

HP OpenView Select Identity

For the Red Hat Enterprise Linux and
Windows 2003 Operating Systems

Software Version: 4.0

Installation Guide

March 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). 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

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 administrators who use HP OpenView Select Identity as their Business Services Identity Management solution. This guide provides detailed procedures for installing and configuring the Select Identity system.

Typographical Conventions

This guide uses the following typographical conventions:

Convention	Description
Bold	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

1	Welcome to HP OpenView Select Identity	1
	Introduction	1
	System Architecture	3
	Security and Communication	5
	Internationalization	6
	Technical Qualifications for Installing Select Identity	7
2	System Requirements	9
	Installation Process Overview	9
	Reviewing Minimum Recommendations	10
	Supported Configurations	10
	Installation to Directories with Embedded Spaces	10
	Database Server Requirements	11
	BEA WebLogic Server Requirements	12
	Select Identity Interface Requirements	13
	Ports Required for Firewall Configuration	13
3	Configuring the Database Server	15
	Oracle Database Configuration	15
	Configuring an MS SQL Database Server	17
4	Installing Select Identity on BEA WebLogic	21
	Single or Clustered Server Installation	21
	Select Identity Installation Requirements	22
	Important Installation Information	22
	Prerequisite Configuration Procedure	23
	Editing the Default startWebLogic Script on a Single-Server Installation	24
	Select Identity Installer Process Summary	25

Select Identity Installer Procedure	26
Validating the Installation	35
Restarting WebLogic After Installing Select Identity	36
Select Identity Manual Installation Procedure	36
Creating Select Identity Directories and Copying Installation Files	37
Creating the myStartWL Script on a Single Server	39
Starting WebLogic	41
Configuring the Mail Session	42
Configuring JMS Settings	43
Configuring New JMS Connection Factories	44
Configuring a JMS File Store	46
Configuring a JMS Server	48
Creating the JMS Queues on a Single Server	51
Configuring JMS Queues on a Clustered Server	54
Configuring the JMS Audit Queues on a Clustered Server	57
Configuring JMS Topics on a Clustered Server	57
Creating the JMS Topics on a Single Server	58
Creating JMS Server Members	59
Modifying the JMS Template for JMS Queues and Topics	62
Configuring a JDBC Connection Pool	64
Configuring the JDBC Data Source	68
Modifying the WebLogic Server Class Path	70
Configuring the Select Identity Execute Queues	73
Enabling Anonymous Admin Lookup	75
Starting the WebLogic Server	76
Deploying Select Identity on WebLogic	76
Additional Configuration	80
Configuring the JTA Settings	80
Deploying the Select Identity Online Help Files	80
5 Configuring HP OpenView Select Identity	83
Configuring TruAccess.properties Required Settings	83
Setting the Database Repository Property	83
Additional Required Settings	84
Generating a Custom Keystore	85
Creating the Custom Keystore	86

Integrating the Keystore with Select Identity	87
Recommended Configuration	89
Custom User Interface Properties	89
How to Set Properties	90
User Interface Sections	90
Customization Properties	91
Default Properties	93
Internationalization and Localization	94
UTF-8 Encoding on Oracle 10G	95
iPlanet LDAP Configuration	96
Set Encoding in Internet Explorer	96
Adding Supported Language Fonts	96
Additional Configuration Options	97
6 Upgrading Select Identity	101
Upgrading from Versions Prior to 3.3.1	101
Upgrading from Version 3.3.1 to 4.0	101
Preparing to Upgrade	102
Downloading the Oracle JDBC driver	102
Stopping Select Identity Traffic	103
Preparing the WebLogic Server	103
Modifying Resources	105
Preliminary Migration Steps	106
Running the Migration Script	107
Troubleshooting	107
Command Line Options	108
7 Uninstalling HP OpenView Select Identity	109
Using the Wizard to Uninstall from the WebLogic Server	109
Manually Uninstalling from the WebLogic Server	109
Manually Uninstalling WebLogic	110
Deleting the EAR File	110
Deleting the Connectors	110
Deleting the Data Source	111
Deleting the Connection Pool	111
Deleting the Mail Session	111

Uninstalling the Select Identity Database	112
A Logging	113
B Troubleshooting	117
General Installation Errors	117
System Errors on WebLogic	119
Migration Errors	120
C Configuring TruAccess.properties	121
TruAccess.properties Settings	121
Attribute Mapping for Search Efficiency	133
Glossary	137
Index	149

1 Welcome to HP OpenView Select Identity

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 section covers the following topics:

- [Introduction](#)
- [System Architecture](#)
- [Security and Communication](#)
- [Internationalization](#)

Introduction

HP OpenView Select Identity (Select Identity) addresses the formidable challenges of managing identity within complex, multi-organizational business processes.

The Select Identity solution automates user account provisioning and management, and administrates access privileges across platforms, applications, and corporate boundaries. It provides robust workflow, user self-service, reporting, and delegated administration capabilities.

Traditional identity management systems employ the user-centric model of roles to distribute access. In an extended enterprise, roles proliferate exponentially to accommodate the numerous complex business relationships that exist between users, organizations, resources, and security policies.

Select Identity's contextual identity management is a dramatic advancement in identity management. Identity management provides a service-centric approach to managing identity. In any company, employees, customers, and partners participate in services or business processes that comprise the

operation of the company. For example, these processes might include “order processing” or “accounts receivable.” Each Service may consist of a number of applications or resources that require unique access privileges depending on the Service, its participants, and corporate policy. Identity Management incorporates these complex relationships and leverages them to automate the tasks associated with managing identity, including:

- Provisioning accounts and privileges
- Approving workflows
- Delegating administrative rights
- Enforcing security policy
- Reporting

Identity management mitigates the limitations of the traditional role and rule-based identity management, enabling scalability throughout the extended enterprise while reducing deployment times and management costs.

Key features of Select Identity include:

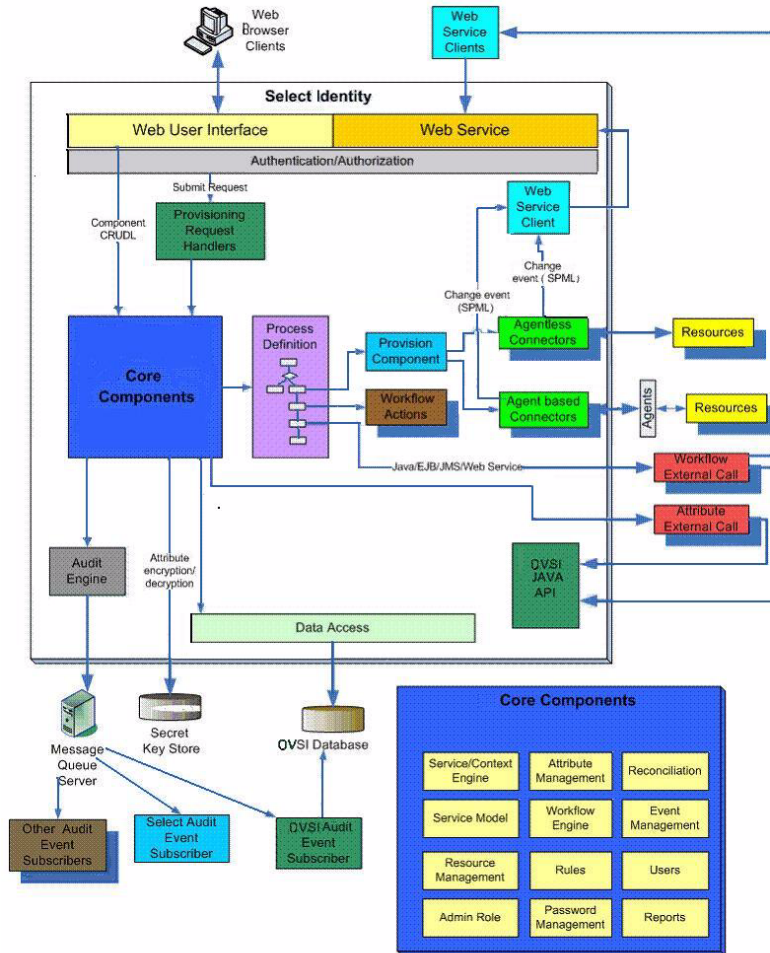
- **Centralized Management** – Provides a single point of control for managing users and entitlements.
- **Provisioning** – Automates the creation, update, and deletion of information system accounts and entitlements across the enterprise.
- **Extreme Delegation** – Enables administrative rights to be distributed to multiple tiers of functional departments, customers, and partners.
- **Workflow** – Automates identity-related processes such as access approval and provisioning, and integrates these with other business processes.
- **User Self-Service** – End users can initiate access to services, change passwords, set password hints, and update general identity information through a simple web interface.
- **Password and Profile Management** – Manages and distributes password and user profile information among enterprise information systems.
- **Audit and Reporting** – Provides standardized and on-demand reporting on permissions, actions, and account activity.

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

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 85 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 94.

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 15).
- 3 Configure the Web Application server for use with Select Identity (For BEA WebLogic, see [Prerequisite Configuration Procedure](#) on page 23).
- 4 Install Select Identity (see [Installing Select Identity on BEA WebLogic](#) on page 21).

- 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 85).
- 6 Configure the `TruAccess.properties` file for your environment (see [Configuring HP OpenView Select Identity](#) on page 83 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 is supported on the following configurations:

Web Server	Platform	Database
BEA WebLogic Server 8.1.5	Red Hat Enterprise Linux v3	Oracle 10G
BEA WebLogic Server 8.1.5	Windows 2003	Oracle 9i
BEA WebLogic Server 8.1.5	Windows 2003	MS-SQL 2000

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.

Oracle 10g	
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)

Oracle 9i	
Version	Oracle Database, version 9i
Operating System	Microsoft Windows 2003
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)

MS-SQL	
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: <code>weblogic.jdbc.sqlserver.SQLServerDriver</code>

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 systems running Select Identity on WebLogic servers.

BEA WebLogic	
Version	BEA WebLogic Server, v8.1, sp5
Operating System	Red Hat Enterprise Linux v3
Processor	1 GHz CPU

BEA WebLogic	
Memory (RAM)	512 MB of RAM (minimum) 1 GB RAM (recommended)
Disk space	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 Execute the schema creation script by running the following:

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

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

- b Verify that no error message results.

