HP OpenView Select Identity

Software Version: 4.12

Installation Guide

Document Release Date: March 2007

Software Release Date: March 2007

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

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

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils.
- Commons-collections.
- Commons-logging.
- Commons-digester.
- Commons-httpclient.
- Element Construction Set (ecs).
- Jakarta-poi.
- Jakarta-regexp.
- Logging Services (log4j).

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge.
- iText (for JasperReports) developed by SourceForge.
- BeanShell.
- Xalan from the Apache XML Project.
- Xerces from the Apache XML Project.
- Java API for XML Processing from the Apache XML Project.

- SOAP developed by the Apache Software Foundation.
- JavaMail from SUN Reference Implementation.
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation.
- Java Cryptography Extension (JCE) from SUN Reference Implementation.
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation.
- OpenSPML Toolkit from OpenSPML.org.
- JGraph developed by JGraph.
- Hibernate from Hibernate.org.
- BouncyCastle engine for keystore management, bouncycastle.org.

Trademark Notices

UNIX® is a registered trademark of The Open Group.

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

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

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

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

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

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

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

Support

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

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

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

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

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

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

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

This section covers the following topics:

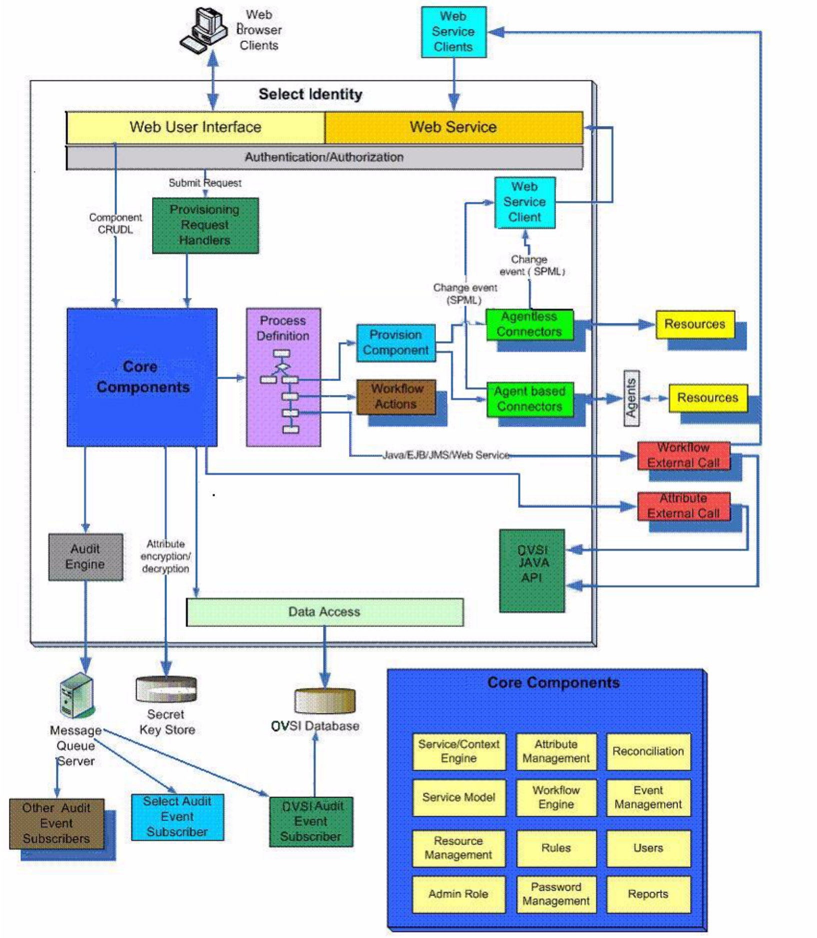
- System Architecture
- Security and Communication
- Connectors
- Internationalization
- Technical Qualifications for Installing Select Identity

System Architecture

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

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

Figure 1 HP OpenView Select Identity Architecture



The Context Engine and Identity Business Process Services components of the Select Identity architecture are of particular importance to administrators and personnel responsible for deploying and maintaining the Select Identity system. These components contain the functions that administrators use most. These functions include the following:

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

Function	Description
Workflow Studio	Enables the definition of identity-related business processes that can be executed for access to services or any other event within the Select Identity system.
Reconciliation	Ensures the proper coordination of provisioning workflow across multiple resources.
Auditing and Reporting	Provides robust standard and custom reporting facilities over user entitlements and system event history.
Forms	Automates the creation of electronic forms used by end users to register for access to services, change their passwords, set password hints, and update personal information.
Tiered Authority	Enables the secure, multi-tiered delegation of administrative tasks, such as management of identity profiles and entitlements, to functional departments, customers, and partners.

Security and Communication

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

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

Keystores

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

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

By generating the keystore, you add security to data exchange in Select Identity. See Setting Up the Select Identity Keystores on page 110 for details.

Integration

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

Connectors

Leveraging an open, standard, J2EE Connector Architecture (JCA) bus, Select Identity uses predefined connectors to access back-end system data stores. Connectors are configured during the installation process and are easy to deploy. Select Identity offers a software developer's kit (SDK) to support custom connector development.

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

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

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

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

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

Internationalization

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

For more information about the internationalized Select Identity, see Internationalization and Localization on page 119.

Technical Qualifications for Installing Select Identity

Select Identity installation is a lengthy process that requires a strong technical background. You must have the following qualifications or knowledge:

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

- Database administration skills
- Installation and administration training on your Web application server
- General familiarity with background technology such as HTTP and JCA
- Overall familiarity with Select Identity product architecture in the context of the Web application server environment.

2 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 Requirements
- Supported Configurations
- Database Server Requirements
- BEA WebLogic Server Requirements
- IBM WebSphere Server Requirements
- Select Identity Interface Requirements
- Ports Required for Firewall Configuration

Installation Process Overview

The following is an overview of the complete installation process:

1. Review the requirements and recommendations in this chapter.
2. Configure the Web application server for use with Select Identity, as documented in Prerequisite Configuration on page 31.
3. Configure the database and load the Select Identity schema.
4. If installing on a cluster, configure a shared Network File System folder where Select Identity will be installed.
5. Set up the Select Identity security framework before installing Select Identity, as documented in Chapter 6, Configuring Select Identity.
6. Ensure that you have the correct policy files, as documented in the installation section for your Web application server.
7. Install Select Identity, as documented in Chapter 4, Installing Select Identity on IBM WebSphere 6.0.2.
8. If you are installing a localized version of Select Identity using the Select Identity language media kit, mount the Language Media CD, locate the documentation, and follow the instructions on how to deploy specific languages.
9. Configure the `TruAccess.properties` file for your environment, using the information provided in Chapter 6, Configuring Select Identity and in Appendix A, TruAccess Properties.

10 Install and configure the connectors that will be used with your system. Refer to the *Connector Installation Guides* supplied with your connectors for instructions.

Reviewing Minimum Requirements

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

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

Supported Configurations

Select Identity release 4.12 is supported on the following configurations:

Web Application Server	**Platform**	**Database**
BEA WebLogic Server 8.1.5	Red Hat Enterprise Linux AS 3.0	Oracle 10.2.0.2.0 Oracle 9i
BEA WebLogic Server 8.1.5	Windows Server 2003 Enterprise SP1 32-bit	MS-SQL 2000 SP4 Oracle 10.2.0.2.0 Oracle 9i
BEA WebLogic Server 8.1.5	HP-UX 11.23 Itanium	Oracle 10.2.0.2.0
BEA WebLogic Server 8.1.5	Sun Solaris 10 SPARC	Oracle 9i
IBM WebSphere and IBM WebSphere - ND Version 6.0.2.15	SP1 32-bit	MS-SQL 2000 SP4 Oracle 10.2.0.2.0
IBM WebSphere and IBM WebSphere - ND Version 6.0.2.15	HP-UX 11i (v1) PA-RISC	Oracle 10.2.0.2.0
IBM WebSphere and IBM WebSphere - ND Version 6.0.2.15	Red Hat Enterprise Linux v3	Oracle 10.2.0.2.0

Database Server Requirements

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

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

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

Oracle 10G

Operating System	• Red Hat Enterprise Linux v3 • Windows Server 2003, Standard Edition, SP1 32-bit • Windows Server 2003, Enterprise Edition, SP1 32-bit • Windows Server 2003, DataCenter Edition, SP1 32-bit • HP-UX 11.23 Itanium • HP-UX 11i (v1) PA-RISC
Processor	Minimum processor speed: 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 10.2.0.2.0 (`oracle.jdbc.OracleDriver`)

Oracle 9i

Operating system	• Windows Server 2003, Standard Edition, SP1 32-bit • Windows Server 2003, Enterprise Edition, SP1 32-bit • Windows Server 2003, DataCenter Edition, SP1 32-bit • Sun Solaris 10 SPARC
Processor	Minimum processor speed: 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 Server 2000 Service Pack 4, Enterprise Edition

Operating system	• Windows Server 2003, Standard Edition, SP1 32-bit • Windows Server 2003, Enterprise Edition, SP1 32-bit • Windows Server 2003, DataCenter Edition, SP1 32-bit
Processor	Intel Pentium or compatible, minimum speed 166 MHz
Memory (RAM)	Enterprise Edition: 512MB RAM; 1024MB recommended
Disk space	95 - 270 MB available hard disk space for the server; 250 MB for a typical installation
JDBC driver	*For WebLogic 8.1:* BEA MS SQL Server Type 4 driver, class name: `weblogic.jdbc.sqlserver.SQLServerDriver` *For WebSphere 6.0.2:* WebSphere embedded ConnectJDBC driver for MS SQL Server(XA), class name: `com.ibm.websphere.jdbcx.sqlserver.SQLServerDataSource`

Unicode Encoding

Select Identity is only supported on a database with UTF-8 encoding. Other forms such as UTF-16, UCS2, and UCS4 are not supported.

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.

Operating System	• Red Hat Enterprise Linux v3 • HP-UX 11i (v1) PA-RISC • HP-UX 11.23 Itanium • Sun Solaris 10 SPARC
Processor	Minimum processor speed: 1 GHz
Memory (RAM)	512 MB (minimum)1 GB (recommended)
Disk space	Approximately 820MB

IBM WebSphere Server Requirements

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

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

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

Operating System	Red Hat Enterprise Linux v3 Windows Server 2003 Enterprise SP1 32-bit HP-UX 11i PA-RISC
Processor	Minimum processor speed: 1 GHz
Memory (RAM)	768 MB RAM (minimum) 1 GB RAM (recommended)
Disk space	Approximately 820MB

Select Identity Interface Requirements

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

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

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

Ports Required for Firewall Configuration

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

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

- 9001 for WebSphere
- 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 use port 23 (Telnet) or 22 (SSH).

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

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

3 Database Server Configuration

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

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

➤ Internationalized character support reduces the maximum allowable number of characters in Select Identity character fields.

When using non-ASCII character support with internationalized versions of Select Identity, the character length limit on all character fields is one-third of the numerical limit for ASCII characters. This is because non-ASCII character sets such as those used in Japanese or Chinese require three bytes per character as opposed to one byte for ASCII.

This chapter contains the following topics:

- Configuring an Oracle Database Server
- Configuring an MS SQL Database Server

Configuring an Oracle Database Server

Create an Oracle database for use by Select Identity by running SQL scripts.

To create the database and load the Select Identity schema on an Oracle server, complete the following steps:

1 Create a directory on the server that will serve as the Select Identity database home directory.

Do not put spaces into the directory name.

2 Copy the following files from the database home directory on the Select Identity CD to the database home directory:

```
oracle_concero_ddl.sql
```

```
oracle_concero_dml.sql
```

3 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 the operating sysem command line.

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

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

```
CREATE TABLESPACE <tablespace_name>

DATAFILE '<install_dir>/oracle/oradata/<ORACLE_SID>/
<tablespace_name>.dbf'

SIZE 100M (or greater) AUTOEXTEND ON NEXT 50M (or greater)

MAXSIZE unlimited;
```

This example creates 100MB of tablespace then automatically extends it as needed. The `<tablespace_name>` is your chosen name for the Select Identity tablespace. You reference this name when you create the database user in step 5.

5. Create a user account for Select Identity to access the tables, as shown in the following example for Oracle 9i (see the information below for additional information about Oracle 10G):

```
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>;
```

Where:

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

The `oracle_concero_ddl.sql` script, in step 8, 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.

For Oracle 10g Release 2, the following permissions must also be set:

```
GRANT CONNECT TO user_name;

GRANT RESOURCE TO user_name;

GRANT CREATE TABLE TO user_name;

GRANT CREATE VIEW TO user_name;

GRANT CREATE SEQUENCE TO user_name;

GRANT CREATE PROCEDURE TO user_name;
```

6. If you are running Select Identity on IBM WebSphere 6.0.2, repeat step 5, to create an additional user account that the Java Messaging Service (JMS) will use to access the Select Identity database. You can also repeat step 4 first to create a separate tablespace for the JMS user account. You do not need to perform this step for BEA WebLogic systems.

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

7. If running Select Identity on IBM WebSphere 6.0.2, change to the first user account you created, by entering the following command:

   ```
   CONNECT user_name/password
   ```

8. Regardless of the Web application server, create the schema for the Select Identity database, as follows:

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

   b. Execute the copied script by running the following:

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

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

   c. Verify that no error message results.

9. Insert the required default data into the Select Identity database:

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

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

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

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

   c. Verify that no error message results.

⚠ Ensure that the **truaccess.email.batchcount** setting is less than 1000 on an Oracle-based system. The default for this setting is 50. See Appendix A, TruAccess Properties.

After you have installed Select Identity, check and modify database and other settings in the `TruAccess.properties` file, which is installed with Select Identity. Refer to Appendix A, TruAccess Properties for more information.

Configuring an MS SQL Database Server

Create an MS-SQL 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 an MS-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 following files from the database directory on the Select Identity CD to the Select Identity database home directory on the SQL Server system:

   ```
   mssql_concero_ddl.sql
   ```

   ```
   mssql_concero_dml.sql
   ```

3. Log in to the Microsoft SQL Server Enterprise Manager interface.

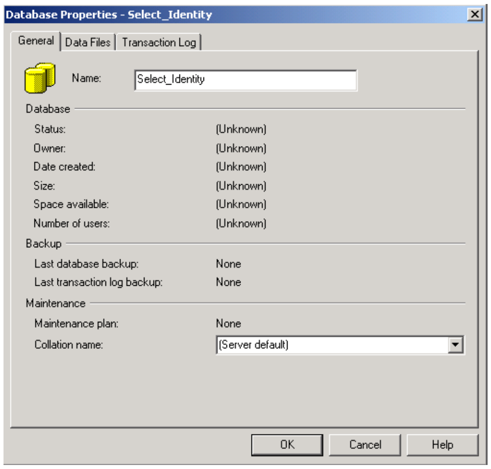
4. In Enterprise Manager, expand **Microsoft SQL Server** → **Tools** → **SQL Server Configuration Properties** → **Processor**.

5. Change the setting for **Max. Worker Threads** to `700`.

6 In Enterprise Manager, expand **Microsoft SQL Server** → **SQL Server Group** → **server**, where server is the name of the SQL Server instance.

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

Figure 2 Database Properties



Name: Select_Identity

Database

Status: (Unknown)
Owner: (Unknown)
Date created: (Unknown)
Size: (Unknown)
Space available: (Unknown)
Number of users: (Unknown)

Backup

Last database backup: None
Last transaction log backup: None

Maintenance

Maintenance plan: None
Collation name: (Server default)

8 Enter a name for the database, such as `Select_Identity`.

9 Click **OK** to finish creating the database.

10 Create a user account to manage the Select Identity database by completing the following steps:

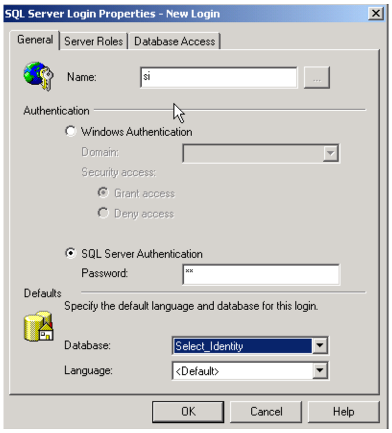
a Select the **Microsoft SQL Server** → **SQL Server Group** → **server** → **Security folder** in the Enterprise Manager tree.

b Create a new login for the new database by right-clicking **Logins** and selecting **New Login.**

The SQL Server **Login Properties** dialog opens.

11 If installing on IBM WebSphere, create a second database user account that will be used by the Java Messaging Service (JMS).

Figure 3 SQL Server Login Properties



Name: si

Authentication

○ Windows Authentication
Domain:
Security access:
● Grant access
○ Deny access

● SQL Server Authentication
Password: **

Defaults

Specify the default language and database for this login.

Database: Select_Identity
Language: <Default>

c On the **General** tab, enter a user name such as SI, enter a password, and select **SQL Server Authentication** as the authentication type.

d Select the new database (Select_Identity) from the **Database** list. Keep the remaining default settings.

e Click **OK**.

f Confirm your password when prompted.

g Click the **Database Access** tab.

h Check the **Permit** box next to the Select Identity database user.

i Assign the `db_owner` and `public` permissions to the new user.

j Click **OK** to save your settings.

12 Create the Select Identity database schema by performing the following steps:

a Launch the SQL Query Analyzer by selecting T**ools** → **SQL Query Analyzer**.

b Select the new database (SI) from the **Database** list.

13 Load the `mssql_concero_ddl.sql` script from the Select Identity database home directory you created in step 2 on page 27:

a Click the **Open** icon. Locate the Select Identity home directory.

b Select the `mssql_concero_ddl.sql` file.

c Click **Open**.

d Run the script by clicking the **Execute Script** or **Play** button.

e Verify that no error message is displayed.

14 Insert the required default data into the Select Identity database by performing the following steps:

f Clear the previous script by clicking the **Clear Query Window** button.

g Load the `mssql_concero_dml.sql` script from the directory you created in step 2 on page 27.

h Click the **Execute Script** button.

i Messages in the console indicate that rows are being created.

j Verify that no error message is displayed.

k Close the SQL Query Analyzer and the Microsoft SQL Server Enterprise Manager.

After you have installed Select Identity, check and modify database and other settings in the `TruAccess.properties` file, which is installed with Select Identity. Refer to Appendix A, TruAccess Properties for more information.

Ensure that the following TruAccess property is set as follows:

```
hp.si.idgen.increment=200
```

This property controls the size of reserved Select Identity-generated database table row IDs on each server. For MS SQL Server, a setting of 200 is recommended to enable the database to manage concurrent processing and locking as efficiently as possible.

4 Installing Select Identity on IBM WebSphere 6.0.2

This chapter describes how to install Select Identity on an IBM WebSphere 6.0.2 application server, with either MS-SQL 2000 or Oracle 10G.

This chapter includes the following topics:

- Important Installation Information
- Prerequisite Configuration
- Using the Select Identity Installer
- Manual Installation Procedures
- Logging In to Select Identity on IBM WebSphere

Introduction

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

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

Prerequisite Configuration

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

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

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

Prerequisites for All Installations

The following prerequisites must be complete on all WebSphere installations:

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

- The proxy server is configured.
- WebSphere is installed on a system that meets the requirements listed in Chapter 2, Requirements.
- Security is enabled for the WebSphere admin console.
- The `HAManagerService` must be enabled in WebSphere. This is enabled by default and can be verified by viewing the `hamanagerservice.xml` config files in your WebSphere home directory.
- Your Select Identity database server is configured as documented in Chapter 3, Database Server Configuration.
- Two new user accounts have been created on the database (one for Select Identity and one for JMS), and the Select Identity database schema has been loaded, as documented in Configuring an Oracle Database Server on page 25, or in Configuring an MS SQL Database Server on page 27.
- The security framework has been set up, using the instructions in Setting Up the Select Identity Keystores on page 110.

Prerequisites Specific to Cluster Installations

On a cluster, additional prerequisites are as follows:

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

Installation to Directories with Embedded Spaces

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

Preparing to Install Select Identity

To prepare WebSphere for installation, complete the following steps:

1. Upgrade the policy files on the WebSphere application server to“unlimited strength” policy files, by downloading the following files from IBM’s Web site (if you are installing on HP-UX, you must obtain these policy files from Sun Microsystems’ Web site):

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

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

2. Copy the policy files from step 1 to `%WAS_HOME%/java/jre/lib/security.`

3 If using Oracle, download the Oracle thin driver `ojdbc14.jar` to the machine running the installer. The installer prompts for the path to this file.

> The Oracle 10G driver is required.

4 On a cluster, configure the network file system for the installation directory.

5 For easier access to documentation, copy the product documentation PDF files from the `/docs` directory on the HP OpenView Select Identity product CD, to a directory of your choice on the application server.

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

- Ensure that your Select Identity database server is configured as documented in Chapter 3, Database Server Configuration.

6 Configure the custom external keystores and encryption keys, as described in Setting Up the Select Identity Keystores on page 110.

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

7 On a standalone installation, start the WebSphere Application Server. On a cluster, start the Deployment Manager and all node agents in the cluster.

8 If using the installer process, tail the following log files before starting the installer and monitor the output closely during installation:

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

Important Installation Information

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

For all WebSphere 6.0.2 Configurations:

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

- The SMTP email host to be used by Select Identity.
- The database server host name and IP address.
- The operating system login ID used when installing WebSphere.
- The login ID and password for the Select Identity and JMS database user accounts created in Chapter 3, Database Server Configuration.
- The IP address and host name of the WebSphere admin server.
- The login ID and password for the user account with which WebSphere was installed.
- The directory location of the keystore parameter file. See Setting Up the Select Identity Keystores on page 110.
- The location of the Oracle thin driver Java archive file, if applicable.

For Clusters:

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

- The directory location on the Network File System where Select Identity shared files will be stored.
- The name of the cluster on which you are installing the Select Identity application.
- The name of the cluster that provides JMS clustering.
- The IP address and host name of every server in both clusters.
- The directory locations of any processes that you will need to start or stop, such as the WebSphere console or node managers.

Using the Select Identity Installer

This section describes how to install Select Identity using the installer. Before starting this procedure, you must complete the Prerequisite Configuration on page 31.

Auto-Installation Procedure

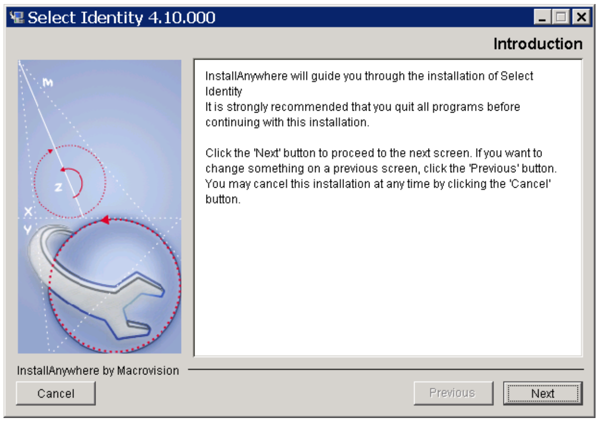
1 Log on to the operating system as the same user that was used to install WebSphere.

You must copy and run the installer directly on the application server's local machine, or the Deployment Manager node in a cluster. Do not try to run the installer remotely.

2 Mount the Select Identity CD and navigate to the installation directory.

3 Run the `install.bin` or `install.exe` executable to open the **Introduction** page of the InstallAnywhere installer.

Figure 4 The InstallAnywhere Introduction page

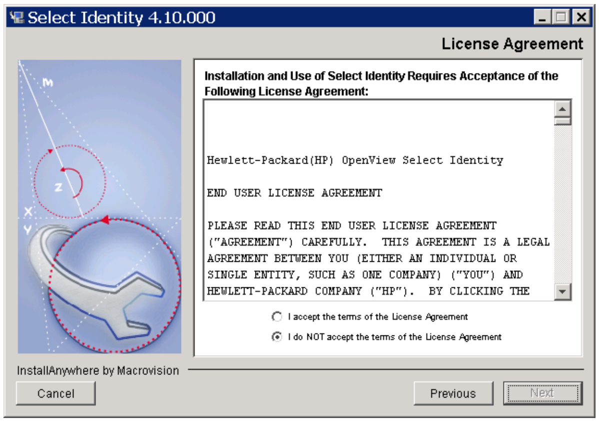


InstallAnywhere will guide you through the installation of Select Identity
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button. You may cancel this installation at any time by clicking the 'Cancel' button.

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

Figure 5 The License Agreement page



Select Identity 4.10.000

License Agreement

Installation and Use of Select Identity Requires Acceptance of the Following License Agreement:

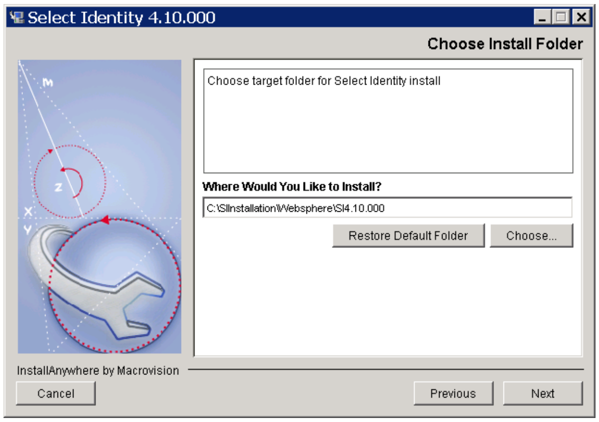
```
Hewlett-Packard(HP) OpenView Select Identity

END USER LICENSE AGREEMENT

PLEASE READ THIS END USER LICENSE AGREEMENT
("AGREEMENT") CAREFULLY.  THIS AGREEMENT IS A LEGAL
AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR
SINGLE ENTITY, SUCH AS ONE COMPANY) ("YOU") AND
HEWLETT-PACKARD COMPANY ("HP").  BY CLICKING THE
```

○ I accept the terms of the License Agreement

● I do NOT accept the terms of the License Agreement

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

Figure 6 The Choose Install Folder page



Select Identity 4.10.000

Choose Install Folder

Choose target folder for Select Identity install

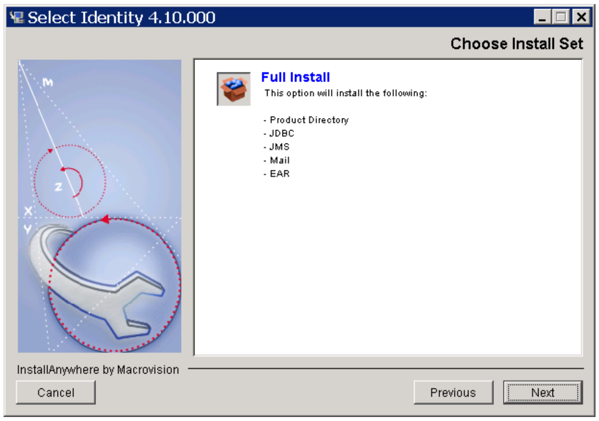
Where Would You Like to Install?

