

HP Select Identity

Software Version: 4.20

Installation Guide

Document Release Date: September 2007
Software Release Date: September 2007



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© 2002-2007 Hewlett-Packard Development Company, L.P.

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

This product includes software developed through the DOM4J Project (<http://dom4j.org/>). Copyright © 2001-2005 MetaStuff, Ltd. All Rights Reserved.

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

This product includes software developed by Sun Microsystems (<http://www.sun.com>). Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software licensed under the Mozilla Public License version 1.1. Copyright © 1998-2004 The Mozilla Organization (<http://www.mozilla.org/MPL/>).

This product includes software developed by Free Software Foundation, and is licensed under the GNU Lesser General Public License Version 2.1, February 1999. Copyright © 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

The JBoss® app server is Copyright © 2000-2006, Red Hat Middleware LLC and individual contributors, and is licensed under the GNU LGPL.

Portions Copyright © 2001-2004, Gaudenz Alder All rights reserved.

Copyright © 2002-2006, Marc Prud'hommeaux <mwp1@cornell.edu> All rights reserved.

This product includes copyrighted software developed by E. Wray Johnson for use and distribution by the Object Data Management Group (<http://www.odmg.org/>). Copyright © 1993-2000 Object Data Management Group, All rights reserved.

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

This product includes software developed by Sam Stephenson. Copyright © 2005 Sam Stephenson.

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

The Select Identity product CD contains a `license` directory where you can find the license agreements for each of the third-party products used in this product.

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software 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 and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

| | | |
|----------|--|----|
| 1 | Introduction | 13 |
| | System Architecture | 13 |
| | Security and Communication | 15 |
| | Java 2 Security | 16 |
| | Keystores | 16 |
| | Integration | 16 |
| | Connectors | 16 |
| | Internationalization | 17 |
| | Technical Qualifications for Installing Select Identity | 17 |
| | Variable Conventions Used in this Document | 18 |
| 2 | Requirements | 19 |
| | Installation Process Overview | 19 |
| | Reviewing Minimum Requirements | 20 |
| | Supported Configurations | 20 |
| | Database Server Requirements | 21 |
| | Unicode Encoding | 22 |
| | BEA WebLogic Server Requirements | 22 |
| | IBM WebSphere Server Requirements | 23 |
| | Select Identity Interface Requirements | 23 |
| | Ports Required for Firewall Configuration | 24 |
| 3 | Database Server Configuration | 25 |
| | Configuring an Oracle Database Server | 25 |
| | Configuring an MS SQL Database Server | 27 |
| 4 | Installing Select Identity on IBM WebSphere 6.1.x | 31 |
| | Introduction | 31 |
| | Prerequisite Configuration and Verification | 31 |
| | Prerequisites for All Installations | 32 |
| | Prerequisites Specific to Cluster Installations | 32 |
| | Installation to Directories with Embedded Spaces | 32 |
| | Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security | 33 |
| | Create a Select Identity Administrator | 33 |
| | Add the Monitor and Configurator Roles for the Select Identity Administrator | 34 |
| | Append Permissions to the app.policy File | 34 |
| | Clusters | 34 |
| | Stand-alone Servers | 35 |

| | |
|--|----|
| Move All External Call JAR Files | 35 |
| Secure the WebSphere Environment and Limit Access | 35 |
| Secure the WebSphere Environment | 35 |
| Allow Only Authorized Users to Access Cos Naming Service | 36 |
| Preparing to Install Select Identity | 36 |
| Important Installation Information | 37 |
| For all WebSphere 6.1.x Configurations: | 37 |
| For Clusters: | 38 |
| Using the Select Identity Installer | 38 |
| Auto-Installation Procedure | 38 |
| If Auto-Installation is Not Successful | 48 |
| Manual Installation Procedures | 48 |
| How This Section is Organized | 48 |
| Creating Directories and Copying Files | 49 |
| Configuration Scope | 50 |
| Creating J2C Authentication Data Entries | 50 |
| Creating the JDBC Providers | 51 |
| MS-SQL Configuration: Changing the Default Transaction Isolation Level | 53 |
| Creating the Data Sources | 53 |
| Create the First Data Source | 54 |
| Create the Second Data Source for JMS | 55 |
| Configuring the Select Identity Service Integration Bus | 56 |
| Setting Bus Security | 57 |
| Adding Bus Members | 57 |
| Creating JMS Queue Bus Destinations | 58 |
| Creating JMS Topic Bus Destinations | 60 |
| Creating JMS Resources | 60 |
| Creating JMS Queue Connection Factories | 61 |
| Creating JMS Topic Connection Factories | 62 |
| Creating the JMS Queues | 62 |
| Creating the JMS Topics | 64 |
| Creating Activation Specifications | 65 |
| Configuring the Select Identity Mail | 67 |
| Configure the Select Identity Mail Provider | 67 |
| Configure the SMTP Protocol Provider | 67 |
| Configuring the Select Identity Mail Session | 68 |
| Deploying Select Identity and the Online Help | 69 |
| Updating The Select Identity Application Settings | 70 |
| Set the Class Loader Mode and WAR Class Load Policy | 71 |
| Set the Transaction Timeout | 71 |
| Enabling the Startup Bean Service | 72 |
| Configuring the Java Virtual Machine | 73 |
| Configuring Logging for Select Identity | 74 |
| Configuring Global Security | 74 |
| Verifying the Select Identity Installation | 75 |
| Updating the Classloading Strategy of attributemapper.war | 76 |
| Configuring WebSphere for Mutual Authentication | 78 |

| | |
|---|-----|
| Prerequisites | 78 |
| Procedure – Single Server | 79 |
| Set Up Security | 79 |
| Set Up the Environment | 84 |
| Set Up the Servers | 86 |
| Procedure – Clustered Servers | 91 |
| Set Up Security | 91 |
| Set Up the Environment | 97 |
| Set Up the Servers | 99 |
| Logging In to Select Identity | 105 |

5 Installing Select Identity on BEA WebLogic 9.2 107

| | |
|---|-----|
| Introduction | 107 |
| Single-server or Cluster Installation | 107 |
| Checking Your Installation Environment | 108 |
| Important Installation Information | 108 |
| Prerequisite Configuration | 109 |
| Pre-Installation Tasks for Installing Select Identity on WebLogic | 110 |
| Enable the Combined Role Mapping | 110 |
| Create the SIAdministrators Group | 111 |
| Create the siadministrator User | 111 |
| Create the SIAdministrator Security Role in the Domain | 112 |
| Select Identity Installer Process Summary | 113 |
| Select Identity Installer Procedure | 114 |
| Select Identity Manual Installation Procedure | 122 |
| Creating Select Identity Directories and Copying Installation Files | 122 |
| Creating the WebLogic Startup Script Manually on a Single Server | 124 |
| Starting WebLogic | 126 |
| Configuring the Mail Session | 127 |
| Configuring JMS Settings for a Single Server and Cluster Servers | 128 |
| Creating the JMS System Module | 128 |
| Creating JMS Connection Factories: Queue and Topic | 129 |
| Creating Queue Connection Factories | 129 |
| Creating Topic Connection Factories | 131 |
| Configuring the JMS File Store | 132 |
| Creating the JMS Server | 133 |
| Configuring the Paging Store | 134 |
| Creating JMS System Resources: Destination Key, Topics, and Queues | 135 |
| Creating the Destination Key | 135 |
| Creating Topics | 136 |
| Creating Queues | 138 |
| Configuring the JTA Settings | 141 |
| Creating a JDBC Connection Pool | 141 |
| Configuring a JDBC Connection Pool and Data Source | 144 |
| Modifying the WebLogic Server Class Path | 145 |
| Enabling Anonymous Admin Lookup | 147 |

| | |
|---|------------|
| Starting the WebLogic Server | 147 |
| Deploying the Select Identity Application. | 148 |
| Deploying the Select Identity Online Help Files | 149 |
| Post-Installation Steps. | 149 |
| Configuring WebLogic for Mutual Authentication. | 149 |
| Prerequisites | 150 |
| Procedure – Single Server | 150 |
| Procedure – Clustered Servers. | 155 |
| Logging In to Select Identity. | 156 |
| 6 Configuring Select Identity. | 157 |
| Configuring Required TruAccess Properties | 157 |
| How to Set Properties. | 157 |
| Required Settings | 157 |
| Directory Locations | 158 |
| Staging Directories for One-Time Reconciliation and Import Jobs | 158 |
| Email Sender | 158 |
| Attribute Maximum Length | 159 |
| Select Identity URL. | 159 |
| Database Settings | 159 |
| Workflow Settings | 159 |
| Helpdesk Contact Message | 159 |
| Reconciliation Task Retry | 159 |
| Reconciliation Task Termination | 160 |
| Optional Settings | 160 |
| Configuring Delegated Request Dependency Control | 160 |
| Disabling and Re-Enabling Delegated Request Dependency | 160 |
| Setting Up Keystores, Truststores, and Security Framework. | 160 |
| Bootstrap Keystore | 161 |
| Setting Up the Bootstrap Keystore on a New Installation or an Installation with Default Keystores | 161 |
| Non-Hardware Security Module (HSM) Procedure for Bootstrap Keystore Setup | 161 |
| Hardware Security Module (HSM) Procedure for Bootstrap Keystore Setup. | 165 |
| Upgrading the Bootstrap Keystore from an Earlier Version (pre-4.10) | 166 |
| Adding Keys to the Bootstrap Keystore for Key Rotation | 167 |
| Keystores and Key Pairs for Mutual Authentication and Secure Object Migration. | 168 |
| Creating the Mutual Authentication Key | 169 |
| Creating the Object Migration Keys. | 170 |
| Creating the Truststore | 171 |
| Setting TruAccess Properties for the Security Framework | 171 |
| Recommended Configuration | 171 |
| Extending User Searches | 172 |
| How to Specify Extended User Search Attributes | 172 |
| Adding Display Columns for Extended Attributes | 173 |
| Disabling the Extended Search Features. | 174 |
| Custom User Interface Properties | 174 |
| User Interface Sections. | 174 |

| | |
|---|------------|
| Customization Properties | 175 |
| com.hp.ovsi.ui.masthead.fgcolor | 175 |
| com.hp.ovsi.ui.masthead.bgcolor | 175 |
| com.hp.ovsi.ui.logo.image.src | 175 |
| com.hp.ovsi.ui.common.header.image.src | 175 |
| com.hp.ovsi.ui.landing.named.image.src | 175 |
| com.hp.ovsi.ui.landing.named-top.image.src | 175 |
| com.hp.ovsi.ui.landing.named.image.style | 175 |
| com.hp.ovsi.ui.landing.named-top.image.style | 175 |
| com.hp.ovsi.ui.landing.common.image.src | 175 |
| com.hp.ovsi.ui.landing.box.right.bgcolor | 176 |
| com.hp.ovsi.ui.landing.users.image.src | 176 |
| com.hp.ovsi.ui.landing.requests.image.src | 176 |
| com.hp.ovsi.ui.landing.selfservice.image.src | 176 |
| com.hp.ovsi.ui.landing.servicestudio.image.src | 176 |
| Default Values for User Interface Properties | 176 |
| Internationalization and Localization | 177 |
| Translation Customization | 177 |
| Localizing the Date and Time Format | 178 |
| Functional Overview | 178 |
| Custom Date and Time Formats | 178 |
| Setting the Calendar Language | 178 |
| Setting the Date and Time Default Format in the TruAccess Properties File | 179 |
| Setting the Semantics in Oracle | 179 |
| Using MS SQL Scripts for i18n | 179 |
| Configuration for Specific Environments or Platforms | 179 |
| Tuning the WebLogic Application and Database Servers | 180 |
| Optimizing JMS Distributed Queues and WebLogic Work Managers | 180 |
| Tuning the Database Server | 180 |
| UTF-8 Encoding on Oracle 10g | 181 |
| iPlanet LDAP Configuration | 181 |
| Set Encoding in Internet Explorer | 182 |
| Adding Supported Language Fonts | 182 |
| Additional Configuration Options | 182 |
| Configuring Java 2 Security for Select Identity on WebSphere | 184 |
| Deploying the SI Application | 184 |
| 7 Upgrading Select Identity | 185 |
| Pre-Migration Activities | 185 |
| Upgrade Requirements for Select Identity | 185 |
| Preparing to Upgrade | 185 |
| Stopping Select Identity Traffic | 186 |
| General Application Server Preparation | 186 |
| Database Migration | 186 |
| Oracle Upgrade Procedures | 186 |
| Importing Data into a New Oracle Server | 187 |
| Upgrading the Oracle Database | 187 |

| | |
|--|------------|
| MS SQL Upgrade Procedures | 187 |
| Importing Data into a New MS SQL Server 2005 | 187 |
| Upgrading the Select Identity MS SQL Server | 188 |
| Platform Migration | 188 |
| WebLogic Migration from 8.15/8.16 to 9.21 MP1 | 188 |
| WebSphere Migration from 6.012 to 6.10 Patch 9 | 188 |
| Select Identity Upgrade Procedure | 189 |
| 8 Integrating Select Identity with Service Desk, Select Audit, and Service Center | 191 |
| Select Identity – Service Desk Integration | 191 |
| Required Files | 191 |
| External Call from Select Identity to Service Desk | 192 |
| Workflow Template for Integrated Password Management | 192 |
| Functional Scenarios | 192 |
| Password Management Request from Select Identity Triggers New Service Call in Service Desk | 192 |
| Service Call and Workflow Data Exchange and Interaction | 192 |
| Accessing the Select Identity Request Status Page from Service Desk | 193 |
| Configuration Tasks in Service Desk | 193 |
| Customizing a Number Field for the Request ID | 193 |
| Customizing a String Field for Request Failure Information | 194 |
| Activating a String Field for the Request Link | 194 |
| Customizing a Short String Field for the Request Type | 194 |
| Creating a Smart Action | 197 |
| Linking a Service Calls to Select Identity Password Requests | 198 |
| Select Identity Configuration Tasks | 198 |
| System Context | 199 |
| Process Flow | 200 |
| Select Identity – Select Audit Integration | 201 |
| Requirements and Recommendations | 201 |
| Setting Up Integration in Select Identity | 201 |
| The Select Audit Agent | 201 |
| TruAccess Properties | 202 |
| Configuring the Select Identity Database | 202 |
| Setting Up Integration in Select Audit | 203 |
| Data Filtering and Report Access Matrices | 203 |
| Report Mapping | 204 |
| Select Identity – Service Center Integration | 219 |
| Configuration File Customizations | 220 |
| Script Library Customizations | 220 |
| Script Customizations | 220 |
| Table Customizations | 221 |
| contacts Table | 221 |
| cm3r Table | 221 |
| cm3t Table | 221 |
| Form Customizations | 222 |
| Change Management Customizations | 223 |

| | |
|--|------------|
| Change Category Customizations | 223 |
| Change Phase Customizations | 223 |
| Task Related Customizations | 225 |
| Service Catalog Customizations | 225 |
| Select Identity Externalcall Customizations | 226 |
| Test Case Operation Examples | 227 |
| Example 1 - Request Received from the Service Center | 227 |
| Example 2 - Request Received from Select Identity | 228 |
| 9 Uninstalling Select Identity | 231 |
| Auto-Uninstalling Select Identity | 231 |
| Manually Uninstalling Select Identity from IBM WebSphere | 231 |
| Undeploying the Online Help or Another Application | 232 |
| Manually Uninstalling from the WebLogic Server | 232 |
| Deleting the EAR File | 232 |
| Deleting the Connectors | 233 |
| Deleting the Data Source | 233 |
| Deleting the Messaging | 233 |
| Deleting the Mail Session | 234 |
| Removing an Oracle Select Identity Database | 234 |
| A TruAccess Properties | 235 |
| TruAccess Properties Summary | 235 |
| General Settings | 235 |
| Asynchronous Provisioning Delay | 236 |
| Audit Settings | 236 |
| Authentication Settings | 237 |
| Auto User Import Settings | 237 |
| Batch Processing Settings | 237 |
| Bulk Upload Settings | 238 |
| Cache Settings | 238 |
| Connector Schema Directory | 239 |
| Delegated Request Dependency Control | 239 |
| Email Settings | 239 |
| External Calls Settings | 240 |
| JNDI Data Source Settings | 240 |
| Localization Settings | 240 |
| Notification Event Settings | 241 |
| Operations Templates | 241 |
| Page Redirect Timeout | 241 |
| Reconciliation Settings | 241 |
| Report Settings | 242 |
| Repository Type Settings | 243 |
| Schema Settings | 243 |
| Search Settings | 243 |
| Security Framework and Keystore Settings | 245 |
| Self-Registration Settings | 245 |
| Server Management Settings | 245 |

| | |
|--|------------|
| User and Account Settings..... | 245 |
| Web Service Request Settings | 247 |
| Workflow Settings..... | 247 |
| XML Mapping File | 248 |
| B WebLogic Logging Options..... | 249 |
| C Upgrading the Select Identity Database (up to Version 4.13) | 253 |
| Running Oracle Migration Scripts | 253 |
| Running MS SQL Migration Scripts..... | 254 |
| D Running the Migration Utility: 3.3.1–4.01 | 257 |
| Updating the TruAccess Properties File..... | 257 |
| Preliminary Migration Steps..... | 258 |
| Running the Migration Script..... | 258 |
| Running the Migration Utility in an Oracle RAC Configuration..... | 258 |
| Troubleshooting | 259 |
| Post-Migration Steps | 260 |
| E Running the Migration Utility: 4.01–4.10..... | 261 |
| Oracle Database Upgrade Procedure | 261 |
| Running the Migration Utility in an Oracle RAC Configuration..... | 262 |
| MS SQL Database Upgrade Procedure..... | 263 |
| Troubleshooting a Database Upgrade | 263 |
| Index..... | 265 |

1 Introduction

This guide provides instructions for installing HP 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 Select Identity Administration Guide* and the Select Identity online help.

This section covers the following topics:

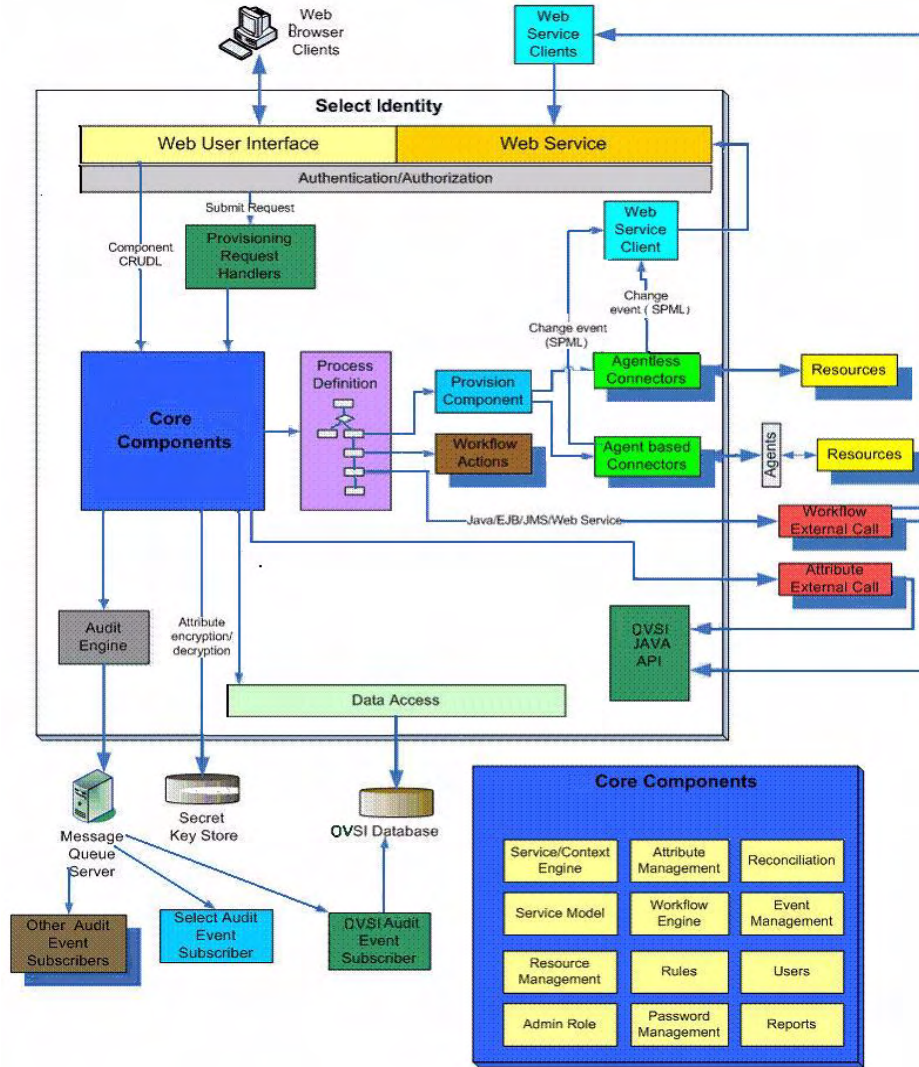
- [System Architecture](#)
- [Security and Communication](#)
- [Connectors](#)
- [Internationalization](#)
- [Technical Qualifications for Installing Select Identity](#)
- [Variable Conventions Used in this Document](#)

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 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. |
| 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.

Java 2 Security

Select Identity supports Java 2 Security for WebSphere 6.1.x. You can optionally use Java 2 Security as an added security layer for your Web applications. See [Chapter 4, Installing Select Identity on IBM WebSphere 6.1.x](#) for details.

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 Keystores, Truststores, and Security Framework](#) on page 160 for details.

Integration

Select Identity can exchange data dynamically with the following HP Identity Center applications: Service Desk, Select Audit, and Service Center. See [Chapter 8, Integrating Select Identity with Service Desk, Select Audit, and Service Center](#) for details.

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 installation and configuration guide for each connector. 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 Select Identity Connector Developer Guide*.

Internationalization

The Select Identity application is internationalized, and is localized to languages specified on the labeling of the localized Select Identity product CD. The Select Identity server is supported in a non-US environment with internationalization encoding. In addition, all supported connectors are internationalization encoded.

See [Internationalization and Localization](#) on page 177 for details on the internationalized Select Identity.

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 to perform and troubleshoot the procedure successfully:

- 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.

Variable Conventions Used in this Document

The following table contains a list of variable conventions used in throughout this document for ease of use:

| Variable | Description |
|---------------------------|---|
| <WebSphere_Home> | The location (directory) of your WebSphere application server installation. |
| <WebLogic_Home> | The location (directory) of your WebLogic application server installation. |
| <BEA_Home> | The location (directory) of your BEA installation (the level above your <WebLogic_Home> directory). |
| <WebSphere_CD_Root> | The WebSphere root directory on the installation CD. |
| <WebLogic_CD_Root> | The WebLogic root directory on the installation CD. |
| <SI_Install_Dir> | The location (directory) of your Select Identity installation. |
| <Server_Name> | The name of your server. |
| <Database_Name> | The name of your database. |
| <Database_Type> | The type of your database, such as Oracle 10g or MS SQL 2005. |
| <Java_Home_Directory > | The location (directory) of your Java installation. |

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 and Verification](#) on page 31.
- 3 Configure the database and load the Select Identity schema, as documented in [Chapter 3, Database Server Configuration](#).
- 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 in [Chapter 4, Installing Select Identity on IBM WebSphere 6.1.x](#), or [Chapter 5, Installing Select Identity on BEA WebLogic 9.2](#).
- 7 Install Select Identity, as documented in [Chapter 4, Installing Select Identity on IBM WebSphere 6.1.x](#), or [Chapter 5, Installing Select Identity on BEA WebLogic 9.2](#).
- 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 is supported on the following configurations:

| Web Application Server | Platform | Database | JDK |
|-------------------------------|--|---|--|
| BEA WebLogic 9.2 | Red Hat Enterprise Linux AS v4.0 EM64T/AMD64 | Oracle 10g | jrockit-R27.2.0-jdk1.5.0_06-linux_x86_64 |
| BEA WebLogic 9.2 | HP-UX 11i (v2) Itanium 64 bit | Oracle 10g | JDK 5.0.08 Itanium |
| BEA WebLogic 9.2 | HP-UX 11i (v3) Itanium 64 bit | Oracle 10g | JDK 5.0.08 Itanium |
| BEA WebLogic 9.2 | Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 | Oracle 10g | jrockit-jdk1.5.0_06-win_x86_64 |
| BEA WebLogic 9.2 | Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 | MS SQL 2005 (with emulate 2-phase commit) | jrockit-jdk1.5.0_06-win_x86_64 |
| IBM WebSphere 6.1.09 | Red Hat Enterprise Linux AS v4.0 EM64T/AMD64 | Oracle 10g | Embedded JDK |
| IBM WebSphere 6.1.09 | HP-UX 11i (v2) Itanium 64 bit | Oracle 10g | Embedded JDK |

| Web Application Server | Platform | Database | JDK |
|-------------------------------|--|-------------------------------|--------------|
| IBM WebSphere 6.1.09 | HP-UX 11i (v3) Itanium 64 bit | Oracle 10g | Embedded JDK |
| IBM WebSphere 6.1.09 | Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 | Oracle 10g | Embedded JDK |
| IBM WebSphere 6.1.09 | Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 | MS SQL 2005 (with XA enabled) | Embedded JDK |

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 | <ul style="list-style-type: none"> • Red Hat Enterprise Linux AS v4.0 EM64T/AMD64 • HP-UX 11i (v2) Itanium (64 bit for WebLogic 9.2) • HP-UX 11i (v3) Itanium (64 bit for WebLogic 9.2) • Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 |
| 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 | The required disk space will depend on the size of your installation. |
| JDBC driver | <p>For WebLogic: oracle.jdbc.xa.client.OracleXADataSource (included with WebLogic)</p> <p>For WebSphere: Oracle 10.1.0.4 JDBC driver\ojdbc14.jar</p> |

MS-SQL Server 2005, Enterprise Edition

| | |
|-------------------------|---|
| Operating system | Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 |
| Processor | Intel Pentium or compatible, minimum speed 166 MHz |
| Memory (RAM) | Enterprise Edition: 512MB RAM; 1024MB recommended |
| Disk space | The required disk space will depend on the size of your installation. |
| JDBC driver | For WebLogic: BEA's MS SQL Server Driver (Type 4) Versions: 7.0, 2000, 2005, class name: weblogic.jdbc.sqlserver.SQLServerDriver For WebSphere: Microsoft SQL Server 2005 JDBC Driver (sqljdbc_1.1.1501.101_enu.exe) |

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 following guideline applies only to Windows and Linux installations:

- Earlier 32-bit versions of WebLogic automatically installed two JDK selections for you to choose from. The 64-bit versions of WebLogic do not come with Java installed. So you will need to download and install JRockit from BEA's Web site. It is *very* important that you install the correct version. Here is the version of JRockit that will work with WebLogic 9.2:

JRockit 5.0 R26.4 CR302700 (for use with WLS 9.2 MP1)

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

| | |
|-------------------------|--|
| Operating System | <ul style="list-style-type: none"> • Red Hat Enterprise Linux AS v4.0 EM64T/AMD64 • HP-UX 11i (v2) Itanium (64 bit for WebLogic 9.2) • HP-UX 11i (v3) Itanium (64 bit for WebLogic 9.2) • Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 |
| 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 install the WebSphere server on a different system than the database server for optimal performance and ease of management, when configuring your WebSphere server.

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

| | |
|-------------------------|--|
| Operating System | <ul style="list-style-type: none"> • Red Hat Enterprise Linux AS v4.0 EM64T/AMD64 • HP-UX 11i (v2) Itanium 64 bit • HP-UX 11i (v3) Itanium 64 bit • Win2003 Standard, Enterprise, Datacenter EM64T/AMD64 |
| 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 6.0 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:

- 9080 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
- 9443 for WebSphere
- 7002 for WebLogic
- You must pick one other unused port if you are using Mutual Authentication for WebSphere.

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 add spaces to the directory name.
- 2 Copy the following files from the Oracle database home directory on the Select Identity CD to the directory you just created:

```
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 system 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 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 9](#), 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.

- 6 Set the following Oracle 10g permissions:

```

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;

```

- 7 If you are running Select Identity on IBM WebSphere 6.1.x, 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 Server.

- ▶ 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.

- 8 If running Select Identity on IBM WebSphere 6.1.x, change to the first user account you created, by entering the following command:

```
CONNECT user_name/password
```

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

- a Copy the schema creation script from the 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.

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

- a Copy the data creation script from the product CD.

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

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

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

- c Verify that no error message results.



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.

Do not include spaces into the directory name.

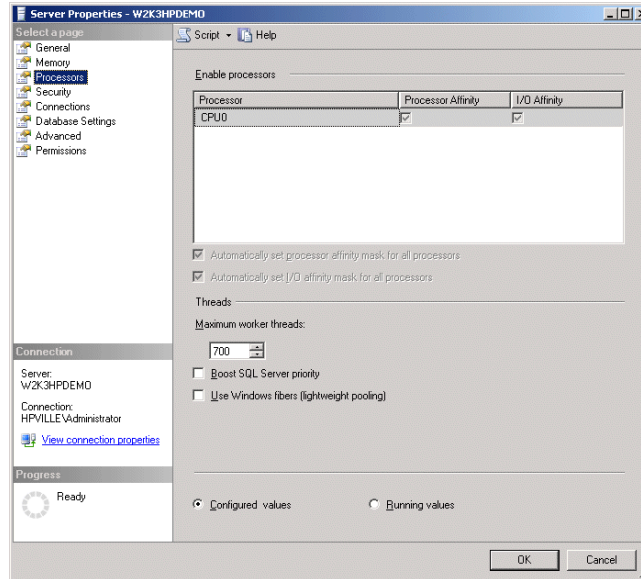
- 2 Copy the following files from the database directory on the Select Identity CD to the Select Identity database home directory on the SQL Server system:

```
mssql_concero_ddl.sql
```

```
mssql_concero_dml.sql
```

- 3 Log in to the Microsoft SQL Server Management Studio.
- 4 In SQL Server Management Studio, right click on the **<instance name>** and click on **Properties**.
- 5 On the **Server Properties** window, click on **Processors**.
- 6 In the **Maximum worker threads** field, select 700.

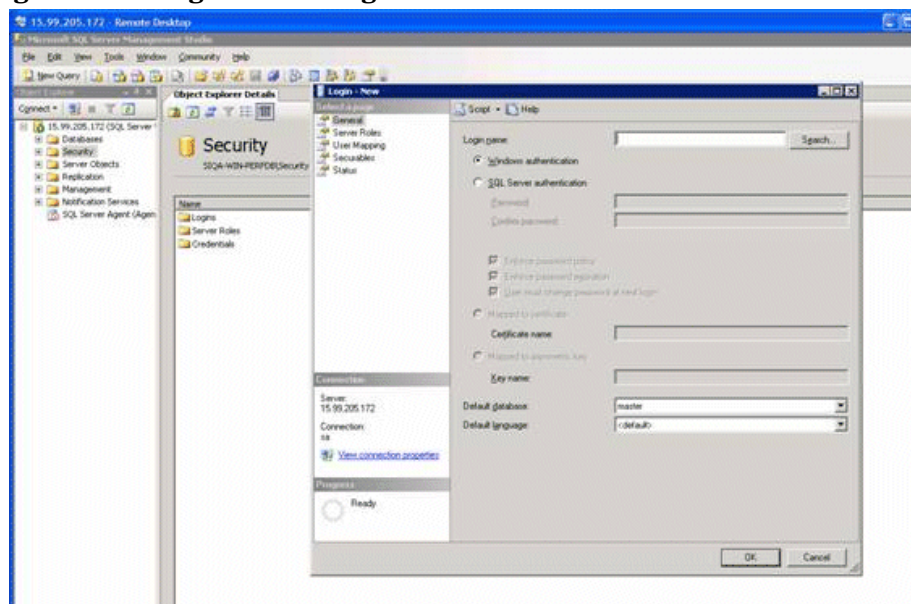
Figure 2 Database Server Properties



- 7 In SQL Server Management Studio, expand the <instance name>, and right click on **Database**.
- 8 Enter a name for the database.
- 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 In the left panel, expand **Security**.
 - b Right-click on **Logins** and selecting **New Login**.

The SQL Server **Login - New** page opens.

Figure 3 Login - New Page



- c In the **Login name** field, enter SI for the login name.

- d Select the **SQL Server Authentication** option, and enter and confirm a new password in the provided fields.
 - e Click **OK**.
 - f In the left panel, right-click on **Databases**, and select the **New Database** option.
 - g Enter `SI` for the database name.
 - h Click **OK**.
 - i In the left panel, expand **Databases**, and then expand the `SI` database you just created.
 - j Right-click on **Security** and select **New User**.
 - k Set the user name and `SI` login values.
 - l Set the role membership to `db_owner`.
 - m In the left panel, expand **Databases**, and select the `SI` database you just created.
 - n Right-click on **Security** and select **New Schema**.
 - o Set the schema name and schema owner values.
 - p In the left panel, expand **Databases**, and select the `SI` database you just created.
 - q Expand **Security > Users**, and double-click on the `SI` user you created.
 - r Edit the schema information, keeping the same settings you used when creating a new schema.
 - s Expand **Security > Logins**.
 - t Select the `SI` login you created.
 - u Edit the default database information, keeping the same settings you used when creating a new database.
 - v Click **OK** to save your new login user account.
- 11 If installing on IBM WebSphere, create a second database user account that will be used by the Java Messaging Service (JMS). To do so, repeat these steps, giving your database a unique name.
- 12 Load the `mssql_concero_ddl.sql` script from the Select Identity database home directory at the beginning of this section.
- a Select **File** → **Open** → **File**.
 - b Locate the Select Identity database home directory and choose the `mssql_concero_ddl.sql` file.
 - c Click **Open**.
 - d Connect using **SQL Server Authentication** and the new login user ID and password you created earlier in this section. This should automatically select the new database created for Select Identity.
 - e Click on **Execute** to run the script and verify there are no errors.
- 13 Insert the required data into the Select Identity database by performing the following steps:
- a Select **File** → **Open** → **File**.
 - b Locate the Select Identity database home directory and choose the `mssql_concero_dml.sql` file.

- c Click **Open**
- d Connect using SQL Server Authentication and the new login user ID and password you created earlier in this section. This should automatically select the new database created for Select Identity.
- e Click on **Execute** to run the script and verify there are no errors.

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 6.1.x

This chapter describes how to install Select Identity on an IBM WebSphere 6.1.x application server, with either MS-SQL 2005 or Oracle 10G.

This chapter includes the following topics:

- [Introduction](#)
- [Prerequisite Configuration and Verification](#)
- [Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security](#)
- [Preparing to Install Select Identity](#)
- [Important Installation Information](#)
- [Using the Select Identity Installer](#)
- [Manual Installation Procedures](#)
- [Updating the Classloading Strategy of attributemapper.war](#)
- [Configuring WebSphere for Mutual Authentication](#)
- [Logging In to Select Identity](#)

Introduction

The 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 6.1.x 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 and Verification

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 completed on all WebSphere installations before you begin to install Select Identity:

- 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 script named `wsadmin.bat` or `wsadmin.sh` (located at `%WAS_HOME%/bin`) can be executed at the command line without any problems.
- The `HAManagerService` must be enabled in WebSphere. This is enabled by default and can be verified by viewing the `hamanagerservice.xml` configuration files in your WebSphere application profile directory.
- Your Select Identity database server is configured as documented in [Chapter 3, Database Server Configuration](#). Also, if you are using MS SQL 2005, make sure XA is enabled.
- 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 Keystores, Truststores, and Security Framework](#) on page 160. (Note, for a new install that uses `OVSKeyStoreUtilities` to create the keystore, this step can not be executed until the files have been installed.)
- When choosing your `<WebSphere_Home>` directory location for the installation, make sure the directory path is succinct; Windows has a directory path limit of 256 bytes. This will avoid Select Identity deployment issues.

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, 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.

Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security

If you wish to enable Java 2 security for your Select Identity implementation, you must perform a *one-time configuration* using the WebSphere console *prior to installing Select Identity*.

To enable Java 2 Security in your implementation, perform the following processes:

- Perform the pre-installation steps discussed in this section:
 - [Create a Select Identity Administrator](#) on page 33.
 - [Add the Monitor and Configurator Roles for the Select Identity Administrator](#) on page 34.
 - [Append Permissions to the app.policy File](#) on page 34.
 - [Secure the WebSphere Environment and Limit Access](#) on page 35. (This set of steps must be performed *after* the Select Identity application has been fully configured as discussed in [Chapter 6, Configuring Select Identity](#).)
- Perform a series of steps *each time you deploy* the Select Identity application, as discussed in [Configuring Java 2 Security for Select Identity on WebSphere](#) on page 184.

Create a Select Identity Administrator

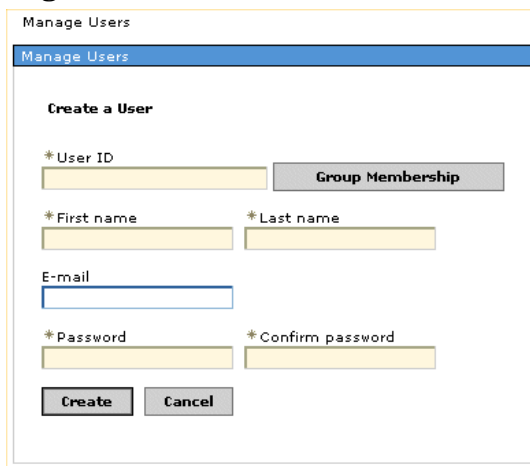
To configure perform WebSphere to enable Java 2 security, you must create a Select Identity Administrator.

- ▶ Prior to creating the Select Identity Administrator, you must set up a database repository to store the username and password.

To create a Select Identity Administrator, perform the following steps:

- 1 From the left panel of the WebSphere console, expand **Users and Groups** and select **Manage Users**.
- 2 Click **Create**.

Figure 4 Manage Users



The screenshot shows a web console window titled "Manage Users". Inside, there is a sub-section titled "Create a User". The form contains several input fields and a button:

- *User ID: A text input field.
- Group Membership: A dropdown menu.
- *First name: A text input field.
- *Last name: A text input field.
- E-mail: A text input field.
- *Password: A text input field.
- *Confirm password: A text input field.
- Buttons: "Create" and "Cancel".

- 3 Set the field values as follows to create a Select Identity administrator:

- **User ID:** Enter the user ID `siadministrator`.
 - **First Name:** Enter the administrator's first name.
 - **Last Name:** Enter the administrator's last name.
 - **Password:** Enter a password for the administrator.
 - **Confirm Password:** Confirm the password for the administrator.
- 4 Click **Create**.

Add the Monitor and Configurator Roles for the Select Identity Administrator

Next, you will need to add the monitor and configurator roles for the Select Identity administrator you created:

- 1 From the left panel of the WebSphere console, expand **Users and Groups** and select **Administrative User Roles**.
- 2 Click **Add**.

Figure 5 Add User Roles

- 3 In the **User** field, enter `saiadministrator`.
- 4 In the **Roles** field, select **Monitor** and **Configurator**.
- 5 Click **Apply**.

Append Permissions to the app.policy File

In order for Java 2 security to function properly with Select Identity installed on WebSphere, you must append the following permissions to the `app.policy` file:

```
// For AXIS module implementations
grant codeBase "file:<WAS_HOME>/AppServer/—" {
permission java.security.AllPermission;
};
// The directory for external calls implementation jar files
grant codeBase "file:<SI_Installation>/ExternalCalls/—" {
permission java.security.AllPermission;
};
```

Clusters

For each cluster node, these permissions must be appended to the `app.policy` file on the computer that runs the Deployment Manager server.

The files can be found at:

```
<WebSphere_Home>/AppServer/profiles/<deployment_manager>/config/cells/  
<cell_name>/nodes/<node>/app.policy
```

where <deployment_manager> is usually Dmgr01.

These files will be replicated to the cluster nodes by the Deployment Manager during the cluster startup to the following directories:

```
<WebSphere_Home>/AppServer/profiles/<profile_name>/config/cells/  
<cell_name>/nodes/<node>
```

Stand-alone Servers

For stand-alone servers, append these permissions to the app.policy located at:

```
<WebSphere_Home>/profiles/AppSrv01/config/cells/<cell_name>/nodes/<node>
```

Move All External Call JAR Files

For both clusters and stand-alone servers, you must move all external call JAR files to the <SI_Install_Dir>/ExternalCalls directory before enabling Java 2 security.

Secure the WebSphere Environment and Limit Access

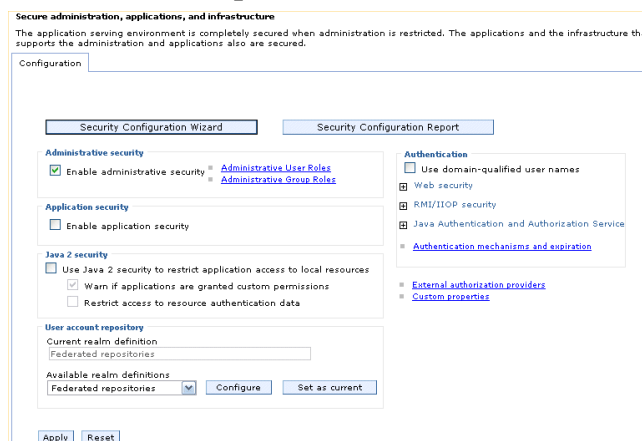
Finally, once the Select Identity application is configured, you must perform another set of steps *only once* to secure the WebSphere environment and allow only authorized users to access the Cos Naming service.

Secure the WebSphere Environment

To secure the WebSphere environment, perform the following steps:

- 1 In the left pane of the WebSphere console, expand **Security** and select **Secure Administration, Application, and Infrastructure**.

Figure 6 Secure the WebSphere Environment



- 2 Select the following checkboxes:
 - **Enable Administrative Security**
 - **Enable Application Security**

- Use Java 2 Security to Restrict Application Access to Local Resources

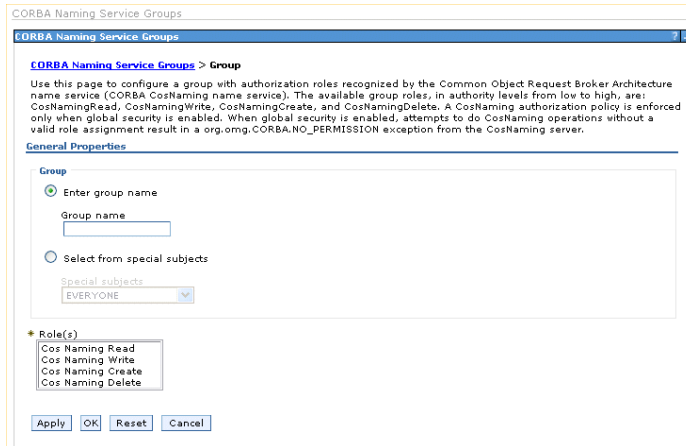
3 Click **Apply**.

Allow Only Authorized Users to Access Cos Naming Service

To allow only authorized users to access the Cos Naming service, perform the following steps:

- 1 In the left pane of the WebSphere console, expand **Environment** and select **Naming** → **CORBA Naming Service Groups**.
- 2 Click **Add**.

Figure 7 Allow Only Authorized Users




- 3 Select the **Select from Special Subjects** radio button.
- 4 From the **Special Subjects** drop-down list, select **ALL_AUTHENTICATED**.
- 5 From the **Roles** list, select the following:
 - **Cos Naming Read**
 - **Cos Naming Write**
 - **Cos Naming Create**
 - **Cos Naming Delete**
- 6 Click **OK**.
- 7 In the resulting table, if an **EVERYONE** subject exists, select it and click **Remove**.
- 8 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 9 Restart your server(s) to instantiate your changes.

Preparing to Install Select Identity

To prepare WebSphere for installation, complete the following steps:

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

US_export_policy.jar
local_policy.jar

- ▶ If you are installing Select Identity in a location other than the United States, you may need location-specific policy files.
- 2 Copy the policy files from [step 1](#) to %WAS_HOME%/java/jre/lib/security.
 - 3 If using Oracle, download the Oracle thin driver `ojdbc14.jar` to the machine running the installer. The installer prompts for the path to this file.
 - ▶ The Oracle 10G driver is required.
 - ▶ Each application server in the cluster must be able to access this file using this path. The path could be a location on a Network File System or the file can be copied to the same local path on each server.
 - 4 On a cluster, configure the network file system to allow the installation directory to be reached from each server.
 - 5 For easier access to documentation, copy the product documentation PDF files from the `/docs` directory on the 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 Keystores, Truststores, and Security Framework](#) on page 160.
-  Do not attempt to launch Select Identity until the security framework has been completely set up. The files must be present before the installation can complete.
- 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 6.1.x 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 and password 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 directory location of the keystore parameter file. See [Setting Up Keystores, Truststores, and Security Framework](#) on page 160.
- The location of the Oracle thin driver Java archive file, if applicable.

For Clusters:

Select Identity installation on a cluster in WebSphere 6.1.x 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.

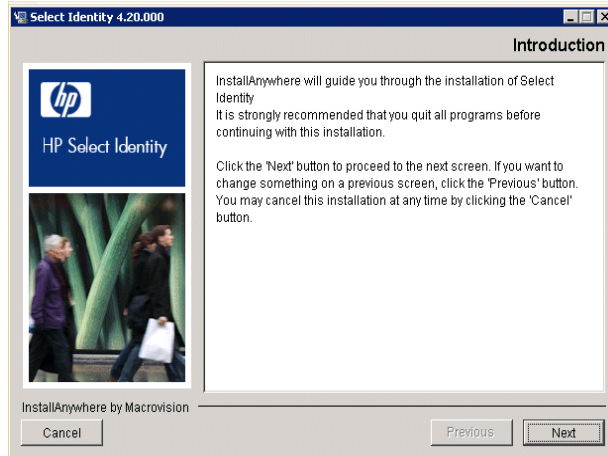
Using the Select Identity Installer

This section describes how to install Select Identity using the installer. Before starting this procedure, you must complete the [Prerequisite Configuration and Verification](#) on page 31.

Auto-Installation Procedure

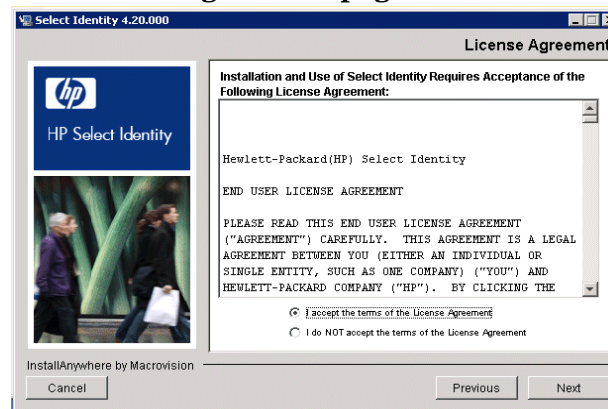
- 1 Log on to the operating system as the same user that was used to install WebSphere.
You must copy and run the installer directly on the application server's local machine, or the Deployment Manager node in a cluster. Do not try to run the installer remotely.
- 2 Mount the Select Identity CD and navigate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

Figure 8 The Introduction page



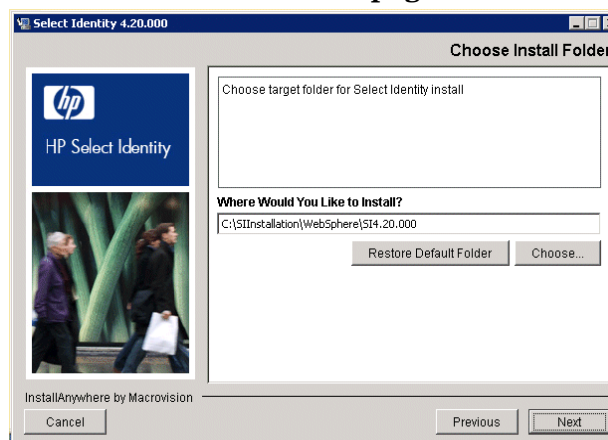
- 4 Click **Next** to review the license agreement.

Figure 9 The License Agreement page



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

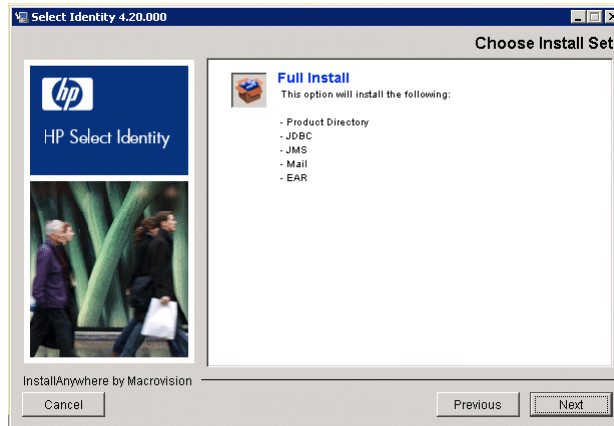
Figure 10 The Choose Install Folder page



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

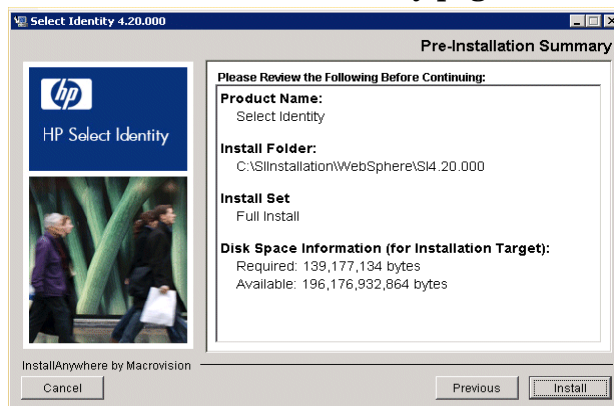
On a cluster, ensure that the installation directory is a shared file system directory.

Figure 11 The Choose Install Set page



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

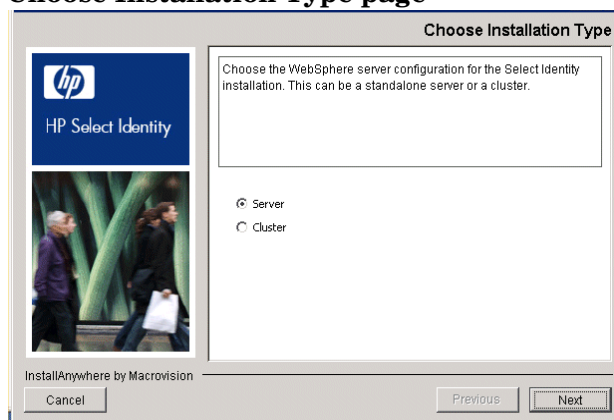
Figure 12 The Pre-Installation Summary page



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

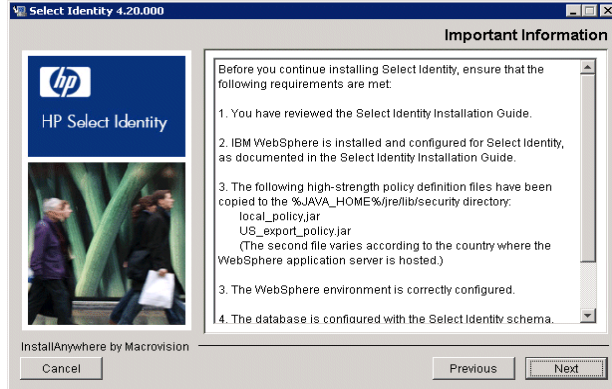
The wizard installs the files according to your settings. A progress bar indicates that the installation is in progress. When installation is complete, the installer displays the **Choose Installation Type** page.

Figure 13 Choose Installation Type page



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

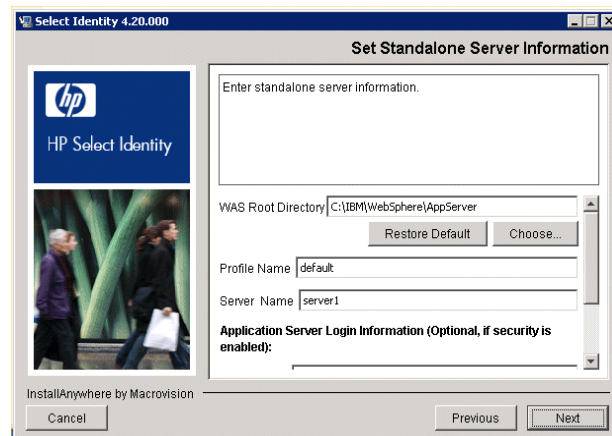
Figure 14 The Important Information page



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

- If you are performing a standalone installation, the installer proceeds to the **Set Server Information** page (Figure 15).
- If you are performing a cluster installation, the installer proceeds to the **Set Cluster Information** page (Figure 16).

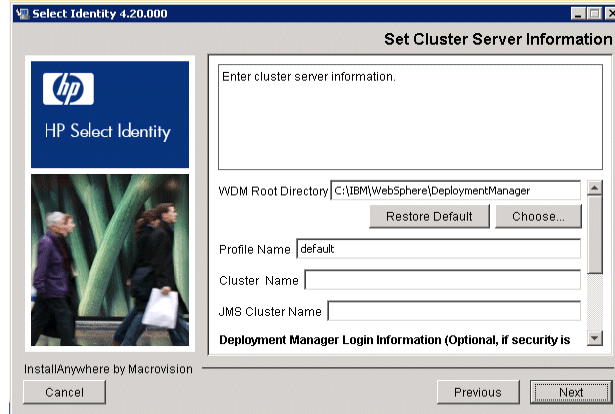
Figure 15 The Set Server Information page (standalone installation)



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

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

Figure 16 The Set Cluster Information page (cluster installation)



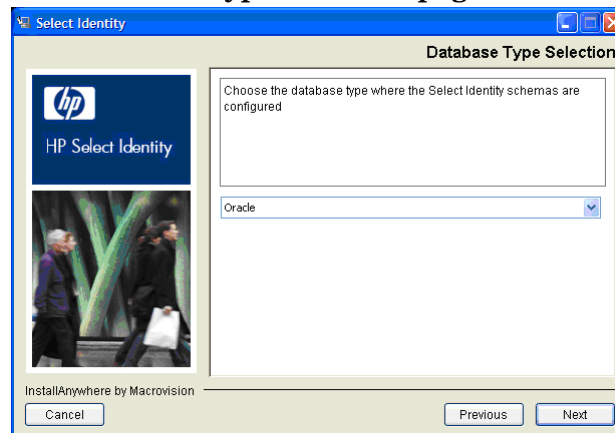
13 Specify cluster settings, as follows:

- **WDM Root Directory** — The directory where the WebSphere application server is installed.
 - **Profile Name** — The profile on which you are installing Select Identity.
 - **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.
 - **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.

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

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

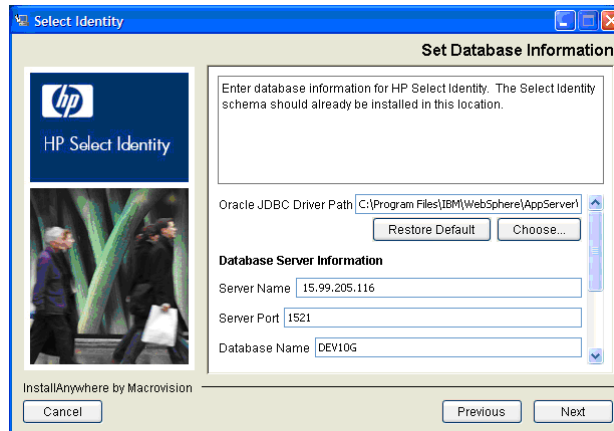
Figure 17 The Database Type Selection page



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

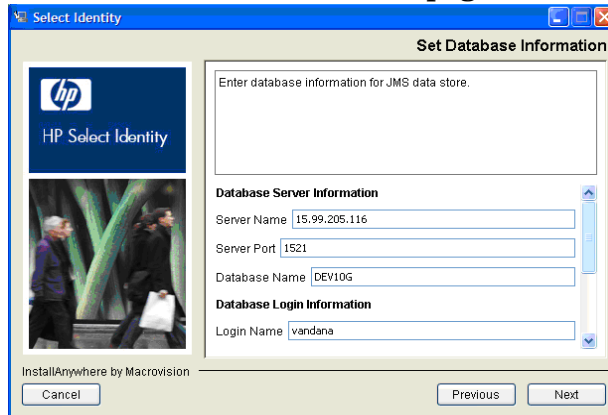
- ▶ The instructions and illustrations that describe the database settings are based on Oracle 10g. If you are using MS-SQL 2005, you will need to make appropriate selections for this database.

Figure 18 The Set Database Information page (Select Identity)



- 16 Complete the fields with the appropriate information about the Select Identity database user account:
 - **Server Name** — The hostname or IP address of the database server.
 - **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.
 - **JDBC Driver Path** — The full path to the JDBC driver file (including the actual file name.)
 - For Oracle: `ojdbc.jar`
 - For MS SQL 2005 (Microsoft Driver): `sqljdbc.jar`
- 17 After making the settings, click **Next** to proceed to the **Set Database Information** page for JMS.

Figure 19 The Set Database Information page (JMS)



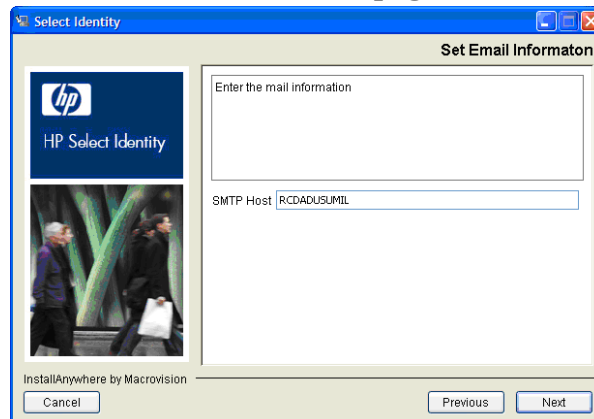
18 Complete the fields with the appropriate information about the JMS database user account:

- **Server Name** — The hostname or IP address of the database server.
- **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 `<WebSphere_Home>\bin`), to create the JMS data tables. This is a Windows-specific example. More information for all installation types (Windows, HP-UX, Linux) is available about this setting at IBM's public WebSphere technical library on the Internet.

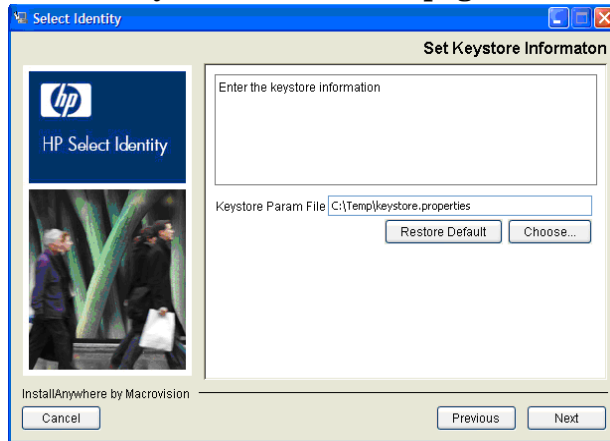
19 After making the settings, click **Next** to proceed to the **Set Email Information** page.

Figure 20 The Set Email Information page



- 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 21 The Set Keystore Information page

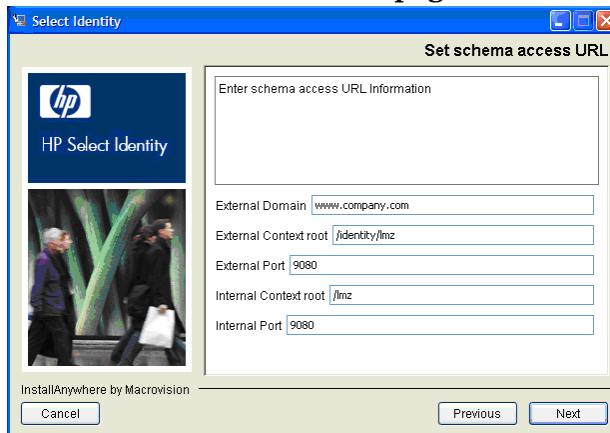


- Click **Choose** and browse to the file system location of the keystore parameters file (keystore.properties).

- ▶ The correct directory location of the keystore.properties file is documented in [Setting Up Keystores, Truststores, and Security Framework](#) on page 160.
- Complete this task at part of the [Prerequisite Configuration and Verification](#) on page 31.

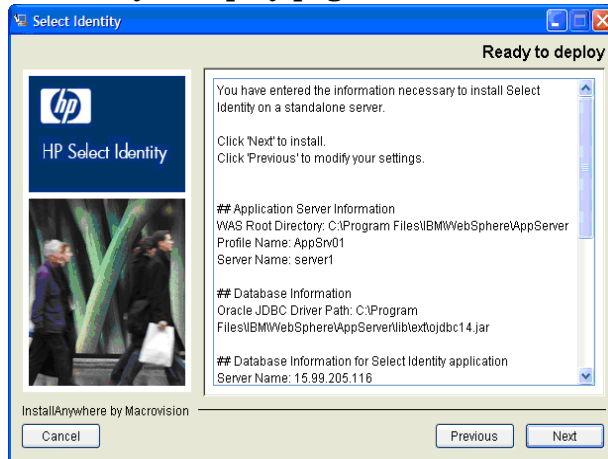
- Click **Next** to proceed to the **Set schema access URL** page.

Figure 22 The Set schema access URL page



- Complete the fields with the appropriate information about the schema access URL:
 - **External Domain** — The external (outside of the firewall) domain for the schema access URL.
 - **External Context Root** — The external context root for the schema access URL.
 - **External Port** — The external port number for the schema access URL.
 - **Internal Context Root** — The internal (inside of the firewall) context root for the schema access URL.
 - **Internal Port** — The internal port number for the schema access URL.
- Click **Next** to proceed to the **Ready to Deploy** page.

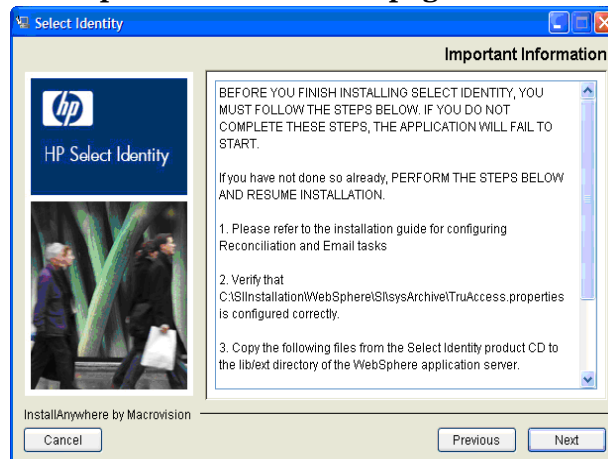
Figure 23 The Ready to deploy page



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

When Select Identity is installed and deployed, the installer displays the **Important Information** page.

Figure 24 The Important Information page



26 Be sure to read the information provided on the **Important Information** page.

27 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
- sysArchive/bcprov-jdk15-135.jar
- sysArchive/commons-logging-1.1.jar

28 Stop and restart the server or the Select Identity cluster (as applicable), so that WebSphere loads the .jar files that you copied in [step 27](#).

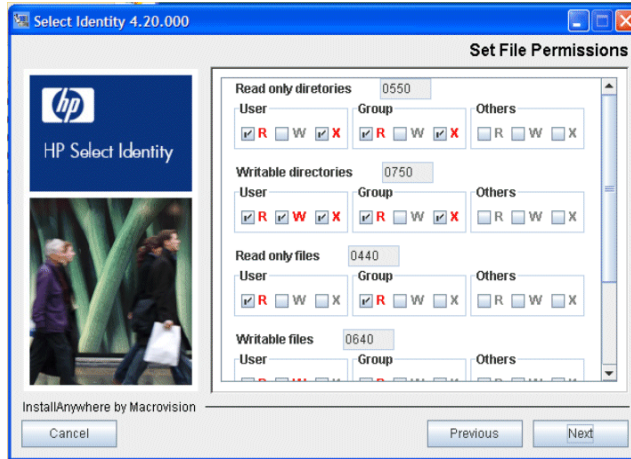
29 Refer to [Chapter 6, Configuring Select Identity](#), and [Appendix A, TruAccess Properties](#) for information about configuring the TruAccess.properties file for your environment.

30 Deploy the online help, as documented in [Deploying Select Identity and the Online Help](#) on page 69.

31 Configure the WebSphere logging features for Select Identity, as documented in [Configuring Logging for Select Identity](#) on page 74.

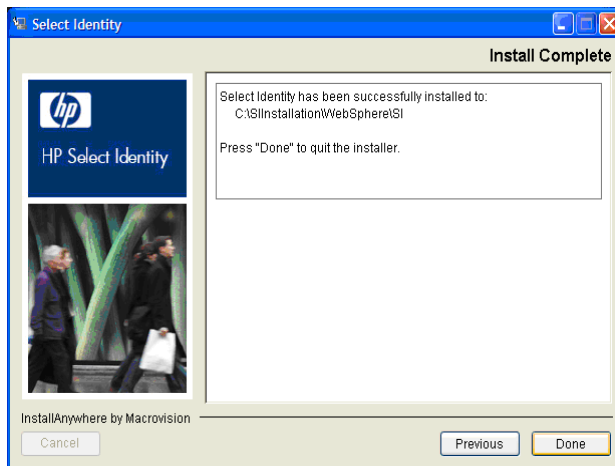
- 32 Stop and restart the WebSphere application server.
On a cluster, stop and restart all Node Agents and Deployment Manager.
- 33 Click **Next** to display the **Set File Permissions** page—if you are running in HP-UX or Linux. For Windows installations, clicking **Next** displays the **Install Complete** page.

Figure 25 The Set File Permissions page



- 34 Use this page to set read/write/execute permissions for directories and files accessed by users and groups.
 - R=read permissions
 - W=write permissions
 - X=execute permissions
- 35 Click **Next** to display the **Install Complete** page.

Figure 26 The Install Complete page



- 36 Click **Done** to close the installer.
- 37 If using global security, refer to [Configuring Global Security](#) on page 74.
- 38 You can now log in to Select Identity, as documented in [Logging In to Select Identity](#) on page 105.

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 231. 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](#)
- [Deploying Select Identity and the Online Help](#)
- [Updating The Select Identity Application Settings](#)
- [Configuring the Java Virtual Machine](#)
- [Configuring Logging for Select Identity](#)

How This Section is Organized

This section does not provide detailed instructions about how to navigate in IBM WebSphere 6.1.x; 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. In this document, this directory is referred to using the following variable:

<SI_Install_Dir>.

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 <SI_Install_Dir> directory:
 - <SI_Install_Dir>/deploy
 - <SI_Install_Dir>/email
 - <SI_Install_Dir>/recon
 - <SI_Install_Dir>/recon/reconroot
 - <SI_Install_Dir>/recon/reconbackup
 - <SI_Install_Dir>/recon/reconstaging
 - <SI_Install_Dir>/reports
 - <SI_Install_Dir>/sysArchive
 - <SI_Install_Dir>/temp
 - <SI_Install_Dir>/upload
 - <SI_Install_Dir>/userimport
 - <SI_Install_Dir>/userimport/adbackup
 - <SI_Install_Dir>/userimport/adroot
 - <SI_Install_Dir>/userimport/adstaging
- 3 Copy the following files from the Select Identity product CD to the <SI_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 <SI_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 <WebSphere_Home>/lib/ext directory from the Select Identity product CD:
 - sysArchive/connector.jar
 - sysArchive/ovsii18n.jar
 - sysArchive/bcprov-jdk15-135.jar

- `sysArchive/commons-logging-1.1.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 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 [IBM WebSphere Server Requirements](#) on page 23.
- 10 Log on to the WebSphere Administrative Console as **admin**.

Configuration Scope

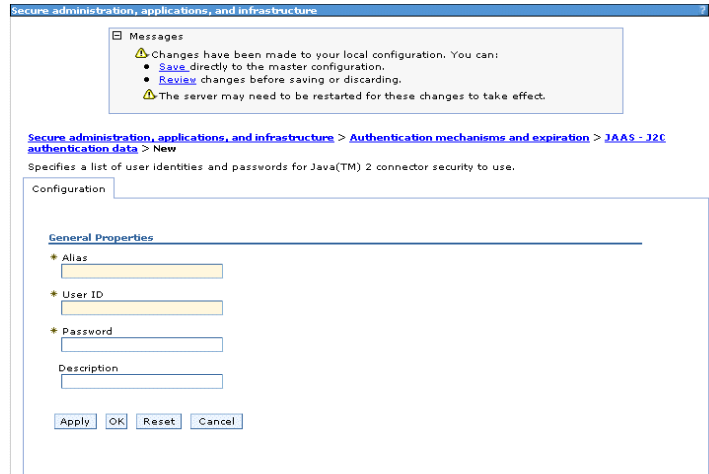
The scope selection is crucial to many of the manual installation procedures in both standalone and cluster configurations. Use the following table for reference regarding the correct scope selection for the configuration items listed:

| | 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 From the left panel of the console, expand **Security** and select **Secure administration, applications, and infrastructure**.
- 2 Under **Authentication**, expand **Java Authentication and Authorization Service**.
- 3 Select **J2C Authentication Data**.
- 4 Click **New**.

Figure 27 Enter J2C Authentication Data



- 5 Create a data entry for Select Identity, with the fields set as follows:
 - **Alias:** SI Oracle10G or SI MSSQL
 - **User ID:** <DB_LOGIN>
 - **Password:** <DB_PASSWORD>
- 6 Click **Apply**.
- 7 Create an additional authentication data entry for the JMS datastore, with the fields set as follows:
 - **Alias:** SI Oracle10g_JMS or SI JMS_MSSQL
 - **User ID:** <JMS_DB_LOGIN>
 - **Password:** <JMS_DB_PASSWORD>
- 8 Click **Apply**.
- 9 Click **OK** to see your entries in the provided table.
- 10 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

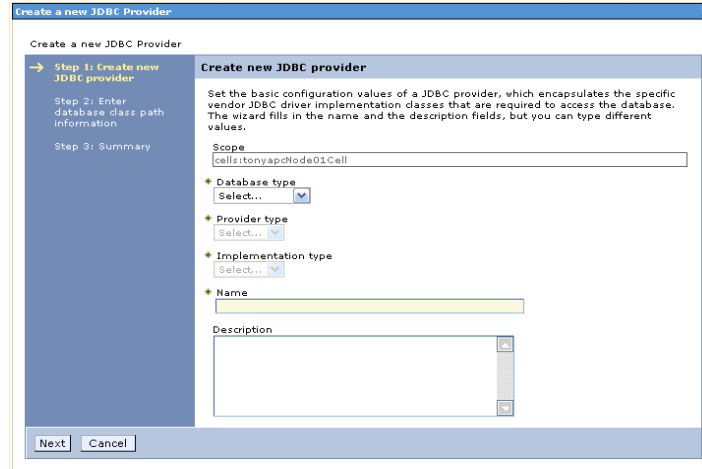
Creating the JDBC Providers

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 SI Oracle JDBC Provider or SI MSSQL JDBC Provider, depending on your database.

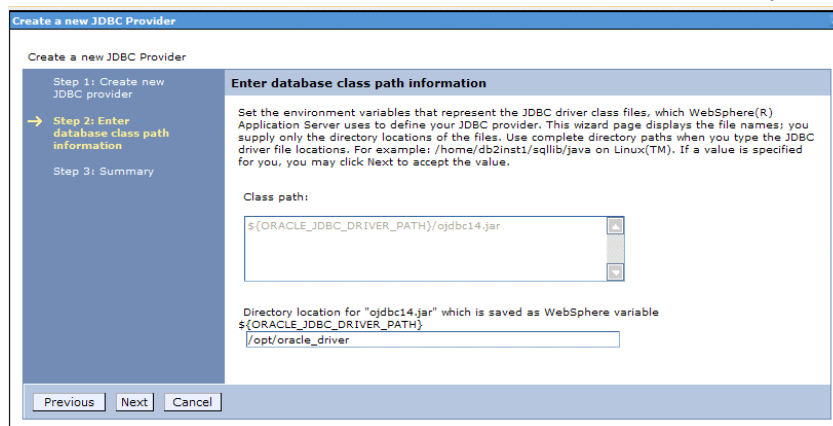
- 1 From the left panel of the console, expand **Resources** and select **JDBC** → **JDBC Providers**.
- 2 Set the cluster **Scope** (the Select Identity cluster) using the drop-down box.
- 3 Click **New**.

Figure 28 Create New JDBC Provider



- 4 Make the following selections:
 - **Database Type:** Enter **Oracle** or **SQL Server** as appropriate to your database server.
 - **Provider Type:**
 - For MS SQL, select the user-defined JDBC provider.
 - For Oracle, select the Oracle JDBC driver.
 - **Implementation Type:** Select XA data source regardless of the database type.
 - **Name:**
 - For MS SQL, enter:
`com.microsoft.sqlserver.jdbc.SQLServerXADataSource` if you are using the Microsoft driver. Note, the classpath should be set to `sqljdbc.jar`.
 - For Oracle, keep the default name: Oracle JDBC Driver (XA).
- 5 Click **Next**.
- 6 If you select Oracle as your JDBC Driver, you will receive the following screen (which is not presented if you select the Microsoft driver). Here you enter the path for the database driver.

Figure 29 Create New JDBC Provider - Oracle Driver Only



- 7 Click **Next**.
- 8 Click **Finish**.

- 9 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 10 Repeat this procedure to create a second JDBC provider, with the **Scope** set to the JMS cluster, and the **Name** set to SI Oracle10g JMS JDBC Provider, or SI MSSQL JMS JDBC Provider.

MS-SQL Configuration: Changing the Default Transaction Isolation Level

If you are using MS-SQL 2005, configure the JDBC provider by setting the correct Default Transaction Isolation Level.

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

- 1 From the left panel of the console, expand **Resources** and select **JDBC** → **Data Resources**.
- 2 Click the name of the Data Source for which you want to customize the Default Transaction Isolation Level.
- 3 Under **Additional Properties**, click **Custom Properties**.
- 4 Click **New** to add a new custom property.

Figure 30 Change the Default Transaction Isolation Level

The screenshot shows a 'Custom Properties' dialog box. At the top, it says 'Data sources > Default DataSource > Custom properties > New'. Below that is a brief instruction: 'Use this page to specify custom properties that your enterprise information system (EIS) requires for the resource providers and resource factories that you configure. For example, most database vendors require additional custom properties for data sources that access the database.' The main area is titled 'Configuration' and contains a 'General Properties' section. It has a 'Scope' field with the value 'cells:tonyapcNode01Cell:nodes:tonyapcNode01:servers:server1' and a 'Required' checkbox. The 'Name' field is highlighted in yellow. Below it are 'Value' and 'Description' fields. The 'Type' is set to 'java.lang.String'. At the bottom are 'Apply', 'OK', 'Reset', and 'Cancel' buttons.

- 5 In the **Name** field, name this property `webSphereDefaultIsolationLevel`.
- 6 Enter 2 as the value.
- 7 Click **OK**.
- 8 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 9 Repeat this procedure for the second JDBC provider created in [Creating the JDBC Providers](#) on page 51

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 SI data source under the Select Identity JDBC Provider, on the Select Identity cluster. Locate the SI JMS DataSource under the Select Identity JMS JDBC Provider, on the JMS cluster.

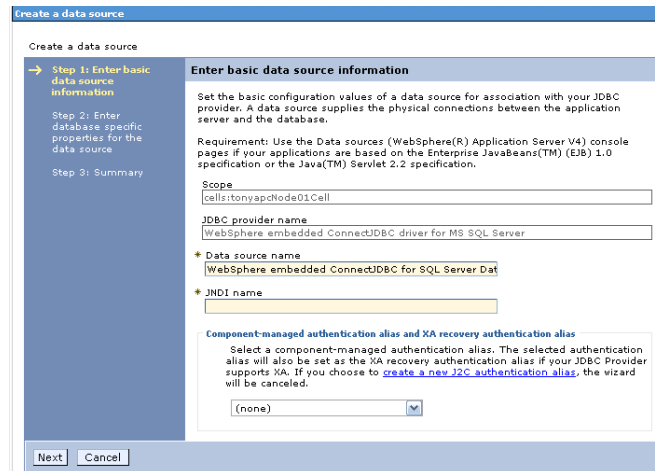
On a standalone installation, Locate both data sources under the HP Select Identity JDBC Provider.

Create the First Data Source

To create the data sources, perform the following steps:

- 1 In the console, navigate to and display the JDBC Provider named SI<Database_Type> JDBC Provider, that you created in [Creating the JDBC Providers](#) on page 51.
- 2 Under **Additional Properties**, click **Data Source**.
- 3 Click **New** to create a data source for Select Identity.

Figure 31 Create a Data Source



- 4 Set the following fields, as listed:
 - **Scope:** the scope for your data source
 - **JDBC Provider Name:** JDBC provider name (such as WebSphere)
 - **Data Source Name:** SI DataSource
 - **JNDI Name:** jdbc/TruAccess
 - **Component-managed Authentication Alias and XA Recovery Authentication Alias:** SI Oracle10g or SI MSSQL
- 5 Click **Next**.
- 6 Set the following fields, as listed:
 - For the MS SQL driver:
 - **Database name:** enter your database name
 - **Server name:** enter your database server name
 - **Port number:** enter your database server port number
 - For the Oracle driver:
 - **URL:** enter the URL
 - **Data store helper class name:** enter the data store helper class name
- 7 Click **Next**.
- 8 Click **Finish**.

- 9 Navigate to the data source you just created, and select it.
- 10 Under **Additional Properties**, select **Connection Pool Properties**.
- 11 Set the following fields, as listed:
 - **Connection Timeout:** 300
 - **Maximum Connections:** 200
 - **Minimum Connections:** 1
- 12 Click **Apply**.
- 13 Click **OK**.
- 14 Under **Additional Properties**, click the link to **WebSphere Application Server Data Source Properties**.
- 15 Set the following fields, as listed:
 - **Statement Cache Size:** 50
- 16 Click **Apply**.
- 17 Click **OK**.
- 18 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Create the Second Data Source for JMS

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

- 1 In the console, navigate to and display the JDBC Provider named SI<Database_Type> JDBC Provider, that you created in [Creating the JDBC Providers](#) on page 51.
- 2 Under **Additional Properties**, click **Data Source**.
- 3 Click **New** to create a data source for JMS.

Figure 32 Create a Data Source for JMS

- 4 Set the following fields, as listed:
 - **Scope:** the scope for your data source
 - **JDBC Provider Name:** DBC provider name (such as WebSphere)
 - **Data Source Name:** SI JMS DataSource

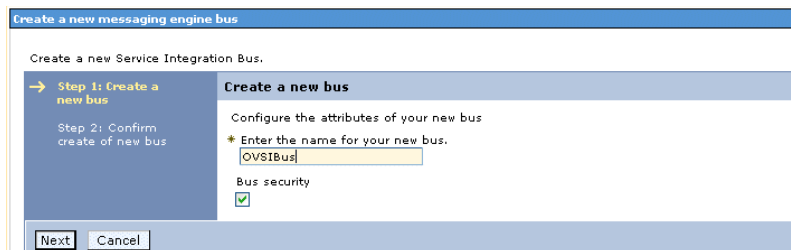
- **JNDI Name:** jdbc/TruAccess_JMS
 - **Component-managed Authentication Alias and XA Recovery Authentication Alias:** SI Oracle10g_JMS or SI JMS MSSQL
- 5 Click **Next**.
 - 6 Set the following fields, as listed:
 - For the MS SQL driver:
 - **Database name:** enter your database name
 - **Server name:** enter your database server name
 - **Port number:** enter your database server port number
 - For the Oracle driver:
 - **URL:** enter the URL
 - **Data store helper class name:** enter the data store helper class name
 - 7 Navigate to the data source you just created, and select it.
 - 8 Under **Additional Properties**, click **Connection Pool Properties**.
 - 9 Make the following settings:
 - **Connection Timeout:** 100
 - **Maximum Connections:** 300
 - **Minimum Connections:** 1
 - 10 Click **Apply**.
 - 11 Click **OK**.
 - 12 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Configuring the Select Identity Service Integration Bus

To configure the Select Identity service integration bus:

- 1 From the left panel, expand to **Service Integration** and select **Buses**.
- 2 Click **New**.

Figure 33 Create a New Bus



- 3 Name the bus **OVSIBus**.
- 4 Click **Next**.
- 5 Click **Finish**.
- 6 In the table, select the bus you just created.

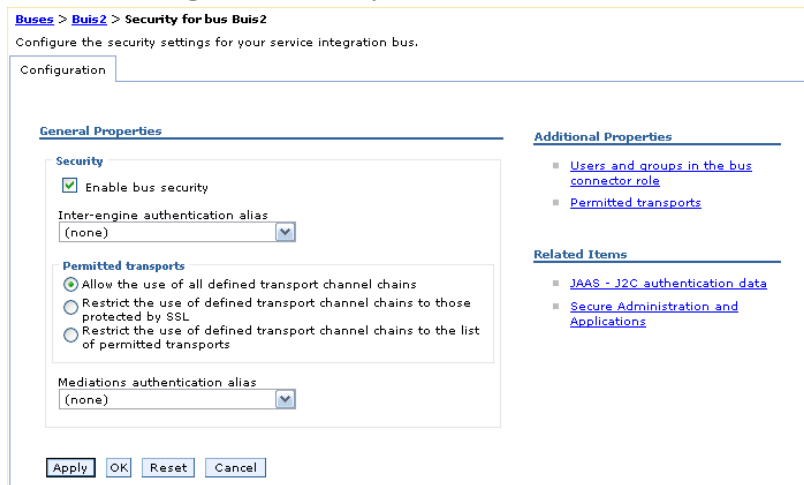
- 7 Set the **High Message Threshold** to 500,000.
- 8 Click **Apply**.
- 9 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Setting Bus Security

To set bus security, perform the following steps:

- 1 In the left panel, expand **Service Integration** and select **Buses**.
- 2 In the table, select the bus you created in [Configuring the Select Identity Service Integration Bus](#) on page 56.
- 3 Under **Additional Properties**, select **Security**.

Figure 34 Setting Bus Security



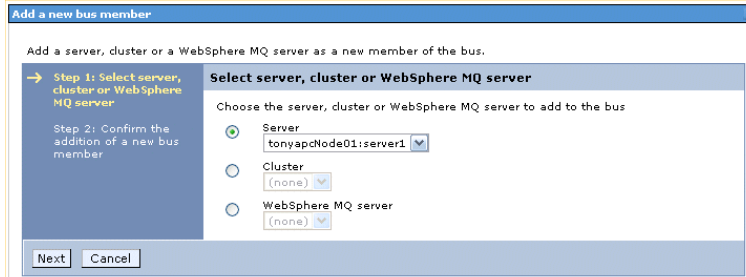
- 4 Select the **Allow use of all defined transport channel chains** option.
- 5 Click **Apply**.
- 6 Click **OK** to return to the previous page.

Adding Bus Members

To add bus members, perform the following steps:

- 1 From the left panel, expand **Service Integration** and select **Buses**.
- 2 In the table, select the bus you created in [Configuring the Select Identity Service Integration Bus](#) on page 56.
- 3 Under **Topology**, select **Bus Members**.
- 4 Click **Add** to add the member appropriate to your WebSphere configuration.

Figure 35 Add Bus Members



- 5 Add a server, cluster, or WebSphere MQ server as a new bus member:
 - For standalone servers, add the WebSphere server as a bus member.
 - For clusters, add your JMS cluster as a bus member.
- 6 Click **Next**.
- 7 Select the **Data Store** option.
- 8 Click **Next**.
- 9 (For MS SQL only) Select the **Use Existing Data Source** option.
- 10 In the **Data Source JNDI Name** field, enter the new member as follows: jdbc/TruAccess_JMS.
- 11 In the **Schema Name** field, enter <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.
- 12 Select the JMS data store **Authentication Alias** (SI Oracle10g_JMS) that you created in [Creating J2C Authentication Data Entries](#) on page 50.
- 13 Select the **Create Tables** option.
- 14 Click **Next**.
- 15 Click **Finish**.
- 16 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating JMS Queue Bus Destinations

This section explains how to create the JMS queue bus destination. The following are important pointers for creating these:

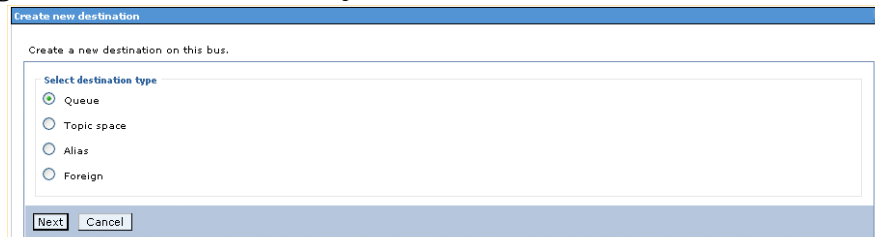
- Assign each JMS queue bus destination to the bus members you created in [Adding Bus Members](#) on page 57.
- Ensure that you enter the value for each identifier in the **Identifier** field *exactly* as listed below in the following list.
- Create a JMS queue bus destination for each of the following:
 - **jms.OVSIAuditProcQ**
 - **jms.OVSIChangeReconProcessorQueue**
 - **jms.OVSIMessageAckQueue**
 - **jms.OVSIReconQueue**

- **jms.OVSI SaudQ**
- **jms.OVSI ServiceAssignQueue**
- **jms.OVSI WorkflowQueue**
- **jms.OVSI SchedulerQueue**
- **jms.OVSI EntCacheQueue**
- **jms.OVSI ResReconQ**
- **jms.OVSI ResReconDispatcherQ**
- **jms.OVSI BulkQueue**
- **jms.OVSI WfRequestExpireQueue**
- **jms.OVSI RecoveryQueue**
- **jms.OVSI UserImportPQueue**
- **jms.OVSI DAProcQ**
- **jms.OVSI KeyRotationQueue**
- **jms.OVSI RecoveryProcQ**

To create a JMS queue bus destination:

- 1 From the left panel, expand to **Service Integration** and select **Buses**.
- 2 In the table, select the bus you created in [Configuring the Select Identity Service Integration Bus](#) on page 56.
- 3 Under **Destination Resources**, select **Destinations**.
- 4 Click **New**.

Figure 36 Create a JMS Queue Bus Destination



- 5 Select the **Queue** option.
- 6 Click **Next**.
- 7 In the **Identifier** field, enter the identifier exactly as defined in the list above.
- 8 Click **Next**.
- 9 Assign the queue to the appropriate bus member.
- 10 Click **Next**.
- 11 Click **Finish**.
- 12 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating JMS Topic Bus Destinations

This section explains how to create the JMS topic bus destinations. The following are important pointers for creating these:

- Assign each JMS topic bus destination to the bus members you created in [Adding Bus Members](#) on page 57.
- Ensure that you enter the value for each identifier in the **Identifier** field *exactly* as listed below in the following list.
- Create a JMS topic bus destination for each of the following:
 - **jms.OVSAuditBroadcast**
 - **jms.OVSCacheTopic**

To create a JMS topic bus destination:

- 1 From the left panel, expand to **Service Integration** and select **Buses**.
- 2 In the table, select the bus you created in [Configuring the Select Identity Service Integration Bus](#) on page 56.
- 3 Under **Destination Resources**, select **Destinations**.
- 4 Click **New**.

Figure 37 Create a JMS Topic Bus Destination



- 5 Select the **Topic space** option.
- 6 Click **Next**.
- 7 In the **Identifier** field, enter the identifier exactly as defined in the list above.
- 8 Click **Next**.
- 9 Assign the queue to the appropriate bus member.
- 10 Click **Next**.
- 11 Click **Finish**.
- 12 Save your changes to the master configuration by clicking **Save** in the **Messages** box 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
- Eighteen 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 JMS Queue Bus Destinations](#) on page 58 and [Creating JMS Topic Bus Destinations](#) on page 60.

Creating JMS Queue Connection Factories

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

- 1 From the left panel, expand **Resources** and select **JMS** → **JMS Providers**.
- 2 Select the **Scope** appropriate to your configuration.
- 3 In the table, select **Default messaging provider**.
- 4 Under **Additional Properties**, click **Queue Connection Factories**.
- 5 Click **New**.

Figure 38 Create JMS Queue Connection Factory

- 6 Set the listed queue connection factory fields as follows:
 - **Name:** `jms.OVSIQCF`
 - **JNDI Name:** `jms/OVSIQCF`
 - **Bus Name:** `OVSIBus`
- 7 Click **Apply**.
- 8 Under **Additional Properties**, select **Connection Pool Properties**.
- 9 Set the **Maximum Connections** field to 100.
- 10 Click **Apply**.
- 11 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating JMS Topic Connection Factories

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

- 1 From the left panel, expand **Resources** and select **JMS** → **JMS Providers**.
- 2 Select the **Scope** appropriate to your configuration.
- 3 In the table, select **Default messaging provider**.
- 4 Under **Additional Properties**, click **Topic Connection Factories**.
- 5 Click **New**.

Figure 39 Create JMS Topic Connection Factory

The screenshot shows the configuration dialog for a JMS Topic Connection Factory. It is divided into several sections:

- General Properties:**
 - Administration:**
 - Scope: [Node=tonyapcNode01]
 - Provider: [Default messaging provider]
 - Name: []
 - JNDI name: []
 - Description: []
 - Category: []
 - Connection:**
 - Bus name: [Select...]
 - Target: []
 - Target type: [Bus member name]
 - Target significance: [Preferred]
- Additional Properties:**
 - Connection pool properties
- Related Items:**
 - JAAS - J2C authentication data
 - Buses

A note on the right states: "The additional properties will not be available until the general properties for this item are applied or saved."

- 6 Set the listed queue connection factory fields as follows:
 - **Name:** `jms.OVSITCF`
 - **JNDI Name:** `jms/OVSITCF`
 - **Bus Name:** `OVSIBus`
- 7 Click **Apply**.
- 8 Under **Additional Properties**, select **Connection Pool Properties**.
- 9 Set the **Maximum Connections** field to 100.
- 10 Click **Apply**.
- 11 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating the JMS Queues

Perform the following steps to create the JMS queues:

- 1 From the left panel, expand **Resources** and select **JMS** → **JMS Providers**.
- 2 Select the **Scope** appropriate to your configuration.
- 3 In the table, select **Default messaging provider**.

- 4 Under **Additional Properties**, select **Queues**.
- 5 Click **New**.

Figure 40 Create the JMS Queues

The screenshot shows the 'General Properties' configuration window for a JMS Queue. It is divided into two main sections: 'Administration' and 'Connection'.
Administration Section:
 - **Scope:** Node=tonyapNode01
 - **Provider:** Default messaging provider
 - **Name:** (empty text field)
 - **JNDI name:** (empty text field)
 - **Description:** (empty text area with scrollbars)
Connection Section:
 - **Bus name:** Select... (dropdown menu)
 - **Queue name:** Select... (dropdown menu)
 - **Delivery mode:** Application (dropdown menu)
 - **Time to live:** (empty text field) milliseconds
 - **Priority:** (empty text field)
 On the right side, there is a 'Related Items' section with a tree view showing 'Buses'.

- 6 Create each of the following JMS queues. Be sure to enter values for the **Name** and **JNDI Name** fields exactly as they are listed in the table.

| Name | JNDI Name |
|--|-----------------------------------|
| jms.OVSIAuditProcQ | jms/OVSIAuditProcQ |
| jms.OVSIChangeReconProcessorQueue | jms/OVSIChangeReconProcessorQueue |
| jms.OVSIMessageAckQueue | jms/OVSIMessageAckQueue |
| jms.OVSIReconQueue | jms/OVSIReconQueue |
| jms.OVSI SaudQ | jms/OVSI SaudQ |
| jms.OVSI ServiceAssignQueue | jms/OVSI ServiceAssignQueue |
| jms.OVSI WorkflowQueue | jms/OVSI WorkflowQueue |
| jms.OVSI SchedulerQueue | jms/OVSI SchedulerQueue |
| jms.OVSI EntCacheQueue | jms/OVSI EntCacheQueue |
| jms.OVSI ResReconQ | jms/OVSI ResReconQ |
| jms.OVSI ResReconDispatcherQ | jms/OVSI ResReconDispatcherQ |
| jms.OVSI BulkQueue | jms/OVSI BulkQueue |
| jms.OVSI WfRequestExpireQueue | jms/OVSI WfRequestExpireQueue |
| jms.OVSI RecoveryQueue | jms/OVSI RecoveryQueue |
| jms.OVSI UserImportPQueue | jms/OVSI UserImportPQueue |

| Name | JNDI Name |
|--------------------------|--------------------------|
| jms.OVSIDAProcQ | jms/OVSIDAProcQ |
| jms.OVSIKeyRotationQueue | jms/OVSIKeyRotationQueue |
| jms.OVSIRecoveryProcQ | jms/OVSIRecoveryProcQ |

- 7 For each queue, set the following fields as listed under **Connection**:
 - **Bus Name:** Select **OVSIBus**.
 - **Queue Name:** Select the name corresponding to the queue.
- 8 Click **Apply** after entering the settings for each queue, before creating the next.
- 9 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating the JMS Topics

Perform the following steps to create the JMS topics:

- 1 From the left panel, expand **Resources** and select **JMS** → **JMS Providers**.
- 2 Select the **Scope** appropriate to your configuration.
- 3 In the table, select **Default messaging provider**.
- 4 Under **Additional Properties**, select **Topics**.
- 5 Click **New**.

Figure 41 Create the JMS Topics

The screenshot shows a configuration form for a JMS Provider. It is divided into two main sections: **Administration** and **Connection**. On the right side, there is a **Related Items** panel showing a tree view with **Buses**.

Administration Section:

- Scope:** Node=tonyapcNode01
- Provider:** Default messaging provider
- Name:** (Empty text field)
- JNDI name:** (Empty text field)
- Description:** (Empty text area)

Connection Section:

- Topic name:** (Empty text field)
- Bus name:** Select.. (Dropdown menu)
- Topic space:** Select.. (Dropdown menu)
- JMS delivery mode:** Application (Dropdown menu)
- Time to live:** (Empty text field) milliseconds

- 6 Create each of the following JMS topics. Be sure to enter values for the **Name** and **JNDI Name** fields exactly as they are listed in the table.

| Name | JNDI Name | Topic Space |
|-------------------------------|------------------------|------------------------|
| jms.OVSIAuditBroadcast | jms/OVSIAuditBroadcast | jms.OVSIAuditBroadcast |
| jms.OVSICacheTopic | jms/OVSICacheTopic | jms.OVSICacheTopic |

► For cluster installations, you must create the `jms.OVSIAuditBroadcast` topic twice—once in the Select Identity cluster and once in the JMS cluster.

- 7 For each topic, set the following fields as listed under **Connection**:
 - **Bus Name:** Select **OVSIBus**.
 - **Topic Name:** Enter the name corresponding to the topic.
- 8 Click **Apply** after entering the settings for each queue, before creating the next.
- 9 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Creating Activation Specifications

Perform the following steps to create the activation specifications:

- 1 From the left panel, expand **Resources** and select **JMS** → **JMS Providers**.
- 2 Select the **Scope** appropriate to your configuration.
- 3 In the table, select **Default messaging provider**.
- 4 Under **Additional Properties**, select **Activation Specifications**.
- 5 Click **New**.

Figure 42 Create the Activation Specifications

The screenshot shows the 'General Properties' dialog box for creating activation specifications. It is divided into two main sections: 'Administration' and 'Destination'.
 In the 'Administration' section:
 - 'Scope' is set to 'Node=tonyapcNode01'.
 - 'Provider' is set to 'Default messaging provider'.
 - 'Name' and 'JNDI name' are empty text input fields.
 - 'Description' is a text area with a scroll bar.
 In the 'Destination' section:
 - 'Destination type' is set to 'Queue' (dropdown menu).
 - 'Destination JNDI name' is an empty text input field.
 - 'Message selector' is an empty text input field.
 - 'Bus name' is a dropdown menu with 'Select...' selected.
 - 'Acknowledge mode' is set to 'Auto-acknowledge' (dropdown menu).
 On the right side, there is a 'Related Items' list with two items: 'JAAS - J2C authentication data' and 'Buses'.

- 6 Set the fields *exactly* as listed for each activation specification in the following table. Select **Queue** as the **Destination Type**, and select **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.OVSIIDAProcQ | eis/OVSIIDAProcQ | jms/OVSIIDAProcQ | 10 |
| eis.OVSIChangeReconProcessorQueue | eis/OVSIChangeReconProcessorQueue | jms/OVSIChangeReconProcessorQueue | 10 |
| eis.OVSIEntCacheQueue | eis/OVSIEntCacheQueue | jms/OVSIEntCacheQueue | 10 |
| eis.OVSIKeyRotationQueue | eis/OVSIKeyRotationQueue | jms/OVSIKeyRotationQueue | 10 |
| eis.OVSIMessageAckQueue | eis/OVSIMessageAckQueue | jms/OVSIMessageAckQueue | 1 |
| eis.OVSIReconQueue | eis/OVSIReconQueue | jms/OVSIReconQueue | 2 |
| eis.OVSIResReconDispatcherQ | eis/OVSIResReconDispatcherQ | jms/OVSIResReconDispatcherQ | 10 |
| eis.OVSIRecoveryProcQ | eis/OVSIRecoveryProcQ | jms/OVSIRecoveryProcQ | 10 |
| eis.OVSIRecoveryQueue | eis/OVSIRecoveryQueue | jms/OVSIRecoveryQueue | 10 |
| eis.OVSIResReconQ | eis/OVSIResReconQ | jms/OVSIResReconQ | 10 |
| eis.OVSIISaudQ | eis/OVSIISaudQ | jms/OVSIISaudQ | 10 |
| eis.OVSIISchedulerQueue | eis/OVSIISchedulerQueue | jms/OVSIISchedulerQueue | 5 |
| eis.OVSIServiceAssignQueue | eis/OVSIServiceAssignQueue | jms/OVSIServiceAssignQueue | 10 |
| eis.OVSIUserImportPQueue | eis/OVSIUserImportPQueue | jms/OVSIUserImportPQueue | 2 |
| eis.OVSIWorkflowQueue | eis/OVSIWorkflowQueue | jms/OVSIWorkflowQueue | 10 |
| eis.OVSIWfRequestExpireQueue | eis/OVSIWfRequestExpireQueue | jms/OVSIWfRequestExpireQueue | 3 |

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

| Name | JNDI Name | Destination JNDI Name | Maximum Concurrent Endpoints |
|------------------------|------------------------|------------------------------|-------------------------------------|
| eis.OVSIAuditBroadcast | eis/OVSIAuditBroadcast | jms/OVSIAuditBroadcast | 1 |
| eis.OVSIICacheTopic | eis/OVSIICacheTopic | jms/OVSIICacheTopic | 10 |

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

- 8 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Configuring the Select Identity Mail

The following sections explain how to configure the Select Identity Mail Provider, SMTP Protocol Provider, and Mail Session.

Configure the Select Identity Mail Provider

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

- 1 From the left panel of the console, expand **Resources** and select **Mail** → **Mail Providers**.
- 2 Set the appropriate **Scope** as specified in [Configuration Scope](#) on page 50.
- 3 Click **New**.

Figure 43 Configure the Select Identity Mail Provider

[Mail Providers](#) > New

Use this page to create a mail provider, an object that encapsulates the protocol providers that your mail application requires. Select the built-in mail provider for access to the three default protocol providers: SMTP, IMAP, and POP3. These protocol providers suffice for most applications.

Configuration

General Properties

* Scope
cells:tonyapcNode01.Cell

* Name

Description

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

- Protocol providers
- Mail sessions
- Custom properties

Apply OK Reset Cancel

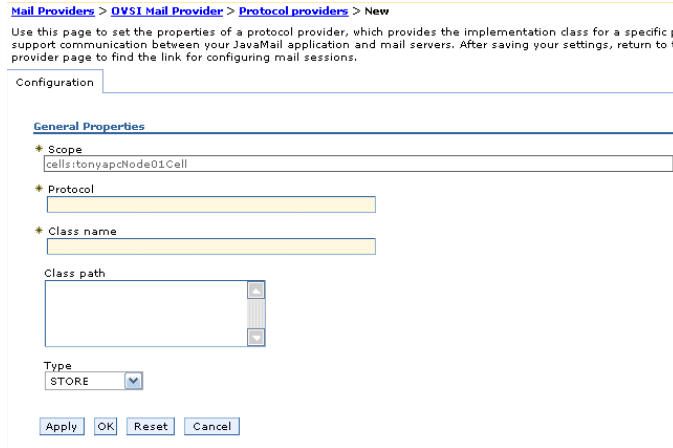
- 4 Set the following mail provider fields:
 - **Name:** OVSI Mail Provider.
 - **Description:** Enter an appropriate description.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Configure the SMTP Protocol Provider

Perform the following steps to create an SMTP protocol provider:

- 1 From the left panel of the console, expand **Resources** and select **Mail** → **Mail Providers**.
- 2 In the table, select the Mail Provider you created in [Configuring the Select Identity Mail](#) on page 67.
- 3 Under **Additional Properties**, select **Protocol Providers**.
- 4 Click **New**.

Figure 44 Configure the SMTP Protocol Provider



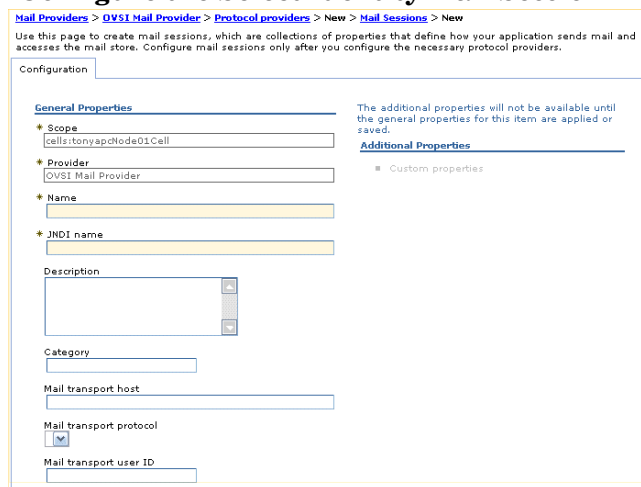
- 5 Set the SMTP protocol provider fields as follows:
 - **Protocol:** smtp
 - **Class name:** com.sun.mail.smtp.SMTPTransport
 - **Type:** TRANSPORT
- 6 Click **Apply**.
- 7 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Configuring the Select Identity Mail Session

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

- 1 From the left panel of the console, expand **Resources** and select **Mail** → **Mail Providers**.
- 2 In the table, select the Mail Provider you created in [Configuring the Select Identity Mail](#) on page 67.
- 3 Under **Additional Properties**, select **Mail Sessions**.
- 4 Click **New**.

Figure 45 Configure the Select Identity Mail Session



- 5 Set the mail session fields as follows:

- **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
- 6 Click **Apply**.
 - 7 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Deploying Select Identity and the Online Help

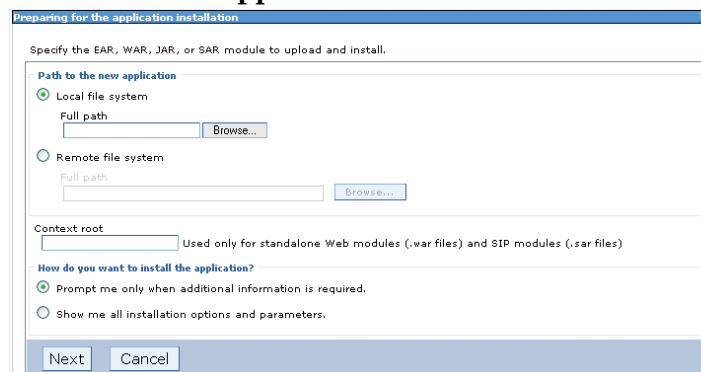
Select Identity is provided as an Enterprise Application Repository (.ear) file, for deployment through the WebSphere **Install New Application** page.

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 From the left panel, expand **Applications** and select **Install New Application**.

Figure 46 Install New Application



- 2 Under **Path to the New Application**, select **Remote File System**.
- 3 Next browse to the Select Identity home directory created in [Creating Directories and Copying Files](#) on page 49.
- 4 Open the \deploy directory, select was6_lmz.ear, and click **OK**.
- 5 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.
- 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.
 - ▶ Steps 12-18 are only displayed if you uncheck the “Prompt me only when additional information is required” option.
- 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.

For the `was6_lmz.ear` deployment, you should see the following settings on **Summary** 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 | |
| Distribute application | Yes |
| Deploy Web services | No |
| Pre-compile JSP | No |
| Deploy enterprise beans | No |

- 17 Click **Finish** after you have reviewed the installation options.
- 18 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 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

The following sections discuss updating the Select Identity application settings.

Set the Class Loader Mode and WAR Class Load Policy

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

- 1 From the left panel, expand **Applications** and select **Enterprise Applications**.
- 2 In the table, select your Select Identity application.
- 3 Under **Detail Properties**, select **Class Loading and Update Detection**.

Figure 47 Set the Class Loader Mode and WAR Class Load Policy

Enterprise Applications > DefaultApplication > Class loader

Use this page to configure the reloading of classes when application files are updated.

Configuration

General Properties

Reload classes when application files are updated

Polling interval for updated files
1000 Seconds

Class loader order

Classes loaded with parent class loader first

Classes loaded with application class loader first

WAR class loader policy

Class loader for each WAR file in application

Single class loader for application

Apply OK Reset Cancel

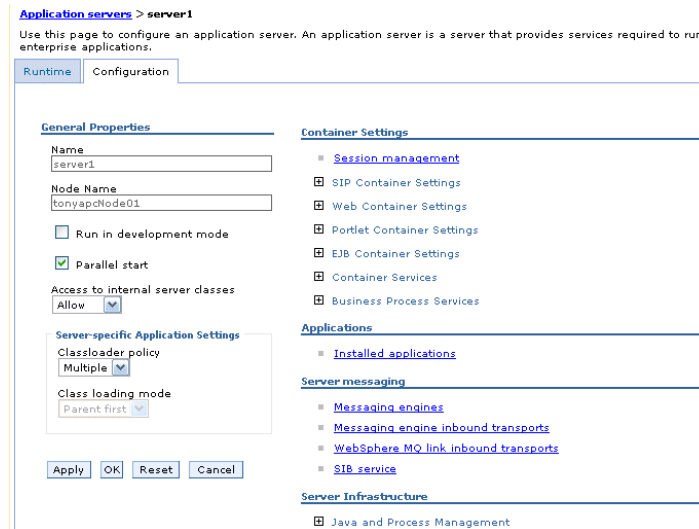
- 4 Make the following selections:
 - Enter a value (in seconds) for **Polling Interval for Updated Files**.
 - Select **Classes loaded with application class loader first**.
 - Select **Class loader for each WAR file in application**.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Set the Transaction Timeout

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

- 1 From the left panel, expand **Servers** and select **Application Servers**.
- 2 In the table, select the application server or each cluster node in turn.

Figure 48 Set the Transaction Timeout



- 3 Under **Container Settings**, select **Container Services** → **Transaction Services**.
- 4 Set the field labeled **Total Transaction Lifetime Timeout** to 300.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

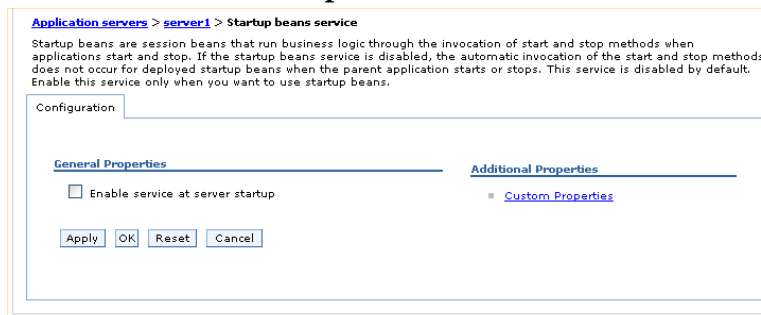
Enabling the Startup Bean Service

The following section explains how to enable the startup bean service for your application servers or clusters within a server.

To enable the startup bean service, perform the following steps:

- 1 From the left panel, expand **Servers** and select **Application Servers**.
- 2 In the table, select the application server, or each cluster node in turn.
- 3 On the **Configuration** tab, select **Container Settings** → **Container Services** → **Startup Beans Service**.

Figure 49 Enable the Startup Bean Service



- 4 Select the **Enable service at server startup** checkbox.
- 5 Click **Apply**.
- 6 Click **OK** to return to the previous page.

Configuring the Java Virtual Machine

The following section discusses configuring the Java Virtual Machine.

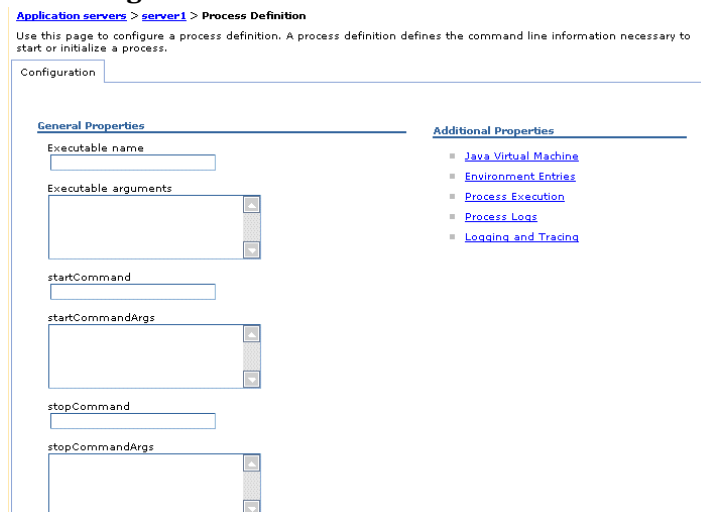
For cluster installations, perform the following steps for each server in the Select Identity cluster.

For standalone installations, perform the following steps for the WebSphere server.

To configure the Java Virtual Machine, perform the following steps:

- 1 From the left panel, expand **Servers** and select **Application Servers**.
- 2 In the table, select the application server, or each cluster node in turn.
- 3 Under **Server Infrastructure**, expand **Java and Process Management** item and select **Process Definition**.

Figure 50 Configure Java Virtual Machine



- 4 On the **Process Definition** page, under **Additional Properties**, select **Java Virtual Machine**.
- 5 On the **Java Virtual Machine** page, set the listed fields as follows:
 - **Generic JVM arguments (HP-UX only):**

```
"-Dcom.truologica.truaccess.property.file=<SI_Install_Dir>/sysArchive/TruAccess.properties -Djava.awt.headless=true"
```
 - **Generic JVM arguments (Linux only):**

```
"-Dcom.truologica.truaccess.property.file=<SI_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 by clicking **Save** in the **Messages** box at the top of the page.