6 Insert the required default data into the Select Identity database:

- a Run the data creation script by entering the following command:

<path>/oracle_concero_dml.sql

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

- b Verify that no error message results.

Configuring an MS SQL Database Server

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

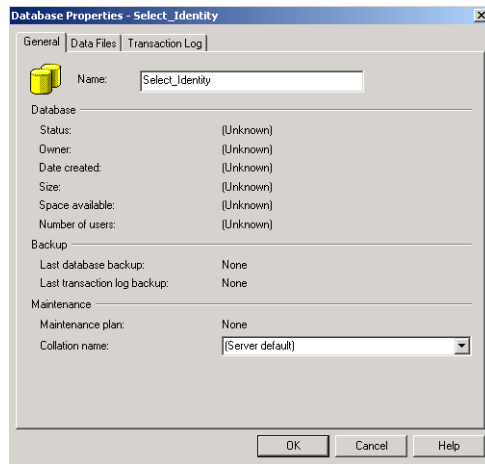


Ensure that your MS SQL Database is configured to be case-insensitive, and that it is configured in Mixed-Authentication mode.

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.
- 1 Log in to the Microsoft SQL Server Enterprise Manager interface.
- 2 In Enterprise Manager, expand **Microsoft SQL Server** → **SQL Server Group** → **server**, where **server** is the name of the SQL Server instance.

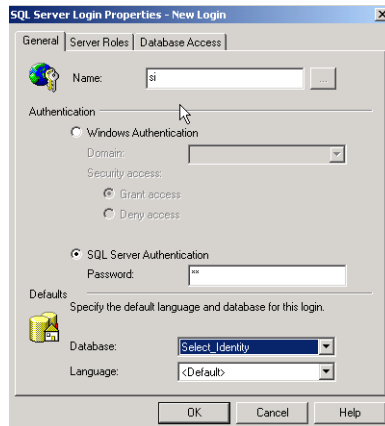
3 Right-click **Databases**, and select **New Database....**



4 Enter a name for the database, such as **Select_Identity**. Click **OK** to finish creating the database.

5 Create a database user that can be used to manage the Select Identity database. Complete the following steps to do so:

- 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 displays.



- 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**. Confirm your password when prompted.
 - f Click the **Database Access** tab.
 - g Click the **Permit** checkbox next to the Select Identity database user.
 - h Assign the **db_owner** and **public** permissions to the new user.
 - i Click **OK** to save your settings.
- 6 Create the Select Identity database schema by following these 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 `concerto_ddl.sql` SQL script from the Select Identity home directory you created in [Step 2](#) on page 17.
 - Click the **Open** icon.
 - Locate the Select Identity home directory.
 - Select the `concerto_ddl.sql` file.
 - Click **Open**.
 - d Run the script by clicking the **Execute Script** or Play button.
 - e Verify that an error message is not displayed.
- 7 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 `concerto_dml.sql` SQL script from the directory you created in [Step 2](#) on page 17.
 - 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.

4 Installing Select Identity on BEA WebLogic

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.

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.

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.

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](#)

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 5, 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 23 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.

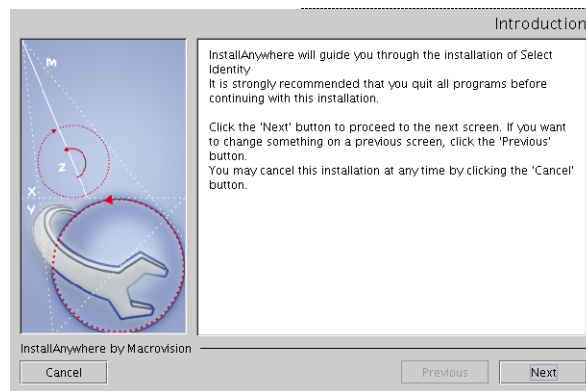
- 3 Mount the HP OpenView Select Identity product CD.
- 4 We recommend using the `install.exe` or `install.bin` file located under the VM directories.
- 5 Copy the following files into a convenient location on the Admin server from the HP OpenView Select Identity product CD:

Linux: `installer.bin`

Windows: `installer.exe`

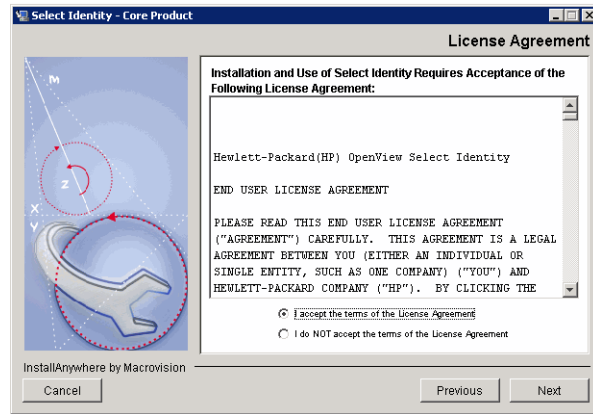
- 6 Run the executable named `install.bin` (Linux) or `install.exe` (Windows) to open the HP OpenView Select Identity Installer, as shown in [Figure 2](#).

Figure 2 The HP OpenView Select Identity Installer Introduction



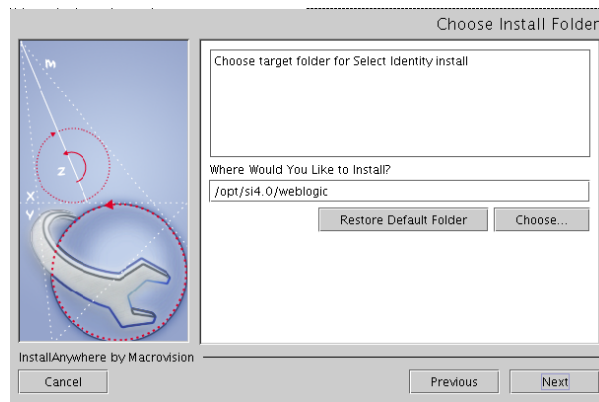
- 7 Click **Next** to proceed to the **License Agreement** page.

Figure 3 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 4 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.

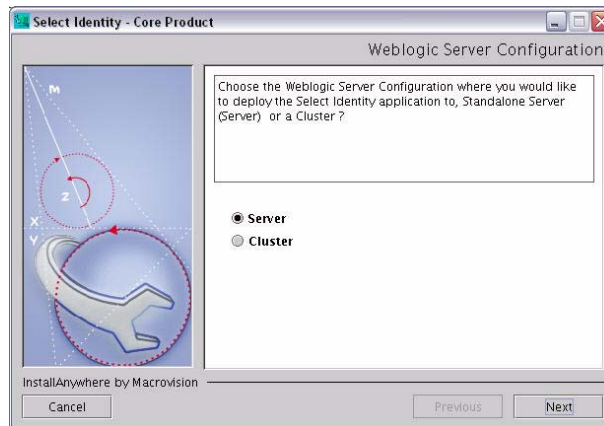
Figure 5 The Pre-Installation Summary page



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.

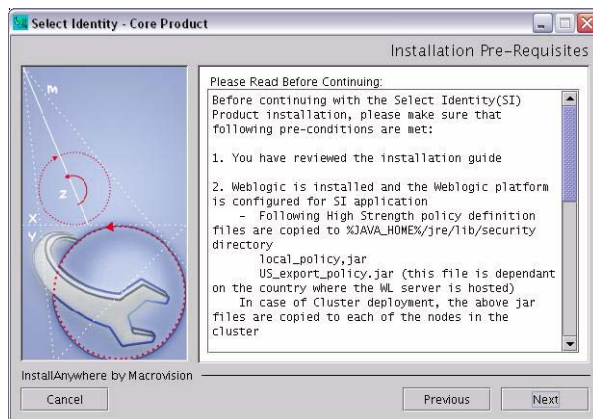
Figure 6 The Server Configuration Page



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.

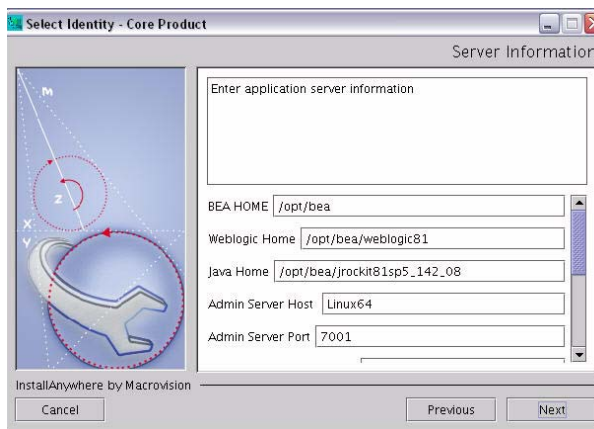
Figure 7 Installation Prerequisites page



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 8 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

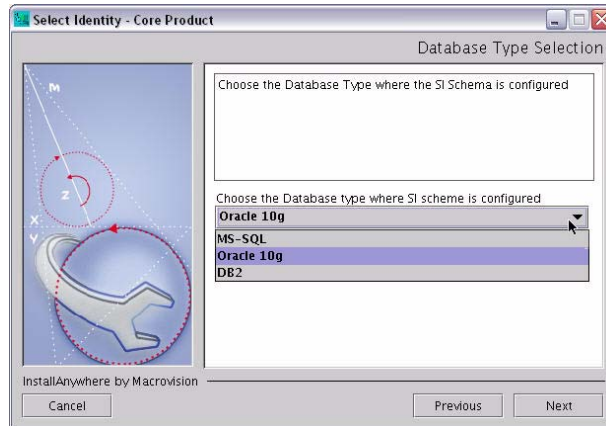
- **Server Port** — The port used by Select Identity
- **Domain Name** — The application domain of the installation
- **Admin Server Login Name** — The WebLogic Admin user name
- **Admin Server Password** — The password for the WebLogic Admin user
- **Cluster Name** — The name of the cluster or server, 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 15 for more information.

Figure 9 The Database Type Selection page, on a Linux system



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

Figure 10 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.

