login ID for the database server administrator user
- The IP address and host name of the WebSphere admin server

For clusters:

- The directory location on the Network File System where Select Identity shared files will be stored.

This does not apply to JMS file stores, which should not be located under a shared file system but on a private drive.

- The cell and cluster name on which you are installing Select Identity.
- The IP address and hostname of every server in the cluster.
- The directory locations of any processes that you will need to start or stop, such as the WebSphere console or node managers.

## Prerequisite Configuration Procedure

You can install Select Identity on a WebSphere standalone server or on multiple servers in a cluster. In each case, you must perform the prerequisite configuration steps in this section.



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

On an IBM WebSphere cluster, ensure the following prerequisites are met:

- WebSphere is installed on every node and meets the system requirements as listed in [System Requirements](#) on page 7.
- The Network Deployment Manager is configured with appropriate cells, 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.

### Configuration Steps

To prepare WebSphere for installation, complete the following steps:

- 1 Start the WebSphere server, if it is not running.
- 2 Verify that the correct policy files are present on the WebSphere server and determine if the system needs to be upgraded to the “unlimited strength” policy files.


In Windows, you can typically find these files in the following location:

```
$WAS_HOME\java\jre\lib\
```

The policy files are:

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

If either file is absent, you can download it from the IBM Web site..

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

- 3 For standalone and every server in a cluster, copy the following files to the `$WAS_HOME/lib/ext` directory:  

```
sysArchive/connector.jar  
sysArchive/ovsii18n.jar
```
- 4 Make sure that these files reside in this directory when starting the WebSphere application server.
- 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. The online help is deployed as a Web Application Archive (a `.war` file) after you have installed Select Identity.

- 6 Ensure that the system on which WebSphere is installed meets the minimum requirements, as documented in [System Requirements](#) on page 7.
- 7 Ensure that your Select Identity database is configured as described in [Configuring the Database Server](#) on page 15.
- 8 Log on to the WebSphere Administrative Console as admin.
- 9 Copy the following JCE files to %WAS\_HOME%/java/jre/lib/security. Perform this step on every node if you are installing on a cluster.

US\_export\_policy.jar

local\_policy.jar

- 10 Copy sunjce\_provider.jar to %WAS\_HOME%/java/jre/lib/ext. Perform this step on every node if you are installing on a cluster.

For Windows, you can obtain these files from IBM's Web site; for Unix, you can obtain them from Sun Microsystems' Web site.

- 11 Be sure you set the following properties in the TruAccess.properties file before starting Select Identity for the first time, to ensure that the database will initialize correctly:

```
truaccess.repository.type=<your_database>
truaccess.repository.oracle.driver.bea=<yes or no>
```

If you are using the BEA driver for ORACLE (not the thin driver), set the second property to yes; otherwise, no. See [Configuring TruAccess.properties Required Settings](#) on page 129 for more details.

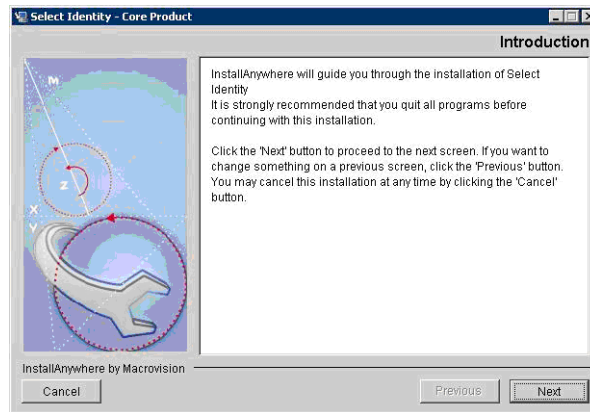
## Using the Select Identity Installer

This section contains procedures for installing Select Identity using the installer. Before completing these steps, be sure to complete the procedures included in the [Prerequisite Configuration Procedure](#) on page 82.

## Installation Wizard Procedure

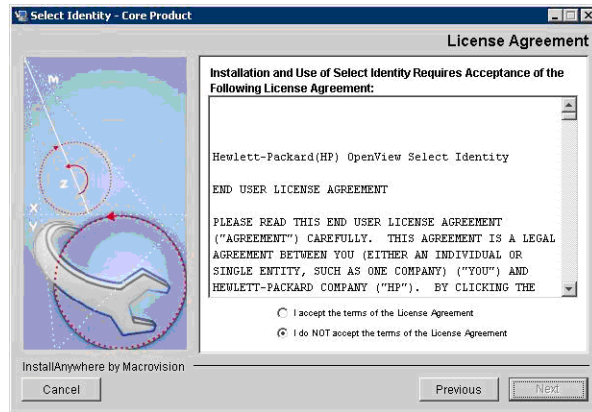
- 1 Log on to the operating system as the same user that was used to install WebSphere. You must run the installer directly from the application server's local machine, or the Deployment Manager's node in a cluster; it is not possible to run the installer remotely.
- 2 Mount the Select Identity CD, navigate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

**Figure 53 The InstallAnywhere Introduction page**



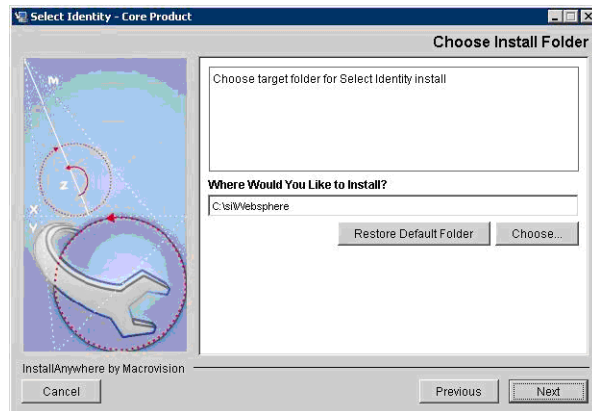
- 3 Click **Next** to review the License Agreement.

**Figure 54 The License Agreement page**



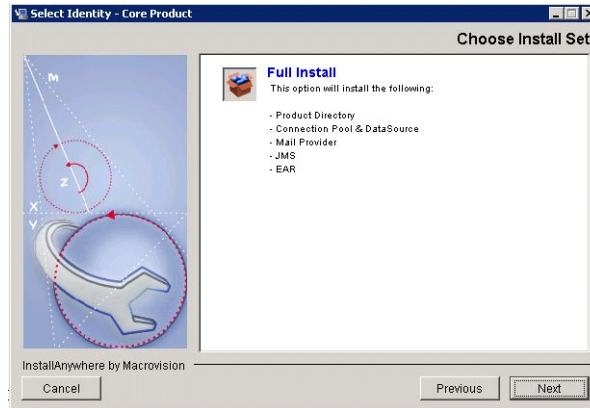
- 4 Click the radio button labeled **I Accept the License Agreement** and click **Next** to proceed to the **Choose Install Folder** page.

**Figure 55 The Choose Install Folder Page**



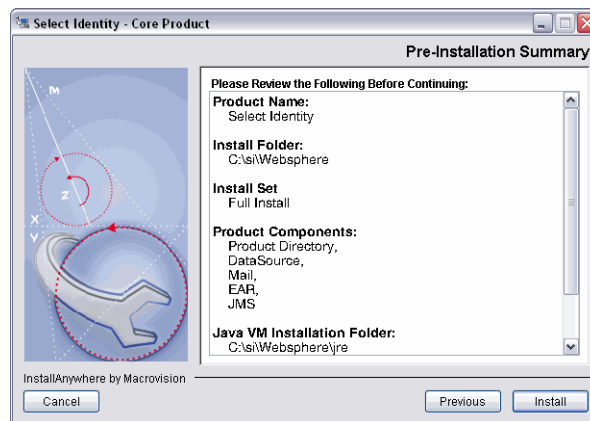
- 5 Enter or browse to the path to the intended Select Identity home directory and click **Next** to proceed to the **Choose Install Set** page.

**Figure 56 The Choose Install Set Page**



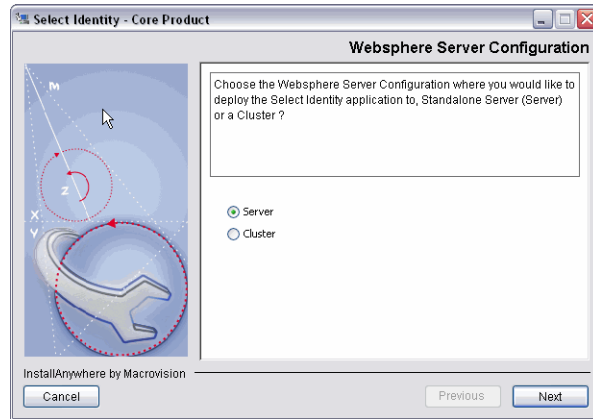
- 6 Select **Full Install** to accept the default configuration and click **Next** to proceed to the **Pre-Installation Summary** page.
- 7 Review the summary information before you click **Install** to continue.

**Figure 57 The Pre-Installation Summary Page**



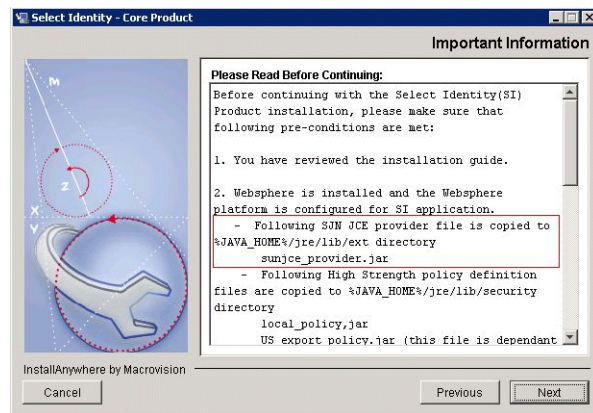
The wizard installs the files according to your settings. A progress bar indicates that the installation is in progress. When installation is complete, the installer displays the **Server Configuration** page.

**Figure 58 Server Configuration Page**



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

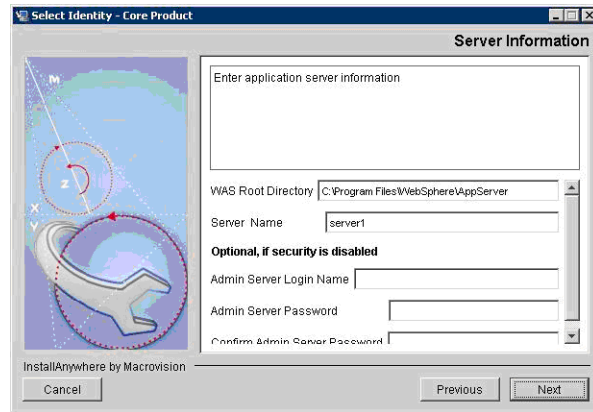
**Figure 59 The Important Information page**



- 10 Review and follow the instructions on this page, then click **Next** to proceed.
- 11 If you are installing on a cluster, skip to the instructions [For Clustered Servers](#) on page 92.

If you are installing on a standalone server, proceed to [Step 12](#).

**Figure 60 The Server Information page**



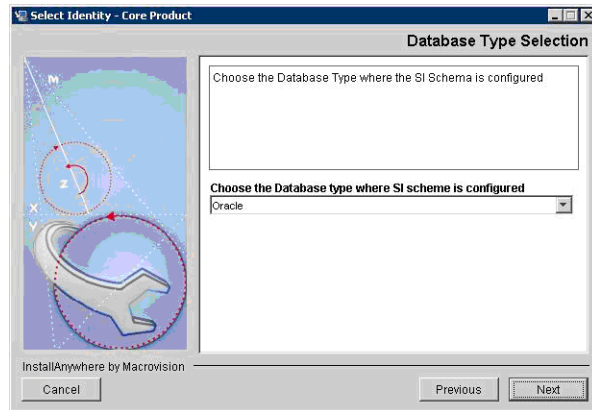
12 Specify settings for the admin server, as follows:

- **WAS Root Directory** — The directory where the WebSphere Application Server is installed (typically C:\Program Files\WebSphere\AppServer on a Windows system).
- **Server Name** —The host name of the node on which you are installing Select Identity
- **Admin Server Login Name** — The user name for logging into the WebSphere Admin Server.
- **Admin Server Password** — The password of the Admin account. This is optional when the Deployment Manager does not have security enabled. If you enter a password, you must also confirm it in the **Confirm Admin Server Password** field.

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

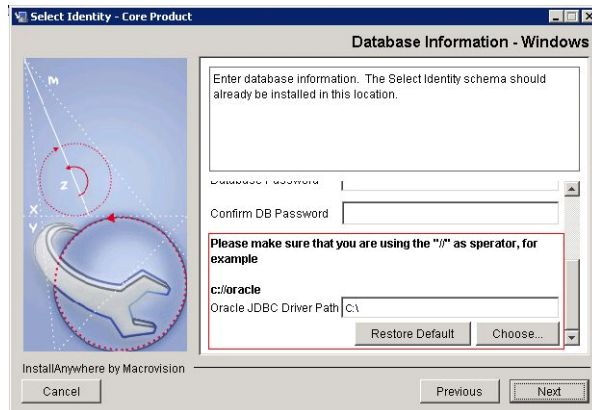
14 When installation is complete, the installer displays the **Database Type Selection** page.

**Figure 61 The Database Type Selection page**



- 15 Select your database type and click **Next** to proceed to the **Database Information** page.

**Figure 62 The Database Information Page**



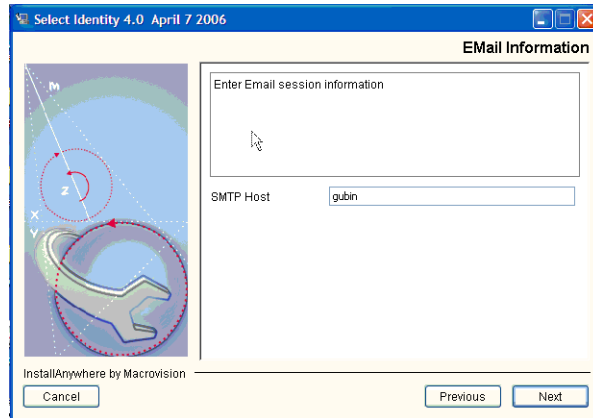
- 16 Complete the fields with the appropriate information about your database:
  - **Database Server Name** — The host name of the database server.
  - **Database Server Port** — The port on which the database server communicates with Select identity.
  - **Database Name** — The name of the Select Identity database.
  - **Database Login** — The user name for logging in to the database.