Configuring Logging for Select Identity

Configure logging for Select Identity by setting the logging file location. This procedure is not essential, but is strongly recommended.

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

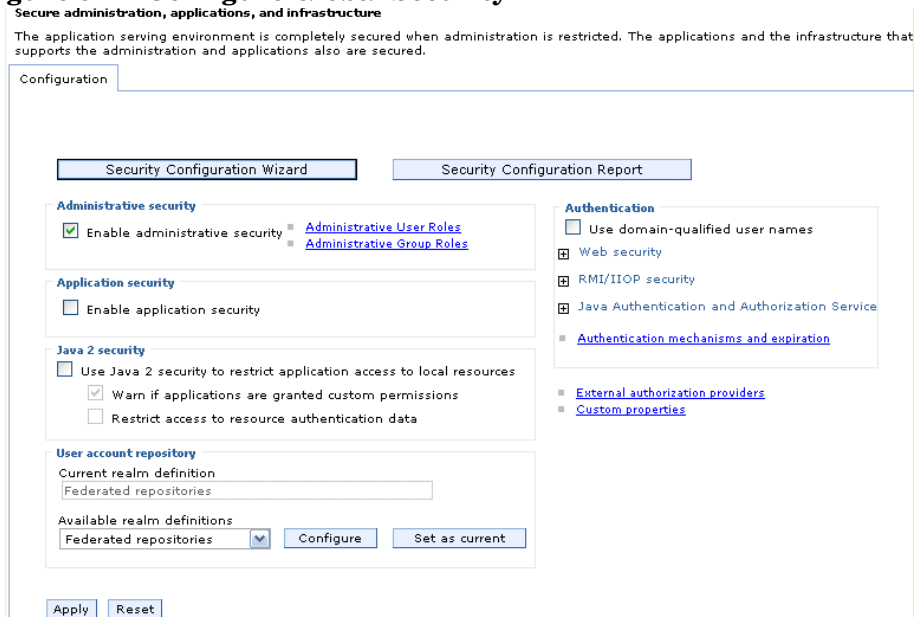
- 1 From the left panel, expand **Troubleshooting** and select **Logs and Trace**.
- 2 In the table, select the application server, or each cluster node in turn.
- 3 Under **General Properties**, select **JVM Logs**.
- 4 Change the content of the **File Name** field to reflect the directory location 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 by clicking **Save** in the **Messages** box at the top of the page.

Configuring Global Security

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

- 1 From the left panel, expand **Security** and select **Secure administration, applications, and infrastructure**.
- 2 Ensure that the setting labeled **Use Java 2 security to restrict application access to local resources** is disabled, unless you choose to use Java 2 security. For more information on configuring Java 2 security, see [Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security](#) on page 33.

Figure 51 Configure Global Security



- 3 Check **Enable administrative security** and configure the user account repository as desired. See the IBM Websphere technical documentation for more information.
- 4 Click **Apply**.

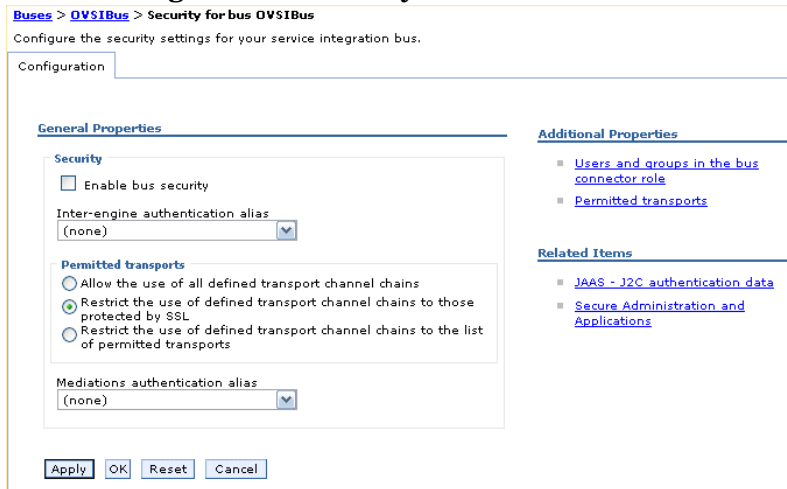
- 5 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 6 From the left panel, expand **Environment** and select **Naming** → **CORBA Naming Service Groups**.
- 7 In the table, select **Everyone**.
- 8 Enable **Read** and **Write** permissions for this group.
- 9 Click **Apply**.
- 10 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

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 From the left panel, expand **Service integration** → **Buses**.
- 2 In the table, select **OVSIBus**.
- 3 Under **Additional Properties**, select **Security**.

Figure 52 Configure Bus Security



- 4 Uncheck the **Enable bus security** setting.
- 5 Click **Apply**.
- 6 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

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.

▶ Before the Select Identity application can be used, you must restart the Deployment Manager, Node Managers, and application servers. If you are *not* using Java 2 Security as discussed in [Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security](#) on page 33, you can restart these systems now. If you *are* using Java 2 Security, you should restart these systems after the RunAs roles are set. This is discussed in [Chapter 6, Configuring Select Identity](#).

There are additional configuration steps for WebSphere installations. See [Chapter 6, Configuring Select Identity](#) to finish the process.



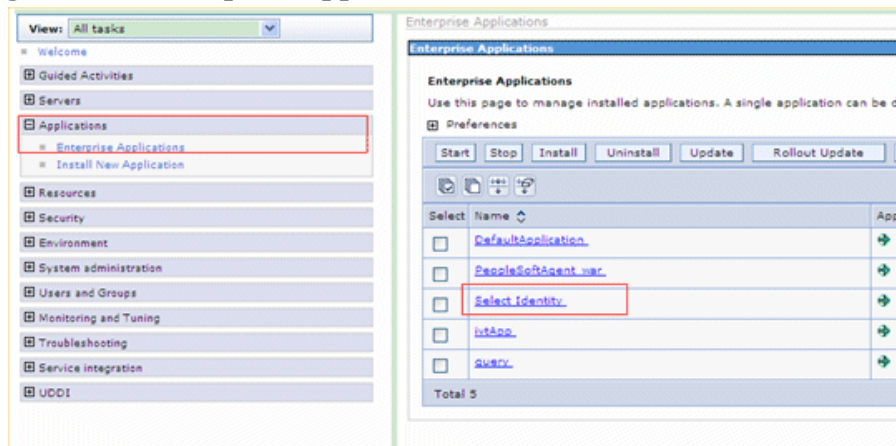
Do not launch the Select Identity application until you have set up the security framework as described in [Setting Up Keystores, Truststores, and Security Framework](#) on page 160. This is a critical step.

Updating the Classloading Strategy of attributemapper.war

After you have successfully installed Select Identity, you must manually update the classloading strategy of the attributemapper.war file. To do so:

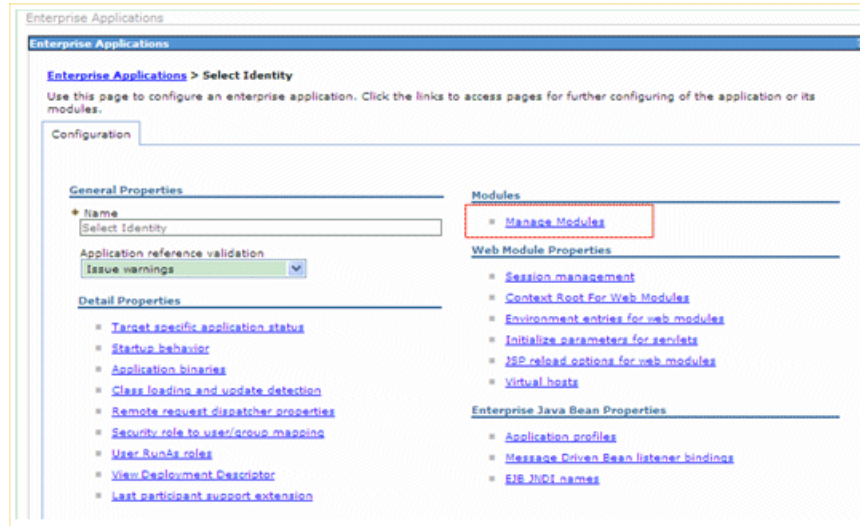
- 1 Log on to the WebSphere application server console.
- 2 From the left panel, select **Applications** → **Enterprise Applications**.

Figure 53 Enterprise Applications Table



- 3 Click on **Select Identity**.
The **General Properties** page opens.

Figure 54 General Properties



- 4 Under **Modules**, click **Manage Modules**.

A list of modules appears:

Figure 55 Manage Moduels

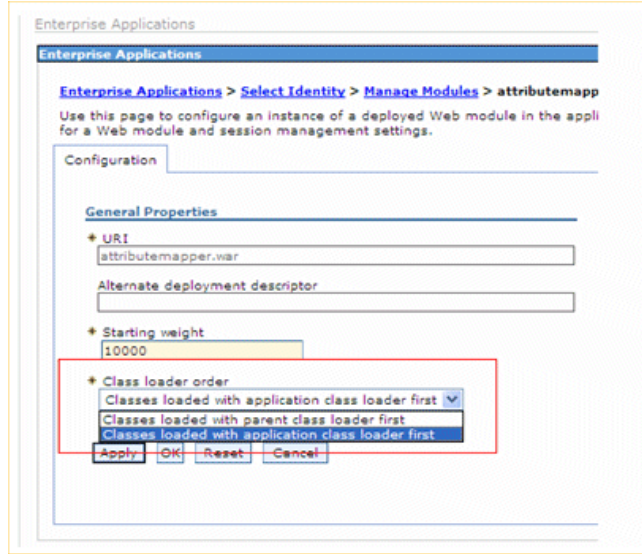
| | | | |
|--------------------------|--------------------------------------|--|------------|
| <input type="checkbox"/> | Generated by XDoclet | std_batchExecEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_flowcontrolEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_ovsdintegrationEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_ovsisecurityhelperEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_archivemgrEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_datapolicyEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_keyrotationjobEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | Generated by XDoclet | std_appInitEjb.jar,META-INF/ejb-jar.xml | EJB Module |
| <input type="checkbox"/> | SelectIdentity | lmz.war,WEB-INF/web.xml | Web Module |
| <input type="checkbox"/> | attributemapper.war | attributemapper.war,WEB-INF/web.xml | Web Module |
| <input type="checkbox"/> | Apache-Axis2 | ovsiAxis2.war,WEB-INF/web.xml | Web Module |

OK Cancel

- 5 Click on **attributemapper.war**.

The **General Properties** page opens.

Figure 56 General Properties



- 6 Under **Class loader order**, select **Classes loaded with application class loader first**.
- 7 Click **Apply**.
- 8 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Configuring WebSphere for Mutual Authentication

You must perform this procedure to configure WebSphere system security parameters and enable mutual authentication, secure object migration, and key rotation features.

Prerequisites

The following conditions must be met before you can perform either procedure:

- You have installed WebSphere on your application server.
- Your WebSphere application has been configured for Select Identity.
- You have administrative privileges to the WebSphere server.
- You know the keystore and truststore file locations.
- You know how your business uses SSL and Select Identity.
- You have identified whether you will be using Select Identity in secure or regular HTTP mode.
- You have determined, if Select Identity is running in secure mode only, if all client browsers will be required to have signed certificates.

Procedure – Single Server

Setting up a single WebSphere server to enable mutual authentication requires modifications to the following WebSphere settings, each of which is explained in a detailed procedure in sections that follow:

- [Set Up Security](#) on page 79
- [Set Up the Environment](#) on page 84
- [Set Up the Servers](#) on page 86

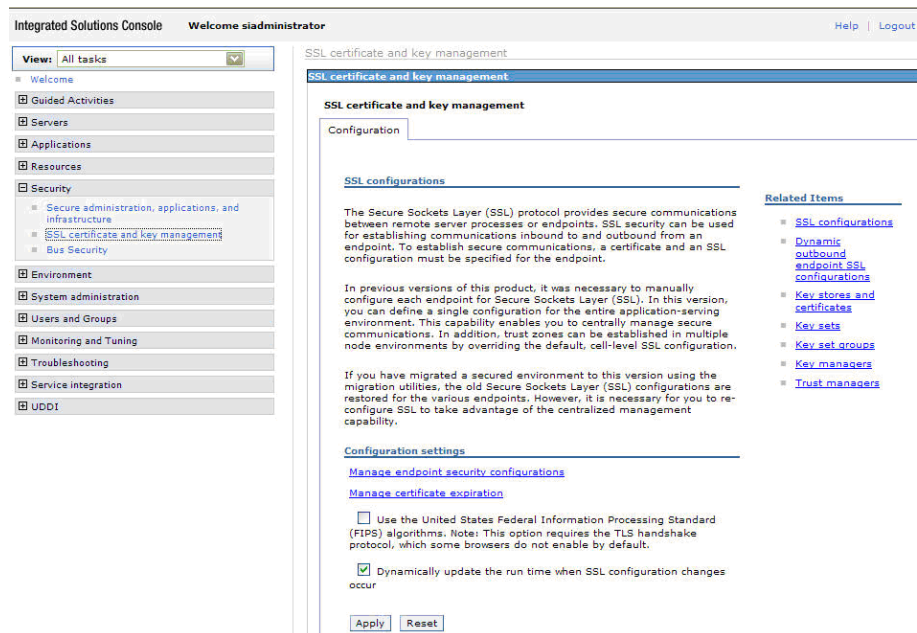
Set Up Security

To set up the WebSphere application server security parameters to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 Log on to the WebSphere application server console.
- 2 From the left panel, select **Security** → **SSL Certificate and Key Management**.

The **SSL Certificate and Key Management** page opens.

Figure 57 SSL Certificate and Key Management

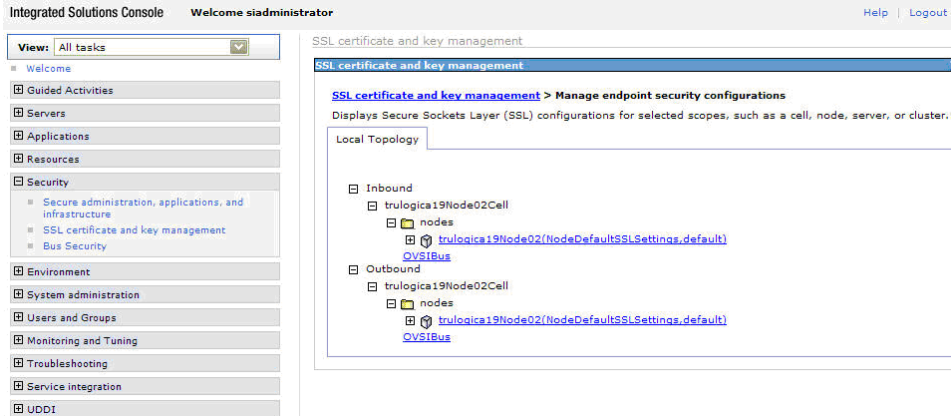


- 3 Click the **Manage endpoint security configurations** link.

The **Manage endpoint security configurations** page opens.

- 4 Under **Local Topology**, expand the **Inbound** section.

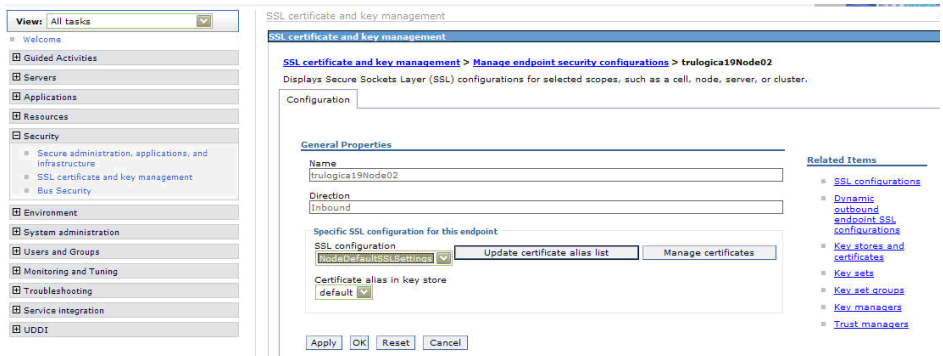
Figure 58 Local Topology - Inbound Section



5 Select the **Inbound** default node.

The **General Properties** page for the default inbound node displays.

Figure 59 General Properties - Inbound Node



6 From the **Specific SSL configuration for this endpoint** dropdown, select **NodeDefaultSSLSettings**.

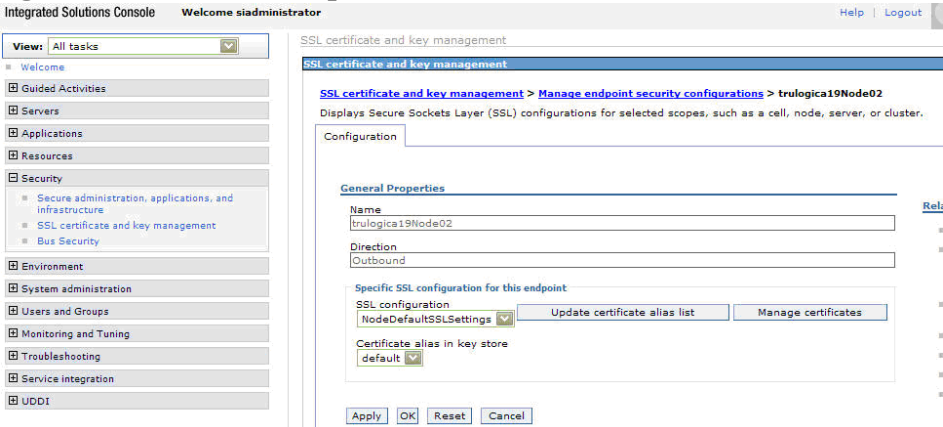
7 Click **OK**.

8 Under **Local Topology**, expand the **Outbound** section.

9 Select the **Outbound** default node.

The **General Properties** page for the default outbound node displays.

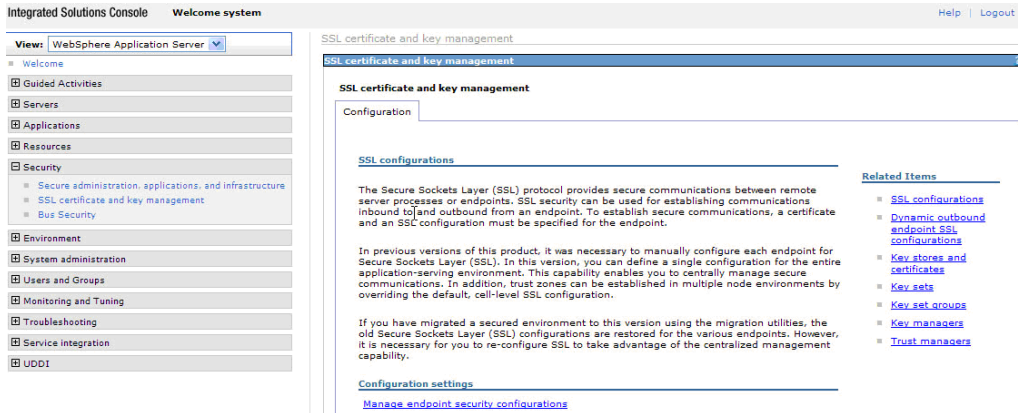
Figure 60 General Properties - Outbound Node



- 10 From the **Specific SSL configuration for this endpoint** dropdown, select **NodeDefaultSSLSettings**.
- 11 Click **OK**.
- 12 Verify that your settings are saved by WebSphere.
- 13 From the left panel, select **Security** → **SSL Certificate and Key Management**.

The **SSL Certificate and Key Management** page opens.

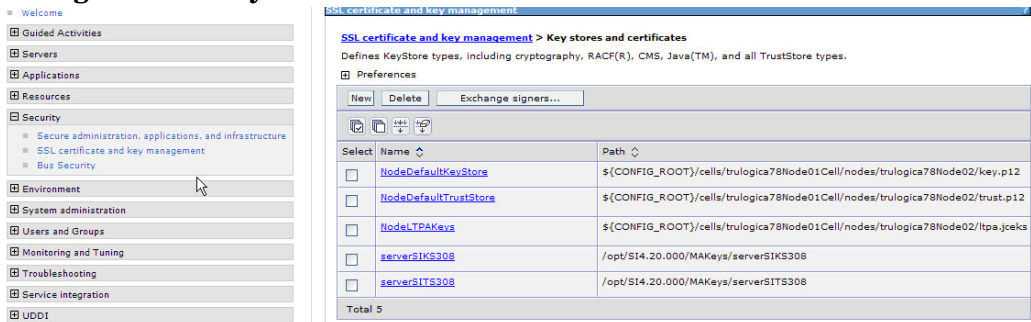
Figure 61 SSL Certificate and Key Management



- 14 Under **Related Items**, select **Keystores and Certificates**.

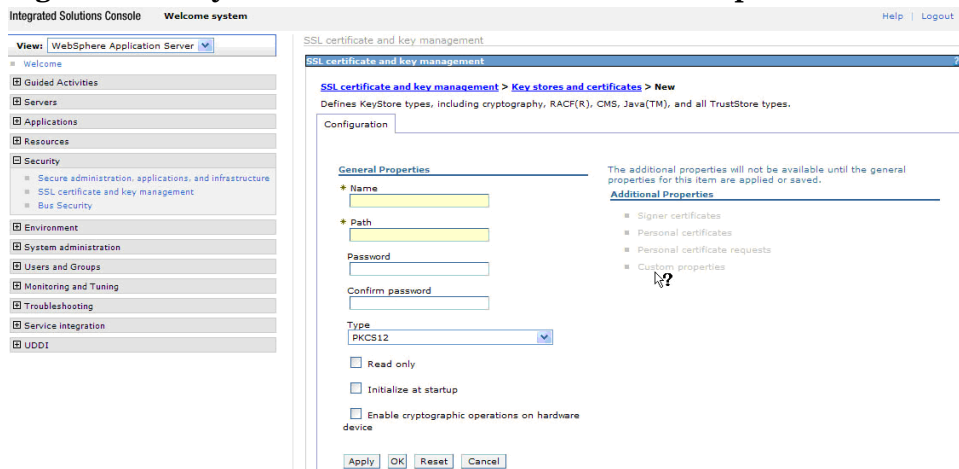
The **Keystores and Certificates** page opens.

Figure 62 Keystores and Certificates



- 15 Click **New** to create your keystore.

Figure 63 Keystores and Certificates - General Properties

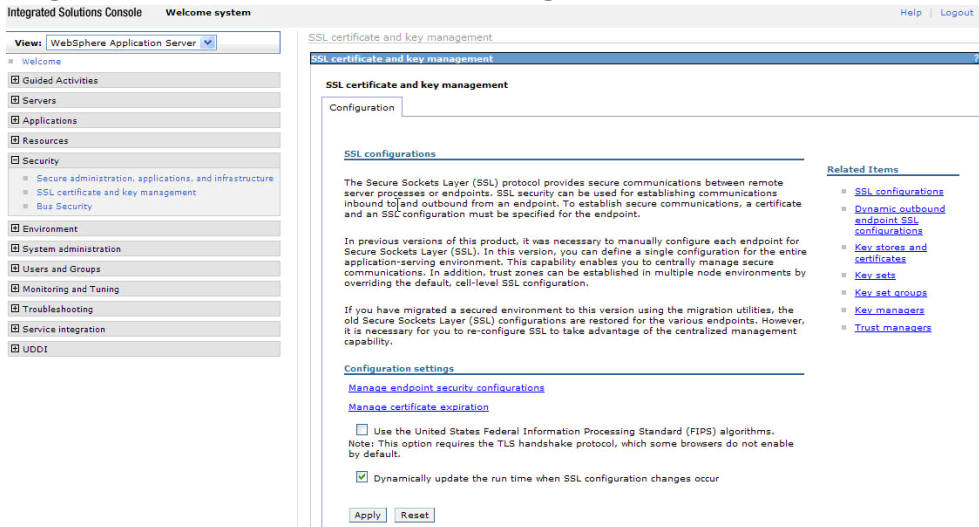


- 16 Under the **General Properties** section, complete the following fields:
 - Enter a name for your keystore in the **Name** field.
 - Enter the file path of your keystore in the **Path** field.
 - Enter a keystore password in the **Password** field.
 - Select the keystore type (JKS, JCEKS, etc.) from the **Type** list.
- 17 Click **OK**.

The **Keystores and Certificates** page opens.
- 18 Click **New** to create your truststore.
- 19 Under the **General Properties** section, complete the following fields:
 - Enter a name for your truststore in the **Name** field.
 - Enter the file path of your truststore in the **Path** field.
 - Enter a truststore password in the **Password** field.
 - Select the truststore type (JKS, JCEKS, etc.) from the **Type** list.
- 20 Click **OK**.
- 21 From the left panel, select **Security** → **SSL Certificate and Key Management**.

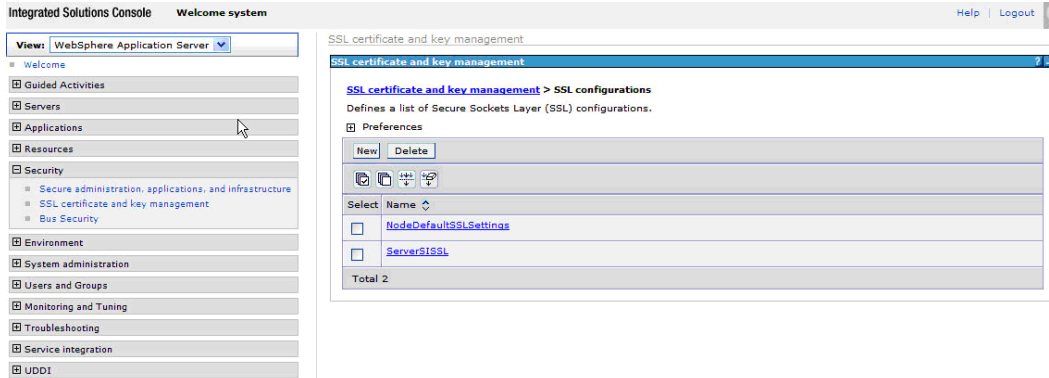
The **SSL Certificate and Key Management** page opens.
- 22 Under **Related Items**, select **SSL Configurations**.

Figure 64 Related Items - SSL Configurations



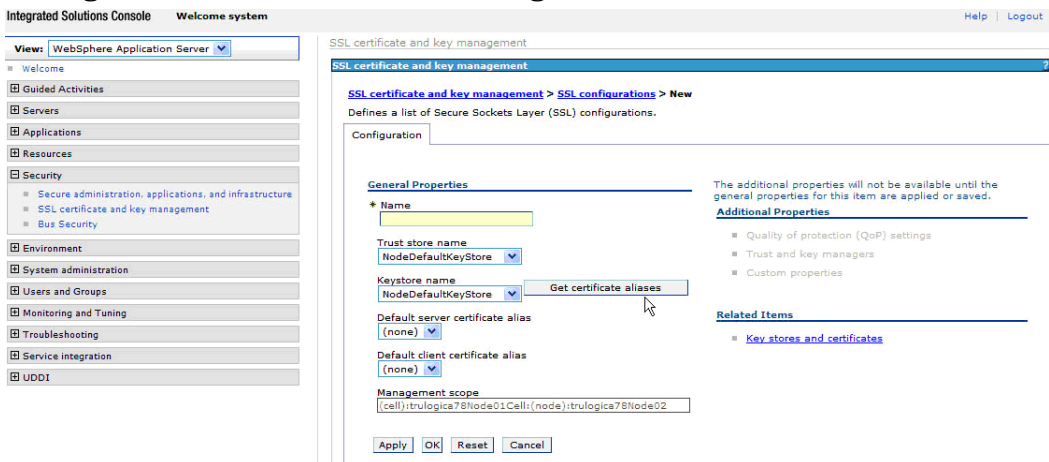
The **SSL Configurations** page opens.

Figure 65 SSL Configurations



23 Click **New** to create an SSL configuration.

Figure 66 Create New SSL Configuration



24 Under **General Properties**, enter a name for the new SSL configuration in the **Name** field.

25 In the **Truststore name** field, enter the name of the truststore you just created.

26 In the **Keystore name** field, enter the name of the keystore you just created.

27 Click **Get Certificate Aliases**.

This option populates the server and client certificate alias fields with your available choices.

28 Select your default server certificate alias from the **Default Server Certificate Aliases** list.

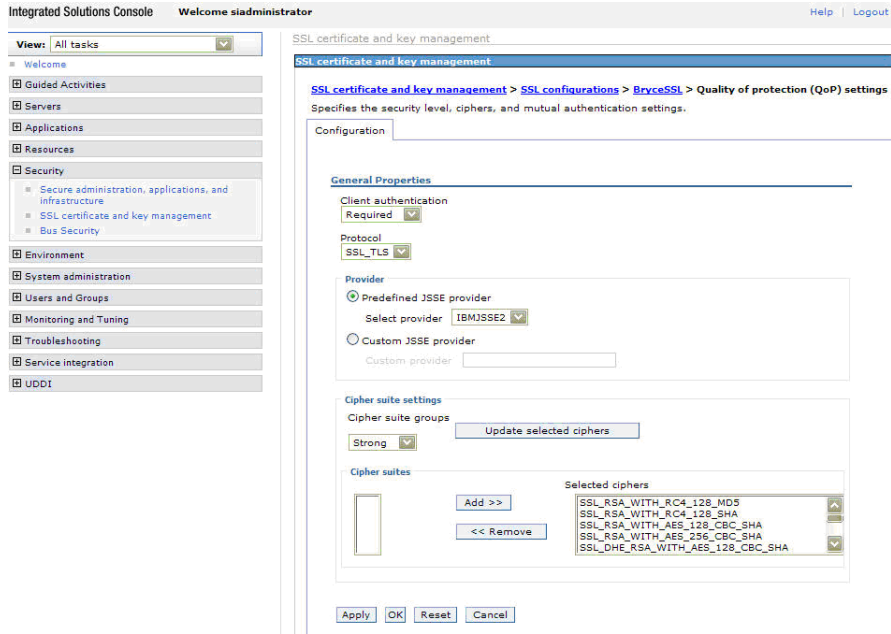
29 Select your default client certificate alias from the **Default Client Certificate Aliases** list.

30 Click **OK**.

31 Under **General Properties**, select **Quality of Protection (QoP) Settings**.

The **Quality of Protection (QoP) Settings** page opens. Use this page to select a level of authentication and other protection parameters that may be required for your environment.

Figure 67 Quality of Protection (QoP) Settings



- 32 From the **Client Authentication** list, select **Required**.
- 33 Click **OK**.
- 34 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

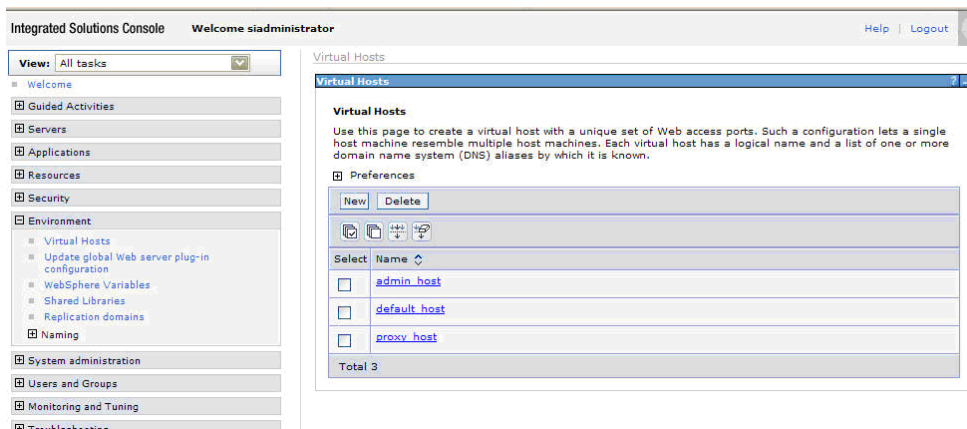
Set Up the Environment

To set up the environment for your WebSphere application servers to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 From the left panel, select **Environment** → **Virtual Hosts**.

The **Virtual Hosts** page opens.

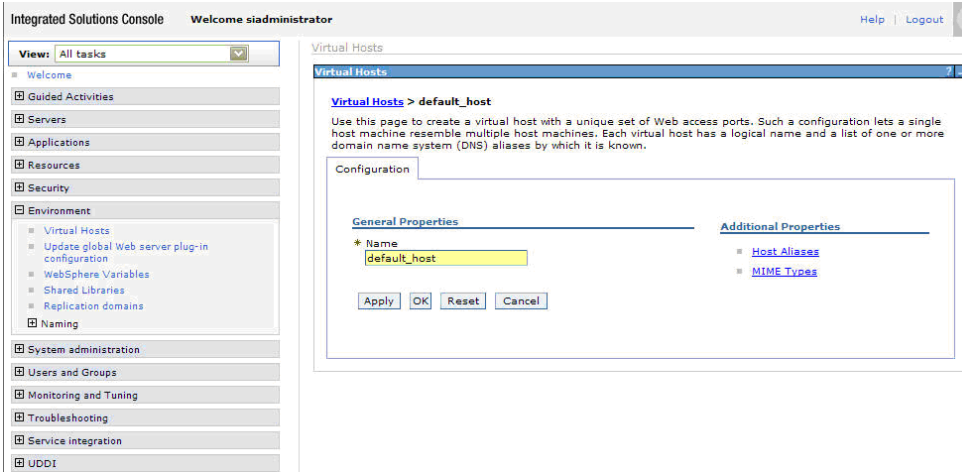
Figure 68 Virtual Hosts



- 2 From the **Virtual Hosts** page, select **Default Host**.

The **Virtual Hosts Default Host** page opens. Use this page to set parameters for the **Default Host**.

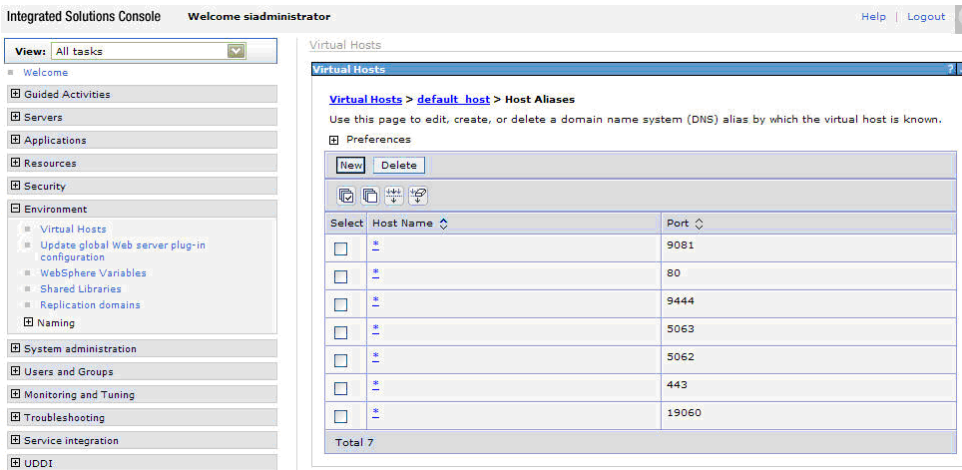
Figure 69 Virtual Hosts - Default Host



3 From the **Default Host** page, select **Host Aliases**.

The **Host Aliases** page opens.

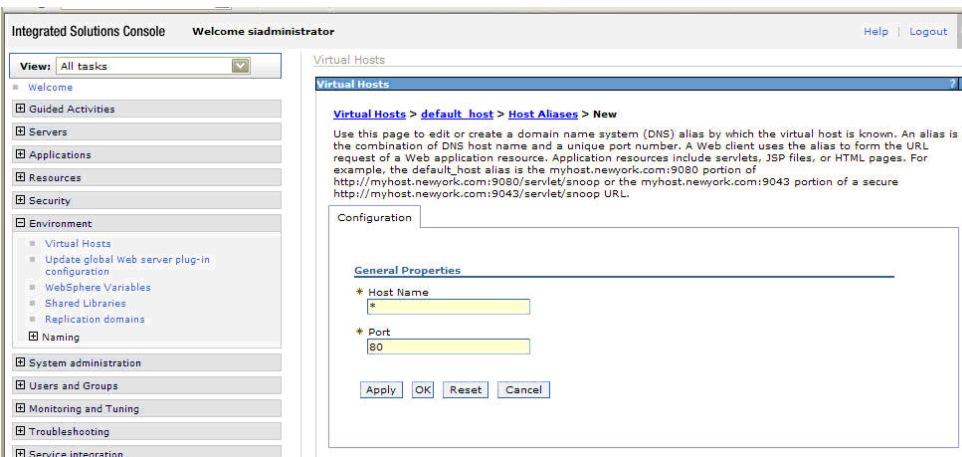
Figure 70 Host Aliases



4 From the **Host Aliases** page, click **New**.

The **New Host Aliases** page opens. Use this page to create an alias name for the new host.

Figure 71 New Host Aliases



5 Enter a unique port number in the **Port** field.

- 6 Click **OK**.
- 7 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

Set Up the Servers

To set up WebSphere application servers to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 From the left panel, select **Servers** → **Application Servers**.

The **Application Servers** page opens. This page displays a list of servers that are available.

- 2 Select the server you want to configure.

The **Configuration** page opens for the server you selected. You can now modify your server settings.

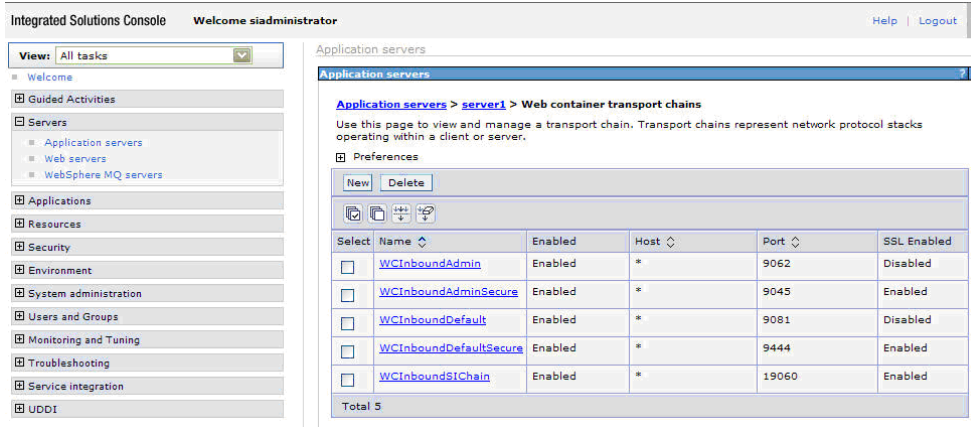
Figure 72 Application Server - Configuration



- 3 Under **Container Settings**, expand **Web Container Settings**.
- 4 Select **Web Container Transport Chains**.

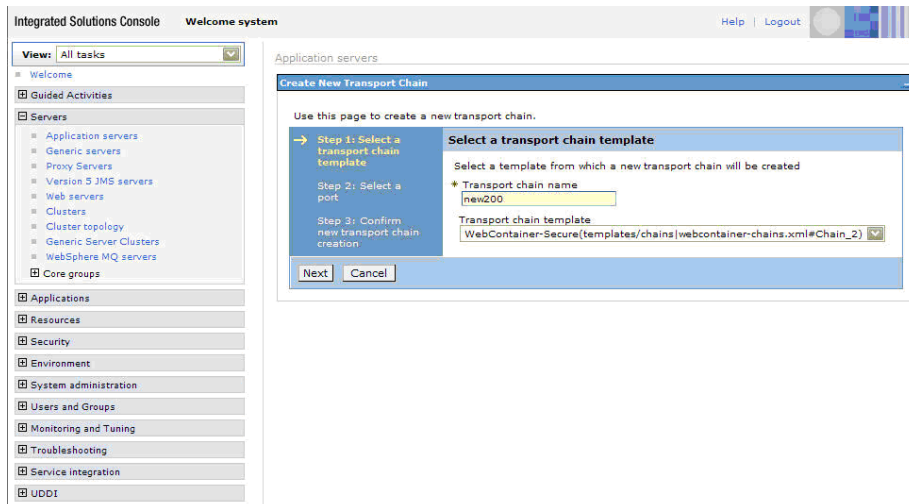
The **Web Container Transport Chains** page opens.

Figure 73 Web Container Transport Chains



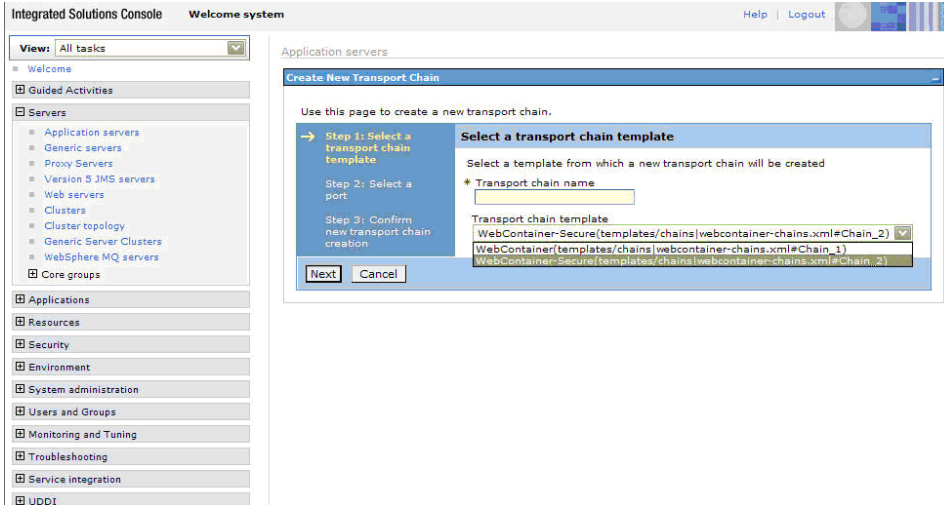
- 5 From the **Web Container Transport Chains** page, click **New**.
The **Create New Transport Chain** page opens.

Figure 74 Create New Transport Chain



- 6 Enter the transport chain name in the **Transport Chain Name** field. For example: WCInboundSICChain.
- 7 Select the secure chain template from the **Transport Chain Template** list.

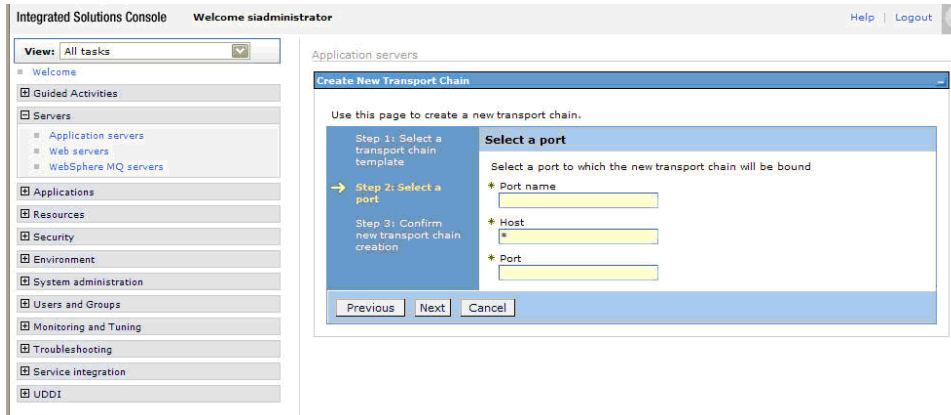
Figure 75 Create New Transport Chain



8 Click **Next**.

The **Create New Transport Chain - Select a Port** page opens. Use this page to identify the port for the new transport chain.

Figure 76 Create New Transport Chain



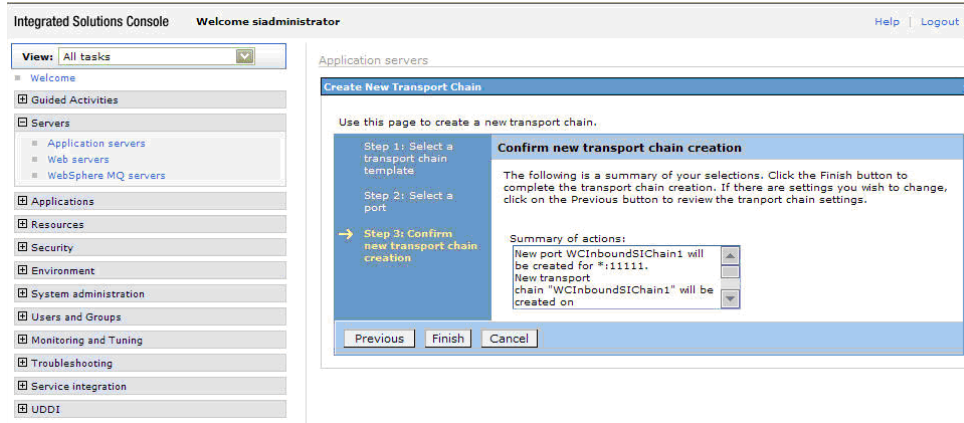
9 In the **Port Name** field, enter the name of the port that you created in [Set Up the Environment](#) on page 84.

10 In the **Port** field, enter the port number that you defined in [Set Up the Environment](#) on page 84.

11 Click **Next**.

The **Confirm New Transport Chain Creation** new transport chain creation page opens.