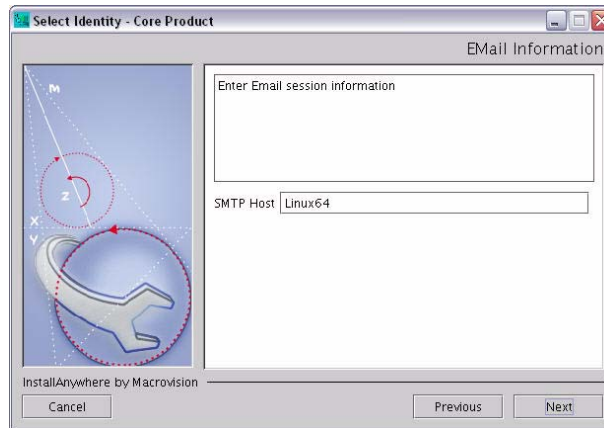
The installer prepopulates the fields based on previous selections.

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 11 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 12 Important Information page for single servers

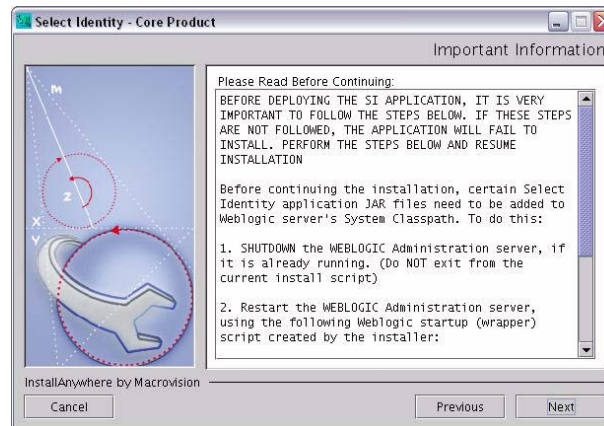
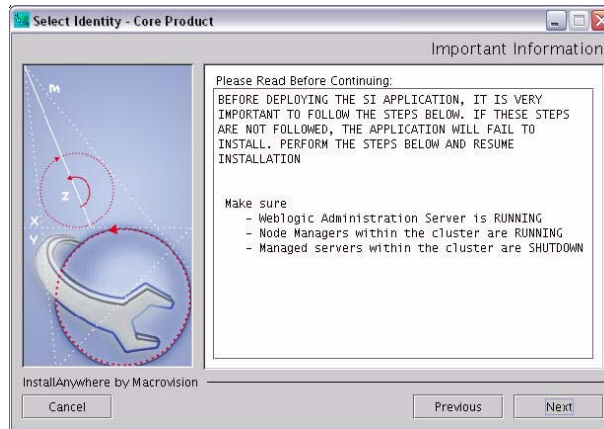


Figure 13 Important information page for clustered servers



- 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**.

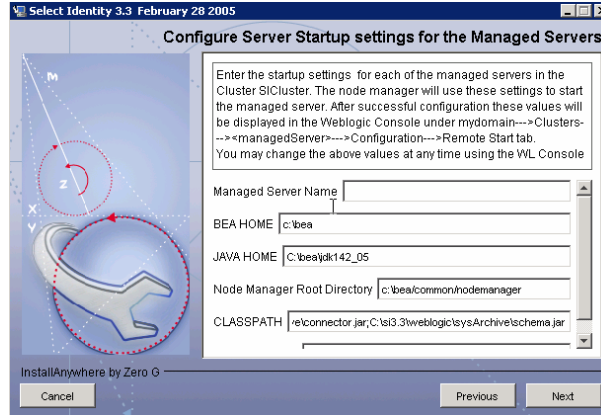
The installer verifies the WebLogic Admin server configuration information and begins to install Select Identity.



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 35.
- 29 If you are installing on a cluster, click **Next** to proceed to the **Managed Server Configuration** page.

Figure 14 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 80 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 22.
- [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 83 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 15 Example myStartWL script for Windows systems

```

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

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

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

call startweblogic.cmd

```

Figure 16 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 17 WebLogic Server Home Page



Configuring the Mail Session

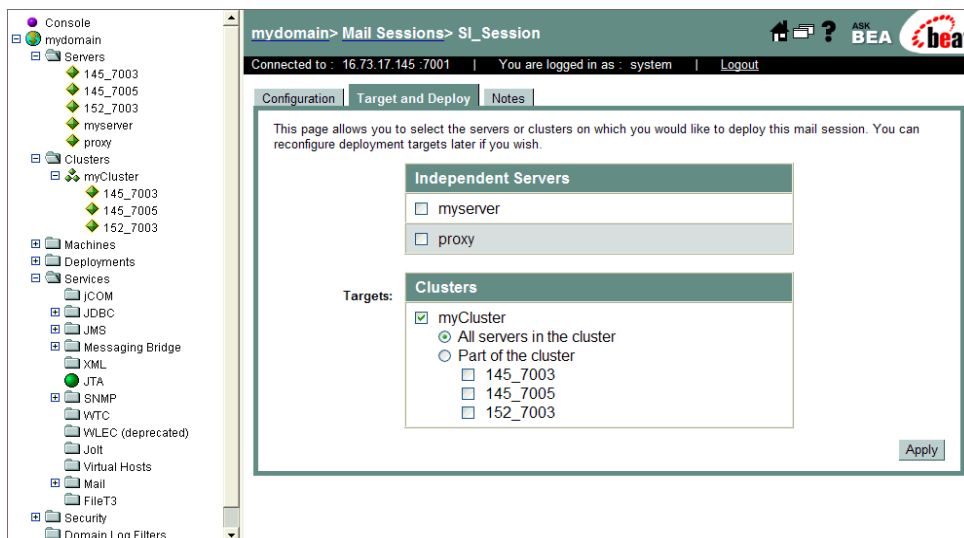
Configure the mail session for Select Identity, as follows:

- 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
Name	Enter a name for the mail session.
JNDIName	Enter mail/TruAccess
Properties	Enter the IP address of the mail server. For example: mail.smtp.host=192.168.1.52.

Click **Create** to save these settings and proceed to the **Target and Deploy** page. The illustration in [Figure 18](#) shows an example for a clustered server. If you are installing on a single server, only independent (single) servers are available for deployment.

Figure 18 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	Clustered servers: — Uncheck to indicate False . Single servers: — Check to indicate True (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 19 JMS Connection Factory Target and Deploy Page

The screenshot shows the BEA WebLogic console interface. At the top, the breadcrumb navigation reads "mydomain > JMS Connection Factories > jms.OVSITCF". The user is logged in as "weblogic". The page has three tabs: "Configuration", "Target and Deploy" (which is active), and "Notes".

The main content area contains the following text: "This page allows you to select the servers or clusters on which you would like to deploy this JMS connection factory. You can reconfigure deployment targets later if you wish."

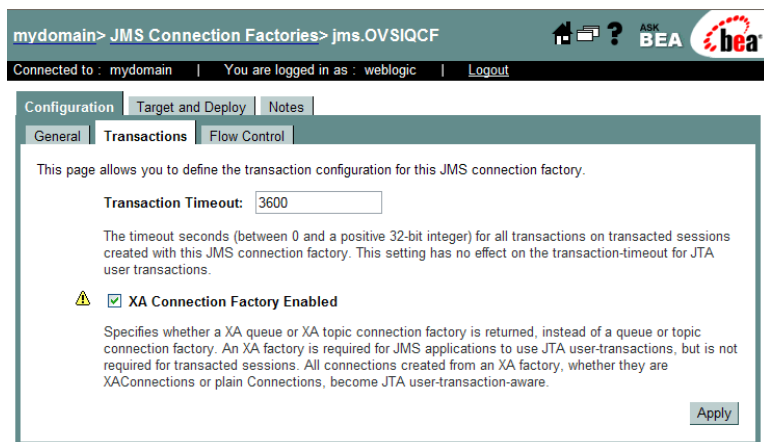
There are two main sections for target selection:

- Independent Servers:** A list with two entries: "myserver" and "proxy", each with an unchecked checkbox.
- Targets: Clusters:** A list with three entries: "MyCluster" (checked), "All servers in the cluster" (radio button selected), and "Part of the cluster" (radio button unselected). Under "Part of the cluster", there are two sub-entries: "64_7003" and "65_7003", each with an unchecked checkbox.

At the bottom of the form area, there is a note: "The targets in the current domain on which this item can be deployed. The targets value" and an "Apply" button.

- 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 20 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 21 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
FileStore	JMSFileStore

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

Figure 22 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 Server1 is the server ID in the cluster.
Temporarily store the Select Identity Service Assignment, Reconciliation, and Cache cleanup JMS messages	OVSI Paging Store Server1 Server1 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 23 JMS Servers Page

mydomain > JMS Servers

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

A JMS server manages connections and message requests on behalf of JMS clients.

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

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

[Customize this view...](#)

Name	Persistent Store	Temporary Template	Bytes Maximum	Messages Maximum	
WSStoreForwardInternalJMSServermyserver	FileStore	n/a	-1	-1	

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

Figure 24 Create a new JMS Server Page

mydomain > JMS Servers > Create a new JMS Server...

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

Configuration | Target and Deploy | Monitoring | Notes

General | Thresholds & Quotas

This page allows you to define the general configuration parameters for this JMS server. A JMS server manages connections and message requests on behalf of clients. (You must define a JMS server before you can configure any JMS destinations.)

Name:
 The name of this JMS server.

Persistent Store:
 The persistent store (either file-based or JDBC-based) for this JMS server, which will be used as a physical repository for storing persistent message data. In order to select a store, first configure either a JMS file store or JDBC store using the JMS > Stores node. The selected store cannot be the same as the selected paging store, or the same store used by any other JMS server.

Paging Store:
 The name of the paging store for this JMS server, which is a dedicated JMS file store where non-persistent messages can be temporarily paged when this JMS server's message load reaches a specified threshold--if paging is enabled on the Thresholds & Quotas tab. In order to select a paging store, first configure a dedicated "paging" JMS file store using the JMS > Stores node. The selected paging store cannot be the same as the selected non-paging store, or the same store used by any other JMS server.

Temporary Template:
 The name of an existing JMS template to use when creating all temporary queues and topics for this JMS server. Specifying a value for this field allows JMS applications to create temporary destinations.

Expiration Scan Interval: seconds
 A specified waiting period, in seconds (between 0 and a positive 32-bit integer) that defines how long the JMS server will pause between its cycles of scanning local destinations for expired messages to be processed. Setting this value to 0 disables active message expiration scans; messages still expire, but are cleaned up less quickly by the server.