- **Database Password and Confirm Database Password** — the password for logging in to the database
- **Oracle JDBC Driver Path** — The path to the Oracle JDBC driver

17 Click **Next** to proceed to the **Email Information** page.


**Figure 63 The Email Information page**



- 18 Specify the name of the SMTP host Select Identity will use when sending email, then click **Next** to proceed to the **Set WebSphere Variable** page.
- 19 As described in the reminder on the **Set WebSphere Variable** page, ensure that the environment variable is set.
- 20 Click **Next**. After completing the server, email, and database settings, the installer displays the **Installation Complete** page.
- 21 Click **Done** to close the installer.
- 22 Refer to [Appendix B, Configuring TruAccess.properties](#) for information about configuring the `TruAccess.properties` file for your environment.
- 23 Stop and restart WebSphere.
- 24 After WebSphere has restarted, set the JTA timeout to 300 seconds, as documented in the manual installation procedures under [Deploying the JDBC Provider and Data Source for Oracle, Step 13](#).
- 25 Log in to Select Identity using the information in [Logging In to Select Identity on IBM WebSphere](#) on page 127.

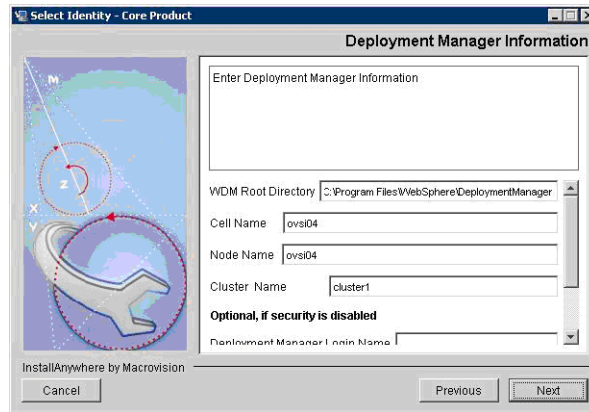
## For Clustered Servers

The instructions in this section apply only if you are installing Select Identity on a WebSphere cluster. This part of the installation procedure is where the individual nodes in the cluster are specified.

-  During this process, do not use the **Previous** button. There is a limitation in the InstallAnywhere installer that can cause installation to fail when this control is used as intended for cluster node installation.

- 1 After reviewing the **Important Information** page shown in [Figure 59](#), click **Next** to proceed to the **Deployment Manager Information** page.

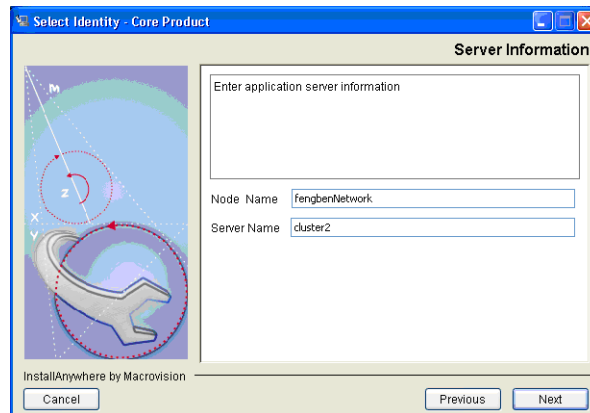
**Figure 64 The Deployment Manager Information page**



- 2 Specify settings for the WebSphere Deployment Manager, by completing each of the fields as follows:
  - **WDM Root Directory** — The directory where the WebSphere Deployment Manager is installed (typically C:\Program Files\WebSphere\DeploymentManager) on a Windows system.
  - **Cell Name** — The name of the WebSphere cell on which the server is located. This limits the visibility to all servers on the named cell.
  - **Node Name** — The name of the node; this limits visibility to all servers on the named node. Node scope has precedence over cell scope.
  - **Deployment Management Login Name** — The user name for logging into the WebSphere Deployment Manager.

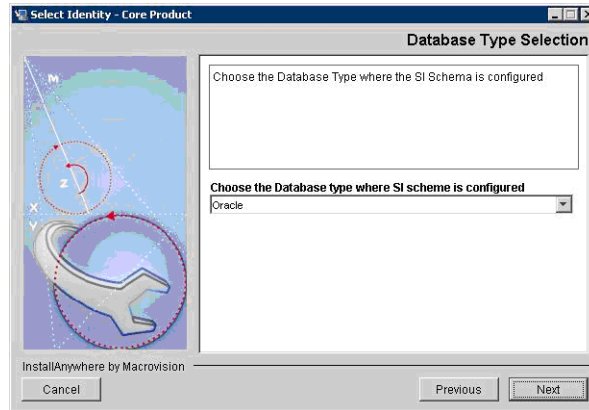
- **Deployment Management Password** — The password of the Admin account. A value is not required if security is not enabled. This is optional when the Deployment Manager does not have security enabled. If you enter a password, you must also confirm it in the **Confirm Deployment Management Password** field.
  - **Cluster Name** — the name of the cluster on which you are installing Select Identity
- 3 After making the settings, click **Next** to proceed to the **Application Server Information** page.

**Figure 65 the Application Server Information page**



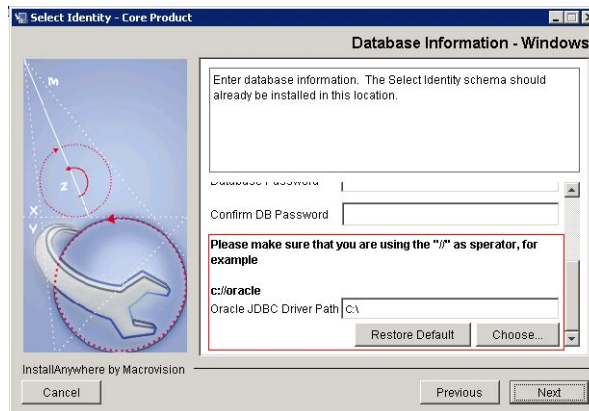
- 4 Specify settings for the WebSphere Application Server, as follows:
- **Node Name** — The WebSphere name of the node on which you are installing Select Identity.
  - **Server Name** — The host name of the node on which you are installing Select Identity.
- 5 After making the settings, click **Next** to proceed to the **Database Type Selection** page.

**Figure 66 The Database Type Selection page**



- 6 Select your database type from the menu and click **Next** to proceed to the **Database Information** page.

**Figure 67 The Database Information Page**

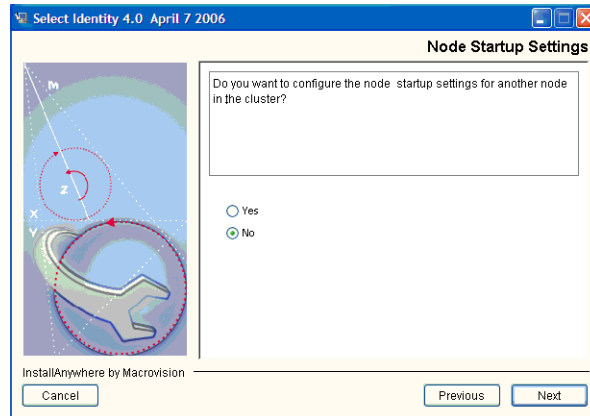


- 7 Complete the fields as follows:
  - **Database Server Name** — The host name of the database server.
  - **Database Server Port** — Used to communicate with Select Identity.
  - **Database Name** — The name of the database.
  - **Database Login** — The user name for logging in to the database.
  - **Database Password and Confirm Database Password** — The password for logging in to the database.

- **Oracle JDBC Driver Path** — The path to the Oracle JDBC driver.

8 Click **Next** to proceed to the **Node Startup Settings** page.

**Figure 68 The Node Startup Settings page**



9 If you need to install Select Identity on additional nodes, click **Yes**. Otherwise, click **No** to proceed to the **Email Information** page, and click **Next**.

10 Proceed as documented from [Step 14](#) on page 89.

## Manual Installation Procedures

This section covers the following topics:

- [Creating Directories and Copying Files](#)
- [Configuration Scope](#)
- [Creating a Select Identity Mail Session](#)
- [Creating a J2C Authentication Data Entry](#)
- [Deploying the JDBC Provider and Data Source for Oracle](#)
- [Configuring a JMS Queue Factory](#)
- [Configuring a JMS Topic Factory](#)
- [Creating the JMS Queues](#)
- [Creating JMS Topics](#)

- [Configuring the Application Server](#)
- [Configuring the Message Listener Service](#)
- [Configuring Server Components](#)
- [Deploying Select Identity](#)

## Creating Directories and Copying Files

The following steps prepare the application 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, storing its files and subdirectories. The product installation and connector installations will reference this directory. For example, you could create the `C:\Select_Identity` directory on Windows or `/opt/Select_Identity` on UNIX.

On a cluster, this directory must be in the network file system, accessible by all servers in the cluster. Refer to the Weblogic installation guide for more information.

- 2 Copy the following files from the Select Identity product CD to the new directory.

Additional directories may be required based on the configuration of the `TruAccess.properties` file. See [Configuring TruAccess.properties](#) on page 143 for details.

- `application/websphere_lmz.ear` for WebSphere
- `properties/TruAccess.properties`

Create a new sub-directory for each connector type that you install and install connector-specific information in its respective directory.

For standalone and every server in a cluster, copy the following files to the `$WAS_HOME/lib/ext` directory:

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

Make sure that these files reside in this directory when starting the WebSphere application server.

- 3 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. The online help is deployed as a Web Application Archive after you have installed Select Identity.
- 4 Ensure that the system where WebSphere is installed meets the *minimum* requirements, as documented in [System Requirements](#) on page 9.
- 5 Log on to the WebSphere Administrative Console as **admin**.
- 6 Copy the following JCE files to %WAS\_HOME%/java/jre/lib/security. Perform this step on every node if you are installing on a WebSphere cluster.  

```
US_export_policy.jar
local_policy.jar
```
- 7 Copy sunjce\_provider.jar to %WAS\_HOME%/java/jre/lib/ext.
- 8 For Windows, you can obtain these files from IBM's Web site; for Unix, you can obtain them from Sun Microsystems' Web site.

## 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:

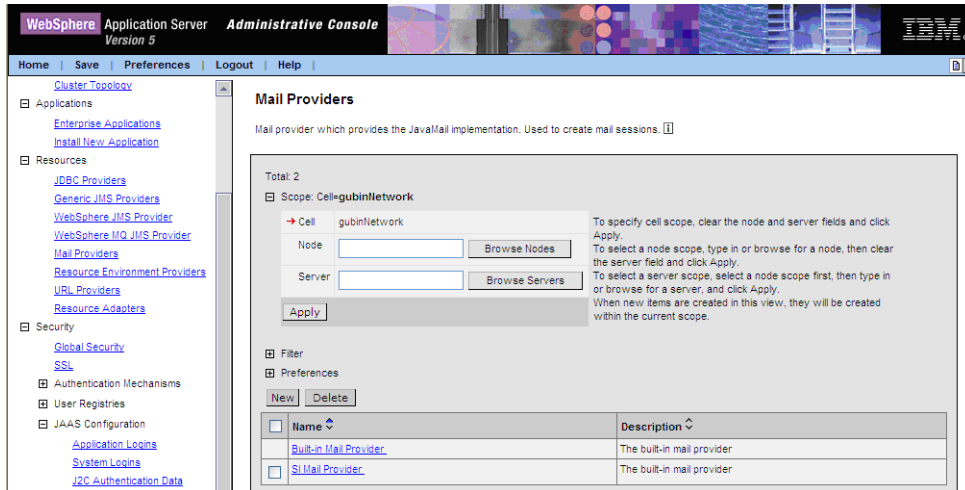
<b>Configuration</b>	<b>Mail</b>	<b>J2C Auth</b>	<b>JDBC Provider</b>	<b>JMS Queue Factory</b>	<b>JMS Topic Factory</b>	<b>JMS Queue</b>	<b>JMS Topic</b>
Standalone	Node	Node	Node	Node	Node	Node	Node
Cluster	Cell	Node	Server	Node	Node	Cell	Cell

## Creating a Select Identity Mail Session

- 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**.

**Figure 69 The Mail Providers page**



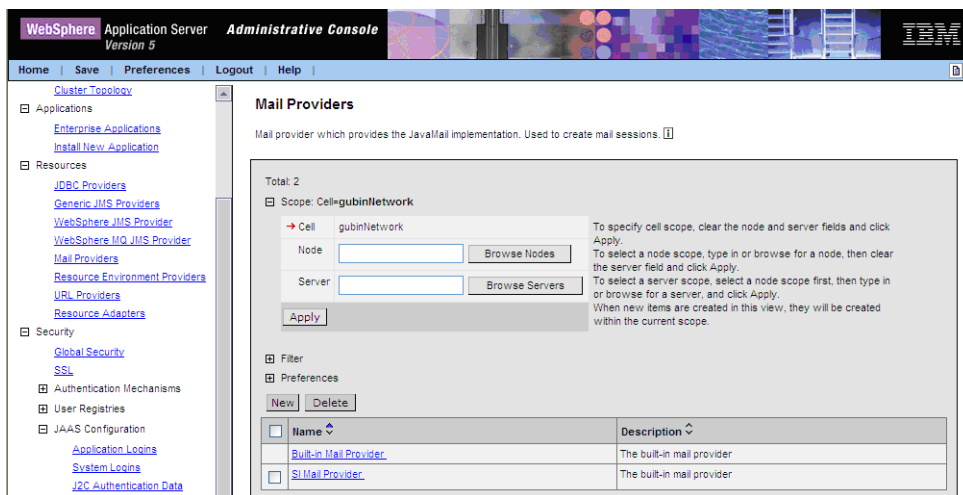
- b Select **Node** for the scope of the new mail session on a Standalone server.

Select **Cell** for the scope of the new mail session on a cluster configuration.

- c Click **Apply**
- d Click **New**, in the center of the page.



**Figure 70 The New Mail Provider page**



- e On the **New Mail Provider** page, complete the fields as follows:
    - Name** — Enter SI Mail Provider.
    - Description** — Enter an appropriate description, such as Select identity Mail Provider.
  - f Click **OK** to create the mail session.
  - g Click **Save**, in the page banner, and then click **Save** again, in the **Save to Master Configuration** area of the page, to save your changes.
- 2 Configure a Select Identity mail session in the new Select Identity mail provider by completing the following steps:
    - a Return to the Mail Providers page.
    - b Click the link to the new provider in the Mail Providers list in the center of the page.
    - c Click the **Mail Sessions** link in the **Additional Properties** area of the **SI Mail Provider** page.

**Figure 71 Creating a new mail session**

[Mail Providers](#) > [SI Mail Session](#) > [Mail Sessions](#) >

**SI Mail Session**

Configurations for mail support.

