IBM Security Identity Manager
Version 6.0

Oracle eBS Adapter Installation and Configuration Guide
Contents

Figures ........................................... v
Tables ............................................. vii

Preface ........................................... ix
About this publication ....................... ix
Access to publications and terminology .... ix
Accessibility ..................................... x
Technical training ................................ x
Support information ......................... x
Statement of Good Security Practices ....... x

Chapter 1. Overview of the adapter ... 1
Features of the adapter ....................... 1
Architecture of the adapter ................. 1
Supported configurations ................... 2

Chapter 2. Preparation for the adapter installation .......... 5
Preinstallation roadmap ...................... 5
Installation roadmap .......................... 5
Prerequisites .................................. 6
Installation worksheet for the adapter ...... 7
Software download for the Oracle eBS adapter .... 7

Chapter 3. Adapter installation ......... 9
Verification of the Dispatcher installation ... 9
Installing the adapter ......................... 9
Start, stop, and restart of the Oracle eBS adapter service .......... 10
SSL connection configuration between the Oracle eBS Adapter and the Oracle eBS database ........ 10
Configuring Oracle eBS database tier ....... 10
Configuring the Tivoli Directory Integrator for Oracle eBS database tier authentication ........ 11
Configuring Tivoli Directory Integrator for Oracle eBS Adapter authentication ................ 12
Changes to the adapter service form ........ 12
JDBC driver location for SSL ................ 13
Importing the adapter profile into the IBM Security Identity Manager server ................. 14
Deploying the custom subforms ............. 15
Verification of the adapter profile installation .......... 15
Adapter user account ......................... 16
Creating an adapter service .................. 16

Chapter 4. First steps after installation 21
Adapter configuration ......................... 21
Customizing the adapter profile ............. 21
Editing adapter profiles on the UNIX or LINUX operating system ..................... 22
Password management when restoring accounts ................ 23
Language pack installation for the Oracle eBS adapter .......... 23
Verifying that the Oracle eBS adapter is working correctly .......... 23

Chapter 5. Troubleshooting of the adapter errors ........ 25
Techniques for troubleshooting problems .......... 25
Warning and error messages ................ 27

Chapter 6. Adapter upgrade ............... 29
Dispatcher upgrade ......................... 29
Profile upgrade ................. 29

Chapter 7. Adapter uninstallation ....... 31
Uninstalling the adapter from the Tivoli Directory Integrator server ................. 31
Removal of the adapter profile from the Tivoli Identity Manager server ................. 31

Chapter 8. Reinstallation of the adapter ... 33
Appendix A. Adapter attributes ......... 35
Attributes by Oracle eBS Adapter actions .......... 37
System Login Add .......................... 37
System Login Change ....................... 37
System Login Delete ....................... 37
System Login Suspend ..................... 37
System Login Restore ..................... 38
Test ....................................... 38
Reconciliation ............................... 38

Appendix B. Adapter installation on a zOS operating system ........ 39

Appendix C. Definitions for ITDI_HOME and ISIM_HOME directories ........ 41

Appendix D. Support information .......... 43
Searching knowledge bases .................. 43
Obtaining a product fix ....................... 44
Contacting IBM Support ....................... 44

Appendix E. Accessibility features for IBM Security Identity Manager .......... 47

Notices ....................................... 49

Index ........................................... 53
Figures

1. The architecture of the Oracle eBS Adapter 2
2. Example of a single server configuration 2
3. Example of a multiple server configuration 3
### Tables

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preinstallation road map</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Installation roadmap</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Prerequisites to run the adapter</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Required information to install the adapter</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Warning and error messages</td>
<td>27</td>
</tr>
<tr>
<td>6</td>
<td>Attributes, descriptions, constraints, and permissions</td>
<td>35</td>
</tr>
<tr>
<td>7</td>
<td>Add request attributes for Oracle</td>
<td>37</td>
</tr>
<tr>
<td>8</td>
<td>Change request attributes for Oracle</td>
<td>37</td>
</tr>
<tr>
<td>9</td>
<td>Suspend request attributes for Oracle</td>
<td>37</td>
</tr>
<tr>
<td>10</td>
<td>Restore request attributes for Oracle</td>
<td>38</td>
</tr>
<tr>
<td>11</td>
<td>Test attributes</td>
<td>38</td>
</tr>
<tr>
<td>12</td>
<td>Reconciliation request attributes for Oracle</td>
<td>38</td>
</tr>
</tbody>
</table>
Preface

About this publication

The Oracle eBS Adapter Installation and Configuration Guide provides the basic information that you can use to install and configure the IBM® Security Identity Manager Oracle E-Business Suite Adapter (Oracle eBS Adapter).

IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

The Oracle eBS Adapter enables connectivity between the IBM Security Identity Manager server and a managed resource. The IBM Security Identity Manager server is the server for your IBM Security Identity Manager product.

Access to publications and terminology

This section provides:

- A list of publications in the IBM Security Identity Manager library.
- Links to Online publications.
- A link to the IBM Terminology website.

IBM Security Identity Manager library


Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central](http://www-01.ibm.com/support/knowledgecenter/SSRMWJ/welcome) provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center


IBM Terminology website

Accessibility
Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training
For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information
IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix D, “Support information,” on page 43 provides details about:
- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.

Statement of Good Security Practices
IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. Overview of the adapter

The Oracle eBS Adapter enables communication between the IBM Security Identity Manager server and the Oracle eBS user database, also known as the FND_USER directory.

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server. Adapters might reside on the managed resource. The IBM Security Identity Manager server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target platform. They perform tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are performed manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity Manager server.

Features of the adapter

The adapter automates user account management tasks.

Automated user account management tasks include:
- Reconciling user accounts and support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending and restoring user accounts

Architecture of the adapter

The adapter contains Tivoli Directory Integrator AssemblyLines that serve one or more account operation.

When IBM Security Identity Manager sends the first request, the required AssemblyLine is loaded into the Tivoli Directory Integrator. The same AssemblyLine is then cached to serve subsequent operations of the same type.