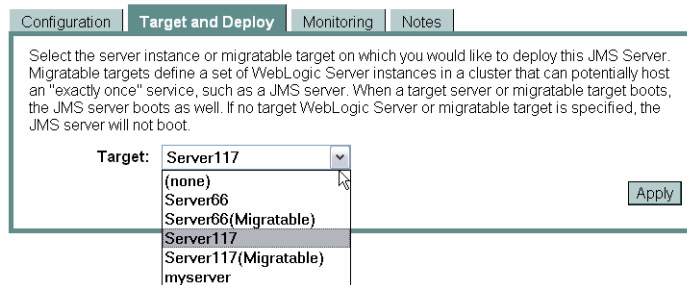
3 Tab from field to field and enter the required information.

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 25 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 True .
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.

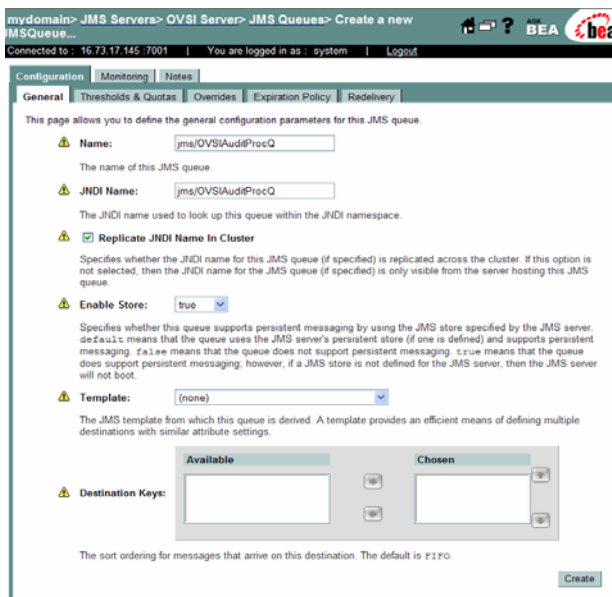
Creating the JMS Queues on a Single Server

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 54.

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 26 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

Purpose	Recommended Name	Required Name
UserRecon Process	jms.OVSIReconQueue	jms/OVSIReconQueue
Resource Reconciliation Flow Control	jms.OVSIResReconDispatcherQ	jms/OVSIResReconDispatcherQ
Resource Reconciliation Processing	jms.OVSIResReconQ	jms/OVSIResReconQ
SA Integration	jms.OVSIISaudQ	jms/OVSIISaudQ
Batch Handling	jms.OVSIISchedulerQueue	jms/OVSIISchedulerQueue
Service Assignment	jms.OVSIServiceAssignQueue	jms/OVSIServiceAssignQueue
Request Expiration	jms.OVSIWfRequestExpireQueue	jms/OVSIWfRequestExpireQueue
Workflow Process	jms.OVSIWorkflowQueue	jms/OVSIWorkflowQueue

- 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 80.

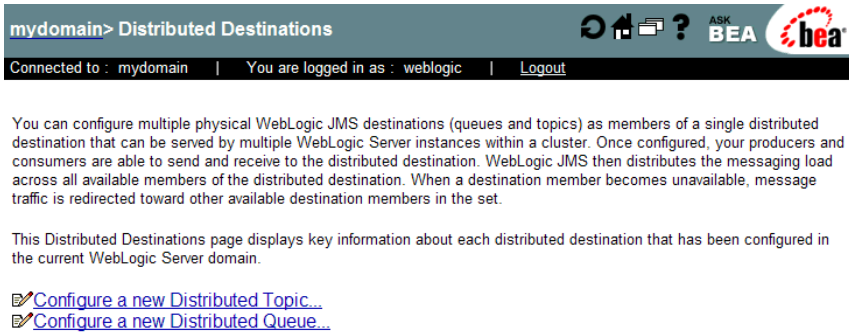
Configuring JMS Queues on a Clustered Server

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** → **Servers** → **Distributed Destinations**.

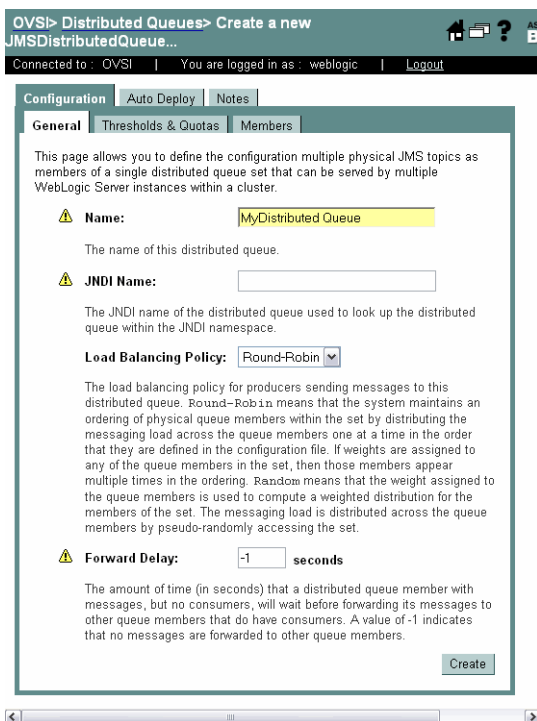
Figure 27 Distributed Destinations Page



The screenshot shows the 'mydomain> Distributed Destinations' page. The top navigation bar includes 'mydomain> Distributed Destinations', a refresh icon, a home icon, a help icon, and the BEA logo. Below the navigation bar, it shows '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. Below this, there 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 28 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
Batch Processing for Bulk Operations	jms.OVSIBulkQueue	jms/OVSIBulkQueue
Service Recon Process	jms.OVSIChangeReconProcessorQueue	jms/OVSIChangeReconProcessorQueue
Entitlement Cache Processing	jms.OVSIEntCacheQueue	jms/OVSIEntCacheQueue
Service Recon Flow Control	jms.OVSIMessageAckQueue	jms/OVSIMessageAckQueue

Process	Recommended Name	Required JNDI Name
User Recon Process	jms.OVSIReconQueue	jms/OVSIReconQueue
Resource Reconciliation Dispatch	jms.OVSIResReconDispatcherQ	jms/OVSIWfResReconDispatcherQ
Resource Reconciliation Processing	jms.OVSIResReconQ	jms/OVSIResReconQ
SA Integration	jms.OVSI SaudQ	jms/OVSI SaudQ
Batch Handling	jms.OVSI SchedulerQueue	jms/OVSI SchedulerQueue
Service Assignment	jms.OVSI ServiceAssignQueue	jms/OVSI ServiceAssignQueue
Workflow Process	jms.OVSI WorkflowQueue	jms/OVSI WorkflowQueue
Request Expire	jms.OVSI WfRequestExpireQueue	jms/OVSI WfRequestExpireQueue

- 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.

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

- 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 51 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.

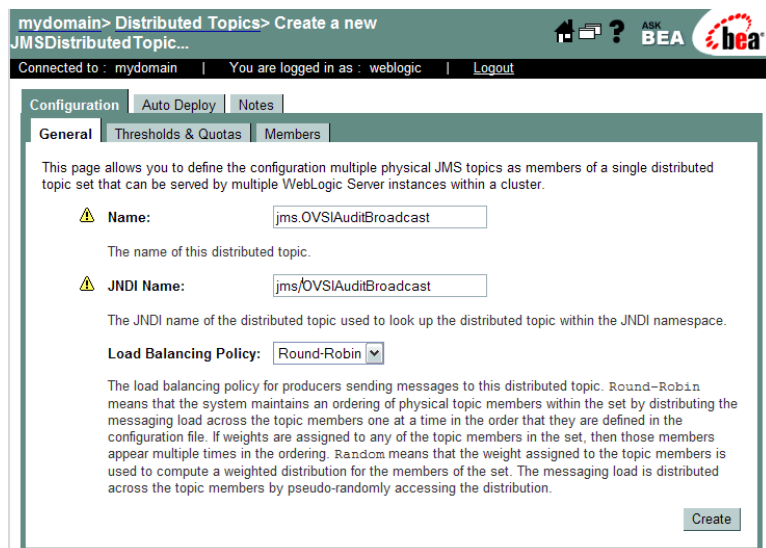
Configuring JMS Topics on a Clustered Server

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** → **Servers** → **Distributed Destinations**.
- 2 Select the **Configure a new JMS Topic** link to open the **Create a new JMS Distributed Topic** page.

Figure 29 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 57.

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** → **<your_OVSI_Server>** → **Destinations**.
- 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 80.

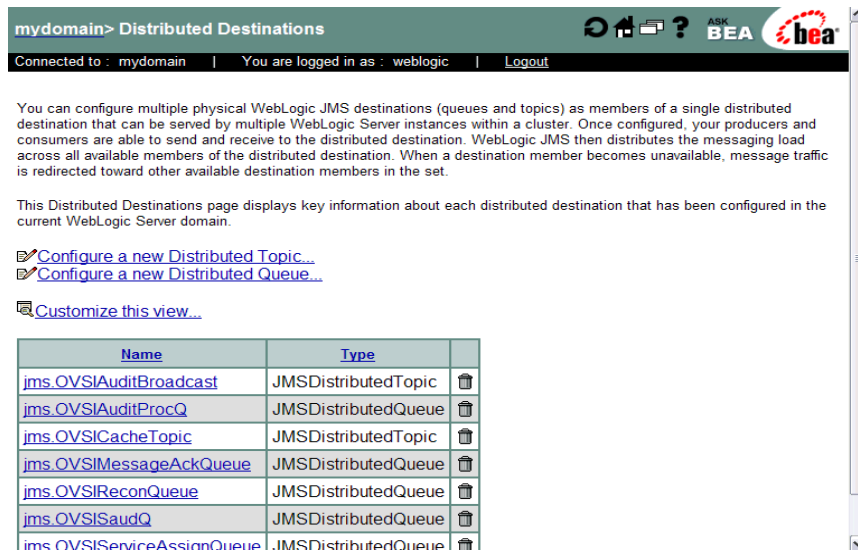
Creating JMS Server Members

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.