Configuration		
<b>General Properties</b>		
Scope	<input type="text" value="cells:ovsi04.nodes:ovsi04"/>	The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	<input type="text" value="SI Mail Session"/>	The required display name for the resource.
JNDI Name	<input type="text" value="mail/TruAccess"/>	The JNDI name for the resource.
Description	<input type="text"/>	An optional description for the resource.
Category	<input type="text"/>	An optional category string which can be used to classify or group the resource.
Mail Transport Host	<input type="text" value="16.157.129.33"/>	Specifies the server to connect to when sending mail.
Mail Transport Protocol	<input type="text" value="smtp"/>	Specifies the transport protocol to use when sending mail.
Mail Transport User ID	<input type="text"/>	Specifies the user ID to use when the mail transport host requires authentication.
Mail Transport Password	<input type="text"/>	Specifies the password to use when the mail transport host requires authentication.
Mail From	<input type="text"/>	Specifies the mail originator.
Mail Store Host	<input type="text"/>	Mail account host (or "domain") name.
Mail Store Protocol	<input type="text" value="pop3"/>	Specifies the protocol to be used when receiving mail.
Mail Store User ID	<input type="text"/>	The user ID of the mail account.
Mail Store Password	<input type="text"/>	The password of the mail account.
Debug	<input type="checkbox"/> Enable debug mode	When true, JavaMail's interaction with mail servers, along with this mail session's properties will be printed to stdout.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		
<b>Additional Properties</b>		
<a href="#">Custom Properties</a> : Properties that may be required for Resource Providers and Resource Factories. For example, most database vendors require additional custom properties for data sources that will access the database.		

d Provide the following information:

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

- e Click **OK** at the bottom of the page. The **Mail Sessions** page now includes the new session.
- f Click **Apply** at the bottom of the Mail Sessions page.
- g Click **Save** to complete the mail session configuration.
- h Click **Save** again, in the **Save to Master Configuration** area in the center of the page.

## Creating a J2C Authentication Data Entry

Complete the steps appropriate to your configuration to create a J2C authentication data entry for the Select Identity database user ID.

### Cluster Configurations

Creating the J2C Authentication Data Entry must be performed at the node level on a cluster, but doing so via the console may cause configuration problems. Therefore, a Jython script is provided below that you can modify and execute to create the J2C Authentication Data Entry without using the console.

Before you perform this procedure on a cluster, refer to the WebSphere documentation.

**Figure 72 J2C Authentication Data Entry creation script for WebSphere clusters**

```
security = AdminConfig.getid('/Security:/')
print security

# Create JAAS Authentication Data
alias = ['alias', '<NODE NAME>/<ALIAS NAME>']
userid = ['userId', '<USER ID>']
password = ['password', '<PASSWORD>']
jaasAttrs = [alias, userid, password]

AdminConfig.create('JAASAuthData', security,
jaasAttrs)
AdminConfig.save()
```

- 1 Use a text editor to enter the script and modify the following items to reflect your actual authentication data:

Item	Value
Node Name	The name of the node as it appears in the WebSphere console
Alias Name	An alias name of your choice
User ID	The user ID for J2C Authentication
Password	The password associated with the authentication user ID

- 2 Save the script to an appropriate location as `createJAAS.py`.
- 3 Execute the script using the following example at the command line from the `WAS_HOME\DeploymentManager\bin` directory:

```
wsadmin -lang jython -f "filename"
```

"filename" should be entered as the path to the script you saved in [Step 2](#).

## Standalone Server Configurations

- 1 Navigate to **Security** → **JAAS Configuration** → **J2C Authentication** data in the left panel of the console.

**Figure 73 The J2C Authentication Data page**

**J2C Authentication Data Entries**

Specifies a list of userid and password for use by Java 2 Connector security. ⓘ

Total: 1

Filter

Preferences

<input type="checkbox"/> Alias	User ID	Description
<input type="checkbox"/> <a href="#">pva04/ORACLE10g</a>	rc80511	

- 2 Click **New**.

**Figure 74 The J2C Authentication Page for Oracle**

[J2C Authentication Data Entries](#) >

**ORACLE10g**

Specifies a list of userid and password for use by Java 2 Connector security. ⓘ

**Configuration**

General Properties		
Alias	<input type="text" value="ORACLE10g"/>	ⓘ Specifies the name of the authentication data entry.
User ID	<input type="text" value="WS1V401RC1"/>	ⓘ Specifies the J2C authentication data user ID.
Password	<input type="password" value="*****"/>	ⓘ Specifies the password to use for the target Enterprise Information System.
Description	<input type="text"/>	ⓘ Specifies an optional description of the authentication data entry. For example, this authentication data entry is used to connect to DB2.

3 Provide the following information:

Field	Value
Alias	Enter a name for the entry, such as Oracle10g.
User ID	Enter the user ID for the Select Identity database user.
Password	Enter the Select identity database user password.

4 Click **OK**.

5 Click **Save** in the page banner.

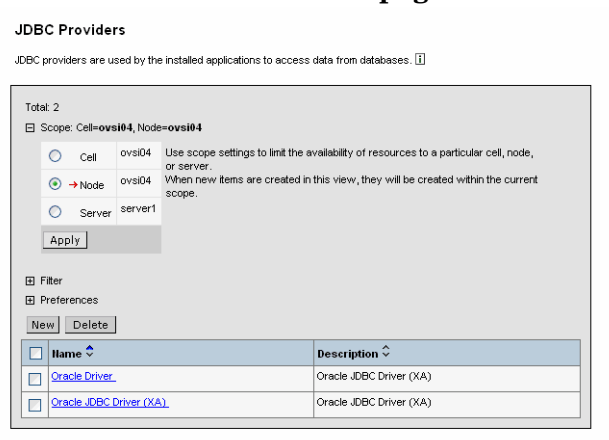
6 Click **Save** in the **Save to Master Configuration** area to complete the J2C Authentication Data Entry.

## Deploying the JDBC Provider and Data Source for Oracle

Deploy the Oracle JDBC Provider by completing the following steps:

1 Navigate to **Resources** → **JDBC Providers**.

**Figure 75 The JDBC Providers page**



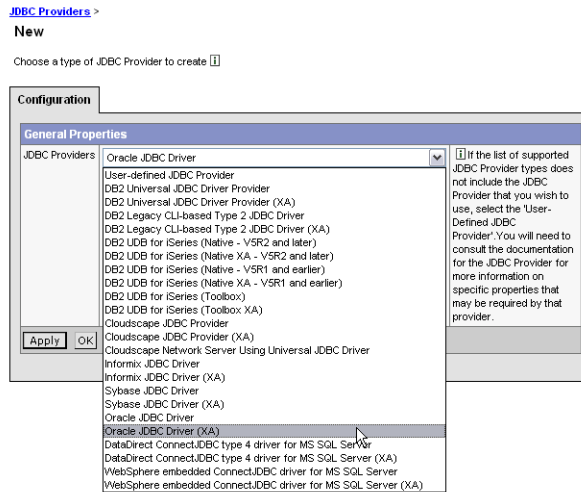
- 2 Select the node on which you are installing from the **Scope** selections, and click **Apply**.



If you are installing on a cluster, these steps must be performed on every server in the cluster.

- 3 Click **New** below the **Scope** selections.
- 4 Open the **JDBC Providers** menu and select the **Oracle Driver** or **Oracle Driver (XA)** option, as appropriate.

**Figure 76 Selecting the JDBC provider type**



- 5 Click **OK** to proceed to the **Configuration** page.

**Figure 77 Configuring a new Oracle JDBC provider**

[JDBC Providers >](#)  
**New**

JDBC providers are used by the installed applications to access data from databases. [?]

**Configuration**

General Properties		
Scope	cells:ovsi03.nodes:ovsi03	[?] The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	Oracle JDBC Driver	[?] The name of the resource provider.
Description	Oracle JDBC Driver	[?] A text description for the resource provider.
Classpath	\$(ORACLE_JDBC_DRIVER_PATH)ojdbc14j or	[?] A list of paths or JAR file names which together form the location for the resource provider classes. Classpath entries are separated by using the ENTER key and must not contain path separator characters (such as '/' or '\'). Classpaths may contain variable (symbolic) names which can be substituted using a variable map. Check your drivers installation notes for specific JAR file names which are required.
Native Library Path		[?] An optional path to any native libraries (.dll's, .so's). Native path entries are separated by using the ENTER key and must not contain path separator characters (such as '/' or '\'). Native paths may contain variable (symbolic) names which can be substituted using a variable map.
Implementation Classname	oracle.jdbc.pool.OracleConnectionPc	[?] The Java classname of the JDBC driver implementation.

Apply OK Reset Cancel

- 6 Enter a name for the JDBC provider in the **Name** field, such as SI Oracle JDBC Driver.
- 7 Enter the path to the JDBC driver in the **ClassPath** field, as indicated by `$(ORACLE_JDBC_DRIVER_PATH)`. This must be correct, otherwise Select Identity will not be able to access the database. (In Windows, the format of the path should be `C:\\oracle\\driver.`)
- 8 Click **Apply** to save your settings.



It is recommended that you locate the jar file on a shared directory on a cluster, in addition to placing a copy on each node.

- 9 Click the link to **Data Sources** at the bottom of the page under **Additional Properties**.



## Figure 78 The JDBC Data Sources page

[JDBC Providers](#) > [Oracle Driver](#) >

### Data Sources

Data Source is used by the application to access the data from the database. A data source is created under a JDBC provider which provides the specific JDBC driver implementation class. [i](#)

Total: 1			
<input type="checkbox"/> Filter			
<input type="checkbox"/> Preferences			
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Test Connection"/>			
<input type="checkbox"/> Name	JNDI Name	Description	Category
<input type="checkbox"/> jdbc:TruAccess	jdbc/TruAccess	Data source template	

10 Click **New** to proceed to the **Configuration** page for the new data source.

## Figure 79 Configuring a new JDBC data source

[JDBC Providers](#) > [Oracle JDBC Driver](#) > [Data Sources](#) >

### New

Data Source is used by the application to access the data from the database. A data source is created under a JDBC provider which provides the specific JDBC driver implementation class. [i](#)

Configuration		
General Properties		
Scope	* cells:ovs03:nodes:ovs03	<a href="#">i</a> The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	* Oracle JDBC Driver DataSource	<a href="#">i</a> The required display name for the resource.
JNDI Name		<a href="#">i</a> The JNDI name for the resource.
Container managed persistence	<input type="checkbox"/> Use this Data Source in container managed persistence (CMP)	<a href="#">i</a> Enable if this data source will be used for container managed persistence of EJBs. This will cause a corresponding CMP connection factory which corresponds to this datasource to be created for the relational resource adapter.
Description	New JDBC Datasource	<a href="#">i</a> An optional description for the resource.
Category		<a href="#">i</a> An optional category string which can be used to classify or group the resource.
Statement Cache Size	10 statements	<a href="#">i</a> Number of free prepared statements per connection. This is different from the old datasource which is defined as number of free prepared statements per data source.
Datasource Helper Classname	com.ibm.websphere.rsadapter.Orac	<a href="#">i</a> The datasource helper that is used to perform specific database functions.
Component-managed Authentication Alias	(none)	<a href="#">i</a> References authentication data for component-managed signon to the resource.
Container-managed Authentication Alias	(none)	<a href="#">i</a> References authentication data for container-managed signon to the resource.
Mapping-Configuration Alias	(none)	<a href="#">i</a> Select a suitable JAAS login configuration from the security-JAAS configuration panel to map the user identity and credentials to a resource principal and credentials that is required to open a connection to the back-end server.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

11 Provide the following information:

Field	Value
<b>Name</b>	Enter a name for the data source. A data source is a pool of managed database connections.
<b>JNDI Name</b>	<b>jdbc/TruAccess.</b>
<b>Component-managed Authentication Alias</b>	Select the J2C Authentication Alias that you created in in the <a href="#">Creating a J2C Authentication Data Entry</a> on page 101.
<b>Container-managed Authentication Alias</b>	Select the J2C Authentication Alias created in <a href="#">Creating a J2C Authentication Data Entry</a> on page 101.

12 Click **OK**, then select the data source you just created.

13 Click the link to **Connection Pool**, at the bottom of the page.

14 Set the **Connection Timeout** field to 300 and click **OK** to return to the **Datasource** page.

15 Click the link to **Custom Properties** at the bottom of the page.

16 Set the **URL** to that for your database, using the following format:

**jdbc:oracle:thin:@<ip>:<oracle port>:<database name>**

17 If you are installing Select Identity with Oracle 9i or 10g, click **New** to add the following custom property:

Field	Value
<b>Name</b>	SetBigStringTryClob
<b>Value</b>	True
<b>Type</b>	java.lang.Boolean

18 Click **OK** to save the new custom property and return to the **Custom Properties** page.

19 Click **OK**, then click **Save** at the top of the **Custom Properties** page.

- 20 If you are installing on a cluster, check **Synchronize Changes**.
- 21 Click **Save** under **Save Master Configuration** to complete JDBC Provider Setup.
- 22 Restart the WebSphere application server or cluster. Refer to the documentation supplied with IBM WebSphere for instructions.
- 23 Click **Test Driver Configuration** to validate the driver configuration. This step is only successful if you have restarted the server or cluster.

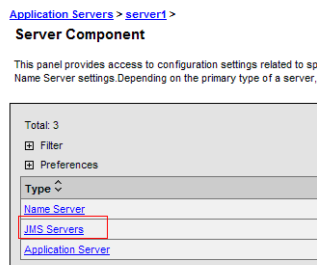
This step verifies that WebSphere can connect to the database. If the connection is successful, the **Configure a JDBC Connection Pool** page opens with a message in the top left corner to indicate that connection was successful.

## Configuring Server Components

- 1 On a standalone server, in the left panel of the console, navigate to **Application Servers**.  
On a cluster, use the left panel to navigate to **Servers** → **JMS Servers**.
- 2 *On a standalone server*, click the link to the application server on which you are installing Select Identity.

*On a cluster*, choose one of the nodes to function as the Select Identity JMS server. Both the Queue Connection Factory and the Topic Connection Factory should point to this node. Refer to [Configuring a JMS Queue Factory](#) on page 113 and [Configuring a JMS Topic Factory](#) on page 115.

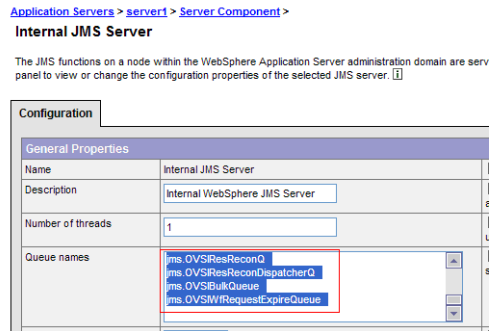
**Figure 80 The Application Servers page**



- 3 On a standalone server, click the link to **Server Components** under **Additional Properties**.