You must install the following components for the adapter to function correctly:
- The RMI Dispatcher
- The Tivoli Directory Integrator connector
- The IBM Security Identity Manager adapter profile

You need to install the RMI Dispatcher and the adapter profile; however, the Tivoli Directory Integrator connector might already be installed with the base Tivoli Directory Integrator product.

Figure 1 on page 2 describes the components that work together to complete the user account management tasks in a Tivoli Directory Integrator environment.
For more information about Tivoli Directory Integrator, see the Quick Start Guide at IBM Security Identity Manager product documentation.

## Supported configurations

There are fundamental components in each environment.

Each environment has the:
- IBM Security Identity Manager server
- Tivoli Directory Integrator server
- Managed resource
- Adapter

The adapter must reside directly on the server running the Tivoli Directory Integrator server.

### Single server configuration

In a single server configuration, install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the Oracle eBS Adapter on one server to establish communication with the Oracle eBS. The Oracle eBS is installed on a different server as described [Figure 2](#).

### Multiple server configuration

In a multiple server configuration, install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, the Oracle eBS Adapter, and the Oracle eBS on different servers.

Install the Tivoli Directory Integrator server and the Oracle eBS Adapter on the same server as described in [Figure 3 on page 3](#).
Figure 3. Example of a multiple server configuration
Chapter 2. Preparation for the adapter installation

Before you install an adapter, plan the installation.

Installing and configuring the adapter involves several steps that you must complete in an appropriate sequence. Review the road maps before you begin the installation process.

Preinstallation roadmap

Before you install the adapter, you must prepare the environment.

Perform the tasks that are listed in Table 1.

Table 1. Preinstallation road map

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software.</td>
<td>Download the software from Passport Advantage® Web site. See “Software download for the Oracle eBS adapter” on page 7.</td>
</tr>
<tr>
<td>Verify that your environment meets the</td>
<td>See “Prerequisites” on page 6.</td>
</tr>
<tr>
<td>software and hardware requirements for the</td>
<td></td>
</tr>
<tr>
<td>adapter.</td>
<td></td>
</tr>
<tr>
<td>Obtain and install the Dispatcher.</td>
<td>Download the software from Passport Advantage website. See “Software download for the Oracle eBS adapter” on page 7. Follow the installation instructions in the dispatcher download package.</td>
</tr>
<tr>
<td>Obtain the necessary information for the</td>
<td>See “Installation worksheet for the adapter” on page 7.</td>
</tr>
<tr>
<td>installation and configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Installation roadmap

To install the adapter, complete the tasks in this installation roadmap.

The tasks are listed in Table 2.

Table 2. Installation roadmap

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the Dispatcher installation.</td>
<td>See “Verification of the Dispatcher installation” on page 9.</td>
</tr>
<tr>
<td>Install the adapter.</td>
<td>See “Installing the adapter” on page 9.</td>
</tr>
<tr>
<td>Import the adapter profile.</td>
<td>See “Verification of the adapter profile installation” on page 15.</td>
</tr>
<tr>
<td>Verify the profile installation.</td>
<td>See “Importing the adapter profile into the IBM Security Identity Manager server” on page 14.</td>
</tr>
<tr>
<td>Create an adapter user account.</td>
<td>See “Adapter user account” on page 16.</td>
</tr>
<tr>
<td>Create a service.</td>
<td>See “Creating an adapter service” on page 16.</td>
</tr>
</tbody>
</table>
### Table 2. Installation roadmap (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an adapter user account.</td>
<td>See “Adapter user account” on page 16.</td>
</tr>
<tr>
<td>Configure the adapter.</td>
<td>See “Adapter configuration” on page 21.</td>
</tr>
</tbody>
</table>

### Prerequisites

Verify that your environment meets all the prerequisites before installing the adapter.

Table 3 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the IBM Tivoli Directory Integrator server.

Note: See the release notes in the adapter package for the most current list of requirements.

### Table 3. Prerequisites to run the adapter

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator server</td>
<td>Version 7.1 fix pack 5 or later</td>
</tr>
<tr>
<td></td>
<td>Version 7.1.1</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>Oracle eBS</td>
<td>A system that runs the Oracle eBS release:</td>
</tr>
<tr>
<td></td>
<td>• 12.0</td>
</tr>
<tr>
<td></td>
<td>• 12.1.1</td>
</tr>
<tr>
<td>Oracle Thin JDBC Driver</td>
<td>All the listed JDBC driver can talk with all the supported version of Oracle except Oracle 10g r2:</td>
</tr>
<tr>
<td>Note: For information about the JDBC driver installation, see [<a href="http://www.oracle.com/technology/software/tech/java/sqlj">http://www.oracle.com/technology/software/tech/java/sqlj</a> jdbc/index.html](<a href="http://www.oracle.com/technology/software/tech/java/sqlj">http://www.oracle.com/technology/software/tech/java/sqlj</a> jdbc/index.html)</td>
<td>• JDBC 8.1.7 Driver</td>
</tr>
<tr>
<td></td>
<td>• JDBC 9.0.1 Driver</td>
</tr>
<tr>
<td></td>
<td>For Oracle 10g r2:</td>
</tr>
<tr>
<td></td>
<td>• JDBC 10.2.0.1.0 Driver</td>
</tr>
<tr>
<td>Network Connectivity</td>
<td>The adapter must be installed on a system that can communicate with the IBM Security Identity Manager service through the TCP/IP network.</td>
</tr>
<tr>
<td>System Administrator Authority</td>
<td>To complete the adapter installation procedure, you must have system administrator authority.</td>
</tr>
</tbody>
</table>

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the *IBM Tivoli Directory Integrator 7.1: Administrator Guide*. 

---

6 IBM Security Identity Manager: Oracle eBS Adapter Installation and Configuration Guide
Installation worksheet for the adapter

You need to collect information before installing an adapter.

Table 4 identifies the information that you need before installing the adapter.