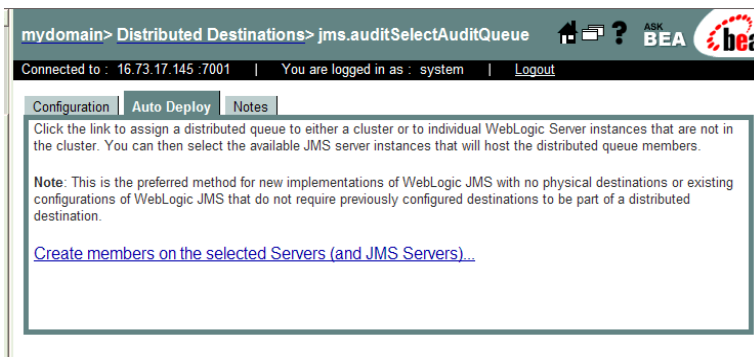
- 1 Open the **Distributed Destinations** page by navigating to **<domain_name>** → **Services** → **JMS** → **Distributed Destinations**.

Figure 30 Distributed Topic Page



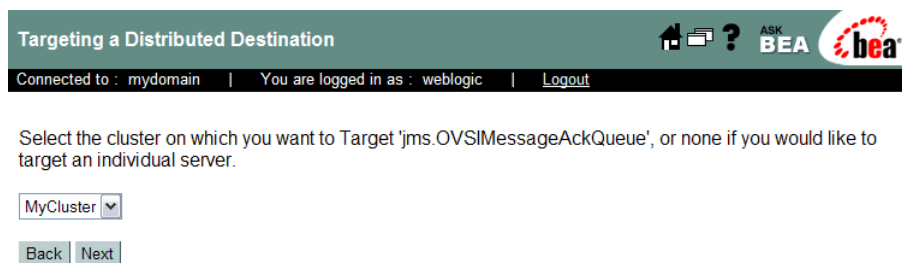
- 2 Select an existing JMS Queue or JMS Topic link in the **Name** column.
The **Distributed Destinations** page opens, showing the last tab that was saved for the selected JMS Queue or Topic.
- 3 Click the **Auto Deploy** tab to view the **Auto Deploy** page.

Figure 31 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 32 Targeting a Distributed Destination Page

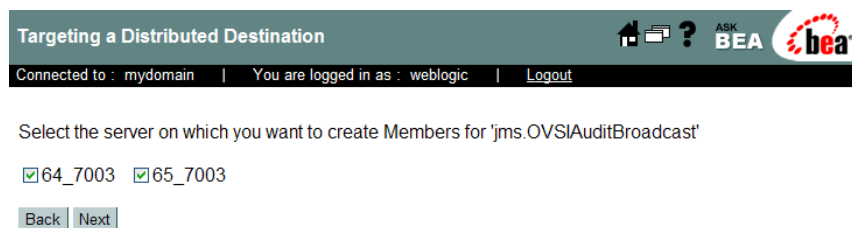


1 Make the correct entry

Server Type	Action
Single Server	Select None 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.

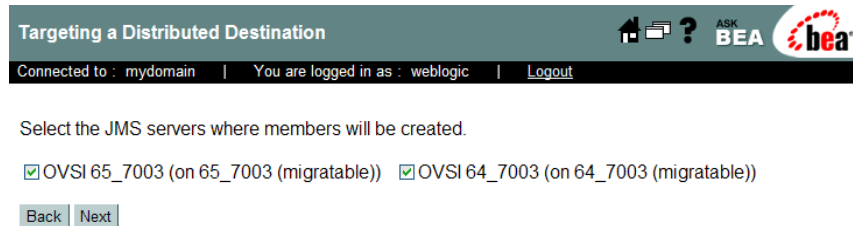
Figure 33 Targeting a Distributed Destination Page to Select Servers



6 Select each server on which you want to create members for the JMS Queue or Topic.

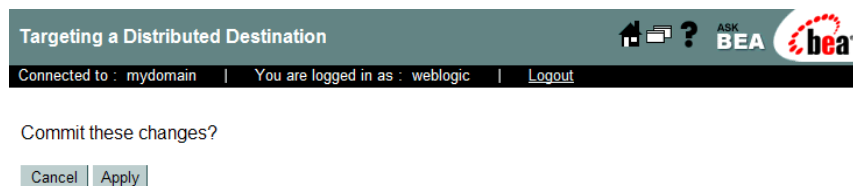
7 Click **Next** to proceed to the next **Targeting a Distributed Destination** page and select servers.

Figure 34 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 35 Targeting Distributed Destination Page: Committing Changes



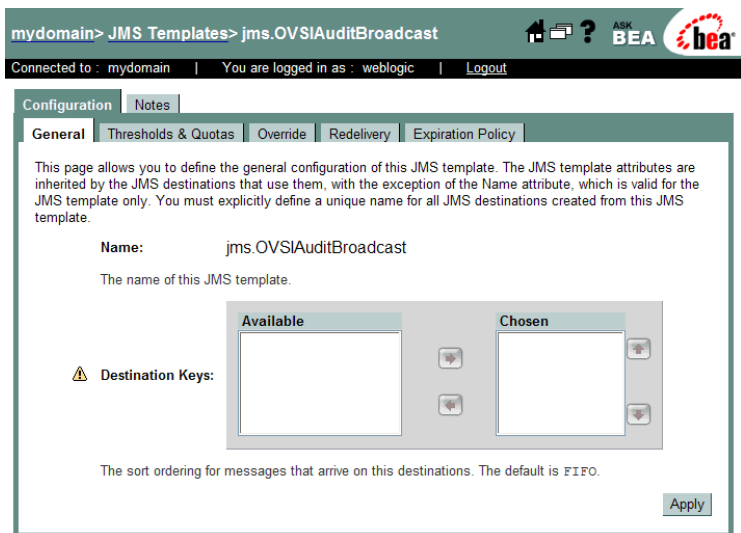
- 10 Click the **Apply** button to commit the changes.
- 11 Repeat this procedure for all JMS Queues and Topics in the Distributed Destinations tree.

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 36 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 True .

- 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 `OVSWorkflowQueue`, 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 37 Configure a JDBC Connection Pool Page

- 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 38 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
Name	Enter a name for the connection pool.
Database Name	Enter the name of the database created on the database server for use by Select Identity. For example, Select_Identity.
Host Name	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.

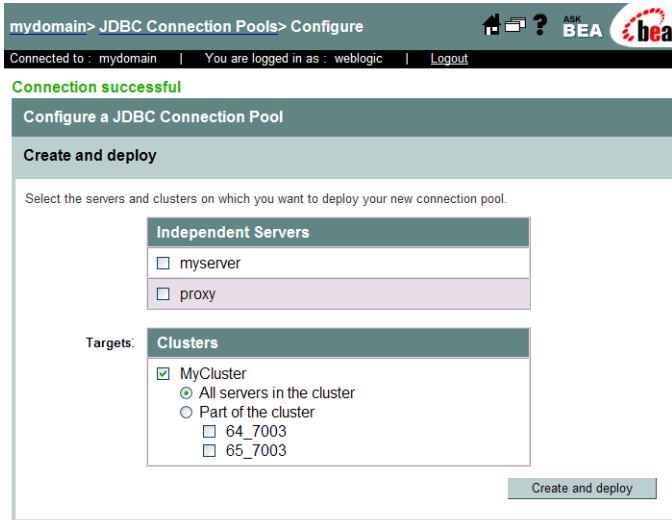
- 8 If you are installing Select Identity with Oracle 9i or 10g, add the following to the **Properties** field. Enter the value on a separate line from any pre-existing content in that field:

```
SetBigStringTryClob=true
```

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

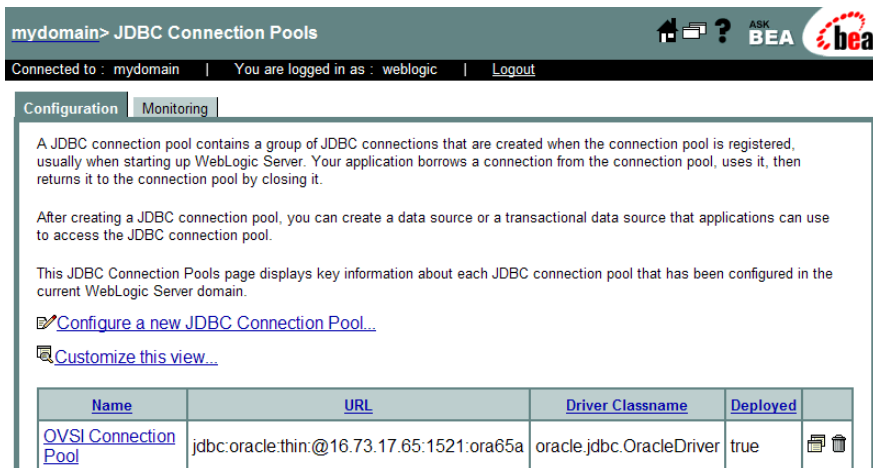
This step verifies that WebLogic can connect to the database. If the connection is successful, the **Configure a JDBC Connection Pool** page opens with a message in the top left corner to indicate that connection was successful.

Figure 39 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 40 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 41 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

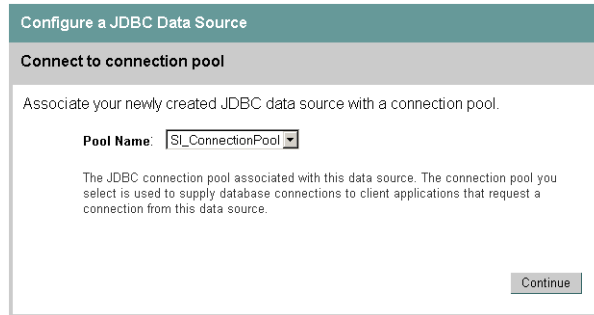
Specifies whether the JDBC resource will emulate participation in a global transaction. This option is only applicable when the associated connection pool uses a non-XA JDBC driver and when global transactions are honored in the data source.