#### 4 Select Internal JMS Servers.

**Figure 81 Internal JMS Servers page**



#### 5 Input the following list of JMS queues:

.jms.OVSIAuditProcQ

.jms.OVSIChangeReconProcessorQueue

.jms.OVSIMessageAckQueue

.jms.OVSIReconQueue

.jms.OVSIISaudQ

.jms.OVSIServiceAssignQueue

.jms.OVSIWorkflowQueue

.jms.OVSI SchedulerQueue

.jms.OVSIEntCacheQueue

.jms.OVSIResReconQ

.jms.OVSIResReconDispatcherQ

.jms.OVSIBulkQueue

.jms.OVSIWfRequestExpireQueue

## Configuring the Generic JVM Arguments

If you are installing on a WebSphere cluster, perform this procedure on every server.






- 1 Select the first server in the cluster, or on a standalone configuration, the server on which you are installing Select Identity.
- 2 Click the link to **Process Definition**.

**Figure 82 The Process Definition page for the application server**

[Application Servers](#) > [clusterServer1](#) >

### Process Definition

A process definition defines the command line information necessary to start/initialize a process. 

Configuration		
General Properties		
Executable name	<input type="text" value="\$JAVA_HOME/bin/java"/>	 Specifies the executable name of the process.
Executable arguments	<input type="text"/>	 Specifies executable commands that run when the process starts.
Working directory	<input type="text" value="\$USER_INSTALL_ROOT"/>	 Specifies the file system directory in which the process will run.
Executable target type	<input type="text" value="JAVA_CLASS"/>	 Specifies whether a Java classname or the name of an executable Jar will be used as the executable target of this Java process.
Executable target	<input type="text" value="com.ibm.ws.runtime.WeServer"/>	 The name of the executable target (a Java class (containing a main() method, or the name of an executable jar), depending on the executable target type.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		
















- 3 Click the link to **Java Virtual Machine**, under **Additional Properties**.

## Figure 83 Java Virtual Machine Configuration

[Application Servers](#) > [clusterServer1](#) > [Process Definition](#) >

### Java Virtual Machine

Advanced Java virtual machine settings. 

Configuration		
General Properties		
Classpath	<input type="text"/>	 Specifies the standard class path in which the Java virtual machine looks for classes.
Boot Classpath	<input type="text"/>	 Specifies bootstrap classes and resources for a JVM. This option is only available for JVMs that support bootstrap classes and resources. You might separate multiple paths by a colon (:) or semi-colon (;), depending on operating system of the node.
Verbose class loading	<input type="checkbox"/>	 Specifies whether to use verbose debug output for class loading. The default is not to enable verbose class loading.
Verbose garbage collection	<input type="checkbox"/>	 Specifies whether to use verbose debug output for garbage collection. The default is not to enable verbose garbage collection.
Verbose JNI	<input type="checkbox"/>	 Specifies whether to use verbose debug output for native method invocation. The default is not to enable verbose JNI.
Initial Heap Size	<input type="text" value="256"/>	 Specifies the initial heap size available to the JVM (in megabytes).
Maximum Heap Size	<input type="text" value="1024"/>	 Specifies the maximum heap size available to the JVM, in megabytes. The default is 256.
Run HProf	<input type="checkbox"/>	 Specifies whether to use HProf profiler support. To use another profiler, specify the custom profiler's settings using the HProf Arguments setting. The default is not to enable HProf profiler support.
HProf Arguments	<input type="text"/>	 Specifies command-line profiler arguments to pass to the Java virtual machine that starts the application server process. You can specify arguments when HProf profiler support is enabled.
Debug Mode	<input type="checkbox"/>	 Specifies whether to use the JVM debug output. The default is not to enable debug mode support.
Debug arguments	<input type="text" value="-Djava.compiler=NONE -Xdebug -Xinc"/>	 Specifies command-line debug arguments to pass to the Java virtual machine that starts the application server process. You can specify arguments when Debug Mode is enabled.
Generic JVM arguments	<input type="text" value="-Dcom.truologica.truaccess.property."/>	 Additional command line arguments for the JVM.
Executable JAR file name	<input type="text"/>	 Specifies a full path name for an executable jar file that the Java virtual machine uses.
Disable JIT	<input type="checkbox"/>	 Configure the JVM such that the Just-In-Time (JIT) compiler is disabled.
Operating system name	<input type="text"/>	 Specifies JVM settings for a given operating system. When started, the process will use the JVM settings for the operating system of the node.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		
Additional Properties		
<a href="#">Custom Properties</a>	Java system properties to be set in the memory for this JVM.	

- Under **Generic JVM Arguments**, enter the location of the `TruAccess.properties` file, such as:

```
-Dcom.truologica.truaccess.property.file=<SI_Install_directory>\\properties\\TruAccess.properties
```

If installing in a Unix environment, add the following to the line above:

```
-Djava.awt.headless=true
```

- Set the **Initial Heap Size** to 256.
- Set the **Maximum Heap Size** to 1024.
- Click **Apply**.

- 8 Click **Save** in the page banner.
- 9 Check the **Synchronize changes** box (In Cluster) click **Save**.

## Configuring a JMS Queue Factory

Create a JMS Queue Factory at the node level. For cluster configurations, create the Queue Factory for each node in the cluster.

- 1 In the left panel of the console, navigate to **Resources** → **WebSphere JMS Provider**

**Figure 84 The WebSphere JMS Providers page**

### WebSphere JMS Provider

A JMS provider enables asynchronous messaging based on the Java Messaging Service (JMS). It provides J2EE connection factories to create connections for specific JMS queue or topic destinations. WebSphere JMS provider administrative objects are used to manage JMS resources for the internal WebSphere JMS provider. [1]

**Configuration**

[-] Scope: Cell=ovs02Network

<b>Cell</b>	ovs02Network		To specify cell scope, clear the node and server fields and click Apply.
<b>Node</b>	<input type="text"/>	<input type="button" value="Browse Nodes"/>	To select a node scope, type in or browse for a node, then clear the server field and click Apply.
<b>Server</b>	<input type="text"/>	<input type="button" value="Browse Servers"/>	To select a server scope, select a node scope first, then type in or browse for a server, and click Apply.
When new items are created in this view, they will be created within the current scope.			
<input type="button" value="Apply"/>			

**General Properties**

Scope	cells:ovs02Network	[1] The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	WebSphere JMS Provider	[1] The name of the resource provider.
Description	Built-in WebSphere JMS Provider	[1] A text description for the resource provider.

**Additional Properties**

<a href="#">WebSphere Queue Connection Factories</a>	
<a href="#">WebSphere Topic Connection Factories</a>	
<a href="#">WebSphere Queue Destinations</a>	
<a href="#">WebSphere Topic Destinations</a>	

- 2 Click the link to **WebSphere Queue Connection Factories**.

**Figure 85 The WebSphere Queue Connection Factories page**

[WebSphere JMS Provider >](#)

**WebSphere Queue Connection Factories**

A queue connection factory is used to create connections to the associated JMS provider of JMS queue destinations, for point-to-point messaging. Use WebSphere Queue Connection Factory administrative objects to manage queue connection factories for the internal WebSphere JMS provider. [?](#)

- 3 Click **New** to proceed to the **Configuration** page for a new Queue Connection Factory.
- 4 Input the **Queue Name** and **JNDI Name**, as follows:

Field	Value
<b>Queue Name</b>	jms.OVSIQCF
<b>JNDI Name</b>	.jms/OVSIQCF
<b>Node</b>	<ul style="list-style-type: none"> <li>• <b>Standalone:</b> Select the node name of the WebSphere application server , or:</li> <li>• <b>Clusters:</b> Select the node you have designated as the JMS server. Refer to <a href="#">Configuring Server Components</a> on page 109</li> </ul>



All the queue factories on each node in a cluster must point to the same JMS server.

- 5 Click **Apply**.
- 6 On the Connection Factories page, click the name of the **Connection Factory** you just created.
- 7 Click the link to **Connection Pools** at the bottom of the page.
- 8 Set the **Max Connections** field to 100.



- 9 Leave all other defaults unchanged.
- 10 Click **Apply**.
- 11 Click **Save** in the page banner.

## Configuring a JMS Topic Factory

Create a JMS Topic Factory at the node level.

- 1 In the left panel of the console, navigate to **Resources** → **WebSphere JMS Provider**.
- 2 Click the link to **WebSphere Topic Connection Factories**.

### Figure 86 The WebSphere Topic Connection Factories page

[WebSphere JMS Provider](#) >

#### WebSphere Topic Connection Factories

A topic connection factory is used to create connections to the associated JMS provider of JMS topic destinations, for publish/subscribe messaging. Use WebSphere Topic Connection Factory administrative objects to manage topic connection factories for the internal WebSphere JMS provider. [1]


Total: 0				
Filter				
Preferences				
New		Delete		
<input type="checkbox"/>	Name	JNDI Name	Description	Category
None				














- 3 Click **New** to open the **Configuration** page for a new topic connection factory.

## Figure 87 The Configuration page for a new JMS topic connection factory

[WebSphere JMS Provider](#) > [WebSphere Topic Connection Factories](#) >

### New

A topic connection factory is used to create connections to the associated JMS provider of JMS topic destinations, for publish/subscribe messaging. Use WebSphere Topic Connection Factory administrative objects to manage topic connection factories for the internal WebSphere JMS provider. 

Configuration		
General Properties		
Scope	<input type="text" value="cells:ovsi02Network"/>	 The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	<input type="text"/>	 The required displayname for the resource.
JNDI Name	<input type="text"/>	 The JNDI name for the resource.
Description	<input type="text"/>	 An optional description for the resource.
Category	<input type="text"/>	 An optional category string which can be used to classify or group the resource.
Node	<input type="text" value="ovsi02Manager"/>	 The WebSphere node name of the administrative node where the JMS server runs for this connection factory. Connections created by this factory connect to that JMS server.
Port	<input type="text" value="DIRECT"/>	 For Topics, we need to specify which of the two ports is to be used in addition to the node (JMS Server). The QUEUED port is for full-function JMS Pub/Sub support; the DIRECT port is for non-persistent, non-transactional, non-durable subscriptions only.
Component-managed Authentication Alias	<input type="text" value="(none)"/>	 References authentication data for component-managed signon to the resource.
Container-managed Authentication Alias	<input type="text" value="(none)"/>	 References authentication data for container-managed signon to the resource.
Mapping-Configuration Alias	<input type="text" value="(none)"/>	 Select a suitable JAAS login configuration from the security-JAAS configuration panel to map the user identity and credentials to a resource principal and credentials that is required to open a connection to the back-end server.
Clone Support	<input type="checkbox"/> Enable clone support	 Enables clone support. When true, the clientID field is required.
Client ID	<input type="text"/>	 JMS client ID Note: Necessary for durable server side subscriptions.
XA Enabled	<input checked="" type="checkbox"/> Enable XA	 Attribute to indicate whether or not the JMS provider is XA enabled or not. This attribute only applies to specialized models of JMSConnectionFactory. It is meaningless for GenericJMSConnectionFactory, as they define such feature enablements through name/value property pairs.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

### 4 Input the following:

Field	Value
Topic Name	jms.OVSITCF

Field	Value
JNDI Name	jms/OVSITCF
Node	<ul style="list-style-type: none"> <li>• <b>Standalone:</b> Select the node name of the WebSphere application server , or:</li> <li>• <b>Clusters:</b> Select the node you have designated as the JMS server in <a href="#">Configuring Server Components</a> on page 109</li> </ul>
Port	Select <b>Queued</b> .

- 5 Click **Apply**.
- 6 On the Connection Factories page, click the name of the **Connection Factory** you just created.
- 7 Click the link to **Connection Pools** at the bottom of the page.
- 8 Set the **Max Connections** field to 100.
- 9 Leave all other defaults unchanged.
- 10 Click **Apply**.
- 11 Click **Save** in the page banner.

## Creating the JMS Queues

Create JMS queues at the node level for standalone installations and at the cell level for clustered configurations. Follow the procedure below for every JMS Queue listed.

- 1 In the left panel of the console, navigate to **Resources** → **WebSphere JMS Provider**.
- 2 Click the link to **WebSphere Queue Destinations** at the bottom of the page.

**Figure 88 JMS Queue Destinations**

[WebSphere JMS Provider](#) >

**WebSphere Queue Destinations**

Queue destinations provided for point-to-point messaging by the internal WebSphere JMS provider. Use WebSphere Queue Destination administrative objects to manage queue destinations for the internal WebSphere JMS provider. [1]

Totat 13

Filter

Preferences

New Delete

<input type="checkbox"/>	Name ↕	JNDI Name ↕	Description ↕	Category ↕
<input type="checkbox"/>	<a href="#">jms.OVSIAuditProcQ</a>	jms/OVSIAuditProcQ		
<input type="checkbox"/>	<a href="#">jms.OVSIBulkQueue</a>	jms/OVSIBulkQueue		
<input type="checkbox"/>	<a href="#">jms.OVSIChangeReconProcessorQueue</a>	jms/OVSIChangeReconProcessorQueue		
<input type="checkbox"/>	<a href="#">jms.OVSIEntCacheQueue</a>	jms/OVSIEntCacheQueue		
<input type="checkbox"/>	<a href="#">jms.OVSIMessageAckQueue</a>	jms/OVSIMessageAckQueue		
<input type="checkbox"/>	<a href="#">jms.OVSIReconQueue</a>	jms/OVSIReconQueue		
<input type="checkbox"/>	<a href="#">jms.OVSIResReconDispatcherQ</a>	jms/OVSIResReconDispatcherQ		
<input type="checkbox"/>	<a href="#">jms.OVSIResReconQ</a>	jms/OVSIResReconQ		
<input type="checkbox"/>	<a href="#">jms.OVSIStdQ</a>	jms/OVSIStdQ		
<input type="checkbox"/>	<a href="#">jms.OVSI SchedulerQueue</a>	jms/OVSI SchedulerQueue		
<input type="checkbox"/>	<a href="#">jms.OVSI ServiceAssignQueue</a>	jms/OVSI ServiceAssignQueue		
<input type="checkbox"/>	<a href="#">jms.OVSI WfRequestExpireQueue</a>	jms/OVSI WfRequestExpireQueue		
<input type="checkbox"/>	<a href="#">jms.OVSI WorkflowQueue</a>	jms/OVSI WorkflowQueue		














- 3 Click **New** to open the **Configuration** page for a new queue destination.

## Figure 89 New JMS Queue Destination Page

[WebSphere JMS Provider](#) > [WebSphere Queue Destinations](#) >

New

Queue destinations provided for point-to-point messaging by the internal WebSphere JMS provider. Use WebSphere Queue Destination administrative objects to manage queue destinations for the internal WebSphere JMS provider. NOTE: The queue name must also be added to the list of queue names in the configuration of the JMS server(s) where the queue is to be hosted. 