C:\SIInstallation\Websphere\SI4.10.000

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

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

Figure 7 The Choose Install Set page



Select Identity 4.10.000

Choose Install Set

Full Install

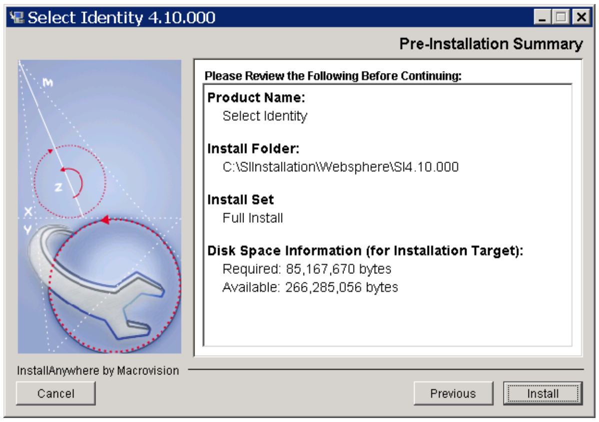
This option will install the following:

- Product Directory
- JDBC
- JMS
- Mail
- EAR

7 **Full Install** is the only option on this page; you do not need to select it. Click **Next** to proceed to the **Pre-Installation Summary** page.

8 Review the summary information before you click **Install** to continue.

Figure 8 The Pre-Installation Summary page



Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
Select Identity

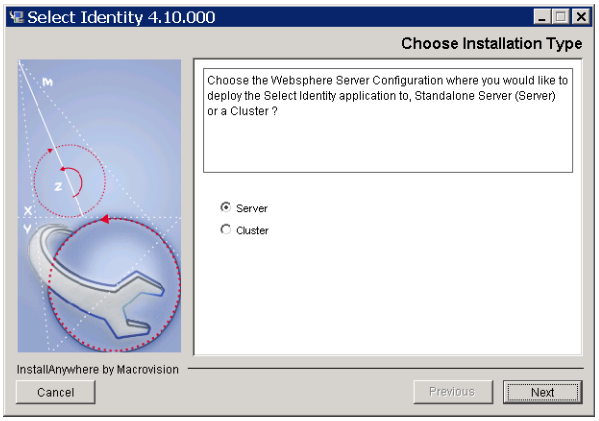
Install Folder:
C:\SIInstallation\Websphere\SI4.10.000

Install Set
Full Install

Disk Space Information (for Installation Target):
Required: 85,167,670 bytes
Available: 266,285,056 bytes

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

Figure 9 Choose Installation Type page



Choose Installation Type

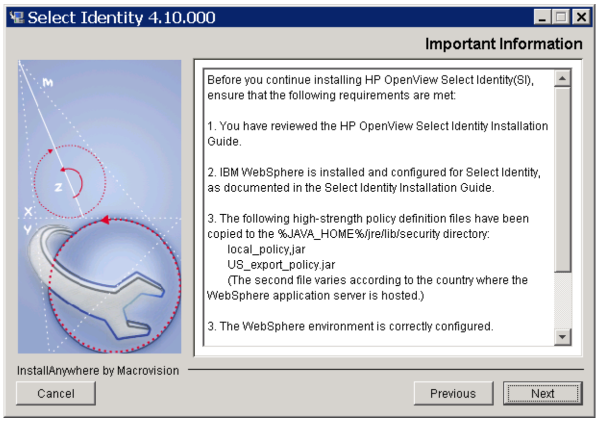
Choose the Websphere Server Configuration where you would like to deploy the Select Identity application to, Standalone Server (Server) or a Cluster ?

● Server
○ Cluster

9 Select **Server** or **Cluster** according to your WebSphere configuration.

10 Click **Next** to proceed to the **Important Information** page.

Figure 10 The Important Information page



Important Information

Before you continue installing HP OpenView Select Identity(SI), ensure that the following requirements are met:

1. You have reviewed the HP OpenView Select Identity Installation Guide.

2. IBM WebSphere is installed and configured for Select Identity, as documented in the Select Identity Installation Guide.

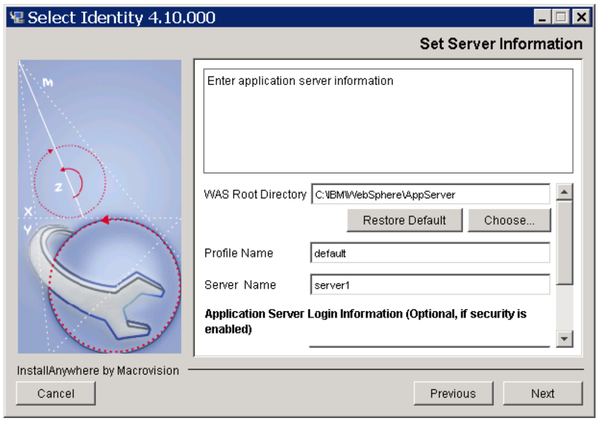
3. The following high-strength policy definition files have been copied to the %JAVA_HOME%/jre/lib/security directory:
    local_policy,jar
    US_export_policy.jar
    (The second file varies according to the country where the WebSphere application server is hosted.)

3. The WebSphere environment is correctly configured.

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

- If you are performing a standalone installation, the installer proceeds to the **Set Server Information** page (Figure 11).
- If you are performing a cluster installation, the installer proceeds to the **Set Cluster Information** page (Figure 12).

Figure 11 The Set Server Information page (standalone installation)



Set Server Information

Enter application server information

WAS Root Directory: C:\IBM\WebSphere\AppServer

Profile Name: default

Server Name: server1

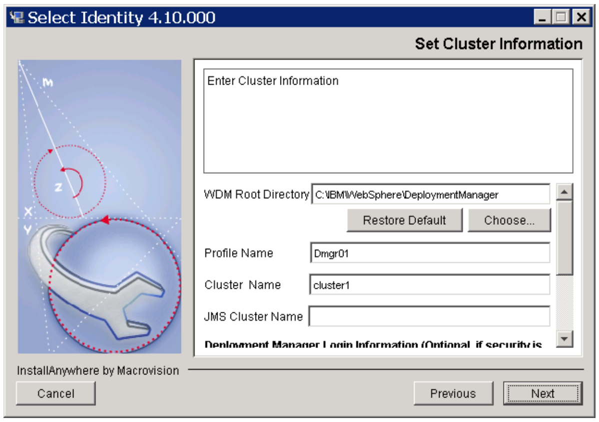
Application Server Login Information (Optional, if security is enabled)

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

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

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

Figure 12 The Set Cluster Information page (cluster installation)



Select Identity 4.10.000

Set Cluster Information

Enter Cluster Information

WDM Root Directory C:\IBM\WebSphere\DeploymentManager

Profile Name Dmgr01

Cluster Name cluster1

JMS Cluster Name

Deployment Manager Login Information (Optional, if security is

13 Specify cluster settings, as follows:

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

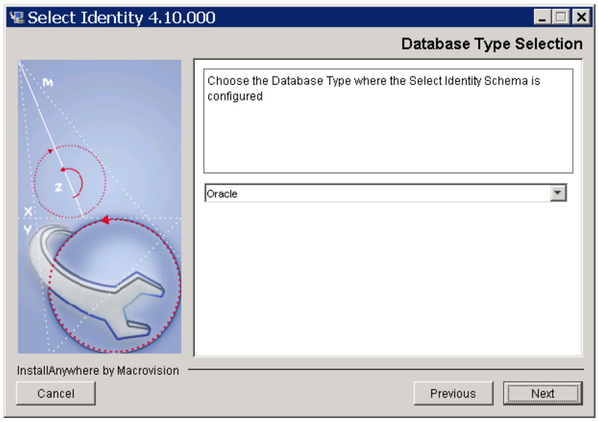
  You do not need to enter login info if security is not enabled. Leave these fields empty if security is not enabled.

- **Cluster Name** – The name of the cluster on which you are installing the Select Identity application.
- **JMS Cluster Name** – The name of the cluster on which JMS messaging will run.

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

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

Figure 13 The Database Type Selection page



Select Identity 4.10.000

Database Type Selection

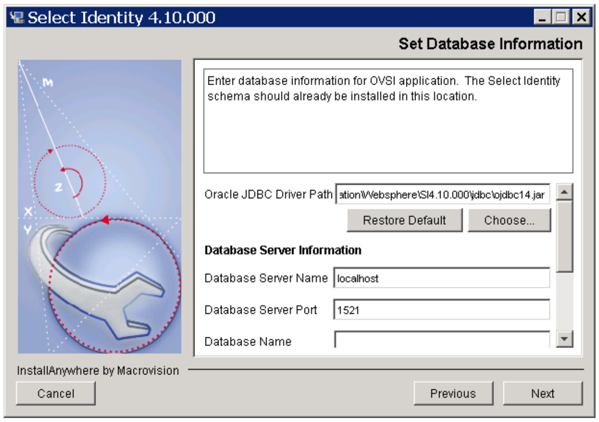
Choose the Database Type where the Select Identity Schema is configured

Oracle

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

> The instructions and illustrations that describe the database settings are based on Oracle 10g. If you are using MS-SQL 2000, you will need to make appropriate selections for this database.

Figure 14 The Set Database Information page (Select Identity)



Set Database Information

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

Oracle JDBC Driver Path: ation\Websphere\SI4.10.000\jdbc\ojdbc14.jar

Database Server Information

Database Server Name: localhost

Database Server Port: 1521

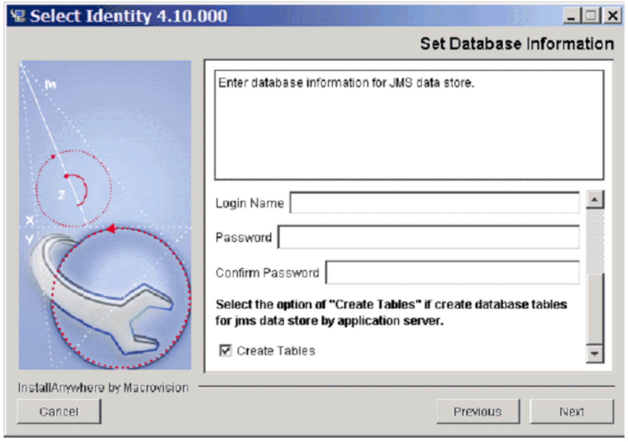
Database Name:

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

- **Database Server Name** — The hostname or IP address of the database server.
- **Database Server Port** — The port on which the database server communicates with Select Identity.
- **Database Name** — The name of the Select Identity database.
- **Database Login** — The Select Identity database user name.
- **Database Password and Confirm Database Password** — The password for logging in to the database.
- **Oracle JDBC Driver Path** — The full path to the Oracle JDBC driver file (including the actual file name: `ojdbc.jar)`. This is not needed for MS-SQL 2000.

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

Figure 15 The Set Database Information page (JMS)



Enter database information for JMS data store.

Login Name

Password

Confirm Password

Select the option of "Create Tables" if create database tables for jms data store by application server.

☑ Create Tables

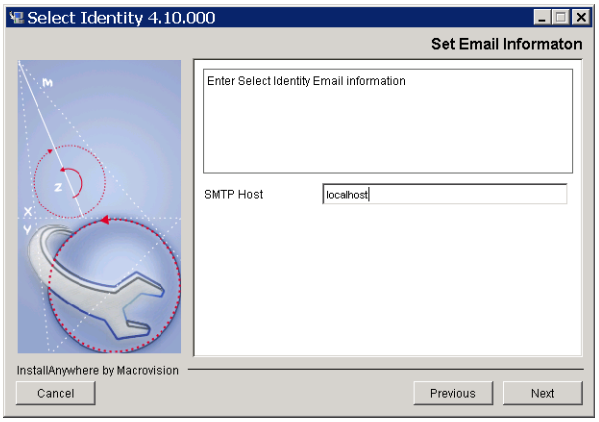
18 Complete the fields with the appropriate information about the JMS database user account:

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

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

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

Figure 16 The Set Email Information page



Select Identity 4.10.000

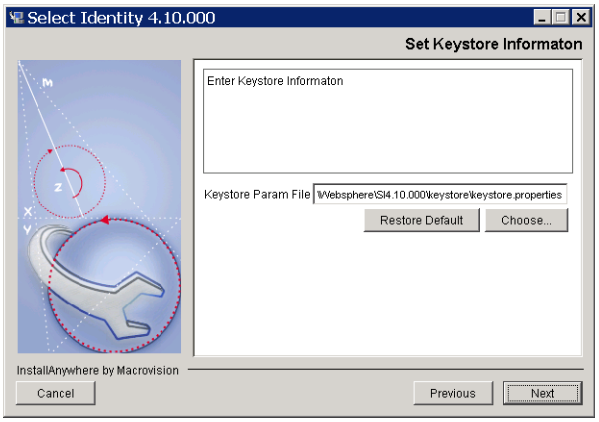
Set Email Informaton

Enter Select Identity Email information

SMTP Host: localhost

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

Figure 17 The Set Keystore Information page



Select Identity 4.10.000

Set Keystore Informaton

Enter Keystore Informaton

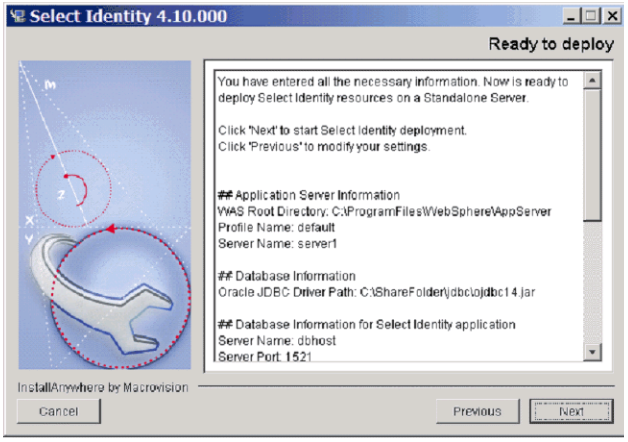
Keystore Param File: \Websphere\SI4.10.000\keystore\keystore.properties

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

> The correct directory location of the `keystore.properties` file is documented in Setting Up the Select Identity Keystores on page 110.
>
> Complete this task at part of the Prerequisite Configuration on page 31.

22 Click Next to proceed to the **Ready to deploy** page.

Figure 18 The Ready to deploy page



```
You have entered all the necessary information. Now is ready to
deploy Select Identity resources on a Standalone Server.

Click 'Next' to start Select Identity deployment.
Click 'Previous' to modify your settings.


## Application Server Information
WAS Root Directory: C:\ProgramFiles\WebSphere\AppServer
Profile Name: default
Server Name: server1

## Database Information
Oracle JDBC Driver Path: C:\ShareFolder\jdbc\ojdbc14.jar

## Database Information for Select Identity application
Server Name: dbhost
Server Port: 1521
```

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

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

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

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

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

26 Stop and restart the server or the Select Identity cluster (as applicable), so that WebSphere loads the `.jar` files that you copied in step 25.

27 Refer to Chapter 6, Configuring Select Identity, and Appendix B, Configuring TruAccess.properties for information about configuring the `TruAccess.properties` file for your environment.

28 Deploy the online help, as documented in Deploying Select Identity and the Online Help on page 56.

29 Configure the WebSphere logging features for Select Identity, as documented in Configuring Logging for Select Identity on page 59.

30 Stop and restart the WebSphere application server.

On a cluster, stop and restart all Node Agents and Deployment Manager.

31 If using global security, refer to Configuring Global Security on page 59.

32 You can now log in to Select Identity, as documented in Logging In to Select Identity on IBM WebSphere on page 60.

If Auto-Installation is Not Successful

If you are unable to launch Select Identity after running the installer, or if the installer returns any errors, it is recommended that you uninstall by running the auto-uninstaller, using the instructions provided in Auto-Uninstalling Select Identity on page 161. This procedure removes any installed components even if the installation is incomplete.

Select Identity cannot be installed on the same server or cluster if a previous copy of the LMZ.ear file is still in place.

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

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

Manual Installation Procedures

This section covers the following topics:

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

How This Section is Organized

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

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

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

Creating Directories and Copying Files

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

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

   For example, create the `C:\SIInstallation` directory on Windows, or `/opt/<OVSI_INSTALL_DIR>` directory on a Linux system.

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

   Refer to the WebSphere installation documentation for more information.

2. Create the following subdirectories in the `<OVSI_INSTALL_DIR>` directory:

- `<OVSI_INSTALL_DIR>/deploy`
- `<OVSI_INSTALL_DIR>/email`
- `<OVSI_INSTALL_DIR>/lib`
- `<OVSI_INSTALL_DIR>/recon`
- `<OVSI_INSTALL_DIR>/recon/reconroot`
- `<OVSI_INSTALL_DIR>/recon/reconbackup`
- `<OVSI_INSTALL_DIR>/recon/reconstaging`
- `<OVSI_INSTALL_DIR>/reports`
- `<OVSI_INSTALL_DIR>/sysArchive`
- `<OVSI_INSTALL_DIR>/temp`
- `<OVSI_INSTALL_DIR>/upload`
- `<OVSI_INSTALL_DIR>/userimport`
- `<OVSI_INSTALL_DIR>/userimport/adbackup`
- `<OVSI_INSTALL_DIR>/userimport/adroot`
- `<OVSI_INSTALL_DIR>/userimport/adstaging`

3. Copy the following files from the Select Identity product CD to the `<OVSI_INSTALL_DIR>/deploy` directory:
   - `application/was6_lmz.ear`
   - `application/ovsil10n_help_en_US.war`
4. Copy the following file from the Select Identity product CD to `<OVSI_INSTALL_DIR>/sysArchive`.
   - `sysArchive/TruAccess.properties`
5. Create a directory for each connector type that you install; install connector-specific information only into its respective directory.
6. On the Websphere application server, or on every node if installing on a cluster, copy the following files to the `$WAS_HOME/lib/ext` directory from the Select Identity Product CD:
   - `sysArchive/connector.jar`
   - `sysArchive/ovsii18n.jar`

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

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

Configuration Scope

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

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

Creating J2C Authentication Data Entries

1. In the left panel of the console, navigate to **Security** → **Global Security**.
2. Expand **JAAS Configuration**, located on the bottom right of the page.
3. Click **J2C Authentication Data Entries, at** the bottom of this group.
4. Click **New**.
5. Create a data entry for Select Identity, with the listed fields set as follows:
   - **Alias:** OVSI Oracle10G or OVSI MSSQL
   - **User ID:** <DB_LOGIN>
   - **Password:** <DB_PASSWORD>
6. Click **Apply**.
7. Create an additional authentication data entry for the JMS datastore, with the listed fields set as follows:
   - **Alias:** OVSI Oracle10g_JMS or OVSI JMS_MSSQL
   - **User ID:** <JMS_DB_LOGIN>
   - **Password:** <JMS_DB_PASSWORD>
8. Click **Apply**.
9. Save your changes to the master configuration.

Creating the JDBC Providers

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

On a standalone installation, create a single JDBC Provider, named `OVSI Oracle JDBC Provider` or `OVSI MSSQL JDBC Provider`, depending on your database.

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

4 Make the following selections:

- **Database Type:** Enter **Oracle** or **MSSQL** as appropriate to your database server.
- **Provider Type:** Select the provider type appropriate to your database, as follows:

  MS SQL: Websphere Embedded DirectConnect Driver

  Oracle: Oracle
- **Implementation:** Select XA data source regardless of the database type.

5 Click **Next**.

6 Enter or select the following items:

- **Name:** OVSI Oracle JDBC Provider or OVSI MSSQL JDBC Provider.
- **Class Path:** Enter the path to the Oracle 10g or MSSQL JDBC driver.

7 Click **Apply**.

8 Save your changes to the master configuration.

9 Repeat step 1 through step 8 to create a second JDBC provider, with the **Scope** set to the JMS cluster, and the **Name** set to `OVSI Oracle10g JMS JDBC Provider`, or `OVSI MSSQL JMS JDBC Provider`.

MS-SQL Configuration: Changing the Default Transaction Isolation Level

If you are using MS-SQL 2000, configure the JDBC provider by setting the correct Default Transaction Isolation Level.

To set the default Transaction Isolation Level, perform the following steps:

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

2 Select the first JDBC Provider.

3 Select **DataSource**.

4 Click the name of the Data Source for which you want to customize the Default Transaction Isolation Level.

5 Under **Additional Properties**, click **Custom Properties**.

6 Click **New** to add a new custom property.

7 Name this property `webSphereDefaultIsolationLevel`.

8 Enter `2` as the value.

9 Click **OK** and save the configuration.

10 Repeat this procedure for the second JDBC provider.

Creating the Data Sources

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

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

On a standalone installation, Locate both data sources under the HP OpenView Select Identity JDBC Provider.

To create the data sources, perform the following steps:

1 Navigate to the JDBC Provider named OVSI<database> JDBC Provider, that you created in Creating the JDBC Providers on page 46.

2 Click **Data Source**, under **Additional Properties**.

3 Click **New**, and create a data source for **Select Identity**:

   a Set the following fields, as listed:

   — **Name:** OVSI DataSource

   — **JNDI Name:** `jdbc/TruAccess`

   — **Data Store Helper Class Name:** `Oracle10g data store helper`, or `WebSphere Branded Connect JDBC data store helper` for MS-SQL.

   — **Component-managed Authentication Alias:** `OVSI Oracle10g` or `OVSI MSSQL`

   Connect JDBC data source properties:

   — **Database name:** <DB_NAME>

   — **Server name:** < DBSERVER_NAME >

   — **Port number:** < DBSERVER_PORT >

   — **Url:** For Oracle only, enter the following:

   ```
   jdbc:oracle:thin:@<DBSERVER_NAME>:<DBSERVER_PORT>:<DB_NAME>
   ```

   b Click the link to **Connection Pools**, at the bottom of the page.

   c Make the following settings:

   — **Connection Timeout:** 300

   — **Maximum Connections:** 200

   — **Connection Pool Size:** 200

   d Click the link to **WebSphere Application Server Data Source Properties,** under **Additional Properties**.

   e Set the following value:

   — **Statement Cache Size:** 50

   f Return to the Select Identity data source page.

   g Apply the Select Identity data source.

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

1 Navigate to the JDBC Provider named OVSI <Database> JMS JDBC Provider, that you created in Creating the JDBC Providers on page 46.

2 Click **Data Source**, under **Additional Properties**.

   a Click **New**, and create a data source for **JMS**:

   b Set the following fields, as listed:

   — **Name:** OVSI JMS DataSource

   — **JNDI Name:** `jdbc/TruAccess_JMS`

- **Data Store Helper Class Name:** `Oracle10g data store helper`, or `WebSphere Branded Connect Data Store Helper` for MS-SQL.
- **Component-managed Authentication Alias:** `OVSI Oracle10g_JMS` or `OVSI JMS MSSQL.`
- **Url:** `jdbc:oracle:thin:@<DBSERVER_NAME>:<DBSERVER_PORT>:<DB_NAME>`

c Click the link to **Connection Pool Properties**, on the top right under **Additional Properties**.

d Make the following settings:

- **Maximum Connections:** 100
- **Connection Timeout:** 300
- **Connection Pool Size:** 100

Connect JDBC data source properties:

- **Database name:** <DB_NAME>
- **Server name:** < DBSERVER_NAME >
- **Port number:** < DBSERVER_PORT >
- **Url:** For Oracle only, enter the following:

```
jdbc:oracle:thin:@<DBSERVER_NAME>:<DBSERVER_PORT>:<DB_NAME>
```

e Return to the **JMS Data Source** page.

f Apply the JMS data source.

g Save your changes to the master configuration.

Configuring the Select Identity Service Integration Bus

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

To create the integration bus, perform the following steps:

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

Adding Bus Members

To add bus members, perform the following steps:

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

3 Set the **Data Source JNDI Name** field for the new member to `jdbc/TruAccess_JMS`.

4 Under **Data Store,** deselect **Default.**

5 Click **Apply**.

6 Save your changes to the master configuration using the **Message** link at the top of the page.

Creating Bus Destinations

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

1 Follow the link to **Destinations**, under **Destination Resources**, in the top right of the page.

2 Create the JMS destination queues listed in the table below.

- Assign each to the bus member you created earlier (this should be the default selection).
- Ensure that you enter each **Name** and **Identitifer** *exactly* as listed below:
  - — **jms.OVSIAuditProcQ**
  - — **jms.OVSIBulkQueue**
  - — **jms.OVSIChangeReconProcessorQueue**
  - — **jms.OVSIEntCacheQueue**
  - — **jms.OVSIMessageAckQueue**
  - — **jms.OVSIReconQueue**
  - — **jms.OVSIResReconDispatcherQ**
  - — **jms.OVSIResReconQ**
  - — **jms.OVSISaudQ**
  - — **jms.OVSISchedulerQueue**
  - — **jms.OVSIServiceAssignQueue**
  - — **jms.OVSIUserImportPQueue**
  - — **jms.OVSIWorkflowQueue**
  - — **jms.OVSIWfRequestExpireQueue**

3 Click **Finish** after entering the settings for each destination, before creating the next.

4 Return to the **Destinations page** and click **New**.

5 Click **Topic Spaces**.

6 Create the topic spaces listed in the following table.

- Assign each topic to the bus member you created earlier (this should be the default selection).
- Ensure that you enter each **Name** *exactly* as listed below:
  - — jms.OVSIAuditBroadcast
  - — jms.OVSICacheTopic

7 Click **Apply** after you create each topic destination.

8 Navigate to **OVSIBus** → **Messaging Engines** → **<your_messaging_engine>** → **Data Store**.

9 Set the **Schema Name** to `<JMSDB_LOGIN_USER>` (in Oracle, the **Schema Name** is the same as the user name; in MS-SQL, the **Schema Name** is the same as the database name).

10 Select the JMS data store **Authentication Alias** (`OVSI Oracle10g_JMS`) that you created in Creating J2C Authentication Data Entries on page 46.

11 When you have created all the queue and topic destinations, save your changes to the master configuration using the **Message** link at the top of the page.

Creating JMS Resources

Creating the JMS resources consists of creating the following components:

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

Each JMS queue and topic, together with its corresponding activation specification, also maps to the bus destinations created in Creating Bus Destinations on page 50.

Creating The Queue and Topic Connection Factories

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

1 In the left panel of the console, navigate to **Resources** → **JMS Providers** → **Default Messaging**.

2 Select the **Scope** appropriate to your configuration, as follows:

- *For standalone servers,* select **Server** scope.
- *For clusters*, select **Cluster** scope (the Select Identity cluster).

3 Under **Connection Factories** in the bottom right of the page, click **JMS Queue Connection Factory**.

4 Click **New**.

5 Set the listed queue connection factory fields as follows:

- **Name:** `jms.OVSIQCF`
- **JNDI Name:** `jms/OVSIQCF`
- **Bus Name:** OVSIBus

6 Click **Apply**.

7 Click the link to **Advanced Connection Pool Properties**, under **Additional Properties** on the top right of the page.