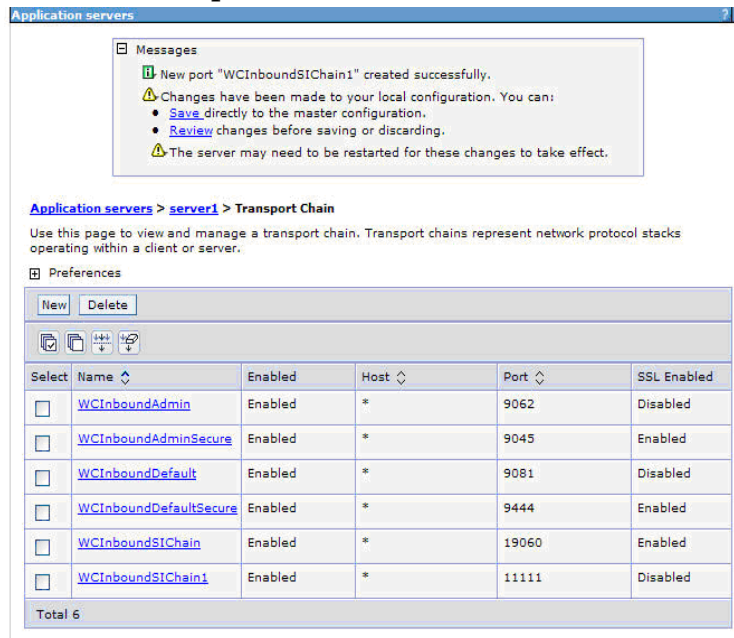
Figure 77 Confirm New Transport Chain Creation



12 Verify you have entered the correct information and click **Finish**.

The **Transport Chain** page reopens with the new transport chain displayed in the list.

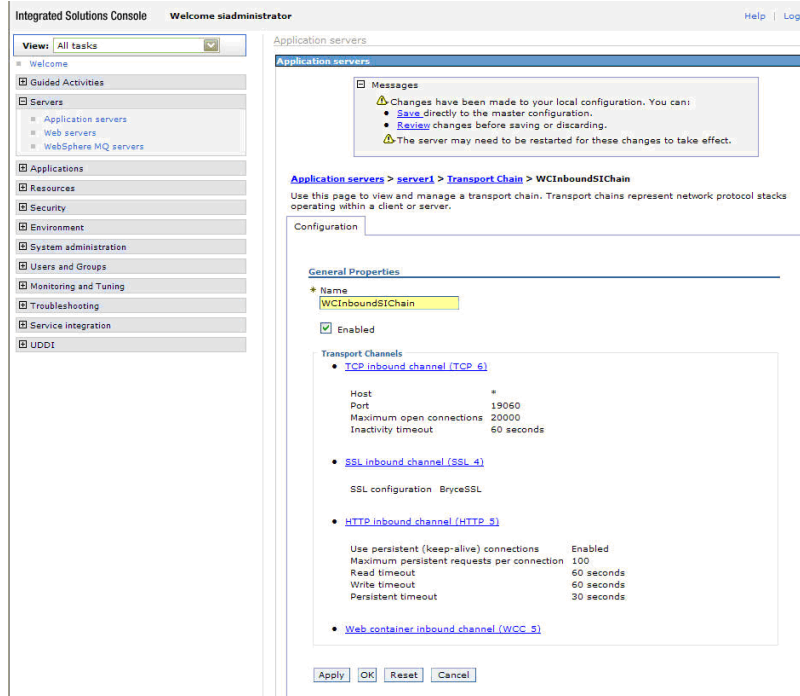
Figure 78 New Transport Chain



13 Select the new transport chain.

The **General Properties** page for the new transport chain opens.

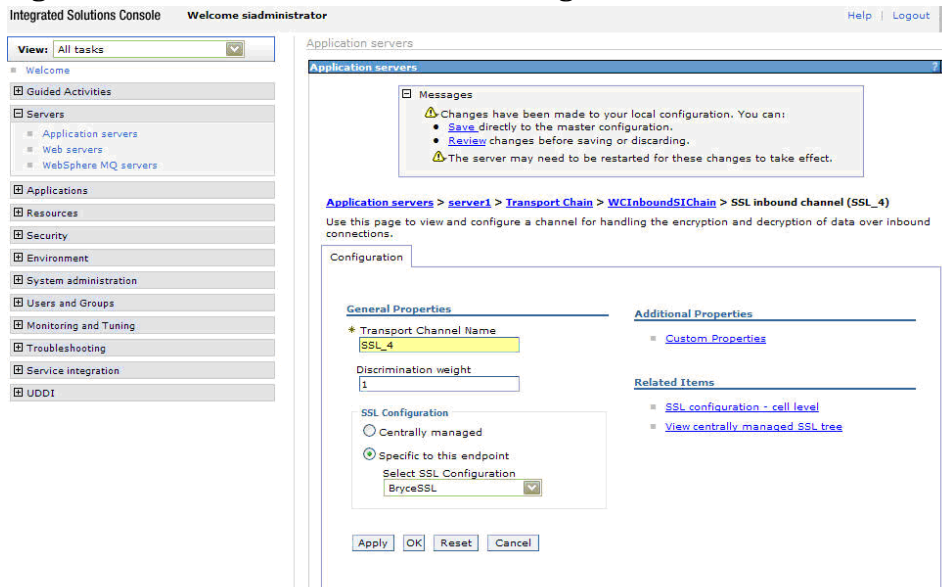
Figure 79 Transport Chain - General Properties



14 Under **General Properties**, select **SSL Inbound Channel**.

The **SSL Inbound Channel Configuration Parameters** page opens.

Figure 80 SSL Inbound Channel Configuration Parameters



15 Under **SSL Configuration**, select **Specific to this endpoint**.

16 From the **Select SSL Configuration** list, select the name of the SSL configuration you created in **Set Up Security** on page 79.

17 Click **OK**.

18 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

19 Restart the server.

- 20 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. Refer to the *HP Select Identity Administration Online Help*.

Procedure – Clustered Servers

Setting up a cluster or multiple clusters of WebSphere servers to enable mutual authentication is very similar to that of configuring a single server. Although some of the steps may appear to be the same, to avoid confusion, the entire cluster configuration process is documented in this section in the following detailed procedures:

- [Set Up Security](#) on page 91
- [Set Up the Environment](#) on page 97
- [Set Up the Servers](#) on page 99

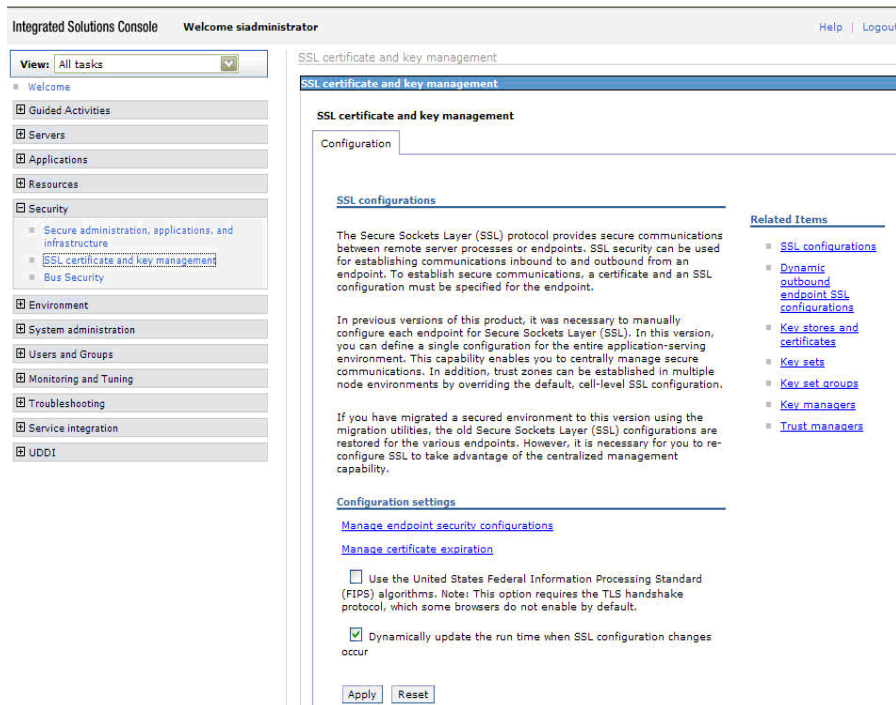
Set Up Security

To set up cluster server security parameters to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 Log on to the WebSphere application server console.
- 2 From the left panel, select **Security** → **SSL Certificate and Key Management**.

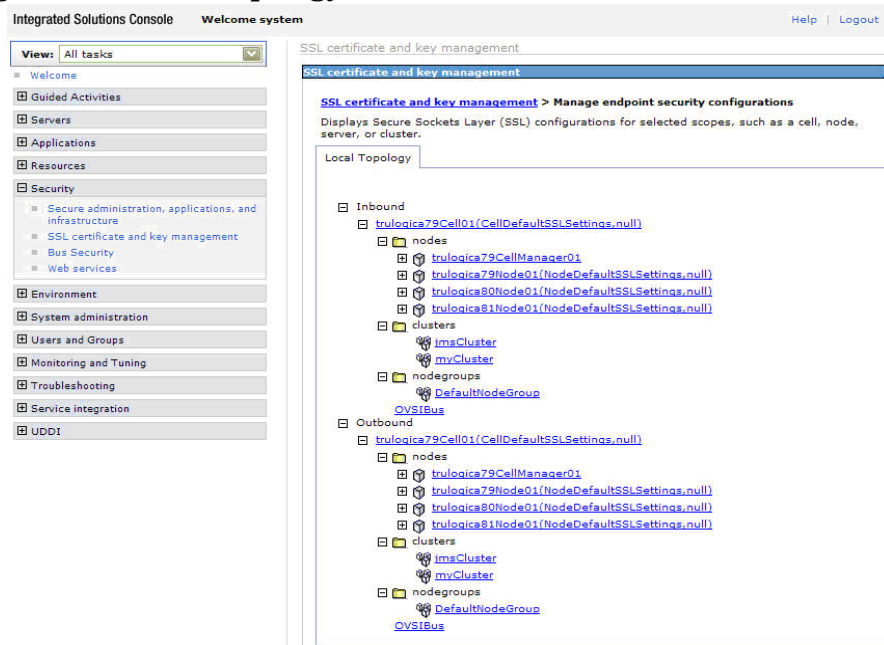
The **SSL Certificate and Key Management** page opens.

Figure 81 SSL Certificate and Key Management



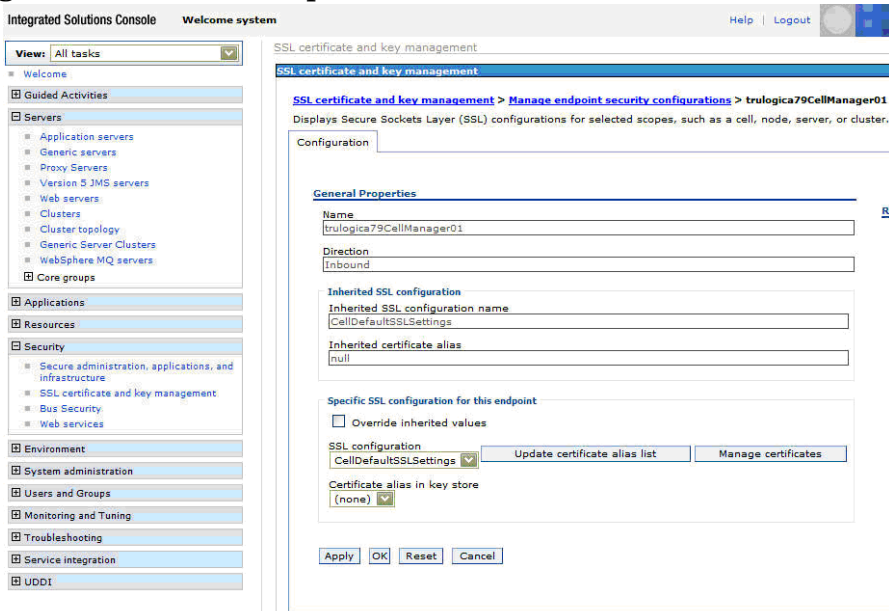
- 3 Select **Manage endpoint security configurations**.
The **Manage endpoint security configurations** page opens.
- 4 Under **Local Topology**, expand the **Inbound** section.

Figure 82 Local Topology - Inbound Section



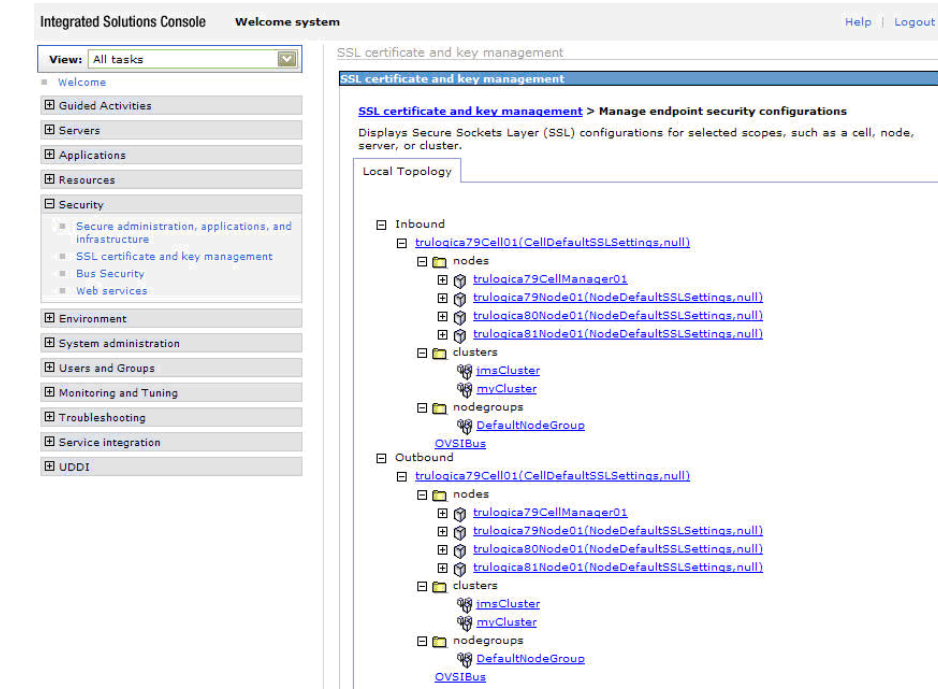
- 5 Expand the inbound default node.
Each inbound cluster node is now visible.
- 6 Select the first node in the cluster.
The **General Properties** page for the node opens.

Figure 83 General Properties - Inbound Node



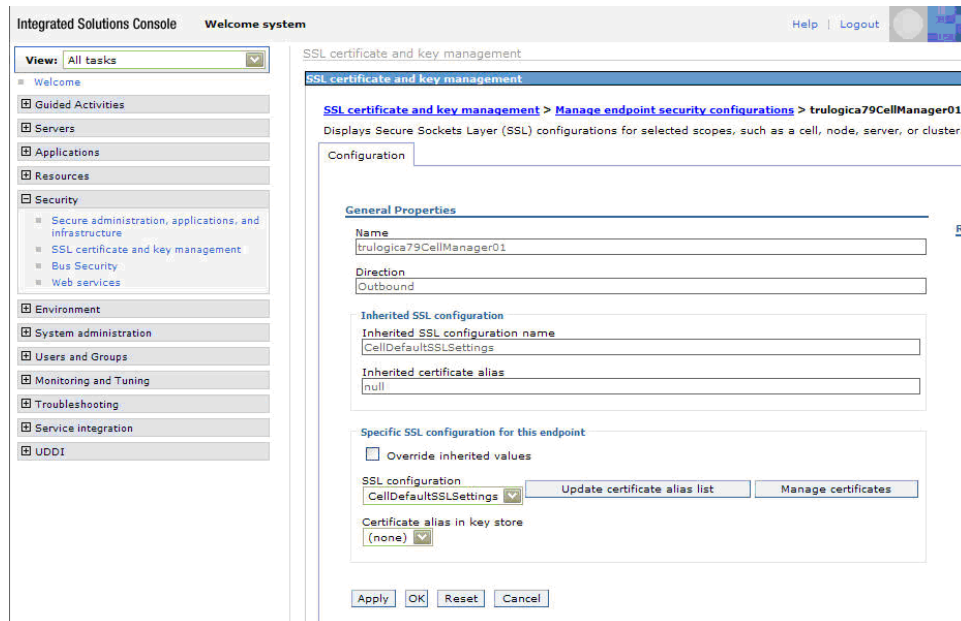
- 7 From the **Specific SSL configuration for this endpoint** dropdown, select **NodeDefaultSSLSettings**.
- 8 Click **OK**.
- 9 Repeat these steps for each outbound cluster node.
- 10 Under **Local Topology**, expand the **Outbound** section.

Figure 84 Local Topology - Outbound Node



- 11 Expand the outbound default node.
Each outbound cluster node is now visible.
- 12 Select the first node in the cluster.
The **General Properties** page for the node opens.

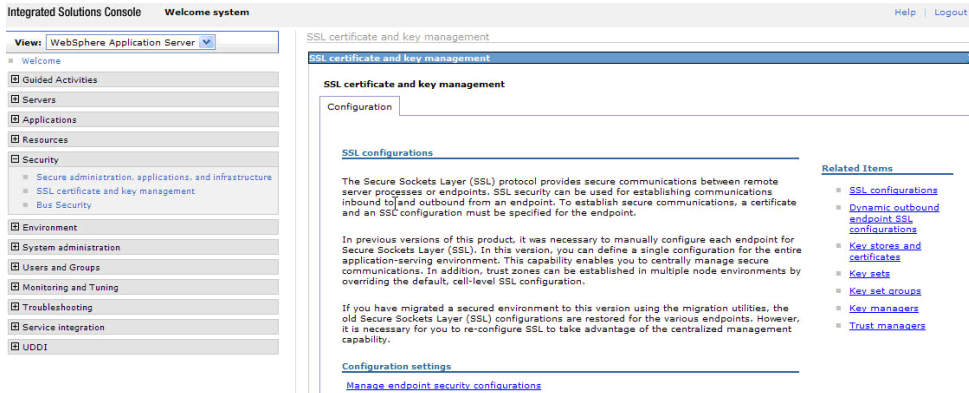
Figure 85 General Properties - Outbound Node



- 13 From the **Specific SSL configuration for this endpoint** dropdown, select **NodeDefaultSSLSettings**.
- 14 Click **OK**.
- 15 Repeat these steps for each inbound cluster node.

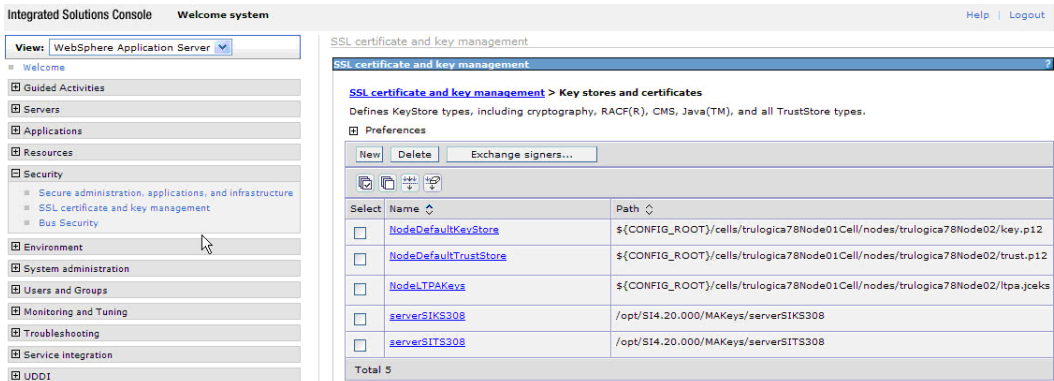
- 16 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 17 From the left panel, select **Security** → **SSL Certificate and Key Management**.
- 18 The **SSL Certificate and Key Management** page opens.

Figure 86 SSL Certificate and Key Management



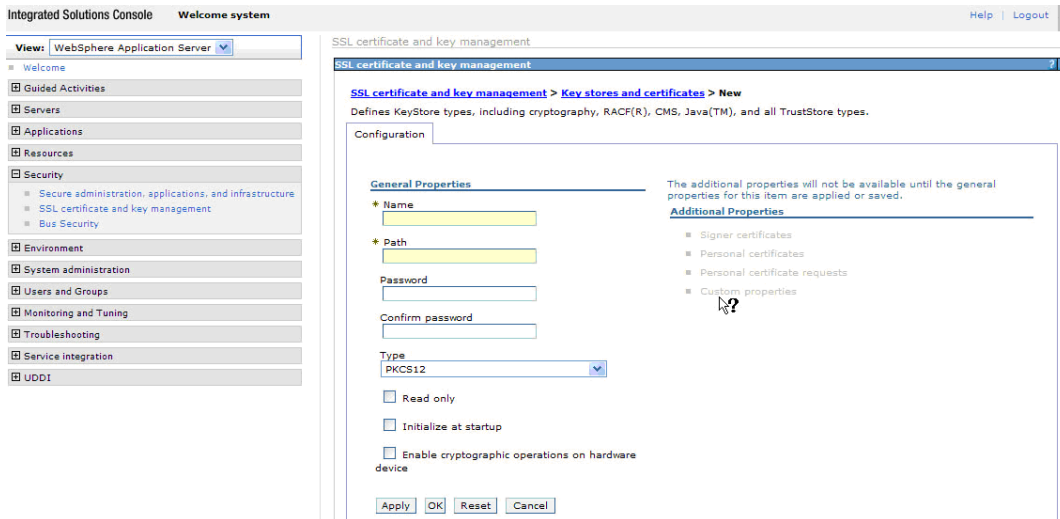
- 19 Under **Related Items**, select **Keystores and Certificates**.
- 20 The **Keystores and Certificates** page opens.

Figure 87 Keystores and Certificates



- 21 Click **New** to create a new keystore.
The **General Properties** page opens to create a new keystore.

Figure 88 Keystores and Certificates - General Properties



22 Under the **General Properties** section, complete the following fields:

- Enter a name for your keystore in the **Name** field.
- Enter the file path of your keystore in the **Path** field.
- Enter a keystore password in the **Password** field.
- Select the keystore type (JKS, JCEKS, etc.) from the **Type** list.

23 Click **OK**.

The **Keystores and Certificates** page opens.

24 Click **New** to create a truststore.

The **General Properties** page opens to create a new truststore.

25 Under the **General Properties** section, complete the following fields:

- Enter a name for your truststore in the **Name** field.
- Enter the file path of your truststore in the **Path** field.
- Enter a truststore password in the **Password** field.
- Select the truststore type (JKS, JCEKS, etc.) from the **Type** list.

26 Click **OK**.

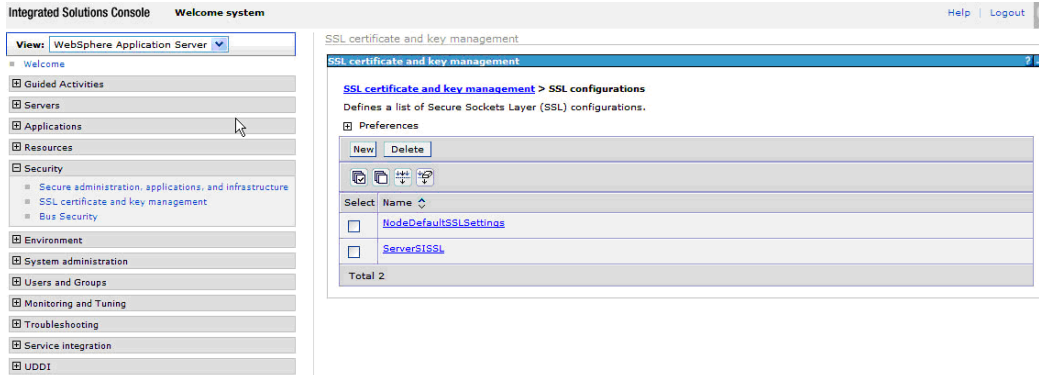
27 From the left panel, select **Security** → **SSL Certificate and Key Management**.

28 The **SSL Certificate and Key Management** page opens, as illustrated in [Set Up Security](#) on page 79.

29 Under **Related Items**, select **SSL Configurations**.

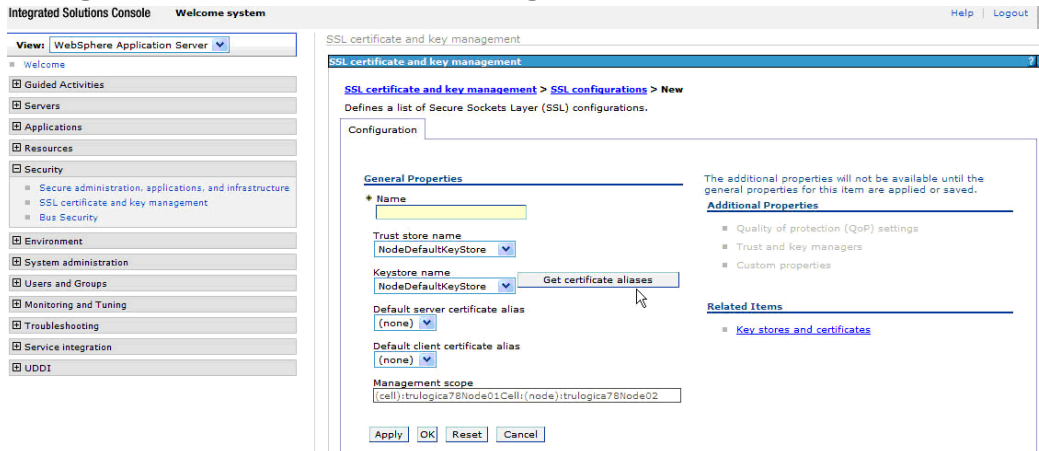
The **SSL Configurations** page opens.

Figure 89 SSL Configurations



30 Click **New** to create an SSL configuration.

Figure 90 Create New SSL Configuration



31 Under **General Properties**, enter a name for the new SSL configuration in the **Name** field.

32 In the **Truststore name** field, enter the name of the truststore you just created.

33 In the **Keystore name** field, enter the name of the keystore you just created.

34 Click **Get Certificate Aliases**.

This populates the server and client certificate alias fields with your available choices.

35 Select your default server certificate alias from the **Default server certificate alias** list.

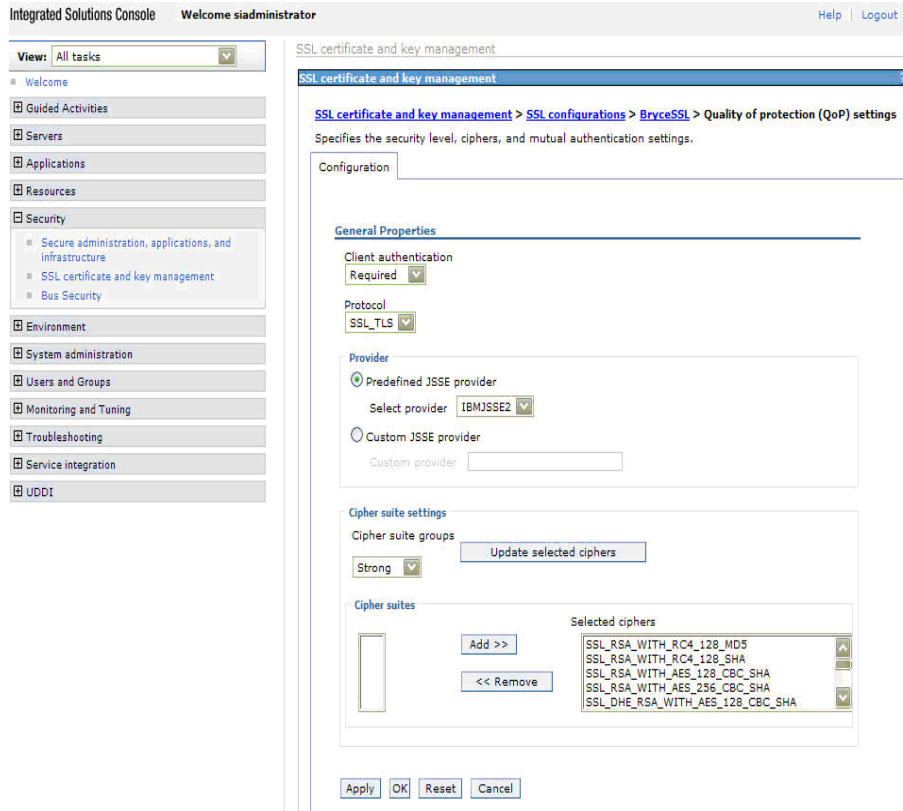
36 Select your default client certificate alias from the **Default server certificate alias** list.

37 Click **OK**.

38 Under **Additional Properties**, select **Quality of Protection (QoP)**.

The **Quality of Protection (QoP) Settings** page opens. Use this page to select a level of authentication and other protection parameters that may be required for your environment.

Figure 91 Quality of Protection (QoP) Settings



- 39 In the **Client Authentication** field, select **Required** from the list.
- 40 Click **OK**.
- 41 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

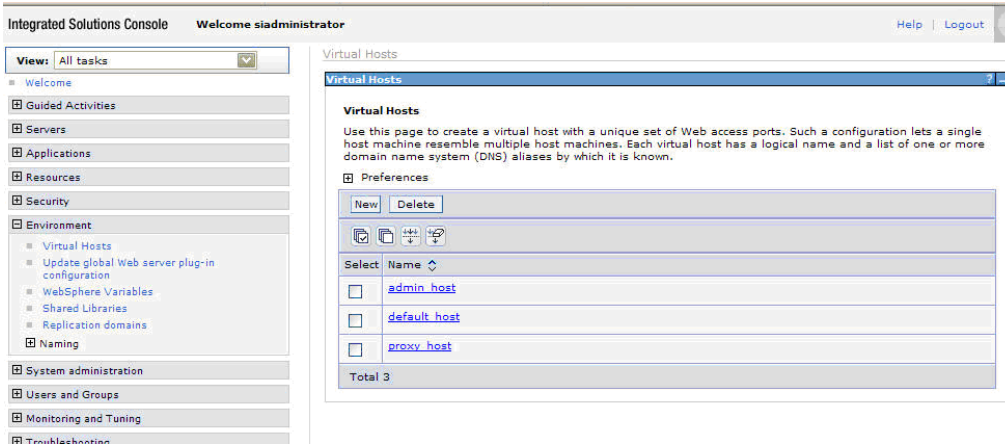
Set Up the Environment

To set up your cluster server environment to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 From the left panel, select **Environment** → **Virtual Hosts**.

The **Virtual Hosts** page opens.

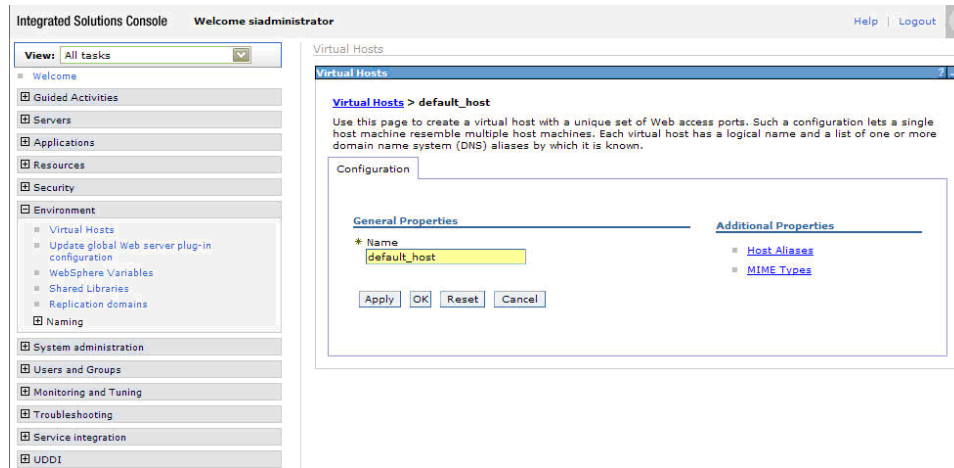
Figure 92 Virtual Hosts



2 From the **Virtual Hosts** page, select **default_host**.

The **Virtual Hosts default_host** page opens.

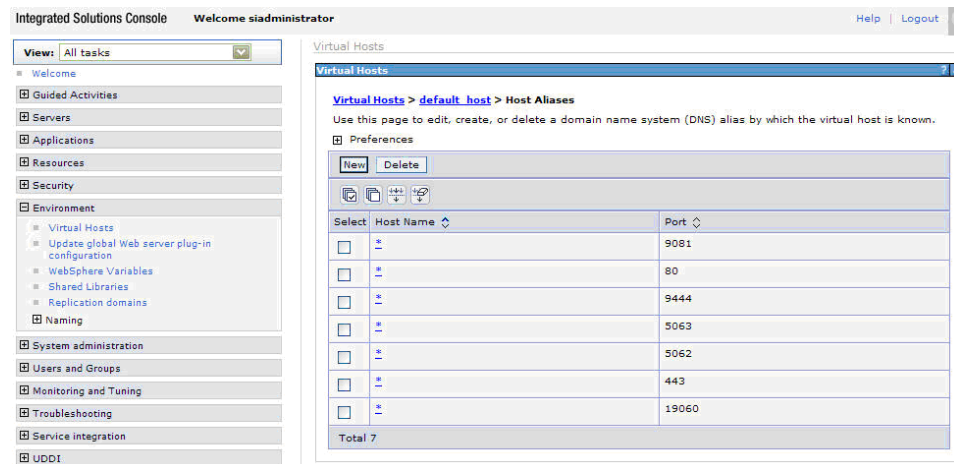
Figure 93 Virtual Hosts - Default Host



3 From the **default_host** page, select **Host Aliases**.

The **Host Aliases** page opens.

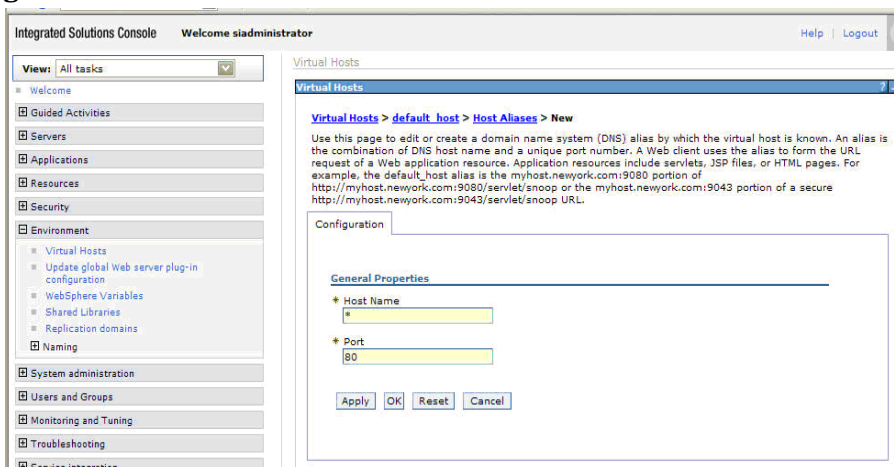
Figure 94 Host Aliases



4 From the **Host Aliases** page, click **New**.

The **New Host Aliases** page opens. Use this page to create an alias name for the new host.

Figure 95 New Host Aliases



- 5 Enter a unique port number in the **Port** field.
- 6 Click **OK**.
- 7 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.

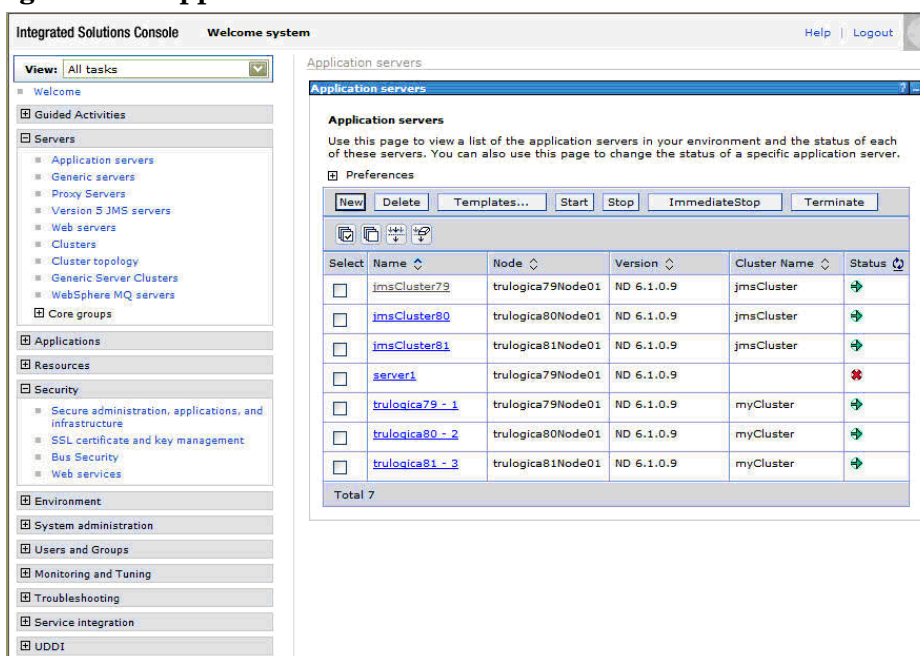
Set Up the Servers

To set up WebSphere application cluster servers to work with Select Identity when mutual authentication is implemented, perform the following steps.

- 1 From the left panel, select **Servers** → **Application Servers**.

The **Application Servers** page opens. This page displays a list of servers that are available.

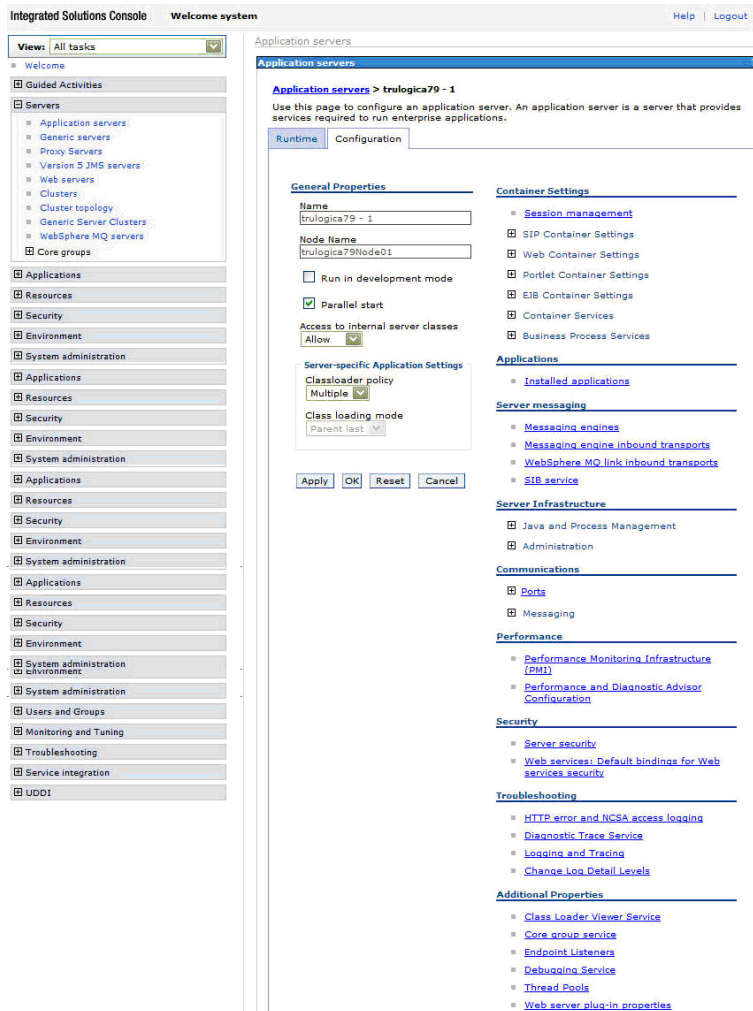
Figure 96 Application Servers



- 2 Select the cluster server you want to configure.

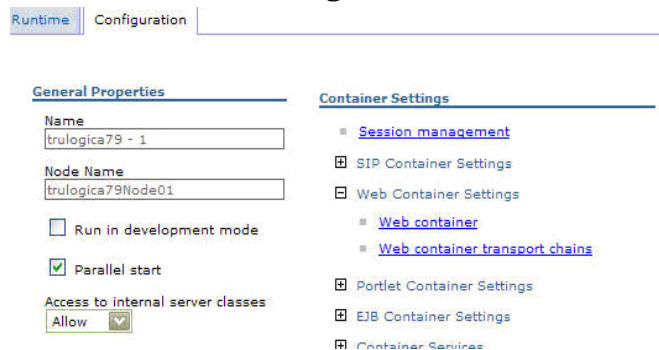
The **Configuration** page opens for the cluster server you selected. You can now modify your cluster server settings.

Figure 97 Server Configuration



3 Under **Container Settings**, expand **Web Container Settings**.

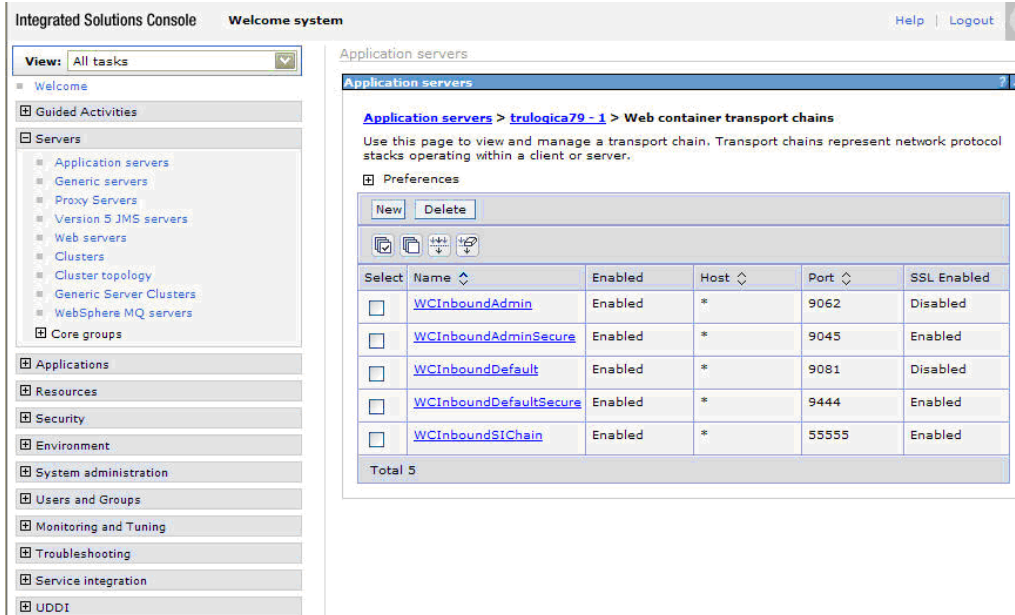
Figure 98 Web Container Settings



4 Under **Web Container Settings**, select **Web Container Transport Chains**.

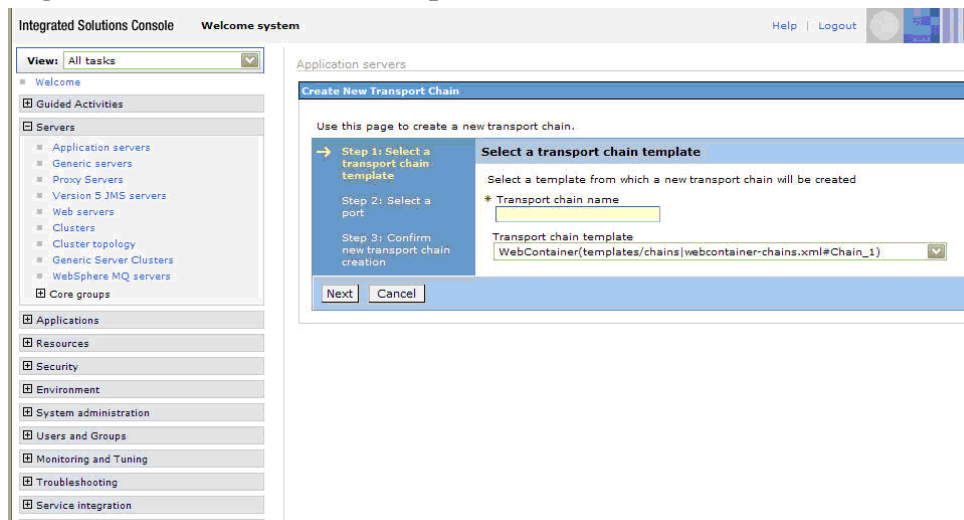
The **Web Container Transport Chains** page opens.

Figure 99 Web Container Transport Chains



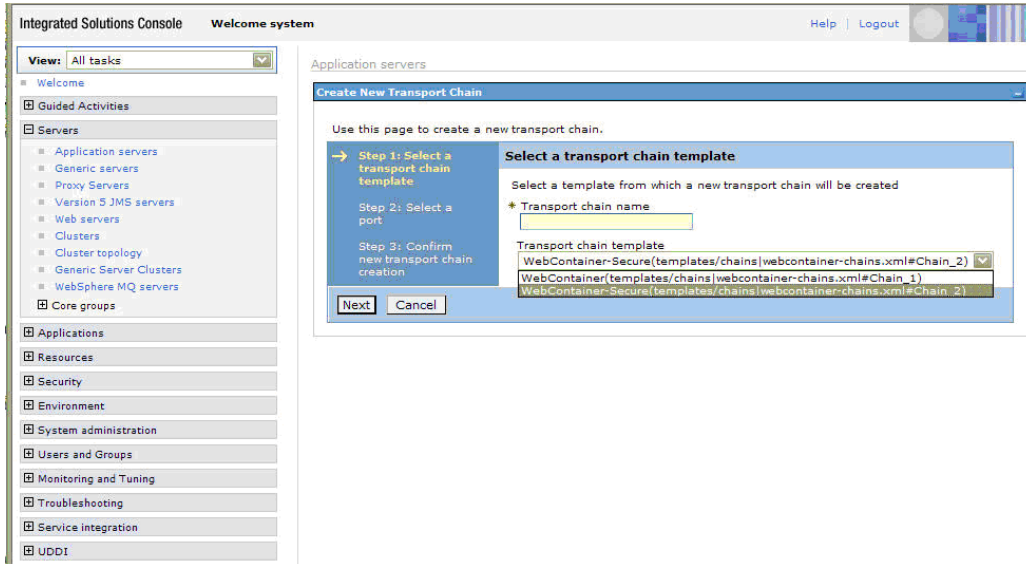
- From the **Web Container Transport Chains** page, click **New**.
The **Create New Transport Chain** page opens.

Figure 100 Create New Transport Chain



- In the **Transport Chain Name** field, enter the transport name. For example: WCInboundSIChain.
- Select the secure chain template from the **Transport Chain Template** list.

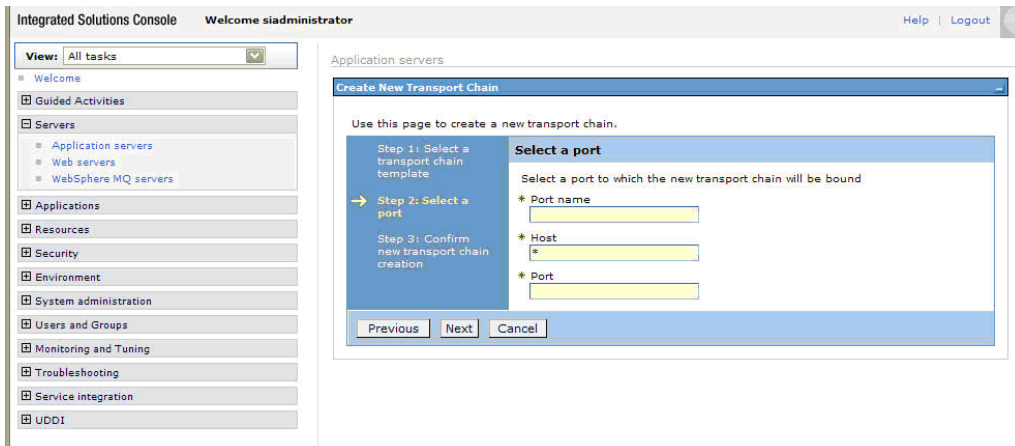
Figure 101 Create New Transport Chain



8 Click **Next**.

The **Create New Transport Chain - Select a Port** page opens. Use this page to identify the port for the new transport chain.

Figure 102 Create New Transport Chain



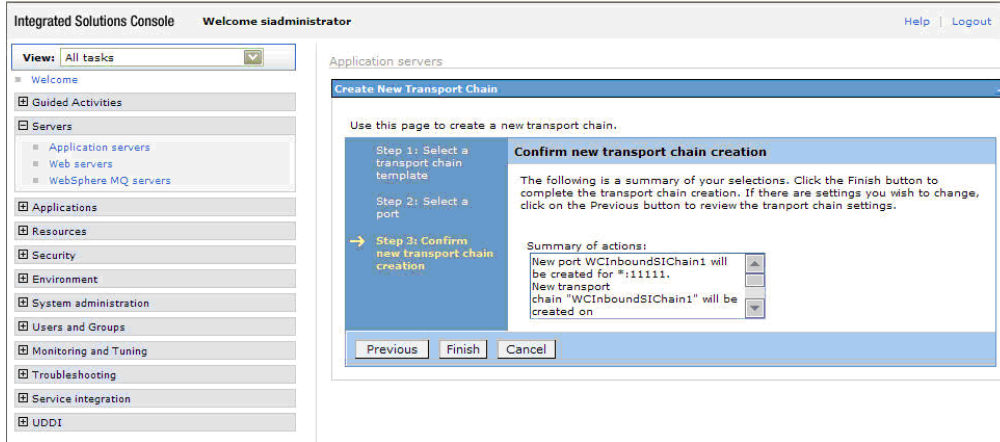
9 In the **Port Name** field, enter the name of the port you created on the previous page.

10 In the **Port** field, enter the port number that you defined in [Set Up the Environment](#) on page 97.

11 Click **Next**.

The **Confirm New Transport Chain Creation** page opens.