Configuration		
General Properties		
Scope	* cells:ovs104:nodes:ovs104	 The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	* <input type="text"/>	 The required display name for the resource.
JNDI Name	* <input type="text"/>	 The JNDI name for the resource.
Description	<input type="text"/>	 An optional description for the resource.
Category	<input type="text"/>	 An optional category string which can be used to classify or group the resource.
Persistence	APPLICATION DEFINED 	 Whether all messages sent to the destination are persistent, non-persistent, or have their persistence defined by the application.
Priority	APPLICATION DEFINED 	 Whether the message priority for this destination is defined by the application or the Specified priority property.
Specified Priority	0 <input type="text"/>	 If the Priority property is SPECIFIED, type here the message priority for this queue, in the range 0 through 9 with 0 as the lowest priority and 9 as the highest priority.
Expiry	APPLICATION DEFINED 	 Whether the expiry timeout for this queue is defined by the application or the Specified expiry property, or messages on the queue never expire (have an unlimited expiry timeout).
Specified Expiry	0 <input type="text"/> milliseconds	 If the Expiry timeout property is SPECIFIED, type here the number of milliseconds after which messages on this queue expire. Valid values are any long value greater than zero.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

#### 4 Name each queue exactly as listed in the following table:

Queue Name	JNDI Name
<b>jms.OVSIAuditProcQ</b>	jms/OVSIAuditProcQ
<b>jms.OVSIBulkQueue</b>	jms/OVSIBulkQueue
<b>jms.OVSIChangeReconProcessor Queue</b>	jms/OVSIChangeReconProcessorQueue
<b>jms.OVSIEntCacheQueue</b>	jms/OVSIEntCacheQueue
<b>jms.OVSIMessageAckQueue</b>	jms/OVSIMessageAckQueue
<b>jms.OVSIReconQueue</b>	jms/OVSIReconQueue
<b>jms.OVSIResReconDispatcherQ</b>	jms/OVSIResReconDispatcherQ

Queue Name	JNDI Name
jms.OVSIResReconQ	jms/OVSIResReconQ
jms.OVSI SaudQ	jms/OVSI SaudQ
jms.OVSI SchedulerQueue	jms/OVSI SchedulerQueue
jms.OVSI ServiceAssignQueue	jms/OVSI ServiceAssignQueue
jms.OVSI WfRequestExpireQueue	jms/OVSI WfRequestExpireQueue
jms.OVSI WorkflowQueue	jms/OVSI WorkflowQueue

- 5 After you input each Queue Name and JNDI Name, click **Apply**.
- 6 Click **Save** in the page banner.

## Creating JMS Topics

Create JMS topics at the node level for standalone installations and at the cell level for clustered configurations. Follow the procedure below for every JMS topic listed.

- 1 In the left panel of the console, navigate to **Resources** → **WebSphere JMS Provider**.
- 2 Click the link to **WebSphere Topic Destinations** at the bottom of the page.

**Figure 90 JMS Topic Destinations page**

[WebSphere JMS Provider](#) >  
**WebSphere Topic Destinations**

Topic destinations provided for publish/subscribe messaging by the internal WebSphere JMS provider. Use WebSphere Topic Destination administrative objects to manage topic destinations for the internal WebSphere JMS provider. [?](#)

Total: 2  
 Filter  
 Preferences


<input type="checkbox"/> Name	JNDI Name	Description	Category
<input type="checkbox"/> <a href="#">jms.OVSI AuditBroadcast</a>	jms/OVSI AuditBroadcast		
<input type="checkbox"/> <a href="#">jms.OVSI CacheTopic</a>	jms/OVSI CacheTopic		












- 3 Click **New** to open the **Configuration** page for a new topic.

**Figure 91 New JMS Topic Configuration page**

[WebSphere JMS Provider](#) > [WebSphere Topic Destinations](#) >

New

Topic destinations provided for publish/subscribe messaging by the internal WebSphere JMS provider. Use WebSphere Topic Destination administrative objects to manage topic destinations for the internal WebSphere JMS provider. 

Configuration		
General Properties		
Scope	* cells:ovs104:nodes:ovs104	 The scope of the configured resource. This value indicates the configuration location for the configuration file.
Name	*	 The required display name for the resource.
JNDI Name	*	 The JNDI name for the resource.
Description		 An optional description for the resource.
Category		 An optional category string which can be used to classify or group the resource.
Topic	*	 This is the string value used to identify the Topic. It can be dot notation and include wildcard characters.
Persistence	APPLICATION DEFINED	 Whether all messages sent to the destination are persistent, non-persistent, or have their persistence defined by the application.
Priority	APPLICATION DEFINED	 Whether the message priority for this destination is defined by the application or the Specified priority property.
Specified Priority	0	 When priority is SPECIFIED, this value specifies the priority for the topic. Valid values are in the range 0-9 with 0 as the lowest priority and 9 as the highest priority.
Expiry	APPLICATION DEFINED	 Whether the expiry timeout for this queue is defined by the application or the Specified expiry property, or messages on the queue never expires (have an unlimited expiry timeout).
Specified Expiry	0 milliseconds	 When expiry is SPECIFIED, this value contains the expiration period for the Topic in milliseconds. Valid values are any long value greater than zero.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

4 Input the **Topic Name** and **JNDI Name** exactly as shown in the table below.

Name	JNDI Name	Topic
<b>jms.OVSIAuditBroadcast</b>	jms/ OVSIAuditBroadcast	jms/ OVSIAuditBroadcast
<b>jms.OVSI_CACHE_TOPIC</b>	jms/OVSI_CACHE_TOPIC	jms/OVSI_CACHE_TOPIC

- 5 Click **Apply**.
- 6 Click **Save** in the page banner.

## Configuring the Application Server

Configure the application server as documented in the following procedure. On a cluster, perform these steps for every node:

- 1 In the left panel of the console, navigate to **Application Server**.
- 2 Click the name of the application server on which you are installing Select Identity.

**Figure 92 The Application Server Configuration page**

[Application Servers](#) >  
**clusterServer1**

An application server is a server which provides services required to run enterprise applications. ⓘ

**Runtime** | **Configuration**

General Properties		
Name	clusterServer1	ⓘ The display name for the server.
Application classloader policy	Multiple ▾	ⓘ Specifies whether there is a single classloader for all applications ("Single") or a classloader per application ("Multiple").
Application class loading mode	Parent last ▾	ⓘ Specifies the class loading mode when the application classloader policy is "Single"

Apply | OK | Reset | Cancel

- 3 Set the **Application Classloader Policy** to **Multiple**.
- 4 Set the **Application Class Loading Mode** to **Parent Last**.
- 5 Click **Apply**.
- 6 Click **Save** in the page banner.

## Configuring the Message Listener Service

Configure the Message Listener service by completing the following steps. If you are installing on a cluster, perform this procedure for every node.

- 1 In the left panel of the console, navigate to **Application Servers**.
- 2 Click the link to the **Message Listener Service**, at the bottom of the page.
- 3 Click the link to **Listener Ports** under **Additional Properties**.
- 4 Click **New**.



## Figure 93 Message Listener Port Configuration Page

Application Servers > clusterServer1 > Message Listener Service >

### Listener Ports

Listener ports for Message Driven Beans to listen upon for messages. Each port specifies the JMS Connection Factory and JMS Destination that an MDB, deployed against that port, will listen upon. [1]

Total: 15					
Filter					
Preferences					
New Delete Start Stop					
<input type="checkbox"/>	Name	Description	Connection factory JNDI name	Destination JNDI name	Status
<input type="checkbox"/>	<a href="#">jms.OVSIAuditBroadcast</a>		jms/OVSITCF	jms/OVSIAuditBroadcast	➔
<input type="checkbox"/>	<a href="#">jms.OVSIAuditProcQ</a>		jms/OVSIQCF	jms/OVSIAuditProcQ	➔
<input type="checkbox"/>	<a href="#">jms.OVSIBulkQueue</a>		jms/OVSIQCF	jms/OVSIBulkQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSIChangeReconProcessorQueue</a>		jms/OVSITCF	jms/OVSIChangeReconProcessorQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSIEntCacheQueue</a>		jms/OVSIQCF	jms/OVSIEntCacheQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSIMessageAckQueue</a>		jms/OVSIQCF	jms/OVSIMessageAckQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSIReconQueue</a>		jms/OVSIQCF	jms/OVSIReconQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSIResReconDispatcherQ</a>		jms/OVSIQCF	jms/OVSIResReconDispatcherQ	➔
<input type="checkbox"/>	<a href="#">jms.OVSIResReconQ</a>		jms/OVSIQCF	jms/OVSIResReconQ	➔
<input type="checkbox"/>	<a href="#">jms.OVSISeaudQ</a>		jms/OVSIQCF	jms/OVSISeaudQ	➔
<input type="checkbox"/>	<a href="#">jms.OVSI SchedulerQueue</a>		jms/OVSIQCF	jms/OVSI SchedulerQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSI ServiceAssignQueue</a>		jms/OVSIQCF	jms/OVSI ServiceAssignQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSI WfRequestExpireQueue</a>		jms/OVSIQCF	jms/OVSI WfRequestExpireQueue	➔
<input type="checkbox"/>	<a href="#">jms.OVSI WorkflowQueue</a>		jms/OVSIQCF	jms/OVSI WorkflowQueue	➔

### 5 Create listener ports for the following queues:

Name	Destination JNDI Name	Connection Factory JNDI Name
jms/OVSIAuditBroadcast	jms/OVSITCF	jms/OVSIAuditBroadcast
jms/OVSIChangeReconProcessorQueue	jms/OVSITCF	jms/OVSIChangeReconProcessorQueue
jms/OVSIAuditProcQ	jms/OVSIQCF	jms/OVSIAuditProcQ
jms/OVSIBulkQueue	jms/OVSIQCF	jms/OVSIBulkQueue
jms/OVSIEntCacheQueue	jms/OVSIQCF	jms/OVSIEntCacheQueue
jms/OVSIMessageAckQueue	jms/OVSIQCF	jms/OVSIMessageAckQueue
jms/OVSIReconQueue	jms/OVSIQCF	jms/OVSIReconQueue

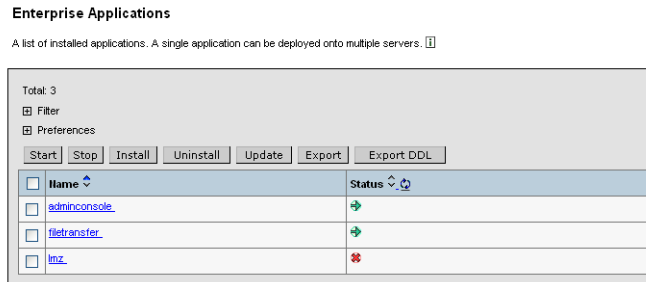
Name	Destination JNDI Name	Connection Factory JNDI Name
jms/OVSIResReconDispatcherQ	jms/OVSIQCF	jms/OVSIResReconDispatcherQ
jms/OVSIResReconQ	jms/OVSIQCF	jms/OVSIResReconQ
jms/OVSIStdQ	jms/OVSIQCF	jms/OVSIStdQ
jms/OVSIStdSchedulerQueue	jms/OVSIQCF	jms/OVSIStdSchedulerQueue
jms/OVSIStdServiceAssignQueue	jms/OVSIQCF	jms/OVSIStdServiceAssignQueue
jms/OVSIStdRequestExpireQueue	jms/OVSIQCF	jms/OVSIStdRequestExpireQueue
jms/OVSIStdWorkflowQueue	jms/OVSIQCF	jms/OVSIStdWorkflowQueue

## Deploying Select Identity

Perform the following steps to deploy Select Identity:

- 1 In the left panel of the console, navigate to **Applications** → **Enterprise Applications**.

**Figure 94 Enterprise Application list**



- 2 Click **Install** above the list of applications.

**Figure 95 Installing a new Enterprise Application**

**Preparing for the application installation**

Specify the EAR/WAR/JAR module to upload and install.

Path:	Browse the local machine or a remote server:	<input type="checkbox"/> Local path: <input type="text"/> <input type="button" value="Browse..."/>	<input type="checkbox"/> Server path: <input type="text"/> <input type="button" value="Browse..."/>	<small>Choose the local path if the ear resides on the same machine as the browser. Choose the server path if the ear resides on any of the nodes in your cell context.</small>
Context Root:	Used only for standalone Web modules (*.war)	<input type="text"/>		<small>You must specify a context root if the module being installed is a WAR module.</small>
<input type="button" value="Next"/> <input type="button" value="Cancel"/>				

- 3 Click **Browse** to locate the `websphere_lmz.ear` file in the file system.
- 4 Click **Next** through each step, accepting the default values except for the **Map modules to application servers** step. For this step, make sure that the correct cluster or server is specified for all modules listed.
- 5 Review the options on the **Summary** page and click **Finish** and then **Save** to install.
- 6 Return to the **Enterprise Applications** page, then click the installed LMZ application.
- 7 Set the **Classloader Mode** to **Parent Last** and set the **WAR Classloader Policy** to **Application**.



Do not pre-compile the JSPs during deployment. This is done in the following step.

- 8 Compile the JSPs (on each server if you are installing on a cluster).
- 9 The file `connector.jar` must be located in the WebSphere classpath. Make sure that this file is copied to the `$WAS_HOME/lib/ext` directory.
- 10 Run the following from the command line:
  - In Unix/Linux:

```
cd $WAS_HOME/bin

JspBatchCompiler.sh -enterpriseapp.name lmz -verbose false
-keepgenerated true -server.name <servername>cd $WAS_HOME/
bin
```
  - In Windows:

```
cd <WAS_HOME>\bin
```

```
JspBatchCompiler.bat -enterpriseapp.name lmz -verbose  
false -keepgenerated true -server.name <servername>
```

Make sure that compilation completes without any errors.

- 11 Install any connectors at the node level.
- 12 On a cluster, configure Virtual hosts from the Network Deployment Manager Console by navigating to **Environment** → **Virtual Hosts**.

Refer to the WebSphere Network Deployment Edition manual for information about virtual host configuration.

- 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.
  - Check the mapping from Web modules to virtual hosts by navigating to **Enterprise Applications** → **Select Identity Application** → **Map Virtual Hosts to Web Modules**. If the virtual host there is `default_host`, you must configure `default_host` in **Environment** → **Virtual Hosts**.
- 13 Update the Web Server Plugin from the Network Deployment Manager Console by selecting **Environment** → **Update Web Server Plugin**.
  - 14 Log out of the WebSphere Administrative Console.
  - 15 Stop and restart the Websphere Application Server; if you are installing on a cluster, you must restart the cluster. Refer to the documentation supplied with IBM WebSphere for instructions.