8 Set the **Max Connections** field to `100`.

9 Click **Apply**.

10 Save your changes to the master configuration using the **Message** link at the top of the page.

11 Return to the **Default Messaging** page.

Perform the following steps to create the topic connection factory:

1 Under **Connection Factories** in the bottom right of the page, click **JMS Topic Connection Factory**.

2 Click **New**.

3 Set the listed topic connection factory fields as follows:

   - **Name:** `jms.OVSITCF`
   - **JNDI Name:** `jms/OVSITCF`
   - **Bus Name:** OVSIBus

4 Click **Apply**.

5 Click the link to **Connection Pool Properties**, under **Additional Properties** on the top right of the page.

6 Set the **Max Connections** field to `100`.

7 Click **Apply**.

8 Save your changes to the master configuration using the **Message** link at the top of the page.

9 Return to the **Default Messaging** page.

Creating the JMS Queues and Topics

Perform the following steps to create the JMS queues:

1 In the left panel of the console, navigate to **Resources** → **JMS Providers** → **Default Messaging**.

2 Select the **Scope** appropriate to your configuration, as follows:

   - *For standalone servers,* select **Server** scope.
   - *For clusters*, select **Cluster** scope (the Select Identity cluster).

3 Click **JMS Queues**, in the bottom right of the page.

4 On the **JMS Queues** page, click **New**.

5 Name the JMS queues as listed in the table below.

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

Name	JNDI Name
jms.OVSIAuditProcQ	`jms/OVSIAuditProcQ`
jms.OVSIBulkQueue	`jms/OVSIBulkQueue`
jms.OVSIChangeReconProcessorQueue	`jms/OVSIChangeReconProcessorQueue`
jms.OVSIEntCacheQueue	`jms/OVSIEntCacheQueue`
jms.OVSIMessageAckQueue	`jms/OVSIMessageAckQueue`
jms.OVSIReconQueue	`jms/OVSIReconQueue`
jms.OVSIResReconDispatcherQ	`jms/OVSIResReconDispatcherQ`
jms.OVSIResReconQ	`jms/OVSIResReconQ`

Name	JNDI Name
jms.OVSISaudQ	`jms/OVSISaudQ`
jms.OVSISchedulerQueue	`jms/OVSISchedulerQueue`
jms.OVSIServiceAssignQueue	`jms/OVSIServiceAssignQueue`
jms.OVSIUserImportPQueue	`jms/OVSIUserImportPQueue`
jms.OVSIWorkflowQueue	`jms/OVSIWorkflowQueue`
jms.OVSIWfRequestExpireQueue	`jms/OVSIWfRequestExpireQueue`

6 For each queue, set the following fields as listed under **Connection**:

- **Bus Name**: Select **OVSIBus**. This populates the **Queue Name** field.
- **Queue Name**: Select the name corresponding to the queue.

7 Click **OK** after entering the settings for each queue, before creating the next:

8 When you have completed the queues listed, save your changes to the master configuration using the **Message** link at the top of the page.

Perform the following steps to create the JMS topics:

1 Return to the **Default Messaging** page.

2 Click **JMS Topics**, in the bottom right of the page.

3 On the **JMS Topics** page, click **New**.

4 Name the JMS topics as listed in the table below.

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

Name	JNDI Name	Topic Space
jms.OVSIAuditBroadcast	`jms/OVSIAuditBroadcast`	`jms.OVSIAuditBroadcast`
jms.OVSICacheTopic	`jms/OVSICacheTopic`	`jms.OVSICacheTopic`

5 For each topic, set the following fields as listed under **Connection**:

- **Bus Name**: Select **OVSIBus**. This populates the **Topic Space** field.
- **Topic Name**: Enter the name corresponding to the topic.

6 Click **OK** after entering the settings for each topic, before creating the next:

7 When you have created all fourteen queues and two topics, save your changes to the master configuration using the **Message** link at the top of the page.

Creating Activation Specifications

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

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

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

2 Click **New**.

3 Select the **Scope** appropriate to your configuration, as follows:

- *For standalone servers,* select **Server** scope.
- *For clusters*, select **Cluster** scope (the Select Identity cluster).

4 Set the fields *exactly* as listed for each activation specification in the following tables:

a For the entries in the table below, select **Queue** as the **Destination Type**, and **OVSIBus** as the **Bus Name**:

Name	JNDI Name	Destination JNDI Name	Maximum Concurrent Endpoints
`eis.OVSIAuditProcQ`	`eis/OVSIAuditProcQ`	`jms/OVSIAuditProcQ`	10
`eis.OVSIBulkQueue`	`eis/OVSIBulkQueue`	`jms/OVSIBulkQueue`	10
`eis.OVSIChangeReconProcessorQueue`	`eis/OVSIChangeReconProcessorQueue`	`jms/OVSIChangeReconProcessorQueue`	10
`eis.OVSIEntCacheQueue`	`eis/OVSIEntCacheQueue`	`jms/OVSIEntCacheQueue`	10
`eis.OVSIMessageAckQueue`	`eis/OVSIMessageAckQueue`	`jms/OVSIMessageAckQueue`	1
`eis.OVSIReconQueue`	`eis/OVSIReconQueue`	`jms/OVSIReconQueue`	2
`eis.OVSIResReconDispatcherQ`	`eis/OVSIResReconDispatcherQ`	`jms/OVSIResReconDispatcherQ`	10
`eis.OVSIResReconQ`	`eis/OVSIResReconQ`	`jms/OVSIResReconQ`	10
`eis.OVSISaudQ`	`eis/OVSISaudQ`	`jms/OVSISaudQ`	10
`eis.OVSISchedulerQueue`	`eis/OVSISchedulerQueue`	`jms/OVSISchedulerQueue`	5
`eis.OVSIServiceAssignQueue`	`eis/OVSIServiceAssignQueue`	`jms/OVSIServiceAssignQueue`	10
`eis.OVSIUserImportPQueue`	`eis/OVSIUserImportPQueue`	`jms/OVSIUserImportPQueue`	2
`eis.OVSIWorkflowQueue`	`eis/OVSIWorkflowQueue`	`jms/OVSIWorkflowQueue`	10
`eis.OVSIWfRequestExpireQueue`	`eis/OVSIWfRequestExpireQueue`	`jms/OVSIWfRequestExpireQueue`	3

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

Name	JNDI Name	Destination JNDI Name	Maximum Concurrent Endpoints
`eis.OVSIAuditBroadcast`	`eis/OVSIAuditBroadcast`	`jms/OVSIAuditBroadcast`	1
`eis.OVSICacheTopic`	`eis/OVSICacheTopic`	`jms/OVSICacheTopic`	10

5 Click **Apply** after entering each activation specification.

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

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

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

1 Create a Select Identity mail provider by completing the following steps:

a In the left panel of the console, navigate to **Resources** → **Mail Providers**.

b Set the appropriate **Scope** as specified in Configuration Scope on page 46:

- • *For standalone servers,* select **Server** scope.
- • *For clusters*, select **Cluster** scope (the Select Identity cluster).

c Set the following mail provider fields:

Name: `OVSI Mail Provider`.

Description: Enter an appropriate description.

d Click **Apply**.

2 Perform the following steps to create an SMTP protocol provider:

a On the **Mail Providers** page, click the link to the **OVSI Mail Provider**.

b On the configuration page for the **OVSI Mail Provider**, select **Protocol Providers** under **Additional Properties**, in the top right of the page.

c Click **New**.

d Set the listed fields as follows:

Protocol: smtp

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

Type: TRANSPORT

e Click **Apply**.

3 Create a Select Identity mail session in the **OVSI Mail Provider** by completing the following steps:

a Return to the **OVSI Mail Provider** configuration page.

b Follow the link to **Mail Sessions**, under **Additional Properties**, in the top right of the page.

c Click **New**.

d Set the mail session fields as listed in the following table:

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

e Click **Apply**.

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

Deploying Select Identity and the Online Help

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

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

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

1. In the left panel of the console, navigate to **Applications** → **Install New Application**.
2. Under **Path to the New Application**, click **Browse** for **Remote File System**, then browse to the Select Identity home directory created in Creating Directories and Copying Files on page 44.
3. Open the `\deploy` directory, select `was6_lmz.ear`, and click **OK**.
4. If you are installing the online help, provide the **Context Root** value for the help file:

   `ovsil10n_help_en_US`

   This value should be adjusted for localized versions of the help.
5. On the **Install New Application** page, click **Next**.
6. Accept the defaults on the **Preparing for the Application Installation** page, and click **Next**.
7. On the **Select Installation Options** page, enter `OVSIApplication` as the **Application Name**.
8. Accept all other defaults on the **Select Installation Options** page and click **Next**.
9. If installing on a standalone server, click **Next** on the **Map Modules to Servers** page. If installing on a cluster, target all application modules to the Select Identity cluster.
10. Click **Next** on the **Provide Listener Bindings for Message-Driven Beans** page.
11. Click **Next** on the **Provide JNDI Names for Beans** page.
12. Click **Next** on the **Map EJB references to beans** page.
13. Click **Next** on the **Map Resource References to Resources** page.

14 Click **Next** on the **Map resource env entry references to resources** page.

15 Click **Next** on the **Map Virtual Hosts for Web modules** page.

16 Click **Next** on the **Ensure all unprotected 2.x methods have the correct level of protection** page.

17 On the **Summary** page, review the settings and correct as needed.

For the `was6_lmz.ear` deployment, you should see the following settings on this page:

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

18 Click **Finish** after you have reviewed the installation options.

19 Deploy the online help by repeating this procedure from step 1, selecting the help `.war` file in place of the Select Identity `.ear` file.

Updating The Select Identity Application Settings

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

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

2 Click the link to the **Configuration** page for the Select Identity application.

3 In the center left of the page, under **Class Loading and File Update Detection**, make the following selections:

- **Class loader mode:** Parent Last
- **WAR class loader policy:** Module

4 Click **Apply.**

5 Save your changes to the master configuration.

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

1. In the left panel of the console, navigate to **Servers** → **Application Servers.**
2. Select the server from the list in the main area of the page.
3. Expand the item labeled **Container Services** in the top center of the page, and click the link to **Transaction Service**.
4. Set the field labeled **Total transaction lifetime timeout** to 300.
5. Apply and then save your settings to the master configuration.

Updating the Server Class Loading Mode

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

1. In the left panel of the console, navigate to **servers** → **Application Servers**.
2. *For cluster installations,* navigate to the **Configuration** page for each server in the Select Identity cluster, and perform the remainder of this procedure on each one.

   For standalone installations, navigate to the **Configuration** page for the WebSphere server.
3. Under **Server-specific Application Settings**, on the left of the **Configuration** page, select **Parent Last** for the **Class Loading Mode**.
4. Click **Apply**.
5. Repeat this procedure for each server if you are installing on a cluster.
6. Save your changes to the master configuration.

Configuring the Java Virtual Machine

1. In the left panel of the console, navigate to **Servers** → **Application Servers**.
2. *For cluster installations,* navigate to the **Configuration** page for each server in the Select Identity cluster, and perform the remainder of this procedure on each one.

   For standalone installations, navigate to the **Configuration** page for the WebSphere server.
3. Under **Server Infrastructure**, in the center right of the page, expand the **Java and Process Management** item, and click **Process Definition**.
4. On the **Process Definition** page, under **Additional Properties** in the top right, click **Java Virtual Machine**.
5. On the **Java Virtual Machine** page, set the listed fields as follows:
   - **Generic JVM arguments (Linux only):**

   ```
   "-Dcom.trulogica.truaccess.property.file=<OVSI_INSTALL_DIR>/
   sysArchive/TruAccess.properties -Djava.awt.headless=true"
   ```

   - **Initial Heap Size**: 256
   - **Maximum Heap Size**: 1024
6. Click **Apply.**
7. Save your changes to the master configuration.

Configuring Logging for Select Identity

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

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

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

1. In the left panel of the console, navigate to **Troubleshooting** → **Logging and Tracing.**
2. Click the link to the application server, or each cluster node in turn.
3. Click **JVM Logs**.
4. Change the content of the **file name** field to reflect the directory location of the Select Identity log file.
5. Click **Apply** after changing this setting on each node in a cluster.
6. Save your changes to the master configuration.

Configuring Global Security

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

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

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

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

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

Verifying the Select Identity Installation

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

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

There are additional configuration steps for WebSphere installations. See Configuring Select Identity on page 107 to finish the process.

Do not launch the Select Identity application until you have set up the security framework as described in Setting Up the Select Identity Keystores on page 110. This is a critical step.

Logging In to Select Identity on IBM WebSphere

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

http://app_svr_host IP:port/lmz/signin.do

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

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

The default login is **sisa**. The password is **abc123**.

5 Installing Select Identity on BEA WebLogic 8.1

This chapter describes how to install and configure HP OpenView Select Identity on a WebLogic application server.

This chapter contains the following sections:

- Introduction
- Single-server or Cluster Installation
- Select Identity Installation Requirements
- Prerequisite Configuration Procedure
- Select Identity Installer Process Summary
- Select Identity Manual Installation Procedure
- Additional Configuration

Introduction

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

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

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

Single-server or Cluster 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 servers and clusters:

- 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.
- You have configured the *security framework* for the Select Identity keystores, as documented in Setting Up the Select Identity Keystores on page 110.

  Configuring the security framework is critical. Do not install Select Identity until you have completed this procedure.

Clusters only:

- The WebLogic Admin Server is running.
- The WebLogic Node Manager is running on every node.
- 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 both single servers and clusters:

- 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). You will need this location for every target server if you are installing on a cluster.

  The directory location of the WebLogic home directory on the WebLogic server or servers. You will need this location for every target server if you are installing on a cluster.
- Weblogic Application domain directory for the Select Identity application.
- The directory location of the keystore parameter file. See Setting Up the Select Identity Keystores on page 110.
- The directory locations of any processes that you will need to start or stop, such as the WebLogic console or node managers.

For clusters only:

- The directory location on the network file system (Linux) or mapped network drive (Windows) where Select Identity shared files will be stored.

By default, the installer configures JMS file stores under the mapped network drive/network file system directory. For performance reasons, you can move these files to a private drive.

- The cluster name where you are installing Select Identity.
- The names of all servers in the cluster.
- The IP address and hostname of all servers in the cluster.
- The name of the target server on which you are installing Select Identity.

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 WebLogic Startup 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 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 WebLogic Startup 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.

> Do not perform this modification if you are installing Select Identity on a cluster.

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

- On Windows:

  ```
  set WEBLOGIC_CLASSPATH=<SI Installation Dir>\weblogic
  \lib\qname.jar;%WEBLOGIC_CLASSPATH%
  ```

- On Linux:

  ```
  WEBLOGIC_CLASSPATH=<SI Installation Dir>/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 manual tasks that you must perform 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 63.

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 Select Identity `.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 path names accurately into the installer fields.

Select Identity Installer Procedure

Complete the following steps to install Select Identity using the auto-installer:

1 Perform the installation at the machine where the Weblogic Admin server is running.

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.

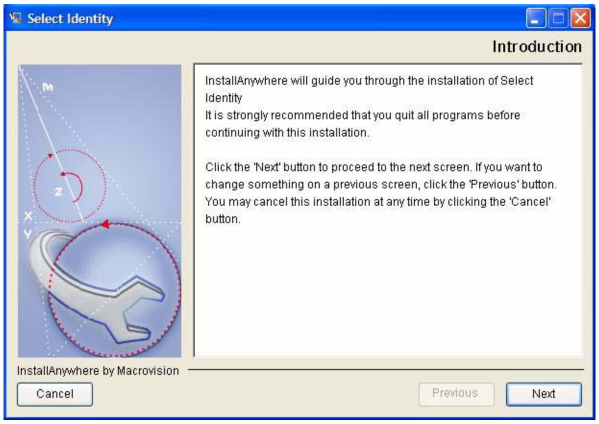
4 Copy the following files into a convenient location on the Admin server from the HP OpenView Select Identity product CD:

Linux: `installer.bin`

Windows: `installer.exe`

5 Run the executable named `install.bin` (Linux) or `install.exe` (Windows) to open the HP OpenView Select Identity Installer, as shown in Figure 19.

Figure 19 The Introduction page

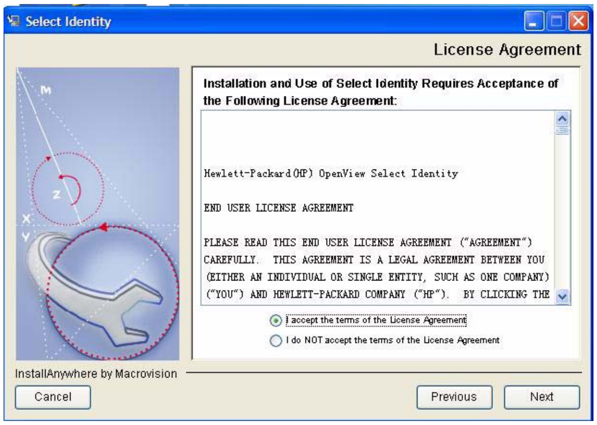


InstallAnywhere will guide you through the installation of Select Identity
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.

6 Click **Next** to proceed to the **License Agreement** page.

Figure 20 The License Agreement page



Installation and Use of Select Identity Requires Acceptance of the Following License Agreement:

Hewlett-Packard (HP) OpenView Select Identity

END USER LICENSE AGREEMENT

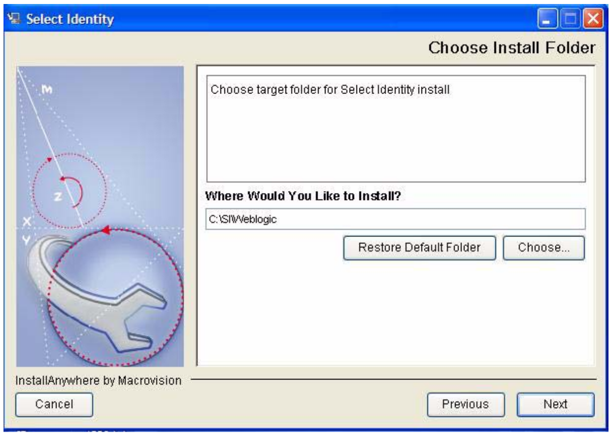
PLEASE READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") CAREFULLY. THIS AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR SINGLE ENTITY, SUCH AS ONE COMPANY) ("YOU") AND HEWLETT-PACKARD COMPANY ("HP"). BY CLICKING THE

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

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

Figure 21 The Choose Install Folder page



Choose target folder for Select Identity install

Where Would You Like to Install?

C:\SI\Weblogic

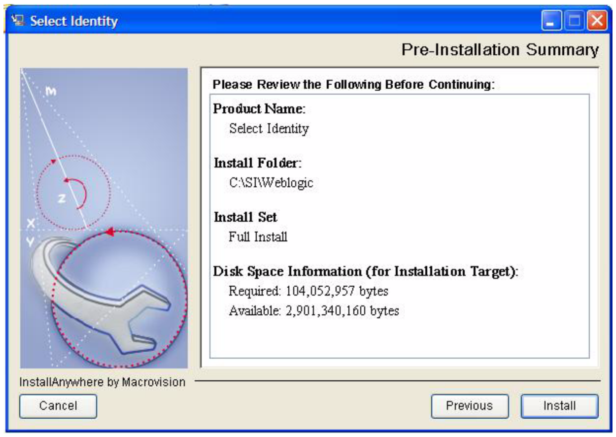
8 This page includes a field labeled **Where Would You Like to Install**, which is populated with a default installation path appropriate to your operating system.

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 cluster, ensure that your chosen installation location is in the shared file system.

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

Figure 22 The Pre-Installation Summary page



Please Review the Following Before Continuing:

Product Name:
Select Identity

Install Folder:
C:\SI\Weblogic

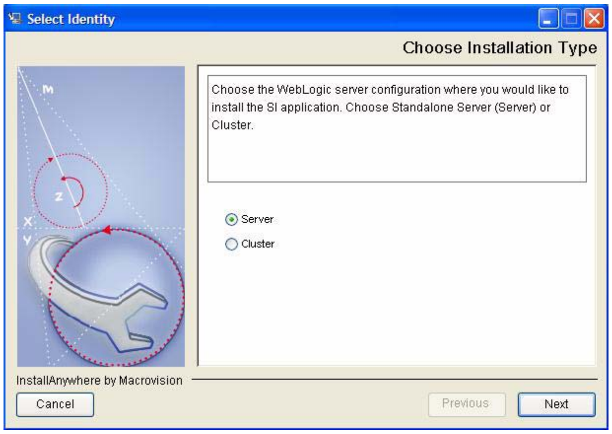
Install Set
Full Install

Disk Space Information (for Installation Target):
Required: 104,052,957 bytes
Available: 2,901,340,160 bytes

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

11 Click **Install**. The installer installs Select Identity and associated files into the chosen folder, then opens the **Choose Installation Type** page.

Figure 23 The Choose Installation Type page



Choose the WebLogic server configuration where you would like to install the SI application. Choose Standalone Server (Server) or Cluster.

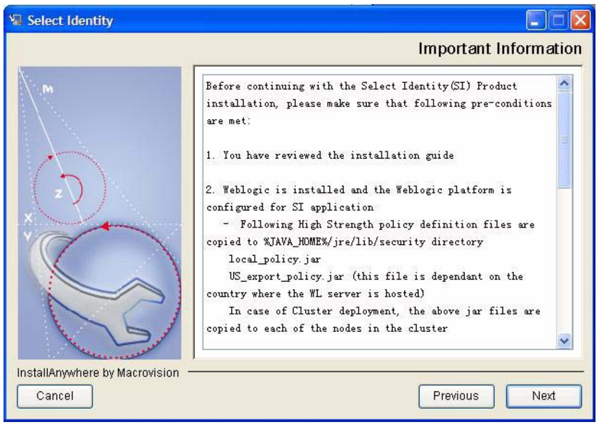
● Server

○ Cluster

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

13 Click **Next** to proceed to the **Important Information** page.

Figure 24 The Important Information page

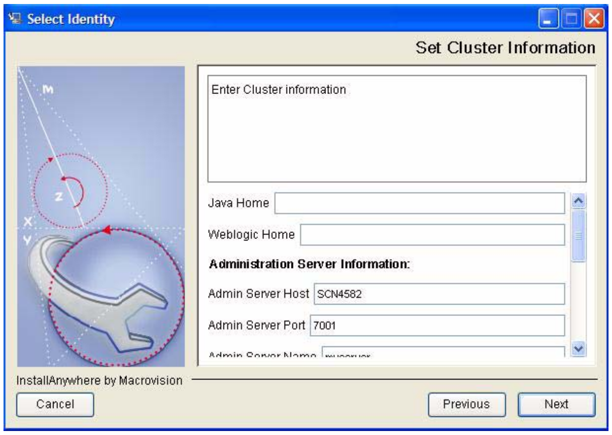


```
Before continuing with the Select Identity(SI) Product
installation, please make sure that following pre-conditions
are met:

1. You have reviewed the installation guide

2. Weblogic is installed and the Weblogic platform is
configured for SI application
   -  Following High Strength policy definition files are
copied to %JAVA_HOME%/jre/lib/security directory
    local_policy.jar
    US_export_policy.jar (this file is dependant on the
country where the WL server is hosted)
    In case of Cluster deployment, the above jar files are
copied to each of the nodes in the cluster
```

14 Review the information and verify that all prerequisites are met before you continue.

15 Click **Next** to proceed to the **Set Server Information** page (standalone server) or the **Set Cluster Information** page (cluster).

Figure 25 The Set Cluster Information page (cluster only)



Select Identity

Set Cluster Information

Enter Cluster information

Java Home

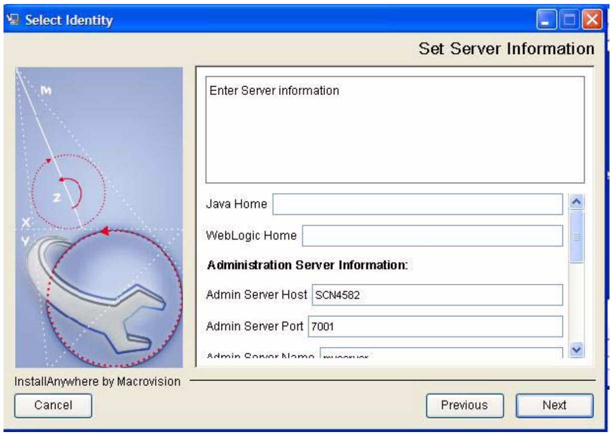
Weblogic Home

Administration Server Information:

Admin Server Host: SCN4582

Admin Server Port: 7001

Figure 26 The Set Server Information page (server only)



Select Identity

Set Server Information

Enter Server information

Java Home

WebLogic Home

Administration Server Information:

Admin Server Host: SCN4582

Admin Server Port: 7001

16 This page contains multiple settings that must be correct. Use the scroll bar to view the whole page. Complete each setting with the appropriate information, as follows:

- **Java Home** — The directory where the JDK is installed.
- **WebLogic Home** — The directory where WebLogic is installed.
- **Admin Server Host** — The hostname of the WebLogic Admin server.
- **Admin Server Port** — The port used by Select Identity.
- **Admin Server Name** — The name of the Admin server, as it appears in the WebLogic console.
- **Domain Path** — The directory location of the WebLogic application domain where Select Identity is being installed.
- **Admin Server Username** — The WebLogic Admin user name.
- **Admin Server Password and Confirm Password** — The password for the WebLogic Admin user.
- **Cluster Name** — The name of the cluster on which you are installing Select Identity, if you are installing on a cluster.

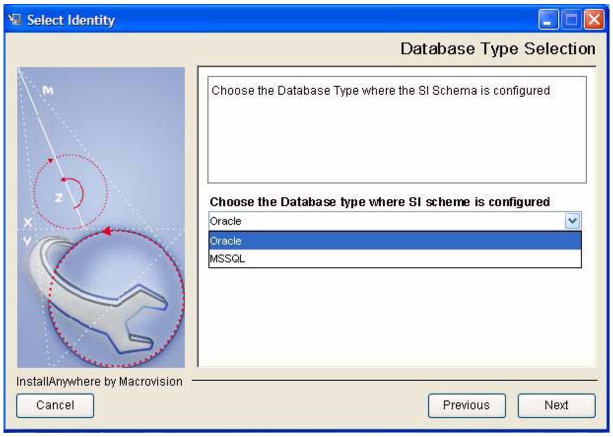
- **Server Name** (under **Target Server Information**) — The name of the server on which you are installing Select Identity, if you are installing on a single server.

17 Click **Next**. Review the information you provided, on the **Confirm User Input** page.

18 If the information is correct, click **Next**. After checking the WebLogic admin server, the installer opens the **Database Type Selection** page.

19 Use the list box to select the database type. This should be the same as the database in which you or your database administrator configured the Select Identity database, as documented in Chapter 3, Database Server Configuration.

Figure 27 The Database Type Selection page



Choose the Database Type where the SI Schema is configured

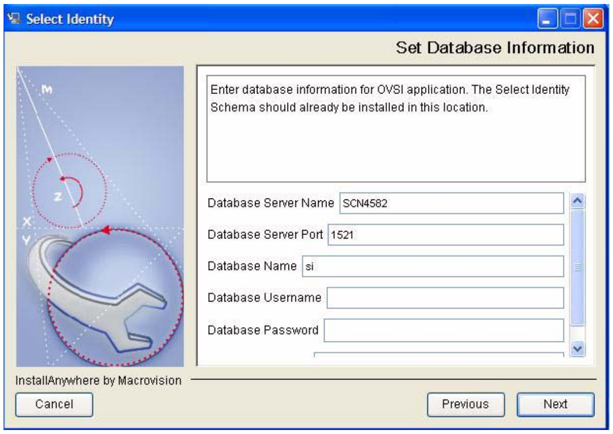
Choose the Database type where SI scheme is configured

Oracle

Oracle
MSSQL

20 Click **Next** to proceed to the **Set Database Information** page.

Figure 28 Set Database Information page



Enter database information for OVSI application. The Select Identity Schema should already be installed in this location.

Database Server Name SCN4582

Database Server Port 1521

Database Name si

Database Username

Database Password

21 Specify the settings for the Select Identity database.

The installer prepopulates the settings based on your previous selections. Use the scroll bar to view all settings.

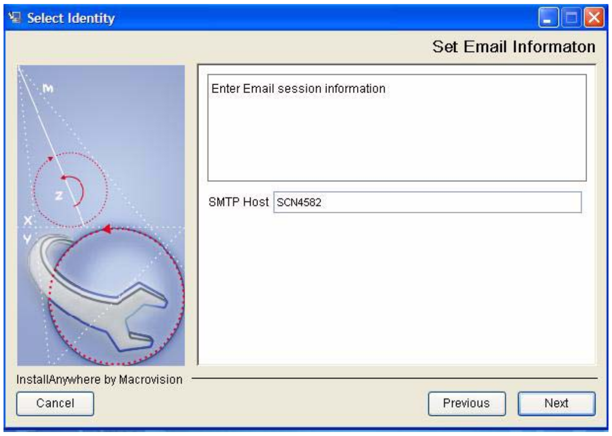
Settings are as follows:

- **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 UserName** — The user name Select Identity uses to access the database.

- **Database Password** and **Confirm Password** — The password for the database user name.

22 Click **Next** to validate the database information and proceed to the **Set Email Information** page.

Figure 29 The Set Email Information page



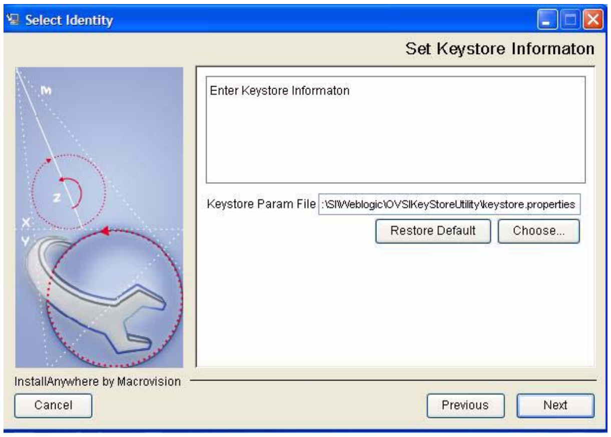
Enter Email session information

SMTP Host SCN4582

23 Specify the name of the SMTP host through which Select Identity sends email.

24 Click **Next** to proceed to the **Set Keystore Information** page.

Figure 30 The Set Keystore Information page



Enter Keystore Informaton

Keystore Param File :\SI\Weblogic\OVSIKeyStoreUtility\keystore.properties

25 Enter the path to the `keystore.properties` file. See Setting Up the Select Identity Keystores on page 110.

26 Perform the step appropriate to your installation type:

- On a *single-server* installation:

  Click **Next** to proceed to the **Ready to Install** page, and follow this procedure from step 28 on page 72.

- On a *cluster* installation:

  Click **Next** to proceed to the **Set Cluster Remote Start Information** page, and follow this procedure from step 27 on page 70.

27 Set the cluster remote start settings, as follows (cluster only). The fields auto-populate based on your previous settings, but you must enter the user name and password manually. Settings made in this page apply to all managed servers in the cluster:

- **BEA Home** — Directory where WebLogic is installed.
- **Java Home** — Directory where the JDK is installed.
- **Root Directory** — Location of the WebLogic Node Manager root directory.
- **Start Arguments** — This field is prepopulated by the installer. Do not change its contents except as specified below:

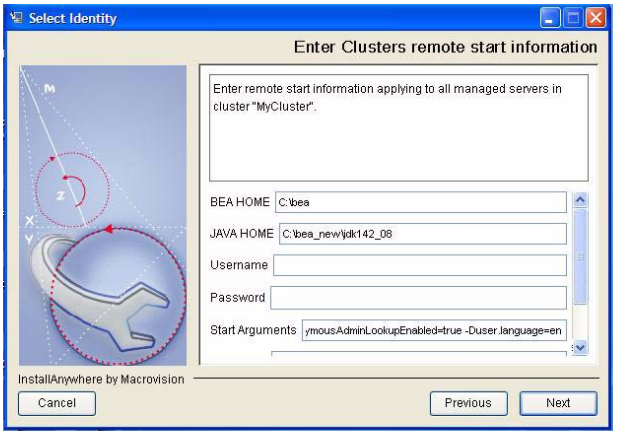
  If you are *not* using BEA's JRockit Java Developer Kit (regardless of your operating system environment), add the argument `-XX:MaxPermSize=256m` to the end of the arguments.
- **Username** and **Password** — The user name and password for all managed servers.
- **Classpath** — This field contains the individual directory locations of each of the following `.jar` files:
  - `commons-logging.jar`
  - `connector.jar`
  - `ovsii18n.jar`
  - `qname.jar`
  - `tools.jar`
  - `weblogic.jar`
  - `weblogic_sp.jar`

  The installer autopopulates paths to the files listed above, based on your previous settings. These must be correctly set. If you set them manually on any of the managed servers, the files are located in one of the following directory locations:
  - The `lib` directory in `<Java_home>` (for `tools.jar`)
  - The `lib` directory in the `<SI-install-dir>` (for `commons-logging.jar` and `qname.jar`)
  - The `sysarchive` directory in the `<SI-install-dir>` (for `connector.jar` and `ovsii18n.jar`)
  - The `lib` directory under the `server` directory in `<WebLogic_Home>` (for `weblogic.jar` and `weblogic_sp.jar`)

  This page autopopulates values intended for all managed servers in the cluster, on the assumption that all the managed servers have the same configuration for each field. If individual managed servers require different settings, modify them after installation using the WebLogic administrative console.

Click **Next** when you have set the **Cluster Remote Start** settings, to proceed to the **Ready to Install** page.

Figure 31 The Enter Cluster Remote Start Information page



Enter Clusters remote start information

Enter remote start information applying to all managed servers in cluster "MyCluster".

BEA HOME C:\bea

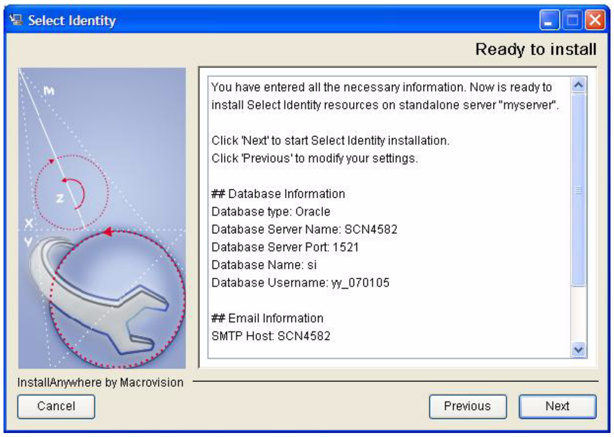
JAVA HOME C:\bea_new\jdk142_08

Username

Password

Start Arguments ymousAdminLookupEnabled=true -Duser.language=en

Figure 32 The Ready to Install page



Ready to install

You have entered all the necessary information. Now is ready to install Select Identity resources on standalone server "myserver".

Click 'Next' to start Select Identity installation.
Click 'Previous' to modify your settings.

Database Information
Database type: Oracle
Database Server Name: SCN4582
Database Server Port: 1521
Database Name: si
Database Username: yy_070105

Email Information
SMTP Host: SCN4582

28 Click **Next** when you have reviewed the information on the **Ready to Install** page.

29 What happens next depends on whether you are installing on a cluster or on a standalone server.

On a single server, the procedure is as follows:

➤ If the target server is not the same as the admin server, choose the manual option and restart the target server manually.

a The installer configures your system and then displays an alert that offers you the choice between restarting the WebLogic server automatically or manually.

b Click **AutoRestart** to restart the WebLogic server automatically, or **Cancel** to exit the installer and start the WebLogic server manually.

c If you click **Cancel**, stop and restart your WebLogic server using the installer-generated script, and then return to the installer to complete the installation.

⚠ It is very important that you start the Weblogic server using the installer-generated script because this updates the class path entry correctly. This script is named `MyStartWL`, and is located in the WebLogic home directory.

d If you select **AutoRestart**, the installer restarts the WebLogic server, deploys Select Identity, displays information about the installation result, and finally informs you that the installation is complete.

On a cluster, the procedure is as follows:

a The installer configures your system and then displays an alert asking you to restart all of the managed servers in the cluster.

b Stop and restart every managed WebLogic server in the cluster.

c Return to the installer to complete the process.

30 Click **Done** to exit the installer.

> ⚠ 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.**
>
> See the instructions in Chapter 9, Uninstalling Select Identity.

Post-Installation Steps

After installing Select Identity, perform the following:

- On a cluster, modify the JMS file and paging stores so that they are stored on local server directories. For optimal performance, you cannot locate these stores on shared directories. Refer to the manual configuration instructions in Configuring JMS File and Paging Stores on page 80.
- Verify the settings in the `TruAccess.properties` file, particularly the correct database type. Check that any paths it contains match your specific system environment. Refer to Appendix A, TruAccess Properties.
- The installer configures logging automatically. If your system requires custom logging configuration, refer to Appendix B, Logging for information.

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 62.
- Complete all of the Prerequisite Configuration Procedure on page 63 (this includes setting up the security framework, as documented in Setting Up the Select Identity Keystores on page 110.
- 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 and ovsil10n_help_en_US.war 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 these files.

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 TruAcess.properties file.

➤ See TruAccess Properties on page 165 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 WebLogic Startup Script Manually on a Single Server

When installing manually on a standalone server, you must set the JVM arguments by creating and using a custom startup script for WebLogic, named `myStartWL.sh` (Linux) or `myStartWL.cmd` (Windows).

Perform this task by opening and editing the default WebLogic Startup script file (`startWebLogic.sh` or `startWebLogic.cmd`) and then saving it, as described in this section.

The following is 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.
- Adding the `connector.jar` and `ovsii18n.jar` to the classpath

Figure 33 Example myStartWL script for Windows systems

```
set JAVA_OPTIONS=-server -Xms256m -Xmx1024m -XX:MaxPermSize=256m
-Dcom.trulogica.truaccess.property.file="C:\si4.11\weblogic\sysArchiv
e\TruAccess.properties"
-Djava.util.logging.config.file="C:\si4.11\weblogic\sysArchive\loggin
g.properties"

set
CLASSPATH=C:\si4.11\weblogic\sysArchive\connector.jar;C:\si4.11\weblo
gic\sysArchive\ovsii18n.jar;C:\si4.11\weblogic\sysArchive;C:\si4.11\w
eblogic\lib\commons-logging.jar;C:\si4.11\weblogic\lib\qname.jar;%CLA
SSPATH%

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

call startweblogic.cmd
```

Figure 34 Example myStartWL script for Linux systems

```
#!/bin/sh

JAVA_OPTIONS="-server -Xms256m -Xmx1024m -XX:MaxPermSize=200m
-Dcom.trulogica.truaccess.property.file=/opt/si4.11/weblogic/
sysArchive/TruAccess.properties -Djava.awt.headless=true
```

```
-Djava.util.logging.config.file=/opt/si4.11/weblogic/sysArchive/
logging.properties
-Dweblogic.management.anonymousAdminLookupEnabled=true"

export JAVA_OPTIONS

CLASSPATH=/opt/si4.11/weblogic/sysArchive:/opt/si4.11/weblogic/
sysArchive/connector.jar:/opt/si4.11/weblogic/sysArchive/schema.jar:/
opt/si4.11/weblogic/sysArchive/ovsii18n.jar:/opt/si4.11/weblogic/lib/
commons-logging.jar:/opt/si4.11/weblogic/lib/qname.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.

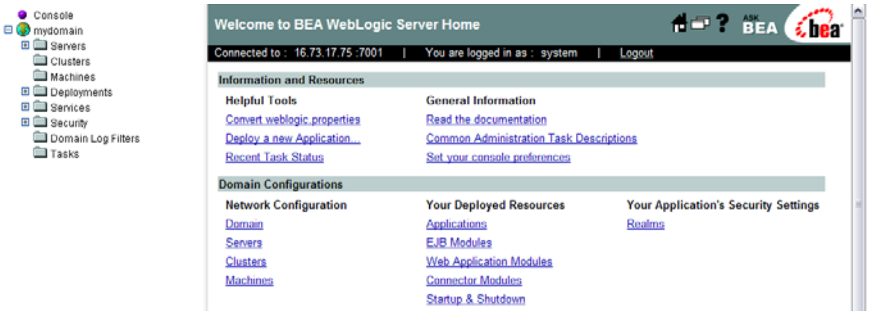
Choose the correct script according to your operating system (Linux or Windows):

```
<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain_name>/
startWebLogic.sh
```

```
<WEBLOGIC_INSTALL_DIR>\user_projects\domains\<Domain_name>\startWebLo
gic.cmd
```

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

Figure 35 WebLogic Server Home page



Welcome to BEA WebLogic Server Home

Connected to : 16.73.17.75 :7001 | You are logged in as : system | Logout

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.

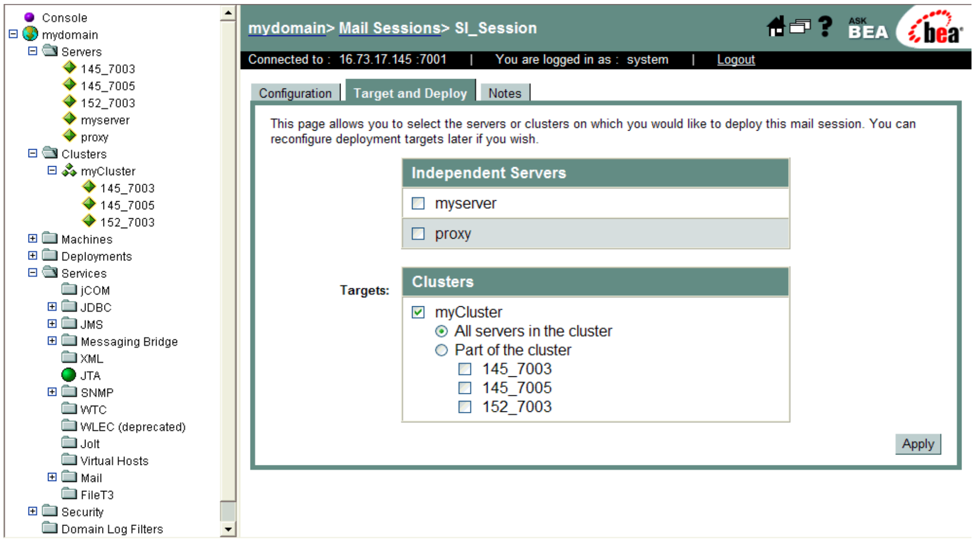
2 Click the link to **Configure a New Mail Session** at the bottom of the page.

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 36 shows an example for a clustered server. If you are installing on a single server, only independent (single) servers are available for deployment.

Figure 36 Target and Deploy page for clusters



mydomain> Mail Sessions> SI_Session

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

This page allows you to select the servers or clusters on which you would like to deploy this mail session. You can reconfigure deployment targets later if you wish.

Targets:

Independent Servers

□ myserver

□ proxy

Clusters

☑ myCluster

● All servers in the cluster

○ Part of the cluster

□ 145_7003

□ 145_7005

□ 152_7003

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 JMS File and Paging Stores

- 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 conection 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	`jms.OVSIQCF`	`jms/OVSIQCF`
Select Identity Topic Connection Factory	`jms.OVSITCF`	`jms/OVSITCF`

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

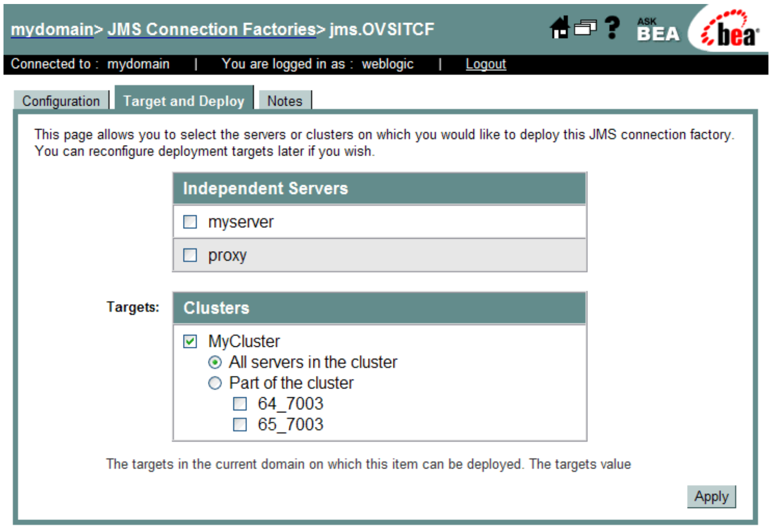
Field	Action
Server Affinity Enabled	**Clustered servers:** — Uncheck to indicate **False**. **Single servers:** — Check to indicate **True** (default).
Message Maximum	10

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 37 JMS Connection Factory Target and Deploy page



mydomain> JMS Connection Factories> jms.OVSITCF

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

Configuration | Target and Deploy | Notes

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.

Targets:

Independent Servers

☐ myserver

☐ proxy

Clusters

☑ MyCluster

● All servers in the cluster

○ Part of the cluster

☐ 64_7003

☐ 65_7003

The targets in the current domain on which this item can be deployed. The targets value

Apply

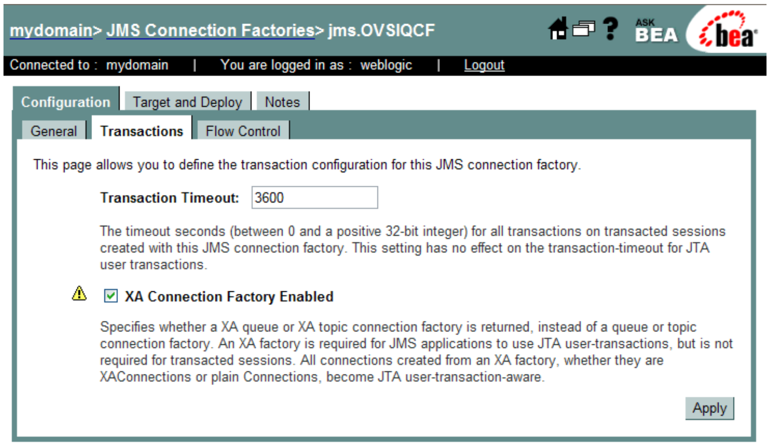
8 Select **All servers in the cluster** to deploy the Connection Factory to each node. On a single server, select the name of the independent server.

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 38 Transactions page



mydomain> JMS Connection Factories> jms.OVSIQCF

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

Configuration | Target and Deploy | Notes

General | Transactions | Flow Control

This page allows you to define the transaction configuration for this JMS connection factory.

Transaction Timeout: 3600

The timeout seconds (between 0 and a positive 32-bit integer) for all transactions on transacted sessions created with this JMS connection factory. This setting has no effect on the transaction-timeout for JTA user transactions.

⚠ ☑ **XA Connection Factory Enabled**

Specifies whether a XA queue or XA topic connection factory is returned, instead of a queue or topic connection factory. An XA factory is required for JMS applications to use JTA user-transactions, but is not required for transacted sessions. All connections created from an XA factory, whether they are XAConnections or plain Connections, become JTA user-transaction-aware.

Apply

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 JMS File and Paging Stores

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.

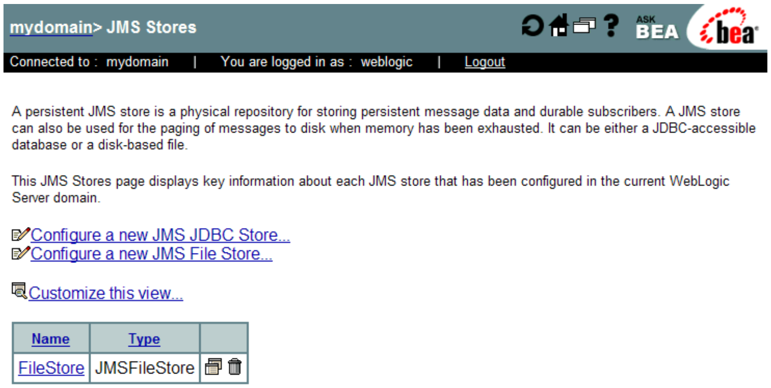
Each JMS server must have a unique persistent file store, which corresponds to that JMS server. The same file store cannot be used by another JMS server. A new file store must be created for each new JMS server.

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

To configure the JMS file and paging stores, perform the following steps:

1 Open the **JMS Stores** page by navigating to ***<domain_name>*** → **Services** → **JMS** → **Stores**.

Figure 39 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.

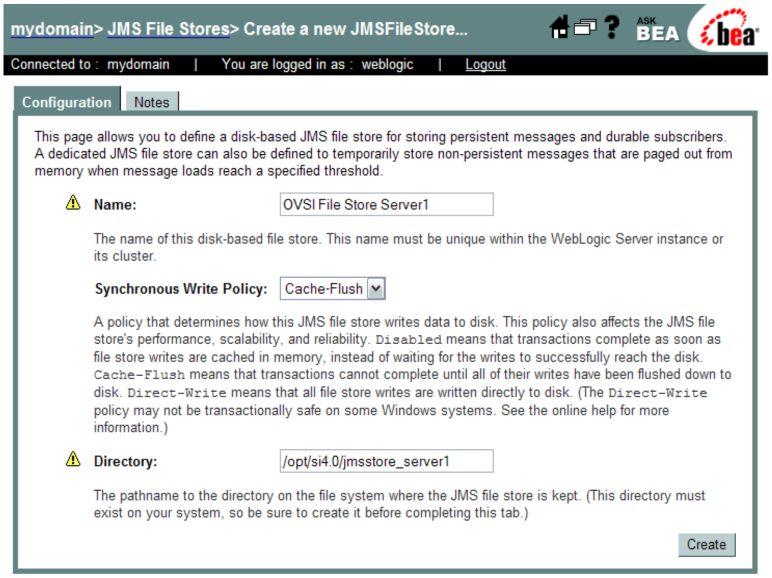
Configure a new JMS JDBC Store...
Configure a new JMS File Store...

Customize this view...

Name	Type	
FileStore	JMSFileStore	

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

Figure 40 JMS Store page



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

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

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:** OVSI File Store Server1

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

Synchronous Write Policy: Cache-Flush

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:** /opt/si4.0/jmsstore_server1

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 In the **Name** field, 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 In the **Directory** field, enter the path to the file and paging store.

For example: `<OVSI_INSTALL_DIR>/jmsstore<Server1>`

`<Server1>` is the server ID in the cluster.

> Do not use shared directory locations for file and paging stores. These file stores should be in local server directories for optimal performance.

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.

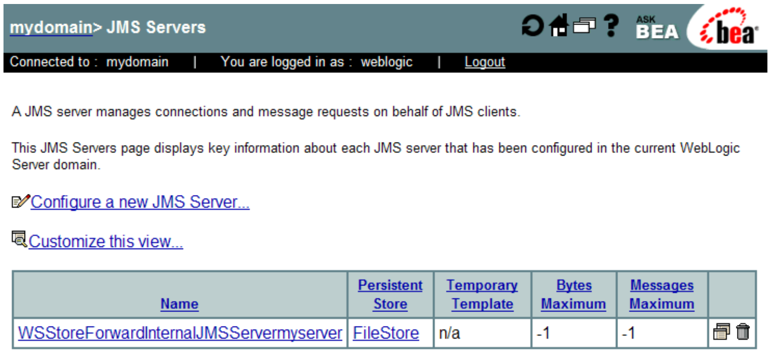
Configuring a JMS Server

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 41 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.

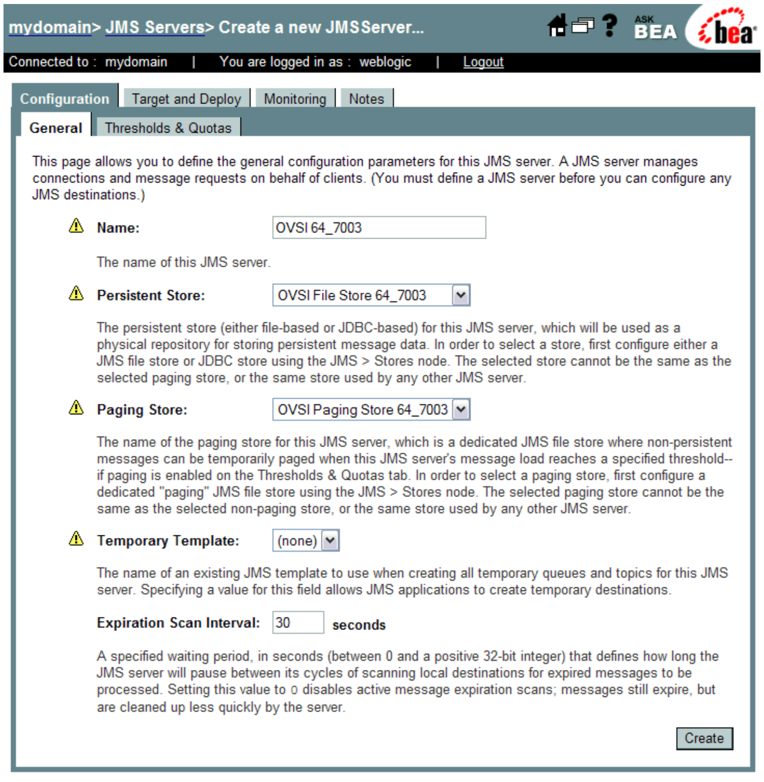
Configure a new JMS Server...

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 42 Create a new JMS Server page


mydomain> JMS Servers> Create a new JMSServer...
ASK BEA
Connected to : mydomain | You are logged in as : weblogic | Logout
Configuration
Target and Deploy
Monitoring
Notes
General
Thresholds & Quotas
Create

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:** OVSI 64_7003

The name of this JMS server.

⚠ **Persistent Store:** OVSI File Store 64_7003

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:** OVSI Paging Store 64_7003

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:** (none)

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: 30 **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.

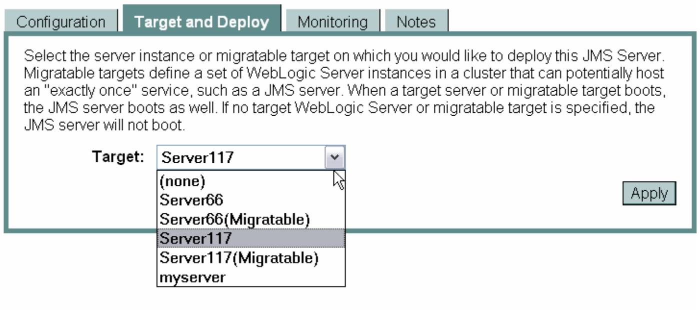
3 Tab from field to field and enter the required information.

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 43 JMS Server Target and Deploy page



Select the server instance or migratable target on which you would like to deploy this JMS Server. Migratable targets define a set of WebLogic Server instances in a cluster that can potentially host an "exactly once" service, such as a JMS server. When a target server or migratable target boots, the JMS server boots as well. If no target WebLogic Server or migratable target is specified, the JMS server will not boot.