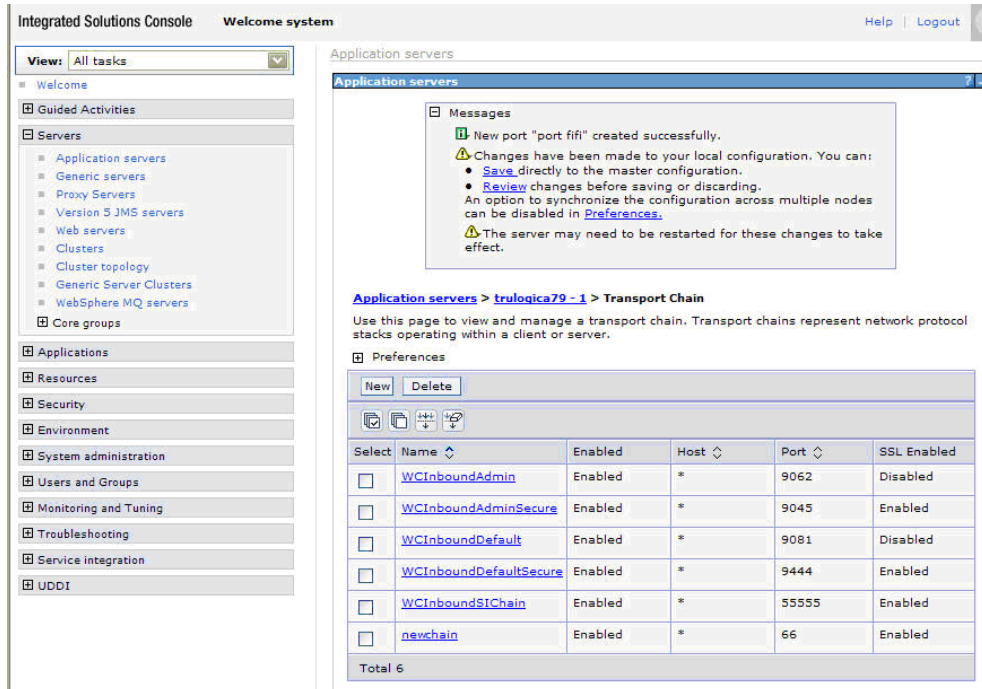
Figure 103 Create New Transport Chain



12 Verify you have entered the correct information and click **Finish**.

13 The **Transport Chain** page reopens with the new transport chain displayed in the list.

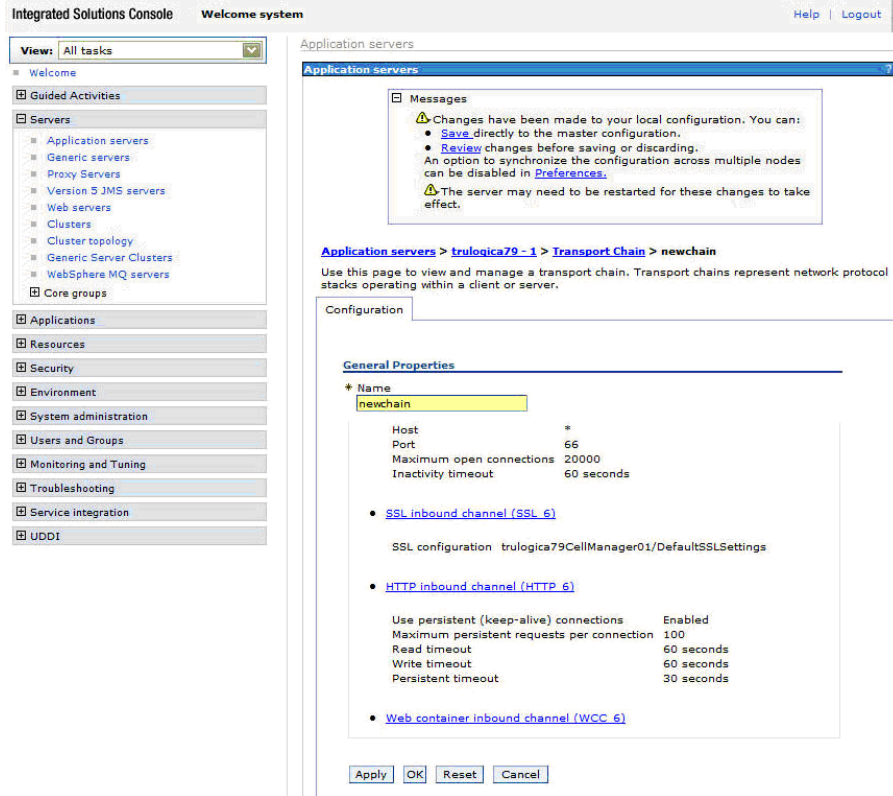
Figure 104 Transport Chain



14 Select the new transport chain you just created.

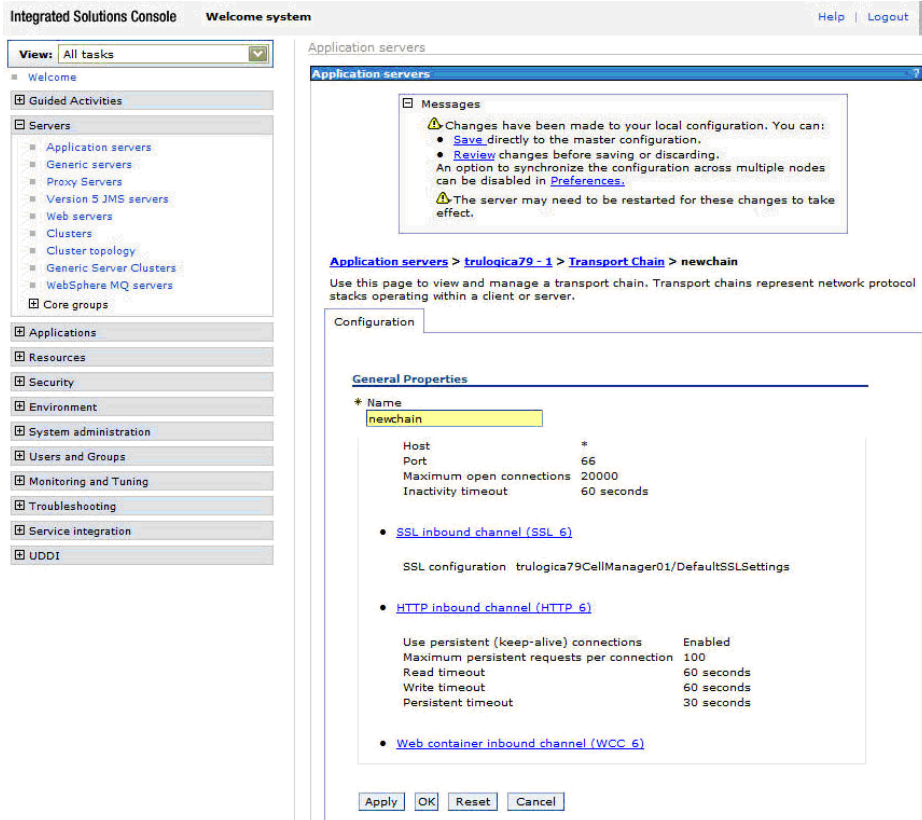
The **General Properties** page for the new transport chain opens.

Figure 105 Create New Transport Chain - General Properties



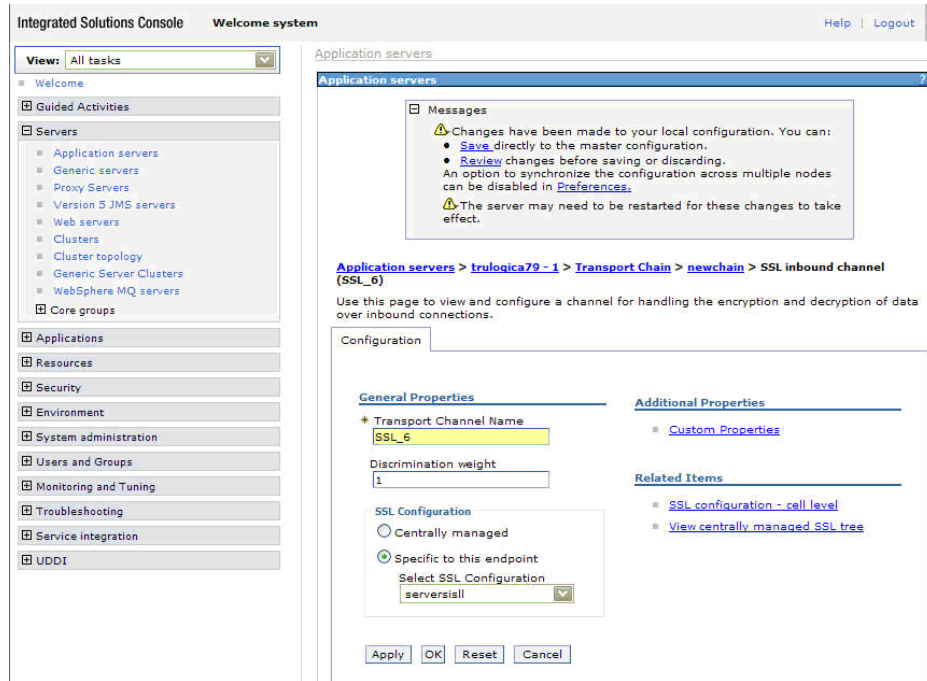
15 Under **General Properties**, select **SSL Inbound Channel**.

Figure 106 SSL Inbound Channel Configuration Parameters



The **SSL Inbound Channel Configuration Parameters** page opens.

Figure 107 SSL Inbound Channel Configuration Parameters



- 16 Under **SSL Configuration**, select **Specific to this endpoint**.
- 17 From the **Select SSL Configuration** list, select the name of the SSL configuration you created earlier in **Set Up Security** on page 91.
- 18 Click **OK**.
- 19 Save your changes to the master configuration by clicking **Save** in the **Messages** box at the top of the page.
- 20 Restart the server.
- 21 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. Refer to the *HP Select Identity Administration Online Help*.

Logging In to Select Identity

To log in to Select Identity, 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 **sis**. The password is **abc123**. We recommend that you change this as soon as possible.

5 Installing Select Identity on BEA WebLogic 9.2

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

This chapter contains the following sections:

- [Introduction](#)
- [Single-server or Cluster Installation](#)
- [Checking Your Installation Environment](#)
- [Prerequisite Configuration](#)
- [Pre-Installation Tasks for Installing Select Identity on WebLogic](#)
- [Select Identity Installer Process Summary](#)
- [Select Identity Manual Installation Procedure](#)
- [Post-Installation Steps](#)
- [Configuring WebLogic for Mutual Authentication](#)
- [Logging In to Select Identity](#)

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 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.

Checking Your Installation Environment

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

For standalone and cluster installations, the requirements are as follows:

- 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 Select Identity bootstrap keystore for the security framework of Select Identity, as documented in [Chapter 6, Configuring Select Identity](#).



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

For cluster installations only, additional requirements are as follows:

- The WebLogic administration server is running.
- The WebLogic Node Manager is running on every node.
- The cluster has a shared file system for storing application data (such as properties files, input/output directories for reconciliation, and user import jobs).

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 you will need the following information:

- 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 administration 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 (e.g. 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 Keystores, Truststores, and Security Framework](#) on page 160.
- 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, you will need the following additional information:

- The directory location on the network file system (UNIX) 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

Earlier 32-bit versions of WebLogic automatically installed two JDK selections for you to choose from. The 64-bit versions of WebLogic do not come with Java installed. So you will need to download and install JRockit from BEA's Web site. It is *very* important that you install the correct version. Here is the only version of JRockit that will work with WebLogic 9.2:


JRockit 5.0 R26.4 CR302700 (for use with WLS 9.2 MP1)

It is critical that you configure the WebLogic server correctly before you begin the installation process. Perform this procedure before you begin to install Select Identity using either the installer or the manual installation process.

To configure WebLogic server prior to installing Select Identity, perform the following steps:

- 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 WebLogic administration server.

 Directory locations may differ on your system.

- a For UNIX, change directories to:


```
<BEA_Home>/<Java_Home_Directory>/jre/lib/security
```

For Windows, change directories to:

```
<BEA_Home>\<Java_Home_Directory>\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 WebLogic server are correct, skip to [Pre-Installation Tasks for Installing Select Identity on WebLogic](#). Otherwise, proceed to [step 3](#).
- 3 Open a Web browser on WebLogic server and go to the following URL:
http://java.sun.com/javase/downloads/index_jdk5.jsp
- 4 On the Java Downloads Web page, locate the download link for the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0**. 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.

Pre-Installation Tasks for Installing Select Identity on WebLogic

The following sections describe some pre-installation steps that *must* be performed using the WebLogic console prior to installing Select Identity on WebLogic. The Select Identity application will fail to deploy if you do not perform these pre-installation tasks. The main pre-installation tasks include:

- [Enable the Combined Role Mapping](#)
- [Create the SIAdministrators Group](#)
- [Create the siadministrator User](#)
- [Create the SIAdministrator Security Role in the Domain](#)

Enable the Combined Role Mapping

To enable the combined role mapping, perform the following steps:

- 1 Log on to the WebLogic console.
- 2 Click **Lock & Edit** in the **Change Center** panel.
- 3 From the left panel, select **Security Realms**.
- 4 In the table, select **myrealm**.
- 5 On the **Configuration** tab, be sure the **Combined Role Mapping Enabled** checkbox is selected.

Figure 108 Enable Combined Role Mapping



- 6 Click **Save**.
- 7 Click **Activate Changes** in the **Change Center** panel.

Create the SIAdministrators Group

To create the SIAdministrators group, perform the following steps:

- 1 In the WebLogic console, select **Security Realms**.
- 2 In the table, select **myrealm**.
- 3 On the **Users and Groups** tab, select the **Groups** sub-tab.
- 4 Click **New**.

Figure 109 Create the SIAdministrators Group

Create a New Group

OK Cancel

Group Properties
The following properties will be used to identify your new Group.

What would you like to name your new Group?

Name: SIAdministrators

How would you like to describe the new Group?

Description: SIAdministrators

Please choose a provider for the group.

Provider: DefaultAuthenticator

OK Cancel

- 5 In the **Name** field, enter SIAdministrators (typed exactly as shown here).
- 6 In the **Description** field, enter SIAdministrators (typed exactly as shown here).
- 7 From the **Provider** drop-down list, select the **DefaultAuthenticator** option.
- 8 Click **OK**.

Create the siadministrator User

To create the siadministrator user, perform the following steps:

- 1 In the WebLogic console, select **Security Realms**.
- 2 In the table, select **MyRealm**.
- 3 On the **Users and Groups** tab, select the **Users** sub-tab.
- 4 Click **New**.

Figure 110 Create the siadministrator User

Create a New User

OK Cancel

User Properties
The following properties will be used to identify your new User.

What would you like to name your new User?

Name:

How would you like to describe the new User?

Description:

Please choose a provider for the user.

Provider:

The password is associated with the login name for the new User.

Password:

Confirm Password:

OK Cancel

- 5 In the **Name** field, enter `siadministrator` (typed exactly as shown here).
- 6 In the **Description** field, enter `siadministrator` (typed exactly as shown here).
- 7 From the **Provider** drop-down list, select the **DefaultAuthenticator** option.
- 8 In the **Password** field, enter a password for the user.
- 9 In the **Confirm Password** field, re-enter the password.
- 10 Click **OK**.
- 11 Click **Activate Changes**.

Create the SIAdministrator Security Role in the Domain

To create the SIAdministrator security role in the domain, perform the following steps:

- 1 In the WebLogic console, select **Security Realms**.
- 2 In the table, select **myrealm**.
- 3 Select the **Roles and Policies** tab.
- 4 Select the **Realm Roles** sub-tab.
- 5 In the table, expand **Domain** →<Your WebLogic Server>.
- 6 Click on **Roles** (do not expand).
- 7 Click **New**.

Figure 111 Create the SIAdministrator Security Role in the Domain

Create a New Domain Scoped Role

OK Cancel

Role Properties
The following properties will be used to identify your new role.

What would you like to name your new role?

Name: SIAdministrator

Which role mapper would you like to use with this role?

Provider Name: XACMLRoleMapper

OK Cancel

- 8 In the **Name** field, enter `SIAdministrator` (typed exactly as shown here).
- 9 From the **Provider** drop-down list, select `XACMLRoleMapper`.
- 10 Click **OK**.
- 11 In the **Domain Scoped Roles** table, which immediately displays, select `SIAdministrator` (typed exactly as shown here).
- 12 Click **Add Conditions**.
- 13 From the **Predicate List**, select `Group`.
- 14 Click **Next**.
- 15 In the **Group Argument Name** field, enter `SIAdministrators` (typed exactly as shown here), and click **Add**.
- 16 Click **Finish**.
- 17 Click **Save**.

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](#) on page 109.

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:

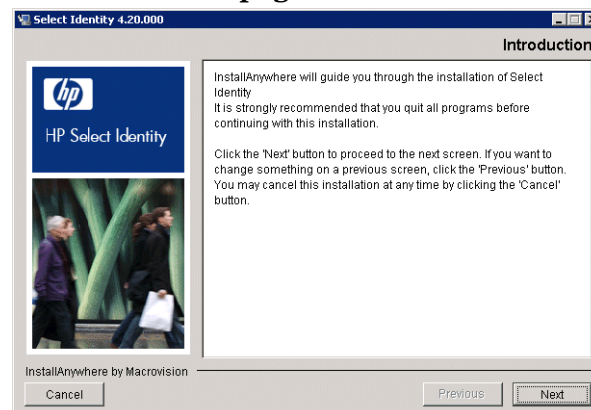
- Validate all preconditions; for example, it does not verify installation of the Select Identity schema.
- Install WebLogic domain, servers, and clusters; WebLogic must be installed before you begin installing Select Identity.
- Verify the existence of <Java_Home_Directory>, <WebLogic_Home>, or application domain directories. You must have the <Java_Home_Directory> and <WebLogic_Home> 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:

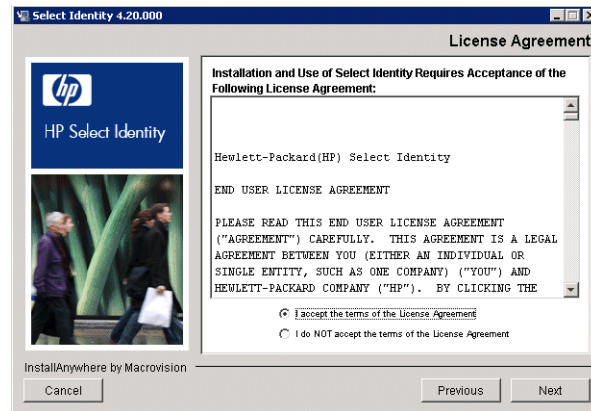
- 1 Perform the installation at the machine where the WebLogic administration server is running.
- 2 Log on to the server with the user account that was used to install WebLogic.
If you log on with a different user ID, you will not have the permissions or access needed to install and run Select Identity.
- 3 Mount the Select Identity product CD.
- 4 Copy the following files into a convenient location on the Admin server from the Select Identity product CD:
UNIX: `installer.bin` and `installer.properties`
Windows: `installer.exe` and `installer.properties`
- 5 Run the executable named `install.bin` (UNIX) or `install.exe` (Windows) to open the Select Identity Installer.

Figure 112 The Introduction page



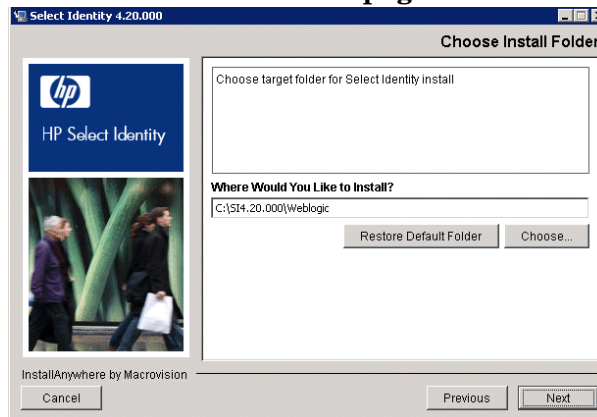
- 6 Click **Next** to proceed to the **License Agreement** page.

Figure 113 The License Agreement page




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

Figure 114 The Choose Install Folder page



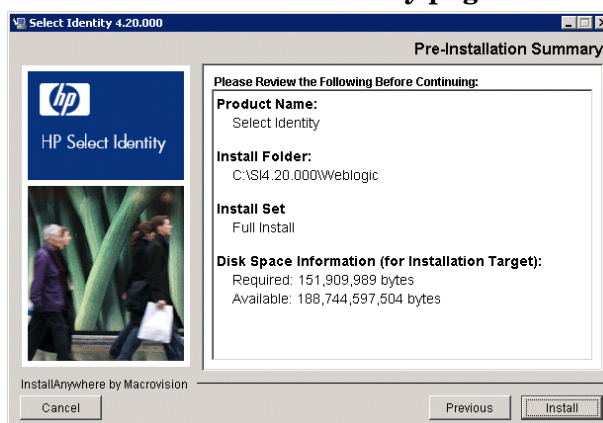
- 8 This page includes a field labeled **Where Would You Like to Install**, which is populated with a default installation path appropriate to your operating system.

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.

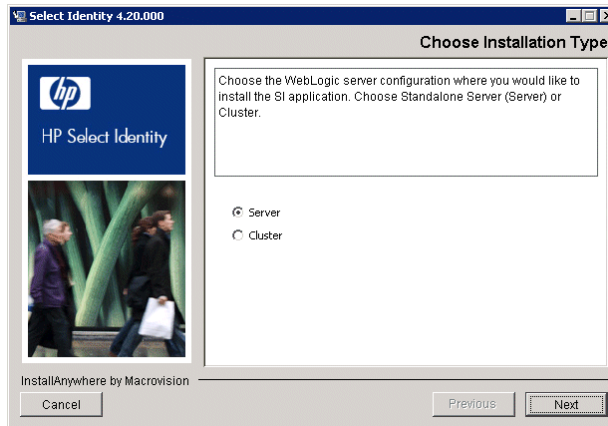
- 9 Click **Next** to proceed to the **Pre-Installation Summary** page.

Figure 115 The Pre-Installation Summary page



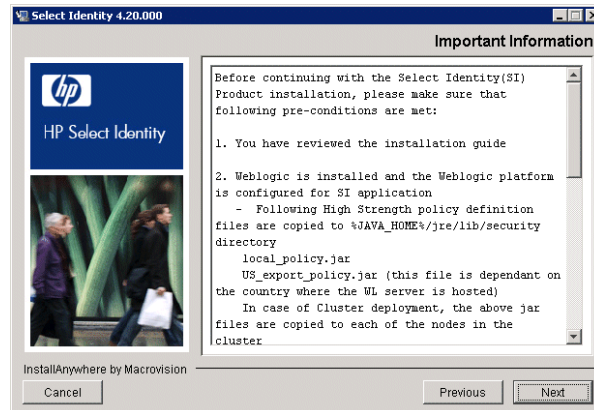
- 10 Verify the information on the **Pre-Installation Summary** page and ensure that you have completed all required steps.
- 11 Click **Install**. The installer displays a progress bar while it installs Select Identity and associated files into the chosen folder, then opens the **Choose Installation Type** page.

Figure 116 The Choose Installation Type page



- 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 117 The Important Information page



- 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 118 The Set Cluster Information page (cluster only)

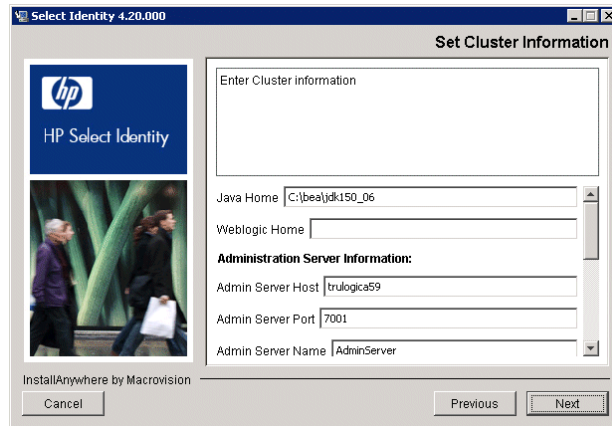
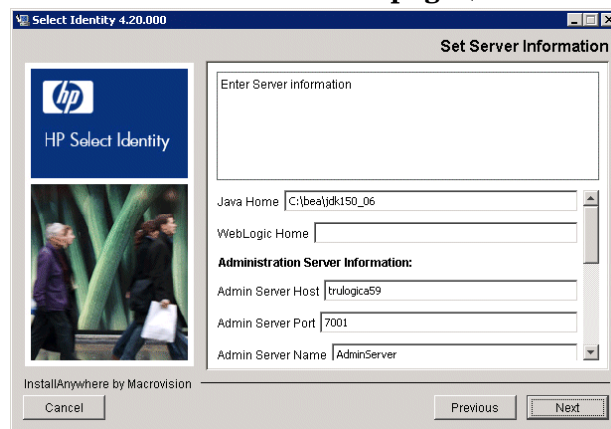


Figure 119 The Set Server Information page (server only)

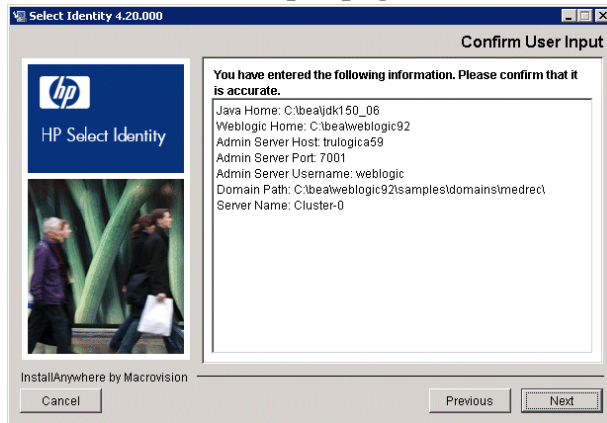


- 16 This page contains multiple settings that must be correct. Use the scroll bar to view the whole page. Complete each setting with the appropriate information, as follows:
- **Java Home** — The home directory where the JDK is installed.
 - **WebLogic Home** — The home directory where WebLogic is installed (for example, c:\bea\weblogic92).
 - **Admin Server Host** — The hostname of the WebLogic administration server.
 - **Admin Server Port** — The port used by Select Identity.
 - **Admin Server Name** — The name of the WebLogic administration server, as it appears in the WebLogic console.
 - **Admin Server Username** — The WebLogic administrator user name.
 - **Admin Server Password and Confirm Password** — The password for the WebLogic administrator user.
 - **Domain Path** — The directory location of the WebLogic application domain where Select Identity is being installed.
 - **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 admin server on which you are installing Select Identity, if you are installing on a single server.

- 17 Click **Next**.

18 Review the information you provided, on the **Confirm User Input** page.

Figure 120 The Confirm User Input page

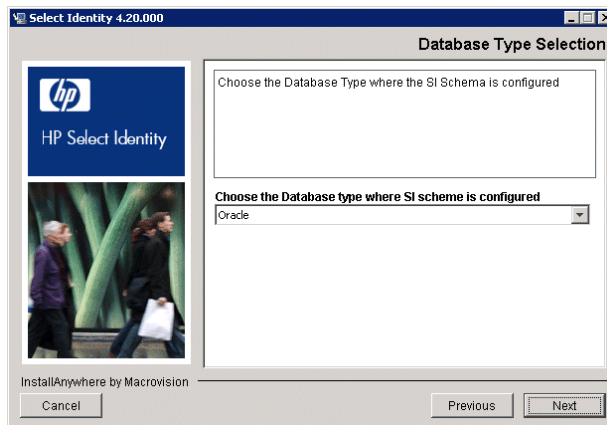


19 If the information is correct, click **Next**.

20 After checking the WebLogic administration server, the installer opens the **Database Type Selection** page.

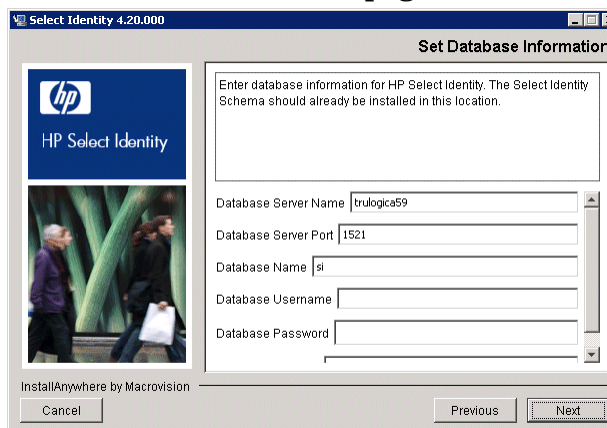
21 Use the list box to select the database type. This should be the same as the database in which you or your database administrator configured the Select Identity database, as documented in [Chapter 3, Database Server Configuration](#).

Figure 121 The Database Type Selection page



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

Figure 122 Set Database Information page



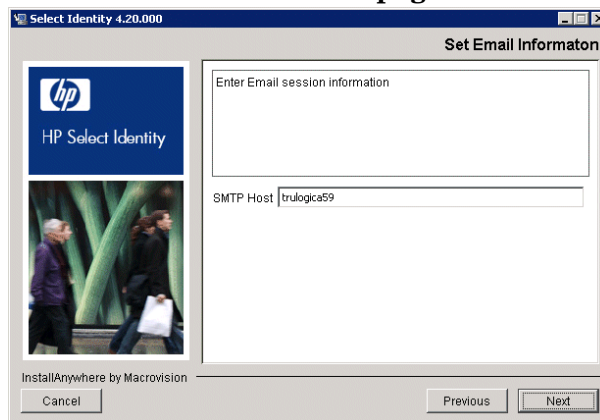
- 23 Specify the settings for the Select Identity database.

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

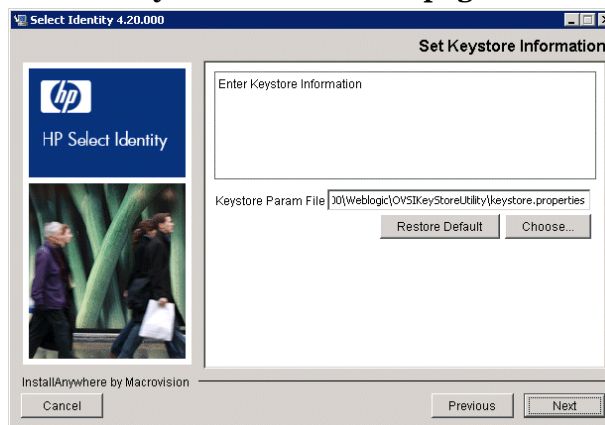
Figure 123 The Set Email Information page



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

- 26 Click **Next** to proceed to the **Set Keystore Information** page.

Figure 124 The Set Keystore Information page

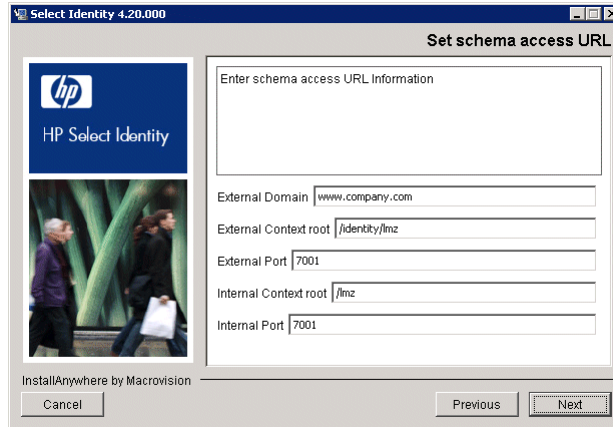


- 27 Enter the path to the `keystore.properties` file. See [Setting Up Keystores, Truststores, and Security Framework](#) on page 160.

▶ For a cluster, the `keystore.properties` file and keystore path must be on a mapped drive/network file system.

- 28 Click **Next** to proceed to the **Set schema access URL** page.

Figure 125 The Set schema access URL page



- 29 Complete the fields with the appropriate information about the schema access URL:
- **External Domain** — The external (outside of the firewall) domain for the schema access URL.
 - **External Context Root** — The external context root for the schema access URL.
 - **External Port** — The external port number for the schema access URL.
 - **Internal Context Root** — The internal (inside of the firewall) context root for the schema access URL.
 - **Internal Port** — The internal port number for the schema access URL.
- 30 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 32](#) on page 121.
 - On a *cluster* installation:
Click **Next** to proceed to the **Set Cluster Remote Start Information** page, and follow this procedure from [step 31](#) on page 120.
- 31 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** — The home directory where WebLogic is installed.
 - **Java Home** — The home directory where the JDK is installed.
 - **Root Directory** — The 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:
 - `bcprov-jdk15-135.jar`
 - `commons-logging-1.1.jar`

- connector.jar
- ovsi18n.jar
- tools.jar
- weblogic.jar

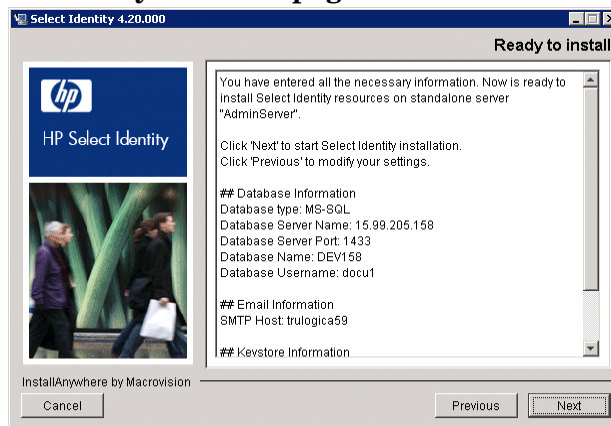
The installer autopopulates paths to the files listed above, based on your previous settings. These must be correctly set. If you set them manually on any of the managed servers, the files are located in one of the following directory locations:

- The lib directory in <Java_Home_Directory> (for tools.jar)
- The sysArchive directory in the <SI_Install_Dir> (for commons-logging-1.1.jar)
- The sysArchive directory in the <SI_Install_Dir> (for connector.jar and ovsi18n.jar)
- The lib directory under the server directory in <WebLogic_Home> (for weblogic.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 126 The Ready to Install page



- 32 Click **Next** when you have reviewed the information on the **Ready to Install** page.
- 33 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:

- 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 `<SI_Install_DIR>/scripts/weblogic/myStartWL`.

- 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.

- 34 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](#).

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 in addition to the procedures outlined in this section to install Select Identity manually:

- Check to make sure your system meets the specifications in [Checking Your Installation Environment](#) on page 108.
- Complete all of the [Prerequisite Configuration](#) on page 109 (this includes setting up the security framework, as documented in [Setting Up Keystores, Truststores, and Security Framework](#) on page 160).



The left panel 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

Before you begin installing Select Identity, create the directories and copy the files listed in this section.

- 1 Create the Select Identity home directory, referred to as `<SI_Install_Dir>` in this chapter, 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 <SI_Install_Dir> directory:

- <SI_Install_Dir>/deploy
- <SI_Install_Dir>/sysArchive
- <SI_Install_Dir>/lib
- <SI_Install_Dir>/temp
- <SI_Install_Dir>/recon/reconroot
- <SI_Install_Dir>/recon/reconstaging
- <SI_Install_Dir>/recon/reconbackup
- <SI_Install_Dir>/reports
- <SI_Install_Dir>/userimport/adroot
- <SI_Install_Dir>/userimport/adbackup
- <SI_Install_Dir>/userimport/adstaging
- <SI_Install_Dir>/jmsstore<Server1>
- <SI_Install_Dir>/jmsfilestore
- <SI_Install_Dir>/jmspagingstore
- <SI_Install_Dir>/scripts/lib
- <SI_Install_Dir>/scripts/weblogic
- <SI_Install_Dir>/keystoreutility
- <SI_Install_Dir>/email
- <SI_Install_Dir>/schema

— 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:

<SI_Install_Dir>/scripts

4 Copy the application/lmz.ear and application/ovsil10n_help_en_US.war file from the Select Identity product CD to the <SI_Install_Dir>/deploy directory.

For cluster installations, since a network directory is used for Select Identity installation, there is no need to copy files over to each cluster node.

5 Copy these files into the <SI_Install_Dir>/sysArchive directory:

- bcprov-jdk15-135.jar
- commons-logging-1.1.jar
- properties/TruAccess.properties
- lib/ovsil18n.jar
- connector/connector.jar
- ovsd-web-api.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 10g:

```
truaccess.repository.type=<oracle10>
truaccess.repository.oracle.driver.bea=yes
hpsi.schema.accessurl.internal=http://localhost:7001/lmz
hpsi.schema.accessurl.external=http://www.company.com:7001/lmz
```

- For Microsoft SQL Server:

```
truaccess.repository.type=mssql
truaccess.repository.mssql.driver.bea=yes
```



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 settings are valid in the `TruAccess.properties` file.



See [TruAccess Properties](#) on page 235 for more details.

- 8 Copy the `logging.properties` file from the default location in the WebLogic Server `<Java_Home_Directory>/jre/lib` into the `sysArchive` directory.

- For clusters: Copy the `logging.properties` file to a location that is accessible by 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>/jrockit90_150_06/jre/lib` directory for UNIX 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 `<SI_Install_Dir>` directory, such as `sysArchive`.

- 9 Copy the product documentation from the `docs` directory on the 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:

Windows

`cpappend.bat` and `myStartWL.cmd`

UNIX

`myStartWL.sh`

Open and edit the default WebLogic Startup script file and save it, as described in this section.

The following is an example of what should be added to the `cpappend.bat` file:

```
set CLASSPATH=%CLASSPATH%;%1
```

The following is an example of what should be added to the `myStartWL` file:

- Setting the memory
- Location of TruAccess.properties
- Location of logging.properties
- Headless=true setting.
- Adding the connector.jar and ovsii18n.jar to the classpath

Windows example:

```
set CLASSPATH=.
set JAVA_VM=-server
set USER_MEM_ARGS=-Xms256m -Xmx1024m -XX:MaxPermSize=256m
set JAVA_OPTIONS=-Dcom.trulogica.truaccess.property.file="<SI_Install_Dir>\sysArchive\TruAccess.properties" -Dweblogic.management.anonymousAdminLookupEnabled=true
for %%i in ("<SI_Install_Dir>\sysArchive\*.jar") do call ".\cpappend.bat" %%i
for %%i in ("<SI_Install_Dir>\lib\*.jar") do call ".\cpappend.bat" %%i
rem for %%i in ("<SI_Install_Dir>\OVSIKeyStoreUtility\*.jar") do call ".\cpappend.bat" %%i
set EXT_PRE_CLASSPATH=%CLASSPATH%

set PATH=#DOMAIN_DIR#
cd /D "#DOMAIN_DIR#"
call startweblogic.cmd
```

UNIX example:

```
#!/bin/sh
export JAVA_VM=-server
export USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:MaxPermSize=256m"
export JAVA_OPTIONS="-Dcom.trulogica.truaccess.property.file=<SI_Install_Dir>/sysArchive/TruAccess.properties -Djava.awt.headless=true -Dweblogic.management.anonymousAdminLookupEnabled=true"

DIRLIBS=<SI_Install_Dir>/sysArchive/*.jar
for i in ${DIRLIBS}
do
    if [ -z "$CLASSPATH" ] ; then
        CLASSPATH=$i
    else
        CLASSPATH="$i":$CLASSPATH
    fi
done

DIRLIBS=<SI_Install_Dir>/lib/*.jar
for i in ${DIRLIBS}
do
    if [ -z "$CLASSPATH" ] ; then
        CLASSPATH=$i
    else
        CLASSPATH="$i":$CLASSPATH
    fi
done