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator Home Directory</td>
<td>The \textit{ITDI_HOME} directory contains the \texttt{jars/connectors} subdirectory that contains adapter JAR files. For example, the \texttt{jars/connectors} subdirectory contains the JAR files for the UNIX adapter.</td>
<td>Windows: \begin{itemize} \item for version 7.1: \texttt{drive\Program Files\IBM\TDI\V7.1} \end{itemize} UNIX: \begin{itemize} \item for version 7.1: \texttt{/opt/IBM/TDI/V7.1} \end{itemize}</td>
</tr>
<tr>
<td>Adapters solution directory</td>
<td>For more information about the adapter solution directory, see the \textit{Dispatcher Installation and Configuration Guide}.</td>
<td>Windows: \begin{itemize} \item for version 7.1: \texttt{drive\Program Files\IBM\TDI\V7.1\timsol} \end{itemize} UNIX: \begin{itemize} \item for version 7.1: \texttt{/opt/IBM/TDI/V7.1/timsol} \end{itemize}</td>
</tr>
</tbody>
</table>

Software download for the Oracle eBS adapter

Download the software through your account at the IBM Passport Advantage website.

Go to [IBM Passport Advantage](https://www.ibm.com)

See the \textit{IBM Security Identity Manager Download Document} for instructions.

Note:

You can also obtain additional adapter information from IBM Support.
Chapter 3. Adapter installation

All the Tivoli Directory Integrator-based adapters require the Dispatcher for the adapters to function correctly.

If the Dispatcher is installed from a previous installation, do not reinstall it unless there is an upgrade to the Dispatcher. See "Verification of the Dispatcher installation."

After verifying the Dispatcher installation, you might need to install the Tivoli Directory Integrator connector. Depending on your adapter, the connector might already be installed as part of the Tivoli Directory Integrator product and no further action is required.

Verification of the Dispatcher installation

If this installation is the first Tivoli Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter.

You must install the dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.


Installing the adapter

This task provides all the necessary steps for installing the adapter software.

Before you begin

Make sure you do the following:

• Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 6.
• Obtain a copy of the installation software. See "Software download for the Oracle eBS adapter" on page 7.
• Obtain system administrator authority. See "Prerequisites" on page 6.

About this task

The adapter uses the IBM Tivoli Directory Integrator JDBC connector. This connector is available with the base Tivoli Directory Integrator product. Because the Tivoli Directory Integrator JDBC connector is already installed, you need to install only the RMI Dispatcher. See "Verification of the Dispatcher installation."

To install the RMI Dispatcher, see the IBM Security RMI Dispatcher Installation and Configuration Guide.
What to do next

After you finish the adapter installation, do the following:

- Import the adapter profile. See “Importing the adapter profile into the IBM Security Identity Manager server” on page 14.
- Create a user account for the adapter on IBM Security Identity Manager. See “Adapter user account” on page 16.

Start, stop, and restart of the Oracle eBS adapter service

To start, stop, or restart the adapter, you must start, stop, or restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Tivoli Directory Integrator instance.

See the topic about starting stopping, and restarting the dispatcher service in the Dispatcher Installation and Configuration Guide.

SSL connection configuration between the Oracle eBS Adapter and the Oracle eBS database

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

If the Oracle eBS database is configured to require SSL client authentication, you must configure a keystore.

To configure the truststore for the dispatcher, you must minimally import the Certification Authority (CA) certificate. This certificate is the one used to sign the certificate for the Oracle eBS database.

Note:

- All the files in the following tasks are in the solutions directory. For example: TDI_HOME/timsol.
- The store password ThePwd12 in the code examples is a variable. Substitute your password for ThePwd12.

Configuring Oracle eBS database tier

Use the Oracle tools to configure both the truststore and the keystore on the Oracle eBS database tier.

About this task

The Oracle Wallet Manager and the orapki command, are used in the following steps. The following task sets up a self-signed certification authority, truststore, and keystore.

Procedure

1. Create a self-signed certificate authority. Issue the following commands:
   ```
   mkdir authority
   orapki wallet create -wallet ./authority -pwd=ThePwd12
   ```
orapki wallet add -wallet ./authority -dn "CN=authority, C=US" -keys 2048
-sel_signed -validity 3650 -pwd=ThePwd12

orapki wallet export -wallet ./authority -dn "CN=authority, C=US"
-cert CA.cer-pwd=ThePwd12

The CA.cer file is the trusted certificate that is used in the keytool command to import a CA certificate into the truststore for the dispatcher.

2. Create stores for Oracle eBS database tier authentication
Issue the following commands:

   mkdir server

orapki wallet create -wallet ./server -auto_login -pwd=ThePwd12

orapki wallet add -wallet ./server -trusted_cert -cert CA.cer -pwd=ThePwd12

orapki wallet add -wallet ./server -dn "CN=server, C=US" -keys 2048
-pwd=ThePwd12

orapki wallet export -wallet ./server -dn "CN=server, C=US" -request creq.cer
-pwd=ThePwd12

orapki cert create -wallet ./authority -request creq.cer -cert signed.cer
-validity 3650 -pwd=ThePwd12

orapki wallet add -wallet ./server -user_cert -cert signed.cer -pwd=ThePwd12

3. Configure the Oracle network. You must configure the listener.ora and sqlnet.ora files on the Oracle eBS database tier to enable SSL. These files are typically edited with the Oracle Net Manager or with a text editor. These files are in the ORACLE_HOME/network/admin/instance directory of the database tier. This example does not require adapter authentication. If you want to require authentication for the Oracle eBS Adapter, set SSL_CLIENT_AUTHENTICATION to TRUE.

   a. Edit the listener.ora file.
   b. Locate the following lines and substitute the appropriate values for
     SERVER_WALLET_LOCATION and HOSTNAME.

     SSL_CLIENT_AUTHENTICATION = FALSE
     WALLET_LOCATION = (SOURCE = (METHOD = FILE)(METHOD_DATA =
                      (DIRECTORY = SERVER_WALLET_LOCATION))
                      ))
     LISTENER = (DESCRIPTION_LIST = (DESCRIPTION =
                      (ADDRESS = (PROTOCOL = TCPS)(HOST = HOSTNAME)(PORT = 2484)))
                      ))

     Note: Port 2484 is typically used for SSL communication (TCPS protocol).
   c. Edit the sqlnet.ora file.
   d. Locate the following lines and substitute the appropriate values for
      highlighted values.