## Configuring Logging for Select Identity

Configure WebSphere logging for Select Identity, if desired, by performing the following steps. On a cluster, perform these steps on every node:

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

**Figure 96 The Logging and Tracing page**

**Logging and Tracing**  
 Configure logs and specify trace settings. ⓘ

Total: 7  
 Filter  
 Preferences

Server	Node	Type	Status
<a href="#">dmgr</a>	ovs02Manager	servers	➔
<a href="#">msserver</a>	ovs02	servers	➔
<a href="#">msserver</a>	ovs01	servers	➔
<a href="#">nodeagent</a>	ovs02	servers	➔
<a href="#">nodeagent</a>	ovs01	servers	➔
<a href="#">server1</a>	ovs01	servers	➔
<a href="#">server2</a>	ovs02	servers	➔

2 Click the link to the application server.

**Figure 97 Logging settings**

**Logging and Tracing**  
 Configure logs and specify trace settings.

Logging and Tracing	
<a href="#">Diagnostic Trace</a>	View and modify the properties of the diagnostic trace service.
<a href="#">JVM Logs</a>	View and modify the settings for the Java Virtual Machine (JVM) System.out and System.err logs.
<a href="#">Process Logs</a>	View or modify settings for specifying the files to which standard out and standard error streams write.
<a href="#">IBM Service Logs</a>	Configure the IBM service log, also known as the activity log.

- 3 Click **JVM Logs**.
- 4 Change the content of the **file name** field to reflect the location of the Select Identity log file.

There are additional configuration steps for Websphere installations. See [Configuring HP OpenView Select Identity](#) on page 129 to finish configuring Select Identity.

## Logging In to Select Identity on IBM WebSphere

To log in to Select Identity on WebSphere, you 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.

---

# 6 Configuring HP OpenView Select Identity

This chapter provides important information for both required and recommended configuration of Select Identity after it has been installed. Topics covered in this section are as follows:

- [Configuring TruAccess.properties Required Settings](#)
- [Recommended Configuration](#)
- [Default Properties](#)
- [Custom User Interface Properties](#)
- [Generating a Custom Keystore](#)
- [Internationalization and Localization](#)



If you are installing in a clustered environment, these configuration steps must be performed on all nodes in the cluster.

## Configuring TruAccess.properties Required Settings

Several configuration settings are made by modifying the content of the `TruAccess.properties` file. 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.

### Setting the Database Repository Property

An important step in configuring the database takes place after you configure the web application server and install Select Identity.

*Before starting Select Identity for the first time, set the following properties in the `TruAccess.properties` file so that the database initializes correctly, if you have not done so already:*

```
truaccess.repository.type=<your_database>
truaccess.repository.oracle.driver.bea=no
```

## Additional Required Settings

The following `TruAccess.properties` settings are required:

```
truaccess.sender.email
```

Specify a general email address that will be used as the sender's address for email sent by Select Identity. For example:

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

This address must exist on the SMTP server configured for use by the Select Identity application server.

You can also specify a value for `truaccess.sender.name` to coincide with this setting, such as:

```
truaccess.sender.name=si_admin
com.hp.si.user.attributes.maxlength=10
```

Attribute Max Length default value (kilobyte).

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

Provide values 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.repository.type=oracle
```

This setting defines the type of database server you are using. Possible values are `mssql` for Microsoft SQL Server, or `oracle` for Oracle. Values are in lowercase. Oracle is the default setting; you must change this if you are running Select Identity with a Microsoft SQL 2000 server.

```
truaccess.repository.oracle.driver.bea
```



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.

```
truaccess.upload.fileidir
```

Specify a valid location on the Select Identity server that can be used as temporary storage while Select Identity uploads files to the database.

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

Specify the **SI Provisioning Password Change** workflow template for password reset.

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

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

You can configure other settings in the `TruAccess.properties` file to do the following:

- Customize the graphical interface - see [Custom User Interface Properties](#) on page 135.
- Optimize Select Identity - see [Recommended Configuration](#) on page 135.
- Use any custom generated keystore in the `TruAccess.properties` file. See [Generating a Custom Keystore](#) on page 131 for details.

For a complete listing and description of all settings in the `TruAccess.properties` file, see [Configuring TruAccess.properties](#) on page 169.

## Generating a Custom Keystore

If you wish to enable the Select Identity server to encrypt and decrypt data it stores in the database using your keystore rather than the default provided by Select Identity or a keystore provided by a HSM device, you must generate the keystore and integrate it into Select Identity. A keystore is a database of keys. The private keys are associated with a certificate chain, which authenticates

the corresponding public key. The keystore also contains certificates from trusted entities. By generating the keystore, you add another layer of security to the data that is exchanged in the Select Identity system.



You must perform this procedure before using Select Identity. You cannot use your keystore to decrypt data after Select Identity stores (and encrypts) data in the database using the default keystore.

Follow the procedures in the following sections to generate and use a keystore in Select Identity:

- [Creating the Custom Keystore](#)
- [Integrating the Keystore with Select Identity](#)

## Creating the Custom Keystore

Complete the following steps to generate a keystore:

- 1 Copy the contents of the `SI40\keystore\` directory on the Select Identity CD to a keystore directory on the Select Identity server. The files include the following:
  - `ks_gen.sh` and `ks_gen.bat` — Script that generates a keystore containing the secret key to encrypt and decrypt data.
  - `SIPubKey` — Binary file that contains the public key to encrypt the password of the keystore and alias.
  - `SIKeyStoreUtil.jar` — Executables of the Keystore utility.
  - `bcprov-jdk14-130.jar` — Executables of the Bouncy Castle Java Cryptography RSA implementation.
  - `sunjce_provider.jar` — Executables of the Sun Java Cryptography implementation.
  - `commons_logging.jar` — Executables for Jakarta Commons Logging.
  - `utils_log.jar` — Utility executables for Select Identity.
- 2 Ensure that the JRE on the Application server used by OVSI is included in the `PATH` environment variable.
- 3 Run the `ks_gen.bat` (on Windows) or `ks_gen.sh` (on UNIX) script and follow the instructions, using the distributed public key file during the process.

- 4 Save the secret string you use in case Support needs to analyze encrypted data for data recovery.

The resulting keystore properties file should look similar to this:

```
#Select Identity Keystore Parameters
#Fri. Aug 20 10:02:42 CDT 2005
si.keystore.alias=test_alias
si.keystore.storepass=<encoded string>
si.keystore.keypass=<encoded string>
si.keystore.filepath=c:/temp/SI/test.keystore
```

- 5 If you are configuring Select Identity for use with HSM, edit the keystore properties file and change `si.keystore.filepath` to point to the keystore you have generated outside of Select Identity.

## Integrating the Keystore with Select Identity

You must configure the Select Identity server to use the keystore. Complete the following steps:

- 1 Shutdown the Select Identity server. Enter the following at the command line:

For Linux: `./stopWebLogic.sh`

For Windows: `stopWebLogic.cmd`

- 2 Edit the keystore properties file and change the location where the keystore is saved (specified by the `si.keystore.filepath` parameter).
- 3 Add the following line in the `TruAccess.properties` file:

**si.keystore.paramfile=<location\_of\_keystore\_properties\_file>**

- 4 If configuring for use with a Hardware Security Module (HSM), perform the following steps:
  - a Configure the client portion of your HSM provider on each node of your weblogic server that is running Select Identity. Refer to the instructions provided by your HSM provider.
  - b Add any additional jar files to the Select Identity classpath that may be required for Select Identity to use the HSM provider.

Example additional class path entry for NCipher HSM:

```
/opt/nfast/java/classes/jutils.jar:/opt/nfast/java/  
classes/keysafe.jar:/opt/nfast/java/classes/  
kmcsp.jar:/opt/nfast/java/classes/kmjava.jar:/opt/  
nfast/java/classes/nfjava.jar:/opt/nfast/java/  
classes/rsaprivenc.jar
```

- c Add the appropriate properties to the `TruAccess.properties` file:

If configuring for an Eracom HSM:

The cipher algorithm used to encrypt and decrypt two-way passwords in Select Identity:

```
com.hp.ovsi.encryptdecrypt.algorithm=DESede/ECB/  
PKCS5Padding
```

**EncryptionKey Provider Details if the provider is external (Hardware Security Module):**

```
com.hp.ovsi.encryptionkey.provider.classname  
=au.com.eracom.crypto.provider.ERACOMProvider  
com.hp.ovsi.encryptionkey.provider.position=2  
com.hp.ovsi.encryptionkey.keystoretype=CRYPTOKI
```

If configuring for a NCipher HSM:

The cipher algorithm used to encrypt and decrypt two-way passwords in Select Identity is as follows:

```
com.hp.ovsi.encryptdecrypt.algorithm=AES/ECB/  
PKCS5Padding
```

**EncryptionKey Provider Details if the provider is external (Hardware Security Module):**

```
com.hp.ovsi.encryptionkey.provider.classname=com.ncip  
her.provider.km.nCipherKM  
com.hp.ovsi.encryptionkey.provider.position=2  
com.hp.ovsi.encryptionkey.keystoretype=nCipher.world
```

- 5 Restart the WebLogic Server.

# Recommended Configuration

Before you start using Select Identity, it is strongly recommended that you customize it for the best performance. You may also want to customize the graphical interface to reflect your company information, as well as change some of the interface default settings. The following sections describe how to optimize and customize Select Identity.

- [Recommended Configuration](#)
- [Custom User Interface Properties](#)
- 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.

For WebLogic, add `Xmx1024m` as a java option in the `myStartWL` script for a single server installation. On a cluster, add this to the **Arguments** field of the **Remote Start** settings for each server in the cluster.

- Set logging level to `WARNING`.

In the JRE `logging.properties` file, add the following line:

```
.level=WARNING
```

See [Logging](#) on page 161 for more information about configuring the `logging.properties` file.



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

## 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 document lists these properties and explains their use and possible range of values for each.

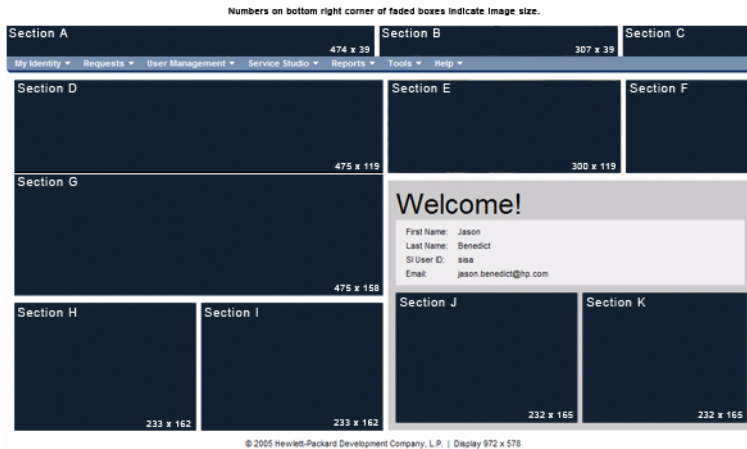
## How to Set Properties

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.

## User Interface Sections

The user interface is divided into sections, which are identified in [Figure 98](#). The descriptions of the properties that follow use this diagram for reference.

**Figure 98 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 (figure ?). 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 (figure ?).

#### [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 (figure ?) 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 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 – WebLogic 8.1.5
- Database – Oracle 10G

- [Connectors – LDAP/UTF-8](#)



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

## Configuration for Specific Environments or Platforms

The following sections provide platform and environment-specific configurations.

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

## Tuning the WebLogic Application and Database Servers

This section provides instructions for performance tuning the WebLogic application server/cluster and database server.

### Optimizing JMS Distributed Queues and Weblogic Execute Queues

The recommended configuration for a server or servers in a cluster varies according to whether the goal is to optimize for reconciliation or for UI Request performance.

Select Identity distributes its workload among the servers in a cluster via the JMS queues. Using the weight factors of distributed queue members in the WebLogic cluster, background processing such as user reconciliation and workflow execution can be moved to dedicated reconciliation servers.

The following JMS queues are mainly used during user reconciliation:

- `jms.OVSIReconQueue`
- `jms.OVSIWorkflowQueue`

For example, to schedule 90% of the workload on the reconciliation server and 10% on the front-end server in a cluster of two servers, the weight factors should be 90 for the distributed queue members of the above queues hosted by the intended reconciliation server and 10 for the intended front-end server.



When a reconciliation server is stopped, the front-end server will take over the entire workload until the reconciliation server is restarted.

On WebLogic, Select Identity uses separate execute queues for processing HTTP, SOAP, and EJB requests when the following execute queues are defined:

- `hp.ovsi.HTTP`
- `hp.ovsi.SOAP`
- `hp.ovsi.EJB`

The **Thread Limit** and **Thread Priority** settings can be used on these queues to control CPU usage by front-end and background tasks:

- The total number of threads defined for the above queues plus the standard default WebLogic execute queues should not exceed the limit of the total number of threads per process imposed by the operating system on the server.
- The thread limit for `hp.ovsi.SOAP` queue should not exceed three (3), to avoid high memory consumption during Web service calls. On servers that will not handle Web service requests, this execute queue can be removed to avoid having idle threads dedicated to it.
- On a single server that needs to process UI HTTP requests quickly or on the cluster node dedicated for processing the UI requests, the thread priority and the thread count should be increased for the `hp.ovsi.HTTP` queue and decreased for the `hp.ovsi.EJB` queue. A typical setting in this case would be as follows:

Queue Name	Thread Count	Thread Increase	Thread Priority
<code>hp.ovsi.HTTP</code>	25	5	10
<code>hp.ovsi.SOAP</code>	3	0	5
<code>hp.ovsi.EJB</code>	16	0	5

- On the cluster node dedicated for processing the reconciliation requests, the thread priority and the thread count should be increased for the `hp.ovsi.EJB` queue and decreased for the `hp.ovsi.HTTP` queue. A typical setting in this case would be:

Queue Name	Thread Count	Thread increase	Thread Priority
hp.ovsi.HTTP	5	5	10
hp.ovsi.SOAP	3	0	5
hp.ovsi.EJB	24	0	5

- On a single server or a cluster node that will process both UI and the reconciliation requests, the thread priority and the thread count should be set as follows:

Queue Name	Thread Count	Thread Increase	thread Priority
hp.ovsi.HTTP	15	5	5
hp.ovsi.SOAP	3	0	5
hp.ovsi.EJB	16	0	5

## 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.

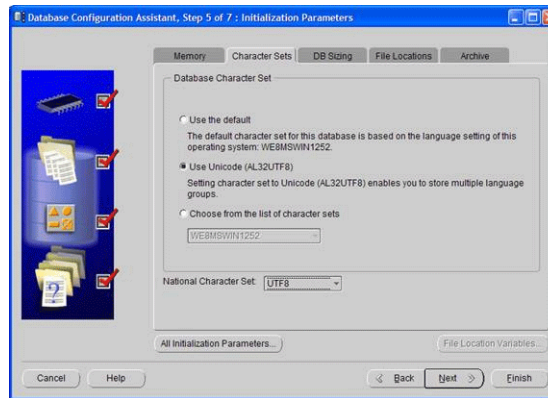
Some servers, such as Oracle, have the parameters controlling the maximum number of concurrent sessions that can be established at the same time from any client application.

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:

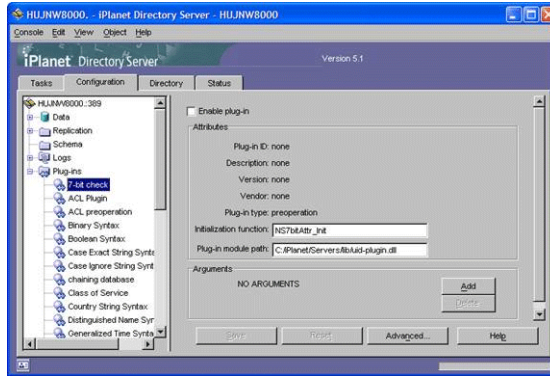
- 1 For Oracle 10g, open the Initialization Parameters window and select the **Character Set** tab.
- 2 Select the **Use Unicode (AL32UTF8)** radio button as shown.



## 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. Clicking  connects you to 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=50
```



---

# 7 Upgrading Select Identity

The HP OpenView Select Identity product CD for version 4.0 includes a migration script that performs an upgrade from versions 3.3.1 to 4.0 automatically. This includes upgrading the Select Identity application as well as reconfiguring the database so that it is compatible with version 4.0.