export EXT_PRE_CLASSPATH=$CLASSPATH
cd <User_Domain_Dir>
sh <User_Domain_Dir>/startWebLogic.sh
```

-Djava.util.logging.config.file=<SI_Install_Dir>/sysArchive/logging.properties

Starting WebLogic

To start WebLogic, following these steps:

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

Windows:

<SI_Install_Dir>\scripts\myStartWL.cmd

UNIX:

<SI_Install_Dir>/scripts/myStartWL.sh

For *clustered* server installations, start the WebLogic administration server by executing the appropriate script from the WebLogic administration server's command line.

Windows:

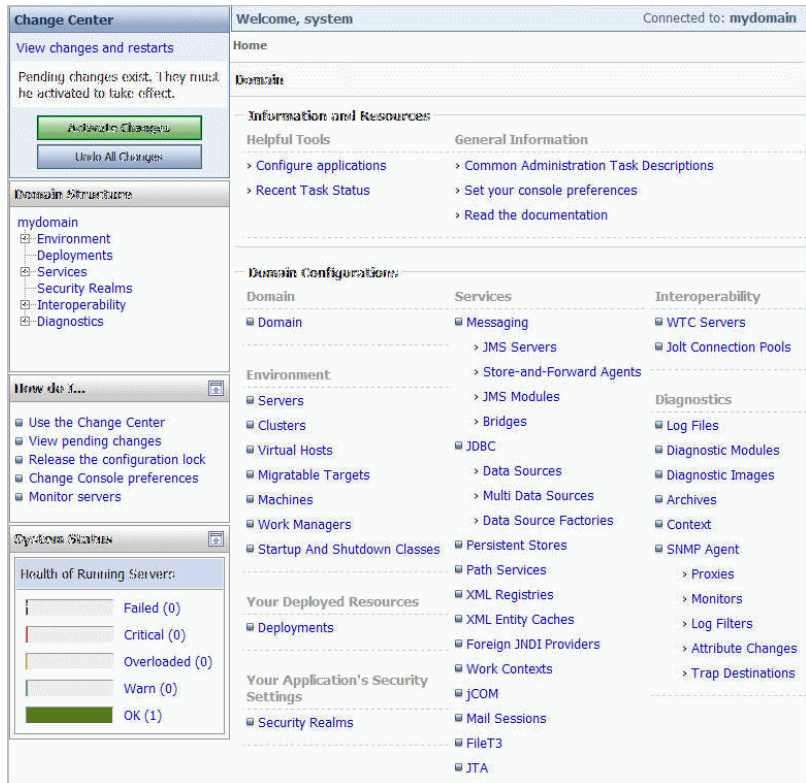
<WebLogic_Home>\user_projects\domains\<Domain_name>\startWebLogic.cmd

UNIX:

<WebLogic_Home>/user_projects/domains/<Domain_name>/startWebLogic.sh

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

Figure 127 WebLogic Server Console Home Page

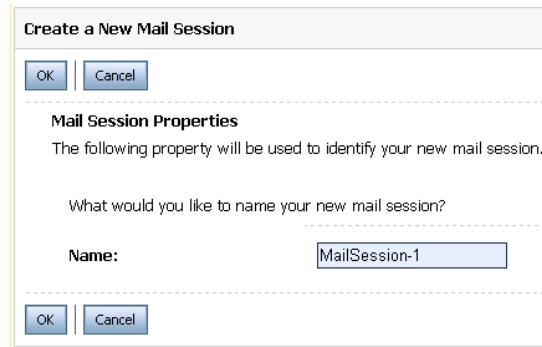


Configuring the Mail Session

To configure the mail session for Select Identity, follow these steps:

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 On the **Domain Structure** panel, beginning at the domain you created during the WebLogic installation, navigate to **<My Domain> → Services → Mail Sessions**.
- 3 On the **Summary of Mail Sessions** page, click **New** in the **Mail Sessions** table.
- 4 On the **Create a New Mail Session** page, type the name of your new mail session in the **Name** box and click **OK**. The following message will display at the top of your page, “*Mail session created successfully.*”

Figure 128 Create a New Mail Session



- 5 In the **Mail Sessions** table, click the name of the mail session you just created in the previous step.
- 6 On the Settings for **<your_mailsession>** page, enter `mail/TruAccess` in the **JNDIName** box.
- 7 In the **JavaMail Properties** box, enter the IP address of the mail server:
`mail.smtp.host=192.168.1.52`
- 8 Click **Save**. A confirmation message displays at the top of the page, “*Settings updated successfully.*”
- 9 On the **Targets** tab, select **<Your Admin Server>** in the **Servers** table. For clusters, select all the servers in the cluster.
- 10 Click **Save**.
- 11 On the **Change Center** panel, click **Activate Changes**.

A confirmation message displays at the top of the page, “*All changes have been activated. No restarts are necessary.*”



Even though you have been clicking the **Save** button along the way, your changes will not take effect until you click **Activate Changes**.

Each time you click **Activate Changes**, this confirmation message will display, “*All changes have been activated. No restarts are necessary.*”

Throughout this manual installation process, you can click **Activate Changes** → **Lock & Edit** as often as you like.

Configuring JMS Settings for a Single Server and Cluster Servers

The following procedures are required to configure the JMS settings for a single server and cluster servers:

- [Creating the JMS System Module](#)
- [Creating JMS Connection Factories: Queue and Topic](#)
- [Configuring the JMS File Store](#)
- [Creating the JMS Server](#)
- [Configuring the Paging Store](#)
- [Creating JMS System Resources: Destination Key, Topics, and Queues](#)

Creating the JMS System Module

The first procedure in configuring the JMS settings for both, single server and cluster servers is to create the JMS system module. Follow these steps to create the JMS module:

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 Continuing on the **Settings for <Your Admin Server>** page, click **New** in the **Summary of Resources** table.
- 3 On the **JMS Modules** page, click **New** in the **JMS Modules** table.
- 4 On the **Create JMS System Module** page, enter a name for the JMS system module that you are creating in the **Name** box.

Figure 129 Create JMS System Module

Create JMS System Module

Back Next Finish Cancel

The following properties will be used to identify your new module.
JMS system resources are configured and stored as modules similar to standard J2EE modules. Such resources include queues, topics, connection factories, templates, destination keys, quota, distributed queues, distributed topics, foreign servers, and JMS store-and-forward (SAF) parameters. You can administratively configure and manage JMS system modules as global system resources.

What would you like to name your System Module?

Name: SystemModule-0

What would you like to name the descriptor file name? If you do not provide a name, a default will be assigned.

Descriptor File Name:

Where would like to place the descriptor for this System Module, relative to the Jms configuration sub-directory of your domain?

Location In Domain:

Back Next Finish Cancel

- 5 Enter a name for the descriptor file in the **Descriptor File Name** box, or you can leave this box blank to accept a default name.
- 6 In the **Location in Domain** box, enter the location where you want to store the descriptor file and click **Next**.
- 7 From the **Targets** table, select **<Your Admin Server>** in the **Servers** table. For clusters, select all the servers in the cluster.
- 8 Click **Next**.
- 9 Select the properties to which you will target your new JMS system module. For example, select **<Your Admin Server>** for a stand-alone installation.

- 10 To add resources now, check **Would you like to add resources to this JMS system module?** and click **Finish**.

A confirmation message displays, “*The JMS module was created successfully.*”

- 11 On the **Change Center** panel, click **Activate Changes**.

Creating JMS Connection Factories: Queue and Topic

Select Identity requires two JMS connection factories: queue and topic. Now that you have created the JMS system module, you will need to create the connection factories.

Creating Queue Connection Factories

Follow these steps to create a Select Identity *queue* connection factory:

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 From the left panel, expand **Services** and select **JMS Modules** → **JMS Modules**.
- 3 Continuing on the **Settings for <Your Admin Server>** page, click **New** in the **Summary of Resources** table.
- 4 On the **Create a New JMS System Module Resource** page, select **Connection Factory** and click **Next**.

Figure 130 Create JMS System Module Resource

Create a New JMS System Module Resource

Back Next Finish Cancel

Connection Factory Properties
The following properties will be used to identify your new connection factory. The current module is SystemModule-0.

What would you like to name your new connection factory?

Name:

What JNDI Name would you like to use to look up your new connection factory?

JNDI Name:

Back Next Finish Cancel

- 5 In the **Name** field, enter `jms.OVSIQCF` as the filename of your new queue connection factory.
- 6 In the **JNDI Name** field, enter `jms/OVSIQCF` as the required *JNDI* name of your new queue connection factory and click **Next**.
- 7 In the **Targets** table, **<Your Admin Server>** is the default (and the only available) target for single servers. For clusters, select all the servers in the cluster.
- 8 Click **Finish**.
- 9 Notice how the **Summary of Resources** table is now populated with the new information. A confirmation message displays, “*Connection factory created successfully.*”
- 10 On the **Change Center** panel, click **Activate Changes** and then click **Lock & Edit**.
- 11 In the **Summary of Resources** table, click on the *queue* connection factory filename that you just created in [step 5](#) on page 129.
- 12 On the **Settings for <Your Connection Factory>** page, navigate to the **Configuration** → **Default Delivery** tab.

Figure 131 Settings for <Your Connection Factory> - Default Delivery Tab

Settings for jms.OVSIQCF

Configuration Subdeployment Notes

General **Default Delivery** Client Transactions Flow Control Load Balance Security

Save

Use this page to define the default delivery configuration parameters for this JMS connection factory, such as the default delivery mode, default time to live, etc.

Default Priority: 4 The default priority used for messages when a priority is not explicitly defined. [More Info...](#)

Default Time-to-Live: 0 The maximum length of time, in milliseconds, that a message will exist. This value is used for messages when a priority is not explicitly defined. A value of 0 indicates that the message has an infinite amount time to live. [More Info...](#)

Default Time-to-Deliver: 0 The delay time, in milliseconds, between when a message is produced and when it is made visible on its destination. [More Info...](#)

Default Delivery Mode: Persistent The default delivery mode used for messages when a delivery mode is not explicitly defined. [More Info...](#)

Default Compression Threshold: 2147483647 The number of bytes for the serialized message body so any message exceeds this limit will trigger message compression when the message is sent or received by the JMS message producer or consumer. [More Info...](#)

Send Timeout: 10 The maximum length of time, in milliseconds, that a sender will wait when there isn't enough available space (no quota) on a destination to accommodate the message being sent. [More Info...](#)

Default Unit-of-Order for Producer: None The default Unit-of-Order name for producers that connect using this connection factory. A Unit-of-Order allows for messages to be processed in a certain order, even among multiple recipients. [More Info...](#)

13 Select **Persistent** from the **Default Delivery Mode** drop-down box and click **Save**.

Figure 132 Settings for <Your Connection Factory> - Client Tab

Settings for jms.OVSIQCF

Configuration Subdeployment Notes

General Default Delivery **Client** Transactions Flow Control Load Balance Security

Save

Use this page to define the client configuration parameters for this JMS connection factory, such as client id for durable subscribers, acknowledge policy, etc.

Client ID for Durable Subscribers: An optional client ID for a durable subscriber that uses this JMS connection factory. Configuring this value on the connection factory prevents more than one JMS client from using a connection from the factory. [More Info...](#)

Allow Close() Within onMessage() Specifies whether the connection factory creates message consumers that allow a close() method to be issued within its onMessage() method call. [More Info...](#)

Client Acknowledge Policy: All Acknowledge policy for non-transacted sessions that use the CLIENT_ACKNOWLEDGE mode. All indicates that calling acknowledge on a message acknowledges all unacknowledged messages received on the session. Previous specifies that calling acknowledge on a message acknowledges only unacknowledged messages up to, and including, the given message. [More Info...](#)

Maximum Messages per Session: 10 The maximum number of messages that can exist for an asynchronous session and that have not yet been passed to the message listener. When the Synchronous Prefetch Mode is enabled, this value also affects synchronous sessions with a message consumer that will prefetch messages in one server access. [More Info...](#)

Prefetch Mode for Synchronous Consumer: Disabled Specifies whether a synchronous consumer will prefetch messages (that is, messages sent from the server to the client) in one server access. [More Info...](#)

Multicast Overrun Policy: Keep Old The policy to use when the number of outstanding multicast messages reaches the value specified in MessagesMaximum and some messages must be discarded. [More Info...](#)

14 On the **Transactions** tab, check **XA Connection Factory Enabled** and click **Save**.

Figure 133 Settings for <Your Connection Factory> - Transaction Tab

Settings for jms.OVSIQCF

Configuration Subdeployment Notes

General Default Delivery Client **Transactions** Flow Control Load Balance Security

Save

Use this page to define the transaction configuration for this JMS connection factory. You can define a transaction time-out value, and also indicate whether an XA queue or XA topic connection factory is returned, which create sessions that are JTA user-transaction aware.

Transaction Timeout: 3600 The timeout value (in seconds) for all transactions on connections created with this connection factory. [More Info...](#)

XA Connection Factory Enabled Indicates whether a XA queue or XA topic connection factory is returned, instead of a queue or topic connection factory. An XA connection factory can be used to create an XAConnection, which in turn may be used to create an XASession, which in turn may be used to obtain an XAResource for use inside a transaction manager. [More Info...](#)

Save

- On the **Load Balance** tab, check **Server Affinity Enabled** for single servers to indicate “true”. For clusters, uncheck this box to indicate “false”.

Figure 134 Settings for <Your Connection Factory> - Load Balance Tab

Settings for jms.OVSITCF

Configuration | Subdeployment | Notes

General | Default Delivery | Client | Transactions | Flow Control | **Load Balance** | Security

Save

Use this page to define the load balancing configuration parameters for this JMS connection factory, which includes enabling load balancing and server affinity.

Load Balancing Enabled Specifies whether non-anonymous producers created through a connection factory are load balanced within a distributed destination on a per-call basis. [More Info...](#)

Server Affinity Enabled Specifies whether a server instance that is load balancing consumers or producers across multiple members destinations of a distributed destination, will first attempt to load balance across any other physical destinations that are also running on the same server instance. [More Info...](#)

Save

- Click **Save**.
- On the **Change Center** panel, click **Activate Changes**. A confirmation message displays, “*All changes have been activated. No restarts are necessary.*”

Creating Topic Connection Factories

Continuing from creating the Select Identity *queue* connection factory, follow these steps to create the *topic* connection factory:

- On the **Change Center** panel, click **Lock & Edit**.
- In the **JMS Modules** table, click the name of the JMS module you created [step 4](#) on page 128.
- In the **Summary of Resources** table, click **New**.
- On the **Create a New JMS System Module Resource** page, select **Connection Factory** and click **Next**.

Figure 135 Create a New JMS System Module Resource

Create a New JMS System Module Resource

Back Next Finish Cancel

Connection Factory Properties
The following properties will be used to identify your new connection factory. The current module is SystemModule-0.

What would you like to name your new connection factory?

Name:

What JNDI Name would you like to use to look up your new connection factory?

JNDI Name:

Back Next Finish Cancel

- In the **Name** field, enter `jms.OVSITCF` as the filename of your new topic connection factory.
- In the **JNDI Name** field, enter `jms/OVSITCF` as the required *JNDI* name of your new topic connection factory and click **Next**.
- In the **Targets** table, **<Your Admin Server>** is the default (and the only available) target for single servers. For clusters, select all the servers in the cluster.
- Click **Finish**.

- 9 Notice how the **Summary of Resources** table is now populated with the new information. A confirmation message displays, *“Connection factory created successfully.”*
- 10 On the **Change Center** panel, click **Activate Changes** and then click **Lock & Edit**.
- 11 In the **Summary of Resources** table, click on the *topic* connection factory filename that you just created.
- 12 On the **Settings for <Your Connection Factory>** page, navigate to the **Configuration** → **Default Delivery** tab.
- 13 Select **Non-Persistent** from the **Default Delivery Mode** drop-down box and click **Save**.
- 14 On the **Client** tab, enter **10** in the **Maximum Messages per Session** box and click **Save**.
- 15 On the **Transactions** tab, check **XA Connection Factory Enabled** and click **Save**.
- 16 On the **Load Balance** tab, check **Server Affinity Enabled** for single servers to indicate “true”. For clusters, uncheck this box to indicate “false”.
- 17 Click **Save**.
- 18 On the **Change Center** panel, click **Activate Changes**. A confirmation message displays, *“All changes have been activated. No restarts are necessary.”*

Configuring the JMS File Store

Now that you have configured both of the Select Identity connection factories, queue and topic, you must next configure the JMS file store. The JMS settings define the file store that the JMS queue writes to for each server. One file store and one paging store must be set up for each node within a cluster. Only a single instance of each is needed on a single server installation.

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

If you are installing on a cluster, repeat this procedure for each node.

Follow these steps to configure the JMS file store:


- 1 If you have not done so already, create a directory on your system that will hold the file store you are about to configure.
 -  Do not use shared directory locations for file and paging stores. For optimal performance, these file stores should be in local server directories.
- 2 On the **Change Center** panel, click **Lock & Edit**.
- 3 From the **Domain Structure** panel, navigate to **<My Domain>** → **Services** → **Persistent Stores**.
- 4 On the **Summary of Persistent Stores** page, click **New** → **Create FileStore** in the **Persistent Stores** table.

Figure 136 Create a New File Store

The screenshot shows a 'Create a New File Store' dialog box. At the top, there are navigation buttons: 'Back', 'Next', 'Finish', and 'Cancel'. Below this is the 'File Store Properties' section, which includes the instruction: 'The following properties will be used to identify your new file store.' The first question is 'What would you like to name your new file store?' with a 'Name:' label and a text box containing 'FileStore-0'. The second question is 'Select a server instance for this file store.' with a 'Target:' label and a dropdown menu showing 'examplesServer'. The third question is 'The pathname to the directory on the file system where the file store is kept. This directory must exist on your system, so be sure to create it before completing this tab.' with a 'Directory:' label and an empty text box. At the bottom, there are another set of navigation buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 5 On the **Create a New File Store** page, enter the name of your new file store in the **Name** box.
- 6 In the **Target** box, select **<Your Admin Server>** for a single server. For clusters, each specific cluster node (for example, node1, node2, node3...).
- 7 In the **Directory** box, enter the path of the directory created in [step 1](#) on page 132, that will hold the file store.
- 8 Click **Finish**.
- 9 On the **Summary of Persistent Stores** page, click your new **FileStore** name displaying in the **Persistent Stores** table.
- 10 On the **Settings for <Your File Store>** page, click **Advanced** on the **FileStore** tab.

Figure 137 Create a New File Store - Advanced Settings

The screenshot shows the 'Settings for FileStore-1' page. At the top, there are tabs for 'Configuration', 'Monitoring', and 'Notes', with 'Configuration' selected. Below the tabs is a 'Save' button. The main content area has the instruction: 'Use this page to configure a disk-based file store for storing subsystem data, such as persistent JMS messages or Store-and-Forward messages.' There are five configuration sections, each with a label, a value, and a description: 1. 'Name:' with value 'FileStore-1' and description 'The name of this file store. This name must be unique within the WebLogic Server instance or its cluster. More Info...'. 2. 'Target:' with value 'examplesServer' and description 'The list of all WebLogic Server instances that have been defined in the current domain and are therefore candidates for hosting this file store. More Info...'. 3. 'Directory:' with value 'C:\filestore' and description 'The path name to the file system directory where the file store maintains its data files. More Info...'. 4. 'Advanced' section (expanded) with 'Logical Name:' and an empty text box, and description 'The name used by subsystems to refer to different stores on different servers using the same name. More Info...'. 5. 'Synchronous Write Policy:' with value 'Direct-Write' and description 'The disk write policy that determines how the file store writes data to disk. More Info...'. At the bottom, there is another 'Save' button.

- 11 In the **Synchronous Write Policy** drop-down box, select **Cache-Flush** and click **Save**.
- 12 On the **Change Center** panel, click **Activate Changes**.

Creating the JMS Server

Each JMS server must have its own unique persistent file store and paging store corresponding to it. In this section you will create a JMS server with its corresponding persistent file store. The paging store will be configured in the next section.

If you are installing on a cluster, repeat this procedure for each node.

Follow these steps to create the JMS server:

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 From the **Domain Structure** panel, navigate to **<My Domain> → Services → Messaging → JMS Servers**.
- 3 On the **Summary of JMS Servers** page, click **New** in the **JMS Servers** table.

Figure 138 Create a New JMS Server

- 4 On the **Create a New JMS Server** page, enter a new name for the JMS server in the **Name** box.
- 5 In the **Persistent Store** drop-down box, select the file store that you created in [step 5](#) on page 133 and click **Next**.
- 6 In the **Target** drop-down box, select **<Your Admin Server>** for a single server. For clusters, create a JMS server for each server in the cluster. Select one target for each JMS server (for each server in the cluster). In other words, one JMS server should target one server.
- 7 Click **Finish**.
- 8 For clusters, repeat this procedure until all the servers are set up.
- 9 On the **Change Center** panel, click **Activate Changes**.

Configuring the Paging Store

Now that you have configured the persistent file store and created the JMS server, it is time to configure the paging store. To do this, follow these steps:

- 1 If you have not done so already, create a directory on your system that will hold the paging store you are about to configure.
 - ▶ Do not use shared directory locations for file and paging stores. These file stores should be in local server directories for optimal performance.
- 2 On the **Change Center** panel, click **Lock & Edit**.
- 3 Continuing on the **Summary of JMS Servers** page, in the **JMS Servers** table, click the JMS server name that you created in [step 4](#) on page 134.
- 4 On the **Settings for <Your JMS Server>** page, navigate to the **Configuration → General** tab.

Figure 139 Settings for JMS Server - General Tab

Settings for JMSServer-0

Configuration | Logging | Targets | Monitoring | Control | Notes

General | Thresholds and Quotas | Session Pools

Save

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them. A JMS server's primary responsibility for its destinations is to maintain information on what persistent store is used for any persistent messages that arrive on the destinations, and to maintain the states of durable subscribers created on the destinations.

Use this page to define the general configuration parameters for this JMS server.

| | | |
|--|-------------|---|
| Name: | JMServer-0 | The name of this JMS server. More Info... |
| Persistent Store: | FileStore-1 | The file or database in which this JMS server stores persistent messages. If unspecified, the JMS server uses the default persistent store that is configured on each targeted WebLogic Server instance. More Info... |
| Paging Directory: | | Specifies where message bodies are written when the size of the message bodies in the JMS server exceeds the message buffer size. More Info... |
| Message Buffer Size: | -1 | The amount of memory (in bytes) that this JMS server can use to store message bodies before it writes them to disk. When the JMS server writes the message bodies to disk, it clears them from memory. More Info... |
| <input checked="" type="checkbox"/> Hosting Temporary Destinations | | Specifies whether this JMS server can be used to host temporary destinations. More Info... |
| Module Containing Temporary Template: | (none) | The name of a JMS module that contains a template that this JMS server can use to create temporary destinations. More Info... |
| Temporary Template Name: | | The name of a configured JMS template that this JMS server uses to create temporary destinations. More Info... |

- 5 Enter the directory of the paging store in the **Paging Directory** field.
For example enter, <SI_Install_Dir>/jmsstore<Server1>
where <Server1> is the server ID in the cluster.
- 6 In the **Message Buffer Size** field, enter **100000000** (hint: that's 8 zeros) and click **Save**.
- 7 On the **Configuration** → **Thresholds & Quotas** tab, enter **100000000** (100MB) (8 zeros) in the **Bytes Threshold High** box.
- 8 In the **Bytes Threshold Low** box, enter **10000000** (10MB) (hint: that's 7 zeros).
- 9 In the **Bytes Maximum** box enter **-1** for an unlimited quota. The JMS server limit must be higher than the limit for queues.
- 10 In the **Blocking Send Policy** box, select **FIFO** and click **Save**.
- 11 On the **Change Center** panel, click **Activate Changes**.

Creating JMS System Resources: Destination Key, Topics, and Queues

In this section you will create the JMS system resources for both, single and cluster servers. This includes the destination key, topics, and queues. You must create and configure each of the specific resources that are listed in this section.

Creating the Destination Key

Follow these steps to create the destination key:

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 From the **Domain Structure** panel, navigate to <My Domain> → **Services** → **Messaging** > **JMS Modules**.
- 3 On the **JMS Modules** page, in the **JMS Modules** table, click the JMS module name that you created earlier in [Creating the JMS System Module](#) on page 128.
- 4 On the **Configuration** tab of the **Settings for <Your JMS Module>** page, click **New** in the **Summary of Resources** table.

Figure 140 Create a New JMS System Module Resource

Create a New JMS System Module Resource

Back Next Finish Cancel

Choose the type of resource you want to create.
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

Depending on the type of resource you select, you are prompted to enter basic information for creating the resource. For targetable resources, like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations, you can also proceed to targeting pages for selecting appropriate server targets. You can also associate targetable resources with subdeployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources.

| | |
|--|---|
| <input type="radio"/> Connection Factory | Defines a set of connection configuration parameters that are used to create connections for JMS clients. More Info... |
| <input type="radio"/> Queue | Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer. More Info... |
| <input type="radio"/> Topic | Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers. More Info... |
| <input type="radio"/> Distributed Queue | Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients. More Info... |
| <input type="radio"/> Distributed Topic | Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. More Info... |
| <input type="radio"/> Foreign Server | Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain. More Info... |

- 5 On the **Create a New JMS System Module Resource** page, click **Destination Sort Key** and then click **Next**.
- 6 In the **Name** box, enter `jms.PriorityDestinationKey` as the filename of the **Destination Sort Key** and click **OK**.
- 7 On the **Change Center** panel, click **Activate Changes**.

Creating Topics

Now that you have created the destination key, follow these steps to create the topics:

▶ For clusters, you must create and configure every JMS topic listed in this procedure. But since the topics are deployed to the nodes automatically, it is not necessary to repeat this procedure for the individual nodes.

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 Continuing on the **Settings for <Your JMS Module>** page, on the **Configuration** tab, click **New** in the **Summary of Resources** table.

Figure 141 Create a New JMS System Module Resource

Create a New JMS System Module Resource

Back Next Finish Cancel

Choose the type of resource you want to create.
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

Depending on the type of resource you select, you are prompted to enter basic information for creating the resource. For targetable resources, like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations, you can also proceed to targeting pages for selecting appropriate server targets. You can also associate targetable resources with subdeployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources.

| | |
|--|---|
| <input type="radio"/> Connection Factory | Defines a set of connection configuration parameters that are used to create connections for JMS clients. More Info... |
| <input type="radio"/> Queue | Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer. More Info... |
| <input type="radio"/> Topic | Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers. More Info... |
| <input type="radio"/> Distributed Queue | Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients. More Info... |
| <input type="radio"/> Distributed Topic | Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. More Info... |
| <input type="radio"/> Foreign Server | Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain. More Info... |

- 3 On the **Create a New JMS System Module Resource** page, click **Topic**. (For clusters, click **Distributed Topic** and input the name and JNDI information for this distributed topic. Leave the default target as the cluster name.)
- 4 Click **Next**.

Figure 142 Create New Topic

You will create the following two JMS topics; one at a time. Each topic will have a filename and a JNDI name, as shown in the following table:

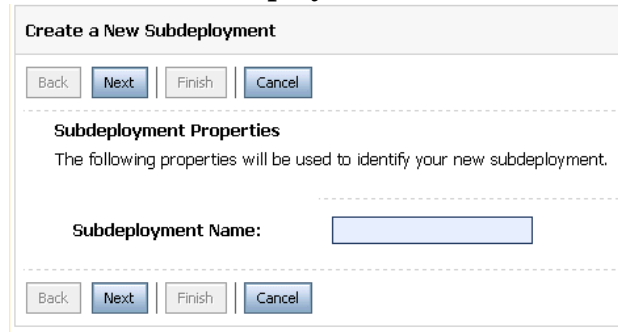
| Topic Filename | Topic JNDI Name |
|------------------------|------------------------|
| jms.OVSIAuditBroadcast | jms/OVSIAuditBroadcast |
| jms.OVSIcCacheTopic | jms/OVSIcCacheTopic |

- 5 In the **Name** box, enter the topic filename.
- 6 In the **JNDI Name** box, enter the topic JNDI name and click **Next**.
- 7 In the **Subdeployments** drop-down list, select the target of the subdeployment as the JMS server that you just created. If a subdeployment does not exist, you can create one as described in the steps that follow.
- 8 Click **Finish**.

If the subdeployment is not listed, follow these steps to create a new one:

- a From the **Domain Structure** panel, navigate to **Services** → **Services** → **Messaging** > **JMS Modules**.
- b In the **JMS Modules** table, click on the JMS module for which you will create the subdeployment.
- c Click the **Subdeployments** tab.
- d In the **Subdeployments** table, click **New**. The **Create a New Subdeployment** page displays.

Figure 143 Create New Subdeployment



- e In the **Subdeployment Name** box, enter the name of the new subdeployment.
 - f Click **Next**.
 - g Select the target server for the subdeployment.
 - h Click **Finish**.
- 9 In the **Targets** table, select the JMS server that you created earlier in [Creating the JMS Server](#) on page 133.
 - 10 Click **Finish**. A confirmation message displays, *“The JMS Topic was created successfully.”* Repeat these steps to create the second JMS topic. Remember, for clusters it is not necessary to repeat this procedure for the individual nodes.
 - 11 When you have created the second topic, click **Activate Changes** on the **Change Center** panel.

Creating Queues

You have now created the destination key and two topics. The only resources that you have left to create are the queues.

Continuing on the **Settings for <Your JMS Module>** page, follow these steps to create the JMS queues:

- ▶ For clusters, you must create and configure every JMS queue listed in this procedure. But since the queues are deployed to the nodes automatically, it is not necessary to repeat this procedure for the individual nodes.
- 1 On the **Change Center** panel, click **Lock & Edit**.
 - 2 On the **Configuration** tab, click **New** in the **Summary of Resources** table.

Figure 144 Create a New JMS System Module Resource

- 3 On the **Create a New JMS System Module Resource** page, select **Queue**. For clusters, select **Distributed Queue** and input the name and JNDI information for this distributed queue. Leave the default target as the cluster name.
- 4 Click **Next**.

Figure 145 Create New Queue

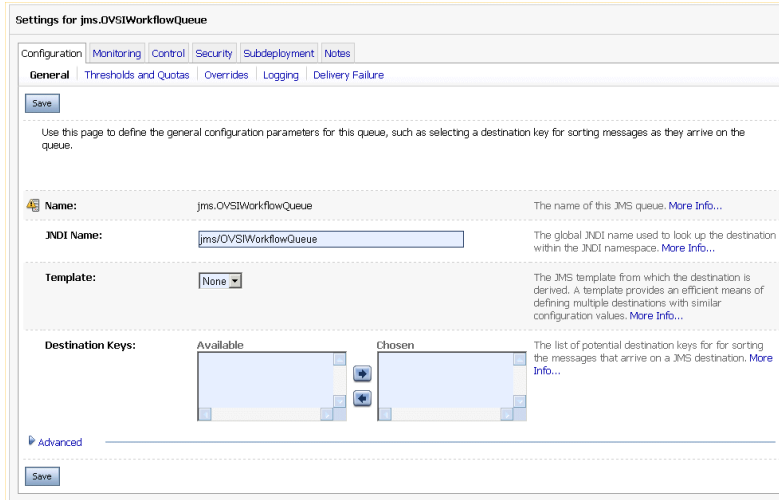
You will create each of the following JMS queues; one at a time. Each queue will have a filename and a JNDI name, as shown in the table below.

| Queue Filename | Queue JNDI Name |
|-----------------------------------|-----------------------------------|
| jms.OVSIAuditProcQ | jms/OVSIAuditProcQ |
| jms.OVSIBulkQueue | jms/OVSIBulkQueue |
| jms.OVSIChangeReconProcessorQueue | jms/OVSIChangeReconProcessorQueue |
| jms.OVSIIDAProcQ | jms/OVSIIDAProcQ |
| jms.OVSIEntCacheQueue | jms/OVSIEntCacheQueue |
| jms.OVSIKeyRotationQueue | jms/OVSIKeyRotationQueue |
| jms.OVSIMessageAckQueue | jms/OVSIMessageAckQueue |
| jms.OVSIReconQueue | jms/OVSIReconQueue |
| jms.OVSIRecoveryProcQ | jms/OVSIRecoveryProcQ |

| Queue Filename | Queue JNDI Name |
|------------------------------|------------------------------|
| jms.OVSIRecoveryQueue | jms/OVSIRecoveryQueue |
| jms.OVSIResReconDispatcherQ | jms/OVSIResReconDispatcherQ |
| jms.OVSIResReconQ | jms/OVSIResReconQ |
| jms.OVSIISaudQ | jms/OVSIISaudQ |
| jms.OVSIISchedulerQueue | jms/OVSIISchedulerQueue |
| jms.OVSIServiceAssignQueue | jms/OVSIServiceAssignQueue |
| jms.OVSIUserImportPQueue | jms/OVSIUserImportPQueue |
| jms.OVSIWfRequestExpireQueue | jms/OVSIWfRequestExpireQueue |
| jms.OVSIWorkflowQueue | jms/OVSIWorkflowQueue |

- 5 In the **Name** box, enter the queue filename.
- 6 In the **JNDI Name** box, enter the queue JNDI name and click **Next**.
- 7 In the **Subdeployments** drop-down list, select the subdeployment for your new queue.
If the subdeployment is not listed, follow these steps:
 - a Click **Create a New Subdeployment**. The Create a New Subdeployment page displays.
 - b In the **Subdeployment Name** box, enter the name of the new subdeployment, and click **OK**.
- 8 In the **Targets** table, select the JMS server that you created earlier in [Creating the JMS Server](#) on page 133.
- 9 Click **Finish**. A confirmation message displays, *"The JMS Queue was created successfully."* Repeat these steps until all of the listed queues have been created. For clusters it is not necessary to repeat this procedure for the individual nodes.
- 10 On the **Change Center** panel, click **Activate Changes** then click **Lock & Edit**.
- 11 After you have created all the JMS queues, you will need to return to the OVSIWorkflowQueue to complete the setup for it. In the **Summary of Resources** table, click the filename `jms.OVSIWorkflowQueue`.

Figure 146 Settings for jms.OVSIWorkflowQueue



- 12 On the **Settings for jms.OVSIWorkflowQueue** page, click the **Configuration →Delivery Failure** tab.
- 13 In the **Expiration Policy** drop-down box, select **Redirect**.
- 14 In the **Error Destination** drop-down box, select `jms.OVSIWfRequestExpireQueue` and click **Save**.
- 15 On the **Configuration →Overrides** tab, select **Persistent** from the **Delivery Mode Override** drop-down box, and click **Save**.
- 16 On the **Change Center** panel, click **Activate Changes**.

You have now completed the tasks of creating the JMS system resources: the destination key, topics, and queues.

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 On the **Change Center** panel, click **Lock & Edit**.
- 2 Open the **JTA** page by navigating to `<My Domain> →Services →JTA`.
- 3 Set the timeout to **300** seconds in the **Timeout Seconds** field.
- 4 Click **Save**.
- 5 On the **Change Center** panel, click **Activate Changes**.

Creating a JDBC Connection Pool

All of the JMS settings are now configured. Next, you will create and configure a JDBC connection pool and data source that will enable WebLogic to communicate with the database server.

To create a JDBC connection pool, follow these steps:

- 1 On the **Change Center** panel, click **Lock & Edit**.

- From the **Domain Structure** panel, navigate to **<My Domain> → Services → JDBC → Data Sources**.
- On the **Summary of JDBC Data Sources** page, click **New** in the **Data Sources** table.

Figure 147 Create a New JDBC Data Source

The screenshot shows a dialog box titled "Create a New JDBC Data Source". At the top, there are navigation buttons: "Back", "Next", "Finish", and "Cancel". Below the title bar, the text "JDBC Data Source Properties" is displayed, followed by the instruction: "The following properties will be used to identify your new JDBC data source." The dialog contains four main sections, each with a question and a corresponding input field:

- Name:** The question is "What would you like to name your new JDBC data source?". The input field contains "JDBC Data Source-0".
- JNDI Name:** The question is "What JNDI name would you like to assign to your new JDBC Data Source?". The input field is empty.
- Database Type:** The question is "What database type would you like to select?". The drop-down menu is set to "PointBase".
- Database Driver:** The question is "What database driver would you like to use to create database connections?". The drop-down menu is set to "*PointBase's Driver (Type 4 XA) Versions: 4X,5,X".

At the bottom of the dialog, there are navigation buttons: "Back", "Next", "Finish", and "Cancel".

- On the **Create a New JDBC Data Source** page, enter a name for the new JDBC data source in the **Name** box.
- In the **JNDI Name** box, enter `jdbc/TruAccess`.
- In the **Database Type** drop-down box, select your database type.
- In the **Database Driver** drop-down box, select the appropriate database driver:
 - For Oracle, select the Oracle Driver (Thin XA) Versions: 9.0.1, 9.2.0, 10.
 - For MS-SQL, select BEA's MS-SQL Server Driver (Type 4) Versions: 7.0, 2000, 2005.
- Click **Next**.
- If you are using MS-SQL as your database, select the **Emulate Two-Phase Commit** option.
- Click **Next** again.

Figure 148 Create a New JDBC Data Source

The screenshot shows the 'Create a New JDBC Data Source' wizard at the 'Connection Properties' step. The title bar reads 'Create a New JDBC Data Source'. At the top, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. Below the title bar, the section is titled 'Connection Properties' with the instruction 'Define Connection Properties.' The form contains several input fields with labels and questions:

- Question: 'What is the name of database you would like to connect to?'
Label: 'Database Name:'
Input: 'Select_Identity'
- Question: 'What is the name or IP address of the database server?'
Label: 'Host Name:'
Input: (empty)
- Question: 'What is the port on the database server used to connect to the database?'
Label: 'Port:'
Input: '3306'
- Question: 'What database account user name do you want to use to create database connections?'
Label: 'Database User Name:'
Input: (empty)
- Question: 'What is the database account password to use to create database connections?'
Label: 'Password:'
Input: (empty)
- Label: 'Confirm Password:'
Input: (empty)

At the bottom of the form, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 11 On the next **Create a New JDBC Data Source** page, enter the name of the database created on the database server for use by Select Identity in the **Database Name** box. For example, enter `Select_Identity`.
- 12 In the **Host Name** box, enter the IP address or host name of the database server.
- 13 In the **Port** box, enter the database port. The default port for Oracle is **1521**. For MS SQL, accept the default.
- 14 In the **Database User Name** box, enter the Select Identity database admin user name.
- 15 In the **Password/Confirm Password** boxes, enter the database user password.
- 16 Click **Next**.
- 17 If you are installing Select Identity with Oracle, add the following on a separate line in the **Properties** field:

```
SetBigStringTryClob=true
```
- 18 Click **Test 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 the connection was successful.
- 19 Click **Next**. The **Create a New JDBC Data Source** page opens.

Figure 149 Create a New JDBC Data Source

The screenshot shows the 'Create a New JDBC Data Source' wizard at the 'Select Targets' step. The title bar reads 'Create a New JDBC Data Source'. At the top, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. Below the title bar, the section is titled 'Select Targets' with the instruction: 'You can select one or more targets to deploy your new JDBC data source. If you don't select a target, the data source will be created but not deployed. You will need to deploy the data source at a later time.' Below this instruction is a table with the following content:

| Servers |
|--------------------------------------|
| <input type="checkbox"/> AdminServer |

At the bottom of the form, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 20 In **Select Targets** box, select one or more targets to deploy your new JDBC data source. If you do not select a target, the data source will be created but not deployed. You will need to deploy the data source at a later time.
- 21 Click **Finish**.
- 22 On the **Change Center** panel, click **Activate Changes**.

Configuring a JDBC Connection Pool and Data Source

To configure a JDBC connection pool and data source, follow these steps:

➤ For clusters, repeat this procedure for each server in the cluster.

- 1 On the **Change Center** panel, click **Lock & Edit**.
- 2 From the **Domain Structure** panel, navigate to <My Domain> →**Services** →**JDBC** →**Data Sources**.
- 3 On the **Summary of JDBC Data Sources** page, click the **Data Source** you just created.

Figure 150 Settings for a JDBC Data Source

The screenshot shows the 'Settings for JDBC Data Source-0' configuration page. At the top, there are tabs for 'Configuration', 'Targets', 'Monitoring', 'Control', 'Security', and 'Notes'. Below these is a sub-tabbed interface with 'General', 'Connection Pool', 'Transaction', 'Diagnostics', and 'Identity Options'. The 'General' tab is selected. The page contains several sections:

- A header section with instructions: 'Click the **Lock & Edit** button in the Change Center to modify the settings on this page.' and 'Applications get a database connection from a data source by looking up the data source on the Java Naming and Directory Interface (JNDI) tree and then requesting a connection. The data source provides the connection to the application from its pool of database connections. This page enables you to define general configuration options for this JDBC data source.'
- A 'Name' field with the value 'JDBC Data Source-0' and a description: 'A unique name that identifies this data source in the WebLogic domain. [More Info...](#)'
- A 'JNDI Name' field with the value 'jdbc/TruAccess' and a description: 'The JNDI path to where this data source is bound. By default, the JNDI name is the name of the data source. [More Info...](#)'
- A 'Row Prefetch Enabled' checkbox which is checked, with a description: 'Enables multiple rows to be "prefetched" (that is, sent from the server to the client) in one server access. [More Info...](#)'
- A 'Row Prefetch Size' field with the value '48' and a description: 'If row prefetching is enabled, specifies the number of result set rows to prefetch for a client. [More Info...](#)'
- A 'Stream Chunk Size' field with the value '256' and a description: 'Specifies the data chunk size for streaming data types. [More Info...](#)'

 At the bottom, there is another instruction: 'Click the **Lock & Edit** button in the Change Center to modify the settings on this page.'


- 4 Navigate to the **Configuration** →**Connection Pool** tab on the **Settings for <Your JDBC Data Source>** page.
- 5 In the **Initial Capacity** box, enter 15.
- 6 In the **Maximum Capacity** box, enter 100.
 - **Maximum Capacity** defines the maximum number of connections per server. If you set the maximum capacity to 100, that means the maximum number of connections for the first server is 100. For each additional server, the maximum number of connections is increased by 50.
- 7 In the **Capacity Increment** box, enter 5.
- 8 In the **Statement Cache Type** drop-down box, select **LRU** or **Fixed**.
- 9 In the **Statement Cache Size** box, enter 50 for both, a single server or a cluster.
- 10 Click **Save**.

- 11 Click the **Advanced** button.
- 12 Check the **Test Connection On Reserve** box and click **Save**.
- 13 Navigate to the **Configuration** → **Targets** tab on the **Settings for <Your JDBC Data Source>** page.
- 14 Ensure that your server is selected and click **Save**.
- 15 On the **Change Center** panel, click **Activate Changes**.

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.

 For clusters, repeat this procedure for each server in the cluster.

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

Windows:

```
stopWebLogic.cmd
```

UNIX:

```
./stopWebLogic.sh
```

On a cluster, to stop the servers through the WebLogic console: in the left panel of the console, click on the cluster name and select each node to stop. Click **Start/Stop this Cluster**.

- 2 After restarting the server(s), navigate to **<My Domain>** → **Environment** → **Servers**.
- 3 On the **Servers** table, look in the **State** column to verify the state of the server.
- 4 To modify a server, click on it in the **Servers** table.
- 5 On the **Settings for <Your Server>** page, navigate to the **Configuration** → **Server Start** tab.
- 6 On the **Change Center** panel, click **Lock & Edit**.
- 7 Enter the required information as follows in the provided fields. Specific paths may vary on your system:

| Field | Action |
|------------------|--|
| Java Home | <p>Windows: <BEA_Home>\jrockit-jdk1.5.0_06\ UNIX: <BEA_Home>/jrockit90_150_06 For single servers: Do not make this setting.</p> |
| BEA Home | <p><BEA_Home> The actual path to the WebLogic home directory, for example: /opt/bea For single servers: Do not make this setting.</p> |

| Field | Action |
|-----------------------|--|
| Root Directory | <p><BEA_Home>/common/nodemanager</p> <p>The path to the Node Manager for the cluster.</p> <p>For single servers:</p> <p>Do not make this setting.</p> |
| Class Path | <p>Class paths are the directory locations of critical system files, and they must be provided in the correct order. Use the examples below for reference.</p> <p>Windows:</p> <pre>C:\<SI_Install_Dir>\sysArchive\bcprov-jdk15-135.jar C:\<BEA_Home>\jrockit-jdk1.5.0_06\lib\tools.jar; C:\<BEA_Home>\weblogic92\server\lib\weblogic.jar; C:\<SI_Install_Dir>\weblogic\sysArchive\connector.jar; C:\<SI_Install_Dir>\weblogic\sysArchive\ovsii18n.jar; C:\<SI_Install_Dir>\weblogic\lib\commons-logging-1.1.jar</pre> <p>UNIX:</p> <pre>/opt/<SI_Install_Dir>\sysArchive\bcprov-jdk15-135.jar /opt/<BEA_Home>/jrockit90_150_06/lib/tools.jar: /opt/<BEA_Home>/weblogic92/server/lib/weblogic.jar: /opt/<SI_Install_Dir>/weblogic/sysArchive/connector.jar: /opt/<SI_Install_Dir>/weblogic/sysArchive/ovsii18n.jar: /opt/<SI_Install_Dir>/weblogic/sysArchive/ commons-logging-1.1.jar</pre> <p>For single servers:</p> <p>Set the class path by editing the <code>myStartWL.sh</code> or <code>myStartWL.cmd</code> script in the WebLogic domain directory where you will be running Select Identity.</p> |
| Arguments | <pre>-server -Xms256m -Xmx1024m</pre> <p>If you are <i>not</i> using BEA's JRockit Java Developer Kit (regardless of your operating system environment), add the argument <code>-XX:MaxPermSize=256m</code> to the end of the arguments.</p> <p>On Windows systems, add the argument <code>-Dcom.truologica.truaccess.property.file=<SI_Install_Dir>/sysArchive/TruAccess.properties</code></p> <p>On UNIX systems, add the argument <code>-Djava.awt.headless=true</code></p> <p>Add the argument that specifies the location and name of the <code>logging.properties</code> file for that server, using the example below for reference:</p> <pre>-Djava.util.logging.config.file=<SI_Install_Dir>/ sysArchive/myServer1_logging.properties</pre> <p>For single servers:</p> <p>You must set these arguments by editing the <code>myStartWL.cmd</code> or <code>myStartWL.sh</code> script in the WebLogic Server domain directory where you will be running Select Identity.</p> <p>For clusters:</p> <p>Use a UNC notation in a clustered environment. For example,</p> <pre>\\x.x.x.x\sysArchive\TruAccess.properties</pre> |

- 8 For clusters, repeat this process until you have updated each server in the cluster.
- 9 Click **Save**.

- 10 On the **Change Center** panel, click **Activate Changes**.

Enabling Anonymous Admin Lookup

To enable Anonymous Admin Lookup, perform the following steps:

- 1 From the **Domain Structure** panel, navigate to **<My Domain> → Services → JTA**. The **Settings for <My Domain>** page displays.

Figure 151 Settings for <My Domain>

Settings for wl_server

Configuration | Monitoring | Control | Security | Web Service Security | Notes

General | **JTA** | EJBs | Web Applications | SMP | Logging | Log Filters

Save

Use this page to define the Java Transaction API (JTA) configuration of this WebLogic Server domain.

| | | |
|--|-------|---|
| Timeout Seconds: | 500 | The transaction timeout seconds for active transactions, before the prepared state. More Info... |
| Abandon Timeout Seconds: | 6400 | The transaction abandon timeout seconds for transactions in the second phase of the two-phase commit (prepared and later). More Info... |
| Before Completion Iteration Limit: | 10 | The maximum number of cycles that the transaction manager will perform the beforeCompletion synchronization callback for this WebLogic Server domain. More Info... |
| Max Transactions: | 10000 | The maximum number of simultaneous in-progress transactions allowed on a server in this WebLogic Server domain. More Info... |
| Max Unique Name Statistics: | 1000 | The maximum number of unique transaction names for which statistics will be maintained. More Info... |
| Checkpoint Interval Seconds: | 300 | The interval at which the transaction manager creates a new transaction log file and checks all old transaction log files to see if they are ready to be deleted. More Info... |
| <input checked="" type="checkbox"/> Forget Heuristics | | Specifies whether the transaction manager will automatically perform an XAResource forget operation for heuristic transaction completions. More Info... |
| Unregister Resource Grace Period: | 30 | The grace period (number of seconds) that the transaction manager waits for transactions involving the resource to complete before unregistering a resource. The grace period can help minimize the risk of abandoned transactions because of an unregistered resource, such as a JDBC More Info... |

- 2 On the **<MyDomain> → Security → General** tab, check the **Anonymous Admin Lookup Enabled** box and click **Save**.

▶ You may also edit the `TruAccess.properties` file in `<SI_Install_Dir>/sysArchive/` to point to the correct URL:

```
hpsi.schema.accessurl.internal=http://localhost:7001/lmz
hpsi.schema.accessurl.external=http://www.company.com:7001/lmz
```

Starting the WebLogic Server

On a single server, start the WebLogic server process at the command line by entering the appropriate script, according to your operating system:

Windows:

```
myStartWL.cmd
```

UNIX:

```
./myStartWL.sh
```

On a cluster, to start the servers through the WebLogic console:

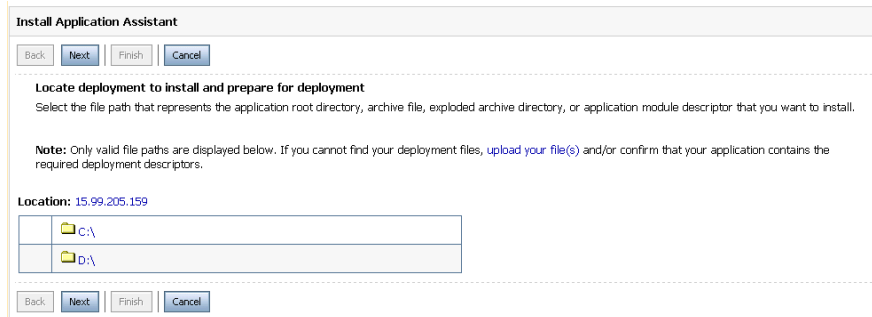
- 1 In the left panel of the console, select **Environment → Clusters → <SI Cluster> → Control**.
- 2 Select each server, and then click **Start**.

Deploying the Select Identity Application

Follow these steps to deploy Select Identity on the WebLogic server:

- 1 Log in to the **WebLogic Server Console**.
- 2 On the **Change Center** panel, click **Lock & Edit**.
- 3 From the **Domain Structure** panel, navigate to **<My Domain> → Deployments**. The **Summary of Deployments** page displays.
- 4 On the **Control** tab, click **Install** in the **Deployments** table.

Figure 152 Install Application Assistant



- 5 On the **Install Application Assistant** page, click the drive and then the path where the deployment files reside.
- 6 Drill down the path until you locate and select the `lmz.ear` file, which resides in the `<SI_Install_Dir>/deploy` directory created in [Creating Select Identity Directories and Copying Installation Files](#) on page 122.
- 7 Click **Next**.
- 8 Choose your targeting style for deploying Select Identity and click **Next**.
- 9 Select the deployment target (select the cluster if you are installing on a WebLogic cluster) and click **Next**. The `lmz.ear` file will deploy, module by module, onto the selected target. The deployment may take a few minutes to complete.
- 10 If desired, you can enter optional settings and click **Next**.
- 11 Review your choices and click **Finish**.
- 12 Review the list to make sure all files deployed successfully.
- 13 Click **Save**.
- 14 On the **Change Center** panel, click **Activate Changes**.
- 15 Verify that the JMS Settings are correct.
 - ▶ If a setting is not specified, accept the WebLogic default. Refer to [Configuring JMS Settings for a Single Server and Cluster Servers](#) on page 128 and [Configuring JMS Settings for a Single Server and Cluster Servers](#) on page 128.
- 16 After installing Select Identity, refer to [Appendix B, WebLogic Logging Options](#) 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.

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 `ovsill10n_help_en_US.war` file, which is stored on the Select Identity product CD, in the `application` directory with the `lmz.ear` application file.
 - 2 Copy the `.war` file into the `<SI_Install_Dir>/deploy` directory.
 - 3 Use the instructions provided in [Deploying the Select Identity Application](#) on page 148 to locate and deploy the help files in the same way as you did for `lmz.ear`.
- Additional product documentation is provided in PDF format in the `/docs` directory on the Select Identity product CD. Copy these documents to the directory location of your choice.

Post-Installation Steps

After installing Select Identity, perform the following additional steps:

- 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 the Paging Store](#) on page 134.
- 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, WebLogic Logging Options](#) for information.
- After installation, remove the `qname.jar` file (which is located at `c:\<SI_Install_Dir>\Weblogic\lib\qname.jar`) from the classpath.

Configuring WebLogic for Mutual Authentication

Perform this procedure to configure WebLogic system security parameters and enable mutual authentication functionality.

- A best practice recommendation is to use a new keystore to avoid having to change an existing keystore for other applications that may be implemented already.

Prerequisites

The following conditions must be met before you can perform this procedure:

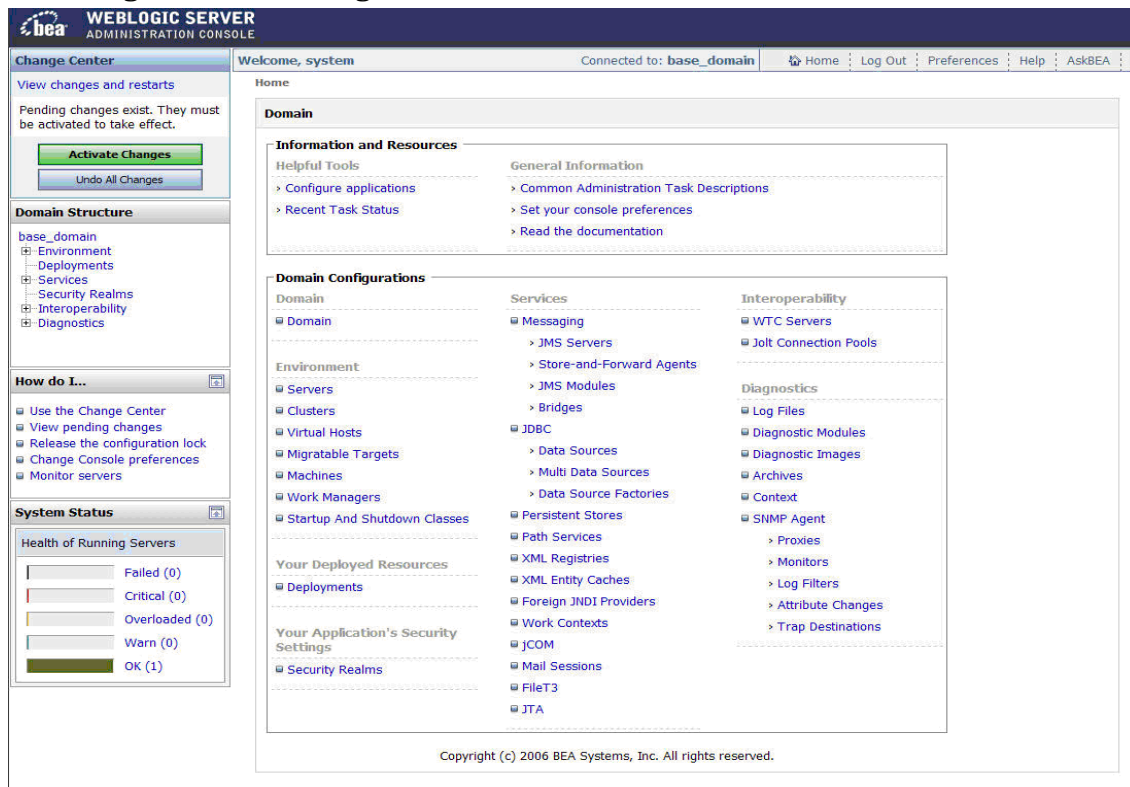
- You have administrative privileges to the WebLogic server.
- You know the keystore and truststore file locations.
- You know how your business uses SSL and Select Identity.
- You have identified whether you will be using Select Identity in secure or regular HTTP mode.
- You have determined if Select Identity is running in secure mode only.

Procedure – Single Server

To configure a single WebLogic server to enable mutual authentication, perform the following steps:

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

Figure 153 WebLogic Server Console



- 2 From the **Domain Structure** panel, navigate to **<My Domain> → Environment → Servers**. The **Summary of Servers** page displays, containing a list of all servers that are available.

Figure 154 Summary of Servers

The screenshot shows the WebLogic Server Administration Console interface. The main content area is titled "Summary of Servers" and contains the following text:

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration. This page summarizes each server that has been configured in the current WebLogic Server domain.

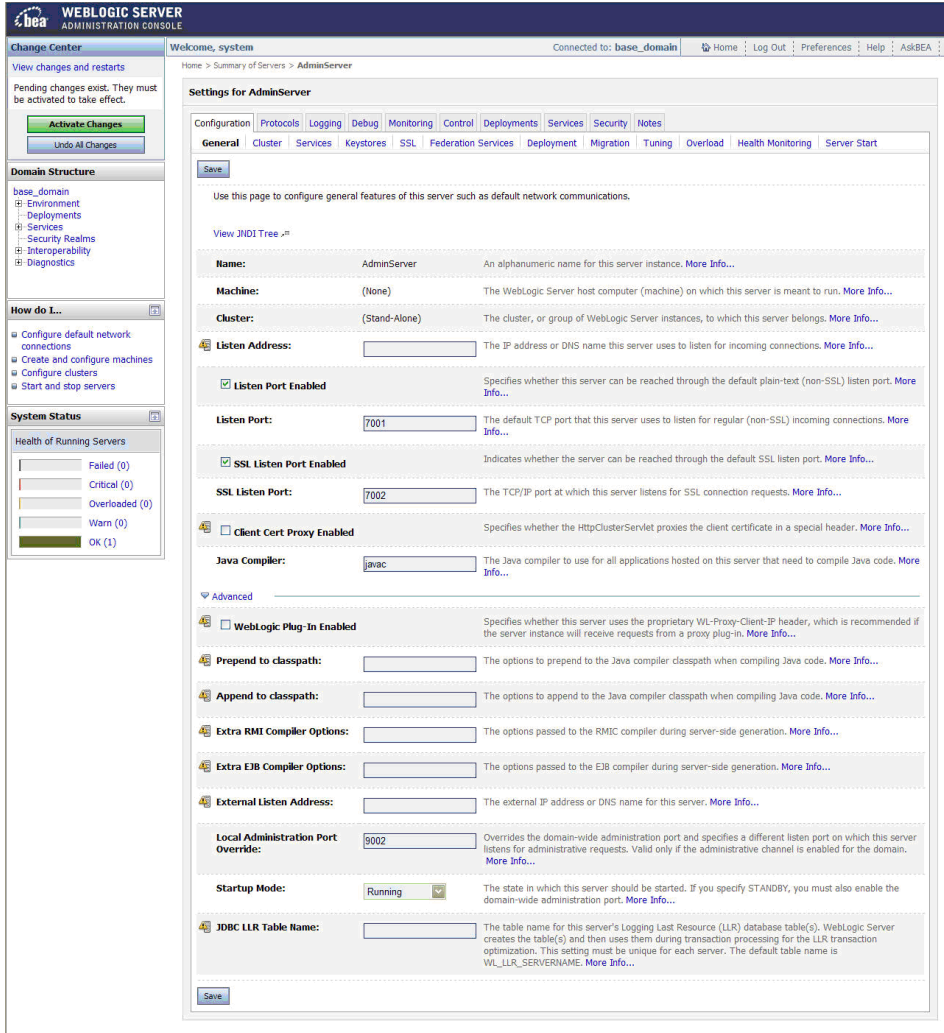
Below the text is a table of servers. The table has columns for Name, Cluster, Machine, State, Health, and Listen Port. There is one server listed: AdminServer(admin), which is in the RUNNING state with a health of OK and is listening on port 7001.

The left sidebar contains several sections:

- Change Center:** View changes and restarts. No pending changes exist. Click the Release Configuration button to allow others to edit the domain. Buttons: Lock & Edit, Release Configuration.
- Domain Structure:** base_domain
 - Environment
 - Deployments
 - Services
 - Security Realms
 - Interoperability
 - Diagnostics
- How do I...:**
 - Create Managed Servers
 - Delete Managed Servers
 - Delete the Administration Server
 - Start and stop servers
- System Status:** Health of Running Servers
 - Failed (0)
 - Critical (0)
 - Overloaded (0)
 - Warn (0)
 - OK (1)

- 3 Select the server you want to configure. In this example, select **AdminServer(admin)** . The **Settings for <Your Admin Server>** page opens. You will use this page to configure general features of this server such as the default network communications.

Figure 155 Settings for <Your Admin Server>



4 Click the **Configuration** → **KeyStores** tab.

The **Keystores** page opens.

Figure 156 Keystores Tab

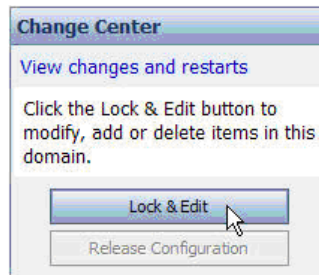
Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). The **Keystores** page allows you to view and define keystore configurations. These settings help you manage the security of message transmissions.

After you configure identity and trust keystores for a WebLogic server instance, you can configure its SSL attributes. These attributes include information about the identity and trust location for particular server instances. You will use the **Configuration: SSL** page (discussed later in this section) to identify this information.

- 5 On the **Change Center** panel, click **Lock & Edit**.

This allows you to make changes to the page. After you make changes, the option name temporarily changes to **Activate Changes**.

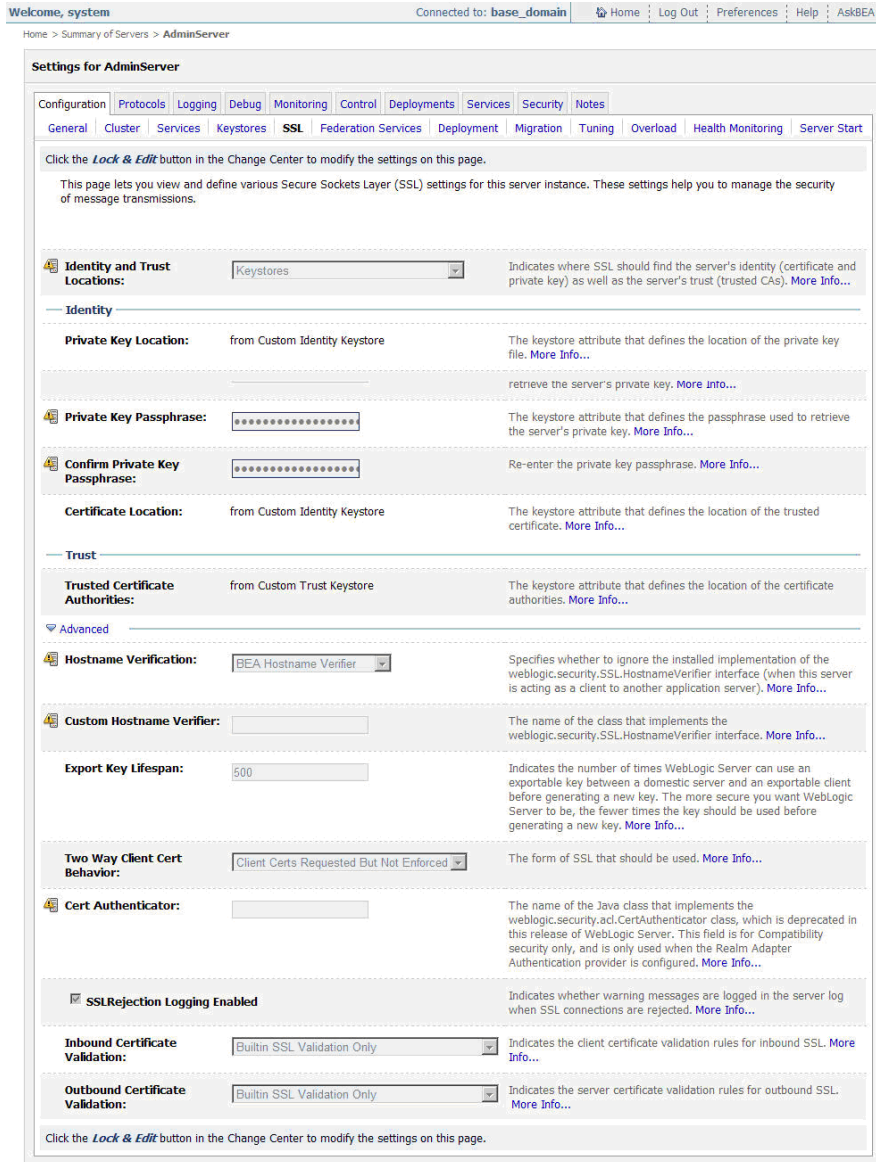
Figure 157 Lock & Edit Button



- 6 In the **Identity** and **Trust** sections, enter the appropriate values.
- 7 Click **Save**, and then click **Activate Changes**.
- 8 Click the **SSL** tab.

The **SSL Configuration** page opens. This page enables you to view and define SSL settings for this server instance.

Figure 158 SSL Configuration



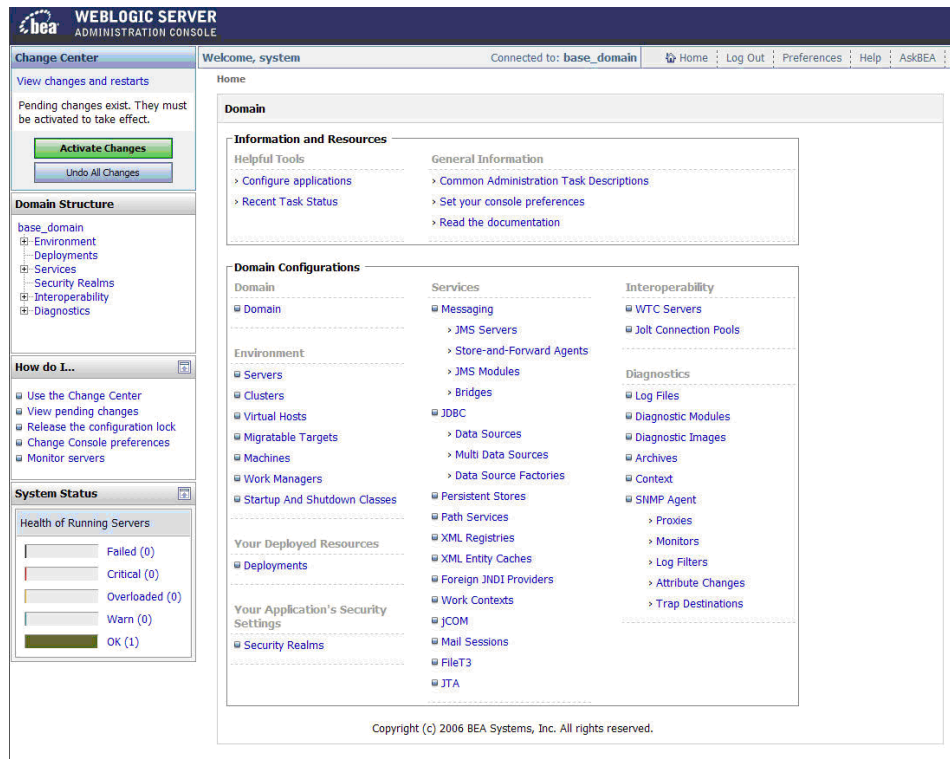
- 9 Be sure the **Two Way Client Cert Behavior** field is set to **Client Certs Requested But Not Enforced**.
- 10 On the **Change Center** panel, click **Lock & Edit**.
- 11 Enter the appropriate values for the **SSL Configuration** page.
- 12 Click **Save**, then click **Activate Changes**.
A success message displays under the tabs.
- 13 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. For more information, refer to the *HP Select Identity Administration Online Help*.

Procedure – Clustered Servers

To configure a cluster of WebLogic servers to enable mutual authentication, secure object migration, and key rotation functionality, perform the following steps:

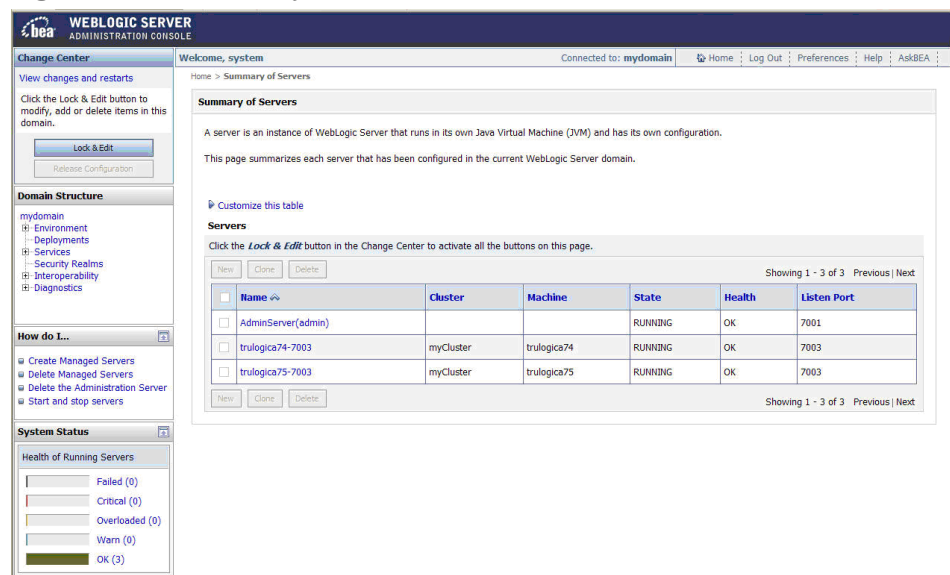
- 1 Log in to the **WebLogic Server Console**.

Figure 159 WebLogic Server Console




- 2 From the **Domain Structure** panel, navigate to **<My Domain> → Environment → Servers**. The **Summary of Servers** page displays, containing a list of all servers that are available.

Figure 160 Summary of Servers



You can now see the server and the cluster group, which in the above example, displays two servers that are part of the cluster.

- 3 Click the admin server and configure the keystore and truststore information by following the procedure that you used to configure a single server. (See steps 5-12 for configuring a WebLogic single server.)
- 4 Configure the keystore and truststore information for each server in the cluster by following the procedure that you used to configure a single server.
- 5 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. For more information, refer to the *HP Select Identity Administration Online Help*.

 When installing keystores, you can verify your installation by turning on the WebLogic auto debugging property. For more information about how to do this, refer to your WebLogic reference materials.

Logging In to Select Identity

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

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

The default login is **sis**. The password is **abc123**. We recommend that you change this as soon as possible.

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 Keystores, Truststores, and Security Framework](#)
- [Recommended Configuration](#)
- [Custom User Interface Properties](#)
- [Internationalization and Localization](#)
- [Configuration for Specific Environments or Platforms](#)
- [Configuring Java 2 Security for Select Identity on WebSphere](#)



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 `<SI_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 235.

How to Set Properties

To change the default value of any property in the `TruAccess.properties` file, use a text editor 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=<SI_Install_Dir>/userimport/adroot`
- `ovsi.ad.backupdir=<SI_Install_Dir>/userimport/adbackup`
- `ovsi.ad.stagingdir=<SI_Install_Dir>/userimport/adstaging`
- `truaccess.recon.rootdir=<SI_Install_Dir>/recon/reconroot`
- `truaccess.recon.stagingdir=<SI_Install_Dir>/recon/reconstaging`
- `truaccess.recon.backupdir=<SI_Install_Dir>/recon/reconbackup`
- `truaccess.batch.reportdir=<SI_Install_Dir>/reports`
- `truaccess.upload.fileldir=<SI_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.fileldir=<common root directory>
```

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

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

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

```
<truaccess.upload.fileldir>/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.fileidir
```

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
```

Reconciliation Task Retry

This property sets the number of times that a task is retried before the termination process is marked as failed. The default setting is 3.