    SSL_CLIENT_AUTHENTICATION = FALSE
    WALLET_LOCATION = (SOURCE = (METHOD = FILE)(METHOD_DATA =
                        (DIRECTORY = SERVER_WALLET_LOCATION))
                        ))

Configuring the Tivoli Directory Integrator for Oracle eBS database tier authentication

   You must import a CA certificate into the truststore.
Procedure
1. Import a CA certificate into the truststore. Issue the command:
   ```
   keytool -import -v -alias OACA -file CA.cer -keystore truststore.jks
   -storetype JKS -storepass "ThePwd12"
   ```
2. In the solutions.properties file, set the following properties:
   ```
   javax.net.ssl.trustStore=truststore.jks
   javax.net.ssl.trustStorePassword=ThePwd12
   javax.net.ssl.trustStoreType=jks
   ```
   **Note:** If the `javax.net.ssl.trustStore` property is already set to a truststore other than `truststore.jks`, import the CA certificate into that file instead.
3. Set the keystore properties. If a keystore is not required and no keystore properties are set in the solutions.properties file, use the truststore properties values for the keystore properties:
   ```
   javax.net.ssl.keyStore=truststore.jks
   javax.net.ssl.keyStorePassword=ThePwd12
   javax.net.ssl.keyStoreType=jks
   ```

Configuring Tivoli Directory Integrator for Oracle eBS Adapter authentication

If the Oracle eBS database is configured for SSL client authentication, you must configure a keystore.

Before you begin

You created a self-signed certificate authority in the Oracle eBS Adapter database tier.

Procedure
1. Create a JKS keystore. Issue the following commands:
   ```
   keytool -genkey -alias OADB -dname "CN=client,C=US" -storetype JKS
   -keystore client.jks -keyalg RSA -storepass "ThePwd12"
   keytool -certreq -alias OADB -file creq.cer -keystore client.jks
   -storepass "ThePwd12"
   orapki cert create -wallet ./authority -request creq.cer -cert signed.cer
   -validity 3650 -pwd=ThePwd12
   keytool -import -v -alias OACA -file CA.cer -keystore client.jks
   -storepass "ThePwd12"
   keytool -import -v -alias OADB -file signed.cer -keystore client.jks
   -storepass "ThePwd12"
   ```
2. Set the following properties in the solutions.properties file:
   ```
   javax.net.ssl.keyStore=client.jks
   javax.net.ssl.keyStorePassword=ThePwd12
   javax.net.ssl.keyStoreType=jks
   ```

Changes to the adapter service form

To enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database, you must supply information for the Oracle eBS adapter service form.

To access the service form, use the Manage Services utility on the IBM Security Identity Manager console. Supply following information for the fields on the service form.
Use SSL communication with Oracle?
Click this check box.

Oracle EBS Service Port
Change the value to the TCPS port. For example 2484.

Oracle EBS Server Distinguished Name
Optional. When a value is entered for this field, the entry is verified against the Oracle eBS database server certificate.

Note:
- Start the listener and database services with the same user who created the wallet, so that they are both able to access the wallet.
- The wallet location is provided in both the sqlnet.ora and the listener.ora files. Typically, both files contain the same wallet location. However, the listener.ora file can use its own wallet.
  - The distinguished name of the certificate pointed by the wallet in the sqlnet.ora file is the name to which the Oracle eBS Adapter must verify. This requirement applies only if a distinguished name is supplied on the service form.
  - Include a distinguished name in the service form as an extra measure of security. Doing so prevents another server from faking the identity.
- For information about how to configure SSL with the Oracle JDBC Thin driver, go to the Oracle website. Search for the Oracle technical white paper SSL with Oracle JDBC Thin Driver.

JDBC driver location for SSL
You must download the JDBC Thin driver to support SSL.

Obtain the JDBC Thin driver from either:
- The ORACLE_HOME/jdbc/lib directory of the database tier
- The JDBC Driver Downloads page on the Oracle Technology Network (OTN) website.

Depending on your JRE, select the appropriate driver. The driver for JRE 1.5 is ojdbc5.jar. The driver for JRE 1.6 is ojdbc6.jar.

Copy the appropriate driver to the TDI_HOME/jars/3rdparty/others directory on the Tivoli Directory Integrator server.

Remove previous versions of the JDBC Thin driver from the TDI_HOME/jars/3rdparty/others directory. For example:
- ojdbc14.jar
- classes12.zip
- nls_charset12.zip
- classes111.zip
- nls_charset11.zip

Note: The .zip file in the list might alternatively be named as jar files. For example classes12.jar.
Importing the adapter profile into the IBM Security Identity Manager server

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage. Use the profile to create an adapter service on IBM Security Identity Manager server and establish communication with the adapter.

Before you begin

Before you begin to import the adapter profile, verify that the following conditions are met:

- The IBM Security Identity Manager server is installed and running.
- You have root or Administrator authority on IBM Security Identity Manager.

About this task

Before you can create an adapter service, the IBM Security Identity Manager server must have an adapter profile to recognize the adapter. The files that are packaged with the adapter include the adapter profile JAR file. You can import the adapter profile as a service profile on the server with the Import feature of IBM Security Identity Manager.

The JAR file includes all the files that are required to define the adapter schema, account form, service form, and profile properties. You can extract the files from the JAR file to modify the necessary files and package the JAR file with the updated files.

To import the adapter profile, perform the following steps:

Note:

- When you import the adapter profile and if you receive an error related to the schema, see the trace.log file for information about the error. The trace.log file location is specified by using the handler.file.fileDir property defined in the IBM Security Identity Manager enRoleLogging.properties file. The enRoleLogging.properties file is installed in the ISIM_HOME\data directory.
- Restart IBM Security Identity Manager for the change to take effect.

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, expand Configure System and click Manage Service Types.
3. On the Manage Service Types page, click Import to display the Import Service Types page.
4. Specify the location of the JAR file in the Service Definition File field by performing one of the following tasks:
   - Type the complete location of where the file is stored.
   - Use Browse to navigate to the file.
5. Click OK.
Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the OraEBSSubForms.zip file.

