

Oracle® Identity Manager

Readme

Release 9.1.0.2

E14764-06

May 2010

The Oracle Identity Manager release 9.1.0.2 patch set enables you to upgrade to Oracle Identity Manager release 9.1.0.2 from the following releases:

- Oracle Identity Manager release 9.1.0.1
- Oracle Identity Manager release 9.1.0 (running on Oracle Application Server) on which the patch set for Arabic language support has been installed

You can upgrade to release 9.1.0.2 if any one of the following conditions is true:

- You are running Oracle Identity Manager release 9.1.0 on Oracle Application Server and the patch set for Arabic language support has been installed.

Note: Contact Oracle Support for information about the patch set for Arabic language support.

- You are running Oracle Identity Manager release 9.1.0.1 on any application server.

This document contains release notes and installation instructions for the patch set.

This document is divided into the following sections:

- [Section 1, "What's New in Oracle Identity Manager Release 9.1.0.2?"](#)
- [Section 2, "Certified Components"](#)
- [Section 3, "Upgrading to Oracle Identity Manager Release 9.1.0.2"](#)
- [Section 4, "Resolved Issues"](#)
- [Section 5, "Known Issues and Workarounds"](#)
- [Section 6, "Customizations"](#)
- [Section 7, "Related Documents"](#)
- [Section 8, "Documentation Accessibility"](#)

1 What's New in Oracle Identity Manager Release 9.1.0.2?

The following sections discuss new features introduced in Oracle Identity Manager release 9.1.0.2:

- [Section 1.1, "Support for Segregation of Duties \(SoD\)"](#)
- [Section 1.2, "Support for Offline Provisioning"](#)
- [Section 1.3, "Support for Capture and Use of Entitlement Data"](#)

- Section 1.4, "Introduction of the Bulk Load Utility"
- Section 1.6, "Support for Connection Pooling"
- Section 1.7, "Support for the Arabic Language"
- Section 1.8, "Enhanced Support for Integration Between Oracle Role Manager and Oracle Identity Manager"
- Section 1.9, "Additional Changes on the Oracle Identity Manager UIs"
- Section 1.10, "New Scheduled Tasks"
- Section 1.11, "New Reports"
- Section 1.12, "New APIs"
- Section 1.13, "New System Properties"
- Section 1.14, "New Adapters"

1.1 Support for Segregation of Duties (SoD)

In the Oracle Identity Manager implementation of SoD, IT privilege (entitlement) requests submitted by a user are checked and approved by an SoD engine and other users. Multiple levels of system and human checks can be introduced to ensure that even changes to the original request are vetted before they are cleared. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to the user.

See Also: "Segregation of Duties (SoD) in Oracle Identity Manager" in *Oracle Identity Manager Tools Reference* for more information

1.2 Support for Offline Provisioning

In online provisioning, multiple provisioning operations that constitute a provisioning request are performed in sequence. In addition, the provisioning request is treated as a single transaction. This approach could cause performance issues. In addition, there is a higher probability of transaction timeout and, therefore, the entire transaction being rolled back.

In offline provisioning, provisioning operations within a request are converted into JMS messages. There is one JMS message submitted for each resource provisioned to each user. Processing of each JMS message is treated as a single transaction, and it is asynchronous and independent of other JMS messages. Processing of the other messages continues even if one transaction times out. This approach offers better performance and a lower probability of transaction timeout.

The Failed Off-line Provisioning Messages report provides details of failed messages.

The Remove Failed Off-line Messages scheduled task has been introduced to remove failed messages from the database table in which these messages are stored.

See the "Enabling Offline Provisioning" chapter in *Oracle Identity Manager Best Practices Guide* for more information.

1.3 Support for Capture and Use of Entitlement Data

From this release onward, you can mark a child process form field as an entitlement and then enable the capture of data related to the entitlement. By enabling this feature for all resource objects defined in your Oracle Identity Manager installation, you can

generate reports related to entitlements that are available for provisioning and entitlements that have been assigned to users.

See the "Using Entitlement Data" chapter in *Oracle Identity Manager Tools Reference* for more information.

1.4 Introduction of the Bulk Load Utility

The Bulk Load utility is aimed at automating the process of loading large volumes of user and account data into Oracle Identity Manager. It helps reduce the downtime involved in loading data. You can use this utility either immediately after you install Oracle Identity Manager or at any time during the production lifetime of Oracle Identity Manager.

See the "Bulk Load Utility" chapter in *Oracle Identity Manager Tools Reference* for more information.

1.5 Support for Future-Dated Reconciliation Events

Some target systems allow future-dating (effective-dating) of certain user lifecycle events. For example, an administrator on the target system can specify that a user's account must be enabled on 17-April-2009 by setting the Effective End Date to that date for the account. You can configure the Process Deferred Recon Events scheduled task to correctly respond to these future-dated reconciliation events. This scheduled task is described in [Section 1.10, "New Scheduled Tasks"](#). The scheduled task is used in conjunction with the createReconciliationEvent API. This API is listed in [Section 1.12, "New APIs"](#)

1.6 Support for Connection Pooling

Oracle Identity Manager supports connection pooling from this release onward. A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

See Oracle Identity Manager connector documentation for information about using this feature.

1.7 Support for the Arabic Language

Arabic language support has been included in release 9.1.0.2 for Oracle Identity Manager installed on Oracle Application Server. See [Section 3.10, "Applying the Patch for Arabic Language Support"](#) for information about applying this patch set.

1.8 Enhanced Support for Integration Between Oracle Role Manager and Oracle Identity Manager

This section lists the UI changes introduced in release 9.1.0.2.

Features Disabled in Oracle Identity Manager Administrative and User Console

The following features are *disabled* in the Administrative and User Console when the property `XL.OIM-ORM.Integration.Deployed` is set to `true`. These features are disabled when you integrate Oracle Identity Manager with Oracle Role Manager. However, if you do not integrate Oracle Identity Manager and Oracle Role Manager, then those features will still be seen in Oracle Identity Manager.

Note: The disabled features are now available through the Oracle Role Manager Console. See *Oracle Role Manager User's Guide* for more information.

- **User Details**

- Editing group membership details

- **Organizations**

- Creating administrative groups for organizations

- **User Groups**

- Creating user groups
 - Editing or deleting group details of user groups
 - Creating administrative user groups
 - Assigning users or sub groups to user groups
 - Removing members from user groups
 - Assigning and removing access policies to user groups

- **Access Policies**

- If the Access Policy is created through Oracle Role Manager Console, then you cannot edit the following values of Access Policy:

- Resources to be provisioned by this access policy
 - Groups for this access policy

- If the Access Policy is created through Oracle Role Manager Console, then you can view only the following properties:

- Access Policy Details
 - * Name
 - * Description
 - * With Approval
 - * Retrofit Access Policy
 - * Priority
 - Resource Form Data
 - Process Form Data

Note: During reconciliation between Oracle Role Manager and Oracle Identity Manager, only entitlement data in the access policies is sent to Oracle Identity Manager.

- **Resource Management**

Creating resource administrator groups

1.9 Additional Changes on the Oracle Identity Manager UIs

The following changes have been made on the Oracle Identity Manager UIs:

Note: These changes are in addition to the ones described in the ["Enhanced Support for Integration Between Oracle Role Manager and Oracle Identity Manager"](#) section.

- A login page appears when you access the Diagnostic Dashboard home page. You can access the Diagnostic Dashboard by using a URL in the following format:

`http://HOST:PORT/XIMDD`

The account credentials that you use to log in are the same as your OIM User credentials.

- An error page appears when login to the Diagnostic Dashboard fails, or when a user tries to run a script in the Diagnostic Dashboard.
- A LOGOUT link is displayed if you access the Diagnostic Dashboard through the following URL:

`http://<host>:<port>/XIMDD/SystemVerification`

- In the Oracle Identity Manager Design Console, a new field `Future Date` is added in the Reconciliation Manager form.
- A filter is introduced for the Rules in a group for Membership Rule.

1.10 New Scheduled Tasks

The following scheduled tasks have been introduced in this release:

- [Section 1.10.1, "Scheduled Tasks for the SoD Feature"](#)
- [Section 1.10.2, "Scheduled Tasks for Working with Entitlement Data"](#)
- [Section 1.10.3, "Scheduled Tasks for the Offline Provisioning Feature"](#)
- [Section 1.10.4, "Other Scheduled Tasks"](#)

1.10.1 Scheduled Tasks for the SoD Feature

The following scheduled tasks have been introduced along with the SoD feature:

Get SOD Check Results Provisioning

This scheduled task is used to fetch the SOD Check Results if the SOD Engine is asynchronous in nature. For an asynchronous SOD Engine, the SOD Check Results are not available all at the same time. So, this schedule task must be run after the SOD Check has been initiated. It is run only if SOD Check is triggered through Direct Provisioning or Form Edit.

Get SOD Check Results Approval

This scheduled task helps in getting back the SOD Check Results in case of request based provisioning (if SOD Check was initiated during Approval).

Resubmit Uninitiated Provisioning SOD Checks

During direct provisioning, if the SoD check remains in the SODCheckNotInitiated state or SODCheckCompletedWithError state, then you can run the Resubmit Uninitiated Provisioning SOD Checks task to initiate the SoD check. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitiated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state will be completed in the next run of the Get SOD Check Results Provisioning scheduled task.

Resubmit Uninitiated Approval SOD Checks

During request-based provisioning, if the SoD check remains in the SODCheckNotInitiated state or SODCheckCompletedWithError state, then you can run the Resubmit Uninitiated Approval SOD Checks scheduled task to initiate the SoD check. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitiated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state will be completed in the next run of the Get SOD Check Results Approval scheduled task.

1.10.2 Scheduled Tasks for Working with Entitlement Data

The following scheduled tasks have been introduced for working with entitlement data:

Entitlement List

The Entitlement List scheduled task identifies the entitlement attribute from the child process form table and then copies entitlement data from the LKV table into the ENT_LIST table.

Entitlement Assignments

The Entitlement Assignments scheduled task is used for first-time copying of data about assigned entitlements into the ENT_ASSIGN table. This task identifies the entitlement attribute from the child process form table and then copies data about assigned entitlements from the child process form table into the ENT_ASSIGN table. A record created in the ENT_ASSIGN table corresponds to an entitlement assigned to a particular user on a particular target system.

Entitlement Updatations

The Entitlement Updatations scheduled task updates the ENT_ASSIGN table with changes to entitlement assignment data in the child process form tables. Triggers created by the Entitlement Assignments scheduled task copy changes made to entitlement assignment data into a staging table. The Entitlement Updatations scheduled task processes data in the staging table and makes the required changes to data in the ENT_ASSIGN table.

1.10.3 Scheduled Tasks for the Offline Provisioning Feature

The following scheduled tasks have been introduced along with the offline provisioning feature:

Remove Failed Off-line Messages

This scheduled task has been introduced to remove failed messages from the database table in which these messages are stored.

1.10.4 Other Scheduled Tasks

The following scheduled task can be used after reconciliation of user or account data from target systems:

Configuring the Process Deferred Recon Events

Some target systems of Oracle Identity Manager allow effective-dating of certain user lifecycle events, such as hiring and designation changes. In other words, you can set a future date for such a change to a user's record, and the change will take effect on the specified day.

See Also: *Oracle Identity Manager Administrative and User Console Guide* for detailed information about working with scheduled tasks.

The Process Deferred Recon Events scheduled task has been added to support reconciliation of effective-dated reconciliation events. Reconciliation scheduled tasks fetch all modified records into Oracle Identity Manager. The following sequence of steps describes how future-dated events are processed:

Note: It is not mandatory to configure the Process Deferred Recon Events scheduled task.

1. When the Reconciliation Manager encounters a future-dated reconciliation event, it sets the status of the event to `Event Deferred`, if the date value of `Future Date` passed to the API is greater than the `Current System Date` and the `Future Date` column in the database is set to `date passed`.
2. When the Process Deferred Recon Events scheduled task is run, it checks if the date value stored in the database is less than or equal to the `Current System Date`. If yes, then it processes the Recon Event as the existing recon flow and changes the status of the Recon Event accordingly. If not, then it does not perform any action.

1.11 New Reports

The following reports have been introduced in release 9.1.0.2:

Note: These reports are available as part of BI Publisher based reports on Oracle Technology Network. To download the reports bundle:

1. Visit the Oracle Technology Network Web site at http://www.oracle.com/technology/products/id_mgmt/oxp/index.html
 2. Under the Technical Information section, click **Oracle Identity Manager 9.1.0.2 - BI Publisher Reports**.
-
-

Off-line Resource Provisioning Messages

The Off-line Resource Provisioning Messages report provides details of failed messages. This report has been introduced along with the offline provisioning feature.

Entitlement Access List

The Entitlement Access List report lists users who are currently assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements are assigned.

Entitlement Access List History

The Entitlement Access List History report lists users who had been assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements were assigned.

User Resource Entitlement

The User Resource Entitlement report lists the current entitlements of users whom you specify while generating the report. The report displays basic user information and entitlement details.

User Resource Entitlement History

The User Resource Entitlement History report lists details of past entitlements assigned to users whom you specify while generating the report. The report displays basic user information and entitlement details.

1.12 New APIs

Table 1 lists the new application programming interfaces (APIs) that are added in release 9.1.0.2.

Table 1 *New APIs in Release 9.1.0.2*

Interface	API Method	Description
<code>tcAccessPolicyOperationsIntf</code>	<code>public void updateEntitlementToAccessPolicy (long policyKey, long[] entitlementKey) throws tcPolicyNotFoundException, tcAPIException, tcEntitlementNotFoundException</code>	Updates a set of entitlements mapped to an Access Policy. The entitlement data provided should be final as it overrides the existing data.
<code>tcAccessPolicyOperationsIntf</code>	<code>public Thor.API.tcResultSet getMappedEntitlements (long policyKey) throws tcPolicyNotFoundException, tcAPIException</code>	The returned attributes contain the following columns: Entitlements.Resource ID Entitlements.Key Entitlements.Entitlement Entitlements.Entitlement Code Entitlements.Entitlement Valid Flag

Table 1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
tcAccessPolicyOperationsIntf	public void unAssignObjects(long policyKey, long[] objectKeys, boolean removeFormData) throws tcPolicyNotFoundException, tcAPIException, tcBulkException	Cleans up the existing associated form data for objects of an Access Policy.
tcRulesOperationsIntf	tcResultSet findRuleElements(long rulekey) throws tcRuleNotFoundException, tcAPIException	The returned attributes contain the following columns: Rule Designer.RuleElement.Attribute Rule Designer.RuleElement.Attribute Source Rule Designer.RuleElement.Attribute Value Rule Designer.RuleElement.Child Key Rule Designer.RuleElement.Key Rule Designer.RuleElement.Operation Rule Designer.RuleElement.Sequence Rule Designer.RuleElement.User-Defined Form
tcLookupOperationsIntf	public tcResultSet getLookupCodesForDecoded(String psLookupCode, String decodedValues) throws tcAPIException, tcInvalidLookupException	Returns, in the form of a tcResultSet, a list of lookup encoded values with associated decoded values.
tcReconciliationOperationsIntf	public long createReconciliationEvent(String psObjectName, Map poData, boolean pbFinishEvent, java.sql.Date futureDate) throws tcAPIException, tcObjectNotFoundException;	Returns the key for future-dated reconciliation events created for the specified object. The status of these events is EventDeferred.