- Enter the following information:

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

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

Figure 42 Connect to Connection Pool Page



- 5 Select the connection pool from the **Pool Name** list box that was created in [Configuring a JDBC Connection Pool](#) on page 64.
- 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 43 Servers Page With Running Servers

mydomain > Servers

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

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	
64_7003	7003	true	RUNNING	
65_7003	7003	true	RUNNING	
myserver	7001	true	RUNNING	
proxy	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
Java Home	<p><BEA_HOME>/jrockit81sp5_142_08 (Linux)</p> <p><BEA_HOME>\JDK142_08\ (Windows)</p> <p>For single servers:</p> <p>You do not need to make this setting.</p>
BEA Home	<p><BEA_HOME></p> <p>The actual path to the WebLogic home directory, for example:</p> <p>/opt/bea</p> <p>For single servers:</p> <p>You do not need to make this setting.</p>

Field	Action
Root Directory	<p data-bbox="511 222 939 248"><BEA_HOME>/common/nodemanager</p> <p data-bbox="511 256 1068 282">The path to the Node Manager for the cluster.</p> <p data-bbox="511 300 725 326">For single servers:</p> <p data-bbox="511 335 961 361">You do not need to make this setting.</p>
Class Path	<p data-bbox="511 395 1260 482">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="511 499 632 526">Windows:</p> <p data-bbox="511 543 1275 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="511 743 589 769">Linux:</p> <p data-bbox="511 786 1253 1003">/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="511 1020 725 1046">For single servers:</p> <p data-bbox="511 1064 1282 1142">You set the class path by editing the myStartWL.sh or myStartWL.cmd script in the WebLogic domain directory where you will be running Select Identity.</p>

Field	Action
Arguments	<pre>-server -Xms256m -Xmx1024m</pre> <p>In Windows, add the argument <code>-XX:MaxPermSize=256M</code></p> <pre>-Dcom.truologica.truaccess.property. file=/<OVSI_INSTALL_DIR>/sysArchive/ TruAccess.properties</pre> <p>On Linux systems only, add the argument</p> <pre>-Djava.awt.headless=true</pre> <p>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>-Djava.util.logging.config.file= <OVSI_INSTALL_DIR>/ sysArchive.myServer1_logging.properties</pre> <p>For single servers:</p> <p>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>

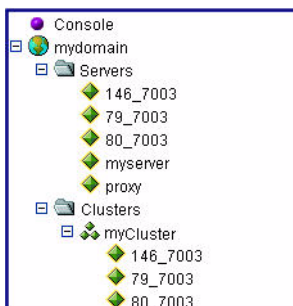
- 6 Click **Apply**.
- 7 On a Weblogic cluster, repeat the process until you have updated each server in the cluster.

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 44 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 45](#).

Figure 45 Execute Queues Configuration Page

mydomain> Servers> 146_7003> Execute Queue

Connected to : 16.73.17.80 :7001 | You are logged in as : system | [Logout](#)

Configuration | Monitoring

Requests to a WebLogic Server instance are placed in an execute queue. Each request is assigned to a thread within the queue that performs the work. By default, a new WebLogic Server instance is configured with a default execute queue, `weblogic.kernel.default`, that contains 15 threads. In addition, WebLogic Server provides two other pre-configured queues: `weblogic.admin.HTTP` and `weblogic.admin.RMI`. Because these queues are reserved for communicating with the Administration Console and for administrative traffic, you cannot reconfigure them. Unless you configure additional execute queues and assign applications to them, Web applications and RMI objects use `weblogic.kernel.default`.

This page displays current runtime characteristics and statistics for the server's active execute queues.

[Configure a new Execute Queue...](#)

[Customize this view...](#)

Name	Queue Length	Thread Priority	Thread Count	
weblogic.kernel.Default	65536	5	5	

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

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

- 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

- When you have completed the fields for each queue, click **Apply**.
- 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:

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

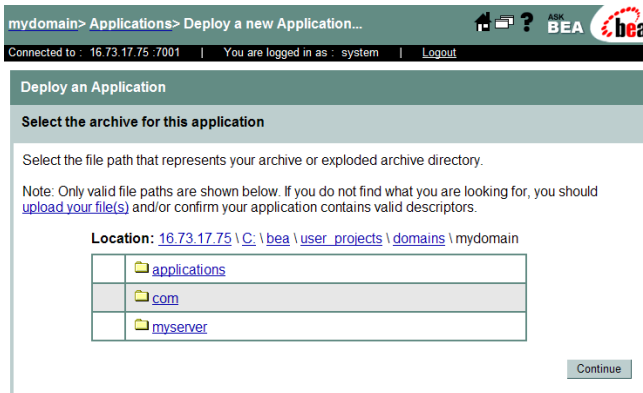
- In the left pane of the console, right-click the cluster and select **Start/ Stop this Cluster**.

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 46 Deploy an Application Page

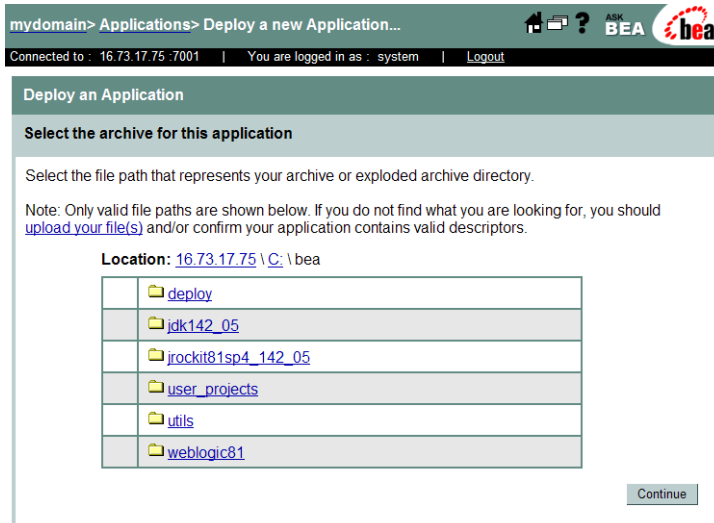


- 4 Locate and select the `1mz.ear` file, which resides in the `<OVSI_INSTALL_DIR>/deploy` directory created in [Creating Select Identity Directories and Copying Installation Files](#) on page 37.

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

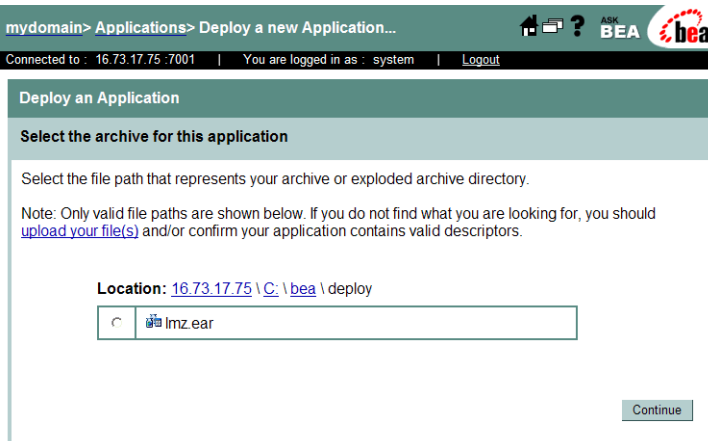
The second **Deploy an Application** page displays with the `bea` subdirectories.

Figure 47 Second Deploy an Application Page



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

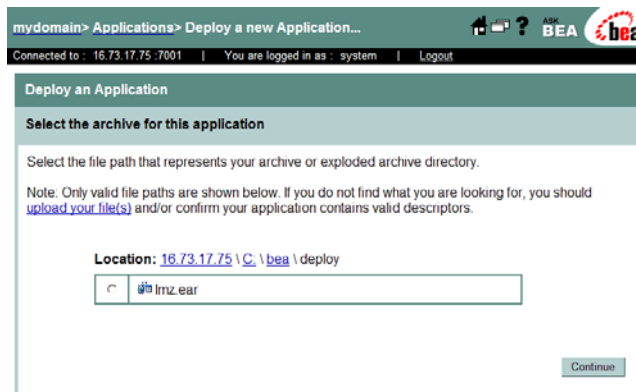
Figure 48 Third Deploy an Application Page



- 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 49 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 50 Deploy Page to Validate Select Identity Deployment

The screenshot shows the BEA WebLogic Administration Console interface. At the top, it indicates the user is logged in as 'system' and the application is 'mydomain> Applications> Imz'. The 'Deploy' tab is selected, showing the deployment status for EJB Modules. Below this, there is a table listing various EJB modules, all of which are in a 'Success' state. At the bottom of the page, there is a section for 'Deployment Status for Web Application Modules' with a table showing the 'Imz' application and 'attribemapper' module, both successfully deployed. Buttons for 'Stop Application' and 'Redeploy Application' are visible at the very bottom.


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
apointEjb.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
systemmgrntEjb.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
provisionconcoerEjb.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
autodiscoveryEjb.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

Module	Target	Target Type	Deployment Status	Status of Last Action
Imz	myCluster	Cluster	Available	Success
attribemapper	myCluster	Cluster	Available	Success


Buttons: 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 43 and [Configuring JMS Settings](#) on page 43.