Read these instructions carefully *before* attempting to upgrade.

This section covers the following:

- [Upgrading from Version 3.3.1 to 4.0](#)
- [Preparing to Upgrade](#)
- [Preliminary Migration Steps](#)
- [Running the Migration Script](#)

## Upgrading from Versions Prior to 3.3.1

If you are upgrading from a version of Select Identity prior to 3.3.1, please contact Hewlett-Packard Technical Support for individual assistance. Upgrading the application and migrating the database contents requires the use of several scripts.

## Upgrading from Version 3.3.1 to 4.0

Your WebLogic server and Select Identity application must meet the following requirements to be suitable for upgrading to Select Identity Version 4.0 using this procedure:

- Select Identity version 3.3.1 (patch 3 or higher)

- Unix-based platform (including Linux and Cygwin)
- Oracle Client version 9i or 10g installed, with SQLplus in the system path
- Java 1.4.2 or better, set up in the system path
- The `J2EE.jar` file from WebLogic (`WebLogic.jar`) or another Web server.
  - You must set the variable `J2EE_JAR` in scripts to point to the file in question.
- Oracle 10.1.0.4 or later

## Preparing to Upgrade

Before migrating, ensure that WebLogic has no users connected to it. You must also undeploy the old version of Select Identity and shut down the WebLogic server. This is to prevent loss of auditing and other data.

### 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 migration script. Otherwise, the appropriate version of the JDBC driver file `ojdbc14.jar` can be found in the Oracle Home directory in `jdbc\lib`.

In the instructions that follow, note that Oracle may change the layout of their web site at any time, especially when new versions of the software are released. To download the driver, you will need to register as a member of the Oracle Technology Network. There is no charge for this membership.

- 1 Open your Web browser and go to **www.oracle.com**
- 2 Click the **Technology Network** link at the top of the page.
- 3 Under the **Technologies, Utilities and Drivers** section, click the link to **Oracle JDBC Drivers**.
- 4 Click 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 a new account.
- 8 After logging in or creating your account, the driver will be downloaded.
- 9 Copy the `ojdbc14.jar` file to the `lib` directory under the `Migrator` directory, or edit the `JDBC_CLASSPATH` in `oracle_run_migrate.sh` to point to where `ojdbc14.jar` lives.

## Stopping Select Identity Traffic

Perform the following procedure to stop all traffic on Select Identity:

- 1 Ensure that other users are not connected to the WebLogic server or to Select Identity. No new requests should be initiated until migration is complete.
- 2 Access the Select Identity 3.3.1 client.
- 3 On the login page, verify the Select Identity version that you have installed. This information is located under the login fields, at the bottom of the page. .




Do not proceed with these steps if the Select Identity version is earlier than 3.3.1 patch 3.

- 4 Log in to the Select Identity 3.3.1 client.
- 5 Approve any “pending” workflow tasks before starting the migration process.
- 6 Verify that any pending or in process requests or reconciliations have completed using the status reports.
- 7 Log out of Select Identity.

## Preparing the WebLogic Server

Perform the following procedure to prepare and shut down WebLogic:

- 1 Log in to the WebLogic console.

- 2 Shut down the WebLogic server and any managed servers.
  - 3 Using the navigation tree in the left pane of the console, navigate to **YourDomain>Deployments>Applications>lmz.ear**
  - 4 Log in at the command line and access the WebLogic administrative server, with the user ID of your choice.
  - 5 Back up your existing 3.3.1 Select Identity directories and files.
  - 6 Save your existing `TruAccess.properties` file. You may need to reference it when configuring the new file.
  - 7 Uninstall the previous release of Select Identity (3.3.1) using the manual uninstall steps specified in [Uninstalling HP OpenView Select Identity](#) on page 157.
  - 8 Install the new release of Select Identity (4.0) using the manual steps specified in [Select Identity Manual Installation Procedure](#) on page 35.
-  You do not need to create a new database.
- 9 Make the following updates to the `Truaccess.properties` file to meet your specific migration needs:

<b>If</b>	<b>Then</b>
The value for <code>fixedtemplate.bulk_default</code> is set to <code>ReconciliationDefaultProces</code>	Change it to either the <b>SIBulkOneStageApproval</b> or the <b>SI Provisioning Only Bulk</b> template. Continue.
The value for <code>fixedtemplate.bulk_default</code> is set to anything else	Continue
The value for <code>truaccess.fixedtemplate.bulk_move</code> is set to <code>ReconciliationDefaultProces</code>	Change it to either the <b>SIBulkOneStageApproval</b> or the <b>SI Provisioning Only Bulk</b> template.
The value for <code>truaccess.fixedtemplate.bulk_move</code> is set to anything else	Continue

<b>If</b>	<b>Then</b>
If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was set to SHA-1	Continue
If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was set to SHA-256	Continue
If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was <i>not</i> set	Add <code>com.hp.ovsi.messagedigest.algorithm</code> to the <code>truaccess.properties</code> file, with the value set to SHA-1.

10 Click **Import Configuration** to import the selected file.

11 Verify that your resource passwords are still synchronized.

<b>If the Resource Passwords</b>	<b>Then</b>
Are still in sync	Continue
Are not in sync	Follow the steps to modify the resources and resynchronize the passwords described in <a href="#">Modifying Resources</a> on page 153

12 Restart the managed servers to ensure that the changes are propagated to all the servers if you are updating a cluster.

## Modifying Resources

Perform the following procedure when you migrate to a new versions of 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.

Restart the managed servers to ensure that the changes are propagated to all the servers if you are updating a cluster.

## Preliminary Migration Steps

- 1 If you wish to reduce the amount of on-screen messages about migration progress, edit the `logging.properties` file to set the output level to `Warn`.
- 2 Unzip the Migration files.
- 3 Edit the following environment variables in `oracle_run_migate.sh`
  - `ORASERVER` — The IP address or domain name of the Oracle database server
  - `ORAPORT` — The database port the Oracle database listens on, usually 1521
  - `ORACLE_SID` — Connection identifier for the database where Select Identity is running
  - `ORAUSER` — Username (schema name) that has the Select Identity data
  - `ORAPWD` — Password for the user (schema) that has the Select Identity data
- 4 Verify that the `J2EE_JAR` environment variable in `oracle_run_migate.sh` is specifying a valid `J2EE.jar` file. If you are configured to run WebLogic, the default value will probably work. If you are not configured for WebLogic, change the `J2EE_JAR` environment variable to specify a valid file.
- 5 Edit the `java.util.logging.FileHandler.pattern` entry in the `logging.properties` file to point to a valid directory entry. This is where the java log files will be written.



- 6 Shut down the Select Identity application and disconnect any other users from the database. You may want to shut down the database listener by logging on as the oracle user and executing `lsnrctl stop`. This prevents initiation of any new remote database connections.
- 7 Make a backup of the database.

## Running the Migration Script

To run the migration script:

- 1 Change directories to the main directory for the migration files.
- 2 Execute the following command:

```
sh ./oracle_run_migrate.sh
```

The script runs through each step and displays a message to inform you as the steps are completed. When all steps are completed, the script displays a notification on-screen.

## Troubleshooting

- If the database connection information is set incorrectly in `oracle_run_migrate.sh`, the script does not fail after the first step and tries to run each step. This is caused by SQL Plus not returning an error code for this condition. Since neither SQL Plus nor the migration scripts can connect to the database, no harm is done. After fixing the incorrect connection information, just run the script again.
- The migration script runs each step in order. Should there be a failure during any step, the failure is logged and migration halted
- If there is a failure, first review the entries in the `migrationlog` table under the Select Identity schema. Log on to SQL Plus as the Select Identity owner and run the `oracle_migration_report.sql` script. This displays the status of each step.
- If the failure is during one the java migration steps, review the screen output or the log files in the directory specified by the `java.util.logging.FileHandler.pattern` entry in `logging.properties`.

- After the problem is resolved, you can resume running the migration by executing the `oracle_migrate.sh` script with the `-r` option (see below).

## Command Line Options

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

- `j` — Run a single step and stop (`-j` option).

For example, `oracle_run_migrate.sh -j 6` runs step 6 and stops.

- `r` — Resume execution at the specified step (`-r` option).

For example, `oracle_migrate.sh -r 12` resumes migration by running step 12 and then continues to run the remainder of the steps until the end of the script.

---

# 8 Uninstalling HP OpenView Select Identity

There are a number of places where Select Identity stores information. To completely uninstall the product you must perform ALL of the steps in each section. This section covers:

- Using the Wizard to Uninstall from the WebLogic Server
- Manually Uninstalling from the WebLogic Server
- Uninstalling the Select Identity Database

## Using the Wizard to Uninstall from the WebLogic Server

To use the uninstall wizard to remove Select Identity from the WebLogic Server, run the `Uninstall Select Identity.exe` (on Windows) or `Uninstall Select Identity.bin` (on UNIX) to launch the wizard. These files reside in the Select Identity home directory on the WebLogic Server. Follow the prompts. When complete, the wizard removes the LMZ file, data source, connection pool, and mail session.

## Manually Uninstalling from the WebLogic Server

This chapter describes how to manually remove Select Identity from a WebLogic server.

## Manually Uninstalling WebLogic

The following sections provide steps for a complete uninstall from WebLogic.

- Deleting the EAR File
- Deleting the EAR File
- Deleting the Data Source
- Deleting the Connection Pool
- Deleting the Mail Session


### Deleting the EAR File

To uninstall Select Identity on WebLogic, you delete the `lmz.ear` file from the WebLogic server.



Make sure that all dependencies on the system are removed.


Complete the following steps:

- 1 Log in to the WebLogic Server Console.
- 2 Select the `<domain_name>` → **Deployments** → **Applications** folder.
- 3 Click the **Delete** button () next to the `lmz` application.
- 4 When prompted to confirm the deletion, click **Yes**.

### Deleting the Connectors

You may have any number of connectors installed to support system resources. If you are completely uninstalling the Select Identity product you will want to uninstall the connectors.


Complete the steps listed below:

- 1 Log in to the WebLogic Server Console.
- 2 Select the `<domain_name>` → **Deployments** → **Connector Module** folder.
- 3 Click the **Delete** button () next to the connectors that you have installed.
- 4 When prompted to confirm the deletion, click **Yes**.

- 5 Click **Continue**.


## Deleting the Data Source

Perform the following steps to delete the Select Identity data source:

- 1 Log in to the WebLogic Server Console.
- 2 Select the **<domain\_name>** → **Services** → **JDBC** → **Data Sources** folder.
- 3 Click the **Delete** button () next to the **jdbc/TruAccess** connection.
- 4 When prompted to confirm the deletion, click **Yes**.
- 5 Click **Continue**.


## Deleting the Connection Pool

Perform the following steps to delete the Select Identity connection pool:

- 1 Log in to the WebLogic Server Console.
- 2 Select the **<domain\_name>** → **Services** → **JDBC** → **Connection Pools** folder.
- 3 Click the **Delete** button () next to the connection pool that was used by the data source.
- 4 When prompted to confirm the deletion, click **Yes**.
- 5 Click **Continue**.

## Deleting the Mail Session

Perform the following steps to delete the Select Identity mail session:

- 1 Log in to the WebLogic Server Console.
- 2 Select the **<domain\_name>** → **Services** → **JDBC** → **Mail Session** folder.
- 3 Click the **Delete** button () next to the **mail/TruAccess** connection.
- 4 When prompted to confirm the deletion, click **Yes**.
- 5 Click **Continue**.

# Uninstalling the Select Identity Database

After you uninstall the product from the web server, you can uninstall the data and tables from the database. This section describes how to uninstall the Oracle database.

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

- 1 From an 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 Logging

HP OpenView Select Identity implements `java.util.logging.Logger`, as defined by the Java 2, Standard Edition, v 1.4.1 API Specification. During installation, the `logging.properties` file is copied from the HP OpenView Select Identity Product CD to a subdirectory on the WebLogic server. This file defines how Select Identity logs messages and exceptions, according to the specification.

This appendix documents the logging options available for you to configure. For more detail about each option, refer to the `Logger` class in the API specification.

- **Handlers**

Handlers define where messages are logged. You *must* configure the following handlers in `logging.properties`: `ConsoleHandler` and `FileHandler`. In addition, the following handlers are available: `MemoryHandler` and `StreamHandler`. In the example on [page 161](#), a `FileHandler` and `ConsoleHandler` are configured (you must also configure the handler's format, as shown in the following example):

```
# List of global handlers
handlers = java.util.logging.FileHandler,
java.util.logging.ConsoleHandler

# Properties for the FileHandler
java.util.logging.FileHandler.limit = 500000
...
```

- **Message format**

Defines the format of logged messages based on the handler type. For example:

```
# Properties for the FileHandler
java.util.logging.FileHandler.pattern = /temp/log/
java.log
java.util.logging.FileHandler.limit = 5000000
```

```
java.util.logging.FileHandler.count = 20
java.util.logging.FileHandler.formatter =
java.util.logging.SimpleFormatter
```

Note the **pattern** attribute for FileHandler, which defines the location of the log file. The file location is relative to the user's root directory (the user under which the WebLogic server is running). This directory must exist. If it does not, Select Identity will not start.

For example, if you specify **log/log.txt** and the WebLogic server is running under the administrative user whose home directory is /user/admin, the file is written to the /user/admin/log/log.txt file. You can also specify an absolute path, such as /temp/log/log.txt.

Refer to the Logger class in the API specification for a list of format parameters required for each handler type.

- **Log level**

Defines the level of logging output. You can specify a level for all messages or only those written by a specific component. The levels can be set from SEVERE (smallest amount of log information) WARNING, INFO, CONFIG, FINE, FINER, to FINEST (greatest amount of log information). The main logging levels are defined as follows:

SEVERE = Logs major errors that usually prevent a feature or even the entire product from working. Includes bugs and errors caused by incorrect installation/setup.