Target: Server117

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

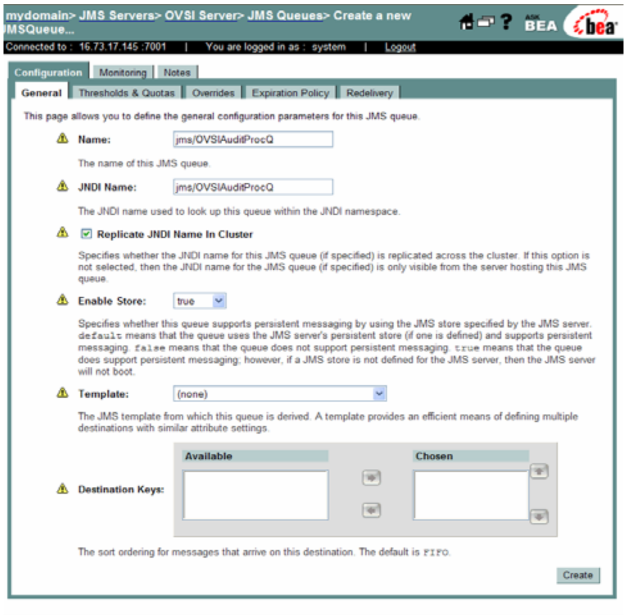
You must configure each JMS Queue listed in this procedure. If you are installing on a clustered server, skip this procedure and proceed to Configuring JMS Queues on a Clustered Server on page 86.

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 44 Configure a New JMS Queue page


mydomain> JMS Servers> OVSI Server> JMS Queues> Create a new JMSQueue...
ASK BEA
bea
Connected to : 16.73.17.145 :7001 | You are logged in as : system | Logout
Configuration
Monitoring
Notes
General
Thresholds & Quotas
Overrides
Expiration Policy
Redelivery
Available
Chosen
Create

This page allows you to define the general configuration parameters for this JMS queue.

Name: jms/OVSIAuditProcQ

The name of this JMS queue.

JNDI Name: jms/OVSIAuditProcQ

The JNDI name used to look up this queue within the JNDI namespace.

☑ Replicate JNDI Name In Cluster

Specifies whether the JNDI name for this JMS queue (if specified) is replicated across the cluster. If this option is not selected, then the JNDI name for the JMS queue (if specified) is only visible from the server hosting this JMS queue.

Enable Store: true

Specifies whether this queue supports persistent messaging by using the JMS store specified by the JMS server. `default` means that the queue uses the JMS server's persistent store (if one is defined) and supports persistent messaging. `false` means that the queue does not support persistent messaging. `true` means that the queue does support persistent messaging; however, if a JMS store is not defined for the JMS server, then the JMS server will not boot.

Template: (none)

The JMS template from which this queue is derived. A template provides an efficient means of defining multiple destinations with similar attribute settings.

Destination Keys:

The sort ordering for messages that arrive on this destination. The default is `FIFO`.

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`
UserRecon Process	`jms.OVSIReconQueue`	`jms/OVSIReconQueue`
Resource Reconciliation Flow Control	`jms.OVSIResReconDispatcherQ`	`jms/OVSIResReconDispatcherQ`
Resource Reconciliation Processing	`jms.OVSIResReconQ`	`jms/OVSIResReconQ`
SA Integration	`jms.OVSISaudQ`	`jms/OVSISaudQ`
Batch Handling	`jms.OVSISchedulerQueue`	`jms/OVSISchedulerQueue`
Service Assignment	`jms.OVSIServiceAssignQueue`	`jms/OVSIServiceAssignQueue`

Purpose	Recommended Name	Required Name
Request Expiration	`jms.OVSIWfRequestExpireQueue`	`jms/OVSIWfRequestExpireQueue`
User Import Process	`jms.OVSIUserImportPQueue`	`jms/OVSIUserImportPQueue`
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 106.

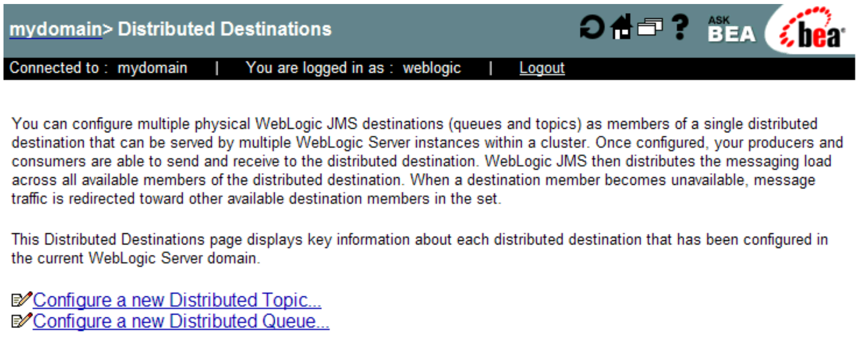
Configuring JMS Queues on a Clustered Server

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

Perform the following steps to configure the JMS Queues:

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

Figure 45 Distributed Destinations page



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

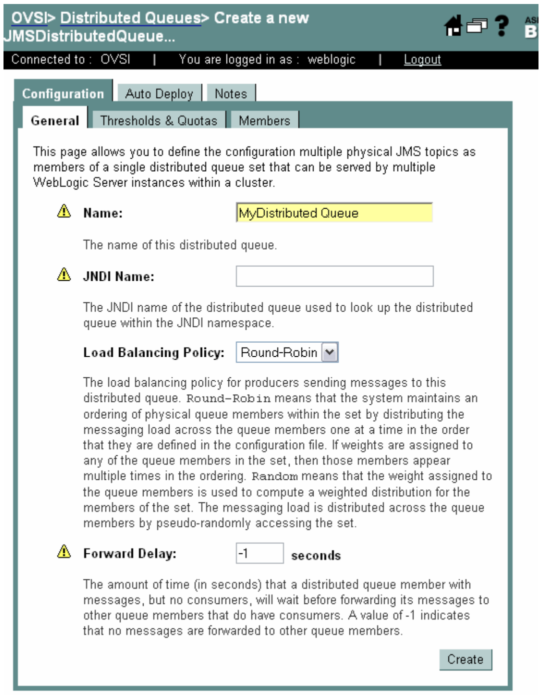
You can configure multiple physical WebLogic JMS destinations (queues and topics) as members of a single distributed destination that can be served by multiple WebLogic Server instances within a cluster. Once configured, your producers and consumers are able to send and receive to the distributed destination. WebLogic JMS then distributes the messaging load across all available members of the distributed destination. When a destination member becomes unavailable, message traffic is redirected toward other available destination members in the set.

This Distributed Destinations page displays key information about each distributed destination that has been configured in the current WebLogic Server domain.

Configure a new Distributed Topic...
Configure a new Distributed Queue...

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

Figure 46 Create a New JMS Distributed Queue page



OVSI> Distributed Queues> Create a new JMSDistributedQueue...

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

This page allows you to define the configuration multiple physical JMS topics as members of a single distributed queue set that can be served by multiple WebLogic Server instances within a cluster.

⚠ **Name:** MyDistributed Queue

The name of this distributed queue.

⚠ **JNDI Name:**

The JNDI name of the distributed queue used to look up the distributed queue within the JNDI namespace.

Load Balancing Policy: Round-Robin

The load balancing policy for producers sending messages to this distributed queue. `Round-Robin` means that the system maintains an ordering of physical queue members within the set by distributing the messaging load across the queue members one at a time in the order that they are defined in the configuration file. If weights are assigned to any of the queue members in the set, then those members appear multiple times in the ordering. `Random` means that the weight assigned to the queue members is used to compute a weighted distribution for the members of the set. The messaging load is distributed across the queue members by pseudo-randomly accessing the set.

⚠ **Forward Delay:** -1 **seconds**

The amount of time (in seconds) that a distributed queue member with messages, but no consumers, will wait before forwarding its messages to other queue members that do have consumers. A value of -1 indicates that no messages are forwarded to other queue members.

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.OVSIChangeRecon ProcessorQueue`	`jms/OVSIChangeReconProcessor Queue`
Entitlement Cache Processing	`jms.OVSIEntCacheQueue`	`jms/OVSIEntCacheQueue`
Service Recon Flow Control	`jms.OVSIMessageAck Queue`	`jms/OVSIMessageAckQueue`
User Recon Process	`jms.OVSIReconQueue`	`jms/OVSIReconQueue`
Resource Reconciliation Dispatch	`jms.OVSIResRecon DispatcherQ`	`jms/ OVSIWfResReconDispatcherQ`
Resource Reconciliation Processing	`jms.OVSIResReconQ`	`jms/OVSIResReconQ`
SA Integration	`jms.OVSISaudQ`	`jms/OVSISaudQ`
Batch Handling	`jms.OVSISchedulerQueue`	`jms/OVSISchedulerQueue`

Process	Recommended Name	Required JNDI Name
Service Assignment	`jms.OVSIServiceAssignQueue`	`jms/OVSIServiceAssignQueue`
Workflow Process	`jms.OVSIWorkflowQueue`	`jms/OVSIWorkflowQueue`
Request Expire	`jms.OVSIWfRequestExpireQueue`	`jms/OVSIWfRequestExpireQueue`

4 Tab to the **Load Balancing Policy** field and enter **Round Robin**.

5 Tab to the **Forward Delay** field and enter **0**.

6 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 84 for each node, using the queue settingas documented in that procedure. Use the notes below for guidance:

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

Configuring JMS Topics on a Clustered Server

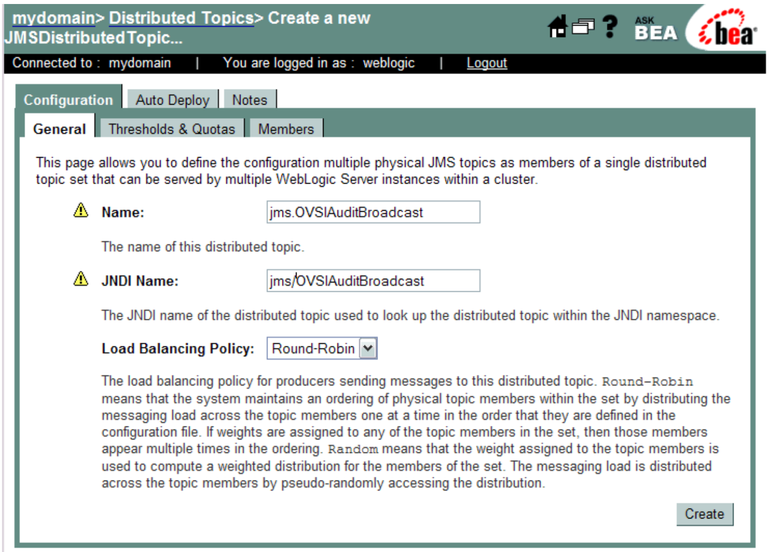
You must configure each JMS Topic listed in this procedure, but you do not need to repeat the procedure for the individual nodes because the JMS Topics are deployed to the nodes automatically.

Perform the following steps to configure the JMS Topics:

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

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

Figure 47 Create a new JMS Topic page


mydomain> Distributed Topics> Create a new JMSDistributedTopic...
ASK BEA
bea
Connected to : mydomain | You are logged in as : weblogic | Logout
Configuration
Auto Deploy
Notes
General
Thresholds & Quotas
Members
Create

This page allows you to define the configuration multiple physical JMS topics as members of a single distributed topic set that can be served by multiple WebLogic Server instances within a cluster.

⚠ Name: jms.OVSIAuditBroadcast

The name of this distributed topic.

⚠ JNDI Name: jms/OVSIAuditBroadcast

The JNDI name of the distributed topic used to look up the distributed topic within the JNDI namespace.

Load Balancing Policy: Round-Robin

The load balancing policy for producers sending messages to this distributed topic. `Round-Robin` means that the system maintains an ordering of physical topic members within the set by distributing the messaging load across the topic members one at a time in the order that they are defined in the configuration file. If weights are assigned to any of the topic members in the set, then those members appear multiple times in the ordering. `Random` means that the weight assigned to the topic members is used to compute a weighted distribution for the members of the set. The messaging load is distributed across the topic members by pseudo-randomly accessing the distribution.

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.OVSICacheTopic`	`jms/OVSICacheTopic`

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 88.

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

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

2 Click the link to the **Configure a new JMS Topic** page.

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

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

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 106.

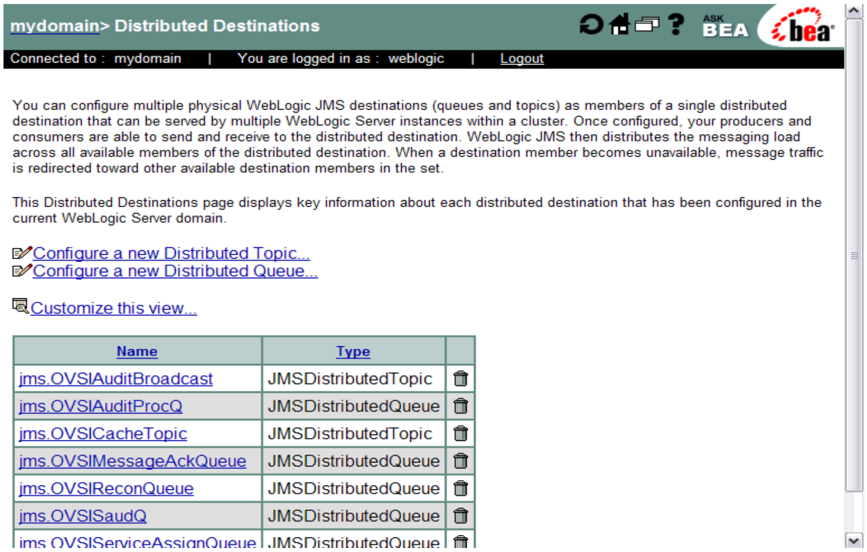
Creating JMS Server Members

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 48 Distributed Topic page



mydomain> Distributed Destinations

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

You can configure multiple physical WebLogic JMS destinations (queues and topics) as members of a single distributed destination that can be served by multiple WebLogic Server instances within a cluster. Once configured, your producers and consumers are able to send and receive to the distributed destination. WebLogic JMS then distributes the messaging load across all available members of the distributed destination. When a destination member becomes unavailable, message traffic is redirected toward other available destination members in the set.

This Distributed Destinations page displays key information about each distributed destination that has been configured in the current WebLogic Server domain.

Configure a new Distributed Topic...
Configure a new Distributed Queue...

Customize this view...

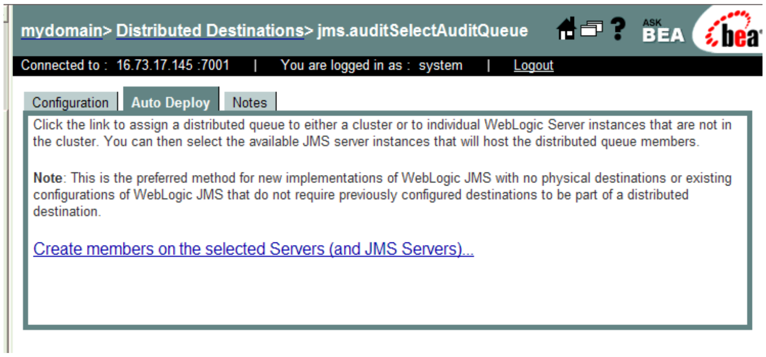
Name	Type	
jms.OVSIAuditBroadcast	JMSDistributedTopic	🗑
jms.OVSIAuditProcQ	JMSDistributedQueue	🗑
jms.OVSICacheTopic	JMSDistributedTopic	🗑
jms.OVSIMessageAckQueue	JMSDistributedQueue	🗑
jms.OVSIReconQueue	JMSDistributedQueue	🗑
jms.OVSISaudQ	JMSDistributedQueue	🗑
jms.OVSIServiceAssignQueue	JMSDistributedQueue	🗑

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 49 Auto Deploy page


mydomain> Distributed Destinations> jms.auditSelectAuditQueue
ASK BEA
bea
Configuration
Auto Deploy
Notes

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

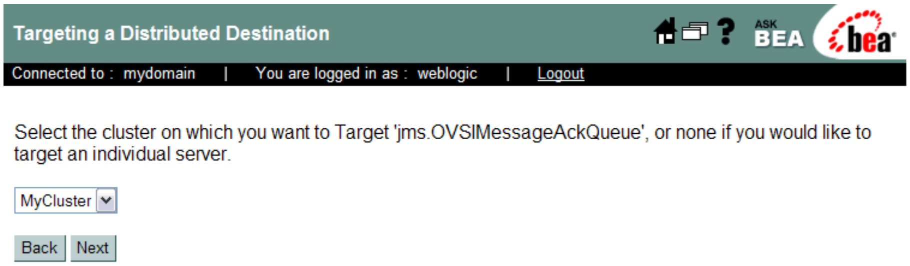
Click the link to assign a distributed queue to either a cluster or to individual WebLogic Server instances that are not in the cluster. You can then select the available JMS server instances that will host the distributed queue members.

Note: This is the preferred method for new implementations of WebLogic JMS with no physical destinations or existing configurations of WebLogic JMS that do not require previously configured destinations to be part of a distributed destination.

Create members on the selected Servers (and JMS Servers)...

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

Figure 50 Targeting a Distributed Destination page



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

Select the cluster on which you want to Target 'jms.OVSIMessageAckQueue', or none if you would like to target an individual server.

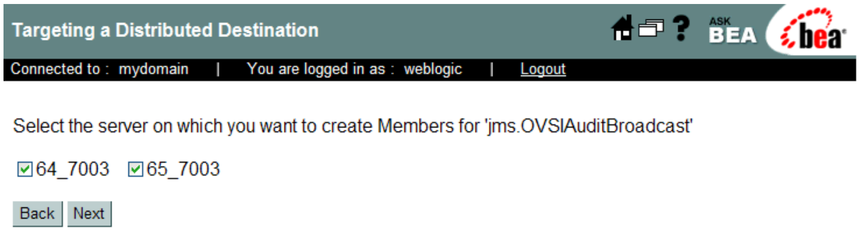
MyCluster

5 Make the correct entry

Server Type	Action
Single Server	Select **None** in the field displayed.
Clustered Server	Select your cluster in the field displayed.

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

Figure 51 Targeting a Distributed Destination page to Select Servers



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

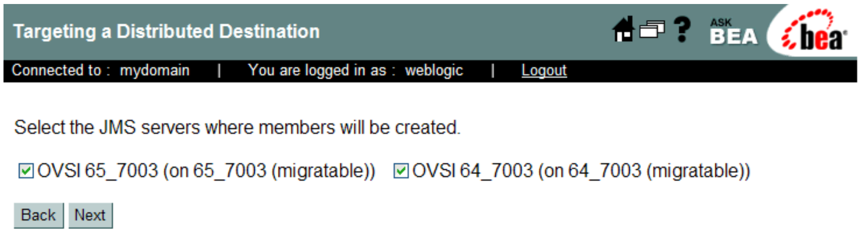
Select the server on which you want to create Members for 'jms.OVSIAuditBroadcast'

☑64_7003 ☑65_7003

7 Select each server on which to create members for the JMS Queue or Topic.

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

Figure 52 Targeting a Distributed Destination page: Selecting Servers



Targeting a Distributed Destination

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

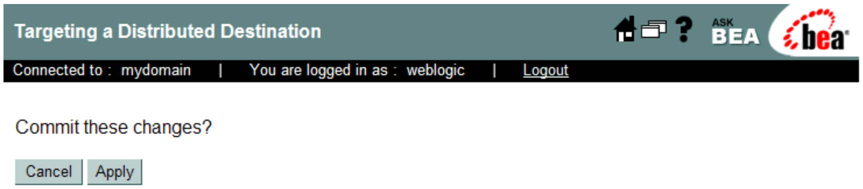
Select the JMS servers where members will be created.

☑ OVSI 65_7003 (on 65_7003 (migratable)) ☑ OVSI 64_7003 (on 64_7003 (migratable))

9 Select each JMS server on which members are to be created.

10 Click **Next** to proceed to the next **Targeting a Distributed Destination** page and commit the changes for the JMS Queue or Topic.

Figure 53 Targeting Distributed Destination page: Committing Changes



Targeting a Distributed Destination

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

Commit these changes?

11 Click the **Apply** button to commit the changes.

12 Repeat this procedure for all JMS Queues and Topics in the Distributed Destinations tree.

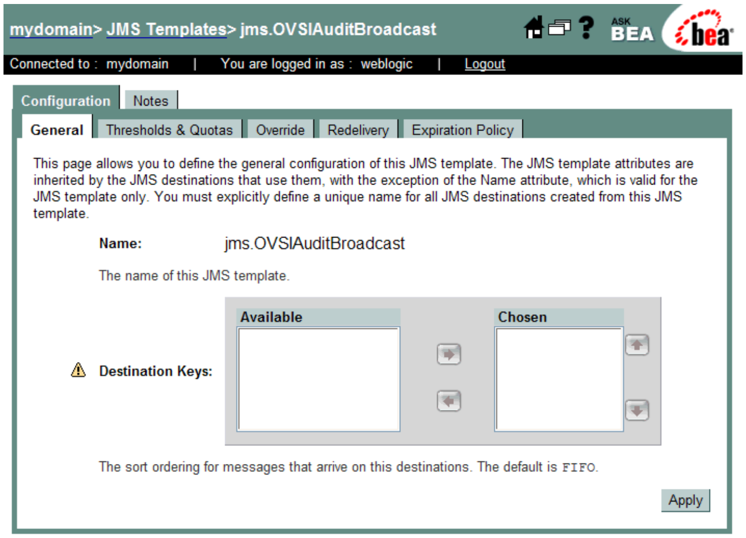
Modifying the JMS Template for JMS Queues and Topics

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 54 JMS Templates General page



mydomain> JMS Templates> jms.OVSIAuditBroadcast

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

This page allows you to define the general configuration of this JMS template. The JMS template attributes are inherited by the JMS destinations that use them, with the exception of the Name attribute, which is valid for the JMS template only. You must explicitly define a unique name for all JMS destinations created from this JMS template.

Name: jms.OVSIAuditBroadcast

The name of this JMS template.

⚠ **Destination Keys:**

The sort ordering for messages that arrive on this destinations. The default is `FIFO`.

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 `OVSIWorkflowQueue`, click the **Override** tab and set the **Delivery Mode Override** to **Persistent**.

12 Repeat the procedure until all of the existing JMS Queue and Topic templates have been set up.

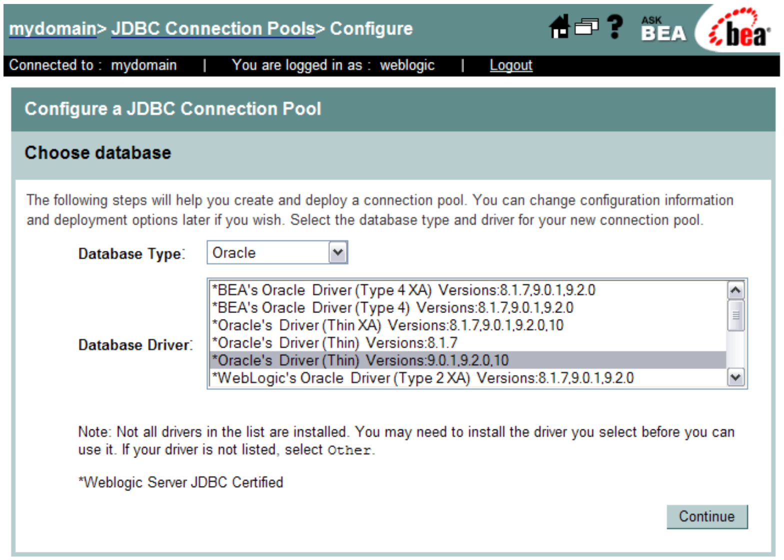
Configuring a JDBC Connection Pool

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

1 Open the **JDBC Connection** page by navigating to **<*domain_name*>** → **Services** → **JDBC** → **Connection Pools**.

2 Open the **Configure a JDBC Connection Pool** page by clicking the link to **Configure a new JDBC Connection Pool**.

Figure 55 Configure a JDBC Connection Pool page



mydomain> JDBC Connection Pools> Configure

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

Configure a JDBC Connection Pool

Choose database

The following steps will help you create and deploy a connection pool. You can change configuration information and deployment options later if you wish. Select the database type and driver for your new connection pool.

Database Type: Oracle

Database Driver:

*BEA's Oracle Driver (Type 4 XA) Versions:8.1.7,9.0.1,9.2.0
*BEA's Oracle Driver (Type 4) Versions:8.1.7,9.0.1,9.2.0
*Oracle's Driver (Thin XA) Versions:8.1.7,9.0.1,9.2.0,10
*Oracle's Driver (Thin) Versions:8.1.7
*Oracle's Driver (Thin) Versions:9.0.1,9.2.0,10
*WebLogic's Oracle Driver (Type 2 XA) Versions:8.1.7,9.0.1,9.2.0

Note: Not all drivers in the list are installed. You may need to install the driver you select before you can use it. If your driver is not listed, select `Other`.

*Weblogic Server JDBC Certified

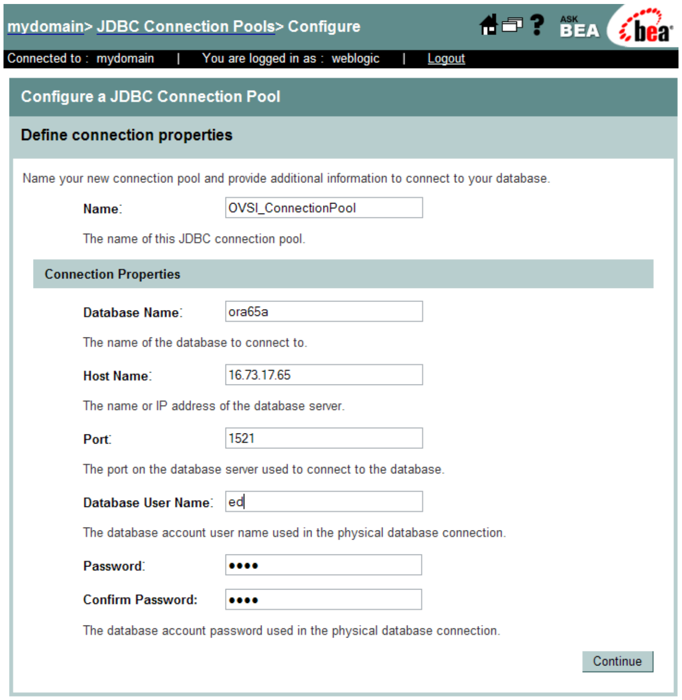
3 Select the database type that corresponds to your database from the **Database Type** list box.

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 56 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: OVSI_ConnectionPool

The name of this JDBC connection pool.

Connection Properties

Database Name: ora65a

The name of the database to connect to.

Host Name: 16.73.17.65

The name or IP address of the database server.

Port: 1521

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

Database User Name: ed

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.
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.