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 83 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 76 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 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.filedir
```

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 89.
- Optimize Select Identity - see [Recommended Configuration](#) on page 89.
- Use any custom generated keystore in the `TruAccess.properties` file. See [Generating a Custom Keystore](#) on page 85 for details.

For a complete listing and description of all settings in the `TruAccess.properties` file, see [Configuring TruAccess.properties](#) on page 121.

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 113 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.

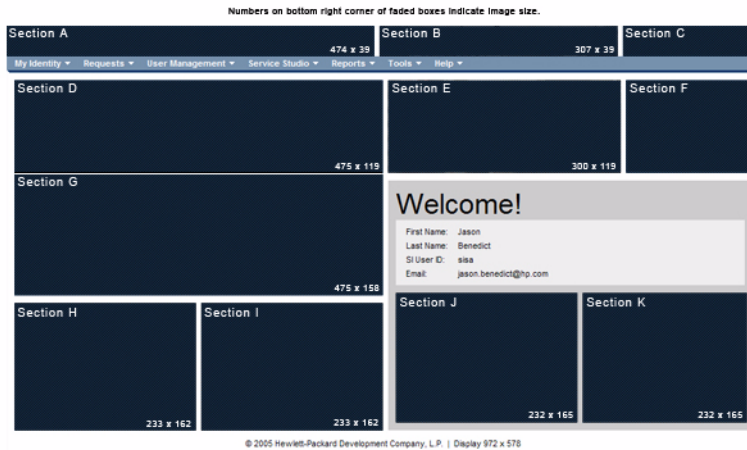
How to Set Properties

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 51](#). The descriptions of the properties that follow use this diagram for reference.

Figure 51 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.

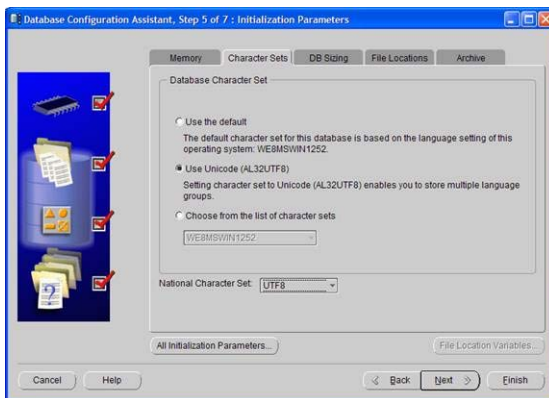
The following sections provide platform and environment-specific configurations.

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

UTF-8 Encoding on Oracle 10G

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

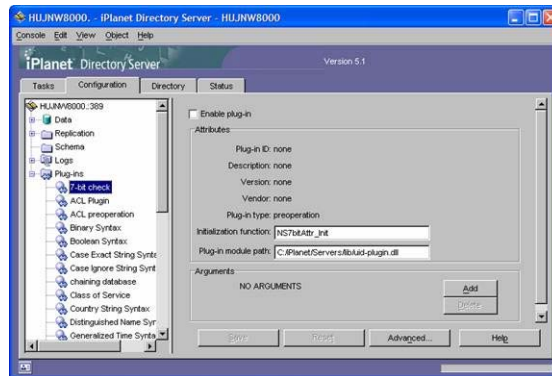
- 1 For Oracle 10g, open the Initialization Parameters window and select the **Character Set** tab.
- 2 Select the **Use Unicode (AL32UTF8)** radio button as shown.



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

6 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 109.
 - 8 Install the new release of Select Identity (4.0) using the manual steps specified in [Select Identity Manual Installation Procedure](#) on page 36.
-  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:

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

If	Then
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.

If the Resource Passwords	Then
Are still in sync	Continue
Are not in sync	Follow the steps to modify the resources and resynchronize the passwords described in Modifying Resources on page 105

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.

7 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 113](#), 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.SMPTimerTask.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 113 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 105 to resynchronize the passwords in the new version.

B Configuring TruAccess.properties

Configure general settings for HP OpenView Select Identity server and interface by editing the `TruAccess.properties` file. This file provides settings for triggers that determine the way that Select Identity operates. Consider each with great care.

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 89.

- **`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=smt

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.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.

- **truaccess.method=http**
truaccess.host=localhost
truaccess.port=7001

Specifies the URL construction to the Select Identity system within email notifications.

- **truaccess.pageredirect.timeout=10**

Specifies the time-out (in seconds) for page redirects.

- **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.

- **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**.

- **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 login URL, and the logout URL for cleaning up the session.

- **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.

- **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.

- **truaccess.provisioning.delay=2**

Specifies the delay (in seconds) for asynchronous provisioning.

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

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

- **truaccess.resource.record.max=1000**

Specifies the maximum number of users updated during reconciliation.

- **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=4.0**

Specifies the version number of OVSI; do not change this value.

- **truaccess.hibernate.config=/com/tru logica/truaccess/util/persistence/mssqlserver.hibernate.cfg.xml**

Specifies the hibernate property file. *Leave this property commented.*

- **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 =S\ Provisioning\ Only
com.hp.ovsi.default.workflowtemplate.delegated.enable service =S\ Provisioning\ Only
com.hp.ovsi.default.workflowtemplate.delegated.moveuser =SIBulkOneStageApproval
com.hp.ovsi.default.workflowtemplate.delegated.viewservice =S\ 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.

- **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 Select Audit

- **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.

- **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=sisa**
truaccess.expire.administrator.adminFunc=Concero Sys Admin

Specifies the default OVSI system administrator user ID and administrative role.

- **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 terminational occurs.

- **personId.attributes=FirstName,LastName**
standardId.attributes=personId,Email
__managerEmailLookup.attributes=Email

Specifies the attributes for external calls.

- **truaccess.policy.id=1**

Specifies the default OVSI policy identifier.

- **truaccess.recon.rootdir=c:/temp/reconroot**
truaccess.recon.stagingdir=c:/temp/reconstaging
truaccess.recon.backupdir=c:/temp/reconbackup
truaccess.recon.filename.timeformat=yyyy_MM_dd_H_mm
truaccess.recontimer.startdelay=30
truaccess.recontimer.timeinterval=30
truaccess.recon.task.check.threshold=3
truaccess.recon.check_serviceassignment_authadd=false

Specifies the attributes for account reconciliation.

- **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
- **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
- **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.
- **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.

- **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.needsssl=false

Specifies external authentication for Web Service requests when uncommented

- **com.hp.ovsi.default.notification.approve=Add\ User**
- The default email template for Approve Notification Event
- **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.i18n.labels.debug = false**

Debug resource bundle strings

- **com.hp.ovsi.help.web = http://support.hp.com**

URL for external web help

- **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.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.default.notification.approve=Add\ User**

The default email template for Approve Notification Event

- **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.

- **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.

- **si.rsa.provider=org.bouncycastle.jce.provider.BouncyCastle Provider**

Specifies the provider of the key store parameters. *Do not modify this setting.*

- **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 should end with a period (.).

- **com.hp.si.selfreg.schedule=true**

Specifies whether the “schedule time” field in the self-registration form will be visible.

- **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.

- **truaccess.user.extra=PhBus, PhHome, PhMobile, Company,Department, DOB, Addr1, Addr2, City, State, Zip, Country, CostCenter, ExpirationDate, UserDescription, _Status**

Extra attributes associated with the users. These following fields support null values truaccess.user.extra=PhBus, PhHome, PhMobile, Company,Department, DOB, Addr.

- **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

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

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

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

Determines additional user search criteria fields.

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

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

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

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

- **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.

- **com.hp.si.locales=en,en_US,zh_CN,ko**

Supported locales (US English is default).

- **server.manager.enable=true**

Allows you to set the server management properties when set to the default (true).

- **ovsi.ad.emailCC=your.email@yourdomain.com**

Specifies the email address pattern used by OVSI to validate email addresses.

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

Determines the connector schema directory.

- **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 questions. If set to false, the user must reset their own password.

- **truaccess.batch.report.file.maxsize = 1000000**

Specifies the maximum email size of a batch report.

- **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.

- **com.hp.si.request.report.day=14**

Specifies the last `n` 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.

- **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.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.

- **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.email.attachment.size=500**

Defines the maximum size of an email attachment if component limit size option is on (hidden default set to 500K).

- **si.volumedata.report.email.limitsize=true**

Indicates whether or not report size should be limited (hidden, default set to true, limit the report).

- **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 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
- **si.autodiscovery.audit=false (hidden, default to false)**
Whether to audit user import
- **si.serviceassignment.batchsize=xx (hidden, default to 20)**
Number of users to process in one JMS message
- **si.serviceassignment.server.num = X**
Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.
- **si.recon.webservice.report.generate=2**
Whether to generate and send report for Web Service recon. 0 - Never, 1 - Only Initial Report when no request is processed, 2 - always
- **si.recon.policybased=true (hidden, default to true)**
Policy Based Recon Switch
- **si.recon.server.num = X**
Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.
- **si.recon.processor.num = X**
Hidden, default set to 8.

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 'XXXXXXXXXX';
 - 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.<Attribute Name>.column=<Column Name>**), the attribute name is assumed to be the column name

Glossary

A

Access Control List (ACL)

An abstraction that organizes entitlements and controls authorization. An ACL is list of entitlements and users that is associated with a secured object, such as a file, an operation, or an application. In an ACL-based security system, protected objects carry their protection settings in the form of an ACL.

Access Management

The process of authentication and authorization.

Action

A task that can be performed within each Select Identity capability.

In Workflow Studio, an action invokes functions provided by the workflow engine or external applications within an activity. For example, you can log information to a file, set a property to be used later in the workflow, call an external process, provision a user in Select Identity, or store data in a database.

See also: [Capability](#)

Activity

A task that may occur when a workflow template is executed (in Workflow Studio). Activities are the core components of workflow templates; they do the work necessary to provision users. An activity can set a property to be used throughout the workflow, track approvals, start a subworkflow, send email, call an external application, and so on.

AD Connector

Active Directory Connector.

Admin Role

A template that defines the administrative actions that can be performed by a user. An Administrative Service is created to provide access to roles. Users are then given access to the Service. Users with administrative roles can also grant their set of roles to another administrator within their Service context.

Approval Process

The process of approving the association, modification, or revocation of entitlements for an identity. This process is automated of these through workflow templates.

Approver

A Select Identity administrator who has been given approval actions through an Admin Role.

Attribute

An individual field that helps define an identity profile. For each identity, an attribute has a corresponding value. For example, an attribute could be “department” with possible values of “IT,” “sales,” or “support.”

API

Application Program Interface. A set of routines, protocols, and tools used to build a software application.

Audit Report

A report that provides regular account interaction information within the Select Identity system.

Authentication

Verification of an identity’s credentials.

Authoritative Source

A resource that has been designated as the “authority” for identity information. Select Identity accounts can be reconciled against accounts in an authoritative source.

Authorization

Real-time enforcement of an identity's entitlements. Authentication is a prerequisite for authorization.

B

Block

A special type of activity that serves two purposes: to define information to be used by a subset of activities (block-level properties) and to provide block-level reporting. For example, you might define a block that submits an approval request, waits for the response, and returns the status of the request to the workflow. In other words, think of a block as a process within a template.

Block Type

A property that is assigned to a block in a workflow template using the `blockType` property in end block activity. The report template uses this property to identify how block information is rendered in the resulting report.

Business Service

A product or facility offered by, or a core process used by, a business in support of its day-to-day operations. Example business services could include an online banking service, the customer support process, and IT infrastructure services such as email, calendaring, and network access.