WARNING = Logs minor errors and messages to be aware of that may indicate a problem with data, but should not hinder Select Identity as a whole.

INFO = Logs general tasks that are occurring, but does not provide many details.

FINEST = Logs detailed information about all logging output. This setting is used for debugging and helping to determine invalid setup issues.

Each level shows all the levels above it, so FINEST shows everything.

You can selectively modify the logging levels of the different components by specifying different levels for each. For example:

```
com.truologica.truaccess.util.persistence.PersistenceManager.level=FINEST
```



```
com.truologica.truaccess.util.scheduler.dao.BatchDAOImpl.l  
evel=FINE
```

```
com.truologica.truaccess.reconciliation.util.Reconciliatio  
nTimerTask.level=WARNING
```

```
com.truologica.truaccess.util.SMPTTimerTask.level=WARNING
```



Hibernate provides a lot of information when the logging level is set to **FINEST**. If you do not want the Hibernate log messages, add the following line to the **JRE** `logging.properties` file:

```
net.sf.hibernate.level=WARNING
```

In the following example, the default logging level is set to **WARNING** but a log level is also specified for the **LDAP** connector component (you must also specify a handler for component-specific log levels):

```
# Set the logging level for the root of the namespace.  
# This becomes the default logging level for all Loggers.  
.level=WARNING  
  
# List of global handlers  
...  
  
# Properties for the FileHandler  
...  
  
# Default level for ConsoleHandler. This can be used to  
# limit the levels that are displayed on the console even  
# when the global default has been set to a trace level  
java.util.logging.misc.ConsoleHandler.level = FINEST  
com.truologica.truaccess.connector.ldap.ldapv3.LDAPConnect  
or.level = FINE
```



---

# A Troubleshooting

This chapter provides error messages that you may encounter when configuring the WebLogic server for use with HP OpenView Select Identity. A suggested solution is also provided for each message.

This section covers the following:

- [General Installation Errors](#)
- [System Errors on WebLogic](#)
- [Migration Errors](#)

## General Installation Errors

The following list summarizes the most common installation problems:

Most problems are connection pool and datasource related. To avoid this problem, verify the communication between the WebLogic server and database by deploying a dummy connection pool and testing it in the WebLogic console. Typical problems are:

- Connection failure to the database due to wrong password, driver, dbname and port, domain name, server name, or database server not running.
- A Pre-existing partially installed SI\_Connection pool. This should be removed (Weblogic console)
- Incorrect path settings: make sure all paths and values specified are correct.
- If you enter an extra backslash at the end of a path name when entering Application Server settings, this creates an extra slash in the `myStartWL` script.

- If the SQL Server is on a port other than 1433, change the port setting. The installer does not handle other ports.
- JMS should be configured by the installer. If it fails in this section, it may still allow you to go on with the install, but you will not be able to login to the Login Screen of SI4.0. The console will produce errors that are JMS related. Check the admin console for JMS templates, etc. If not there, then it is best to uninstall, then re-install.
- The database schema may not have been populated before the installer started. Make sure that the installation prerequisites are met before installing.
- If the Select Identity client does not start after installation. Ensure that the `connector.jar` file is correctly added to the class path.
  - WebLogic Standalone: Verify the `connector.jar` file has been added to the class path in the `Mystartwl.sh` script.
  - WebLogic Cluster: Verify the `connector.jar` file has been added to the classpath for each node. The cluster class path is modified through the remote start setting for each server from the Administrative Console on WebLogic.
- If all labels and text are showing `Cannot Find Bundle Screens` after installing, check the following:
  - The `ovsii18n.jar` is probably not in the class path of the WebLogic server. Verify that the `ovsii18n.jar` file provided on the HP OpenView Select Identity Product CD in the `/library` directory is included in your WebLogic server's class path. Once you have verified that it is in the class path, restart the server to pick up the class path changes.
  - WebLogic Standalone: Verify the `ovsii18n.jar` file has been added to the class path in the `startweblogic.sh` or `myStartWL.sh` files. (The `myStartWL.sh` file is created by the Install Wizard.)
  - WebLogic Cluster: Verify the `ovsii18n.jar` file has been added to the class path for each node. The clustered server's class path is modified through the remote start setting for each server from the Administrative Console on WebLogic.

# System Errors on WebLogic

By default, trace information displays in the window from which the WebLogic Server was started.

- The WebLogic Server does not start.

*Possible Cause:* The `logging.properties` file is not configured properly.

*Possible Solution:* For more information, see [Logging](#) on page 161 for details. In particular, make sure that the directory specified for the FileHandler log file (the **pattern** attribute in the message format) exists.

- The WebLogic Server does not recognize the lmz application.

*Possible Cause:* An anomaly in the installation.

*Possible Solution:* Add the EJBs to the WebLogic server using the WebLogic Server Console.

- When the WebLogic server starts, the following error displays:

```
<Error> <JDBC> <Cannot startup connection pool
"ConceroConnectionPool" weblogic.common.ResourceException:
Could not create pool connection. The DBMS driver exception
was: java.sql.SQLException: SQL Server has been paused.
```

*Possible Cause:* SQL Server is not running.

*Possible Solution:* Start SQL Server.

- When the WebLogic Server starts, the following error displays:

```
<Error> <JDBC> <Cannot startup connection pool
"ConceroConnectionPool" weblogic.common.ResourceException:
Could not create pool connection. The DBMS driver exception
was: java.sql.SQLException:
Login failed for user 'sa'. Severity 14, State 1, Procedure
'null null', Line 0 Unable to connect, please check your
server's version and availability.
at weblogic.jdbc.mssqlserver4.TdsStatement.
microsoftLogin(TdsStatement.java:2872)
```

*Possible Cause:* The user ID or password is configured incorrectly for SQL Server.

- When attempting to sign in to Select Identity (through the web browser), an Error 500 -Internal Server Error displays on the page and the following error message displays in the server's window:

```
<Error> <JDBC> <Error during Data Source creation:
weblogic.common.ResourceException:
DataSource(jdbc.AccessUsDB) can't be created with
non-existent Pool (connection or multi)
(ConceroConnectionPool)>
```

*Possible Cause:* The targets for the JDBC connection pool may not be configured correctly.

- When attempting to create an administrator, this error displays:

```
createAndSendMail exception : javax.mail.SendFailedException:
Sending failed;
nested exception is:
javax.mail.MessagingException: Could not connect to SMTP
host: 65.70.174.236, port: 25;
```

*Possible Cause:* The mail server is not available or the mail server configuration is not correct.

## Migration Errors

Logging in fails. You cannot log in.

*Possible Cause:* Your encryption setting in the `TrucAccess.properties` file is not set correctly.

*Possible Solution:* Compare the previous `com.hp.ovsi.messagedigest.algorithm` setting in your previous `TruAccess.properties` file and make sure that the setting is the same.

Resources are not recognized by Select Identity.

*Possible Cause:* Resource passwords have gotten out of sync in the migration process.

*Possible Solution:* Complete [Modifying Resources](#) on page 153 to resynchronize the passwords in the new version.

# B Configuring TruAccess.properties

Configure general settings for HP OpenView Select Identity server and 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.

Properties can be disabled individually by commenting them out.

## TruAccess.properties Settings

Each property in the file is described below. Properties that should not be edited are specified.

For information about TruAccess properties that allow you to customize the Select Identity user interface, see [Custom User Interface Properties](#) on page 135.

### General Settings

- **`truaccess.dateformat=yyyy-MM-dd`**  
Specifies the date format throughout the OVSI system.
- **`truaccess.timestampformat=yyyy-MM-dd hh:mm:ss a`**  
Specifies the time stamp format throughout the OVSI system.
- **`truaccess.version=<version number>`**  
Specifies the version number of OVSI. *Do not change this value.*
- **`truaccess.hibernate.config=/com/trulogica/truaccess/util/persistence/mssqlserver.hibernate.cfg.xml`**

Specifies the hibernate property file. *Leave this property commented.*

- **truaccess.policy.id=1**

Specifies the default OVSI policy identifier.

- **truaccess.expirationProcessPeriod=30**

Specifies when a manager is sent a notification prior to automatic account expiration (in days). The default is 30days.

- **truaccess.expire.administrator.userId=sis**  
**truaccess.expire.administrator.adminFunc=Concero Sys Admin**

Specifies the default OVSI 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 OVSI client.

- **com.hp.ovsi.help.web = http://support.hp.com**

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 UI date format specified as a date pattern described in `java.text.SimpleDateFormat`. This value can be left empty in order to use OVSI 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  $\geq 4$  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, 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 OVSI.

- **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 OVSI.

- **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=smtptp**

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 OVSI 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 have to modify this setting.

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

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

## Keystore Settings

- **si.rsa.provider=org.bouncycastle.jce.provider.BouncyCastleProvider**

Specifies the provider of the keystore parameters. *Do not modify this setting.*

## Localization Settings

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

Supported locales (US English is 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 the template for certain Select Identity operations. The fixedtemplate workflows are used by operations NOT controlled by Service Role events. i.e. 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 time-out (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 OVSI. 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 OVSI 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  $\geq 4$  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 OVSI 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**

## 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 OVSI 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,LastNam,\_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.

## 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 a termination occurs.
- **si.serviceassign.evaluation=1**  
Specifies whether to evaluate user attributes or service assignments. Specify one of the following values. Skip services previously assigned to users 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`, OVSI 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**

OVSI 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**  
**=S\ Provisioning\ Only**  
**com.hp.ovsi.default.workflowtemplate.delegated.disable-service**

```

=SI\ Provisioning\ Only
com.hp.ovsi.default.workflowtemplate.delegated.enablesevice
=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.

## Attribute Mapping for Search Efficiency

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

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

- Identify the key attributes, such as SSN, employee ID, or email. Make sure that these are defined within OVSI and within the mapping file used for each system resource in which data is stored.
- Add corresponding columns to the `TAUser` table in the OVSI database.
- Drop and recreate the `TASmartAllUserSearchView` view in the OVSI database since the table definitions have been changed.
- Add entries in the `TruAccess.Properties` file.

For example, you may want to use the SSN and `employeeId` attributes to simplify searches. Perform the following:

- 1 Add the following columns to the `TAUser` table and create the corresponding indices:
  - a Add to the `TAUser` table:

```
SSN VARCHAR(11) default 'XXX-XX-XXXX';
EMPID VARCHAR(20) default 'XXXXXXXXXXXX';
```
  - b Create the following indices:

```
TAUSER_SSNIDX on TAUser(SSN);
TAUSER_EMPIDIDX on TAUser(EMPID);
```
- 2 Drop `TASmartAllUserSearchView` from the database, and recreate it as follows:

```
drop view TASmartAllUserSearchView
```

```
create view TASmartAllUserSearchView
AS SELECT T_ID.identObjId AS IdentityId, T_U.*,
T_ID.guid AS Guid, T_ID.taStatus AS Status
```

```
FROM TAIdentityObject T_ID INNER JOIN
TAUser T_U ON T_ID.identObjId = T_U.userId;
```

The `SELECT` and `FROM` parts of the `CREATE VIEW` command determine the query for which `TASmartAllUserSearchView` is a shortcut.

- 3 Update the following properties in the `TruAccess.properties` file:

```
truaccess.user.extra=SSN,EmpId
truaccess.user.extra.SSN.column=SSN
```

**truaccess.user.extra.EmplId.column=EMPID**

If there is no corresponding column mapping (**truaccess.user.extra.<AttributeName>.column=<Column Name>**), the attribute name is assumed to be the column name



# Index

## A

- attribute mapping
  - search, **184**
  - update TruAccess.properties for search, **185**
- attributes
  - search for, **184**
- auditing, **3**

## C

- clustered servers
  - create JMS connection factory, **43**
- configure
  - JDBC connection pool, **63**
  - JMS settings, **42**
  - JTA settings, **79**
- configuring
  - logging, **161**
  - recommended, **135**
  - TruAccess.properties, **129, 169**
  - TruAccess.properties required settings, **129**
- connectors, **4**
- context management, **3**

## D

- database server
  - configuring Oracle, **13**
- database server requirements, **8**

documentation, *v*

## E

Emailed report format, **147**

## F

- firewall configuration, **12**
- forms, **3**
- functional components, **3**

## G

- general settings, **129**
- generating
  - generate the keystore, **131**

## I

- installing:WebSphere installation wizard for standalone server, **85**
- interface requirements, **12**
- interface settings, **129**
- Internationalization, **5**
- internationalization, **140**
  - UTF-8 encoding on Oracle10G, **144**

## J

JDBC connection pool, configure, **63**

- JMS connection factory
  - create for clustered servers, **43**
- JMS Queue
  - create for a single server, **50, 57**
- JMS settings
  - configure, **42**
- JMS settings for a single server
  - create JMS Queue, **50, 57**
- JMS settings for clustered servers
  - set up JMS connection factory, **43**
- JTA settings
  - configure, **79**

## **K**

- keystore, **4, 131**

## **L**

- language fonts, **145**
- localization, **140**
- log files, **161**
- logging.properties
  - configuring, **35, 79**
- login page, **146**

## **M**

- migration, **149**

## **O**

- online help, *vi*
- Oracle
  - internationalization encoding, **144**
- Oracle requirements, **9**

## **R**

- reconciliation, **3**

- reporting, **3**
- requirements
  - Oracle, **9**
  - WebLogic, **11**
- resource management, **3**

## **S**

- search for attributes, **184**
- security, **4**
  - keystore, **4**
- Select Identity
  - configurations supported on, **8**
  - system requirements, **7**
- Self-Registration, **146**
- server settings, **129**
- service management, **3**
- service roles, **3**
- Starting WebLogic, **40**
- system architecture, **1**
- system errors
  - WebLogic, **167**
- system errors on WebLogic, **165**
- system requirements, **7**
  - database server, **8, 9, 10**
  - firewall, **12**
  - interface, **12**
  - web application server, **10, 11**

## **T**

- TAUser database table, **185**
- TCP/IP ports, **12**
- tiered authority, **4**
- troubleshooting, **165**

TruAccess.properties, **129, 169**  
attribute mapping search settings, **185**  
configuring, **169**  
configuring required settings, **129**  
settings, **169**

## **U**

uninstalling, **158**  
upgrade Select Identity, **149**  
user management, **3**  
User Search criteria, **147**  
user searches, **184**  
UTF-8 encoding, **145**

## **V**

virtual user ID, **2**

## **W**

web application server, configuring  
WebLogic, **83**  
web application server requirements, **10, 11**  
WebLogic install, **23**  
manual install, **35**  
WebLogic requirements, **11**  
WebSphere install:installation wizard, **85**  
welcome, **1**  
workflow management, **3**