Table 1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
tcReconciliationOperationsIntf	public long createReconciliationEvent(String psObjectName, Map poData, boolean pbFinishEvent, String psDateFormat, java.sql.Date futureDate) throws tcAPIException, tcObjectNotFoundExcept ion;	Returns the key for future-dated reconciliation events created for the specified object. The status of these events is Event Deferred.
tcReconciliationOperationsIntf	public void updateReconEvent(long rceKey, java.util.Map attributes) throws Thor.API.Exceptions.tc APIException, Thor.API.Exceptions.tc ReconEventNotFoundExce ption, tcAPIException	Updates any attribute of the recon event.
tcGroupOperationsIntf	public Thor.API.tcResultSet findAssignedMembership Rules(java.util.Map searchCriteria) throws Thor.API.Exceptions.tc APIException, tcAPIException	Returns, in the form of a tcResultSet, a list of assigned membership rules of the group. The tcResultSet contains the following column names: <ul style="list-style-type: none"> ■ Groups.Key ■ Groups.Group Name ■ Rule Designer.Key ■ Rule Designer.Name
tcGroupOperationsIntf	public Thor.API.tcResultSet findUnassignedMembersh ipRules(java.util.Map searchCriterias) throws Thor.API.Exceptions.tc APIException, tcAPIException	Returns, in the form of a tcResultSet, a list of unassigned membership rules of the group. The tcResultSet contains the following column names: <ul style="list-style-type: none"> ■ Groups.Key ■ Groups.Group Name ■ Rule Designer.Key ■ Rule Designer.Name ■ Rule Designer.Type
tcEntitlementsOperationsBean	public tcResultSet findEntitlements(Map attributeList)	Returns, in the form of a tcResultSet, a list of entitlements.

Table 1 (Cont.) New APIs in Release 9.1.0.2

Interface	API Method	Description
tcProvisioningOperationsIntf	public tcResultSet findAllOpenProvisioningTasks (Map attributeList , String[] statuses) throws tcAPIException	This method returns a list of all provisioning tasks (and their details) assigned to any user. For displaying the open pending and rejected tasks, the statuses argument filter can be used. The returned object will be a result set with each row having detailed information about each task.
tcFormInstanceOperationsIntf	public void executeSODCheck(long plProcessInstanceKey) throws tcProcessNotFoundExcep tion, tcFormNotFoundExceptio n, tcRequiredDataMissingE xception, tcInvalidValueExceptio n, tcNotAtomicProcessExce ption, tcAPIException	This method initiates the SOD Check by creating SODChecker Task Instance for the process whose instance key is passed as argument.
tcFormInstanceOperationsIntf	public long addProcessFormChildData (long plChildFormDefinitionKey, long plProcessInstanceKey, Map phAttributeList, boolean createHolder, boolean createSODChecker) throw s tcProcessNotFoundExcep tion, tcFormNotFoundExceptio n, tcRequiredDataMissingE xception, tcInvalidValueExceptio n, tcNotAtomicProcessExce ption, tcAPIException	Adds process data to the child form that is associated with an instance of a process in the system. It takes 2 flags for creation of Holder and SODChecker Tasks. Holder Task is used to hold the entitlement task until SODCheck is performed and SODChecker task instantiates the SOD Check (by running the InitiateSODCheck Adapter that must be attached to it).

1.13 New System Properties

The following client-side system properties have been introduced in release 9.1.0.2:

- XL.OIM-ORM.Integration.Deployed

This property is used to determine whether the ORM-OIM integration library is deployed or not. The Oracle Role Manager (ORM) Console governs certain Oracle Identity Manager features, such as creating a group and modifying an access policy.

The default value for this property is `False`.

- `XL.SoDCheckRequired`
This property is used to enable or disable SOD Check.
The default value for this property is `False`.
- `XL.SIL.Home.Dir`
The property must be set to the full path and name of the `SIL_HOME` directory.
The default value for this property is `C : /SIL_HOME`.
- `XL.SoD.Offline.Sync`
If the SoD check remains in the `SODCheckNotInitiated` state or `SODCheckCompletedWithError` state, then you can run one of the following scheduled tasks to initiate the SoD check:
 - Resubmit Uninitiated Provisioning SOD Checks
 - Resubmit Uninitiated Approval SOD Checks
 To enable these scheduled tasks to run automatically at this stage of the process, set the `XL.SoD.Offline.Sync` to `true`. Otherwise, set this system property to `false`. The default value is `true`.

1.14 New Adapters

`InitiateSODCheck`

This adapter initiates the SOD Check. It must be attached to an `SODChecker` Task (that is, any Task whose name is prefixed by 'SODChecker').

2 Certified Components

For information about certified application servers and languages, refer to the following sections:

- [Section 2.1, "Certified Application Servers"](#)
- [Section 2.2, "Certified Languages"](#)

For information about other certified components, refer to the certification matrix on the following page:

http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html

2.1 Certified Application Servers

Note: There is no change in application server certification from release 9.1.0.1 to release 9.1.0.2.

Oracle Identity Manager release 9.1.0.2 is certified for the following application servers:

- IBM WebSphere Application Server 6.1.0.21 and later fix packs (that is, 6.1.0.21 and later)

Note: Stop the IBM WebSphere Application Server. Upgrade IBM WebSphere Application Server and Application client to 6.1.0.21. Restart IBM WebSphere Application Server 6.1.0.21.

- JBoss Application Server 4.2.3 GA
- Oracle Application Server 10.1.3.3 (Upgrade patch 10.1.3.3 applied on top of the base package bundled in Oracle SOA Suite 10g release 10.1.3.1)

Note:

- To update Oracle Application Server JDKs for DST 2007 compliance, you must use the appropriate time zone update utility from your JDK vendor. For information about using JDK vendor time zone update utilities, refer to Note 414153.1 on the My Oracle Support Web site.

You can access the My Oracle Support Web site at

<http://metalink.oracle.com/>

- For the production deployment of Oracle Identity Manager running on Oracle Application Server, you must configure Oracle AQ as the JMS provider. Because of Bug 6718332, Oracle AQ-based JMS cannot be configured on Microsoft Vista at this time. Microsoft Vista is, therefore, supported for only nonclustered development environments with file-based JMS. To update Oracle Application Server JDKs for DST 2007 compliance, you must use the appropriate time zone update utility from your JDK vendor. For information about using JDK vendor time zone update utilities, refer to Note 414153.1 on the My Oracle Support Web site.

-
-
- Oracle WebLogic Server release 10.3.0, 10.3.1 and later

2.2 Certified Languages

Oracle Identity Manager release 9.1.0.2 is certified for the following languages:

- Arabic

Note: The Arabic language is supported only on an Oracle Identity Manager installation running on Oracle Application Server.

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German

- Italian
- Japanese
- Korean
- Portuguese (Brazilian)

The combination of the Portuguese (Brazilian) locale and IBM WebSphere Application Server is not supported. For more information, refer to APAR IZ01077 on the IBM WebSphere Application Server Web site.

- Spanish

See Also: *Oracle Identity Manager Globalization Guide* for detailed information about Oracle Identity Manager globalization support

3 Upgrading to Oracle Identity Manager Release 9.1.0.2

To upgrade from Oracle Identity Manager release 9.1.0.1 to release 9.1.0.2, perform the following procedures:

Note:

- Before you begin the upgrade, extract the contents of the Oracle Identity Manager release 9.1.0.2 patch set to a temporary directory on the computer on which Oracle Identity Manager is installed. This temporary directory is referred to as *PATCH* in this document.
 - You can skip any section that does not apply to your operating environment.
-
-

- [Section 3.1, "Addressing Prerequisites for the Upgrade"](#)
- [Section 3.2, "Deploying or Upgrading to Oracle Identity Manager Release 9.1.0.2 on Oracle WebLogic Server Release 10.3.1 or Later"](#)
- [Section 3.3, "Upgrading the Oracle Identity Manager Database"](#)
- [Section 3.4, "Upgrading Oracle Identity Manager"](#)
- [Section 3.5, "Upgrading the Oracle Identity Manager Design Console"](#)
- [Section 3.6, "Upgrading the Oracle Identity Manager Remote Manager"](#)
- [Section 3.7, "Redeploying the Diagnostic Dashboard"](#)
- [Section 3.8, "Redeploying the SPML Web Service"](#)
- [Section 3.9, "Enabling the Integration with Oracle Role Manager"](#)
- [Section 3.10, "Applying the Patch for Arabic Language Support"](#)
- [Section 3.11, "Reapplying Customizations and Compiling Adapters"](#)

3.1 Addressing Prerequisites for the Upgrade

Before you begin the upgrade procedure, ensure that the following prerequisites are addressed:

- Create backups of the Oracle Identity Manager and application server installation directories.
- Create a backup of the Oracle Identity Manager database.
- Ensure that there are no pending JMS messages to be consumed.

3.2 Deploying or Upgrading to Oracle Identity Manager Release 9.1.0.2 on Oracle WebLogic Server Release 10.3.1 or Later

Note: This section is meant for users who want to deploy or upgrade to Oracle Identity Manager release 9.1.0.2 on Oracle WebLogic Server release 10.3.1 or later. Skip this section if you do *not* want to use Oracle Identity Manager release 9.1.0.2 on Oracle WebLogic Server release 10.3.1 or later.

If you want to deploy or upgrade to Oracle Identity Manager release 9.1.0.2 on Oracle WebLogic Server release 10.3.1 or later, then:

1. If you have not already installed Oracle Identity Manager release 9.1.0.1 on Oracle WebLogic Server release 10.3.0, then install it. See *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server for Release 9.1.0.1* for instructions.
2. Upgrade from Oracle WebLogic Server release 10.3.0 to release 10.3.1 or later as follows:

Note: Read the steps of the procedure before you begin performing it. See Oracle WebLogic Server documentation for detailed instructions.

- a. Set the Java environment variables and the PATH environment variable for the existing Oracle WebLogic Server release 10.3.0 installation.
- b. Stop the application server. If it is a clustered installation, then stop the admin and managed nodes.
- c. In a command window, change to the following directory:
`WEBLOGIC_HOME/utils/bsu`
- d. Run the bsu utility by entering the following command:
 - For Microsoft Windows: `bsu.cmd -gui`
 - For UNIX: `./bsu.sh -gui`

You are prompted to enter your My Oracle Support credentials so that the utility can download the upgrade package.

Performing an offline upgrade is an alternative to the online upgrade. If you want to perform an offline upgrade, see Note 1074946.1 on the My Oracle Support Web site for basic instructions. The Web site can be accessed at:

<http://support.oracle.com>

- e. You might be prompted to specify whether you want to upgrade the bsu utility. Accept the upgrade option. After the bsu utility is upgraded, it restarts itself and you can then proceed with the upgrade of the application server.
 - f. Proceed with the upgrade. During the procedure, select the maintenance pack corresponding to the release of the application server (for example, Maintenance Pack 10.3.2) that you are using and install it over the existing *WEBLOGIC_HOME* directory of the existing release 10.3.0 installation.
3. After the upgrade, restart Oracle WebLogic Server.
 4. Upgrade the Oracle Identity Manager database to the release 9.1.0.2 level. [Section 3.3, "Upgrading the Oracle Identity Manager Database"](#) provides instructions.
 5. Upgrade from Oracle Identity Manager release 9.1.0.1 to release 9.1.0.2. [Section 3.4, "Upgrading Oracle Identity Manager"](#) provides instructions.
 6. From [Section 3.5, "Upgrading the Oracle Identity Manager Design Console"](#) onward, follow the instructions given in this document.

3.3 Upgrading the Oracle Identity Manager Database

The procedure to upgrade Oracle Identity Manager database depends on the database product you are using. The following sections describe the procedure to upgrade Oracle Identity Manager database on Microsoft SQL Server and Oracle Database:

- [Section 3.3.1, "Upgrading Oracle Identity Manager Database on Microsoft SQL Server"](#)
- [Section 3.3.2, "Upgrading Oracle Identity Manager Database on Oracle Database"](#)
- [Section 3.3.3, "Loading Metadata into the Database"](#)
- [Section 3.3.4, "Loading E-Mail Templates"](#)
- [Section 3.3.5, "Using the Oracle Identity Manager Database Validator"](#)

3.3.1 Upgrading Oracle Identity Manager Database on Microsoft SQL Server

To upgrade Oracle Identity Manager database on Microsoft SQL Server 2005:

1. Create a backup of the database.
2. Open a command prompt from the Microsoft SQL Server computer, and then run the following script:

```
PATCH\db\SQLServer\Scripts\oim_db_upg_9101_to_9102.bat
SERVER_NAME[\INSTANCE_NAME] DB_NAME DB_USER_NAME DB_USER_PASSWORD
PATCH\db\SQLServer\Scripts\
```

3. Compile the stored procedures as follows:

- a. In a text editor, open the following BAT file:

```
PATCH\db\SQLServer\StoredProcedures\compile_all_XL_SP.bat
```

- b. For every stored procedure listed in the Sequential Lists section of the `compile_all_XL_SP.bat` file, replace the string `@sysuser` with the database user name. This must be done because Microsoft SQL Server requires functions invoked from a stored procedure to be qualified by the database user name (owner).

Note: Ensure that you replace the entire @sysuser string, including the at sign (@).

- c. Run the following script:

```
PATCH\db\SQLServer\StoredProcedures\compile_all_XL_SP.bat  
SERVER_NAME[\INSTANCE_NAME] DB_NAME DB_USER_NAME DB_USER_PASSWORD  
PATCH\db\SQLServer\StoredProcedures\
```

4. If you are not using the Audit and Compliance Module and if you want to enable it for release 9.1.0.2, then run the following script:

```
PATCH\db\SQLServer\Scripts\SQLServer_Enable_XACM.bat  
SERVER_NAME[\INSTANCE_NAME] DB_NAME DB_USER_NAME DB_USER_PASSWORD  
PATCH\db\SQLServer\Scripts\
```

5. Load the metadata into the Oracle Identity Manager database. See "[Loading Metadata into the Database](#)" for more information about loading the metadata into the database.
6. Enable XA transactions for MSDTC as follows:
- On the computer on which Microsoft SQL Server 2005 is running, click **Start**, **Administrative Tools**, and **Component Services**.
 - Expand the Component Service tree to locate the computer, right-click the computer name, and then select **Properties**.
 - On the MSDTC tab, click **Security Configuration**.
 - Under Security Settings, select **Enable XA Transactions**.
 - Click **OK**, and then save the changes.

3.3.2 Upgrading Oracle Identity Manager Database on Oracle Database

To upgrade Oracle Identity Manager database on Oracle Database:

1. Back up the existing database.

Use the export/backup utility provided with the database to perform a complete backup of the database.