Before you begin

Extract the contents of the OraEBSSubForms.zip file to the subforms folder of the installed IBM Security Identity Manager web application.

For a self service console installation

WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/
itim_self_service.war

For an administrative console installation

WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/
itim_console.war

For Identity Service Center installation

WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/
isim_isc_subform.war

About this task

In a clustered environment the subform must be deployed on each WebSphere application server. If WebSphere version 6.1 is being used, the jdkSourceLevel JSP engine configuration parameter must be set to 15 for each web application on which the subforms are deployed.

Procedure

1. Open the WEB-INF/ibm-web-ext.xmi file from the configuration directory. For example, WAS_PROFILE_HOME/config/cells/cellName/applications/ITIM.ear/deployments/ITIM/webModuleName. The webModuleName is the
itim_self_service.war file or the itim_console.war file or both.

2. Add the following tag within the content of the webappext:webAppExtension tag:

   <jspAttributes xmi:id="JSPAttribute_1" name="jdkSourceLevel" value="15"/>

   Note: The integer n in JSPAttribute_n has to be unique within the file.

3. Save the file.

4. Take one of the following actions:
   - Restart the IBM Security Identity Manager application from the WebSphere Administrative Console.
   - Restart the service.

Verification of the adapter profile installation

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:
   - Might cause the adapter to function incorrectly.
   - Prevents you from creating a service with the adapter profile.
To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see "Creating an adapter service."

If you are unable to create a service using the adapter profile or open an account on the service, the adapter profile is not installed correctly. You must import the adapter profile again.

Adapter user account

You must create a user account for the adapter on the managed resource, therefore, provide account information when you create a service.

For more information about creating a service, see "Creating an adapter service."

The accounts must be able to remotely connect to the Oracle eBS and must have sufficient privileges to administer the Oracle eBS users.

The APPS account owns the Oracle eBS database and the adapter must run as the APPS user unless you have followed special configuration steps. If you use APPS, you do not require configuration changes on the managed resource.

If your security standards do not permit the use of APPS as an administrator account for the Oracle eBS Adapter, you must create a new user and grant required permissions as provided in the nonAPPS.sql file. The nonAPPS.sql file is supplied with the Oracle eBS Adapter compressed file. The adapter depends on wrapper stored procedures when an account other than APPS is used. Create the wrapper stored procedures specified in nonAPPS.sql file.

Creating an adapter service

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.

About this task

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

Note: If the following fields on the service form are changed for an existing service, the IBM Security Identity Manager adapter service on the Tivoli Directory Integrator server must be restarted.

- Service Name
- Password
- Owner
- Service prerequisite

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, click Manage Services and click Create.
3. On the Select the Type of Service page, select Oracle EBS Adapter Service Profile.
4. Click Next to display the adapter service form.

5. To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. Complete the following fields on the service form:

**On the Oracle EBS Profile tab:**

- **Service name**
  Specify a name that defines the adapter service on the IBM Security Identity Manager server.
  
  **Note:** Do not use forward (/) or backward slashes (\) in the service name.

- **Description**
  Optional: Specify a description that identifies the service for your environment.

- **Tivoli Directory Integrator location**
  Optional: Specify the URL for the Tivoli Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher`, where `ip-address` is the Tivoli Directory Integrator host and `port` is the port number for the RMI Dispatcher. The default URL is `rmi://localhost:1099/ITDIDispatcher`

  For information about changing the port number, see IBM Security Dispatcher Installation and Configuration Guide.

- **Oracle EBS Service Name**
  Specify the service name of Oracle eBS database instance to which the adapter must connect.

- **Oracle EBS Service Host**
  Specify the host workstation on which the Oracle eBS database instance is running.

- **Oracle EBS Service Port**
  Specify the port on which the Oracle eBS database service is listening.

- **Use SSL communication with Oracle?**
  Click the check box to force an SSL connection from the adapter to the Oracle eBS database.

- **Oracle EBS Server Distinguished Name**
  Optional. Specify the distinguished name contained in the certificate of the Oracle eBS database. If SSL communication is enabled and this field is not blank, the connection succeeds only if the distinguished names match.

- **Administrator Name**
  Specify the name of the user who has access to the Oracle eBS database and can perform administrative operations.

- **Password**
  Specify the password for the user.

- **Owner**
  Optional: Specify a IBM Security Identity Manager user as a service owner.
Service Prerequisite
Optional: Specify a IBM Security Identity Manager service that is prerequisite to this service.

On the Dispatcher Attributes tab:

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For example, you can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: c:\Files\IBM\TDI\V7.1\profiles or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating systems: system:/opt/IBM/TDI/V7.1/profiles

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 10 assembly lines simultaneously for the service. If you enter 0 in the Max Connection Count field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

On the Status and information tab
This page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click Test Connection to populate the fields.

Last status update: Date
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource that the adapter is connected to.

Adapter version
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the IBM Security Identity Manager server.
TDI version
Specifies the version of the Tivoli Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

Installation platform
Specifies summary information about the operating system where the adapter is installed.

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also
• Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
• Verify the adapter configuration information.
• Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.
Chapter 4. First steps after installation

After you install the adapter, you must perform several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying the adapter works correctly.

Adapter configuration

This chapter describes the configuration options for the Oracle eBS Adapter.

- "Customizing the adapter profile"
- "Editing adapter profiles on the UNIX or LINUX operating system" on page 22

See the IBM Security Dispatcher Installation and Configuration Guide for additional configuration options such as:
- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

About this task

You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms with the Form Designer or CustomLabels.properties. Each adapter has a CustomLabels.properties file for that adapter.

The JAR file is included in the Oracle eBS Adapter compressed file that you downloaded from the IBM website. The JAR file and the files contained in the JAR file vary depending on your operating system.

Note: You cannot modify the schema for this adapter. Attributes cannot be added to or deleted from the schema.