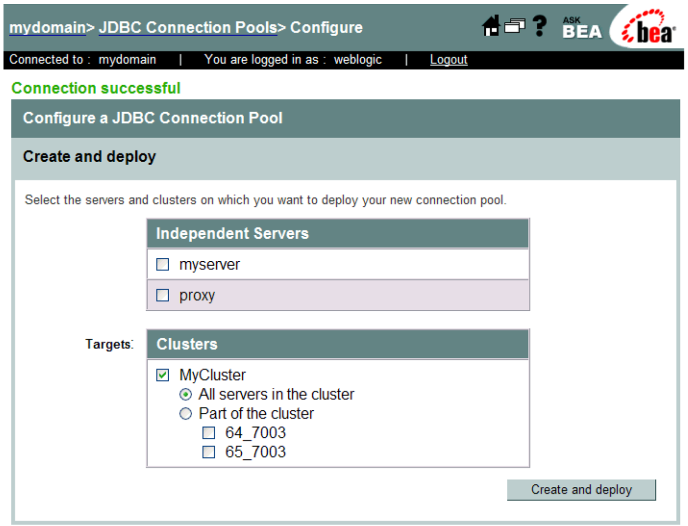
8 If you are installing Select Identity with Oracle 9i or 10g, add the following to the **Properties** field. Enter the value on a separate line from any pre-existing content in that field:

```
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 57 Configure a JDBC Connection Pool page



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

Connection successful

Configure a JDBC Connection Pool

Create and deploy

Select the servers and clusters on which you want to deploy your new connection pool.

Targets:

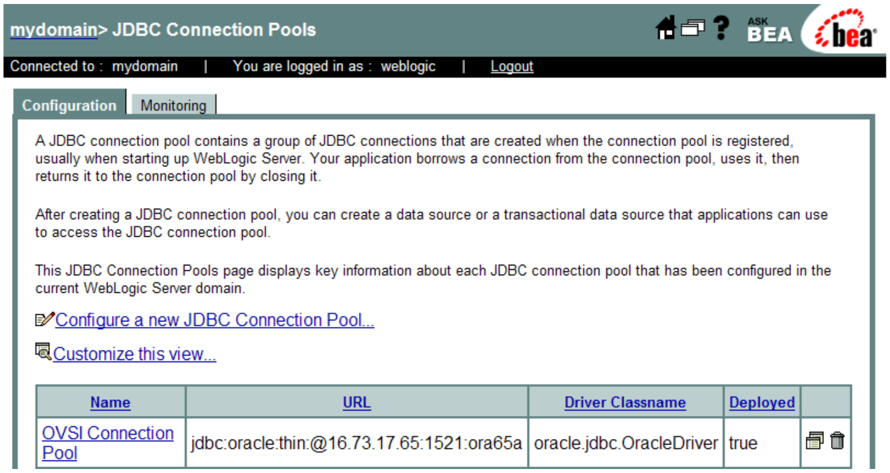
Independent Servers
□ myserver
□ proxy

Clusters
☑ MyCluster
● All servers in the cluster
○ Part of the cluster
□ 64_7003
□ 65_7003

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 58 JDBC Connection Pools Configuration page



mydomain> JDBC Connection Pools
ASK BEA
bea
Connected to : mydomain | You are logged in as : weblogic | Logout
Configuration
Monitoring

A JDBC connection pool contains a group of JDBC connections that are created when the connection pool is registered, usually when starting up WebLogic Server. Your application borrows a connection from the connection pool, uses it, then returns it to the connection pool by closing it.

After creating a JDBC connection pool, you can create a data source or a transactional data source that applications can use to access the JDBC connection pool.

This JDBC Connection Pools page displays key information about each JDBC connection pool that has been configured in the current WebLogic Server domain.

Configure a new JDBC Connection Pool...

Customize this view...

Name	URL	Driver Classname	Deployed	
OVSI Connection Pool	jdbc:oracle:thin:@16.73.17.65:1521:ora65a	oracle.jdbc.OracleDriver	true	

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.

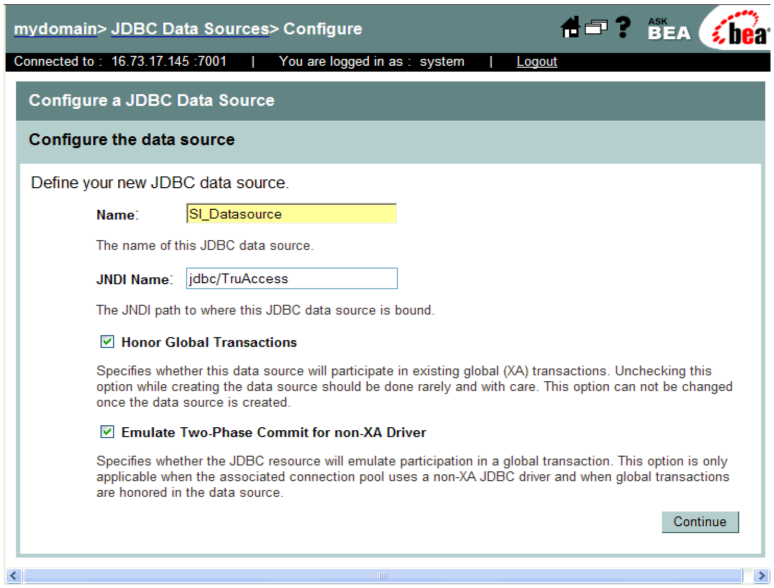
Configuring the JDBC Data Source

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**.

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

Figure 59 Configure a JDBC Data Source page


mydomain> JDBC Data Sources> Configure
ASK BEA
bea
Connected to : 16.73.17.145 :7001 | You are logged in as : system | Logout
Continue

Configure a JDBC Data Source

Configure the data source

Define your new JDBC data source.

Name: SI_Datasource

The name of this JDBC data source.

JNDI Name: jdbc/TruAccess

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

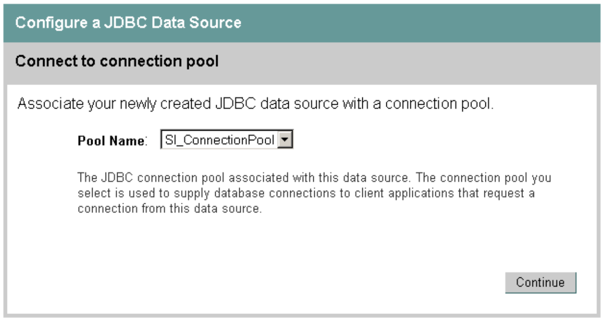
Specifies whether the JDBC resource will emulate participation in a global transaction. This option is only applicable when the associated connection pool uses a non-XA JDBC driver and when global transactions are honored in the data source.

3 Enter the following information:

Field	Action
Name	Enter a name for the new data source.
JNDI Name	Enter `jdbc/TruAccess`.
Honor Global Transactions	Check the box to enable this setting.
Emulate Two-Phase Commit for non-XA Driver	Check the box to enable this setting.

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

Figure 60 Connect to Connection Pool page



Configure a JDBC Data Source

Connect to connection pool

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

Pool Name: SI_ConnectionPool

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

5 Select the connection pool from the **Pool Name** list box that was created in Configuring a JDBC Connection Pool on page 93.

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)

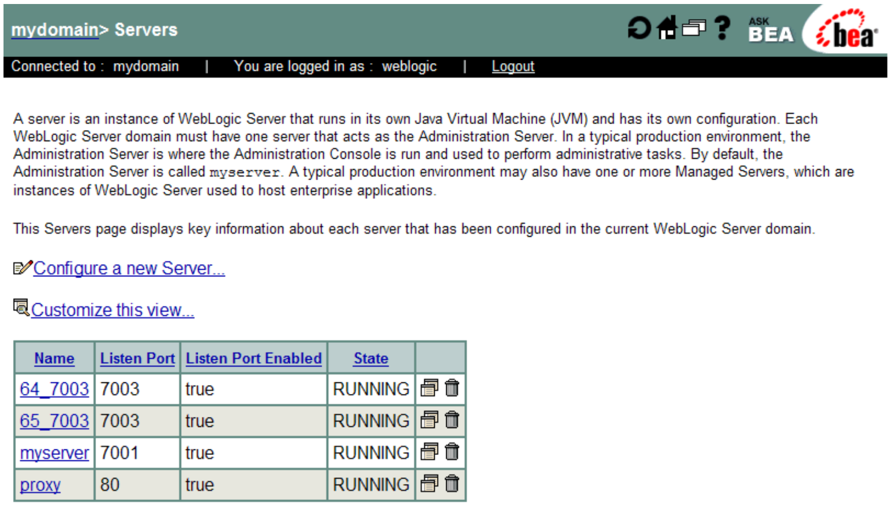
On a cluster, use the following step to stop the servers via the WebLogic console:

- 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 61 Servers page with running 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.

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 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	`<BEA_HOME>/jrockit81sp5_142_08` (Linux) `<BEA_HOME>\JDK142_08\` (Windows) **For single servers:** Do not make this setting.
BEA Home	`<BEA_HOME>` The actual path to the WebLogic home directory, for example: `/opt/bea` **For single servers:** Do not make this setting.
Root Directory	`<BEA_HOME>/common/nodemanager` The path to the Node Manager for the cluster. **For single servers:** Do not make this setting.

Class Path	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.
	Windows:
	`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`
	Linux:
	`/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`
	For single servers:
	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.

Field	Action

Arguments	`-server -Xms256m -Xmx1024m`
	If you are *not* using BEA’s JRockit Java Developer Kit (regardless of your operating system environment), add the argument `-XX:MaxPermSize=256m` to the end of the arguments.
	On Windows systems, add the argument `-Dcom.trulogica.truaccess.property.file=/<OVSI_INSTALL_DIR>/sysArchive/TruAccess.properties`
	On Linux systems, add the argument `-Djava.awt.headless=true`
	Add the argument that specifies the location and name of the logging.properties file for that server, using the example below for reference:
	`-Djava.util.logging.config.file=/<OVSI_INSTALL_DIR>/sysArchive/myServer1_logging.properties`
	For single servers:
	You must set these arguments by editing the `myStartWL.sh` or `myStartWL.cmd` script in the WebLogic domain directory where you will be running Select Identity.

6 Click **Apply**.

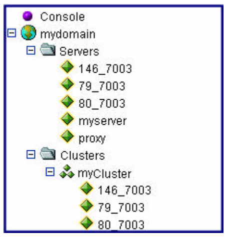
7 On a Weblogic cluster, repeat the process until you have updated each server in the cluster.

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 62 Selecting the server for execute queue configuration



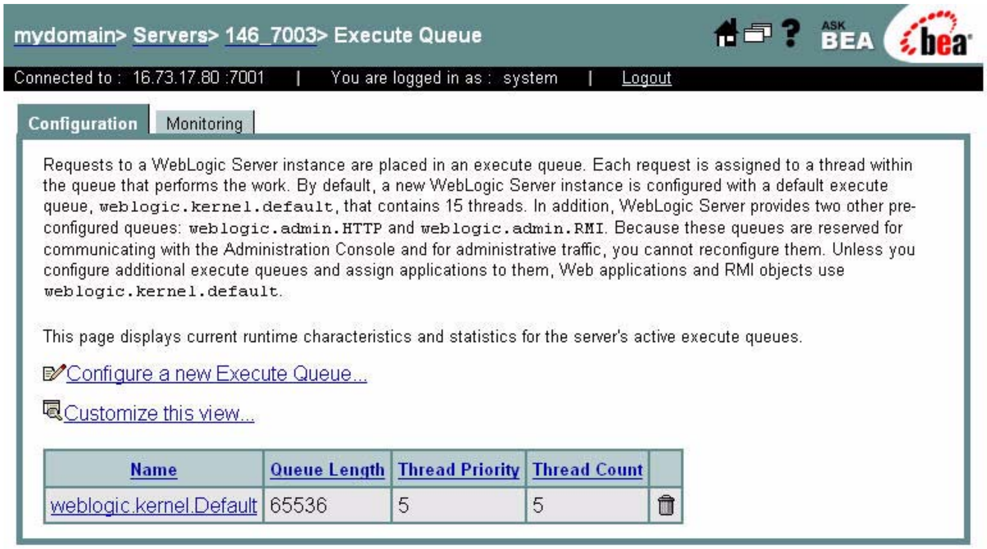
2 On the server page, scroll down to locate the **Advanced Options**.

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 63.

Figure 63 Execute Queues Configuration page



mydomain> Servers> 146_7003> Execute Queue

Connected to : 16.73.17.80 :7001 | You are logged in as : system | Logout

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**.

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

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

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

9 When the the **Execute Queues** page reopens, return to step 6 and repeat until all three queues are created.

Enabling Anonymous Admin Lookup

Enable Anonymous Admin Lookup by performing the following steps:

1 Navigate to the domain where you are installing Select Identity using the left-pane navigation links.

2 On the domain page, scroll down and click the link to **View Domain-Wide Security Settings**.

3 Locate the setting to **Enable Anonymous Admin Lookup**.

4 Check the box, if necessary, to enable this setting.

5 Click **Apply**.

Starting the WebLogic Server

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

```
./myStartWL.sh
```

```
myStartWL.cmd
```

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

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

Deploying Select Identity on WebLogic

Deploy Select Identity on the WebLogic Server as follows:

1 Log in to the **WebLogic Server Console**.

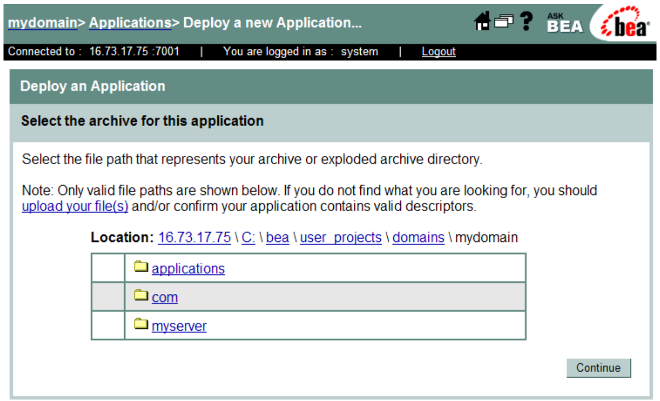
2 Navigate to **<*domain_name*>** → **Deployments** → **Applications**.

The Applications page displays.

3 Select the **Deploy a new Application** link.

The **Deploy a new Application** page opens.

Figure 64 The Deploy a new Application page



mydomain> Applications> Deploy a new Application...

Connected to : 16.73.17.75 :7001 | You are logged in as : system | Logout

Deploy an Application

Select the archive for this application

Select the file path that represents your archive or exploded archive directory.

Note: Only valid file paths are shown below. If you do not find what you are looking for, you should upload your file(s) and/or confirm your application contains valid descriptors.

Location: 16.73.17.75 \ C: \ bea \ user_projects \ domains \ mydomain

applications

com

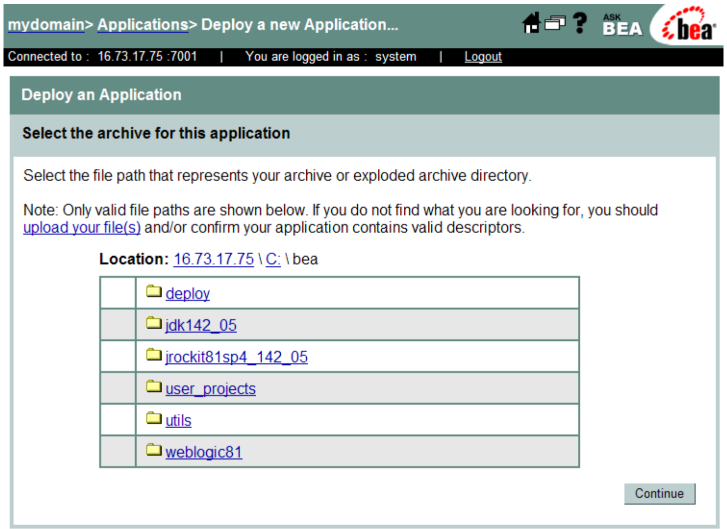
myserver

4 Locate and select the `lmz.ear` file, which resides in the `<OVSI_INSTALL_DIR>/deploy` directory created in Creating Select Identity Directories and Copying Installation Files on page 74.

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

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

Figure 65 Second Deploy a new Application page



Connected to : 16.73.17.75 :7001 | You are logged in as : system | Logout

Deploy an Application

Select the archive for this application

Select the file path that represents your archive or exploded archive directory.

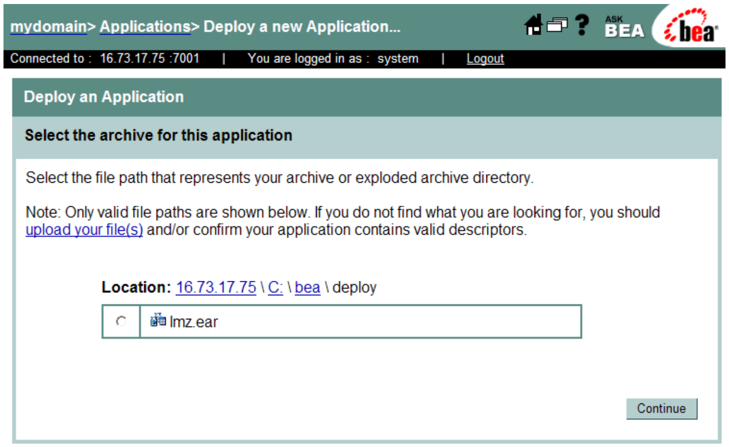
Note: Only valid file paths are shown below. If you do not find what you are looking for, you should upload your file(s) and/or confirm your application contains valid descriptors.

Location: 16.73.17.75 \ C: \ bea

	deploy
	jdk142_05
	jrockit81sp4_142_05
	user_projects
	utils
	weblogic81

5 Open the `deploy` folder to proceed to the third **Deploy a new Application** page.

Figure 66 Third Deploy a new Application page



Connected to : 16.73.17.75 :7001 | You are logged in as : system | Logout

Deploy an Application

Select the archive for this application

Select the file path that represents your archive or exploded archive directory.

Note: Only valid file paths are shown below. If you do not find what you are looking for, you should upload your file(s) and/or confirm your application contains valid descriptors.

Location: 16.73.17.75 \ C: \ bea \ deploy

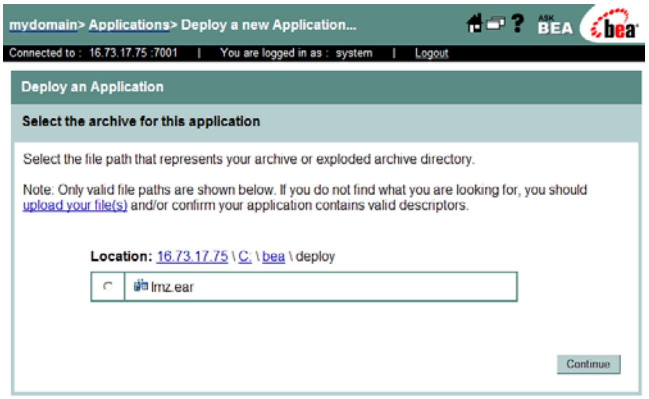
○	lmz.ear

6 Click the radio button next to the `lmz.ear` file.

7 Click **Continue**.

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

Figure 67 Fourth Deploy a new Application page



mydomain> Applications> Deploy a new Application...

Connected to : 16.73.17.75 :7001 | You are logged in as : system | Logout

Deploy an Application

Select the archive for this application

Select the file path that represents your archive or exploded archive directory.

Note: Only valid file paths are shown below. If you do not find what you are looking for, you should upload your file(s) and/or confirm your application contains valid descriptors.

Location: 16.73.17.75 \ C: \ bea \ deploy

○ lmz.ear

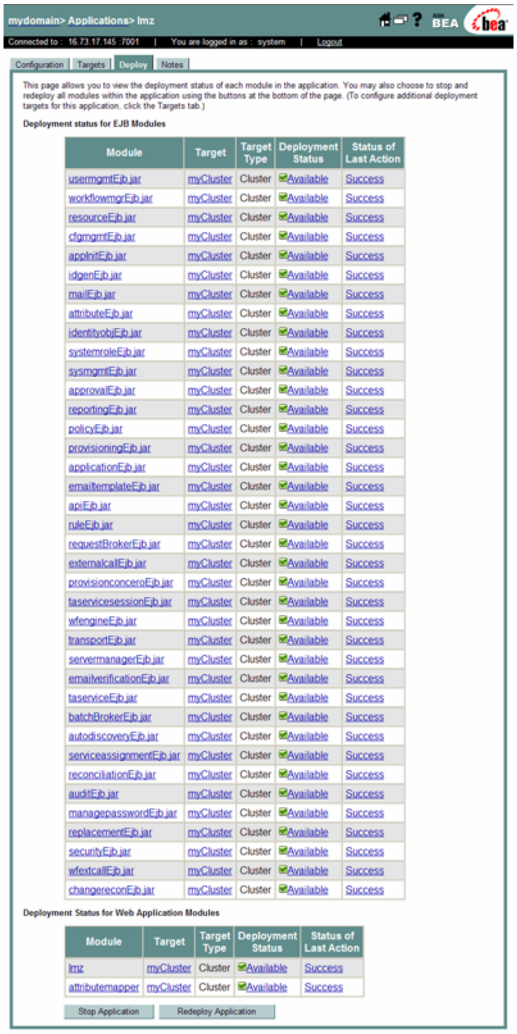
8 Click **Continue**.

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 68 Application page to validate Select Identity deployment



mydomain> Applications> lmz
ASK BEA
bea
Connected to : 16.73.17.145 :7001 | You are logged in as : system | Logout
Configuration
Targets
Deploy
Notes

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

Deployment status for EJB Modules

Module	Target	Target Type	Deployment Status	Status of Last Action
usermgmtEjb.jar	myCluster	Cluster	✓Available	Success
workflowmgrEjb.jar	myCluster	Cluster	✓Available	Success
resourceEjb.jar	myCluster	Cluster	✓Available	Success
cfgmgmtEjb.jar	myCluster	Cluster	✓Available	Success
appInitEjb.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
sysmgmtEjb.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
provisionconceroEjb.jar	myCluster	Cluster	✓Available	Success
taservicesessionEjb.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

Deployment Status for Web Application Modules

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

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 78 and Configuring JMS Settings on page 78.

14 After installing Select Identity, refer to Appendix B, Logging for instructions on configuring the `logging.properties` file.

> Configuring logging is crucial when you install manually. 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 Chapter 6, Configuring Select Identity 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 the 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 `ovsil10n_help_en_US.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 102 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 ***<domain_name>*** → **Deployments** → **Web Application Modules.**

   ➤ Additional product documentation is provided in PDF format in the `/docs` directory on the HP OpenView Select Identity Product CD. Copy these documents to the directory location of your choice.

6 Configuring Select Identity

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

This chapter contains the following topics:

- Configuring Required TruAccess Properties
- Setting Up the Select Identity Keystores
- Recommended Configuration
- Default Values for User Interface Properties
- Custom User Interface Properties
- Internationalization and Localization
- Configuration for Specific Environments or Platforms

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

Configuring Required TruAccess Properties

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

For a complete listing and description of all settings in the `TruAccess.properties` file, see TruAccess Properties on page 165.

How to Set Properties

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

Required Settings

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

Directory Locations

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

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

Staging Directories for One-Time Reconciliation and Import Jobs

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

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

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

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

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

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

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

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

Email Sender

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

The following property controls this setting:

```
truaccess.sender.email
```

The following example illustrates how this setting should be formatted:

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

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

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

Attribute Maximum Length

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

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

Select Identity URL

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

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

Database Settings

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

- Possible values are `mssql` for Microsoft SQL Server, or `oracle` for Oracle.
- Enter the value in lowercase.
- The default setting is `oracle`.

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 the `truaccess.repository.oracle.driver.bea` property to `no`.

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

```
truaccess.upload.filedir
```

Workflow Settings

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

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

Helpdesk Contact Message

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

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

Optional Settings

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

- Customize the graphical interface - see Custom User Interface Properties on page 116.
- Optimize Select Identity - see Recommended Configuration on page 113.

Setting Up the Select Identity Keystores

You must set up and initialize the required keystores before you run Select Identity for the first time, so that the security framework is properly initialized in the database.

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

The Bootstrap Keystore

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

The bootstrap keystore stores the following keys:

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

The Object Migration Keystores

The object migration feature requires the following keystores:

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

Setting Up the Bootstrap Keystore

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

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

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

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

This procedure varies depending on whether or not you are using a Hardware Security Module (HSM). Perform the procedure appropriate to your situation.

Hardware Security Module Procedure for Bootstrap Keystore Setup

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

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

  a Use the HSM utilities to create two secret keys for use with the AES encryption algorithm.

b For both keys, use the same password as the keystore.

2 Create a keystore property file by performing the following steps:

a Run the prepackaged utility `genprop.sh` (Linux) or `genprop.bat` (Windows), using the command line examples below for reference:

— For HSM keystores: `./genprop.sh`

— for HSM (nCipher): `./genprop.sh ncipher nocheck`

b Select option 1 to create a bootstrap keystore.

c When prompted, enter the full path to the property file.

d Make a separate record of the path to the property file.

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

3 Perform this step if you are using **nCipher HSM** for the bootstrap keystore. Skip this step if you are *not* using nCipher HSM:

a Modify the java.security file, `<WAS_INSTALL_DIR>\java\jre\lib\security` by adding the following to the **Provider** list:

```
security.provider.2=com.ncipher.provider.km.nCipherKM
```

b Perform this step on every server if you are installing on a cluster.

Non-HSM Procedure for Bootstrap Keystore Setup

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

1 Execute the packaged tool `genkey.sh` (Linux) or `genkey.bat` (Windows) to create each key in the keystore.

2 Enter the requested information when prompted.

3 Make sure at least one of the keys is using the keystore password. The security framework encryption key must use the keystore password.

Create a keystore property file by performing the following steps:

1 Run the prepackaged utility `genprop.sh` (Linux) or `genprop.bat` (Windows).

2 Select option 1 to create a bootstrap keystore.

3 When prompted, enter the full path to the property file.

4 Make a separate record of the path to the property file.

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

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

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

To set up the bootstrap keystore on Select Identity systems prior to version 4.10, perform the following steps:

1 Create a key in the external keystore, by running the `genkey.sh` or `genkey.bat` utility.

2 Assign this key a key password that is identical to the keystore password. This key is used as the security framework encryption key.

3 Enter the following information in the old keystore property file. Replace the values enclosed by "< >" with the appropriate values:

```
si.keystore.<key alias from old
version>.keyalg=PBEWithMD5AndTripleDES

si.keystore.storetype=JCEKS

si.keystore.keypass.alias=<key alias from new version>

si.keystore.frameworkkey.keyalg=AES/ECB/PKCS5Padding
```

4 If you are using AES keys on a pre-4.10 system, ensure that the `TruAccess.properties` file contains the following setting:

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

Creating the Object Migration KeyStore

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

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

1 Run the `keytool` utility to create a keystore and two keypairs.

2 Generate a certificate request file, as shown in the command line example below, which creates an X509 certificate request file at `./req/myReq.csr` for a certificate at `myKeyAlias` in the keystore:

```
keytool -certreq -keyalg RSA -alias myKeyAlias -file ./req/
myReq.csr-keystore ./ks/myKeyStore -storetype JKS
```

3 You can either send the new request file to your certificate authority for digital signing, or use the following certificate signing commands to sign this certificate locally.

4 Import the signed certificate back to the key store from which you generated the certificate request.

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

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

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

5 Import the certificate into the truststore by performing the following steps:

a Execute `genprop.sh/genprop.bat` to create a property file (select option 2 when prompted).

b Use the Select Identity browser interface to register the property file, under **Security Setup**.

Creating a Trust Store

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

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

Setting TruAccess Properties for the Security Framework

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

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

For Linux/Windows on WebSphere, add or edit the following property:

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

For all other configurations, add or edit the following property:

```
com.hp.ovsi.keypair.provider.classname=com.sun.crypto.provider.SunJCE
```

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

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

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

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

Recommended Configuration

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

The following general settings are recommended:

- When creating the Oracle database connection, always enter the user name in uppercase. This prevents logging errors associated with converting the name to uppercase.
- Set the maximum JVM heap size as **1024** Megabytes or higher.

  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 Configuring Logging for Select Identity on page 59WebLogic Logging Options on page 177 for more information. about configuring the logging.properties file on certain platforms.

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

Extending User Searches

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

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

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

How to Specify Extended User Search Attributes

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

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

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

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

  - truaccess.user.extra=Addr1,PhBus

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Open the `oracle_concero_ddl.sql` script using the database tool or text editor of your choice.

4 Locate and copy every `CREATE VIEW` statement to another, empty, file.

5 Replace every instance of `CREATE VIEW` with `CREATE OR REPLACE VIEW`, and save the resultant script in a new file.

6 Run the new script against the Select Identity database to refresh the views.

Adding Display Columns for Extended Attributes

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

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

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

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

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

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

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

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

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

Disabling the Extended Search Features

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

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

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

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

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

3 Refresh the views as documented on page 115.

Custom User Interface Properties

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

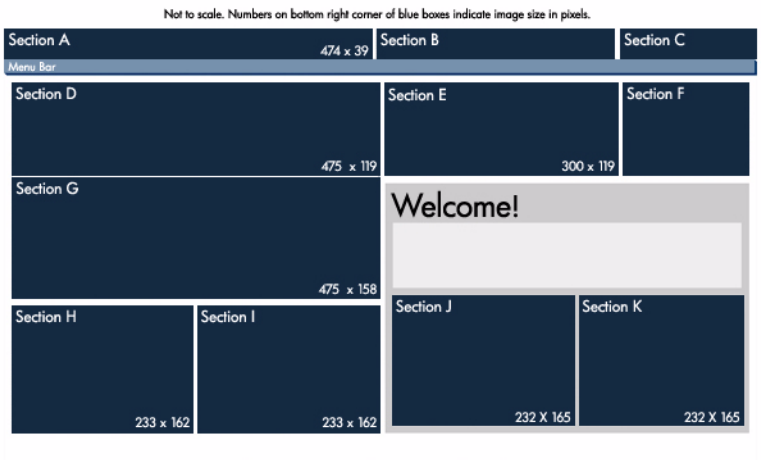
These user interface properties are not required, but they must be present in the `TruAccess.Properties` file and set to the default, if they are not customized.

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

User Interface Sections

The user interface is divided into sections, which are identified in Figure 69. The descriptions of the properties that follow use this diagram for reference.

Figure 69 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 FFFFFF (white).

com.hp.ovsi.ui.masthead.fgcolor

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

com.hp.ovsi.ui.masthead.bgcolor

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

com.hp.ovsi.ui.logo.image.src

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

com.hp.ovsi.ui.common.header.image.src

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

com.hp.ovsi.ui.landing.named.image.src

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

com.hp.ovsi.ui.landing.named-top.image.src

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

com.hp.ovsi.ui.landing.named.image.style

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

com.hp.ovsi.ui.landing.named-top.image.style

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

com.hp.ovsi.ui.landing.common.image.src

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

com.hp.ovsi.ui.landing.box.right.bgcolor

This property will set the background color of Section F.

com.hp.ovsi.ui.landing.users.image.src

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

com.hp.ovsi.ui.landing.requests.image.src

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

com.hp.ovsi.ui.landing.selfservice.image.src

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

com.hp.ovsi.ui.landing.servicestudio.image.src

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

Default Values for User Interface Properties

Default values for these properties are as set below.

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

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

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

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

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

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

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

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

com.hp.ovsi.ui.landing.common.image.src=/images/landing-photo-misc.jpg
com.hp.ovsi.ui.landing.box.right.bgcolor=#036

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

com.hp.ovsi.ui.landing.requests.image.src=/images/

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

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

Internationalization and Localization

Select Identity is internationalized and is able to operate with languages that are supported by the Java Unicode (UTF-8) specification. Internationalization support in Select Identity includes the following capabilities:

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

  XML files used for Select Identity Web services, user import, and rules can take foreign characters as tag or attribute values. The exported XML files through Configuration pages allow foreign characters as well. You can enter foreign characters directly into the XML files as long as they are entered in an editor with UTF-8 encoding enabled. In general, any UTF-8 supported editors can be used for this purpose. However, some editors could store additional hidden characters while saving the file. To ensure that the XML files containing foreign characters are stored correctly, Select Identity recommends using XML editors such as XMLSpy.
- The date and time are displayed in the local format.
- Linguistic sorting is not supported.

Internationalization is supported for Select Identity on the following platforms:

- Application server – WebSphere 6.0.2 and WebLogic 8.1.5
- Database – Oracle 10G
- Connectors – LDAP/UTF-8

➤ Make sure that your database supports the language characters.

Localizing the Date and Time Format

In Select Identity Version 4.12, using Internet Explorer's **Internet Options** to set language preference affects the text and format of dates. In previous versions, specifying language preference affected the field names and messages in the system, but did not affect the date. The underlying date format is not changed, so each user sees the date in their preferred format.

Functional Overview

Select Identity 4.12 provides calendar text for 27 languages. Field names and messages are also available for languages such as Korean and Chinese.

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

The calendar wizard in Version 4.12 uses a clickable calendar for selecting dates, as did previous versions of Select Identity. However, in Version 4.12, the calendar text uses the language that you select in **Internet Options**. Thus, if your preferred language is Japanese, the calendar text displays in Japanese.

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

Custom Date and Time Formats

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

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

Setting the Calendar Language

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

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

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

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

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

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

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

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

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

Refer to Appendix A, TruAccess Properties for more information.

Configuration for Specific Environments or Platforms

The following sections provide platform and environment-specific configurations.

- Tuning the WebLogic Application and Database Servers
- Tuning the Database Server
- UTF-8 Encoding on Oracle 10G
- iPlanet LDAP Configuration
- Set Encoding in Internet Explorer
- Adding Supported Language Fonts

Tuning the WebLogic Application and Database Servers

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

Optimizing JMS Distributed Queues and Weblogic Execute Queues

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

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

The following JMS queues are mainly used during user reconciliation:

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

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

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

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

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

- `hp.ovsi.EJB`

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

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

Queue Name	Thread Count	Thread Increase	Thread Priority
`hp.ovsi.HTTP`	25	5	10
`hp.ovsi.SOAP`	3	0	5
`hp.ovsi.EJB`	16	0	5

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

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

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

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

Tuning the Database Server

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

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

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

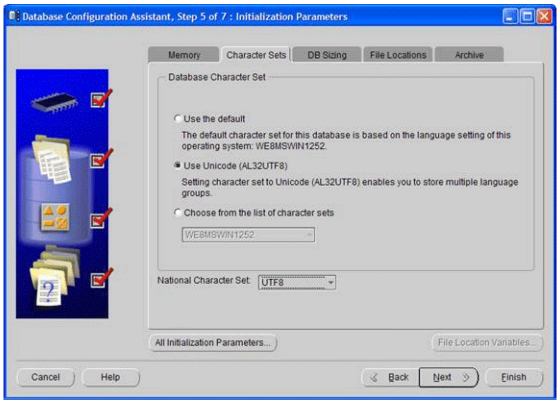
Increasing the number of nodes in the cluster also increases the number of concurrent sessions from Select Identity instances to the database server. The limit of concurrent sessions in the database server should be increased accordingly.

UTF-8 Encoding on Oracle 10G

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

1 For Oracle 10g, open the Initialization Parameters window and select the **Character Set** tab.

2 Select the **Use Uicode (AL32UTF8)** radio button as shown.


Database Configuration Assistant, Step 5 of 7 : Initialization Parameters
Memory
Character Sets
DB Sizing
File Locations
Archive
All Initialization Parameters...
File Location Variables...
Cancel
Help
Back
Next
Finish

Database Character Set

○ Use the default

The default character set for this database is based on the language setting of this operating system: WE8MSWIN1252.

● Use Unicode (AL32UTF8)

Setting character set to Unicode (AL32UTF8) enables you to store multiple language groups.

○ Choose from the list of character sets

WE8MSWIN1252

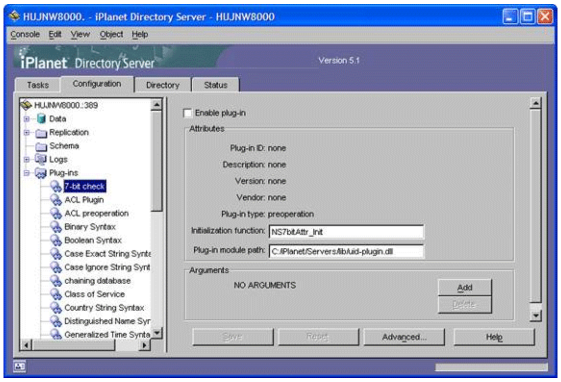
National Character Set: UTF8

iPlanet LDAP Configuration

Perform the following to disable 7-bit ASCII:

1 In iPlanet's Configuration window, expand the plug-ins node and select **7-bit check.**

2 Uncheck **Enable plug-in**, which is selected by default.



□ Enable plug-in

Attributes

Plug-in ID: none

Description: none

Version: none

Vendor: none

Plug-in type: preoperation

Initialization function: NS7bitAttr_Init

Plug-in module path: C:/iPlanet/Servers/lib/uid-plugin.dll

Arguments

NO ARGUMENTS

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:

- 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 Select Identity Home page by setting the following property:

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

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

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

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

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

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

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

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

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

- You can set the following user search criteria:

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

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

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

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

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

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

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

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

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

7 Upgrading Select Identity

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

This section covers the following topics:

- Supported Platforms for Upgrading
- Upgrade Requirements
- Preparing to Upgrade
- Oracle Database Upgrade Procedure

Supported Platforms for Upgrading

The Select Identity upgrade script provided with release 4.12 supports upgrading from release 4.10 or 4.11 on BEA WebLogic 8.1 or IBM WebSphere 6.0.2, with an Oracle 9i or10G or MS-SQL 2000 database, to Select Identity version 4.12. An additional script is provided for upgrading from versions earlier than 4.10.

➤ Select Identity provides migration scripts with each release. If you are upgrading a version prior to version 4.0, contact your HP technical support representative.

Upgrade Requirements

Your Web application server and Select Identity must meet the following requirements to be suitable for upgrading to Select Identity Version 4.12 using this procedure:

- Select Identity version 4.10.
- UNIX-based operating system platform (including Cygwin for Windows-based Select Identity installations).
- Oracle client version 9i or 10G installed, with `SQLplus` or `isql` (as appropriate) in the system path.
- Oracle 10.1.0.4 or later.
- MS-SQL 2000.

➤ Ensure that your Web application server and database server meet the minimum requirements specified in Chapter 2, Requirements.

Preparing to Upgrade

The procedures in this section prepare the Web application server and Select Identity database for upgrading to version 4.12. Follow the instructions corresponding to your system environment.

Downloading the Oracle JDBC Driver

You may need to download and install the Oracle JDBC driver before you can run the upgrade script. JDBC drivers are normally available as part of the Oracle Installation, under `ORACLE_HOME/jdbc/lib/` so the download may not be required.

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

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

Stopping Select Identity Traffic

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

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

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

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

General Web Server Preparation

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

1 Log in to the Web application server administrative or management console.

2 Navigate to the deployed Select Identity lmz.ear application and undeploy it.

3 Shut down the Web application server process and any managed servers/node processes.

4 Log in to the Administrative server at the command line, using an appropriate user ID.

5 Back up the existing 4.0x Select Identity directories and files.

6 Back up the existing TruAccess.properties file in an accessible location. You may need to refer to it when configuring the TruAccess.Properties file after upgrading.

7 Uninstall the old version of Select Identity, as documented in Chapter 9, Uninstalling Select Identity.

8 If you are using an external keystore, refer to the instructions in Setting Up the Bootstrap Keystore on a New Installation or an Installation With Default Keystores on page 110 for information about modifying the TruAccess.properties file.

Oracle Database Upgrade Procedure

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

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

To upgrade Select Identity to 4.12, perform the following steps:

⚠ Before you upgrade, back up the current database and Truaccess.properties file.

1 Ensure that your database server is configured as documented in Configuring an Oracle Database Server on page 25.

2 Ensure that your Web application server is configured as documented in the appropriate installation section in this guide.

3 Set up the Select Identity keystores, as documented in Setting Up the Select Identity Keystores on page 110.

4 Ensure that your Select Identity database is backed up immediately before beginning this procedure.

5 Unzip the upgrade files.

6 Locate the file named setUserEnv.sh and edit the following envionment variables:

- DB_PASS: The password for the above user account.

- DB_PORT: The port the database is listening on. If left blank, this defaults to the appropriate default port for the database being migrated.
- DBSERVER: The IP address or domain name of the Oracle database server.
- DB_USER: The user name for connecting to the Oracle database and accessing the Select Identity schema, typically the same user name that was entered for the database connection when installing the old version of Select Identity.
- DB_VENDOR: The manufacturer of your database, all in lowercase characters (oracle). This setting is optional because the migration script prompts you for this information if you do not provide it here.
- JAVA_BIN: The path and filename of the Java executable used by the Web application server. This optional variable uses JAVA_HOME (if JAVA_HOME has been set), or the system default Java path.
- JAVA_HOME: The path that contains the Java executable used by the Web application server. This optional variable uses the system default Java path if it is not set.
- JDBC_CLASSPATH: The path to the JDBC driver.
- ORAPORT: The database port on which the Oracle database listens for connections, usually 1521. Default is taken from DB_PORT if you have set that variable.
- ORACLE_SID: The connection identifier (from the tnsnames.ora file) for the database server where the Select Identity database is running. This is only used by SQLPlus, not by Java, and is only applicable on an Oracle database.
- TRUACCESS_HOME: The location of the TruAccess.properties file in your existing 4.0.x Select Identity installation. It is critical that this be set correctly.

7. Edit the entry named java.util.logging.FileHandler.pattern in the Logging.properties file, so that it points to a valid directory entry where the Java log files will be written.

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

8. Change directories to the main directory for the upgrade files.

9. Execute the following command if you are upgrading a version prior to 4.10:

   ```
   ./migrator.sh
   ```

   migrator.sh is not needed for 4.10 → 4.1x upgrades.

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

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

10. Execute the following scripts on the Select Identity database schema:

    ```
    oracle_410_411_ddl.sql
    ```

    ```
    oracle_410_411_dml.sql
    ```

    These scripts are located in the following directory:

    ```
    %Migrator%\SQLs\oracle\V4.x\V4.10
    ```

11 After you run the 4.10-4.11 scripts, execute the following scripts on the Select Identity database schema to upgrade to version 4.11.001 (you will not need to upgrade the database beyond this version):

```
oracle_411_411001_ddl.sql
```

```
oracle_411_411001_dml.sql
```

These scripts are located in the following directory:

```
%Migrator%\SQLs\oracle\V4.x\V4.11
```

Troubleshooting a Database Upgrade

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

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

1 The `migrator.sh` script runs each step in numerical order. If a failure occurs during any step, the failure is logged and the script stops. Review the entries in the `migrationlog` table under the Select Identity schema.

2 Log on to SQLplus as the Select Identity owner and run the `oracle_migration_report.sql` script. This shows the status of each step.

3 If the failure occurs during one of the Java upgrade steps, review the screen output or log files in the directory specifed by the `java.util.logging.FileHandler.pattern` entry in the `logging.properties` file.

4 After resolving the problem, resume the script from the last completed step using the -r option. Alternatively, reload the database from backup and restart from the beginning, depending on the issue.

MS SQL Database Upgrade Procedure

To upgrade a Select Identity MS SQL database to version 4.12, perform the following steps:

Before you upgrade, back up the current database and `Truaccess.properties` file.

1 Ensure that your database server is configured as documented in Configuring an MS SQL Database Server on page 27.

2 Ensure that your Web application server is configured as documented in the appropriate installation section in this guide.

3 Ensure that your Select Identity database is backed up immediately before beginning this procedure.

4 Navigate to the following URL and download the JTDS JDBC driver:

```
http://sourceforge.net/project/showfiles.php?group_id=33291
```

5 Use your preferred text editor to configure the script named `setEnv.sh` by setting the following variables:

`TRUACCESS_HOME`: The location of the `TruAccess.properties` file in your existing installation. It is critical that this be set correctly.

`DB_VENDOR`: The manufacturer of your database (`mssql`), in lowercase.

`JDBC_CLASSPATH`: The path to the JDBC driver on the Web Application server, such as the `jtds-1.2.jar` file downloaded in step 4. It is critical that this be set correctly.

`DB_USER`: The user name for connecting to the MSSQL database and accessing the Select Identity schema, typically the same user name that was entered for the database connection when installing the old version of Select Identity.

`DB_PASS`: The password for the above user account.

`DB_PORT`: The database server port on which the MSSQL database listens for connections, usually 1433.

`DBNAME`: The database name for the server where the Select Identity database is running.

6 Execute the following command if you are upgrading from a version earlier than 4.10:

```
./migrator.sh
```

`migrator.sh` is not needed for 4.10 → 4.1x upgrades.

7 Enter the hostname or IP address of the database server if prompted.

The default value is `localhost`.

8 When prompted, enter the database password.

9 Open the MSSQL query analyzer and execute the following scripts on the Select Identity database schema:

```
mssql_410_411_ddl.sql
mssql_410_411_dml.sql
```

These scripts are located in the following directory:

```
%Migrator%\SQLs\mssql\V4.x\V4.10
```

10 After you run the 4.10-4.11 scripts, execute the following scripts on the Select Identity database schema to upgrade to version 4.11.001 (you will not need to upgrade the database beyond this version):

```
mssql_411_411001_ddl.sql
mssql_411_411001_dml.sql
```

These scripts are located in the following directory:

```
%Migrator%\SQLs\mssql\V4.x\V4.11
```

WebSphere Server Upgrade Procedure

You must perform several tasks to upgrade Select Identity on a WebSphere 6.0.2 server, in addition to the Oracle Database Upgrade Procedure on page 129:

1 Create a database user ID for the JMS datastore. Refer to Configuring an Oracle Database Server on page 25 for instructions. You do not need to create a new database when upgrading; only the additional user account is needed.

2 Create or configure the Select Identity bootstrap keystore.

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

If the old environment already has a custom keystore, you can modify the existing keystore to be compatible with Select Identity 4.12.

Create the keystore with a keypair. Refer to Setting Up the Select Identity Keystores on page 110, for instructions.

3 Install the new release of Select Identity (4.12) using the instructions in the Select Identity installation procedure for your Web application server. It is recommended that you use the installer procedure.

4 Add any custom settings that were in the old `TruAccess.properties` file to the new `TruAccess.properties` file.

5 Verify that the resource passwords are still synchronized. For more information, refer to the Select Identity *Online help for Administration*.

If the Resource Passwords	Then
Are still synchronized	Continue.
Are not synchronized	Follow the steps in Synchronizing Resources on page 133.

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

Synchronizing Resources

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

1 Open the Select Identity client.

2 Select **Service Studio** → **Resources** to open the **Resource List** page.

3 Select the first resource in the list.

4 Click **Modify** to open the **Modify Resource** page.

5 Click **Apply** to resynchronize the resource.

6 Click **OK** to save your work and return to the **Resource List** page.

7 Repeat the process until all resources have been resynchronized.

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

8 Integrating Select Identity With Select Audit and Service Desk

This chapter describes integration and interoperation support between Select Identity and Service Desk and Select Audit.

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

This chapter covers the following topics:

- Select Identity–Service Desk Integration
- Select Identity-Select Audit Integration

Select Identity–Service Desk Integration

This section provides information about how to integrate Select Identity 4.12 with Service Desk 4.5, service pack 13.

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

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

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

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

Required Files

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

External Call from Select Identity to Service Desk

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

Workflow Template for Integrated Password Management

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

Functional Scenarios

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

The password management functions are listed below for reference:

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

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

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

Service Call and Workflow Data Exchange and Interaction

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

Accessing the Select Identity Request Status Page from Service Desk

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

Configuration Tasks in Service Desk

Perform the following configuration tasks in the Service Desk administrator console:

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

Task 1: Activating Custom Fields

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

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

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

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

Customizing a Number Field for the Request ID

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

1. In the left panel, navigate to **Data** and select **Custom Fields**.
2. In the right panel, double-click **Service Call** and select **Sc. Number 10** from the **Field** menu.
3. Change the field name to **Request ID**.
4. Select **1234567** as the **Display Format**.
5. Check the **Activate** box.
6. Click the radio button labeled **All Categories**, if it is not selected.
7. Click **OK**.

Customizing a String Field for Request Failure Information

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

1. In the left panel, navigate to **Data** and select **Custom Fields**.
2. In the right panel, double-click **Service Call** and select **Sc. Text 1** from the **Field** menu.
3. Change the field name to **Request Failure Description**.
4. Check the **Activate** box.
5. Click the radio button labeled **All Categories**, if it is not selected.
6. Click **OK**.

Activating a String Field for the Request Link

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

1. In the left panel, navigate to **Data** and select **Custom Fields**.
2. In the right panel, double-click **Service Call** and select **Sc. Text 2** from the **Field** menu.
3. Change the field name to **Request Link.**
4. Check the **Activate** box.
5. Click the radio button labeled **All Categories**, if it is not selected.

Customizing a Short String Field for the Request Type

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

1. In the left panel, navigate to **Data** and select **Custom Fields**.
2. In the right panel, double-click **Service Call** and select **Ser. ShortText 1** from the **Field** menu.
3. Change the field name to **Request Type**.
4. Check the **Activate** box.
5. Click the radio button labeled **All Categories**, if it is not selected.

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

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

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

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

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

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

2 In the right panel, right-click and select **New Service Call Status**.

3 Enter **Failed** in the **Text** field.

4 Select **Accountable** for the **State** field.

5 Repeat step 1 through step 4 to create additional **Status** values if desired.

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

6 Save and close.

Task 3: Creating/Updating a Service Call Template for Select Identity Calls

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

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

1 In the left panel, navigate to **Data** → **Templates** → **Service Call**.

2 Create a new template by right-clicking in the right panel, or double-click an existing template to update it.

3 Name the template **OVSD-OVSI integration Template**.

4 Set the following fields to the specified default values:

- **Status:** Registered
- **Caller:** Current Person
- **Description:** Enter an appropriate description.
- **Information:** Enter any appropriate information.
- **Source ID:** Enter an appropriate ID.

Task 4: Editing the Default Form to Display the Added Fields

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

1 In the left panel, navigate to **Presentation** → **Forms** → **Service Call**.

2 In the right pane, double-click the default form.

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

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

4 Save and close.

Task 5: Creating Database Rules to Send Emails Containing Select Identity URLs

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

When creating database rules in Service Desk, you perform the procedure in a series of wizard pages. Refer to the documentation provided with Service Desk for complete instructions on how to use the rule wizard.

Each database rule contains two actions:

- **Send E-mail Message:** This should include the Select Identity request link in the email body.
- **Update Data:** This should compose the following expression to set into the **Request Link** field:

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

To create the database rules, perform the following steps:

1. Navigate to **Business Logic → Database Rules → Service Call**.
2. In the right pane, right-click and select **New Database Rule**.
3. Create the rules using the example rules in Figure 70 and Figure 71 for reference.
   For **Condition**, specify the exact service call template name, from Task 3.
   For the **URLs**, specify the actual `<host>` and `<port>` of your Select Identity system.
4. Modify the database rules that you created to target the link at the **Request Link** field.

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

   a. Open the **Change/Reset Password** rule in the the **Rule Editor**.
   b. Click **Next** twice to locate the field labeled **Which actions do you want to be performed**.
   c. Click **Add** and select **Update Data**.
   d. Enter a **Name**, at the top of the dialog.
   e. Select **Request Link** from the **Fields** list, and click the icon to the far right of the **Value** field.
   f. In the dialog labeled **Set Value For Set To Request Link**, select **Concatenate** from the **Function** list, then click the icon at the right of the **Value** field under the list.
   g. In the dialog labeled **Set Value for Concatenate**, select the **Fixed Value** and set the value to the following:

      ```
      http://<host>:<port>/lmz/ovsdintg/pwdchangereset.do?userName=
      ```

   h. Click **OK** to return to the dialog labeled **Set Value for Set To Request Link**.

      Notice that the **Value** field contains the URL from step g.

   i. Click the icon to the right of the field labeled **With**, which opens a dialog labeled **Set Value for Concatenate (With)**.
   j. Select **Concatenate** from the Function list again, then click the icon to the right of the **Value** field.
   k. In the dialog labeled **Set Value For Concatenate**, select **Attribute** and click the icon at the right, so that you can select **Caller Account Login Name** from the menu.
   l. Click **OK**.
   m. Click the icon at the right of **With**.
   n. Select the **Concatenate** function again.
   o. Click the icon to the right of **Value**.
   p. Enter `&serviceCallId=` in the **Fixed Value** field, then click **OK**.
   q. Cick the icon to the right of **With**. Select **Attribute**, and click the icon at the right
   r. Enter `ID` into the field and click **OK**.

s Click OK three more times, click **Add To List**, then Click **OK**.

t In the Database Rule wizard, proceed through the remaining pages and save the rule.

u Perform the same steps again for the **Forget Password** rule. For this rule, use the following value for the URL:

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

Figure 70 Forgotten Password Database Rule

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


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

Figure 71 Change Password Database Rule

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


You've made a request to Change or Reset your Password. Please click the links below to
continue the procedure.
<http://<host>:<port>/lmz/ovsdintg/pwdchangereset.do?userName=[Caller;Account;Login
name]&serviceCallId=[ID] >
Regards,
Help Desk
, Attachment Classification: <Unclassified>
Set a value (Update Data) Request Link set to (Concatenate http://<host>:<port>/lmz/
ovsdintg/pwdchangereset.do?userName= With (Concatenate [Caller Account Login name] With
(Concatenate &serviceCallId= With [ID])))
```

Creating a Smart Action

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

1. Navigate to **Business Logic → Actions → Smart Actions → Service Call**.
2. In the right pane, right-click and select **New Smart Action**.
3. Enter the action name in the **Text** field.

4 Select **Internet Explorer** in the **Application** field.

5 Enter the following URL in the **Parameters** field, using the actual host name and port number for your Select Identity system:

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

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

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

1 In the administrator console, navigate to **Service Pages** → **Data** → **Template Settings**.

2 In the right pane, double-click **Service Call**.

3 Change both template settings to the name of the Select Identity calls template (Task 3).

Linking a Service Calls to Select Identity Password Requests

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

1 In the administrator console, navigate to **Service Pages** → **Data** → **Custom Fields.**

2 In the right pane, locate and open the **Service Call** item.

3 Make the following changes:

- Locate one of the fields labeled **Sc. Text n**. Rename the field to **Request Link**.
- Check the box labeled **Activate**.
- Click the radio button labeled **All Categories**.
- Click **OK**.