```
com.hp.si.recon.retry.limit=3
```

Reconciliation Task Termination

Select Identity attempts to determine the status of termination at a predefined interval. This interval is defined by the parameter `com.hp.si.req.term.waitperiod`, which defaults to 100 milliseconds. The number of times this check is executed is determined by `com.hp.si.req.term.waitcount`, which defaults to 6000 times. These two parameters determine how long Select Identity waits for the termination to complete. If the termination is not completed during this period, the termination job is marked as failed.

The following property sets the interval, in milliseconds, between periodic checks by Select Identity to determine if all requests associated with the task have been terminated. The default setting is 100.

```
com.hp.si.req.term.waitperiod=100
```

The following property sets the number of times that Select Identity checks whether all requests associated with the task have been terminated. The default setting is 6000.

```
com.hp.si.req.term.waitcount=6000
```

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 174.
- Optimize Select Identity - see [Recommended Configuration](#) on page 171.

Configuring Delegated Request Dependency Control

Instead of handling requests in random order, delegated request dependency processing allows SI to handle requests in the order they are received at the parent request level. Delegated request dependency avoids conflicts of values between requests submitted for the same user.

▶ Request dependency processing is also known as serialization.

Disabling and Re-Enabling Delegated Request Dependency

By default, delegated request dependency is enabled. To disable delegated request dependency, add the following property set to `true` in the `TruAccess.properties` file:

```
hp.si.delegated.request.nodependency=true
```

Setting Up Keystores, Truststores, and Security Framework

Select Identity now has a new and more robust security framework. When the application runs for the first time, the security framework is initialized in the Select Identity database so that subsequent runs to use the information from the database.

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

Setting up the default security framework profile enables an administrator to change the default security profile settings.



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

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 called the *bootstrap keystore*. The bootstrap keystore stores the following keys:

- A secret key for encrypting data in the database called the database key.
- A second secret key used internally by the security framework.
- (Optional) SPML data encryption key used to encrypt sensitive data in SPML.

There are two possible scenarios for setting 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 you are using a Hardware Security Module (HSM). Perform the procedure appropriate to your situation.

Non-Hardware Security Module (HSM) Procedure for Bootstrap Keystore Setup

The following procedure will create a:

- Keystore called **mykeystore**.
- Database encryption key alias called **myDBKey**.
- Security framework key alias called **mySFKey**.
- SPML data encryption key alias called **spmlenckey_new**.

To create a keystore property file, follow these steps:



This procedure is for a Unix operating system. Use `bat` files for Windows operating systems.

1 Prepare for the keystore configuration.

- Set up the Java™ environment variables to point to a proper JDK. It is recommended that you use the same JDK used by the application server. You can either set up the Java environment variables manually or use the command line setup utilities from the application server running Select Identity.

For example, to use the command line setup utilities from the application server, enter the following information:

In WebSphere

```
cd<WAS_Home>/bin  
. ./setupCmdLine.sh
```

In WebLogic

```
cd<WL_Home>/weblogic81/server/bin  
. ./setWLSEnv.sh
```

- b Run the “Java -version” command to ensure that you are using the appropriate JDK.
 - c Ensure that the `OVSISKeyStoreUtility` files are copied to the server so they can be accessed.
- 2 Create the database encryption key in the keystore.

- a Execute:

```
./genkey.sh
```

This message displays:

This utility creates one AES secret key in a JCEKS keystore.

- b Enter the full path of the store, including the store file name:

```
/opt/<SI_Install_Dir>/OVSISKeyStoreUtility/mykeystore
```

These messages display:

*File does not exist at the specified path.
KeyStore will be created.*

- c Enter the store password:

```
*****
```

- d Enter the key alias:

```
myDBKey
```

- e Enter the key password and then press **Enter** (or, just press **Enter** to use the store password).

- f And again, enter the key password and then press **Enter** (or, just press **Enter** to use the store password).

- g Select a key size from the list:

```
1:128  
2:192  
3:256
```

Select an option: 3

These messages display:

*Engine provider: SunJCE
Starting to verify the generated key.
Verified the generated key.
Finished!*

- 3 Create the security framework key in keystore without a key password.

- a Execute:

```
./genkey.sh
```

This message displays:

This utility creates one AES secret key in a JCEKS keystore.

- b Enter the full path of the store, including the store file name:
`/opt/<SI_Install_Dir>/OVSIKeyStoreUtility/mykeystore`
- c Enter the store password:


- d Enter the key alias:
mySFKey
- e Enter the key password and then press **Enter** (or, just press **Enter** to use the store password).
- f And again, enter the key password and then press **Enter** (or, just press **Enter** to use the store password).
- g Select a key size from the list:
1:128
2:192
3:256

Select an option: **3**

These messages display:


*Engine provider: SunJCE
Starting to verify the generated key
Verified the generated key
Finished!*

4 (Optional) Create the SPML data encryption key-pair in the keystore.

- 
 - Make sure the keytool command is in the \$PATH or %PATH% (Unix or Windows).
 - Color text is user input, black text is command prompt.
 - You can set alias name to whatever you like. `spmlenckey_new` is an example only, it must be unique in the keystore.
 - `keyalg` must be **RSA**.
 - `storetype` must be **jceks**

- a `keytool -genkey -alias spmlenckey_new -keyalg RSA -keystore /opt/<SI_Install_Dir>/OVSIKeyStoreUtility/mykeystore -storetype jceks`
- b Enter the keystore password:

- c Enter your first and last name.
John User
- d Enter the name of your organizational unit.
HVAC
- e Enter the name of your organization.
ABC Company
- f Enter the name of your city or locality.
MS

- g Enter the name of your State or Province.
MyState
 - h Enter the two-letter country code for this unit.
US
 - i Is CN=John User, OU=HVAC, O=ABC Company, L=MS, ST=MyState, C=US correct?
[no]: **y**
 - j Enter key password for <spmlenckey_new>
(RETURN if same as keystore password): **secret**
- 5 Create the bootstrap properties file.
- a Execute:
./genprop.sh
This message displays:
This utility creates a OVSI property file for key and truststores.
 - b Specify the file type to generate:
1:OVSI bootstrap keystore
2:OVSI secure object migration keystore
3:OVSI truststore
Select an option: **1**
 - c Enter the full path for the property file to be saved, including the file name. If the path doesn't include the file name, the default name `keystore.properties` will be used.
`/opt/<SI_Install_Dir>/OVSIKeyStoreUtility/mykeystore.properties`
 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.
This message displays:
The information will be stored in: /opt/<SI_Install_Dir>/OVSIKeyStoreUtility/mykeystore.properties
 - d Enter the full path of the store, including the store file name:
`/opt/<SI_Install_Dir>/OVSIKeyStoreUtility/mykeystore`
 - e Enter the store password:

 - f Enter the store password again:

 - g Enter the store type:
1:JCEKS
2:JKS
3:nCipher.sworld
Select an option: **1**

- h Enter the database encryption key alias:
- i Enter the key password and then press **Enter** (or, just press **Enter** to use the store password).
- j And again, enter the key password and then press **Enter** (or, just press **Enter** to use the store password).
- k Enter the security encryption key alias:

myDBKey

mySFKey

These messages display:

*Verifying the database encryption key Key verified.
Verifying the security framework encryption key Key verified.
Finished!*

Hardware Security Module (HSM) 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 this command line example as a reference 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 only if you are using **nCipher HSM** for the bootstrap keystore, Also, perform it on every server if you are installing on a cluster.

For WebLogic:

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

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

For WebSphere:

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

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

```
security.provider.3=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
```

Upgrading the Bootstrap Keystore from an Earlier Version (pre-4.10)

When upgrading the bootstrap keystore from a prior version of Select Identity (pre-4.10), you will need the old keystore password in order to add a new key.

The following procedure:

- Uses an existing keystore **40ksklp** that contains an existing database encryption key alias **40key**.
- Adds a new key alias **410sfkey**.

The following example shows the content of an old `keystore.properties` file. It assumes the old keystore was generated using the `ks_gen.sh` script (Linux) or `ks_gen.bat` script (Windows) provided in prior versions of Select Identity.

```
Select Identity Keystore Parameters
Fri Nov 03 16:03:59 CST 2006
si.keystore.filepath=/opt/si4.0/weblogic/keystore/40ksklp
si.keystore.storepass=WoYknWktXCHDyZf3l4xjh7qw2lZjaZ+i64LPCAahxjp9rjX
0ArNLdGv0qKR6PHrYPAsMp9Z6YUjhfUvSYyyk9/A9r80qhfjiz9XCF/
GcJ7cPFr9Gtoz6bVdcIXMxg2zLZiaRw43GFUAKlqv13bfeXA6H88W5GWzsm0kIzZDFEck
\=
si.keystore.keypass=OoOZwWSbM9PX/
wPGmGvlyIWAVvqjibW6WK+STCZmM5ddAXsqQcZHbwGCSeUD9g5opzjq2mTXoawu/
SgIimQMRDtGr1fZaWJ42ZkZR86KkHRF8YNxLcLvaE/NXIKknonu5f/
npw8KSK25WB5qu2y6RGqwrG1WavnsEL2rmViO0gk\=
si.keystore.alias=40key
```

Follow these steps to upgrade the bootstrap keystore from an earlier version of Select Identity:

- 1 Prepare for the keystore configuration.
 - a Set up the Java™ environment variables to point to a proper JDK. It is recommended that you use the same JDK used by the application server. You can either set up the Java environment variables manually or use the command line setup utilities from the application server running Select Identity.

For example, to use the command line setup utilities from the application server, enter the following information:

In WebSphere
`cd<WAS_Home>/bin`
`./setupCmdLine.sh`

In WebLogic
`cd<WL_Home>/weblogic81/server/bin`
`./setWLSEnv.sh`
 - b Run the “`Java -version`” command to ensure that you are using the appropriate JDK.
 - c Ensure that the `OVSISKeyStoreUtility` files are copied to the server so they can be accessed.
- 2 Create the security framework key in keystore without a key password.
 - a Execute:
`./genkey.sh`

This message displays:

This utility creates one AES secret key in a JCEKS keystore.

- b Enter the full path of the store, including the store file name:
/opt/<SI_Install_Dir>/weblogic/keystore/40ksklp
- c Enter the old keystore password:

- d Enter the key alias:
410sfkey
- e Press **Enter**.
- f Press **Enter** again.
- g Select a key size from the list:
1:128
2:192
3:256

Select an option: **3**

These messages display:

```
Engine provider: SunJCE
Starting to verify the generated key.
Verified the generated key.
Finished!
```

- 3 Update the old bootstrap properties file by adding the four new lines in bold at the bottom of this file. The items in red will vary depending on your key alias names used in your bootstrap keystore.

```
si.keystore.filepath=/opt/si4.0/weblogic/keystore/40ksklp
si.keystore.storepass=WoYknWKtXCHDyZf3l4xjh7qw2lZjaZ+i64LPCAahxjp9rjX
0ArNLdGv0qKR6PHrYPAsMp9Z6YUjhfUvSYyyk9/A9r80qhfjiz9XCF/
GcJ7cPFR9Gtoz6bVdcIXMxg2zLZiaRw43GFUAKlqv13bfeXA6H88W5GWzsm0kIzZDFEck
\=
si.keystore.keypass=OoOZwWSbM9PX/
wPGmGvlyIWAVvqjibW6WK+STCZmM5ddAXsqQcZHbwGCSeUD9g5opzjq2mTXoawu/
SgIimQMRDtGr1fZaWJ42ZkZR86KkHRF8YNxLcLvaE/NXIKknonu5f/
npw8KSK25WB5qu2y6RGqwrG1WavnsEL2rmViO0gk\=
si.keystore.alias=40key
si.keystore.40key.keyalg=PBEwithMD5AndTripleDES
si.keystore.storetype=JCEKS
si.keystore.keypass.alias=410sfkey
si.keystore.410sfkey.keyalg=AES/ECB/PKCS5Padding
```

Adding Keys to the Bootstrap Keystore for Key Rotation

The database, security framework, and SPML data encryption keys are identified in the bootstrap keystore when you set up Select Identity. When you implement the key rotation feature in Select Identity, the keys are rotated in the bootstrap keystore.

To rotate keys, open the bootstrap keystore file with the *genkey* tool.

Refer to the procedure [Setting Up the Bootstrap Keystore on a New Installation or an Installation with Default Keystores](#) on page 161, and add the keys beginning with the steps that describe how to add keys (step 2 and 3). When you have finished adding keys to the bootstrap keystore, save and close the file.

▶ You are *not* creating a bootstrap keystore again, but opening the bootstrap keystore and adding more keys to it.

To rotate only one key, add only one more key to the bootstrap keystore. To rotate all keys, you will add three keys as follows. The database encryption key and the security framework key are created with the *genkey* tool.

- **Database encryption key** - a secret key
- **Security framework key** - a secret key that must use the keystore password
- **SPML data encryption key** - a key pair

▶ The SPML data encryption key requires a key pair, which cannot be created using the *genkey* tool. Use the JDK *keytool* to create the SPML data encryption key pair and specify **RSA** as the algorithm when creating the key pair.

When you finish adding keys to the bootstrap keystore, go to Select Identity and schedule the key rotation tasks. For more information, refer to the *HP Select Identity Administration Online Help*.

Keystores and Key Pairs for Mutual Authentication and Secure Object Migration

Mutual authentication and secure object migration are optional features in Select Identity. You may opt to implement one or both of them. When implemented, the application server and clients are configured and set up with the appropriate initialized keystores and truststores.

A keystore file is a database of keys that contains both public keys and private keys. Public keys are stored as signer certificates, and private keys are stored in the personal certificates. The keys are used for authentication and data integrity. Private keys in a keystore have a certificate chain associated with them, which authenticates the corresponding public key. A keystore also contains certificates from trusted entities.

The keystore must contain a key pair with a (trusted) certificate signed by a trusted Certification Authority (CA). Trusted certificates are those from the entities you trust. Trusted certificates are also used to validate other certificates. A private key certificate is a public key certificate with its corresponding private keys.

Select Identity supports both one-way secure socket layer (SSL) authentication in which only the server is authenticated and two-way (mutual) SSL authentication in which both the server and client are authenticated.

When you implement secure object migration and/or mutual authentication in Select Identity, in addition to the bootstrap keystore, you must set up the following keystores and truststores:

- A keystore which contains:
 - The mutual authentication key pair
 - The two object migration key pairs: one for signing and one for encryption
- The truststore which contains:
 - Trusted source and destination certificates for secure object migration

- Trusted certificates for mutual authentication



Select Identity mutual authentication requires a single key pair. Object migration requires two key pairs, as explained above. Therefore, if you are implementing both features, you will need a single keystore with three key pairs and a single truststore with the required trusted certificates for both, secure object migration and mutual authentication. Both features use the same keystore and truststore.

The following sections explain how to set up the keystores, truststores, and properties files for mutual authentication and secure object migration.

Creating the Mutual Authentication Key

This keystore is used to store the mutual authentication key pair. You register this keystore in Select Identity using the Security Set Up feature. For more information, refer to the *HP Select Identity Administration Online Help*.

To create a mutual authentication keystore for use in Select Identity 4.20, perform the following steps:

- 1 Run the keytool utility to create a keystore and a key pair.



When you create a key pair, a keystore is automatically created during this process.

- 2 Generate a certificate request file, as shown in this command line example which creates an X.509 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 Send the new request file to your certificate authority for digital signing.
- 4 Import the signed certificate back to the keystore from which you generated the certificate request. The following command line example 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 signed certificate to the appropriate truststore. The following command line example imports the signed certificate file `./signed/signedCert.pem` to `ks/mytruststore` at the key alias named `myKeyAlias`:

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

- 6 Select Identity uses java property files to identify keystores. Generate the property files for the keystore and/or truststore by executing either `genprop.sh` (Linux) or `genprop.bat` (Windows).

When prompted to specify the file type to generate, select the appropriate option:

- For keystores, select option **2:OVSI secure object migration keystore**
 - For truststores, select option **3:OVSI truststore**
- 7 (Optional) Register the keystore and/or truststore on the application server. For more information, refer to [Configuring WebSphere for Mutual Authentication](#) on page 78, and [Configuring WebLogic for Mutual Authentication](#) on page 149.


- 8 Register the keystore and/or truststore property files in Select Identity. For more information refer to the *HP Select Identity Administration Online Help*.

Creating the Object Migration Keys

Select Identity object migration requires two key pairs: one for signing and one for encryption. The key pairs are stored in the object migration keystore. You register this keystore in Select Identity using the Security Set Up feature. For more information, refer to the *HP Select Identity Administration Online Help*.

To create the object migration keystore in Select Identity 4.20, perform the following steps:

- 1 Run the keytool utility to create a keystore **if not already created**, and two key pairs.

 If you have previously created the keystore and key pair for the mutual authentication feature, then the keystore is already created and you must specify the same keystore name in the commands below.

- 2 Generate a certificate request file, as shown in this command line example which creates an X.509 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 Send the new request file to your certificate authority for digital signing.
- 4 Import the signed certificate back to the keystore from which you generated the certificate request. The following command line example 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 signed certificate to the appropriate truststore. The following command line example imports the signed certificate file `./signed/signedCert.pem` to `ks/mytruststore` at the key alias named `myKeyAlias`:

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

- 6 Select Identity uses java property files to identify keystores. Generate the property files for the keystore and/or truststore by executing either `genprop.sh` (Linux) or `genprop.bat` (Windows).

When prompted to specify the file type to generate, select the appropriate option:

- For keystores, select option **2:OVSI secure object migration keystore**
- For truststores, select option **3:OVSI truststore**

- 7 (Optional) Register the keystore and/or truststore on the application server. For more information, refer to [Configuring WebSphere for Mutual Authentication](#) on page 78, and [Configuring WebLogic for Mutual Authentication](#) on page 149.
- 8 Register the keystore and/or truststore property files in Select Identity. For more information refer to the *HP Select Identity Administration Online Help*.

Creating the Truststore

Truststores are used to hold certificates to verify signatures, and to hold the destination encryption keys. Follow these steps to create the truststore or to verify identity:

- 1 Run `keytool` to create a JKS keystore.
- 2 Import the trusted certificates created in the previous procedures for mutual authentication and object migration.
- 3 Generate the property file for the truststore by executing either `genprop.sh` (Linux) or `genprop.bat` (Windows). When prompted to specify the file type to generate, select option **3:OVSI truststore**.
- 4 Use the Select Identity browser interface to register the property file. For more information, refer to the *HP Select Identity System Administration Online Help*.

Setting TruAccess Properties for the Security Framework

After successful installation, you can add or modify the following entries in the `TruAccess.properties` file, as appropriate. Then restart the server or cluster so the settings will take effect.

This property must be set at the start up of Select Identity. It cannot be changed once Select Identity is started with a keystore.

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

For **Linux or 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
si.rsa.algorithm=RSA/ECB/PKCS1Padding
```

If using **SPML** when testing key rotation on HSM setup, add the following property:

```
com.hp.ovsi.external.keypair.provider.classname=com.ncipher.provider.km.nCipherKM
```

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.

- If you are configuring Select Identity and its online help for use over HTTPS, set the following TruAccess property as shown below:

```
truaccess.method=https
```

- 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 74, and [Appendix B, WebLogic Logging Options](#) for more information about configuring the `logging.properties` file.



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, such as 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
```

Follow these steps to configure the **TAUser** table with extra columns for the extended search attributes:

- 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 [Chapter 3, Database Server Configuration](#). You can copy it from the Select Identity 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 173](#).

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

Figure 161 User Interface Sections



Customization Properties

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

[com.hp.ovsi.ui.masthead.fgcolor](#)

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

[com.hp.ovsi.ui.masthead.bgcolor](#)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This property will set the background color of Section F.

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

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

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

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

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

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

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

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

Default Values for User Interface Properties

Default values for these properties are as set below.

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

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

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

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

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

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

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

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

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

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

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

```
com.hp.ovsi.ui.landing.requests.image.src=/images/
```



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

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

Internationalization and Localization

Select Identity is internationalized and is able to operate with languages that are supported by the Java Unicode (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 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 6.1.x and WebLogic 9.2
- Database – Oracle 10G
- MS SQL 2005
- Connectors – LDAP/UTF-8



Make sure that your database supports the language characters.

Translation Customization

The localized languages available from HP are subject to change. Contact your HP representative or HP Partner for the current list or to find out about other localization options from HP. Select Identity has localizable files making it potentially feasible for a third party to perform additional localizations. However, please note that this is subject to a number of stipulations:

- Customers should not expect HP to provide additional detailed documentation on how to translate the product, other than providing the location of the localizable files.
- Customers should not expect all of the strings found in the localizable files to be used by the software. That is, some of the strings in the localizable files may never appear within the software's graphical user interface.

- Customers should not expect all of the localizable strings to exist in the localizable files. That is, some of the strings may not be translatable.
- Customers should be aware of the fact that the product will not necessarily support previous translations. That is, when a new version of Select Identity is released, the translations from prior versions may not be complete and may not even be of use. If a third party is used to translate Select Identity, it is recommended that the translations include ongoing support for updates as the Select Identity product is being updated.
- A call to HP Support may require the problem to be duplicated first by using the English version of the product or one of the officially supported localized versions of the product.

Localizing the Date and Time Format

In Select Identity, 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

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 uses a clickable calendar for selecting dates, as did previous versions of Select Identity. However, 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 select either a 12 or 24-hour clock for time display and entry. The default date and time formats can be overridden 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.

Setting the Calendar Language

- 1 In Internet Explorer, select **Tools** → **Internet Options**.
- 2 On the General tab, open the Languages preference page by clicking **Languages**.
- 3 Click **Add** to open the Add Languages page.
- 4 Select the language(s) you prefer and click **OK** to open the Language Preferences page with the selected languages listed.
- 5 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 will substitute the next language in the list, and so on.
 -  This setting affects all pages displayed in Internet Explorer, not just Select Identity.
- 6 Click **OK** to close the Language Preferences page, and again to close the Internet Options.

Setting the Date and Time Default Format in the TruAccess Properties File

The system administrator can configure the default format of dates and times within Select Identity. The `TruAccess.properties` file establishes several settings that 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 like this:

- 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.

Setting the Semantics in Oracle

By default, Oracle sets the length semantics to **byte**. The semantics must be set to **char** for Unicode encoding. Follow these steps to set the semantics to **char**:

- 1 In the SQLPlus window, enter this command:

```
ALTER SYSTEM SET NLS_LENGTH_SEMANTICS=CHAR SCOPE=BOTH
```

- 2 You must stop and restart the database instance for the new semantic settings to take effect.



Only the database schemas created after you perform step 2 will be affected by the new semantic settings.

Using MS SQL Scripts for i18n

Use these scripts to enable Unicode encoding in MS SQL:

| Use this MS SQL script | to... |
|--------------------------------------|--|
| <code>mssql_ovsi_i18n_ddl.sql</code> | create tables with Unicode data types. |
| <code>mssql_concero_dml.sql</code> | initialize created tables. |

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 Work Managers

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 work managers for processing HTTP, SOAP, and EJB requests. These work managers are defined here:

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

The **Fair Share** and **Capacity Constraint** settings can be used on these work managers to control CPU usage by front-end and background tasks:

- The **Capacity Constraint** for `hp.ovsi.SOAP` queue should not exceed three (10), to avoid high memory consumption during Web service calls. On servers that will not handle Web service requests, this work manager can be removed to avoid having idle threads dedicated to it.

Tuning the Database Server

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

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

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

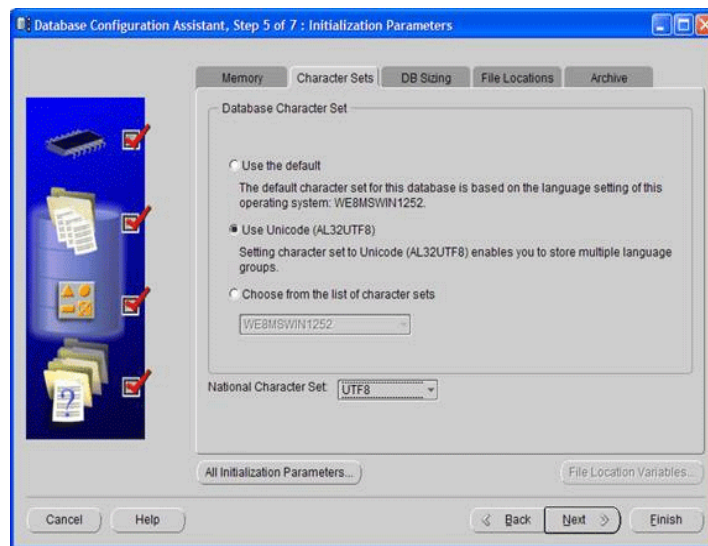
Increasing the number of nodes in the cluster also increases the number of concurrent sessions from Select Identity instances to the database server. The limit of concurrent sessions in the database server should be increased accordingly.

UTF-8 Encoding on Oracle 10g

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

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

Figure 162 Select Use Unicode

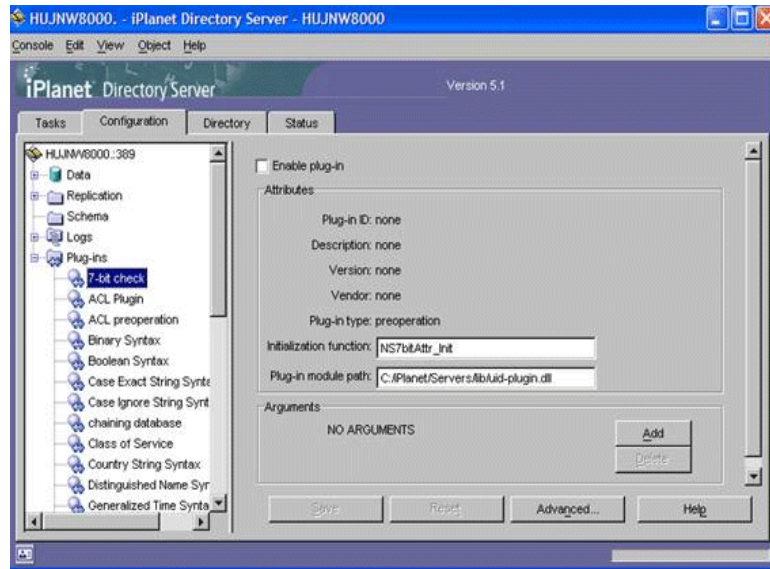


iPlanet LDAP Configuration

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.

Figure 163 Uncheck Enable Plug-in



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 to display the Login page. 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.

When using a third party single signon product, Select Identity must be told not to authenticate users a second time. This is done by setting

```
truaccess.authentication=off.
```

- **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 to display the **Time** field. The default displays. 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 to display. 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 display and in which order on 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=50
```

Configuring Java 2 Security for Select Identity on WebSphere

The following sections discuss post-configuration steps for enabling Java 2 security for Select Identity running on WebSphere.

In order to enable Java 2 security, you must have performed the pre-installation steps discussed in [Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security](#) on page 33.

For more information on Java 2 Security and WebSphere, refer to the WebSphere product documentation, **WAS 6.1 Java 2 Security** (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.doc/info/aes/ae/csec_rsecmgr2.html)

Deploying the SI Application

In order to enable Java 2 security on your WebSphere application server, you must perform this series of steps *each time you deploy* the Select Identity application. This process assigns the RunAs roles of Monitor and SIAdministrator to the siadministrator user.

- 1 Within Select Identity, select the **Manage Application** link before any changes are saved prior to a deployment.
- 2 Select **Applications** → **Enterprise Application** → **Select Identity** → **User RunAs Roles**.
- 3 Select the checkboxes for the following two roles: **SIAdministrator** and **Monitor**.
- 4 In the **Username** field, enter siadministrator.
- 5 In the **Password** field, enter the Select Identity administrator's password you created in [Pre-Installation Steps to Configure WebSphere to Enable Java 2 Security](#) on page 33.
- 6 Click **OK**.
- 7 Click **Save**.

7 Upgrading Select Identity

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

This chapter is divided into 4 sections:

- [Pre-Migration Activities](#)
- [Database Migration](#)
- [Platform Migration](#)
- [Select Identity Upgrade Procedure](#)

Pre-Migration Activities

Read this Pre-Migration Activities section and complete any necessary tasks before beginning the upgrade process.

- ▶ Select Identity provides migration scripts with each release. If you are upgrading from a version prior to version 4.0, contact your HP technical support representative.

Upgrade Requirements for Select Identity

To upgrade Select Identity, your Web application server and Select Identity must meet the following requirements to use this procedure:


- Select Identity version 4.13 must be installed. This migration procedure is from version 4.13 to 4.20. If you have an earlier version, refer to [Appendix C, Upgrading the Select Identity Database \(up to Version 4.13\)](#), then return to this section.
- ▶ 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 you to upgrade the Web application server and Select Identity. Follow the instructions corresponding to your system environment.

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 using a web browser.
- 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 your version of Select Identity is earlier than 4.13. Refer to [Appendix C, Upgrading the Select Identity Database \(up to Version 4.13\)](#).
- 4 Log in to the Select Identity 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 Application 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 Shut down the Web application server process and any managed servers/node processes.
- 3 Log in to the Administrative server at the command line, using an appropriate user ID.
- 4 Back up the existing Select Identity directories and files.
- 5 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.
- 6 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 161 for information about modifying the `TruAccess.properties` file.
- 7 Back up your existing key files: bootstrap and object migration keystores and truststores. You will need to copy the old key files to the same path as the old installation.

Database Migration

This section contains the procedures for upgrading the Select Identity database server. Before beginning these upgrade procedures ensure that your application server is down.

Oracle Upgrade Procedures

Your upgrade may require you to install Oracle on a new server. If so, perform the steps below in [Importing Data into a New Oracle Server](#) prior to performing the [Upgrading the Oracle Database](#) steps.

Importing Data into a New Oracle Server

To transfer your old Oracle database to a new installation of Oracle, follow these steps:

- 1 On the current Select Identity Oracle database server, run:

```
exp <schema owner>/<schema owner password>
```

- 2 Install the new database server and create the Select Identity schema owner.

- 3 Move the dump file to the new database server and run:

```
imp <schema owner>/<schema owner password>
```

► For large databases, refer to the *Oracle DataPump* product documentation.

Upgrading the Oracle Database

To upgrade the Select Identity Oracle database, follow these steps:

- 1 Ensure that your database server is configured as documented in [Chapter 3, Database Server Configuration](#).
- 2 Change directories to the main directory for the upgrade files.
- 3 Log on to SQLPlus as the Select Identity schema owner.
- 4 Execute the following scripts located in `\SQLs\oracle\4.x\4.20` on the Select Identity database installation CD:

- `sqlplus <username>/<password>@<connect_identifier>`

At the SQL prompt, run:

- `spool upgrade.out`
- `@oracle_413_420_ddl.sql`
- `@oracle_413_420_dml.sql`
- `spool off`

- 5 Carefully check the `upgrade.out` file. If the log file contains an error, solve the problem, restore your Select Identity database, then run [step 4](#) again.
- 6 Back up your upgraded Select Identity database.

MS SQL Upgrade Procedures

We recommend that you install a new MS SQL Server 2005 database. If you do, then perform the steps below in [Importing Data into a New MS SQL Server 2005](#) prior to performing the [Upgrading the Select Identity MS SQL Server](#) steps.

Importing Data into a New MS SQL Server 2005

To transfer your old MS SQL database to MS SQL Server 2005, follow these steps:

- 1 To run Backup Database using the SQL Server Enterprise Manager on your current SQL Server, right-click **Database** and select **All Tasks** → **Backup Database**.
- 2 Move the dump file to your new MS SQL Server 2005 database server.

- 3 Install the new MS SQL server, create a new login, and grant “sysadmin” rights to your new login.
- 4 To run Restore Database from your SQL Server Management Studio, right-click on **Database** and select **Restore Database**.

Upgrading the Select Identity MS SQL Server

Perform these steps to upgrade the Select Identity MS SQL Server database:

- 1 Ensure that your database server is configured as documented in [Configuring an MS SQL Database Server](#) on page 27.
- 2 Log on to Database Engine Query as the Select Identity schema owner.
- 3 Change directories to the main directory for the upgrade files.
- 4 Execute the following scripts located in `\SQLs\mssql\V4.x\V4.20` on the Select Identity database installation CD:
 - `mssql_413_420_ddl.sql`
 - `mssql_413_420_dml.sql`
- 5 Carefully check for errors. If an error is found, solve the problem, restore your Select Identity database, then run [step 4](#) again.
- 6 Back up your upgraded Select Identity database.

Platform Migration

Select Identity 4.20 supports WebLogic 9.21 and Websphere 6.1.09.

When you install a new application server and run our installers, it will create a new version of Select Identity. The new version must use the migrated database and existing keystores and truststores. See below for more information on updating the TruAccess.properties file and using the existing keys, keystores, and truststores.

WebLogic Migration from 8.15/8.16 to 9.21 MP1

In preparation of installing Select Identity 4.20, install WebLogic 9.21. We do not recommend upgrading WebLogic.

WebSphere Migration from 6.012 to 6.10 Patch 9

In preparation of installing Select Identity 4.20, install WebSphere 6.10 Patch 9. We do not recommend upgrading WebSphere.

Select Identity Upgrade Procedure

To upgrade Select Identity, you must perform other tasks besides upgrading the appropriate databases. For those instructions, refer to [Appendix C, Upgrading the Select Identity Database \(up to Version 4.13\)](#), [Appendix E, Running the Migration Utility: 4.01–4.10](#), or [Appendix D, Running the Migration Utility: 3.3.1–4.01](#).

If you are upgrading from a Select Identity version older than 4.1, you must follow these steps:

- 1 Create or configure the Select Identity bootstrap keystore. For instructions, refer to [Setting Up the Bootstrap Keystore on a New Installation or an Installation with Default Keystores](#) on page 161.
- 2 Install the new release of Select Identity using the instructions in the Select Identity installation procedure for your Web application server. It is recommended that you use the installer procedure.
- 3 Add any custom settings that were in the old `TruAccess.properties` file to the new `TruAccess.properties` file.
 - Restore your old keystores, truststores, and property files. They will need to be placed in the same path as the old installation. If this is not possible, contact support for assistance to update your database to point to the correct paths. Ensure that the user running the application server can read these files.

8 Integrating Select Identity with Service Desk, Select Audit, and Service Center

This chapter describes integration and interoperation support between Select Identity and Service Desk, Select Audit, and Service Center.

Select Identity can be configured alongside Service Desk, Select Audit, and Service Center 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 Center Integration](#)

Select Identity – Service Desk Integration

This section provides information about how to integrate Select Identity 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 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 6:** Create one smart action.
- **Task 7:** Set the service pages to use the template that you created or updated in **Task 3**.

Task 1: Activating Custom Fields

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

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

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



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

Customizing a Number Field for the Request ID

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

- 1 In the left panel, navigate to **Data** and select **Custom Fields**.
- 2 In the right panel, double-click **Service Call** and select **Sc. Number 10** from the **Field** menu.
- 3 Change the field name to **Request ID**.
- 4 Select **1234567** as the **Display Format**.
- 5 Check the **Activate** box.
- 6 Click the radio button labeled **All Categories**, 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 **OVSF 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 164](#) and [Figure 165](#) 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 **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 to the right of **With**.
 - n Select the **Concatenate** function again.
 - o Click the icon to the right of **Value**.
 - p Enter &serviceCallId= in the **Fixed Value** field, then click **OK**.
 - q Click the icon to the right of **With**. Select **Attribute**, and click the icon at the right
 - r Enter **ID** into the field and click **OK**.

- s Click OK three more times, click **Add To List**, then Click **OK**.
- t In the Database Rule wizard, proceed through the remaining pages and save the rule.
- u Perform the same steps again for the **Forget Password** rule. For this rule, use the following value for the URL:

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

Figure 164 Forgotten Password Database Rule

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

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

Figure 165 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.

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

- 1 Open the Select Identity **Service Studio** menu and select **External Calls**.
- 2 Locate and select the **SDIntegrator** external call.
- 3 Click **Modify** to change the parameter values.
- 4 Make the following changes to the parameters below:
 - **URL:** The hostname or IP address of the Service Desk server (the port is not needed).



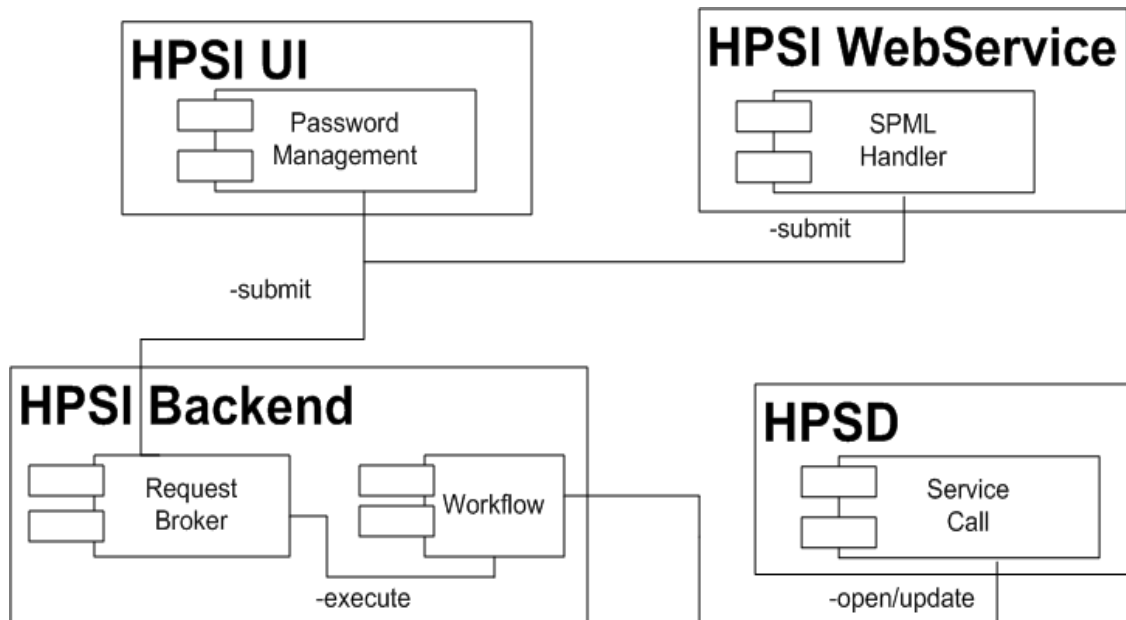
Service Desk will return the server hostname from its configuration in response to Select Identity's external call. Ensure this hostname can be resolved by the Select Identity server before Service Desk is called the first time. If the Select Identity server is unable to resolve this name, it cause the server to hang.

- **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 166](#) 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.

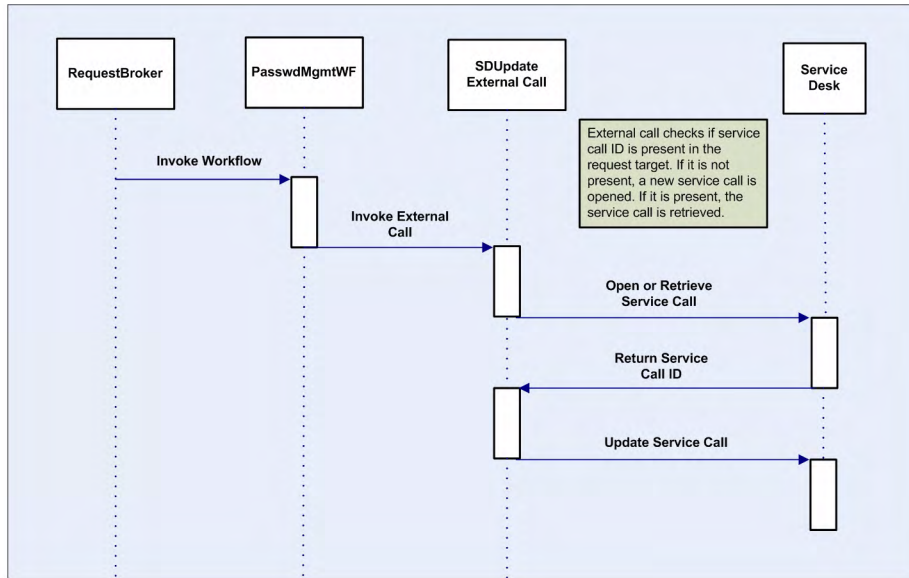
Figure 166 Select Identity-Service Desk integration context



Process Flow

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

Figure 167 Service Call process flow



Select Identity – Select Audit Integration

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

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

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

Requirements and Recommendations

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

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

Setting Up Integration in Select Identity

Select Identity configuration steps are minimal:

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

The Select Audit Agent

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

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

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

TruAccess Properties

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

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

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

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

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

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

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

Configuring the Select Identity Database

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

This operation can be performed in two ways:

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

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

Setting Up Integration in Select Audit

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

Integration can be set up in the following scenarios:

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



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

Data Filtering and Report Access Matrices

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

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

| Report Name | SI User | Non-SI User | SI Not Available | Administrators | Auditors |
|---------------------|---|-------------|------------------|--|--|
| Account Change | If allowed in SI on certain report types (see table below), will have these permissions on related reports: <ul style="list-style-type: none"> • Read, • Execute, • Schedule, • Adhoc | Denied | Denied | Full permissions including: <ul style="list-style-type: none"> • Read, • Write, • Delete, • Execute, • Schedule, • Adhoc, • View • Grant • Revoke | <ul style="list-style-type: none"> • 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:

| In order to see the following Select Audit report... | users must have <i>any</i> of the following 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 |

| In order to see the following Select Audit report... | users must have <i>any</i> of the following report types in Select Identity. |
|---|---|
| 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 |

| 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 | 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 |

| 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 | 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 |

| 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 | 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 |

| 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 | 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 |

| If you have this report type assigned in SI... | you will be able to see these events in Select Audit | | |
|--|--|----------------|-------------------------------------|
| | AUDITEVENTNAME | APPLICATION | COMPONENTEVENTNAME |
| 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 |

| If you have this report type assigned in SI... | you will be able to see these events in Select Audit | | |
|--|--|------------------|-------------------------------------|
| | AUDITEVENTNAME | APPLICATION | COMPONENTEVENTNAME |
| 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 |

| 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 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 |

| 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 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 |

| 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 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 |

| 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 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 |

| 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 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 |

| 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 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 |

| 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 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 |

| If you have this report type assigned in SI... | you will be able to see these events in Select Audit | | |
|--|--|----------------|---------------------|
| | AUDITEVENTNAME | APPLICATION | COMPONENTEVENTNAME |
| Admin Configuration | Workflow export | SelectIdentity | SI workflow export |
| Admin Configuration | Logging Config Change | SelectAccess | loggingConfigChange |
| Admin Configuration | Select Audit Report Config | SelectAudit | |

Select Identity – Service Center Integration

The integration of Select Identity with Service Center will allow users to manage and monitor Select Identity operations such as adding users, resetting passwords, and subscribing services through the Service Center. During the request workflow of the user management function, Select Identity will update the Service Center ticket based on the operation of the workflow.

The Select Identity - Service Center Integration is comprised of four main architectural components:

- The **Service Catalog** provides an interface for the end user to order Select Identity services.
- The **Change Management Customization** processes the service center request and collaborates with the Select Identity workflow.
- The **Web Services** handles the communication between Select Identity and Service Center.
- The Select Identity **Workflow** communicates with the Service Center in the business layer.

This section provides the customizations necessary for integrating Select Identity with Service Center. The following topics are covered:

- [Configuration File Customizations](#)
- [Script Library Customizations](#)
- [Script Customizations](#)
- [Table Customizations](#)
- [Change Management Customizations](#)
- [Select Identity Externalcall Customizations](#)
- [Test Case Operation Examples](#)

Configuration File Customizations

The `serverInfo.xml` configuration file stores the information necessary for generating the Select Identity URL and other information related to Select Identity Web services. You can modify the Select Identity server's URL so that it points to a different Select Identity server. The `serverInfo.xml` configuration file includes these tags:

- The `serverInfo` tag contains information about the Select Identity server. It can be configured to select a different Select Identity server.

```
<serverInfo>
<serverUrl>http://trulogica80.rsn.hp.com:9081/lmz</serverUrl>
</serverInfo>
```
- The `requestBy` tag is used for resetting a user's password in the Service Center Contacts table and for adding service requests. When performing either of these functions, you will enter the Select Identity related username. If this tag is *enabled=true*, then the Select Identity related username is stored in the contacts table. It is searched from there and if *enabled=false*, then the Select Identity related username is left blank and you can enter any Select Identity username.
- The `requestEvents` tag stores the Select Identity URL information regarding dedicated operations from the Service Center. It generates the corresponding `accessURL` based on the `phaseName`. It can also generate information that displays in the button of the Service Center **SIForm** tab and corresponds to the current change phase.

```
<requestEvents>
<requestEvent phaseName="SIDelAddUser"
accessUrl="/ovscintg/user/add.do" targetUser="false"/></requestEvents>
```

To configure the SC Provision Only workflow or any other customized workflow in the `TruAccess.properties` file, change the `truaccess.fixedtemplate.passwordreset` property to the following:

```
truaccess.fixedtemplate.passwordreset=SC\Provision\Only
```

Script Library Customizations

The `SISCIntegrationLib` includes methods for Service Center customization such as parsing the related `xml` file to string.

To customize a common java script in the `ScriptLibrary`, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Toolkit** → **Script Library**.
- 2 In the **Name** field, type `SISCIntegrationLib` and click **Add**.
- 3 Make your customizations and click **Save**.

Script Customizations

The `si.url.generator` script will read related configuration information from the `serverInfo.xml` file stored on the Service Center server. It will also parse the information into the related Select Identity URL in the current phase.

To create the `si.url.generator` script, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Utilities** → **Tools** → **Scripts**.

- 2 On the Script Panel Definition window, enter `si.url.generator` in the **Script Name** field.
- 3 On the Pre RAD Javascript tab, enter the javascript in the form and click **Add**.

Table Customizations

These three tables will require customization:

- contacts Table
- cm3r Table
- cm3t Table

contacts Table

On the contacts table you will need to add the `si.loginname` field. To add this field, follow these steps:

- 1 In Service Center, navigate to **System Definition** → **Tables** → **contacts**.
- 2 On the Overview of the contacts table, click the **Add, delete, or edit fields and keys** link.
- 3 On the Fields and keys definitions for the contacts table, click **New field**.
- 4 In the Create field popup window, enter `si.loginname` as the field name and click **OK**.
- 5 Click **Save**.