The adapter JAR file includes the following files:
- Service.def
- Schema.dsml
- CustomLabels.properties
- erOracleEBSAccount.xml
- erOracleEBSRMIService.xml
- OracleEBSManagerUserAL.xml
- OracleEBSSearchUserAL.xml

To edit the JAR file, perform these steps:
Procedure
1. Log on to the workstation where the Oracle eBS Adapter is installed.
2. On the Start menu, click Programs > Accessories > Command Prompt.
3. Copy the JAR file into a temporary directory.
4. Extract the contents of the JAR file into the temporary directory by running the following command.
   The following example applies to the Oracle eBS Adapter profile. Type the name of the JAR file for your operating system.
   cd c:\temp
   #jar -xvf OraEBSProfile.jar

   The jar command extracts the files into the directory.
5. Edit the file that you want to change.
6. After you edit the file, you must import the file into the IBM Security Identity Manager server for the changes to take effect. To import the file, perform these steps:
   a. Create a JAR file with the files in the \temp directory by running the following commands:
      cd c:\temp
      #jar -cvf OraEBSProfile.jar OraEBSProfile
   b. Import the JAR file into the IBM Security Identity Manager application server. For more information about importing the JAR file, see “Importing the adapter profile into the IBM Security Identity Manager server” on page 14.
   c. Stop and start the IBM Security Identity Manager server.
   d. Stop and start the Oracle eBS Adapter service. See “Start, stop, and restart of the Oracle eBS adapter service” on page 10 for information about stopping and starting the Oracle eBS Adapter service.

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as dos2unix, to remove the ^M characters. You can also use text editors, such as the vi editor, to remove the characters manually.

Example

You can use the vi editor to remove the ^M characters. From the vi command mode, run the following command and press Enter:

:%s/^M//g

When you use this command, enter ^M or Ctrl-M by pressing ^v^M or Ctrl V Ctrl M sequentially. The ^v instructs the vi editor to use the next keystroke instead of issuing it as command.
Password management when restoring accounts

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement.

Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Identity Manager to forego the new password requirement. You can set the Oracle eBS Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the service.def file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the schema.dsml file. Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts being restored might require a password. Remote services will discard the password from the restore action for those managed resources that do not require them.

Edit the service.def file to add the new protocol options, for example:

```xml
<Property Name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_REQUIRED_ON_RESTORE" value = true/>
<Property Name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_ALLOWED_ON_RESTORE" value = false/>
```

By adding the two options in the example above, you are ensuring that you will not be prompted for a password when an account is restored.

Language pack installation for the Oracle eBS adapter

The adapters use a separate language package from the IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing the adapter language pack.

Verifying that the Oracle eBS adapter is working correctly

After you install and configure the adapter, take steps to verify that the installation and configuration are correct.

**Procedure**

1. Test the connection for the service that you created on IBM Security Identity Manager.
2. Run a full reconciliation from IBM Security Identity Manager.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the ibmdi.log file after each operation to ensure that no errors are reported.
5. Verify the IBM Security Identity Manager log file `trace.log` to ensure that no errors are reported when you run an adapter operation.
Chapter 5. Troubleshooting of the adapter errors

Troubleshooting can help you determine why a product does not function properly.

These topics provide information and techniques for identifying and resolving problems with the adapter. It also provides information about troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
• Do all users have the problem?
• (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
• Does the problem happen only at a certain time of day or night?
• How often does the problem happen?
• What sequence of events leads up to the time that the problem is reported?
• Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
• Does the problem always occur when the same task is being performed?
• Does a certain sequence of events need to happen for the problem to occur?
• Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible,
re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix D, “Support information,” on page 43.

### Warning and error messages

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Table 5 contains warnings or errors that might be displayed on the user interface if the adapter is installed on your workstation.

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Warning or error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTGIMT001E</td>
<td>The following error occurred. Error: Either the Oracle eBS service name is incorrect or the service is not up.</td>
<td>Ensure that the Oracle database service name given on IBM Security Identity Manager service form is running.</td>
</tr>
<tr>
<td>CTGIMT001E</td>
<td>The following error occurred. Error: Either the Oracle eBS host or port is incorrect.</td>
<td>Verify that the host workstation name or the port for the Oracle eBS database service is correctly specified.</td>
</tr>
<tr>
<td>CTGIMT002E</td>
<td>The login credential is missing or incorrect.</td>
<td>Verify that you have provided correct login credential on service form.</td>
</tr>
<tr>
<td>CTGIMT001E</td>
<td>The following error occurred. Error: No suitable JDBC driver found.</td>
<td>Ensure that the correct version of the JDBC thin driver is copied onto the workstation where the adapter is installed and that the path is included in the system CLASSPATH variable.</td>
</tr>
</tbody>
</table>
| CTGIMT600E   | An error occurred while establishing communication with the Tivoli Directory Integrator server. | IBM Security Identity Manager cannot establish a connection with Tivoli Directory Integrator. To fix this problem, ensure that:
- The Tivoli Directory Integrator is running.
- The URL specified on the service form for the Tivoli Directory Integrator is correct. |
Chapter 6. Adapter upgrade

The adapter is upgraded by installing the new version of the adapter.

Upgrading the adapter might also involve tasks, such as upgrading the connector, the dispatcher, and the existing adapter profile. To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Adapter installation,” on page 9.

Dispatcher upgrade

Before you upgrade the dispatcher, verify the version of the dispatcher.

Before you upgrade the dispatcher, verify the version of the dispatcher.
• If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
• If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

Note: Stop the dispatcher service before the upgrading the dispatcher and start it again after the upgrade is complete.

Profile upgrade

Read the adapter Release Notes for any specific instructions before importing a new adapter profile into IBM Security Identity Manager.

See "Importing the adapter profile into the IBM Security Identity Manager server" on page 14.

Note: Restart the dispatcher service after importing the profile. Restarting the dispatcher clears the assembly lines cache and ensures that the dispatcher executes the assembly lines from the updated adapter profile.
Chapter 7. Adapter uninstallation

To completely uninstall the Oracle eBS Adapter, you need to perform two procedures:
1. Uninstall the adapter from Tivoli Directory Integrator server.
2. Remove the adapter profile from the IBM Security Identity Manager server.

Uninstalling the adapter from the Tivoli Directory Integrator server

You might need to remove the Oracle eBS Adapter.