4 Edit the default form that you edited in Task 4, to display the **Request Link** field:

a Navigate to **Presentation** → **Forms** → **Service Call**.

b Open the **Service Call** form and drag the **Request Link** from the **Attributes** to the form.

c Save and close the form.

OpenView Select Identity Configuration Tasks

In Select Identity, perform the following steps to configure Service Desk integration. Refer to the Select Identity *Online Help for Administrators* and *Administration Guide* for additional information:

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

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

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

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

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

Task 2: Setting the External Call Parameters

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

1 Open the Select Identity **Service Studio** menu and select **External Calls**.

2 Locate and select the **SDIntegrator** external call.

3 Click **Modify** to change the parameter values.

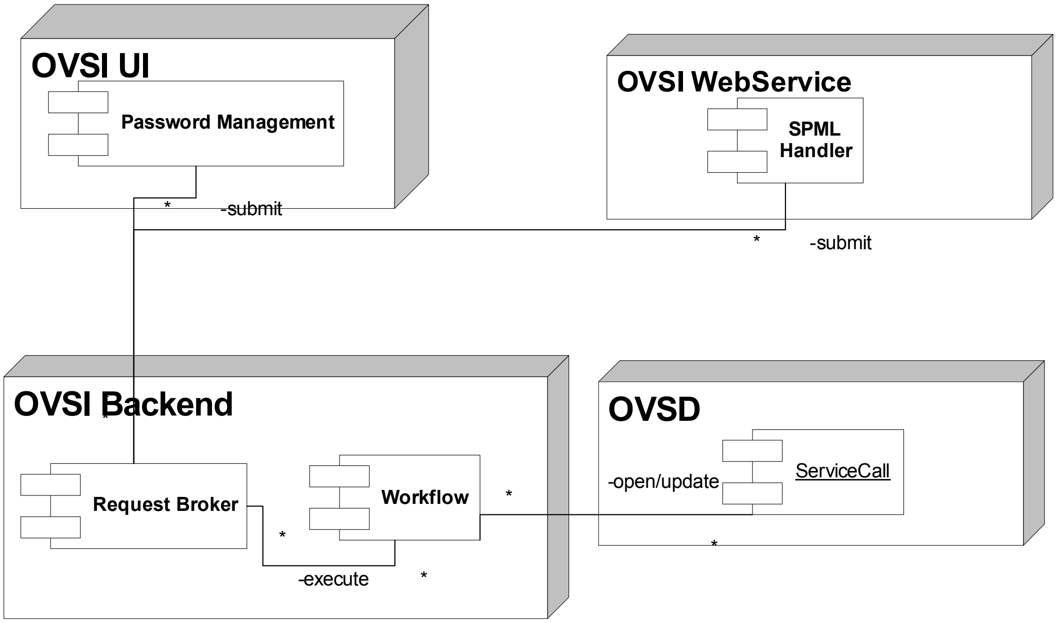
4 Make the following changes to the parameters below:

- **URL:** The hostname or IP address of the Service Desk server (the port is not needed).
- **Login ID:** The Service Desk administrator. Set this to **system**.
- **Password:** The password for the **System** Login ID. The default password for **System** is `servicedesk`.
- **Template name:** The service call template name used for the integration. Enter the template name from Service Desk configuration Task 3.

System Context

Figure 72 shows integration in its architectural context. The Select Identity user interface and back-end component dependencies with Service Desk are displayed as well as the communication between the components.

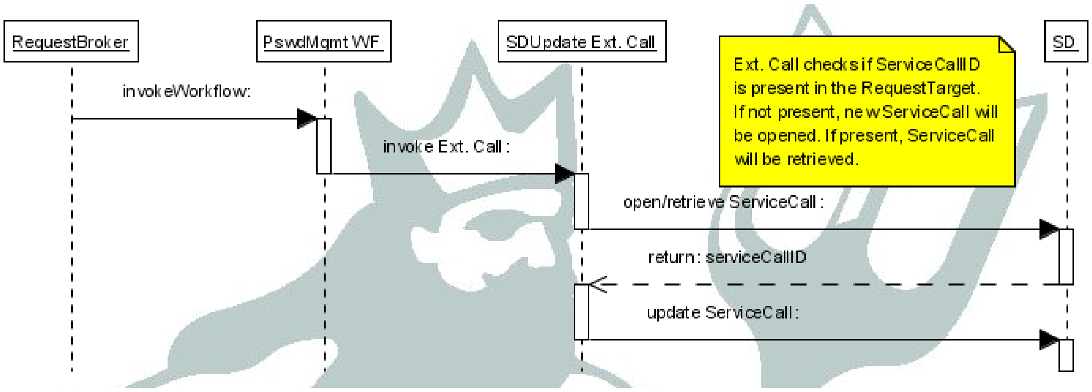
Figure 72 Select Identity-Service Desk integration context



Process Flow

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

Figure 73 Service Call process flow


RequestBroker
PswdMgmt WF
SDUpdate Ext. Call
SD
invokeWorkflow:
invoke Ext. Call :
Ext. Call checks if ServiceCallID is present in the RequestTarget. If not present, new ServiceCall will be opened. If present, ServiceCall will be retrieved.
open/retrieve ServiceCall :
return: serviceCallID
update ServiceCall :

Select Identity-Select Audit Integration

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

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

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

Requirements and Recommendations

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

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

Setting Up Integration in Select Identity

Select Identity configuration steps are minimal:

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

The Select Audit Agent

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

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

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

TruAccess Properties

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

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

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

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

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

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

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

Configuring the Select Identity Database

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

This operation can be performed in two ways:

- Remove the comment marks (indicated by the -- character) from the line at installation time, so that the row will be inserted when the `dml` is run. If you do not invoke this line at installation time, you must run it manually using a tool such as SQLPlus.
- Insert the following fields manually into the `AuditCfgEntry` table:
  - **auditCfgEntryId**
  - **eventType**
  - **status**
  - **namingFactory**
  - **namingProvider**
  - **connectionFactoryName**
  - **destinationName**
  - **destIsTopic**
  - **auditCfgId**
  - **disPosition**
  - values (`2, 0, 1, null, 't3://localhost:7001', 'java:comp/env/jms/auditProcessorQCF', 'java:comp/env/jms/auditSelectAuditQueue', 0, 1, 1`);

Setting Up Integration in Select Audit

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

Integration can be set up in the following scenarios:

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

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

Data Filtering and Report Access Matrices

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

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

Report Name	**SI User**	**Non-SI User**	**SI Not Available**	**Administrators**	**Auditors**
Account Change	If allowed in SI on certain report types (see table below), will have these permissions on related reports: • Read, • Execute, • Schedule, • Adhoc	Denied	Denied	Full permissions including: • Read, • Write, • Delete, • Execute, • Schedule, • Adhoc, • View • Grant • Revoke	• Read • Execute • Schedule • Adhoc
Account Events					
Administrator					
Change History					
Configuration					
Password Management					
Security Events					
Service					
System Activity					
User Activity					
User Summary					
Workflow Events					
Attestation	Read, Execute, Schedule, Adhoc				
Data Integrity	Read, Execute, Schedule, Adhoc				
Raw Message	Denied				

Report Mapping

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

.

To be see this report in Select Audit	**Users need *any* of these report types in Select Identity.**
Account Change Report	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Account Events Report	AuditUser
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
Administrator Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserHint
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Change History Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination

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

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

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

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

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

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

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

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

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

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

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

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

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

9 Uninstalling Select Identity

This section covers the following topics:

- Auto-Uninstalling Select Identity
- Uninstalling Select Identity Manually on IBM WebSphere 6.0.2
- Using the Uninstaller
- Manually Uninstalling from the WebLogic Server
- Uninstalling the Select Identity Database

Auto-Uninstalling Select Identity

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

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

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

⚠ You cannot reinstall Select Identity if the `.ear` file is still deployed on the Web Application server. Be sure to remove it before attempting to reinstall.

Uninstalling Select Identity Manually on IBM WebSphere 6.0.2

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

1 Undeploy the Select Identity was6_lmz.ear application from the **Enterprise Applications** page. See Undeploying the Online Help or Another Application on page 162.

2 Delete the following items. Delete only those instances of each item that are specific to Select Identity:

- The mail provider and session
- JDBC provider
- JMS queue connection factory
- JMS topic connection factory
- JMS queues
- JMS topics

- JMS activation specifications
- Service integration bus (`OVSIBus`)
- Bus destinations

Undeploying the Online Help or Another Application

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

1. Locate the application to remove on the **Enterprise Applications** page.
2. If the application **Status** is **Started** (green arrow), click **Stop** to shut it down; if **Stopped**, skip this step.
3. Confirm that the application status is **Stopped**.

- Select the application that you just stopped, and click **Uninstall** to remove the application from the WebSphere server.

Using the Uninstaller

To use the uninstaller to remove Select Identity:

1. Run the `Uninstall` Select Identity`.exe` (on Windows) or `Uninstall` Select Identity`.bin` (on Linux) to launch the wizard. These files reside in the Select Identity home directory on the Web application server.
2. Follow the prompts in the uninstaller.
3. When complete, the wizard removes the `.ear` file, data source, connection pool, and mail session.

Manually Uninstalling from the WebLogic Server

The following sections describee how to manually remove Select Identity from a WebLogic server.

- Deleting the EAR File
- Deleting the Connectors
- Deleting the Data Source
- Deleting the Connection Pool
- Deleting the Mail Session
- Deleting the JMS Connection Factories
- Deleting the JMS Queues and Topics
- Deleting the JMS Servers
- Deleting the JMS Stores
- Deleting the Templates (Cluster)

- Deleting the Distributed Destination (Cluster)

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 **Delete** (🗑) 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, uninstall the Select Identity 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 theSelect Identity data source:

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

Uninstalling the Select Identity Database

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

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

Uninstalling Oracle

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

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

```
drop user Select_Identity_database_username cascade
```

A TruAccess Properties

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

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

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

TruAccess Properties Summary

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

For information about TruAccess properties that you use to customize the Select Identity user interface, see Custom User Interface Properties on page 116.

For information about TruAccess properties that you use to customize the Select Identity date and time format, see Localizing the Date and Time Format on page 119.

General Settings

- **truaccess.dateformat=yyyy-MM-dd**

  Specifies the date format throughout the Select Identity system.

- **truaccess.timestampformat=yyyy-MM-dd hh:mm:ss a**

  Specifies the time stamp format throughout the Select Identity system.

- **truaccess.version=<version number>**

  Specifies the Select Identity version number. *Do not change this value.*

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

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

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

  Specifies the default Select Identity policy identifier.

- **truaccess.expirationProcessPeriod=30**

  Specifies the time interval prior to automatic account expiration (in days). The default is 30days. At this point, a designated manager is sent a reminder notification.

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

  Specifies the default Select Identity system administrator user ID and administrative role.

- **contact_helpdesk=Please contact the helpdesk.**

  Provides the text for an error message that displays if the user cannot log on to the Select Identity client.

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

  The URL for online assistance and documentation or support.

- **truaccess.homepage=http://www.hp.com com.hp.si.clientName=HP**

  Client Name. Specifies your home page and your company name when uncommented.

- **com.hp.ovsi.i18n.labels.debug = false**

  Debug resource bundle strings

- **ui.locale.date.format=MM/dd/yyyy**

  Defines the preferred date format in the user interface. This is specified as a date pattern described in `java.text.SimpleDateFormat`. This value can be left empty in order to use the default format.

- **com.hp.si.user.attributes.maxlength=10**

  Attribute Max Length default value in KB.

- **si.autodiscovery.audit=false (hidden, default to false)**

  Whether to audit user import

- **si.serviceassignment.server.num = X**

  Hidden, defaults to 3, set > = 4 if the number of nodes in cluster is more than 3.

- **hp.si.idgen.increment=200**

  This property controls the size of reserved Select Identity-generated database table row IDs on each server. For MS SQL Server, a setting of 200 is recommended to enable the database to manage concurrent processing and locking as efficiently as possible.

Asynchronous Provisioning Delay

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

  Specifies the delay (in seconds) for asynchronous provisioning.

Audit Settings

These include settings for exchanging data with Select Audit.

- **truaccess.audit.detail=off**

  Specifies whether to increase the level of detail stored for audit history reports. If set to **on**, performance may be affected.

- **com.hp.ovsi.audit.saud.connector.host=localhost**
  com.hp.ovsi.audit.saud.connector.port=9979
  com.hp.ovsi.audit.saud.connector.client_id=unknown
  com.hp.ovsi.audit.saud.connector.retries=1
  com.hp.ovsi.audit.saud.connector.pool_size=1
  com.hp.ovsi.audit.saud.connector.intervals=500

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

Authentication Settings

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

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

Auto User Import Settings

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

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

Batch Processing Settings

- **truaccess.batch.inprogresstimeout=18000000**

  Specifies the time-out and owner for batch processing for the user import facility. To specify common batch processing, set `truaccess.batch.ownerkey` to **0**, or you can specify a specific WebLogic server.

- **truaccess.batch.reportdir=c:/temp/reports**

  Specifies the policy to pick up the batch files for the user import facility and the directory to which reports are written.

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

  Determines the maximum batch generated file size (in bytes) to be sent as attachment by Select Identity.

- **truaccess.batch.reportdir=c:/temp/reports**
  truaccess.reports.printView.maxRecords = 1000

Specifies the location to save a batch generated file if its size exceeds maximum size limit defined by `truaccess.batch.report.file.maxsize` and the maximum number of records that can be stored by Select Identity.

- **truaccess.sqlQueryInListSize=200**

  Specifies the maximum number of positional parameters to be used in a SQL query "in" list or array as in the query **`select ... where a in (?,?,?,?...)`**

- **truaccess.batchQuerySize=500**

  Specifies the maximum number of queries to be executed in a single batch insert or update statement.

- **si.serviceassignment.batchsize=xx (hidden, default to 20)**

  Number of users to process in one JMS message

Bulk Upload Settings

- **truaccess.upload.filedir=c:/temp**
  truaccess.upload.maxfilesize=10485760

  Specifies a temporary directory that the bulk import process uses. It specifies the maximum upload file size (in bytes) as well.

Cache Settings

- **si.cache.service.local=true**

  Determines whether or not to turn the resource cache on (hidden and default to true)

- **si.cache.resource.localmax=50**

  Maximum entries in service cache (hidden and default to 50)

- **si.cache.service.local=true (hidden and default to true)**

  Whether to turn the service cache on.

  si.cache.service.localmax=100 (hidden and default to 100)

  Max entries in service cache

- **si.cache.service.local.checkdb=false (hidden and default to false)**

  Whether the cached entry should be compared against database.

- **si.cache.taattrdef.local=true (hidden and default to true)**

  Whether to turn attribute definition cache on.

- **si.cache.taattrdef.localmax=300 (hidden and default to 100)**

  Max entries in service cache.

- **si.cache.taattrdef.local.checkdb=false (hidden and default to false)**

  Whether the cached entry should be compared against database

Connector Schema Directory

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

Determines the connector schema directory.

Email Settings

- **truaccess.email.new.timeinterval=120**

  Specifies the time interval (in seconds) that the email daemon uses to send new email.

- **truaccess.email.retry.timeinterval=900**

  Specifies the time interval (in seconds) that the email daemon uses for sending new email if initial attempts were unsuccessful.

- **truaccess.email.retry.maximum=3**

  Specifies the maximum number of retry attempts for sending email. Setting this to **0** causes Select Identity to retry indefinitely.

- **truaccess.email.to.empty=off**

  Specifies whether to send email if the recipient's email address cannot be determined. Specify **on** to send email to the administrator in this event. Specify **off** to suppress this feature.

- **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=smtp

  Determines whether and how Select Identity sends email. If `truaccess.email` is set to **off**, no email is sent.

  Ensure that `truaccess.email.batchcount` is set to less than 1000 for systems running with Oracle databases.

- **truaccess.sender.name=SelectIdentity**
  truaccess.sender.email=selectidentity@hp.com

  Specifies a default name and email address to use if the sender's information cannot be determined.

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

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

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

  Specifies the email address pattern used by Select Identity to validate email addresses.

- **"truaccess.job.retry.timeinterval=600**
  truaccess.job.retry.maximum=3

Specifies the time interval (in seconds) that Select Identity will wait between attempts to execute a function, such as deleting a user, and the maximum number of retries allowed before the request fails.

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

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

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

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

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

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

External Calls Settings

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

  Specifies the attributes for external calls.

JNDI Data Source Settings

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

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

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

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

Localization Settings

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

  Supported locales (US English is the default).

Notification Event Settings

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

  The default email template for Approve Notification Event

Operations Templates

- **truaccess.fixedtemplate.passwordreset=SI\ Password\ Change\Provisioning**
  truaccess.fixedtemplate.terminate=SI\ Provisioning\ Only
  truaccess.fixedtemplate.disable=SI\ Provisioning\ Only
  truaccess.fixedtemplate.enable=SI\ Provisioning\ Only
  truaccess.fixedtemplate.expiration=UserAccountExpirationWF
  truaccess.fixedtemplate.securityviolation=SI\ Email\ Only
  truaccess.fixedtemplate.modifyprofile=SI Provisioning Only
  truaccess.fixedtemplate.passwordexpirenot=SI\ PasswordExpire\Email
  truaccess.fixedtemplate.passwordexpire=SI\ Provisioning\ Only
  truaccess.fixedtemplate.disable.terminate=SI\ Provisioning\Only
  truaccess.fixedtemplate.reconciliation=ReconciliationDefaultProcess
  truaccess.fixedtemplate.recon_enable=ReconciliationDefaultProcess
  truaccess.fixedtemplate.recon_terminate=ReconciliationDefaultProcess
  truaccess.fixedtemplate.recon_disable=ReconciliationDefaultProcess
  truaccess.fixedtemplate.recon_disable_terminate=ReconciliationDefaultProcess
  truaccess.fixedtemplate.bulk_default=ReconciliationDefaultProcess
  truaccess.fixedtemplate.bulk_move=SI Provisioning Only Bulk

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

Page Redirect Timeout

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

  Specifies the timeout (in seconds) for page redirects.

Reconciliation Settings

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

  Specifies the maximum number of users updated during reconciliation.

- **truaccess.recon.rootdir=c:/temp/reconroot**
  truaccess.recon.stagingdir=c:/temp/reconstaging
  truaccess.recon.backupdir=c:/temp/reconbackup
  truaccess.recon.filename.timeformat=yyyy_MM_dd_H_mm
  truaccess.recon.task.check.threshold=3

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

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

  truaccess.recon.check_serviceassignment_authadd=false
  truaccess.recontimer.startdelay=30
  truaccess.recontimer.timeinterval=30

- **truaccess.reconcliation.postprovpolicy=1**

Specifies when Select Identity performs post-provisioning reconciliation. Specify one of the following values:

Perform SI Update if:

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

- **si.recon.policybased=true (hidden, default to true)**

  Policy Based Recon Switch

- **si.recon.server.num = X**

  Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.

- **si.recon.processor.num = X**

  Hidden, default set to 8.

- **truaccess.bulk.postprovpolicy=2**

  Specifies when Select Identity performs post-provisioning after a bulk upload. Specify one of the following values:

  Perform SI Update if:

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

- **com.jp.ovsi.spml.resourcename.separator=+**

  Select Identity reads data files from the `reconroot` directory. The file name should begin with an underscore (_). If the property above is set as shown, then the file placed on `reconroot` will begin with a "+."

Report Settings

- **com.hp.ovsi.volumedata.report.compressed = true**

  Controls whether reports are compressed before being emailed to recipients.

  `true` = reports are compressed

  `false` = reports are not compressed

- **truaccess.generatedFileSizeLimit=2000000**

  Indicates the size of the files (in bytes) that are generated by the reporting subsystem. This is a soft limit; the actual file size may exceed this by a small amount.

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

  Indicates the column(s) on which sorting takes place in the user detail configuration report and the order of the sort.

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

  Specifies the maximum email size of a batch report.

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

  Specifies the number of days for which request status is retrieved by default in the **From** field of the **Request Status** page. If this property is not specified, the value defaults to **14**.

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

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

Repository Type Settings

- **truaccess.repository.type=oracle**

  Set this property to the appropriate database type (`oracle` or `mssql`)

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

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

Schema Settings

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

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

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

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

Search Settings

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

  Specifies the user search criteria fields that are available for selection as search filters. The fields are separated by commas. Use "_Status" to search for the user state status.

- **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. This property must be modified if you change the search results columns as documented in Extending User Searches on page 114. It does not add attribute columns.

- **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.max = 300**

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

Security Framework and Keystore Settings

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

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

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

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

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

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

- **com.hp.ovsi.keypair.provider.classname=com.sun.crypto.provider.SunJCE**

  Set this property to the correct keystore engine provider classname, as follows:

  - `com.sun.crypto.provider.SunJCE` for Sun.
  - `com.ibm.crypto.provider.IBMJCE` for IBM.

Self-Registration Settings

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

  Specifies whether the **Schedule Time** field in the self-registration form will be visible.

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

  Determines the text seen in self-registration instructions.

- **com.hp.ovsi.selfreg.cancel.action.url = http://www.hp.com**

  Specifies the URL used when self-registration is cancelled.

Server Management Settings

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

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

User and Account Settings

- **truaccess.disable=true**
  truaccess.disabledays=1
  truaccess.system.terminate.administrator.userId=sisa
  truaccess.system.expire_notification.administrator.userId=sisa

  Specifies the account disable period before the account is terminated. Set the `truaccess.disable` property to **true** if the user needs to be disabled before termination occurs.

- **si.serviceassign.evaluation=1**

  Specifies whether to evaluate user attributes or service assignments. Specify one of the following values (1 is the default).

  0— Evaluate all (attributes and service assignments)
  1— Skip services previously assigned to users

- **truaccess.singlevalue.attribute.delete=false**

  Specifies whether a user's single value attributes should be deleted.

If this is set to `true`, an error will result during a terminate user operation unless the following properties are all set to `false` as shown below:

truaccess.singlevalue.attribute.delete.FirstName=false
truaccess.singlevalue.attribute.delete.LastName=false
truaccess.singlevalue.attribute.delete.Email=false
truaccess.singlevalue.attribute.delete.Password=false

- **truaccess.user.extra=PhBus, PhHome, PhMobile, Company,Department, DOB, Addr1, Addr2, City, State, Zip, Country, CostCenter, ExpirationDate, UserDescription, _Status**
  truaccess.user.extra.State.column=State
  truaccess.user.extra.City.column=City
  truaccess.user.extra.Country.column=Country
  truaccess.user.extra.Zip.column=Zip
  Use the automatic matching feature for PersonNumber
  truaccess.user.extra.PersonNumber.column=PersonNumber

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

- **com.hp.ovsi.forgetpassword.autogenerate=true**

  Determines if a password is automatically generated for the user if the user indicates the password has been forgotten. If `forgetpassword` is set to true, Select Identity automatically generates a password when the user forgets the password, and provides the correct answers to the Challenge/Response question. If set to false, users must reset their own password.

- **com.hp.ovsi.modify.disableduser=false**

  Select Identity allows modification of a disabled user by default. Set this property to **false** if this should not be allowed.

- **com.hp.si.user.attributes.dropdown.constraint.count=10**

  User Attribute drop-down value count. This property determines if a drop-down list displays or a search is used when a user selects an attribute which contains a constraint list. If the number of constraint values for the attribute is below the property value (such as 50 in the example), a drop-down list will appear on the registration or approval form. If the number of constraint values is equal to or greater than the property value, a search will be required for selecting values from the list.

- **com.hp.ovsi.parentrequestlist.contextcheck=False**

  Returns only those requests that the admin is authorized to view on the Request Status page by default. This is set to false for performance reasons. Change the value to true to enable this behavior.

Web Service Request Settings

- **com.hp.si.webservice.auth.resource=ldap**
  com.hp.si.webservice.auth.ldap.accessurl=ldap://localhost:389
  com.hp.si.webservice.auth.ldap.uidattr=uid
  com.hp.si.webservice.auth.ldap.suffix=ou=People,dc=trulogica,dc=com
  com.hp.si.webservice.auth.ldap.needssl=false

  Specifies external authentication for Web Service requests when uncommented

- **si.recon.webservice.report.generate=2**

  Whether to generate and send report for Web Service reconciliation:

  - 0 - Never

- 1 - Only Initial Report when no request is processed
- 2 - always

Workflow Settings

-
  ```
  com.hp.ovsi.default.workflowtemplate.bulk.addnewuser
  =SIBulkOneStageApproval
  com.hp.ovsi.default.workflowtemplate.bulk.addservice
  =SIBulkOneStageApproval
  com.hp.ovsi.default.workflowtemplate.delegated.addnewuser
  =SI\ OneStageApproval
  com.hp.ovsi.default.workflowtemplate.delegated.addservice=SI\ OneStageApproval
  com.hp.ovsi.default.workflowtemplate.delegated.modifyuser
  =SI\ Provisioning\ Only
  com.hp.ovsi.default.workflowtemplate.delegated.deleteservice
  =SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.disableservice
  =SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.enableservice
  =SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.delegated.moveuser
  =SIBulkOneStageApproval
  com.hp.ovsi.default.workflowtemplate.delegated.viewservice
  =SI\ Provisioning\ Only com.hp.ovsi.default.workflowtemplate.recon.addservice
  =ReconciliationDefaultProcess
  com.hp.ovsi.default.workflowtemplate.recon.deleteservice
  =ReconciliationDefaultProcess
  com.hp.ovsi.default.workflowtemplate.self.addnewuser=SI\ OneStageApproval
  com.hp.ovsi.default.workflowtemplate.self.addservice=SI\ OneStageApproval
  com.hp.ovsi.default.workflowtemplate.self.modifyprofile=SI\ Provisioning\ Only
  com.hp.ovsi.default.workflowtemplate.self.viewprofile=SI\ Provisioning\ Only
  com.hp.ovsi.default.workflowtemplate.service.change.recon
  =SI\ Provisioning\ Only
  ```

  The default workflow templates for User Request Events

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

XML Mapping File

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

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

B Logging

WebLogic Logging Options

This section documents the configurable logging options for BEA WebLogic installations. For more detail about each option, refer to the `Logger` class in the Java 2, Standard Edition, v 1.4.12 API Specification.

HP OpenView Select Identity implements `java.util.logging.Logger`, as defined by the Java 2, Standard Edition, v 1.4.12 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.

- **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 177, 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
  ```

  ```
  # Properties for the FileHandler
  java.util.logging.FileHandler.pattern = c:/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.trulogica.truaccess.util.persistence.PersistenceManager.level=FINEST
```

```
com.trulogica.truaccess.util.scheduler.dao.BatchDAOImpl.level=FINE
```

```
com.trulogica.truaccess.reconciliation.util.ReconciliationTimerTask.level=WARNING
```

```
com.trulogica.truaccess.util.SMTPTimerTask.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.trulogica.truaccess.connector.ldap.ldapv3.LDAPConnector.level =
FINE
```

Index