The `si.loginname` field is customizable and can be modified in the configuration file.

cm3r Table

On the cm3r table you will need to add one new field, `SIRequestId`, in the Web Services API. To add the new field, follow these steps:

- 1 In Service Center, navigate to **System Definition** → **Tables** → **cm3r**.
- 2 On the Overview of the cm3r table, click the **Add, delete, or edit fields and keys** link.
- 3 On the Field and keys definitions for the cm3r table window, click **New field**.
- 4 In the Create field popup window, enter `si.inst.request.id` as the field name and click **OK**.
- 5 In the **Field name in API** box, enter `SIRequestId` and click **Save**.

cm3t Table

On the cm3t table you will need to add one new field, `SIRequestId`, in the Web Services API. To add the new field, follow these steps:

- 1 In Service Center, navigate to **System Definition** → **Tables** → **cm3t**.
- 2 On the Overview of the cm3t table, click the **Add, delete, or edit fields and keys** link.
- 3 On the Field and keys definitions for the cm3r table window, click **New field**.
- 4 In the Create field popup window, enter `si.inst.activity.id` and click **OK**.
- 5 In the **Field name in API box**, `SIInstActivityId` and click **Save**.

You will also need to define the Web Services API values for five other fields.

1 To do this, begin by navigating in Service Center to **System Definition** → **Tables** → **cm3t** →

| Then navigate to... | and... |
|---------------------|---|
| a parent.category | In the Web Services API properties section, click the Include in API box to select it. |
| b parent.change | |
| c work.end | |
| d work.notes | |
| e work.start | |

2 Click **Save**.

Form Customizations

You will need to create these two new forms and add a new notebook tab called **SIForm** in the `cm3r.si.process.g` form:

- `cm3r.si.process` based on `cm3r.HW.server`
- `cm3r.si.process.g` based on `cm3r.HW.server.g`

To create the new forms based on the old ones, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Toolkit** → **Forms Designer**.
- 2 On the Forms Designer window, enter `cm3r.HW` (the name of the form you want to base your first new form on) in the **Form** box and click **Search**.
- 3 Click `cm3r.HW.server` to select it. Then click the little black triangular-shaped option button located on the top right side of this window and click **Copy/Rename**.
- 4 On the Copy/Rename a Format window, enter `cm3r.si.process` (the first new form) in the **New Name** box and click **OK**.
- 5 Click `cm3r.HW.server.g` to select it. This is the form you want to base your second new form on.
- 6 Click the black triangular-shaped option button and click **Copy/Rename**.
- 7 On the Copy/Rename a Format window, enter `cm3r.si.process.g` (the second new form) in the **New Name** box and click **OK**.

To add a new notebook tab called **SIForm** in the `cm3r.si.process.g`, form follow these steps:

- 1 On the Forms Designer window, enter `cm3r.si.process.g` in the **Form** box and click **Search**.
- 2 Click the **Design** button.
- 3 Click the **Notebook Tab** button.
- 4 Click the **page ####** tab.
- 5 In the Notebook Tab Properties section, enter **SIForm** in the **Caption** field. Notice the tab name has changed from **page ####** to **SIForm**.
- 6 Click the **HTML Editor** button and drag it to the body of the **SIForm** tab. To configure the HTML viewer component's properties section:

- a In the **Input** field, enter `$$sihtmlcode`
 - b In the **Visible Condition** field, enter `[current.phase]?"SIDelAddUser", "SIDelAddService", "SIDelResetPWD":1,1,1,0`
 - c Uncheck the **Visible** checkbox.
- 7 Click **OK**.

Change Management Customizations

There are two types of change customizations that are required:

- Change Category
- Change Phase

Change Category Customizations

You will need to add the following change category customizations.

- Users will create changes with three related change categories to invoke corresponding operations from Service Center to Select Identity:
 - SI-DelAddUserFromSC
 - SI-DelResetPWDFromSC
 - SI-DelAddServiceFromSC
- Operations in Select Identity can invoke Service Center to log a change incident and then close it when the operation is finished. So one change category for all operations from Select Identity to Service Center is needed.
 - SI-GeneralFromSI

To add the new change categories, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Services** → **Change Management** → **Changes** → **Change Categories**.
- 2 In the **Category Name** box, enter `SI-DelAddUserFromSC`.
- 3 In the Change Phases section, enter these change phases (1 per line):
 - **PreApproval**
 - **SIDelAddUser**
 - **PostApproval**
- 4 Click **Add**.
- 5 Repeat these steps for each related change category.

Change Phase Customizations

You will need to add the following change phase customizations.

- Three related change phases for corresponding operations from Service Center to Select Identity:
 - SIDelAddUser
 - SIDelResetPWD

- SIDelAddService
- One change phase for all operations from Select Identity to Service Center:
 - SIGeneralProcess
- Two other change phases for all approval related operations:
 - PreApproval
 - PostApproval

All of the related change phases must be associated with the `cm3r.si.process` form. The phases in the four change categories all use the `si.url.generator` script to generate the corresponding URL information. The `SIGeneralProcess` phase is used for the `SI-GeneralFromSI` category. The `PreApproval` and `PostApproval` phases are defined for all Select Identity related categories and can be further customized.

The following table outlines the phase information for each change category.

| Change Category | First Phase | Second Phase | Third Phase |
|------------------------|------------------|-----------------|--------------|
| SI-DelAddUserFromSC | PreApproval | SIDelAddUser | PostApproval |
| SI-DelResetPWDFromSC | PreApproval | SIDelResetPWD | PostApproval |
| SI-DelAddServiceFromSC | PreApproval | SIDelAddService | PostApproval |
| SI-GeneralFromSI | SIGeneralProcess | PostApproval | |

To add the new change phases, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Services** → **Change Management** → **Changes** → **Change Phases**.
- 2 In the **Change Phase** box, enter `SIDelAddUser`.
- 3 Click the **Alerts/Open & Close Behavior** tab.
- 4 In the Close Behavior section, click **Close - open next phase or exit on last phase (no cancel)**.
- 5 Click the **Model/Tasks** tab.
- 6 In the When last task is closed section, click **Close this phase**.
- 7 Click the **Scripts/Views** tab.
- 8 In the **Update** box, enter `si.url.generator` and click **Add**.
- 9 Repeat these steps for the `SIDelResetPWD` and `SIDelAddService` change phases.

To add the approval phases for the change categories, follow these steps:

- 1 In the **Change Phase** box, enter `PreApproval`.
- 2 Click the **Script/Views** tab.
- 3 In the Views section, enter `cm3r.si.process` in the **Default** box and click **Add**.
- 4 In the **Change Phase** box, enter `PostApproval`.
- 5 Click the **Approval/Review** tab.
- 6 In the Approvals section, enter `SecApproval`.
- 7 Click the **Scripts/Views** tab.
- 8 In the Views section, enter `cm3r.si.process` in the **Default** box and click **Add**.

To add the `SIGeneralProcess` change phase, follow these steps:

- 1 In the **Change Phase** box, enter **SIGeneralProcess**.
- 2 Click the **Model/Tasks** tab.
- 3 In the When last task is closed section, click **Close this phase**.
- 4 Click the **Scripts/Views** tab.
- 5 In the Views section, enter **cm3r.si.process** in the **Default** box and click **Add**.

Task Related Customizations

You will need to add the following task related customizations.

- One task category for corresponding operations:
 - `SIRequest`
- One task phase for the `SIRequest` task category:
 - `SIWorkflow`
- Associate the `SIWorkflow` task phase with each of the following change phases:
 - `SIDelAddUser`
 - `SIDelResetPWD`
 - `SIDelAddService`
 - `SIGeneralProcess`

To add the change phases to the `SIWorkflow` task phase, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Services** → **Change Management** → **Tasks** → **Task Phases**.
- 2 On the Edit Phase Record tab, enter **SIWorkflow** in the **Task Phase** box and click **Add**.
- 3 On the Edit Category Record tab, enter **SIRequest** in the **Category Name** box.
- 4 Verify that **SIWorkflow** is highlighted in the **Task Phases** section.
- 5 Select **SIDelAddUser** from the **Available Change Phases** drop-down list and click **Add**.
- 6 Repeat these steps for each of the change phases.

Service Catalog Customizations

You will need to add the following service catalog customizations.

- Add one service catalog:
 - `SI Tasks`
- Create three service catalog items using Select Identity tasks as the parent catalog:
 - `Delegate Add User`
 - `Delegate Reset Password`
 - `Delegate Add Service`

To add the service catalog, follow these steps:

- 1 In Service Center, navigate to **Menu Navigation** → **Services** → **Service Catalog** → **Service Catalog**.

- 2 On the Search Item Definitions window, click the **Add New Category** link.
- 3 On the New Service Catalog Category Wizard window, enter **SI Tasks** in the **Category Name** box.
- 4 Enter the category description and click **Next**.
- 5 Select **Top Level** and click **Next**.
- 6 Select **Items and/or Bundles** and click **Next**.
- 7 A confirmation message displays, “*Service Catalog Category added.*” Click **OK**.

To create the three service catalog items using Select Identity tasks as the parent catalog, follow these steps:

- 1 On the Search Catalog Item Definitions window, click the **Add New Catalog Item** link.
- 2 On the New Service Catalog Item Wizard window, enter the name and description of the new Service Catalog Item and click **Next**.
- 3 In the **Connector** drop-down list, select **Open a Change**. This interface type will be used when the user selects the new item from the catalog.
- 4 From the **In Category** drop-down list, select **SI Tasks** and click **Next**. The new item will belong to this category.
- 5 In the **Change Type** drop-down list, select **SI-DelAddServiceFromSC** and click **Next**. This is the type of change request the item will create.
- 6 Click **Finish**.
- 7 Repeat these steps for each of the three change types.

Select Identity Externalcall Customizations

The Externalcall parameter will create a new Service Center ticket and send all target information and the Request Id to the ticket. It will also create a Service Center task for each subtask of Select Identity. The Externalcall parameter informs the Service Center workflow when the Select Identity workflow is finished or has encountered an error. It also updates the work notes of the Service Center task in each block of the Select Identity workflow.

You will need to set the following four Externalcall parameters to **SCIntegrator**:

- URL - The Service Center Web service, such as `http://servicecenterhost:12670/sc61server/ws`. You can modify the URL to point to a different Service Center server. If you modify it, be sure to include the new changes in the `SISCmapping.xml` file.
- SC_ADMIN - The Service Center admin username. You can change it to a different Service Center admin username.
- SC_PASSWORD - The Service Center admin’s password. You can reset it to a different password.
- MAPPING_PATH - The path of the mapping file. You can change it to the location of your `SISCmapping.xml` file. The `SISCmapping.xml` file is the only file that can be customized in Select Identity. If you change the Service Center Web service’s API, be sure to modify this file to include the new changes.

To set the Externalcall parameter, follow these steps:

- 1 In Select Identity, navigate to **Service Studio** → **External Calls**.
- 2 On the External Call List page, select **SCIntegrator** and click **Modify**.

- 3 On the SCIntegrator: Set Parameters page, click **Parameters** in the navigation pane.
- 4 Select one of the four `Externalcall` parameters.
- 5 Click **Apply**.
- 6 Repeat this procedure for each of the four `Externalcall` parameters.
- 7 Click **OK**.

To configure the `SISCmapping.xml` file, follow these steps:

- 1 Open the `SISCmapping.xml` file with WordPad.
- 2 Modify the `SISCmapping.xml` file as needed.

You can customize your workflow based on the SC Provision Only workflow but keep the existing activities such as add item to map, application invocation, log message, etc. For more information, refer to the *HP Select Identity Administration Online Help*.

Test Case Operation Examples

Two test case examples are shown below. The first, is an example of a request received from the Service Center. The second, is an example of a request received from Select Identity.

Example 1 - Request Received from the Service Center

- 1 In Service Center, navigate to **Menu Navigation** → **Services** → **Service Catalog** → **Order from Catalog**.
- 2 On the Service Catalog Entries tab, click the **SI Tasks** link.
- 3 Click in the **Delegate Add User** box to select it.
- 4 Click the **Add Selected Item** link.
- 5 In the Selected Items section, click the **View Cart/Checkout**.
- 6 Click the **Submit Request** link.
- 7 Enter the purpose and all other required information and click the **Submit** link. A confirmation message displays at the top of the window with the Interaction Number.
- 8 To approve the interaction:
 - a Navigate to **File** → **Connect** → **Connections** <sdapprover> and click **Connect**.
 - b Then navigate to **Connections** <sdapprover> → **Menu Navigation** → **Approval Inbox**.
 - c Click the **Interaction Record** that you want to approve.
 - d Click the **Approve all Selected** link. A change ticket will be created.
- 9 To view the newly created change ticket:
 - a In Service Center, navigate to **Menu Navigation** → **Services** → **Service Catalog** → **Search Request**.
 - b On the Basic Interaction Search tab, enter the **Interaction ID** and click **Search**. The detail for the selected interaction will display only if the status is **Open-Linked**.
 - c Click the **Related Records** tab and then click the **Changes** tab. The detail for the newly created related record will display only if the status is **Open-Linked**.
 - d On the Change Request window, click the **Workflow** tab. To view the current expanded workflow, click the “+” in the change phase.

- 10 To approve the change:
 - a In the workflow, click **SecApproval**.
 - b In the Currently Pending Approvals section, click on the **Group/Operator Name** to select it.
 - c Click **Override** → **Approve One**.
- 11 Click the black triangular-shaped option button and click **Refresh**.
- 12 Click the black triangular-shaped option button again and this time click **Next Phase**.
- 13 Click the **SIForm** tab.
- 14 To add a new user in Select Identity, click **Add User**.
- 15 In Select Identity, enter your username and password and click **Sign In**.
- 16 On the Add User: Select Services page, click **Next**.
- 17 On the Add User: Set Service Attributes page, enter your user name and click **Finish**. A confirmation message displays at the top of the User List page.
- 18 To view the status of your request, navigate to **Requests** → **User Request Status List**. Select the request and click **View Request Status** to view the corresponding Service Center change.
- 19 In the Service Center Client, click the black triangular-shaped option button and click **Refresh**.
- 20 Click the **SIForm** tab. When the workflow reaches the third change phase, the component in the SIForm tab will disappear.
- 21 Click the **Description** tab. The description you entered in the Purpose field when you submitted your order from the catalog will display here.
- 22 Click the **Tasks** tab and verify that the task is approved.
- 23 Click the **Description** tab. Detailed information about the task displays here, such as:


```

USER_ADD:C37:SCTest1
RequestEvent:USER_ADD
Requestor:sisa
RequestDate:2007-09-05 15:01:32
TargetUser:C37
ServiceName:SCTest1
SIRequestID:1819
SISubtaskID:1820
      
```
- 24 Click the **Work Notes** tab and notice “*End*” in the **Notes** column.

Example 2 - Request Received from Select Identity

- 1 In Select Identity, navigate to **User Management** → **Add User**.
- 2 On the Add User: Select Services page, click **Next**.
- 3 On the Add User: Set Service Attributes page, enter the user name and click **Finish**.
- 4 On the User Request Status List page, click the **Request ID** and click **View Request Status**.
- 5 In the Service Center Client, click the **Description** tab. Details about the related change displays here, i.e., **USER_ADD:C41:SCTest1**.
- 6 Click the **Tasks** tab and verify that the task is approved.
- 7 Click the **Description** tab. Detailed information about the task displays here, such as:

USER_ADD:C41:SCTest1
RequestEvent:USER_ADD
Requestor:sis
RequestDate:2007-09-05 15:10:12
TargetUser:C41
ServiceName:SCTest1
SIRequestID:1825
SISubtaskID:1826

- 8 Click the **Work Notes** tab and verify “*End*” in the **Notes** column.

9 Uninstalling Select Identity

This section covers the following topics:

- [Auto-Uninstalling Select Identity](#)
- [Manually Uninstalling Select Identity from IBM WebSphere](#)
- [Manually Uninstalling from the WebLogic Server](#)
- [Removing an Oracle 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 `<SI_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.

To use the uninstaller to remove Select Identity:

- 1 Run the `Uninstall Select Identity.exe` (on Windows) or `Uninstall Select Identity.bin` (on UNIX) to launch the wizard. These files reside in the Select Identity home directory on the 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 Select Identity from IBM WebSphere

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 232.
- 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
- Resource adapters—J2C activation specifications
- Resource adapters—J2C administered objects
- JAAS—J2C authentication data

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**.
- 4 Select the application that you just stopped, and click **Uninstall** to remove the application from the WebSphere server.

Manually Uninstalling from the WebLogic Server

The following sections describe how to manually remove Select Identity from a WebLogic server.

- [Deleting the EAR File](#)
- [Deleting the Connectors](#)
- [Deleting the Data Source](#)
- [Deleting the Messaging](#)
- [Deleting the Mail Session](#)

Deleting the EAR File

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

Complete the following steps:

- 1 Log in to the WebLogic Server Console.

- 2 Click **Deployments**
- 3 Select the Application to delete.
- 4 Click **Stop - Force Stop Now**.
- 5 Click **Lock & Edit**.
- 6 Click **Delete**.
- 7 When prompted to confirm the deletion, click **Yes**.
- 8 Click **Activate Changes**

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:

Complete the following steps:

- 1 Log in to the WebLogic Server Console.
- 2 Click **Deployments**
- 3 Select the Connector to delete.
- 4 Click **Stop - Force Stop Now**.
- 5 Click **Lock & Edit**.
- 6 Click **Delete**.
- 7 When prompted to confirm the deletion, click **Yes**.
- 8 Click **Activate Changes**

Deleting the Data Source

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

Complete the following steps:

- 1 Log in to the WebLogic Server Console.
- 2 In the left panel, expand **Open Services** and select **JDBC →Data Sources**.
- 3 Click **Lock & Edit**.
- 4 Select **SI_Data_Source**.
- 5 Click **Delete**.
- 6 When prompted to confirm the deletion, click **Yes**.
- 7 Click **Activate Changes**

Deleting the Messaging

Perform the following steps to delete the Select Identity messaging:

Complete the following steps:

- 1 Log in to the WebLogic Server Console.
- 2 In the left panel, expand **Open Services** and select **Messaging →JMS Modules**.
- 3 Click **Lock & Edit**.
- 4 Select **OVSJ_Module**.
- 5 Click **Delete**.
- 6 When prompted to confirm the deletion, click **Yes**.
- 7 Click **Activate Changes**

Deleting the Mail Session

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

Complete the following steps:

- 1 Log in to the WebLogic Server Console.
- 2 In the left panel, expand **Open Services** and select **Mail Sessions**.
- 3 Click **Lock & Edit**.
- 4 Select **SI_Mail_Session**.
- 5 Click **Delete**.
- 6 When prompted to confirm the deletion, click **Yes**.
- 7 Click **Activate Changes**

Removing an Oracle Select Identity Database

This section describes how to remove 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.

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 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 property should not be edited.

For information about TruAccess properties that you use to customize the Select Identity user interface, see [Custom User Interface Properties](#) on page 174.

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 178.

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/truologica/truaccess/util/persistence/mssqlserver.hibernate.cfg.xml`**
Specifies the hibernate property file. *Leave this property commented.*
- **`truaccess.policy.id=1`**
Specifies the default Select Identity policy identifier.
- **`truaccess.expirationProcessPeriod=30`**
Specifies the time interval prior to automatic account expiration (in days). The default is 30days. At this point, a designated manager is sent a reminder notification.

- **truaccess.expire.administrator.userId=sis**
truaccess.expire.administrator.adminFunc=Concero Sys Admin
Specifies the default Select Identity system administrator user ID and administrative role.
- **contact_helpdesk=Please contact the helpdesk.**
Provides the text for an error message that displays if the user cannot log on to the Select Identity client.
- **com.hp.ovsi.help.web = http://support.hp.com**
The URL for 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 `TruAccess.properties` file, no user import will be scheduled.

Batch Processing Settings

- **truaccess.batch.inprogresstimeout=1800000**
 Specifies the time-out and owner for batch processing for the user 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.

Delegated Request Dependency Control

- **hp.si.delegated.request.nodependency=false**
Specifies that delegated request dependency is enabled.

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.reconciliation.postprovpolicy=1**
Specifies when Select Identity performs post-provisioning reconciliation. Specify one of the following values:
Perform SI Update if:
1 — if all provisioning activities were successful
2 — if the corresponding provisioning activity was successful
3 — always
- **si.recon.policybased=true (hidden, default to true)**
Policy Based Recon Switch
- **si.recon.server.num = X**
Hidden, default to 3, set > = 4 if the number of nodes in cluster is more than 3.
- **si.recon.processor.num = X**
Hidden, default set to 8.
- **truaccess.bulk.postprovpolicy=2**
Specifies when Select Identity performs post-provisioning after a bulk upload. Specify one of the following values:
Perform SI Update if:
1 — if all provisioning activities were successful
2 — if the corresponding provisioning activity was successful
3 — always
- **com.jp.ovsi.spml.resourcename.separator=+**
Select Identity reads data files from the `reconroot` directory. The file name should begin with an underscore (`_`). If the property above is set as shown, then the file placed on `reconroot` will begin with a “+.”
- **com.hp.si.req.term.waitperiod=100**
Sets the interval, in milliseconds, between periodic checks by Select Identity to determine if all requests associated with the task have been terminated. The default setting is 100.
- **com.hp.si.req.term.waitcount=6000**
Sets the number of times that Select Identity checks whether all requests associated with the task have been terminated. The default setting is 6000.
- **com.hp.si.recon.retry.limit=3**
Sets the number of times that a task is retried before the termination process is marked as failed. The default setting is 3.

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 172. 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 = 400**

Specifies the maximum number of records that can display in a limited search. The default setting is 400. Exceeding this number can result in significant system performance degradation.

The following searches impose the limit set by this property:

- Administrator Role search
- Approval Tasks search
- Attribute search
- Bulk Job search
- Bulk Task search
- Certificate search
- Configuration Request Status search
- Disabled User Popup search
- Email Popup search
- External Call search
- Reconciliation Job search
- Reconciliation Task search
- Request Status search
- Resource search
- Rule search
- Server search
- Service Attribute search
- Transfer Account search
- User Bulk List search
- User List search
- User Popup search

The following searches do not impose the limit set by this property.

- Export Configuration Approval Setup search
- Export Connector search
- Export Notification search
- Key Rotation Job search

- Service Assignment search
- User Attribute Constraint Value search
- User Discovery 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=sis
truaccess.system.expire_notification.administrator.userId=sis

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**



The `truaccess.singlevalue.attribute.delete` property is obsolete in release 4.20 and later.

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.needsssl=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.disable**
com.hp.ovsi.default.workflowtemplate.delegated.enable
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 WebLogic Logging Options

This section documents the configurable logging options for BEA WebLogic installations. For more detail about each option in Select Identity 4.20, refer to the `Logger` class in the Java 2, Standard Edition, v 1.5 API Specification.

Select Identity 4.20 implements `java.util.logging.Logger`, as defined by the Java 2, Standard Edition, v 1.5 API Specification.

During installation, the `logging.properties` file is copied from the Select Identity product CD to a subdirectory on 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 249](#), 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.



To prevent sensitive information from being logged, set the logging level for apache as **WARNING**. Ensure that the `logging.properties` file contains the following line: `org.apache.level=WARNING`

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

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

```
com.truologica.truaccess.util.scheduler.dao.BatchDAOImpl.level=FINE
```

```
com.truologica.truaccess.reconciliation.util.ReconciliationTimerTask.level=WARNING
```

```
com.truologica.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.truologica.truaccess.connector.ldap.ldapv3.LDAPConnector.level =
FINE
```


C Upgrading the Select Identity Database (up to Version 4.13)

Appendix C contains the procedures for upgrading the Select Identity Oracle database and the MS SQL 2000 database to version 4.13.

Running Oracle Migration Scripts

To upgrade the Select Identity Oracle database to version 4.13, perform the following steps:



Before you upgrade, back up the current database and the `TruAccess.properties` file.

The following table contains the scripts and migrators required to upgrade the Oracle database. The step number where you begin in this table depends on the version you are migrating from. The steps that proceed your beginning step must be run in the order displayed.

For example, if you are migrating from 3.02, you will start on step 3 and proceed to steps 4, 5, 6, etc., until you reach the end of the table.



When `ddl` and `dml` scripts are both present, always run the `ddl` script first.

| Step Number | Oracle Script |
|-------------|--------------------------------|
| 1 | oracle_301_302_ddl |
| 2 | oracle_301_302_dml |
| 3 | oracle_302_33_ddl |
| 4 | oracle_302_33_dml |
| 5 | oracle_33_331_ddl |
| 6 | oracle_33_331_dml |
| 7 | oracle_331_331patch1_ddl |
| 8 | oracle_331_331patch1_dml |
| 9 | oracle_331patch1_331patch3_ddl |
| 10 | oracle_331patch1_331patch3_dml |
| 11 | oracle_331patch3_331patch4_dml |
| 12 | oracle_331patch4_331patch5_ddl |

| Step Number | Oracle Script |
|-------------|---|
| 13 | Perform this step when you are upgrading from 331patch5. It contains a migration utility embedded in the <code>oracle_331Patch3plus_40_0.59.11</code> folder. Originally, it was packaged incorrectly in a <code>.gz</code> unzipped format. This mistake was corrected in release 4.10. You must unzip the file to read the <code>ReadMe.txt</code> . The procedures to run the migration utility are located in Appendix D, Running the Migration Utility: 3.3.1–4.01 . |
| 14 | Perform this step when you are upgrading from any version of 4.0X. It contains a migration utility embedded in the <code>SI-Migrator-0.59.36</code> folder. You must unzip the file script first. The procedures to run the migration utility are located in Appendix E, Running the Migration Utility: 4.01–4.10 . When the migration utility runs, these scripts will execute automatically (based on the version set on the <code>TruAccess.properties</code> file): <code>oracle_40CR_40CRP1_ddl</code> <code>oracle_40CRP1_40MR_ddl</code> <code>oracle_40CRP1_40MR_dml</code> <code>oracle_4.00_to_4.01_ddl</code> |
| 15 | <code>oracle_410_411_ddl</code> |
| 16 | <code>oracle_410_411_dml</code> |
| 17 | <code>oracle_411_411001_ddl</code> |
| 18 | <code>oracle_411_411001_dml</code> |

Running MS SQL Migration Scripts

To upgrade the Select Identity MS SQL database to version 4.13, perform the following steps:



Before you upgrade, back up the current database and the `TruAccess.properties` file.

The following table contains the scripts and migrators required to upgrade your MS SQL database. The step number where you begin in this table will depend on the version you are migrating from. The steps that proceed your beginning step must be run in the order displayed.

For example, if you are migrating from 3.02, you will start on step 3 and proceed to steps 4, 5, 6, etc., until you reach the end of the table.



When `ddl` and `dml` scripts are both present, always run the `ddl` script first.

| Step Number | MS SQL Script |
|--------------------|---|
| 1 | mssql_301_302_ddl |
| 2 | mssql_301_302_dml |
| 3 | mssql_302_33_ddl |
| 4 | mssql_302_33_dml |
| 5 | mssql_33_331_ddl |
| 6 | mssql_33_331_dml |
| 7 | mssql_331_331patch1_ddl |
| 8 | mssql_331_331patch1_dml |
| 9 | mssql_331patch1_331patch3_ddl |
| 10 | mssql_331patch1_331patch3_dml |
| 11 | mssql_331patch3d_331patch3e_ddl |
| 12 | mssql_331patch3d_331patch3e_dml |
| 13 | <p>Perform this step when you are upgrading from 331patch5. It contains a migration utility embedded in the <code>mssql_331Patch3plus_40_0.59.11</code> folder. It was first packaged incorrectly in a <code>.gz</code> unzipped format. This mistake was corrected in release 4.10. You must unzip the file to read the <code>ReadMe.txt</code>. The procedures to run the migration utility are located in Appendix D, Running the Migration Utility: 3.3.1–4.01.</p> |
| 14 | <p>Perform this step when you are upgrading from any 4.x version. It contains another migration utility embedded in the <code>SI-Migrator-0.59.36</code> folder. You must unzip the file script first. The <code>mssql_4.00_to_4.01_ddl</code> script will automatically execute when the migration utility is run. The procedures to run the migration utility are located in Appendix E, Running the Migration Utility: 4.01–4.10.</p> |
| 15 | mssql_410_411_ddl |
| 16 | mssql_410_411_dml |
| 17 | mssql_411_411001_ddl |
| 18 | mssql_411_411001_dml |

D Running the Migration Utility: 3.3.1–4.01

Appendix D contains procedures for upgrading the database from version 3.3.1 to 4.01. To upgrade from later versions of Select Identity, refer to [Appendix E, Running the Migration Utility: 4.01–4.10](#) or [Appendix C, Upgrading the Select Identity Database \(up to Version 4.13\)](#).

Updating the TruAccess Properties File

Make the following updates to the `TruAccess.properties` file to meet your specific migration needs:

| If | Then |
|---|--|
| The value for <code>fixedtemplate.bulk_default</code> is set to <code>ReconciliationDefaultProces</code> | Change it to either the SIBulkOneStageApproval or the SI Provisioning Only Bulk template. Continue. |
| The value for <code>fixedtemplate.bulk_default</code> is set to anything else | Continue |
| The value for <code>truaccess.fixedtemplate.bulk_move</code> is set to <code>ReconciliationDefaultProces</code> | Change it to either the SIBulkOneStageApproval or the SI Provisioning Only Bulk template. |
| The value for <code>truaccess.fixedtemplate.bulk_move</code> is set to anything else | Continue |
| If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was set to <code>SHA-1</code> | Continue |
| If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was set to <code>SHA-256</code> | Continue |
| If your previous <code>com.hp.ovsi.messagedigest.algorithm</code> was <i>not</i> set | Add <code>com.hp.ovsi.messagedigest.algorithm</code> to the <code>TruAccess.properties</code> file, with the value set to <code>SHA-1</code> . |

Preliminary Migration Steps

- 1 If you wish to reduce the amount of on-screen messages about migration progress, edit the `logging.properties` file to set the output level to `Warn`.
- 2 Unzip the migration files.
- 3 Edit the following environment variables in `oracle_run_migrate.sh`
 - `ORASERVER` — The IP address or domain name of the Oracle database server
 - `ORAPORT` — The database port the Oracle database listens on, usually 1521
 - `ORACLE_SID` — Connection identifier for the database where Select Identity is running
 - `ORAUUSER` — Username (schema name) that has the Select Identity data
 - `ORAPWD` — Password for the user (schema) that has the Select Identity data
- 4 Verify that the `J2EE_JAR` environment variable in `oracle_run_migrate.sh` is specifying a valid `J2EE.jar` file. If you are configured to run WebLogic, the default value will probably work. If you are not configured for WebLogic, change the `J2EE_JAR` environment variable to specify a valid file.
- 5 Edit the `java.util.logging.FileHandler.pattern` entry in the `logging.properties` file to point to a valid directory entry. This is where the java log files will be written.
- 6 Shut down the Select Identity application and disconnect any other users from the database. You may want to shut down the database listener by logging on as the oracle user and executing `lsnrctl stop`. This will prevent the initiation of any new remote database connections.
- 7 Make a backup of the database.

Running the Migration Script

To run the migration script:

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

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

The script will run through each step and display a message informing you as the steps complete. When all the steps have completed, the script will display an on-screen notification.

Running the Migration Utility in an Oracle RAC Configuration

This section contains information about running the migration utility for environments that are running in an Oracle RAC configuration. For the upgrade to complete successfully, the migration utility needs to connect to one specific node in the Oracle RAC. On the machine that will run the migration utility, ensure that there is an entry in the `tnsnames.ora` file that has the Oracle SID of the Oracle node you want to connect to directly as the identifier for the `tnsnames.ora` entry.

You need to use a `tnsnames.ora` entry that connects to just one node in the RAC.

For example, if a node in the RAC has an Oracle SID of `RACNODE1` and an IP of `192.168.100.123`, you could use an entry like this:

```
RACNODE1 =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP) (HOST = 192.168.100.123) (PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SID = RACNODE1)
)
)
```

In the `setUserEnv.sh` script, set the `ORACLE_SID=RACNODE1` and ensure the `DBSERVER=192.168.100.123` and `DBPORT=1521`. The `ORACLE_SID` value must be the actual Oracle SID for the Oracle node you are connecting to and the identifier for the `tnsnames.ora` file entry connecting to the node in the Oracle RAC.



Depending on the version of Select Identity, the names of the environment variables may differ. In versions 3.3.1 - 4.0, `DBSERVER = ORASERVER` and `DBPORT = ORAPORT`

To find the entry to connect with in `tnsnames.ora`, the portion of the upgrade using SQLPlus will connect using the `userid/password` and the `ORACLE_SID` value. For example, a SQLPlus connection is built like this:

```
sqlplus $DB_USER/$DB_PASS@$ORACLE_SID
```

The portion of the upgrade that connects using JDBC will construct the URL to connect to the database. For example, the JDBC URL is constructed like this:

```
-Djdbc.driverClassName=oracle.jdbc.OracleDriver
-Ddatabase.url=jdbc:oracle:thin:@$ DBSERVER:$DB_PORT:$ORACLE_SID
-Ddatabase.user.name=$DB_USER -Ddatabase.user.password=$DB_PASS
```

Troubleshooting

- If the database connection information is *not* set correctly in `oracle_run_migrate.sh`, the script will not fail after the first step. Instead, it will continue to try to run each step. This is caused by SQL Plus not returning an error code for this condition. Since neither SQL Plus nor the migration scripts can connect to the database, no harm is done. After you have fixed the incorrect connection information, you can run the script again.
- The migration script runs each step in numerical order. If a failure occurs during any step, the failure is logged and the migration is halted.
- If there is a failure, first review the entries in the `migrationlog` table under the Select Identity schema. Log on to SQL Plus as the Select Identity owner and run the `oracle_migration_report.sql` script. It will show the status of each step.
- If the failure occurs during one the Java migration steps, review the screen output or log files in the directory specified by the `java.util.logging.FileHandler.pattern` entry in `logging.properties`.
- After resolving the problem, reload the database from backup and restart from the beginning.

Post-Migration Steps

When the migration is complete, update the `truaccess.version` property in the `TruAccess.properties` file so that it contains the correct version. For example, `truaccess.version = 4.01`

E Running the Migration Utility: 4.01–4.10

Appendix E contains the procedures for upgrading Oracle and MS SQL 2000 databases from version 4.01 to 4.10. To upgrade from earlier versions, refer to [Appendix D, Running the Migration Utility: 3.3.1–4.01](#).

Oracle Database Upgrade Procedure

The `migrator.sh` upgrade script calls another script, `setUser.Env.sh`, which contains several environment variables. You can modify the values assigned to these variables to enable the script to run automatically without prompting for information during the upgrade process. If you choose not to set these variables within the subscript, then the upgrade script will prompt you to enter the information each time.

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

To upgrade the Oracle database, follow these steps:

- 1 Unzip the upgrade files.
- 2 Locate the file named `setUserEnv.sh` and edit the following environment 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.
- 3 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 it will log the behavior of the script. Failure to perform this step correctly may result in missing the on-screen status and log message display during parts of the upgrade process.

- 4 Change directories to the main directory for the upgrade files.
- 5 Execute the following command if you are upgrading a version of Select Identity prior to 4.10:

```
./migrator.sh
```

Running the Migration Utility in an Oracle RAC Configuration

This section contains information about running the migration utility for environments that are running in an Oracle RAC configuration. For the upgrade to complete successfully, the migration utility needs to connect to one specific node in the Oracle RAC. On the machine that will run the migration utility, ensure that there is an entry in the `tnsnames.ora` file that has the Oracle SID of the Oracle node you want to connect to directly as the identifier for the `tnsnames.ora` entry.

You need to use a `tnsnames.ora` entry that connects to just one node in the RAC.

For example, if a node in the RAC has an Oracle SID of `RACNODE1` and an IP of `192.168.100.123`, you could use an entry like this:

```
RACNODE1 =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP) (HOST = 192.168.100.123) (PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SID = RACNODE1)
)
)
```

In the `setUserEnv.sh` script, set the `ORACLE_SID=RACNODE1` and ensure the `DBSERVER=192.168.100.123` and `DBPORT=1521`. The `ORACLE_SID` value must be the actual Oracle SID for the Oracle node you are connecting to and the identifier for the `tnsnames.ora` file entry connecting to the node in the Oracle RAC.



Depending on the version of Select Identity, the names of the environment variables may differ. In versions 3.3.1 - 4.0, `DBSERVER = ORASERVER` and `DBPORT = ORAPORT`

To find the entry to connect with in `tnsnames.ora`, the portion of the upgrade using SQLPlus will connect using the `userid/password` and the `ORACLE_SID` value. For example, a SQLPlus connection is built like this:

```
sqlplus $DB_USER/$DB_PASS@$ORACLE_SID
```

The portion of the upgrade that connects using JDBC will construct the URL to connect to the database. For example, the JDBC URL is constructed like this:

```
-Djdbc.driverClassName=oracle.jdbc.OracleDriver
-Ddatabase.url=jdbc:oracle:thin:@$ DBSERVER:$DB_PORT:$ORACLE_SID
-Ddatabase.user.name=$DB_USER -Ddatabase.user.password=$DB_PASS
```

MS SQL Database Upgrade Procedure

To upgrade a Select Identity MS SQL database, perform the following steps:



Before you upgrade, back up the current database and `TruAccess.properties` file.

- 1 Navigate to the following URL and download the JTDS JDBC driver:

```
http://sourceforge.net/project/showfiles.php?group_id=33291
```

- 2 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 `jtids-1.2.jar` file downloaded in [step 1](#). It is critical that this be set correctly.

`DB_USER`: The user name for connecting to the MS SQL database and accessing the Select Identity schema. Typically, it's the same user name that was entered for the database connection when the old version of Select Identity was installed.

`DB_PASS`: The password for the above user account.

`DB_PORT`: The database server port on which the MS SQL database listens for connections, usually 1433.

`DBNAME`: The database name for the server where the Select Identity database is running.

- 3 Execute the following command if you are upgrading from a version earlier than 4.10:

```
./migrator.sh
```

- 4 Enter the hostname or IP address of the database server if prompted.

The default value is `localhost`.

- 5 When prompted, enter the database password.

Troubleshooting a Database Upgrade

Refer to the `readme.txt` 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 this release.



It is important that the scripts run properly. If they do not, your database will be incorrect.

The following steps may assist in tracing the problem and completing the upgrade successfully:

- 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.
- If there is a failure, first review the entries in the `migrationlog` table under the `Select Identity` schema. Log on to SQLplus as the `Select Identity` owner and run the `oracle_migration_report.sql` script. It will show the status of each step.
- If the failure occurs during one of the Java upgrade steps, review the screen output or log files in the directory specified by the `java.util.logging.FileHandler.pattern` entry in the `logging.properties` file.
- After resolving the problem, reload the database from backup and restart from the beginning.

Index

A

- Account Change Report, 204
- Account Events Report, 204
- activation specifications, 66
- Admin Configuration, 218
- administrator, 13
- Administrator Report, 204
- Admin Logged Out, 217
- Admin Login Error, 217
- AES encryption, 165
- agent
 - Select Audit, 201
- agent-based connectors, 17
- API, Service Desk, 192
- application
 - status, 232
 - undeploying, 232
- application settings, WebSphere, 70
- Architecture, 15
- ASCII and non-ASCII field length, 25
- audit and configuration reports, 203
- AuditCfgEntry table, 202
- audit data stream, 201
- auditing, 15
- Audit User Hint, 216
- Audit User Login, 216, 218
- Audit User Password, 216
- Authentication
 - 1-way secure socket layer (SSL), 168
 - 2-way (mutual) secure socket layer, 168
- authentication, 16
- Authority, tiered, 15

B

- browser version, 23
- Business Process Services, 15

C

- Calendar Language
 - Setting, 178
- calendar wizard, 178
- Caller field, 195
- category
 - service call, 194
- Certificate, 171
 - Personal, 168
 - Private key, 168
 - Public key, 168
 - Request file, 169, 170
 - Signer, 168
 - Trusted, 168
- Certification Authorities, 16
- Certification Authority, 168
- Change/Reset Password, 194
- Change History Report, 204
- Change Password, 215
- character sets, 25
- clustered servers
 - create JMS connection factory, 128, 129, 132, 133, 134, 135
- clusters
 - required for WebSphere, 38
- compliance auditing, 201
- concero_ddl.sql, 25, 27
- concero_dml.sql, 25, 27
- configuration reports, 201
- configure
 - JDBC connection pool, 141, 144
 - JMS settings, 128
 - JTA settings, 141
- configuring
 - logging, 249
 - recommended, 171
 - TruAccess.properties, 157, 235
 - TruAccess.properties required settings, 157

- connection factory
 - queue, 61, 62
- connectors, 16
- context, 201, 203
- Context Engine, 15
- context management, 15
- cookies, 23
- CORBA Naming Service Groups, 75, 76, 79, 81, 82, 84, 86, 91, 94, 95, 97, 99
- Customer Service Representative, 192
- custom external keystores, 37
- custom field, 194
- custom fields
 - Service Desk, 195

D

- database, 13, 201
 - and Select Audit, 202
 - user accounts, 32
- database access control, 15
- database rules
 - Service Desk, 196
- database rules, Service Desk, 193
- database server, 37
- database user login, 38
- data filtering, 203
- Date and Time Format
 - Custom, 178
 - Setting in TruAccess properties file, 179
- delegated password change, 192
- delegated request, 193
- delegation, 15
- Description field, 195
- Destination JNDI Name, 66
- Destination Type, 66
- directory naming, 32
- Display Format, 193
- dml file, 201
- documentation, 37
- domains
 - Select Identity and Select Audit, 201

E

- EAR file, 70

- Emailed report format, 183
- embedded spaces, 32
- encryption, 16
 - PC1, 17
 - SHA, 15
- encryption keys, 37
- Endpoints, 66
- entitlements, 15
- Error Changing Password, 215
- event history, 15
- Expire Password Notification, 215

F

- firewall ports, 24
- form,default, 195
- Forms, 15

G

- general settings, 157
- generic JVM Arguments, 73
- Genkey tool, 168
- genprop utility, 165, 169, 170, 171

H

- Hardware Security Module, 161
 - Non, 161
- Hardware Security Modules, 16
- high message threshold, 57
- Hint Setup, 216
- Host aliases, 32, 105
- HSM, 16
- HTTP, 13
- HTTPS, 172
- HTTP transport port, 105

I

- IBM HTTP Server, 32
- Information, 195
- install.bin, 38
- install_trace.log, 37
- InstallAnywhere installer, 38
- installation
 - logging, 37
 - remote, 38

- installation process summary, 19
- installer
 - Select Audit, 203
- installing:WebSphere installation wizard for standalone server, 38
- interface settings, 157
- internationalization, 17, 177
 - UTF-8 encoding on Oracle10G, 181
- interoperation, 201
- IP address, 38

- J**
- J2EE Connector Architecture, 16
- Java 2 security, 74
- Java Naming and Directory Interface, 16
- javascript, 23
- Java Unicode (UTF-8), 177
- JCA, 16
- JDBC connection pool, configure, 141, 144
- JDBC driver, 21
- JDBC port, 24
- JDBC Provider, 54, 55
- JMS
 - database user, 38
 - database user account, 32
 - queue, 61
 - resources, 60
 - topic, 61
- JMS cluster, 58
- JMS clustering, 38
- JMS connection factory
 - create for clustered servers, 128, 129, 132, 133, 134, 135
- JMSDB_LOGIN_USER, 58
- JMS settings
 - configure, 128
- JMS settings for clustered servers
 - set up JMS connection factory, 128, 129, 132, 133, 134, 135
- JMS user, 26
- JNDI, 16
- JNDI Name, 58, 60
- JTA settings
 - configure, 141
- JVM arguments, 73

- JVM heap size, 172
- JVM Logs, 74

K

Key

- Database, 161
- Database encryption, 168
- Pair, 163, 168
- Private, 168
- Public, 168
- Rotation, 167
- Security Framework, 162
- Security framework, 168
- SPML Data Encryption, 161
- SPML data encryption, 168

Keystore

- Adding keys to bootstrap for key rotation, 167
- Bootstrap, 161
- Configuration, 161
- Creating, 169, 170
- Default, 161
- File, 168
- Upgrading from earlier version, 166

- keystore, 168

- keystore parameter file, 38, 108

- keystore property file, 165

- keystores, 16

- keytool, 168, 171

- keytool utility, 169, 170

L

- language fonts, 182

- language media kit, 19

- LDAP, 16

- LDAPS, 16

- local_policy.jar, 37

- localization, 177

- localized version, 19

- log files, 249
 - tail, 37

- logging.properties
 - configuring, 148

- Logging Config Change, 219

- logging in
 - WebSphere, 105, 156

- logical identity, 13

- Login page, 182

M

- mail session, 67, 68
- managed service, 201
- Microsoft Internet Explorer, 23
- Microsoft SQL Server
 - Enterprise Manager, 27
- Migration Utility, 258, 262
- minimum requirements, 20
- MS SQL
 - Select Identity server database upgrade, 188
 - Server database upgrade, 187
 - Server upgrade, 187
- MS SQL scripts
 - Using for i18n, 179
- Mutual authentication, 168
- myStartWL script, 172

N

- nCipher, 165
- nCipher HSM, 165, 171
- Network Deployment Manager, 32
- Network File System, 38
 - installation directory, 37
- Number Field, 193

O

- Object migration
 - Secure, 168
- ojdbc14.jar, 37
- online help, 37
 - deployment, 70
- operating system login, 38
- operating system login ID, 38
- Oracle
 - Database upgrade, 187
 - internationalization encoding, 181
 - Running migration scripts, 253
 - Server upgrade, 187
 - Setting semantics, 179
 - uninstalling, 234
 - Upgrade procedures, 186
- Oracle 10g requirements, 21
- oracle_concero_ddl.sql, 26
- Oracle thin driver, 37
- Oracle thin driver archive, 38
- Oracle Thin Driver Version, 21

- OVSD-OVSI integration Template, 195
- OVSIAuditBroadcast, 60, 65
- OVSIAuditProcQ, 63, 66
- OVSIBulkQueue, 66
- OVSIBus, 61, 62, 64, 66
- OVSIBus
 - security setting, 75
- OVSICacheTopic, 60, 65
- OVSICChangeReconProcessorQueue, 63, 66
- OVSI DataSource, 54, 55
- OVSIEntCacheQueue, 66
- OVSI Mail Session, 69
- OVSIMessageAckQueue, 63, 66
- OVSI Oracle10g, 54, 56
- OVSI Password Management with OVSD, 199
- OVSIReconQueue, 63, 66
- OVSIResReconDispatcherQ, 66
- OVSIResReconQ, 63, 66
- OVSISaudQ, 63, 66
- OVSISchedulerQueue, 66
- OVSIServiceAssignQueue, 63, 66
- OVSITCF, 62
- OVS IUserImportPQueue, 66
- OVS IWfRequestExpireQueue, 66
- OVS IWorkflowQueue, 63, 66

P

- Parent field, 194
- Password, 215
- Password Management Report, 205
- password management request, 192
- Password Policy change, 215
- password request, link, 198
- Password Reset Config Change, 215
- policy files, 36
- ports
 - firewall, 24
- Post-Migration Steps, 260
- private key, 16
- privileges, 13
- processes
 - starting and stopping, 38
- profiles, 15

- protocol providers, mail, 67
- provisioning workflow, 15
- proxy server, 32
- public key, 16

Q

- qualifications for installing, 17
- queue connection factory, 61, 62

R

- Received Login request, 216
- Received Logout request, 216
- reconciliation, 15
- report access
 - Select Audit, 203
- reporting, 15
- report mapping, 204
- Request Failure Description, 195
- Request Failure Description field, 194
- Request ID, 195
- request ID, 193
- Request ID, 193
- request link, 196, 198
- Request Link,, 195
- Request Link field, 194
- request status, 193, 197
- Request Status Page, 193
- Request Status page, 193
- Request Type, 195
- Request Type field, 194
- Reset Password, 215
- Reset Password Service Call, 191
- resource connector, 17
- Resources, 15
- role, 203
- roles
 - service, 15

S

- Sc. Text 1 field, 194
- Sc. Text 2 field, 194
- schema, 13, 19
- schema, Select Identity, 27
- schema name, 58
- scope, 67
- SDIntegrator external call, 192, 198
- SDK, 16
- security, 15, 16
 - Java 2, 74
 - WebSphere console, 32
- Security Events Report, 205
- Security Framework, 37
 - Initialization, 160
 - TruAccess properties, 171
- security framework, 32, 76
- SelectAccess, 217
- Select Audit, 204, 219
 - data filtering, 203
 - viewing configuration reports, 201
- Select Audit connector,, 201
- Select Audit Report Config, 219
- SelectFederation, 217
- Select Identity
 - launching, 76
- Select Identity schema, 19
- Self-Registration, 183
- self-service request, 193
- Sent Login request, 216
- Sent Logout request, 216
- Ser. ShortText 1 field, 194
- sers, 15
- server settings, 157
- Service Call, 193
- service call, 191
- service call,category, 194
- service call, link, 198
- Service Call Category, 194
- Service Call Category field, 193
- service call status, 195
- service call template, 193
- Service Desk
 - database rules, 196
 - smart action, 193
- Service Desk integration
 - configuring in Select Identity, 198
- Service Desk Integration, context, 199
- Service Desk Integration, process flow, 199

- Service Level Agreements, 191
- Service Report, 205
- Service Roles, 15
- services, 15, 201
- SF Admin Logged Out, 217
- SHA, 15
- short string field, 194
- single sign-on, 183
- SLAs, 191
- smart action, 197
- SMTP email host, 37
- Source ID field, 195
- SQL Plus, 25
- SQL Server, 27
- SSH, 16
- SSL, 15, 16
- Starting WebLogic, 126
- State field, 195
- Status field, 195
- Stopping Select Identity Traffic, 186
- string field, 194
- System Activity Report, 205
- SystemOut.log, 37

T

- tablespace, 26
- TAUser table, 172
- Telnet, 16
- template
 - service call, 195, 199
- Terminate User, 214
- Text field, 194, 195
- tickets, Service Desk, 191
- topics, 65
- topology, 31
 - bus members, 57
- Translation Customization, 177
- truaccess.method=https, 172
- TruAccess.properties, 157, 198
 - configuring, 235
 - configuring required settings, 157
 - Select Audit, 202
 - settings, 235

- TruAccess_JMS, 58
- TruAccess Properties
 - Setting, 171
- TruAccess Properties File
 - Updating, 257
- trust store, 168, 171

U

- Uninstalling, 231
- unlimited strength policy files, 36
- upgrade Select Identity, 185
- Upgrading the Bootstrap Keystore, 166
- URL
 - login, 105, 156
- US_export_policy.jar, 37
- user account
 - JMS, 26
 - Select Identity, 26
- user accounts, 13
 - Select Audit, 203
- User Activity Report, 205
- users, 201
- User Search criteria, 183
- User Search Information dialog, 183
- User Summary Report, 205
- UTF-8 encoding, 182

W

- WAR file, 37, 70
- WAS6_LMZ.ear, 70
- webapi.jar, 191
- Web Application Archive, 37
- Web application server
 - performance, 20
 - upgrade requirements, 185
- web application server, configuring WebLogic, 36
- WebLogic
 - Migration from 8.15/8.16 to 9.21 MP, 188
- WebLogic install, 113
 - manual install, 122
- WebSphere, 26
 - Migration from 6.012 to 6.10 patch 9, 188
 - preparing to install SI, 36
 - starting, 37
- WebSphere admin server
 - IP and host name, 38

- WebSphere install:installation wizard, 38
- Workflow, 218
- workflow, 192, 199
- WorkflowChangeRequest approved, 215, 218
- WorkflowChangeRequest rejected, 215
- WorkflowChangeRequest reverted, 215, 218
- WorkflowChangeRequest submitted, 215, 217, 218
- WorkflowConfigChange, 215, 218
- Workflow copy, 216, 218
- Workflow create, 215, 218
- Workflow delete, 215, 218
- Workflow Events Report, 205
- Workflow export, 216, 219
- Workflow import, 214, 216, 218
- Workflow modify, 215, 218
- Workflow Studio, 15, 195
- Workflow Studio online help, 192
- Workflow Studio Service Desk Template, 192
- Workflow view, 216, 218

X

- XML, 17, 201
 - Editor, 177
 - File, 177
 - Spy, 177
- Xmx1024m, 172