About this task

The Oracle eBS Adapter installation installs the RMI Dispatcher only on the Tivoli Directory Integrator server. Therefore, you only need to uninstall from the RMI Dispatcher. There is no uninstall for the Oracle eBS Adapter.

The JAR file needed to uninstall the RMI Dispatcher was created in the
ITDI_HOME\DispatcherUninstall directory when the RMI Dispatcher was installed.

Note: The RMI Dispatcher is required for all adapters based on Tivoli Directory Integrator. If you uninstall the RMI Dispatcher, none of the other installed adapters function.

Complete these steps:

Procedure
1. Stop the adapter service.
2. Run the DispatcherUninstall.jar file. To run the JAR file, double click on the executable file or enter the following command at the command prompt:
   
   `TDI_HOME/jvm/jre/bin/java -jar DispatcherUninstall.jar`

Removal of the adapter profile from the Tivoli Identity Manager server

Before removing the adapter profile, ensure that no objects exist on your IBM Security Identity Manager server that reference the adapter profile.

Examples of objects on the IBM Security Identity Manager server that can reference the adapter profile are:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

Note: The RMI Dispatcher component must be installed on your system for adapters to function correctly in a Tivoli Directory Integrator environment. When you delete the adapter profile for the Oracle eBS Adapter, do not uninstall the RMI Dispatcher.

For specific information about how to remove the adapter profile, see the online help or the IBM Security Identity Manager product documentation.
Chapter 8. Reinstallation of the adapter

There are no special considerations for reinstalling the adapter. You do not need to remove the adapter before reinstalling.

For more information, see Chapter 6, “Adapter upgrade,” on page 29.
Appendix A. Adapter attributes

The IBM Security Identity Manager server communicates with the Oracle eBS Adapter with attributes that are included in transmission packets that are sent over a network.

The combination of attributes, included in the packets, depends on the type of action that the IBM Security Identity Manager server requests from the Oracle eBS Adapter.

Table 6 is a listing of the attributes that are used by the Oracle eBS Adapter. The table gives a brief description, constraints, and permissions. The permissions are:

- **Read**  The attribute is reconciled but not modified by the adapter.
- **Write**  The attribute is modified by the adapter but not reconciled.
- **Read and Write**  The attribute is reconciled and can be modified by the adapter.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Constraints</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>erAccountStatus</td>
<td>Specifies the status of the account as enabled or disabled.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erLastAccessDate</td>
<td>The user's last login date and time in Oracle eBS.</td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>erOraEBSCust</td>
<td>Customer.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSDescription</td>
<td>A short description for the user name.</td>
<td>The description is limited to a maximum of 240 characters.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSLeftPwdAccess</td>
<td>Specifies the number of login accesses remaining (from the current day) until the password expires.</td>
<td>The maximum value is 999999999999999.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSPerson</td>
<td>Person.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSPwdAccesses</td>
<td>Specifies the number of login accesses allowed before the password expires.</td>
<td>The maximum value is 999999999999999.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSPwdLifeSpanDays</td>
<td>Specifies the number of days after which the password expires.</td>
<td>The maximum value is 999999999999999.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSResp</td>
<td>Specifies a directly granted responsibility formatted as Application_Name</td>
<td>Responsibility_Name</td>
<td>Start_Date</td>
</tr>
</tbody>
</table>
### Table 6. Attributes, descriptions, constraints, and permissions (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Constraints</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>erOraEBSSessionNumber</td>
<td>Specifies the session ID</td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>erOraEBSSupp</td>
<td>Specifies a supplier.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSUserEndDate</td>
<td>Specifies the user’s effective end date.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSUserFax</td>
<td>Specifies the user’s fax number</td>
<td>The fax number is limited to a maximum of 80 characters.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSUserMail</td>
<td>Specifies the user’s email address.</td>
<td>The email address is limited to a maximum of 240 characters.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSUserStartDate</td>
<td>Specifies the user’s effective start date.</td>
<td></td>
<td>Read and Write</td>
</tr>
<tr>
<td>erPassword</td>
<td>Specifies the password for the user name.</td>
<td>The password is limited to a maximum of 45 characters.</td>
<td>Write</td>
</tr>
<tr>
<td>erUid</td>
<td>Specifies the user name.</td>
<td>The user name is limited to a maximum of 100 characters.</td>
<td>Read and Write</td>
</tr>
<tr>
<td>erOraEBSSecAttr</td>
<td>Specifies an associated securing attribute formatted as Application_ID</td>
<td>Attribute_Code</td>
<td>Value. Do not use blank spaces. For example, 454</td>
</tr>
<tr>
<td>erOraEBSIndirectResp</td>
<td>Specifies an inherited responsibility formatted like erOraEBSResp.</td>
<td></td>
<td>Read</td>
</tr>
<tr>
<td>erOraEBSDirectRoles</td>
<td>Specifies a directly granted role formatted as a JSON object with the fields role (object) startDate (string) endDate (string) reason (string) The 'role' object is a JSON object with fields name (string), origSystem (string), and origSystemId (string). The date fields (startDate and endDate) are represented as strings with the format yyyyMMddhh24mi'Z'. (For example 200112311345). For example, {&quot;endDate&quot;:null,&quot;reason&quot;:&quot;Granted by XX&quot;,&quot;role&quot;:{&quot;name&quot;:&quot;UMX\ SECURITY_ADMIN&quot;,&quot;origSystem&quot;:&quot;UMX&quot;,&quot;origSystemId&quot;:&quot;0&quot;},&quot;startDate&quot;:&quot;201103150000Z&quot;}.</td>
<td></td>
<td>Read and Write</td>
</tr>
</tbody>
</table>
### Attributes by Oracle eBS Adapter actions

The following lists are typical Oracle eBS Adapter actions by their functional transaction group.

The lists include more information about required and optional attributes sent to the Oracle eBS Adapter to complete that action.

#### System Login Add

A System Login Add is a request to create a new user account with the specified attributes.