See also: [Service](#)

C

Capability

Actions that can be performed within the Select Identity client are grouped by capability, or link, in the interface.

See also: [Action](#)

Challenge and Response

A method of supplying alternate authentication credentials, typically used when a password is forgotten. Select Identity challenges the end user with a question and the user must provide a correct response. If the user answers the question correctly, Select Identity resets the password to a random value and sends email to the user. The challenge question can be configured by the

administrator. The valid response is stored for each user with the user's profile and can be updated by an authenticated user through the Self Service pages.

Configurations

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

Configuration Report

A report that provides current system information for user, administrator, and Service management activities.

Connector

A J2EE connector that communicates with the system resources that contain your identity profile information.

Context

A Select Identity concept that defines a logical grouping of users that can access a Service.

Contextual Identity Management (CIM)

An organizational model that introduces new abstractions that simplify and provide scale to the business processes associated with identity management. These abstractions are modeled after elements that exist in businesses today and include Select Identity Services and Service Roles.

Credential

A mechanism or device used to verify the authenticity of an identity. For example, a user ID and password, biometrics, and digital certificates are considered credentials.

D

Data File

An SPML file that enables you to define user accounts to be added to Select Identity through user import, or reconciliation.

Delegated Administration

The ability to securely assign a subset of administrative roles to one or more users for administrative management and distribution of workload. Select Identity enables role delegation through the Self Service pages from one administrator to another user within the same Service context.

Delegated Registration

Registration performed by an administrator on behalf of an end user.

See also: [Self Registration](#)

E

End User

A role associated to every user in the Select Identity system that enables access to the Self Service pages.

Entitlement

An abstraction of the resource privileges granted to an identity. Entitlements are resource-specific and can be resource account IDs, resource role memberships, resource group memberships, and resource access rights and privileges. Entitlements are also considered privileges, permissions, or access rights.

Expression

A combination of workflow variables and constant values to be evaluated. An expression can be assigned to a new variable or passed to an application as an argument. If you are familiar with a programming language, an expression used in a workflow template is like C or Java expression. Example of expressions can be found in action input parameters, application return values, and transition conditions.

External Call

A programmatic call to a third-party application or system for the purpose of validating accounts or constraining attribute values.

F

Form

An electronic document used to capture information from end users. Forms are used by Select Identity in many business processes for information capture and system operation.

I

Identity

The set of authentication credentials, profile information, and entitlements for a single user or system entity. Identity is often used as a synonym for “user,” although an identity can represent a system and not necessarily a person.

Identity Management

The set of processes and technologies involved in creating, modifying, deleting, organizing, and auditing identities.

Instance

See: [Workflow Instance](#)

J

JAVA

Object oriented programming language.

JCA

Java Connection Architecture. Architecture used to build interfaces between J2EE compliant products and other resources.

JVM

Java Virtual Machine. A platform independent execution environment that converts Java bytecode into machine language then executes it.

L

LDIF

File that modifies and deletes directory objects.

M

Management

The ongoing maintenance of an object or set of objects, including creating, modifying, deleting, organizing, auditing, and reporting.

N

Notifications

The capability that enables you to create and manage templates that define the messages that are sent when a system event occurs.

P

Password Reset

The ability to set a password to a system-generated value. Select Identity uses a challenge and response method to authenticate the user and then allow the user to reset or change a password.

Persistent Variable

A variable that is persisted after an instance is passivated. To extend the variable life cycle to the entire instance, you must create the variable to be persistent. This enables the variable to be created before a wait activity, and it will be accessible after the workflow instance resumes. To make a variable persistent, precede the name with \$. For example, the \$retryCount variable is persistent while retryCount is not.

See also: [Workflow Variable](#)

Policy

A set of regulations set by an organization to assist in managing some aspect of its business. For example, policy may determine the type of internal and external information resources that employees can access.

Process

A repeatable procedure used to perform a set of tasks or achieve some objective. Whether manual or automated, all processes require input and generate output. A process can be as simple as a single task or as complicated a multi-step, conditional procedure.

See also: [Approval Process](#)

Profile

Descriptive attributes associated with an identity, such as name, address, title, company, or cost center.

Property

See: [Workflow Property](#)

Provisioning

The process of assigning authentication credentials to identities.

R

Reconciliation

The process by which Select Identity accounts are synchronized with a system resource. Accounts can be added to the Select Identity system through the use of an SPML data file.

Registration

The process of requesting access to one or more resources. Registration is generally performed by an end user seeking resource access, or by an administrator registering a user on a user's behalf.

See also: [Delegated Registration](#), [Self Registration](#)

Request

An event within the Select Identity system for the addition, modification, or removal of a user account. Requests are monitored through the Request Status capability.

Resource

Any single application or information repository. Resources typically include applications, directories, and databases that store identity information.

Role

A simple abstraction that associates entitlements with identities. A role is an aggregation of entitlements and users, typically organized by job function.

See also: [Admin Role](#)

Rule

A programmatic control over system behavior. Rules in Select Identity are typically used for programmatic assignment of Services. Rules can also be used to detect changes in system resources.

S

Self Registration

Registration performed by an end user seeking access to one or more resources.

See also: [Delegated Registration](#)

Self Service

The ability to securely allow end users to manage aspects of a system on their own behalf. Select Identity provides the following self-service capabilities: registration, profile management, and password management (including password change, reset, and synchronization).

Service

A business-centric abstraction representing resources, entitlements, and other identity-related entities. Services represent the products and services that you offer to customers and partners.

Service Attribute

A set of attributes and values that are available for or required by a Service. Attributes are created and managed through the Attributes pages.

See also: [Attribute](#)

Service Role

A Select Identity abstraction that defines how a logical grouping of users will access a Select Identity Service. The Select Identity Service is a superset of all the identity management elements of a business service.

Service View

A restricted view of a Service that is valid for a group of users. Views enable you to define a subset of Service registration fields, change field names, reorder fields, and mask field values for specific users.

Single Sign-On (SSO)

A session/authentication process that permits a user to enter one set of credentials (name and password) in order to access multiple applications. A Web SSO is a specialized SSO system for web applications.

SPML Data File

See: [Data File](#)

T

Template

See: [Workflow Template](#)

Transition

The definition of a relationship between activities. You can define that one activity always follows another, or you can define a condition that must be met before the workflow transitions from an activity to one or more others. For example, you can define a transition that only allows the workflow to progress if at least two administrators approve a request. If the request is not approved, the workflow can transition to an activity that sends email notification to an administrator.

U

User Import

The process of adding user accounts to the Select Identity system for a specified Service through the use of a data file.

Users

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

V

Variable

See: [Workflow Variable](#)

Variable Expression

See: [Expression](#)

W

Workflow Engine

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

Workflow Instance

An invocation of a workflow template. An instance starts when it is created and ends when it completes (when the last activity is executed). An instance's status and other associated information can be viewed once an instance is created.

Workflow Process

The tasks, procedural steps, organizations or people involved, and required input and output information needed for each step in a business process. In identity management, the most common workflows are for provisioning and approval processes.

Workflow Property

A name-value pair, where the value is a text string. A property stores static data that cannot be changed at runtime. It can be accessed by the workflow API and report template. There are three levels of properties: global, block, and activity.

Workflow Studio

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

Workflow Template

A model of the provisioning process that enables Select Identity to automate the actions that approvers and systems management software must perform.

Workflow Variable

A name-value pair that can be created or changed at runtime in a workflow instance through actions, a workflow API call, or returned by an application invocation. It can be accessed by workflow API, workflow template, and report template. There are levels of variables: global, block, and activity.

See also: [Persistent Variable](#)

Index

A

- attribute mapping
 - search, **133**
 - update TruAccess.properties for search, **134**
- attributes
 - search for, **133**
- auditing, **5**

C

- clustered servers
 - create JMS connection factory, **44**
- configure
 - JDBC connection pool, **64**
 - JMS settings, **43**
 - JTA settings, **80**
- configuring
 - logging, **113**
 - recommended, **89**
 - TruAccess.properties, **83, 121**
 - TruAccess.properties required settings, **83**
- connectors, **5**
- context management, **4**

D

- database server
 - configuring Oracle, **15**
- database server requirements, **10**

documentation, *v*

E

- Emailed report format, **98**

F

- features, **2**
- firewall configuration, **13**
- forms, **5**
- functional components, **4**

G

- general settings, **83**
- generating
 - generate the keystore, **85**

I

- interface requirements, **13**
- interface settings, **83**
- Internationalization, **6**
- internationalization, **94**
 - UTF-8 encoding on Oracle10G, **95**

J

- JDBC connection pool, configure, **64**
- JMS connection factory
 - create for clustered servers, **44**

JMS Queue
 create for a single server, **51, 58**

JMS settings
 configure, **43**

JMS settings for a single server
 create JMS Queue, **51, 58**

JMS settings for clustered servers
 set up JMS connection factory, **44**

JTA settings
 configure, **80**

K

keystore, **5, 85**

L

language fonts, **96**

localization, **94**

log files, **113**

logging.properties
 configuring, **36, 80**

login page, **97**

M

migration, **101**

O

online help, **vi**

Oracle
 internationalization encoding, **95**

Oracle requirements, **11**

R

reconciliation, **4**

reporting, **5**

requirements
 Oracle, **11**
 WebLogic, **12**

resource management, **4**

S

search for attributes, **133**

security, **5**
 keystore, **5**

Select Identity
 configurations supported on, **10**
 system requirements, **9**

Self-Registration, **97**

server settings, **83**

service management, **4**

service roles, **4**

Starting WebLogic, **41**

system architecture, **3**

system errors
 WebLogic, **119**

system errors on WebLogic, **117**

system requirements, **9**
 database server, **10, 11, 12**
 firewall, **13**
 interface, **13**
 web application server, **12**

T

TAUser database table, **134**

TCP/IP ports, **13**

tiered authority, **5**

troubleshooting, **117**

TruAccess.properties, **83, 121**
 attribute mapping search settings, **134**
 configuring, **121**
 configuring required settings, **83**
 settings, **121**

U

uninstalling, **110**
upgrade Select Identity, **101**
user management, **4**
User Search criteria, **98**
user searches, **133**
UTF-8 encoding, **96**

V

virtual user ID, **3**

W

web application server requirements, **12**
WebLogic install, **25**
 manual install, **36**
WebLogic requirements, **12**
welcome, **1**
workflow management, **4**