*Table 7. Add request attributes for Oracle*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPassword</td>
</tr>
<tr>
<td></td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

#### System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

*Table 8. Change request attributes for Oracle*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>erPassword</td>
</tr>
<tr>
<td></td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

#### System Login Delete

This operation is not supported.

#### System Login Suspend

You might need to suspend a system login.

A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

*Table 9. Suspend request attributes for Oracle*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>None</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td></td>
</tr>
</tbody>
</table>
**System Login Restore**

You might need to restore a system login.

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system using the same attributes as the ones before the Suspend function was called.

*Table 10. Restore request attributes for Oracle*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>None</td>
</tr>
<tr>
<td>erAccountStatus</td>
<td>None</td>
</tr>
</tbody>
</table>

**Test**

The following table identifies attributes needed to test the connection.

*Table 11. Test attributes*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**Reconciliation**

You might need to reconcile user account information.

The Reconciliation request synchronizes user account information between IBM Security Identity Manager and the adapter.

*Table 12. Reconciliation request attributes for Oracle*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Appendix B. Adapter installation on a zOS operating system

To install the adapters on the zOS UNIX file system, you only need to install the RMI Dispatcher because the adapter uses the Tivoli Directory Integrator JDBC connector that is available with the base Tivoli Directory Integrator product.

For information about installing the RMI Dispatcher, see the Directory Integrator RMI Dispatcher Installation and Configuration Guide.

After the installation of the adapter is complete, to verify the startup and shutdown of the adapter go to “Start, stop, and restart of the Oracle eBS adapter service” on page 10.
Appendix C. Definitions for ITDI_HOME and ISIM_HOME directories

**ITDI_HOME**

This directory contains the jars/connectors subdirectory that contains files for the adapters.

**Windows**

`drive\Program Files\IBM\TDI\ITDI_VERSION`

For example the path for version 7.1:

`C:\Program Files\IBM\TDI\V7.1`

**UNIX**

`/opt/IBM/TDI/ITDI_VERSION`

For example the path for version 7.1:

`/opt/IBM/TDI/V7.1`

**ISIM_HOME**

This directory is the base directory that contains the IBM Security Identity Manager code, configuration, and documentation.

**Windows**

`path\IBM\isim`

**UNIX**

`path/IBM/isim`
Appendix D. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 44
- “Contacting IBM Support” on page 44

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the [ISA website](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the [demo videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - [IBM Security Identity Manager version 6.0 technotes and APARs (problem reports)](https://www.ibm.com/support/entry/techdocs/ibmsidm/6.0)
   - [IBM Security Identity Manager Support website](https://www.ibm.com/support/entry/techdocs/ibmsidm/6.0)
   - IBM Redbooks®
   - [IBM support communities (forums and newsgroups)](https://www.ibm.com/commerce/community)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

### Obtaining a product fix

A product fix might be available to resolve your problem.

**About this task**

You can get fixes by following these steps:

**Procedure**

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the Fix Central Site. See [http://www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/).
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the “Download package” section.
4. Apply the fix. Follow the instructions in the “Installation Instructions” section of the download document.

### Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the “Software Support Handbook”.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA): Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
     - b. Open ISA.
c. Click Collection and Send Data.

d. Click the Service Requests tab.

e. Click Open a New Service Request

• Online through the IBM Support Portal. You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.

• By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.
Appendix E. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

• Support for the Freedom Scientific JAWS screen reader application
• Keyboard-only operation
• Interfaces that are commonly used by screen readers
• Keys that are discernible by touch but do not activate just by touching them
• Industry-standard devices for ports and connectors
• The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

• You can use the tab keys and arrow keys to move between the user interface controls.
• You can use the Home, End, Page Up, and Page Down keys for more navigation.
• You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click Launch as a separate window.
• You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX  78758  U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to
IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

Index

A
accessibility x, 47
adapter
attributes
by adapter action 37
descriptions 35
permissions 35
customization
options 21
steps 21
features 1
installation
dispatcher requirement 9
preparation 5
steps 9
troubleshooting errors 25
verifying 23
warnings 25
worksheet 7
overview 1
profile
importing 14
overview 1
removal 31
upgrading 14, 29
verification 15
reinstallation 33
RMI Dispatcher 39
SSL communication to the
database 10
supported configurations 2
uninstall 31
upgrading 29
user account 16
zOS UNIX file system 39
adapter installation
overview 1
architecture 1
attributes
adapter action, by
reconciliation 38
restoring 38
suspending 27
by Oracle eBS Adapter action
add 37
change 37
by Oracle eBS Adapter action action
delete 37
descriptions 35
for the adapter 35
authentication for the adapter 12
creating
keystore 10
self-signed certificate authority 10
services 16
truststore 10
custom subforms, deploying 15
database
SSL communication to the
adapter 10
truststore configuration 10
deploying custom subforms 15
directory integrator
connector 1
uninstalling the adapter 31
dispatcher
installation verification 9
upgrading 29
download, software 7
education x
error messages 27
IBM
Software Support x
Support Assistant x
IBM Support Assistant 44
installation
adapter 9
adapter profile 14
first steps 21
language pack 23
roadmap 5
uninstall 31
verification
adapter 23
verify dispatcher 9
worksheet 7
ISA 44
ISIM_HOME definition 41
ITDI_HOME definition 41
JDBC Thin driver
for SSL 13
J
JDBC Thin driver
for SSL 13
keystore for tier configuration 10
knowledge bases 43
L
language pack
installation 23
same for adapters and server 23
logs, trace.log file 14
M
messages
error 27
warning 27
MS-DOS ASCII characters 22
N
notices 49
O
obtaining the JDBC Thin driver 13
online
publications ix
terminology ix
operating system prerequisites 6
Oracle
E-Business Suite Adapter ix
eBS 16
overview 1
P
plan 5
preinstallation roadmap 5
problem-determination x
profile
editing on UNIX or Linux 22
importing 14
publication ix
publications
accessing online ix
list of ix
R
reconciliation 38
removing adapter profiles 31
request attributes 38
restore request 38
restoring accounts
files, changing 23
password requirements 23
RMI dispatcher 1
roadmaps
installation 5
preinstallation 5
© Copyright IBM Corp. 2012, 2014

53