A production database backup includes, but is not limited to, complete export or backup of the Oracle Identity Manager release 9.1.0 or 9.1.0.1 database instance to ensure that, if required, the database can be restored to its original state.

2. If you are using Oracle Database 11g release 11.1.0.7, then apply the following patches:
- 7628358
 - 7598314
 - 7614692
3. Enable execute permissions on the scripts in the *PATCH* directory.
4. To upgrade the database schema from release 9.1.0 to release 9.1.0.2, run the oim_db_upg_910_to_9102.sh (or oim_db_upg_910_to_9102.bat) script on the system on which the release 9.1.0 database is installed.

The command-line usage for the Oracle oim_db_upg_910_to_9102 script is as follows:

```
PATCH/db/oracle/Scripts/oim_db_upg_910_to_9102.sh (or  
oim_db_upg_910_to_9102.bat) ORACLE_SID ORACLE_HOME DB_USER_NAME  
DB_USER_PASSWORD DIRECTORY_IN_WHICH_DB_UPGRADE_ZIP_FILE_IS_EXTRACTED
```

5. To upgrade the database schema from release 9.1.0.1 to release 9.1.0.2, run the oim_db_upg_9101_to_9102.sh (oim_db_upg_9101_to_9102.sh) script on the system on which the release 9.1.0.1 database is installed.

The command-line usage for the script is as follows:

```
PATCH/db/oracle/Scripts/oim_db_upg_9101_to_9102.sh (or  
oim_db_upg_9101_to_9102.bat) ORACLE_SID ORACLE_HOME DB_USER_NAME  
DB_USER_PASSWORD DIRECTORY_IN_WHICH_DB_UPGRADE_ZIP_FILE_IS_EXTRACTED
```

6. If you are not using the Audit and Compliance Module and if you want to enable it for release 9.1.0.2, perform the following steps as appropriate for your database
 - a. Log in to SQL*Plus with the credentials of the Oracle Identity Manager database schema owner.
 - b. Run the *PATCH/db/oracle/Scripts/Oracle_Enable_XACM.sql* script.
7. Load metadata into the Oracle Identity Manager database. See "[Loading Metadata into the Database](#)" for more information.

3.3.3 Loading Metadata into the Database

To load metadata into the database, you must first make the required changes in one of the following files:

Note: Run the script on the computer on which Oracle Identity Manager is installed.

If you are not using the Audit and Compliance Module, then copy one of the following files:

- LoadXML.bat
- LoadXML.sh

If you are using the Audit and Compliance Module, then copy one of the following files:

- LoadXML_XACM.bat
- LoadXML_XACM.sh

This file is located in the *PATCH/db/Metadata* directory.

To load metadata into the database:

Note: You must run the script on the Oracle Identity Manager host computer.

1. Open the LoadXML or LoadXML_XACM script in a text editor.
Set the value of the JAVA_HOME variable.

2. Depending on the operating system on which Oracle Identity Manager is deployed:

■ **For Microsoft SQL Server on Microsoft Windows**

a. In the LoadXML or LoadXML_XACM file, remove REM from the following lines:

```
REM SET SQL_SERVER_DRIVER_DIR=
```

b. Assign the path to the SQL Server driver directory that contains the sqljdbc.jar file:

```
SET SQL_SERVER_DRIVER_DIR=PATH_TO_SQL_DRIVER
```

c. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET XLHOME=
```

d. Specify the full path of the Oracle Identity Manager installation directory.

```
SET XLHOME=OIM_HOME/xellerate
```

Specify the full path up to the xellerate directory.

■ **For Oracle Database on Microsoft Windows**

a. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET ORACLE_DRIVER_DIR=
```

b. Assign the path to the Oracle driver directory containing the Oracle JDBC drivers:

```
SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
```

c. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET JDBC_DRIVER_VERSION=
```

d. Specify name of the Oracle JDBC driver. For example, SET JDBC_DRIVER_VERSION=ojdbc14.jar.

e. In the LoadXML or LoadXML_XACM file, remove REM from the following line:

```
REM SET XLHOME=
```

f. Specify the fullpath for OIM install directory. For example, SET XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY. Specify the path up to the Xellerate directory.

■ **For Oracle Database on UNIX:**

a. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

```
#ORACLE_DRIVER_DIR=  
#export ORACLE_DRIVER_DIR
```

b. Assign the path to the JDBC driver for Oracle, so that the line is similar to the following:

```
ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
export ORACLE_DRIVER_DIR
```

c. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

```
#JDBC_DRIVER_VERSION=
#export JDBC_DRIVER_VERSION
```

d. Specify name of the Oracle JDBC driver. For example,
JDBC_DRIVER_VERSION=ojdbc14.jar.

e. In the LoadXML or LoadXML_XACM file, uncomment the following lines:

```
#XLHOME=
#export XLHOME
```

f. Specify the full path for OIM install directory. For example,
XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY. Mention the path up to the Xellerate directory.

3. Open a command prompt or console and run the LoadXML or LoadXML_XACM script. While running the script, you must enter values for the following parameters (in the given order):
 - **For Microsoft SQL Server:**
 - JDBC URL. For example: `jdbc:sqlserver://DB_HOST_IP:PORT` (replace `DB_HOST_IP` with the IP address of the database host and replace `PORT` with the port number of the database host)
 - Database name
 - Database user name
 - Password
 - **For Oracle Database:**
 - JDBC URL. For example: `jdbc:oracle:thin:@DB_HOST_IP:PORT:SID` (replace `DB_HOST_IP` with the IP address of the database host, `PORT` with the port number of the database host, and `SID` with the database user ID)
 - Database user name
 - Password

3.3.4 Loading E-Mail Templates

To load e-mail templates:

1. Open the `PATCH/db/metadata/LoadXLIF` script in a text editor.
Set the value of the `JAVA_HOME` variable.
2. Depending on the operating system on which Oracle Identity Manager is deployed:

For Microsoft SQL Server on Microsoft Windows

- a. In the LoadXLIF file, remove REM from the following line:

```
REM SET SQL_SERVER_DRIVER_DIR=
```

- b. Assign the path to the Microsoft SQL Server driver directory that contains the `sqljdbc.jar` file:

```
SET SQL_SERVER_DRIVER_DIR=PATH_TO_SQL_DRIVER
```

- c. In the LoadXLIF file, remove REM from the following line:

```
REM SET XLHOME=
```

- d. Specify the full path of the Oracle Identity Manager installation directory.

```
SET XLHOME=OIM_HOME/xellerate
```

Note: Specify the full path up to the xellerate directory.

For Oracle Database on Microsoft Windows:

- a. In the LoadXLIF file, remove REM from the following line:

```
REM SET ORACLE_DRIVER_DIR=
```

- b. Set the path to the Oracle Database driver directory containing the Oracle JDBC drivers:

```
SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
```

- c. Specify the name of the Oracle JDBC driver. For example:

```
SET JDBC_DRIVER_VERSION=ojdbc14.jar.
```

- d. In the LoadXLIF file, remove REM from the following line:

```
REM SET XLHOME=
```

- e. Specify the full path of the Oracle Identity Manager installation directory. For example:

```
SET XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY.
```

Note: Specify the full path up to the xellerate directory.

For Oracle Database on UNIX:

- a. In the LoadXLIF file, uncomment the following lines:

```
#ORACLE_DRIVER_DIR=  
#export ORACLE_DRIVER_DIR
```

- b. In the LoadXLIF file, uncomment the following lines:

```
#XLHOME=  
#export XLHOME
```

- c. Specify the full path of the Oracle Identity Manager installation directory. For example:

```
XLHOME=PATH_TO_ORACLE_IDENTITY_MANAGER_INSTALLATION_DIRECTORY
```

Note: Specify the full path up to the xellerate directory.

3. Open a command prompt or console, and run the LoadXLIF script. While running the script, you must enter values for the following parameters (in the given order):

For Microsoft SQL Server:

- JDBC URL

For example: `jdbc:sqlserver://DB_HOST_IP:PORT`

Replace *DB_HOST_IP* with the IP address of the database host, and replace *PORT* with the port number.

- Database name
- Database user name
- Password
- AUDITCOMPLIANCE

For Oracle Database:

- JDBC URL. For example: `jdbc:oracle:thin:@DB_HOST_IP:SID`

Replace *DB_HOST_IP* with the IP address of the database host, *PORT* with the port number of the database host, and *SID* with the database user ID.

- Database user name
- Password
- AUDITCOMPLIANCE

3.3.5 Using the Oracle Identity Manager Database Validator

The Oracle Identity Manager Database Validator is a command-line interface (CLI) utility that compares objects of two databases and generates a report of the missing and mismatched objects in the destination database.

You can also use this utility to verify an upgrade that you perform.

The Oracle Identity Manager Database Validator compares objects of a standard Oracle Identity Manager schema or a customized Oracle Identity Manager database (source) with a destination database that you specify.

The utility gathers source database details in a table. This information is the standard for comparison. For Oracle Database, the information is saved in a file that is created by the database export utility.

In upgrade scenarios, you can use this utility to verify an upgrade that you perform. You can compare the upgraded Oracle Identity Manager database with the provided standard dump (as source dump). This is to verify the success of Oracle Identity Manager database upgrade after the upgrade patch is applied.

Scenario: You upgrade your Oracle Identity Manager installation from release x.x.1 to release x.x.2 by using a standard upgrade package. Oracle Identity Manager Database Validator identifies the missing and mismatched objects, if any, after the upgrade has been completed.

3.3.5.1 Location and Components The Oracle Identity Manager Database Validator files are at the following location:

Oracle Database

PATCH/db/oracle/Utilities/OIMDBValidator

Microsoft SQL Server

PATCH/db/SQLServer/Utilities/OIMDBValidator

All Oracle Identity Manager Database Validator files are located in the OIMDBValidator directory.

Table 2 provides information about the files that are part of the Oracle Identity Manager Database Validator.

Table 2 Files of the Oracle Identity Manager Database Validator

File	Description
oim_ddl_create_oim_src_db.sql	Creates the oim_src_db table.
oim_dml_populate_oim_src_db.sql	Populates the oim_src_db table with metadata details.
oim_dml_src_do_counts.sql	Takes the row count of Oracle Identity Manager standard tables. This file is optional and is based on your inputs.
If Source is a standard database, then: oim_std_src_db.dmp	If Source is a standard/vanilla database, then the standard dump files is named oim_std_src_db.dmp. For a successful standard vanilla installation, a standard dump accompanies the utility. This standard file for Oracle Database is available at the following location: PATCH/db/oracle/Utilities/OIMDBValidator\SrcInfo This standard file for Microsoft SQL Server is available at the following location: PATCH/db/SQLServer/Utilities/OIMDBValidator\SrcInfo
If Source is a customized database, then: oim_src_db.dmp	You can opt to generate the dump file on your own. This file is created when you want to create a dump file from a source Oracle Identity Manager database of your choice. It is named oim_src_db.dmp, and for Oracle Database, it is available at the following location: For Oracle Database: PATCH/db/oracle/Utilities/OIMDBValidator\SrcInfo For Microsoft SQL Server: PATCH/db/SQLServer/Utilities/OIMDBValidator\SrcInfo
oim_dml_check_oim_version.sql	Selects the version from the oim_src_db table and compares it with the version of the XSD table of the Destination Oracle Identity Manager schema.
oim_ddl_create_oim_dest_db.sql	Creates the oim_dest_db table in the destination Oracle Identity Manager database. This file is used to store the data dictionary information of Oracle Identity Manager.
oim_dml_populate_oim_dest_db.sql	Populates the oim_dest_db table with metadata details.

Table 2 (Cont.) Files of the Oracle Identity Manager Database Validator

File	Description
oim_dml_dest_do_counts.sql	Counts the number of records in the Oracle Identity Manager standard tables. This file is optional and is based on your input.
oim_db_compare.sql	This main comparison script creates a comparison report named <code>COMPARISON_SUMMARY_YYYY_MM_DD_HH_MI.log</code> that lists details of the missing or mismatched objects and the row count difference if any.
oim_ddl_drop_oim_src_dest_db.sql	Drops the tables that are created at the destination. This file is optional and is based on your input.
oim_db_validator.bat (Microsoft Windows)	Runs the utility.
oim_db_validator.sh (UNIX and Linux)	
oim_db_input.bat (Microsoft Windows)	The <code>oim_db_validator.bat</code> file calls the <code>oim_db_input.bat</code> file to get the user input and validate the provided information.
oim_db_input.sh (UNIX and Linux)	The <code>oim_db_validator.sh</code> file calls the <code>oim_db_input.sh</code> file to get the user input and validate the provided information.

3.3.5.2 Oracle Identity Manager Database Validator Functionality To use the Database Validator utility, run the following script:

- On Microsoft Windows: `oim_db_validator.bat`
- On UNIX: `oim_db_validator.sh`

After you run the script, a log file is generated with the following name:

For Microsoft Windows:

- If the utility runs without error:
`oim_db_validator_YYYY_MM_DD_HH_MM.log`
- In case of error: `oim_db_validator_err_YYYY_MM_DD_HH_MM.log`

For UNIX:

- If the utility runs without error:
`oim_db_validator_YYYY_MM_DD_HH_MM.log`
- In case of error: `oim_db_validator_err_YYYY_MM_DD_HH_MM.log`

Authentication

When you run the script, you are prompted to enter the following information:

- Oracle Home/SQL Server name
- Database Name
- Database User name
- Database Password

The utility permits only three connection attempts.

Functionality

The following options are available:

- **Collect Details about the Source Oracle Identity Manager Database:**

Enter **1** to select this option.

Select this option to collect details of a specific source.

The utility generates a .dmp file that is named based on your input of whether or not the source is a standard Oracle Identity Manager installation.

- **For standard Oracle Identity Manager installation:** The file is named as follows:

- For Oracle Database: oim_std_src_db.dmp
- For Microsoft SQL Server: oim_std_src_db.bcp

This file is shipped along with the utility and is available in the following directory:

- For Oracle Database:
PATCH/db/oracle/Utilities/OIMDBValidator\SrcInfo
- For Microsoft SQL Server:
PATCH/db/SQLServer/Utilities/OIMDBValidator\SrcInfo

You can use this file for comparison or upgrade verification.

- **For nonstandard Oracle Identity Manager installation:** The file is named as follows:

- For Oracle Database: oim_std_src_db.dmp
- For Microsoft SQL Server: oim_std_src_db.bcp

- **Compare Source Oracle Identity Manager Database with a Destination Oracle Identity Manager Database:**

Enter **2** to select this option.

Choose either to compare against a standard dump or a user-created dump for a specific source:

- To compare against a standard dump, copy oim_std_src_db.dmp (or oim_std_src_db.bcp) from SourceMetadataDump910 to SrcInfo. If SrcInfo is not already available, then create a new directory. The oim_std_src_db.dmp (or oim_std_src_db.bcp) file is a dump of an Oracle Identity Manager release 9.1.0 vanilla installation.

Note: If the comparison with the standard dump indicates any difference, then contact Oracle support.

- To compare against a user-created dump, copy your dump file to SrcInfo. The name of the dump file must be oim_src_db.dmp or oim_src_db.bcp.

You have options for choosing the source for comparison, whether to calculate the number of rows in the destination Oracle Identity Manager database tables, or to drop the comparison tables.

- **Exit:** Enter **3** to select this option.

Choose this option to close the utility.

3.3.5.3 Sample Comparison Summary Report The following is a sample summary report of the Database Validator utility:

```
#####
#####          R E P O R T          #####
#####
Start Time (hh:mi:ss:mmm) : 15:09:39:370
=====
===== S U M M A R Y =====
=====
OIM OBJECT TYPE SOURCE      DESTINATION      COMPARE STATUS
-----
TABLE                   6                5 1 TABLE MISSING
COLUMN                  26              23 3 COLUMNS MISSING
PK                      6                5 1 PKS MISSING
PK COL                  7                6 1 PK COLS MISSING
FK                      1                0 1 FKS MISSING
FK COL                  1                0 1 FK COLS MISSING
U INDEX                 2                2 SUCCESSFUL
UIDX COL                5                5 SUCCESSFUL
NU INDEX                1                1 SUCCESSFUL
NUIDX COL               1                1 SUCCESSFUL
VIEW                   1                1 SUCCESSFUL
PROCEDURE               1                1 SUCCESSFUL
FUNCTION                1                1 SUCCESSFUL
TRIGGER                 1                1 SUCCESSFUL

===== DETAILS OF
DIFFERENCES =====
##### MISSING OBJECTS #####

MISSING OBJECT'S NAME      MISSING OBJECT'S TYPE
-----
AAP                        TABLE
PK_AAP                     PK
FK_AAD_FK_AAD_AC_ACT      FK

#####MIS-MATCHEDOBJECTS #####
*****
MISSING TABLE COLUMNS
*****
OBJECT NAME      OBJECT TYPE PARENT OBJECT      PARENT OBJECT TYPE DATATYPE
COLUMN LENGTH ISNULL
-----
AAP_KEY          COLUMN     AAP                TABLE          numeric
9 NO
ACT_KEY          COLUMN     AAP                TABLE          numeric
9 NO
AAP_VALUE        COLUMN     AAP                TABLE          varchar
200 YES

*****
COLUMN DETAILS OF PRIMARY KEYS, FOREIGN KEYS & INDEXES
*****
OBJECT NAME      OBJECT TYPE PARENT OBJECT      PARENT OBJECT TYPE COLUMN
```

```

POSITION CHILD TABLE          CHILD TABLE COLUMN
-----
AAP_KEY          PK COL      PK_AAP          PK
1
ACT_KEY          FK COL      FK_AAD_FK_AAD_AC_ACT FK
1 ACT          ACT_KEY

===== SEED METADATA
COMPARISION =====
NO DIFFERENCES FOUND.

End Time (hh:mi:ss:mmm) : 15:09:39:387

```

3.4 Upgrading Oracle Identity Manager

Note:

It is assumed that you have already upgraded the database by performing the procedure described earlier in this document.

Do not attempt to upgrade to release 9.1.0.2 from any other previous Oracle Identity Manager release.

The procedure to upgrade from release 9.1.0 or release 9.1.0.1 to release 9.1.0.2 is divided into the following sections:

- [Section 3.4.1, "Copying Files"](#)
- [Section 3.4.3, "Upgrading Oracle Identity Manager on Oracle WebLogic Server"](#)
- [Section 3.4.4, "Upgrading Oracle Identity Manager on JBoss Application Server"](#)
- [Section 3.4.5, "Upgrading Oracle Identity Manager on IBM WebSphere Application Server"](#)
- [Section 3.4.6, "Upgrading Oracle Identity Manager on Oracle Application Server"](#)

3.4.1 Copying Files

Perform the following steps:

1. Create a backup of the contents of the *OIM_HOME/xellerate* directory.
2. Copy the files listed in [Table 3](#).

Note:

For a clustered installation of Oracle Identity Manager, copy all the files from the *PATCH* directory to the cluster members.

If you want to enable the SoD feature introduced in this release, then you may have to copy additional files. For detailed instructions on enabling the SoD feature, see the "Segregation of Duties (SoD) in Oracle Identity Manager" chapter in *Oracle Identity Manager Tools Reference*.

Table 3 Files to Be Copied from the Deployment Package

Copy Files From	Copy Files To
PATCH/xellerate/lib	OIM_HOME/xellerate/lib
PATCH/xellerate/webapp	OIM_HOME/xellerate/webapp
PATCH/xellerate/DDTemplates	OIM_HOME/xellerate/DDTemplates
<p>Note: If you plan to run Oracle Identity Manager on Oracle WebLogic Server release 10.3.1 or later, then do <i>not</i> copy the DDTemplates directory. For this application server, instructions are provided later in this document.</p>	
PATCH/xellerate/ext	OIM_HOME/xellerate/ext
PATCH/xellerate/customResources	OIM_HOME/xellerate/customResources
<p>Note: If you have modified any of the properties files on your Oracle Identity Manager installation, then create a backup of those files before you overwrite the files with the ones from the PATCH directory. After you copy the files, make the same modifications in the newly copied files.</p>	
PATCH/xellerate/GTC	OIM_HOME/xellerate/GTC
PATCH/xellerate/bin	OIM_HOME/xellerate/bin
Copy the following files from the PATCH/xellerate/setup directory:	OIM_HOME/xellerate/setup
<ul style="list-style-type: none"> ■ setup ■ If you are upgrading from release 9.1.0 with the Arabic language patch set applied, then copy the following files: <ul style="list-style-type: none"> - UpgradeAttestation - UpgradeAttestation.sh (or UpgradeAttestation.bat) ■ If you are using Oracle Application Server, then copy the oc4j-setup file. ■ If you are using IBM WebSphere Application Server, then copy the following files: <ul style="list-style-type: none"> - websphereCheckParameter - WebSphereCreateDataSource.jacl - websphere-setup 	
PATCH/xellerate/SPMLWS	OIM_HOME/xellerate/SPMLWS
PATCH/config	OIM_HOME/xellerate/config

3. The setup directory is in the OIM_HOME directory. You must ensure that the name of the setup directory is in lowercase letters, and not Setup.
4. If you are upgrading from release 9.1.0, then run the UpgradeAttestation script as follows:
 - a. Open the following script files in a text editor:

On Microsoft Windows:

```
OIM_HOME\xellerate\setup\UpgradeAttestation.bat
```

On UNIX:

```
OIM_HOME/xellerate/setup/UpgradeAttestation.sh
```

- b.** Set the path of the JAVA_HOME directory in the file.

If there are spaces in the names of any directory in JAVA_HOME path, then enclose the directory name in double quotation marks as shown in the following example:

```
JAVA_HOME=C:\ "program files" \Java\jdk1.6.0_11
```

- c.** Save and close the file.
- d.** Run one of the following commands:

On Microsoft Windows:

```
OIM_HOME\xellerate\setup\UpgradeAttestation.bat JDBC_DRIVER  
DB_URL OIM_DB_USERNAME OIM_DB_PASSWORD
```

On UNIX:

```
OIM_HOME/xellerate/setup/UpgradeAttestation.sh JDBC_DRIVER DB_URL  
OIM_DB_USERNAME OIM_DB_PASSWORD
```

In this command:

- Replace *JDBC_DRIVER* with the name of the JDBC driver.
- Replace *DB_URL* with the URL for the database.
- Replace *OIM_DB_USERNAME* with the user name for the database.
- Replace *OIM_DB_PASSWORD* with the password for the database

On Microsoft SQL Server, the semicolon (;) and equal sign (=) characters are treated as delimiters. If you are passing arguments with these characters from the command line, then enclose the arguments in double quotes. For example, when running UpgradeAttestation.bat, pass the arguments as shown in the following example:

```
UpgradeAttestation.bat com.microsoft.jdbc.sqlserver.SQLServerDriver  
"jdbc:microsoft:sqlserver://localhost:1433;DatabaseName=XELL;SelectMethod=C  
ursor" user password
```

- 5.** Update the GenerateSnapShot script as follows:

- a.** Create backups of the existing GenerateSnapShot files from the *OIM_HOME/xellerate/bin* directory:

```
GenerateSnapshot.bat
```

```
GenerateSnapshot.sh
```

```
GenerateGPASnapshot.bat
```

```
GenerateGPASnapshot.sh
```

- b.** Copy the GenerateSnapShot files from the *PATCH/xellerate/bin* directory to the *OIM_HOME/xellerate/bin* directory.
- c.** In the *OIM_HOME/xellerate/bin* directory, open the new GenerateSnapShot.sh or GenerateSnapShot.bat in a text editor.

- d. In the file, search for the lines containing the following text:


```
APP_SERVER=@appserver
APP_SERVER_HOME=@app_server_home
JAVA_HOME=@jdk_loc
Profile_Name=@profile_name
```
 - e. Replace the @appserver, @appserver, @app_server_home, @jdk_loc, and @profile_name placeholders with actual values from the backup copy of the GenerateSnapShot file.
 - f. If you are using Microsoft SQL Server, then search for SQL_SERVER_DRIVER_DIR in the file and replace it with the full path of the Microsoft SQL Server driver directory.
 - g. Save and close the file.
6. If you are using Microsoft SQL Server, then copy the sqljdbc.jar file to the lib directory of the application server.
- For a nonclustered installation in JBoss Application Server:


```
JBOSS_HOME\server\default\lib
```

 For a clustered installation in JBoss Application Server:


```
JBOSS_HOME\server\all\lib
```
 - For Oracle WebLogic Server:


```
DOMAIN_HOME\lib
```

Note: For a clustered installation of Oracle Identity Manager, copy `DOMAIN_HOME\lib\` on all the nodes.

- For IBM WebSphere Application Server:


```
WAS_HOME\profiles\<ProfileName>\lib\
```

Note: For a clustered installation of Oracle Identity Manager, copy `WAS_HOME\profiles\<ProfileName>\lib\` on all the nodes.

3.4.2 Modifying the FormMetaData.xml File

Note: The steps described in this section are part of the procedure required to implement the offline provisioning feature. See "[Support for Offline Provisioning](#)" on page -2 for more information about this feature. Create a backup of the existing customized FormMetaData.xml and reapply the changes.

Modify the FormMetaData.xml as follows:

Note: In a clustered environment, perform this step on all nodes of the cluster.

1. Open the FormMetaData.xml file in a text editor. This file is in the *OIM_HOME*/config directory.
2. In the Form name="5" element of the FormMetaData.xml file, add the lines highlighted bold font in the following code block:

```

<Form name="5">
  <!-- Resource Name -->
  <AttributeReference editable="true"
optional="false">-502</AttributeReference>
  <!-- Description -->
  <AttributeReference editable="true"
optional="false">-503</AttributeReference>
  <!--Type-->
  <AttributeReference editable="true"
optional="true">-504</AttributeReference>
  <!-- Target -->
  <AttributeReference editable="true"
optional="true">-505</AttributeReference>
  <!-- Auto Prepopulate -->
  <AttributeReference editable="true"
optional="true">-506</AttributeReference>
  <!-- Allow Multiple -->
  <AttributeReference editable="true"
optional="true">-507</AttributeReference>
  <!-- Allow All -->
  <AttributeReference editable="true"
optional="true">-508</AttributeReference>
  <!-- Auto Save -->
  <AttributeReference editable="true"
optional="true">-509</AttributeReference>
  <!-- Auto Launch -->
  <AttributeReference editable="true"
optional="true">-510</AttributeReference>
  <!-- Self Request Allowed -->
  <AttributeReference editable="true"
optional="true">-511</AttributeReference>
  <!-- Provision By Resource Admin Only -->
  <AttributeReference editable="true"
optional="true">-512</AttributeReference>
  <!-- Off-line Provisioning -->
  <AttributeReference editable="true"
optional="true">-513</AttributeReference>
  <!-- Trusted Source -->
  <AttributeReference editable="true"
optional="true">-514</AttributeReference>
  <!-- Sequence Recon -->
  <AttributeReference editable="true"
optional="true">-515</AttributeReference>
</Form>

<!-- Resource Management section -->
<!-- List of attributes that can be displayed in the "Resource" Form -->
<Attribute name="-501" variantType="long" datalength="50" map="Objects.Key"
/>
<Attribute name="-502" label="taskdetails.label.resourcename"
displayComponentType="TextField" variantType="String" dataLength="80"
map="Objects.Name" />
<Attribute name="-503"
label="UserGroupPolicies.label.columnHeading.policyDescription"

```

```

        displayComponentType="TextField" variantType="String" dataLength="256"
        map="Structure Utility.Description" />
<Attribute name="-504" label="global.label.type"
displayComponentType="LookupField" variantType="long" dataLength="256"
map="Objects.Type">
<ValidValues lookupCode="Lookup.Objects.Object Type"
selectionColumn="lkv_encoded"/>
</Attribute>
<Attribute name="-505" label="requestWizard.message.target"
displayComponentType="TextField" variantType="String" dataLength="256"
map="Objects.Order For" />
<Attribute name="-506" label="global.label.autoprepopulate"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Auto Prepopulate" />
<Attribute name="-507" label="dualListTest.message.resourceallowmultiple"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Allow Multiple" />
<Attribute name="-508" label="global.label.allowall"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Allow All" />
<Attribute name="-509" label="global.label.autosave"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Auto Save" />
<Attribute name="-510" label="global.label.autolaunch"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Auto Launch" />
<Attribute name="-511" label="global.label.selfrequestallowed"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Self Request Allowed" />
<Attribute name="-512" label="global.label.provisionbyresourceadminonly"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Admin Only" />
<Attribute name="-513" label="global.label.offlineprovisioning"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Off-line Provisioning" />
<Attribute name="-514" label="global.label.trustedsource"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Trusted Source" />
<Attribute name="-515" label="global.label.sequencerecon"
displayComponentType="CheckBox" variantType="String" dataLength="1"
map="Objects.Sequence Recon" />

```

3. Save and close the file.

3.4.3 Upgrading Oracle Identity Manager on Oracle WebLogic Server

To upgrade Oracle Identity Manager on Oracle WebLogic Server:

1. Stop the application server. In a clustered environment, stop the admin server, managed servers, and the Node Manager (if you are using the Node Manager).
2. Modify the MaxPermSize JVM memory setting as follows:
 - **If you are using Oracle WebLogic Server release 10.3.0, then:**
 - a. In a text editor, open the *DOMAIN_HOME*/bin/setDomainEnv.sh (or setDomainEnv.cmd) file.
 - b. Search for the following line:

```
MEM_MAX_PERM_SIZE="-XX:MaxPermSize=128m"
```


- c. Change the memory setting from 128 to 256 as follows:

```
MEM_MAX_PERM_SIZE="-XX:MaxPermSize=256m"
```

- **If you are using Oracle WebLogic Server release 10.3.1 or later, then:**

For Microsoft Windows:

- a. In a text editor, open the *DOMAIN_HOME*\bin\setDomainEnv.cmd file.

- b. In this file, search for the following line:

```
set MEM_MAX_PERM_SIZE_32BIT=-XX:MaxPermSize=128m
```

- c. Change this line to the following:

```
set MEM_MAX_PERM_SIZE_32BIT=-XX:MaxPermSize=256m
```

- d. Save and close the file.

For UNIX:

- a. In a text editor, open the *DOMAIN_HOME*/bin/setDomainEnv.sh file.

- b. In this file, search for the following lines:

```
MEM_MAX_PERM_SIZE_32BIT="-XX:MaxPermSize=128m"  
export MEM_MAX_PERM_SIZE_32BIT
```

- c. Change these lines to the following:

```
MEM_MAX_PERM_SIZE_32BIT="-XX:MaxPermSize=256m"  
export MEM_MAX_PERM_SIZE_32BIT
```

- d. Save and close the file.

3. Modify the MEM_ARGS JVM memory settings as follows:

- a. Open the following file in a text editor:

For Windows:

```
DOMAIN_HOME/bin/xlStartWLS.cmd
```

For Non-Windows:

```
DOMAIN_HOME/bin/xlStartWLS.sh
```

- b. Modify the memory arguments as follows:

For Microsoft Windows, if Sun JVM is used:

```
MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m
```

For Microsoft Windows, if BEA JRockit JVM is used:

```
MEM_ARGS=-Xms1280m -Xmx1280m
```

For UNIX, if Sun JVM is used:

```
USER_MEM_ARGS="-Xms256m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m"
```

For UNIX, if BEA JRockit JVM is used:

```
USER_MEM_ARGS="-Xms256m -Xmx1280m -XnoOpt"
```

4. Modify the Managed Server file for a non-Windows platform as follows:

- a. In a text editor, open the *DOMAIN_HOME/bin/xlStartManagedServer.sh* file.
- b. Search for the following lines:

```
export param1=$1
export param2=$2
```

Change them to the following:

```
param1=$1
export param1
param2=$2
export param2
```

5. In the *OIM_HOME/xellerate/setup/weblogic-setup.xml* file:

- a. Search for the following element:

```
<wldeploy action="deploy"
source="${WL_APP_LOCATION}/OIMApplications/WL${application.filename}"
name="Xellerate"
user="${weblogic_login_user}"
password="${weblogic_login_password}"
verbose="true"
adminurl="t3://${weblogic_server_target_url}:${weblogic_server_admin_port}"
debug="${action.deploy.debug}"
targets="${wl.deploy.target}" />
```

- b. Add a timeout value of 5400 as shown:

```
<wldeploy action="deploy"
source="${WL_APP_LOCATION}/OIMApplications/WL${application.filename}"
name="Xellerate"
user="${weblogic_login_user}"
password="${weblogic_login_password}"
verbose="true"
adminurl="t3://${weblogic_server_target_url}:${weblogic_server_admin_port}"
debug="${action.deploy.debug}"
targets="${wl.deploy.target}"
timeout="5400" />
```

6. If you are using Oracle WebLogic Server release 10.3.1 or later, then:

Note:

- For clustered installations, perform this step on all the nodes.
 - If you are using Oracle WebLogic Server release 10.3.0, then you have already copied the *DDTemplates* directory by performing the procedure described in [Section 3.4.1, "Copying Files."](#)
-
-

- a. Open the *PATCH/xellerate/DDTemplates/xlWebApp/weblogic.xml* file in a text editor.
- b. In this file, search for the following block of code:

```
<XDtConfig:ifConfigParamEquals paramName="clustering" value="true">
<XDtConfig:ifConfigParamEquals paramName="replication" value="InMemory">
<session-descriptor>
<persistent-store-type>replicated</persistent-store-type>
</session-descriptor>
```

```

</XDtConfig:ifConfigParamEquals>

<XDtConfig:ifConfigParamEquals paramName="replication" value="Database">
<session-descriptor>
<persistent-store-type>jdbc</persistent-store-type>
<persistent-data-source-jndi-name>xlDS</persistent-data-source-jndi-name>
</session-descriptor>
</XDtConfig:ifConfigParamEquals>
</XDtConfig:ifConfigParamEquals>

```

c. Replace that block of code with the following:

```

<XDtConfig:ifConfigParamEquals paramName="replication" value="InMemory">
<session-descriptor>
<persistent-store-type>replicated_if_clustered</persistent-store-type>
<cookie-http-only>>false</cookie-http-only>
</session-descriptor>
</XDtConfig:ifConfigParamEquals>

<XDtConfig:ifConfigParamEquals paramName="replication" value="Database">
<session-descriptor>
<persistent-store-type>jdbc</persistent-store-type>
<persistent-data-source-jndi-name>xlDS</persistent-data-source-jndi-name>
</session-descriptor>
</XDtConfig:ifConfigParamEquals>

```

d. Save and close the file.

e. Copy all files from the *PATCH/xellerate/DDTemplates* directory to the *OIM_HOME/xellerate/DDTemplates* directory.

7. Apply the patch as follows:

Note: It is recommended that you use the production mode for Oracle Identity Manager deployment. If the Oracle WebLogic Server domain is created in development mode, then the application of the patch might fail with the warning that the lock is obtained by another user. To avoid this issue, you must deselect the Automatically acquire lock option in the WebLogic admin console before you start applying the patch.

a. In a nonclustered environment, start the server by running *OIM_HOME/xellerate/bin/xlStartServer.sh* or *(xlStartServer.bat)*.

In a clustered environment, start the admin server, managed servers, and the Node Manager (if you are using the Node Manager).

b. Run the following command to apply the patch:

```

OIM_HOME/xellerate/setup/patch_weblogic.cmd/sh WEBLOGIC_ADMIN_PASSWORD
OIM_DB_USER_PASSWORD

```

Note: Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

Troubleshooting the Application of the Patch on Oracle WebLogic Server

If application of the patch fails on Oracle WebLogic Server, then perform the following steps:

1. Log in to the WebLogic admin console, and undeploy the Xellerate and Nexaweb application from.
2. Delete the `xellerate.ear` and `Nexaweb.ear` files from the `OIM_HOME/xellerate/OIMApplications` directory.

Note: In a clustered environment, perform this step on all nodes of the cluster.

3. Delete the contents of the `OIM_HOME/xellerate/webapp/precompiled` directory.
4. Delete the `ant_backup.jar`, `optional_backup.jar` and `xercesImpl_backup.jar` files from the `OIM_HOME/xellerate/ant/lib` directory.
5. In a clustered environment, delete the `xellerate` and `Nexaweb` directories from the `BEA_HOME/user_projects/domains/DOMAIN_NAME/servers/AdminServer/tmp/_WL_user` directory.
6. In a clustered environment:
Delete the `xellerate` and `Nexaweb` directories from the `BEA_HOME/user_projects/domains/DOMAIN_NAME/servers/MANAGED_SERVER_NAME/tmp/_WL_user` directory.
Delete the `xellerate` and `Nexaweb` directories from the `BEA_HOME/user_projects/domains/DOMAIN_NAME/servers/MANAGED_SERVER_NAME/stage` directory.
7. Restart Oracle WebLogic Server.

Note: In a clustered environment, restart the managed servers.

8. Open a session, and set the `JAVA_HOME` and `PATH` environment variables.
9. In the same session, rerun the `patch_weblogic` script.

3.4.4 Upgrading Oracle Identity Manager on JBoss Application Server

To upgrade Oracle Identity Manager on JBoss Application Server:

1. Open the following file in a text editor:
On a nonclustered installation:
`JBOSS_HOME/server/default/deploy/jboss-web.deployer/server.xml`
On a clustered installation:
`JBOSS_HOME/server/all/deploy/jboss-web.deployer/server.xml`
2. In this file, change the value of the `emptySessionPath` element to `false`.
3. Run the patch command as follows:
`OIM_HOME/xellerate/setup/patch_jboss.cmd` (or `patch_jboss.sh`)
`OIM_DB_USER_PASSWORD`

Note: If your Oracle Identity Manager installation is running on an RHEL 5 computer with JBoss Application Server 4.2.3 and JDK 1.60.10, then set the JAVA_OPTS parameter to the following:

```
JAVA_OPTS=%JAVA_OPTS% -XX:MaxPermSize=128m -XX:+UseConcMarkSweepGC  
-XX:+CMSClassUnloadingEnabled
```

3.4.5 Upgrading Oracle Identity Manager on IBM WebSphere Application Server

To upgrade Oracle Identity Manager on IBM WebSphere Application Server:

- In a nonclustered environment, run the following command to apply the patch:

Note: Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

```
OIM_HOME/xellerate/setup/patch_websphere.cmd/sh WEBSPHERE_ADMIN_PASSWORD  
OIM_DB_USER_PASSWORD
```

- In a clustered environment:
 1. Ensure that the Network Deployment Manager and all the cluster members are running.
 2. Run the following command from the Network Deployment Manager:

```
OIM_HOME/xellerate/setup/patch_websphere.sh (or patch_websphere.cmd)  
WEBSPHERE_ADMIN_PASSWORD OIM_DB_USER_PASSWORD
```

3.4.6 Upgrading Oracle Identity Manager on Oracle Application Server

To upgrade Oracle Identity Manager on Oracle Application Server:

1. Run the following script:

Note: Ensure that the application server is running before you apply the Oracle Identity Manager patch files. After the patches are applied, you must stop and restart the application server for the patches to take effect.

```
OIM_HOME\xellerate\setup\patch_oc4j.cmd (or patch_oc4j.sh) OAS_ADMIN_PASSWORD  
DATASOURCE_PASSWORD
```

2. Restart the Oracle Identity Manager server. For a clustered installation, restart each node of the cluster.

3.5 Upgrading the Oracle Identity Manager Design Console

To upgrade the Design Console:

1. Create a backup of the `OIM_DC_HOME\xlclient` directory.

2. Replace the contents of the following directory with the contents of the *PATCH/xlclient/lib* directory:

OIM_DC_HOME\xlclient\lib

3. Copy the following files:
 - *XLDesktopClient.ear* from *PATCH/xlclient* to *OIM_DC_HOME\xlclient*
 - *xlFvcUtil.ear* from *PATCH\xlclient* to *OIM_DC_HOME\xlclient*

If you are using IBM WebSphere Application Server as the application server, then update the *xlDataObjectBeans.jar* file as follows:

Note: Ensure that you perform these steps after you have performed the procedure described in "[Upgrading Oracle Identity Manager on IBM WebSphere Application Server](#)".

1. In a Web browser, connect to the WebSphere administrative console by using a URL of the following format:

`http://HOST_NAME:PORT/admin`

2. Log in by using the Oracle Identity Manager administrator account that you specified during installation.
3. Click **Applications**, and then select **Enterprise Applications**.
4. Select **Xellerate application**.
5. Click **Export**.
6. Save the *xellerate.ear* file to a temporary directory.
7. Extract the *xlDataObjectBeans.jar* file from the *xellerate.ear* file.

Note: Ensure that you extract the *xlDataObjectBeans.jar* file and not the *xlDataObjects.jar* file.

8. Copy the *xlDataObjectBeans.jar* file into the *OIM_DC_HOME\xlclient\lib* directory.

3.6 Upgrading the Oracle Identity Manager Remote Manager

To upgrade the Remote Manager:

1. Create a backup of the *OIM_RM_HOME/xlremote/lib* directory.
2. Replace the contents of the *lib* directory with the contents of the *PATCH/xlremote/lib* directory.

3.7 Redeploying the Diagnostic Dashboard

After upgrading to Oracle Identity Manager release 9.1.0.2, you must redeploy the Diagnostic Dashboard by performing the procedure described in one of the following sections:

- Section 3.7.1, "Redeploying the Diagnostic Dashboard on IBM WebSphere Application Server"
- Section 3.7.2, "Redeploying the Diagnostic Dashboard on JBoss Application Server"
- Section 3.7.3, "Redeploying the Diagnostic Dashboard on Oracle Application Server"
- Section 3.7.4, "Redeploying the Diagnostic Dashboard on Oracle WebLogic Server"

3.7.1 Redeploying the Diagnostic Dashboard on IBM WebSphere Application Server

To redeploy the Diagnostic Dashboard on IBM WebSphere Application Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

In addition, perform the following steps if you are using IBM WebSphere Application Server 6.1.0.x:

Note: It is assumed that you have already deployed the XIMDD.war from the *PATCH/Diagnostic Dashboard* directory.

1. Uninstall the XIMDD.war file as follows:
 - a. On the IBM WebSphere Administrative console, expand **Applications**.
 - b. Click **Enterprise Applications**.
 - c. If the application status for XIMDD shows that it is running, then select the check box for XIMDD and click **Stop**.
 - d. Select the check box for XIMDD, and then click **Uninstall**.
 - e. Click the **Save** link in the Save directly to the master configuration option.
2. Extract the xlDataobjectBeans.jar file from the xellerate.ear file as follows:
 - a. On the IBM WebSphere Administrative console, expand **Applications**.
 - b. Click **Enterprise Application**.
 - c. Select **xellerate**, and then click **Export**.
 - d. Click **xellerate.ear**, and then provide a path to save the file.
 - e. Extract the contents of the xellerate.ear file. The xlDataobjectBeans.jar file is one of the files inside the xellerate.ear file.
3. Add the xlDataobjectBeans.jar file to the XIMDD.war file as follows:
 1. Open the *PATCH/Diagnostic Dashboard/XIMDD.war* file.
 2. Add the xlDataobjectBeans.jar file into the XIMDD.war file.
4. Install the revised XIMDD.war file as follows:
 - a. Copy the revised XIMDD.war file to a directory from which it is accessible through the IBM WebSphere Administrative console.
 - b. On the IBM WebSphere Administrative console, expand **Applications**.
 - c. Click **Install New Applications**.
 - d. Browse to and select the XIMDD.war file.

- e. In the **Context root** field, enter `XIMDD`.
- f. Select the **How do you want to install the application** option.
- g. Click **Next**.
- h. On the Select Installation Options page, enter `XIMDD` in the **Application name** field.
- i. Click **Next**.
- j. Select the check box for the **XIMDD.war** module.
- k. Click **Next**.
- l. On the Map Virtual Hosts for Web Module page, select the check box for the `XIMDD.war` module.
- m. Click **Next**.
- n. On the Summary page, click **Finish**.
- o. Click the **Save** link for the Save directly to the master configuration option.
- p. Expand **Applications**.
- q. Click **Enterprise Applications**.
- r. Select the check box for `XIMDD`, and then click **Start**.

3.7.2 Redeploying the Diagnostic Dashboard on JBoss Application Server

To redeploy the Diagnostic Dashboard on JBoss Application Server, use the following file:

`PATCH/Diagnostic Dashboard/jboss/XIMDD.war`

To redeploy the Diagnostic Dashboard, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

3.7.3 Redeploying the Diagnostic Dashboard on Oracle Application Server

To redeploy the Diagnostic Dashboard on Oracle Application Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

After you deploy the `XIMDD.war` file:

1. Open the following file in a text editor:

`ORACLE_HOME/j2ee/OAS_INSTANCE_NAME/application-deployments/XIMDD/orion-application.xml`

2. Search for the following lines:

```
<imported-shared-libraries>
</imported-shared-libraries>
```

3. Replace these lines with the following lines:

```
<imported-shared-libraries>
<import-shared-library name="oim.xml.parser"/>
<remove-inherited name="apache.commons.logging"/>
</imported-shared-libraries>
```

4. Restart the servers by using the `opmnctl` utility.

3.7.4 Redeploying the Diagnostic Dashboard on Oracle WebLogic Server

To redeploy the Diagnostic Dashboard on Oracle WebLogic Server, see "Installing the Diagnostic Dashboard" in *Oracle Identity Manager Administrative and User Console Guide for Release 9.1.0.2*.

3.8 Redeploying the SPML Web Service

If you are using SPML Web service along with Oracle Identity Manager, then you must redeploy the SPML Web service after you upgrade Oracle Identity Manager.

Note: On JBoss Application Server, ensure that the commons-discovery.jar file is in the following directory:

- For a nonclustered installation:
JBOSS_HOME/server/default/lib
- For a clustered installation:
JBOSS_HOME/server/all/lib

If the commons-discovery.jar file is not present in this directory, then download and copy it from the Apache Web site.

If you have customized the EAR file, then you must redo those changes in the EAR file and then redeploy it.

Note: See the application server vendor documentation for information about undeploying the application.

See *Oracle Identity Manager Tools Reference* for information about the deployment procedure.

3.9 Enabling the Integration with Oracle Role Manager

Note: The procedure described in this section is optional. Perform this procedure only if you are integrating Oracle Identity Manager with Oracle Role Manager.

If you are integrating Oracle Identity Manager with Oracle Role Manager, then set the `XL.OIM-ORM.Integration.Deployed` property to `true`. See *Oracle Identity Manager Design Console Guide* for information about working with system properties.

3.10 Applying the Patch for Arabic Language Support

Note: This section describes an optional procedure. Perform this procedure only if you want to use the Arabic locale. You need not perform this procedure if you were already using the Arabic locale before you upgraded to release 9.1.0.2.

If required, you can enable support for the Arabic language after upgrading to Oracle Identity Manager release 9.1.0.2. To enable support for the Arabic language:

1. Log in as the Oracle Identity Manager database schema owner.
2. Run the following script:

```
PATCH/db/oracle/Scripts/dml_update_region_language_to_arabic.sql
```

3.11 Reapplying Customizations and Compiling Adapters

See "[Customizations in Release 9.1.0.2](#)" for information about the changes made in Oracle Identity Manager user interface (UI) related files. After you apply the patch, reapply the customizations in the files.

In addition, compile all adapters. See *Oracle Identity Manager Design Console Guide* for instructions.

4 Resolved Issues

The following table lists issues resolved in Oracle Identity Manager Release 9.1.0.2:

Bug Number	Description
6885766	If users were added to groups using event handlers on user data objects instead of auto-group membership rules, the time taken for access policy evaluation and resource provisioning increased exponentially with the addition of each group.
7153285	The ORA-936 or ORA-921 error was encountered during reconciliation from Oracle Database.
7228951	The ORA-0911 error was encountered when the reconciliation archival utility was run on an Oracle Identity Manager installation for which the Japanese locale was set.
7190428	During reconciliation, a date field in Oracle Identity Manager was not updated if the date field in the reconciliation event was empty (NULL).
5414750	The createDeleteReconciliationEvent method could delete OIM Users even during target resource trusted reconciliation.
7192812	During reconciliation by using a generic technology connector, the JAVA.LANG.NULLPOINTER exception was encountered if the connector tried to update a UDF.
7263248	Custom authentication login modules did not work on an Oracle Identity Manager installation running on Oracle Application Server.
6403137	During reconciliation, an exception was encountered if multivalued attribute data on the target system contained the single quotation mark (') character.
7372341	At the end of a trusted source reconciliation run, the Manager ID field on the OIM User form was not updated on the OIM User form.
7493603	An error was encountered on attempting to regenerate group or resource profiles for auditing.
7445039	The mav.mav_field_length field was not updated through process form changes. It could be updated only through a process task mapping update.
7432421	An exception was encountered if an SPML response to the SPML Web Service contained white space characters.

Bug Number	Description
7558705	An update to the child form in an access policy resulted in loss of data about the state of check boxes (selected or deselected) on the parent form.
6429919	E-mail was not automatically sent to the requester (user) when the user's profile was edited.
7331148	A newly added UDF did not appear on the mapping page for the Generic Technology Connector feature.
7657868	A dependent resource remained in the Waiting state even after the parent resource reached the Provisioned state.
8206680	On an Oracle Identity Manager installation using Microsoft SQL Server 2005, an error was thrown while attempting to run the Resubmit Reconciliation Event task if the keyword <code>with</code> was encountered.
7621211	When an administrator reassigned a task, notification e-mail was not sent to the new assignee and administrator.
7591702	If there were a large number of user records in Oracle Identity Manager, then a user search performed with the asterisk (*) character or a blank value ended in a deadlock situation.
7455899	Access policies did not revoke child records after a reconciliation update was received.
8219167	When a connector definition was exported and then imported, mappings between child tables of the resource object form and the process form were lost.
7831629	Reconciliation failed if two reconciliation attributes had the same field name.
8220275	During target resource reconciliation, the No Match Found event was not created for target system records for which no match was found.
7562283	The request data in the process task adapter mapping returned the Request ID for the Add request for that instance instead of the request ID of the request that initiated the transaction.
8332225	The rules of the default complex password policy in Oracle Identity Manager were different from the password rules in Microsoft Active Directory
7411037	An exception was encountered if a task assignment failed while an API added an approval task.
7330728	There was no API that could accept a Code Key value and find the corresponding Decode value.
6769920	A role could not be deleted by an access policy.
7684896	The e-mail notification feature for a reassigned task was not the same as the feature to send e-mail notification for an assigned task.
8302402	For an Oracle Identity Manager installation set to the Japanese locale, the parent organization name was not displayed in Japanese.
8223798	A resource child form could not be mapped to a process child form in the process definition.
8292615	A warning was displayed on attempting to select multiple resources during request-based provisioning.
7633906	On the Adapter Factory form of the Design Console, a query for an adapter failed if the name of the adapter contained the word <code>ordered</code> .
7045674	The Validation engine of the Generic Technology Connector feature accepted only hashtable parent data.

Bug Number	Description
7299418	The Request Type list displayed on the Administrative and User Console showed values that are not supported in Oracle Identity Manager.
7151075	The Adapter Factory returned the following error message when adding an adapter of the Handle Error type: Field adt_name must be populated before saving.
7114985	The reconciliation manager table could not display more than 10000 rows.
7275601	When a user was configured as a proxy of the user's manager, the user could approve requests of which the user was the target beneficiary.
7268966	A DDL statement was run within a transaction, and the Commit Not Allowed exception was thrown by the createForm(Map) method.
6765667	Task notification e-mail was sent to proxy users who were in the Disabled state.
7257153	During process matching, the case-sensitive check of the reconciliation rule was not correctly applied.
6987230	An error was encountered on searching for a resource containing a UDF of the lookup field type.
7264986	Values returned by the tcAdpEvent.finalizeProcessAdapter adapter were truncated.
7112468	A user who was a member of the approver group could approve the user's own requests.
7477090	When a form was opened for editing, the items selected and saved in lists on the form were replaced by default entries in the lists.
7338467	When a resource was provisioned by an access policy with approval, the User resource access history report showed the name of the access policy in the Provisioned By column of the report.
7440144	Incorrect results were displayed when a pending approval was denied.
7257810	Provision requests for deleted users caused errors when the Scheduled Provisioning Task scheduled task was run.
7498288	The ServletException exception was encountered when a new user logged in to Oracle Identity Manager using Oracle Access Manager as SSO and changed the user's password.
7382874	A dependency error was encountered while importing an XML file containing the definition of a process task that had a modified adapter.
7515549	The NullPointerException exception was encountered during an import on attempting to import child data dependent and the dependent data does not exist.
7322512	When a resource was provisioned through request-based provisioning, the request number was stored in the Provisioned By column. If the resource was later revoked through request-based provisioning, then the request number was not updated for new request.
7438761	Simultaneous access to the same resource did not result in one user getting an exclusive lock.
7577436	An assigned adapter was displayed in both the assigned and unassigned lists.
7418026	When a user was disabled by a group membership rule, the user's resource was not revoked by the access policy.
7492747	The Auto Save and Auto Prepopulate feature did not work when applied on two provisioning processes one after the other.

Bug Number	Description
7562504	When a user is removed from a group, the User Profile management feature deletes the information about the child form. The NumberFormatException exception was encountered when Oracle Identity Manager tried to parse the version of the child form.
7635371	The password reset function did not work correctly with the minimum password age policy.
6372182	An error was encountered when a resource object was associated with multiple provision processes.
7551251	If a resource was requested for a user whose provisioning date was in the future, when the resource is eventually provisioned, the status of the resource remains at Provisioning although the tasks in the provisioning process are completed.
7576302	A logical entity adapter could not be configured to check if an input date argument was empty.
8261674	The following message was displayed on attempting to select a user on the Step 2: Select users page of the Request-Based Provisioning feature: Bad User Selection made
7832304	The logout page was displayed on attempting to log in to the Administrative and User Console.
8232551	The logout page was displayed on refreshing a page after logging in to the Administrative and User Console.
7589327	A user who provided wrong answers to the password challenge questions was not automatically set the Locked state.
7707746	A browser error was encountered on attempting to open a lookup field containing an entry with special characters that the browser did not support.
8213436	When the Group Membership report was run, the ORA-30004 error was encountered because the separator character used was also part of the data in the report.
7616311	An error was encountered if the generic technology connector reconciliation scheduled task did not find the parent identity data source file at the specified staging location.
7493763	The E-mail Address field does not accept some special characters.
8201655	The ORA-1 error was encountered if a requester submitted a second Revoke Resource request on the same resource and the same user.

5 Known Issues and Workarounds

The following sections describe known issues related to Oracle Identity Manager release 9.1.0.2:

- [Section 5.1, "General Known Issues"](#)
- [Section 5.2, "Design Console Known Issues"](#)
- [Section 5.3, "Reports Known Issues"](#)
- [Section 5.4, "Globalization Known Issues"](#)

5.1 General Known Issues

This section describes known issues related to the general run-time operation of Oracle Identity Manager Release 9.1.0.2, including known issues for Oracle Identity Manager server and known issues for the Administrative and User Console not related to reporting.

This section contains the following topics:

- [Section 5.1.1, "Exception May Be Thrown While Using SSO to Log In to Administrative and User Console When Oracle Identity Manager Is Installed in a UNIX/Linux Environment \(Bug 5969651\)"](#)
- [Section 5.1.2, "Stack Overflow Exception Thrown When Importing an XML File \(Bug 5350771\)"](#)
- [Section 5.1.3, "ConcurrentModificationException in JBoss Cluster Configuration When Replicating Session Data \(Bug 5180914\)"](#)
- [Section 5.1.4, "Pending Approvals Cannot Be Filtered by Requester Name \(Bug 5365516\)"](#)
- [Section 5.1.5, "All Records Returned When Filtering Records by the Date Type User Defined Field \(Bug 5376321\) and Searching Using Character Strings \(Bug 5354752\)"](#)
- [Section 5.1.6, "Date Value Entered in Incorrect Format in the Administrative and User Console Date Fields Causes an Error Message to Be Displayed \(Bug 5533945\)"](#)
- [Section 5.1.7, "Errors When Modifying Settings and Assignments for Internal System-Seeded Users \(Bug 5357781\)"](#)
- [Section 5.1.8, "Error Message Displayed After Single Sign-On Timeout Interval in Deployment Manager or WorkFlow Visualizer Windows \(Bug 5553411\)"](#)
- [Section 5.1.9, "Null Pointer Exception Thrown When Running the purgecache.bat Utility \(Bug 5388849\)"](#)
- [Section 5.1.10, "Challenge Questions Page Displayed in Error in Single Sign-On Mode When "Force to set questions at startup" System Property Set to TRUE \(Bug 5565798\)"](#)
- [Section 5.1.11, "System Error May Occur When Accessing Administrative and User Console After Database Is Restarted \(Bug 5563616\)"](#)
- [Section 5.1.12, "Warning Page May Be Displayed in the Administrative and User Console After Receiving "Illegal Script Tag or Characters" Message and Clicking the Back Button \(Bug 5676771\)"](#)
- [Section 5.1.13, "Benign Warning Messages May Appear in Oracle Application Server Log File After Installing Release 9.1.0.2 and Starting Oracle Application Server \(Bug 5840687\)"](#)
- [Section 5.1.14, "Deployment Manager Requires JRE 1.6.0_07 \(Bug 5565793\)"](#)
- [Section 5.1.15, "Exception May Be Encountered if IPv6 Is the Internet Protocol in Use \(Bugs 5637999 and 9273526\)"](#)
- [Section 5.1.16, "Multiple Entries for the Same Request ID Are Displayed on the Pending Approvals Page in Administrative and User Console \(Bug 5910393\)"](#)
- [Section 5.1.17, "Boolean Type Check Box of the User Defined Field Is Not Displayed on Request Submitted Form \(Bug 5374307\)"](#)

- Section 5.1.18, "'Illegal Script Tag or Characters' Message Is Displayed in Lookup Forms"
- Section 5.1.19, "Error Message Logged When a Scheduled Task Is Viewed or Modified (Bug 6379143)"
- Section 5.1.20, "User Profile Information Specified in E-mail Definition Is Not Valid for Approval Tasks (Bug 5671866)"
- Section 5.1.21, "Exception Thrown on Logging in to WebSphere 6.1.0.9 (Bug 6355328)"
- Section 5.1.22, "WSLoginFailedException May Be Thrown in IBM WebSphere Log (Bug 6442226)"
- Section 5.1.23, "IllegalArgumentException and CacheException May Be Thrown After Application Server Is Started (Bug 6415213)"
- Section 5.1.24, "User Password Reset Is Not Supported by SPML Web Service When Password Policies Are Enabled (Bug 6430243)"
- Section 5.1.25, "Search Button Must Be Clicked Twice to Search for a Scheduled Task After Changing the State (Bug 6493690)"
- Section 5.1.26, "NullPointerException Written to Log File When Oracle Application Server Is Shut Down (Bug 6471061)"
- Section 5.1.27, "Some Postinstallation Tests Offered by the Diagnostic Dashboard Are Displayed in the List of Preinstallation Tests (Bug 6512066)"
- Section 5.1.28, "Special Characters Are Not Allowed in Attestation Process Definition (Bug 6514208)"
- Section 5.1.29, "Columns Names Are Displayed Instead of Labels If an Attestation Scope Is Defined Using User-Defined Fields (Bug 6517060)"
- Section 5.1.30, "Reconciliation Event Does Not Exist/Reconciliation Message Failed Log Messages"
- Section 5.1.31, "Multiple Trusted Source Flag and Reconciliation Sequence Flag Not Displayed in the Administrative and User Console (Bugs 6626902 and 6625149)"
- Section 5.1.32, "Resource Name Field of the Create Attestation Process Is Case-Sensitive"
- Section 5.1.33, "Retry Interval and Retry Attempt Limit Values Not Displayed on Task Details Page (Bug 6633903)"
- Section 5.1.34, "Changes to JDBC Connection Pool Attributes May Result in Database User Account Getting Locked (Bug 6621085)"
- Section 5.1.35, "Previously Viewed Workflow Displayed on Creating a New Workflow Event (Bug 6645226)"
- Section 5.1.36, "User ID Containing Special Characters Is Not Displayed in User ID Lookup Fields"
- Section 5.1.37, "Database Error May Be Thrown When Disabling an Organization (Bug 6608036)"
- Section 5.1.38, "Session Timeout System Error Thrown During Workflow Creation Can Be Ignored (Bug 6645683)"
- Section 5.1.39, "Known Issues Related to Generic Technology Connectors"

- Section 5.1.40, "Exception May Be Thrown When a Scheduled Task Runs for Many Hours"
- Section 5.1.41, "Filter by Permission Name Field Might Not Accept Non-ASCII Characters (Bug 7510739)"
- Section 5.1.42, "JspException Might Be Encountered (Bug 7583783)"
- Section 5.1.43, "Java.Lang.Securityexception Exception Might Be Encountered (Bug 7550811)"
- Section 5.1.44, "HeadlessGraphicsEnvironment Exception Might Be Encountered on JBoss Application Server (Bug 7594350)"
- Section 5.1.45, "Java.Lang.IllegalArgumentException Might Be Encountered (Bug 7597447)"
- Section 5.1.46, "Login Attempt on an Idle Login Window May Display the Logout Page (Bug 7249936)"
- Section 5.1.47, "Connection with Oracle Database 11g Might Fail During Certain Oracle Identity Manager Operations (Bugs 7575738 and 7599139)"
- Section 5.1.48, "tcDefaultSignatureImpl Exception Might Be Encountered When a Scheduled Task Is Run (Bugs 7594587 and 7601851)"
- Section 5.1.49, "System Error Encountered on Trying to View an Object Form on Oracle Identity Manager Using Microsoft SQL Server (Bug 7626893)"
- Section 5.1.50, "Values of Some Fields of an Access Policy process form Are Not Displayed While Editing (Bug 7632407)"
- Section 5.1.51, "System Error Encountered on Viewing a Resource Form on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7626893)"
- Section 5.1.52, "List of Open Tasks Not Displayed on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7635735)"
- Section 5.1.53, "JMS Verification in the Diagnostic Dashboard May Fail in IBM-AIX and Oracle Weblogic Server Combination (Bug 8217994)"
- Section 5.1.54, "Not Enough Perm Memory While Using Oracle Identity Manager on Oracle Weblogic Server in HP-JDK"
- Section 5.1.55, "Change Password Might Not Work on an Oracle Identity Manager Installation Running on Oracle WebLogic Server and AIX (Bug 7757901)"
- Section 5.1.56, "Assigned Password Policy Is Removed when the Database User Management Connector for Release 9.0.4.1 Is Imported (Bug 7712797)"
- Section 5.1.57, "User Locked Out of Administrative and User Console on Oracle Identity Manager Running on Oracle WebLogic Server (Bug 8371395)"
- Section 5.1.58, "Some Lookup Queries Might Show Only Code Key Values on the Administrative and User Console (Bug 8494021)"
- Section 5.1.59, "Test Connectivity Option Does Not Work for the SoD Engine IT Resource (Bug 8504052)"
- Section 5.1.60, "Users Data Object of Microsoft Active Directory Connector Overwrites the Users Data Object of Oracle Role Manager Integration Library (Bug 8501702)"
- Section 5.1.61, "Bulk Load Utility Can Load User Data Containing First Name Values That Are Up To 255 Characters in Length (Bug 8519266)"

5.1.1 Exception May Be Thrown While Using SSO to Log In to Administrative and User Console When Oracle Identity Manager Is Installed in a UNIX/Linux Environment (Bug 5969651)

An exception similar to the following one may be thrown the first time you log in to the Administrative and User Console using SSO in a UNIX/Linux environment:

```
[XELLERATE.WEBAPP],Class/Method: tcWebAdminHomeAction/setChallengeQuestions  
encounter some problems: USER_QUES_NOT_DEFINED  
Thor.API.Exceptions.tcAPIException: USER_QUES_NOT_DEFINED
```

To resolve this issue, you must use the Design Console to assign a value of `FALSE` to the `Force to set questions at startup system` property.

5.1.2 Stack Overflow Exception Thrown When Importing an XML File (Bug 5350771)

When you import an XML file, a stack overflow exception may be thrown if the import operation changes the organizational hierarchy. You can safely ignore this exception.

5.1.3 ConcurrentModificationException in JBoss Cluster Configuration When Replicating Session Data (Bug 5180914)

When replicating session data, the JBoss Application Server may fail and generate the following exception in a clustered configuration:

```
16:43:07,296 ERROR [JBossCacheManager] processSessionRepl: failed with  
exception: java.util.ConcurrentModificationException  
16:43:07,296 WARN [InstantSnapshotManager] Failed to replicate  
sessionId:GzUYJdx1SLVxs7ssRtvWwQ**.txq00
```

5.1.4 Pending Approvals Cannot Be Filtered by Requester Name (Bug 5365516)

If you attempt to use the Requester filter to refine the results in the Pending Approvals page, a message indicating that the search did not return any results is displayed. You can use the Requester filter only to refine results by requester ID and not by requester first name or last name.

5.1.5 All Records Returned When Filtering Records by the Date Type User Defined Field (Bug 5376321) and Searching Using Character Strings (Bug 5354752)

In the Administrative and User Console, searching based on the Date Type User Defined Field may return all records instead of just the records matching the specified dates. Using character string input as search criteria may also return all records. To avoid these issues, use the following date format:

`YYYY-MM-DD`

5.1.6 Date Value Entered in Incorrect Format in the Administrative and User Console Date Fields Causes an Error Message to Be Displayed (Bug 5533945)

All dates in the Administrative and User Console must be edited using the calendar icon associated with the **Date** field. Do not edit dates directly by entering text in a **Date** field. Instead, use that field's calendar icon to edit the date value.

5.1.7 Errors When Modifying Settings and Assignments for Internal System-Seeded Users (Bug 5357781)

Do not modify any settings or assignments for internal system-seeded users. If you attempt to modify any settings or assignments for internal system-seeded users, then you may encounter errors.

5.1.8 Error Message Displayed After Single Sign-On Timeout Interval in Deployment Manager or WorkFlow Visualizer Windows (Bug 5553411)

After a Single Sign-On session times out, clicking **Restart** in the Deployment Manager or WorkFlow Visualizer window of the Administrative and User Console may cause a "Client-Side error occurred" error message to be displayed. If this message is displayed, close the browser and then access the Administrative and User Console by using a new browser window.

5.1.9 Null Pointer Exception Thrown When Running the purgecache.bat Utility (Bug 5388849)

When you run the `purgecache.bat` utility, the following exception is thrown:

```
java.lang.NullPointerException
    at
com.opensymphony.oscache.base.AbstractCacheAdministrator
    .finalizeListeners(Abs
tractCacheAdministrator.java:323)
    at
com.opensymphony.oscache.general.GeneralCacheAdministrator
    .destroy(GeneralCacheAdministrator.java:168)
    at net.sf.hibernate.cache.OSCache.destroy(OSCache.java:59)
    at
net.sf.hibernate.cache.ReadWriteCache.destroy(ReadWriteCache.java:215)
    at
net.sf.hibernate.impl.SessionFactoryImpl.close(SessionFactoryImpl.java:542)
```

This exception can be safely ignored.

5.1.10 Challenge Questions Page Displayed in Error in Single Sign-On Mode When "Force to set questions at startup" System Property Set to TRUE (Bug 5565798)

In the Single Sign-On mode, when the `Force to set questions at startup` system property is set to `TRUE`, the Challenge Questions page is displayed instead of the Welcome page of the Administrative and User Console. In the Single Sign-On mode, the `Force to set questions at startup` system property must be set to `FALSE`.

5.1.11 System Error May Occur When Accessing Administrative and User Console After Database Is Restarted (Bug 5563616)

Each application server exhibits different behavior when a database connection is lost during execution. While JBoss Application Server can automatically reestablish a database connection, Oracle WebLogic Server and IBM WebSphere Application Server cannot. For Oracle WebLogic, you can define settings for testing reserved connections, in which case the connections are established automatically. For IBM WebSphere, you must configure your database for high-availability.

5.1.12 Warning Page May Be Displayed in the Administrative and User Console After Receiving "Illegal Script Tag or Characters" Message and Clicking the Back Button (Bug 5676771)

In Microsoft Windows Server 2003 Service Pack 1 (SP1) environments, the "Warning: Page has Expired" page may be displayed if you click the Back button after the "Illegal Script tag or Characters" error message is displayed. You can go back to the first page for creation by clicking the Refresh button on the browser toolbar.

5.1.13 Benign Warning Messages May Appear in Oracle Application Server Log File After Installing Release 9.1.0.2 and Starting Oracle Application Server (Bug 5840687)

After installing Oracle Identity Manager release 9.1.0.1 on Oracle Application Server and then starting Oracle Application Server, warning messages regarding files with the same name but that are not identical may appear in the Oracle Application Server log file. These warning messages are benign and can be safely ignored.

5.1.14 Deployment Manager Requires JRE 1.6.0_07 (Bug 5565793)

An export operation using the Deployment Manager may encounter problems when Microsoft Internet Explorer is configured to use Microsoft Virtual Machine. To reset the default Virtual Machine:

1. Download and install the Sun JRE 1.6.0_07 from the following Web site:
<http://java.sun.com/>
2. Select **Tools** from the Internet Explorer menu.
3. Select **Internet Options**.
4. Select the **Advanced** tab.
5. Scroll down to **Java (Sun)**.
6. Check **Use Java 2v1.6.0_xx for <applet>**.
7. Scroll down to **Microsoft VM**.
8. Deselect **Java console enabled** and **Java logging enabled**.
9. Restart the computer.

Note: JRE 1.6.0_07 is not required to run the Oracle Identity Manager Administrative and User Console—it is only required to run the Deployment Manager.

5.1.15 Exception May Be Encountered if IPv6 Is the Internet Protocol in Use (Bugs 5637999 and 9273526)

If IPv6 is the Internet protocol in use, then you may encounter the following exceptions in the Oracle Identity Manager logs:

- On JBoss Application Server and Linux with Sun JDK 5 or earlier:
IP_MULTICAST_IF:
java.net.SocketException: bad argument for IP_MULTICAST_IF: address not bound to any interface at
java.net.PlainDatagramSocketImpl.socketSetOption(Native Method) at
java.net.PlainDatagramSocketImpl.setOption(PlainDatagramSocketImpl.java:295)

- On Oracle WebLogic Server release 10.3.0 and AIX 5.3 with IBM JDK 1.6:
com.opensymphony.oscache.base.AbstractCacheAdministrator],Could not initialize listener

If you do not need IPv6 support, then you can avoid these exceptions by disabling IPv6 support in the JVM as follows:

1. Open the following script in a text editor:

```
OIM_HOME/bin/xlStartServer.sh
```

2. Add the following line in the script:

```
-Djava.net.preferIPv4Stack=true
```

3. Save the changes to the script, and then run it.

5.1.16 Multiple Entries for the Same Request ID Are Displayed on the Pending Approvals Page in Administrative and User Console (Bug 5910393)

When more than one approval task is assigned to a user, multiple entries for the same request ID are displayed on the Pending Approvals page in the Administrative and User Console. You can select any of the displayed entries to perform the approval process.

5.1.17 Boolean Type Check Box of the User Defined Field Is Not Displayed on Request Submitted Form (Bug 5374307)

The Request Submitted form of the Design Console does not display the Boolean Type User Defined Field check box. If the User Defined Field is set to the Boolean type, then the Request Submitted form displays the number 1 instead of the check box. If the Boolean type is not enabled, then the Request Submitted form displays a blank space.

5.1.18 "Illegal Script Tag or Characters" Message Is Displayed in Lookup Forms

In the Administrative and User Console, the "Illegal Script Tag or Characters" message is displayed if you enter the less than symbol (<), greater than symbol (>), or any combination of these symbols (such as << or >>) in a text field on any page that also has a lookup form, and then click the magnifying glass icon.

If this happens, close the lookup form, remove the illegal characters from the text field, and then click the magnifying glass icon to continue with the procedure.

See Also: The "Special Character Restrictions" section in *Oracle Identity Manager Globalization Guide*

5.1.19 Error Message Logged When a Scheduled Task Is Viewed or Modified (Bug 6379143)

When you view or modify a scheduled task on the Administrative and User Console, the following message may be recorded in the application server log file:

```
MessageDateFieldBean, localName='messageDateField': Illegal character (space) in "name" attribute
```

You can ignore this message.

5.1.20 User Profile Information Specified in E-mail Definition Is Not Valid for Approval Tasks (Bug 5671866)

The user profile information, which is specified in e-mail definitions of type `General`, is not valid for approval tasks.

5.1.21 Exception Thrown on Logging in to WebSphere 6.1.0.9 (Bug 6355328)

After installing IBM WebSphere Application Server 6.1.0.9, when you restart the server and log in to the Administrative Console as `xelsysadm`, an exception is thrown. However, this does not affect functionality and you can safely ignore the exception.

5.1.22 WSLoginFailedException May Be Thrown in IBM WebSphere Log (Bug 6442226)

The `com.ibm.websphere.security.auth.WSLoginFailedException` exception may be thrown for IBM WebSphere 6.1.0.9 configurations. You can ignore this exception.

This exception has been acknowledged by IBM, and you can refer to the following IBM Web page for more information:

<http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg1PK47479>

5.1.23 IllegalArgumentException and CacheException May Be Thrown After Application Server Is Started (Bug 6415213)

Note: This applies only to IBM WebSphere and Oracle Application Server.

The `java.lang.IllegalArgumentException` and `oracle.cabo.image.cache.CacheException` exceptions may be thrown after the application server is started. You can ignore these exceptions.

5.1.24 User Password Reset Is Not Supported by SPML Web Service When Password Policies Are Enabled (Bug 6430243)

If password policies are enabled in Oracle Identity Manager, then the SPML Web Service does not support password reset operations.

5.1.25 Search Button Must Be Clicked Twice to Search for a Scheduled Task After Changing the State (Bug 6493690)

On the Administrative and User Console, you can enable or disable a scheduled task displayed in the search results table for scheduled tasks. However, if you search for a scheduled task after you change its state, you must click the **Search** button once and then again for the task with the modified state to be displayed.

5.1.26 NullPointerException Written to Log File When Oracle Application Server Is Shut Down (Bug 6471061)

When you shut down Oracle Application Server, the `java.lang.NullPointerException` from the `com.thortech.xl.cache.CacheUtil` component is written to the application server log file. You can safely ignore this exception.

5.1.27 Some Postinstallation Tests Offered by the Diagnostic Dashboard Are Displayed in the List of Preinstallation Tests (Bug 6512066)

When you use the Diagnostic Dashboard, although the Test Basic Connectivity, Test Provisioning, and Test Reconciliation tests are available even before you install Oracle Identity Manager, you can use these tests only after you install Oracle Identity Manager.

5.1.28 Special Characters Are Not Allowed in Attestation Process Definition (Bug 6514208)

Special characters are not supported in the attestation process definition. Only alphanumeric characters and the underscore (_) character can be included.

5.1.29 Columns Names Are Displayed Instead of Labels If an Attestation Scope Is Defined Using User-Defined Fields (Bug 6517060)

While defining an attestation process using the Administrative and User Console, if an attestation scope is defined using user-defined fields (UDFs) on the User Scope or Resource Scope page, then columns names are displayed instead of labels in the list of selected attributes.

5.1.30 Reconciliation Event Does Not Exist/Reconciliation Message Failed Log Messages

During reconciliation, an error message similar to the following may be written to the logs:

```
[XELLERATE.JMS],The Reconciliation Event with key 512312 does not exist  
[XELLERATE.JMS],Processing Reconciliation Message with ID 512312 failed.
```

Depending on the application server retry settings, these messages are retried for the specified number of times. If JMS is not able to process these messages after the specified number of retries, then these messages are moved to the dead letter queue.

5.1.31 Multiple Trusted Source Flag and Reconciliation Sequence Flag Not Displayed in the Administrative and User Console (Bugs 6626902 and 6625149)

On the Resource Detail page of the Administrative and User Console, the newly introduced Multiple Trusted Source flag and Reconciliation Sequence flag are not displayed. These flags can be viewed in the Design Console.

5.1.32 Resource Name Field of the Create Attestation Process Is Case-Sensitive

In the Create Attestation process, the Resource Name field is case-sensitive. To correctly configure the attestation process, you must use the exact spelling and case (uppercase and lowercase) of the resource name.

5.1.33 Retry Interval and Retry Attempt Limit Values Not Displayed on Task Details Page (Bug 6633903)

The Retry Interval and Retry Attempt Limit values are not displayed on the Task Details page of the Workflow Visualizer.

5.1.34 Changes to JDBC Connection Pool Attributes May Result in Database User Account Getting Locked (Bug 6621085)

If JDBC connection pool attributes are changed on Oracle Application Server, then the "ORA-28000: the account is locked" error message may be written to the application

server log. When this error occurs, the database user account is locked. This is a known issue with Oracle Application Server when using an indirect password in the connection pool. Oracle Identity Manager connection pools use an indirect password.

If you want to change a connection pool attribute by using the Oracle Application Server Administrative Console, then you can work around this problem as follows:

1. Log in to the Oracle Application Server Administrative Console, and stop the application named `Xellerate`.
2. Change the connection pool attributes.
3. Restart Oracle Application Server.
4. Log in to the Oracle Application Server Administrative Console, and start the `Xellerate` application.

5.1.35 Previously Viewed Workflow Displayed on Creating a New Workflow Event (Bug 6645226)

In the Graphical Workflow Designer, when you click Save after adding a new Workflow Event, the previously viewed workflow is displayed instead of the newly created workflow event.

5.1.36 User ID Containing Special Characters Is Not Displayed in User ID Lookup Fields

During user creation in the Administrative and User Console, if special characters are included in the User ID value, then look-up fields for user IDs will not be able to display that specific user ID. For information about special character restrictions, refer to Oracle Identity Manager Globalization Guide.

5.1.37 Database Error May Be Thrown When Disabling an Organization (Bug 6608036)

When disabling an organization that has child organizations, a database error message may be displayed in addition to the Oracle Identity Manager error message. To avoid this problem, remove parent-child associations before disabling an organization.

5.1.38 Session Timeout System Error Thrown During Workflow Creation Can Be Ignored (Bug 6645683)

A session timeout error may be thrown during creation of a workflow. You can safely ignore this error.

5.1.39 Known Issues Related to Generic Technology Connectors

Refer to the "Known Issues of Generic Technology Connectors" chapter of *Oracle Identity Manager Administrative and User Console*.

5.1.40 Exception May Be Thrown When a Scheduled Task Runs for Many Hours

For Oracle Identity Manager on Oracle Application Server, the following exception may be thrown when a scheduled task runs for many hours:

```
Primary Server went down going to get a fresh object elsewhere in the cluster.  
com.evermind.server.rmi.RMIConnectionException: LRU connection
```

This exception has no impact on the functioning of Oracle Identity Manager and can be ignored.

5.1.41 Filter by Permission Name Field Might Not Accept Non-ASCII Characters (Bug 7510739)

The Filter by Permission Name field on the (Group Details) Permissions page of the Administrative and User Console might not accept non-ASCII characters.

5.1.42 JspException Might Be Encountered (Bug 7583783)

You might encounter exceptions similar to the following:

```
javax.servlet.jsp.JspException: Define tag cannot set a null value
```

You can ignore these exceptions because they do not affect the working of Oracle Identity Manager.

5.1.43 Java.Lang.Securityexception Exception Might Be Encountered (Bug 7550811)

The Java.Lang.Securityexception: Insufficient Method Permission exception might be encountered when Oracle Identity Manager is running on JBoss Application Server. To work around this issue:

1. From the jira.jboss.org Web site, download the patch for issue JBAS-6236.
2. Create the xlSecurityManager.jar file out of the code in the patch.

Note: Steps to create the JAR file are documented in the patch itself.

3. Copy the JAR file to the following location:

- For a nonclustered installation:

JBOSS_HOME/server/default/lib

- For a clustered installation, copy the JAR file into the following directory on all the nodes:

JBOSS_HOME/server/all/lib

4. Open the following file in a text editor:

- For a nonclustered installation:

JBOSS_HOME/server/default/conf/jboss-service.xml

- For a clustered installation:

JBOSS_HOME/server/default/conf/jboss-service.xml

5. In the XML file, search for the following lines:

```
<!-- JAAS security manager and realm mapping -->  
<mbean code="org.jboss.security.plugins.JaasSecurityManagerService"
```

Replace those lines with the following lines:

```
<!-- JAAS security manager and realm mapping -->  
<mbean code="mysec.security.jboss.jaas.OpenJaasSecurityManagerService"
```

6. Restart the server.

5.1.44 HeadlessGraphicsEnvironment Exception Might Be Encountered on JBoss Application Server (Bug 7594350)

The following error might be encountered if Oracle Identity Manager is running on JBoss Application Server:

```
java.lang.ClassCastException: sun.java2d.HeadlessGraphicsEnvironment cannot be cast to sun.awt.Win32GraphicsEnvironment
```

This is a known issue of JDK. For more information, look up Bug 6358034 on the following Web site:

<http://bugs.sun.com>

5.1.45 Java.Lang.IllegalArgumentException Might Be Encountered (Bug 7597447)

You might encounter exceptions similar to the following:

```
java.lang.IllegalArgumentException for creating image cache directory occurred
```

You can ignore these exceptions because they do not affect the working of Oracle Identity Manager.

5.1.46 Login Attempt on an Idle Login Window May Display the Logout Page (Bug 7249936)

Login attempt on an idle login window may display the logout page. Subsequent login attempts are successful. This does not have any functional impact on Oracle Identity Manager.

5.1.47 Connection with Oracle Database 11g Might Fail During Certain Oracle Identity Manager Operations (Bugs 7575738 and 7599139)

During certain Oracle Identity Manager operations, the connection with Oracle Database 11g might fail and the following error gets recorded in the log file:

```
java.sql.SQLException: Listener refused the connection with the following error: ORA-12518, TNS:listener could not hand off client connection
```

When this happens, depending on the application server on which Oracle Identity Manager is running, you might have to restart Oracle Identity Manager.

5.1.48 tcDefaultSignatureImpl Exception Might Be Encountered When a Scheduled Task Is Run (Bugs 7594587 and 7601851)

The following exception might be recorded in the log file when a scheduled task is run:

```
ERROR [ACCOUNTMANAGEMENT] Class/Method: tcDefaultSignatureImpl/verifySignature encounter some problems
```

However, the task is processed correctly on the next run.

5.1.49 System Error Encountered on Trying to View an Object Form on Oracle Identity Manager Using Microsoft SQL Server (Bug 7626893)

You might encounter a system error when you try to view an object form on Oracle Identity Manager using Microsoft SQL Server 2005.

5.1.50 Values of Some Fields of an Access Policy process form Are Not Displayed While Editing (Bug 7632407)

The following issue is observed on Oracle Identity Manager running on Oracle Database 11g release 1 (11.1.0.7):

While trying to edit an access policy that is attached to a resource object, values of some of the access policy process form fields might not be displayed. However, these values are present in the database. If required, you can enter new values and submit them. The new values will be posted to the database, and the access policy will function as expected.

This issue is encountered because of Bug 7632407 in Oracle Database 11g release 1 (11.1.0.7). At the time of this release, there is no patch available for this issue. According to Bug 7632407, you can apply the following workaround if you encounter this issue:

Log in to Oracle Database as `sysdba`, and then run the following command:

```
set "_optimizer_join_elimination_enabled"=false
```

5.1.51 System Error Encountered on Viewing a Resource Form on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7626893)

If a user's resource has been provisioned through request provisioning, then a system error might be encountered when you try to view the resource form from the user's Resource Detail page. This issue is encountered only on an Oracle Identity Manager installation using Microsoft SQL Server.

5.1.52 List of Open Tasks Not Displayed on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7635735)

The following issue is observed only on Oracle Identity Manager using Microsoft SQL Server:

When you click Open Tasks on the Administrative and User Console, an exception might be encountered and the list of open tasks might not be displayed.

5.1.53 JMS Verification in the Diagnostic Dashboard May Fail in IBM-AIX and Oracle Weblogic Server Combination (Bug 8217994)

The JMS verification in the Diagnostic Dashboard may fail in IBM-AIX and Oracle Weblogic Server combination. This does not affect the runtime component. You can ignore this error.

5.1.54 Not Enough Perm Memory While Using Oracle Identity Manager on Oracle Weblogic Server in HP-JDK

If you see any error related to "Permanent generation is full", then increase the Permgen memory in `WLS_DOMAIN_HOME/bin/xlStartWLS.cmd` and/or `WLS_DOMAIN_HOME/bin/xlStartManagedWLS.cmd` based on which script you use to start Oracle Identity Manager. Note that you may have to change the Server Start option on the Weblogic Admin Console if you are starting the Weblogic server by using the console.

5.1.55 Change Password Might Not Work on an Oracle Identity Manager Installation Running on Oracle WebLogic Server and AIX (Bug 7757901)

On an Oracle Identity Manager installation running on Oracle WebLogic Server and AIX, the following error might be encountered when you try to change your password:

"Password does not satisfy the Policies"

5.1.56 Assigned Password Policy Is Removed when the Database User Management Connector for Release 9.0.4.1 Is Imported (Bug 7712797)

A password policy assigned to a user is removed when the Database User Management connector for release 9.0.4.1 is imported using the Connector Installer.

5.1.57 User Locked Out of Administrative and User Console on Oracle Identity Manager Running on Oracle WebLogic Server (Bug 8371395)

Oracle WebLogic Server has a built-in security feature for automatically locking out users who cross a specified number of invalid login attempts. The default is 5 invalid attempts. Oracle Identity Manager has a similar locking mechanism, and the default is 3 invalid attempts. After 3 invalid attempts, Oracle Identity Manager locks the user in the database. If the user continues to make invalid attempts at logging in, then the application server locks the user. When this problem occurs, the user must wait until the session times out and then try logging in again using valid login credentials.

The following configuration change might help avoid this issue:

Note: Changes that you make by performing this procedure apply to all applications running on the application server.

1. Log in to the WebLogic Application Server console.
2. Go to Security Realms > REALM.
3. On the Configuration tab, select the **User Lockout** subtab.
4. You can apply one of the following approaches:
 - Approach 1:
Deselect **Lockout Enabled**.
 - Approach 2:
Modify the following parameters:
 - Lockout Threshold: The maximum number of consecutive invalid login attempts that can occur before a user's account is locked out.
 - Lockout Duration: The number of minutes that a user's account is locked out.
 - Lockout Reset Duration: The number of minutes within which consecutive invalid login attempts cause a user's account to be locked out.
 - Lockout Cache Size: The number of invalid login records (between 0 and 99999) that the server places in a cache.

5.1.58 Some Lookup Queries Might Show Only Code Key Values on the Administrative and User Console (Bug 8494021)

If you want a lookup definition of type Lookup Query to show Decode values and store Code Key values, then the underlying lookup query must meet all of the following conditions:

- The SELECT clause must contain columns from the LKV table, LKU table, or both tables.
- The WHERE clause must contain a condition that uses the LKU_TYPE_STRING_KEY column of the LKU table.

The following is an example of this type of lookup query:

```
SELECT LKV_ENCODED, LKV_DECODED
FROM LKV LKV, LKU LKU
WHERE LKV.LKU_KEY=LKU.LKU_KEY
AND
LKU_TYPE_STRING_KEY= 'Lookup.EBS.UMX.Roles'
```

If the lookup query does not meet all of these conditions, then the lookup definition displays and stores only Code Key values.

5.1.59 Test Connectivity Option Does Not Work for the SoD Engine IT Resource (Bug 8504052)

The Test Connectivity option does not work for the IT resource that you create to hold information about the SoD engine.

5.1.60 Users Data Object of Microsoft Active Directory Connector Overwrites the Users Data Object of Oracle Role Manager Integration Library (Bug 8501702)

The following issue is observed if the Microsoft Active Directory connector is installed after the Oracle Role Manager Integration Library is installed:

The Users data object of the Microsoft Active Directory connector overwrites the Users data object of the Oracle Role Manager Integration Library.

To work around this issue:

1. Log in to the Design Console.
2. Expand **Development Tools**.
3. Click **Data Object Manager** under Business Rule Definition.
4. Search for and open **Users**.
5. Click the **Assign** button for Post-update.
6. Assign the **adpOIMUSERCREATEORUPDATEINORM** entity adapter.
7. Click the **Assign** button for Post-delete.
8. Assign the **adpOIMUSERDELETEINORM** entity adapter.
9. Click **Map Adapters**.
10. Select the **adpOIMUSERCREATEORUPDATEINORM** adapter.
11. Map the **userKey** variable to the **USR_KEY** entity field.
12. Select the **adpOIMUSERDELETEINORM** adapter.
13. Map the **userKey** variable to the **USR_KEY** entity field.

14. Save the changes.

5.1.61 Bulk Load Utility Can Load User Data Containing First Name Values That Are Up To 255 Characters in Length (Bug 8519266)

The length of the `USR.USR_FIRST_NAME` column is 256 characters. However, the Bulk Load Utility can only import First Name values that are less than or equal 255 characters in length.

5.2 Design Console Known Issues

This section describes known issues related to tasks performed using the Release 9.1.0.2 Design Console—it does not contain known issues related to the installation of the Design Console or its translated text. This section contains the following topics:

- [Section 5.2.1, "Invoking FVC Utility on IBM WebSphere May Display "Realm/Cell is Null" Error \(Bug 5563654\)"](#)
- [Section 5.2.2, "Form Designer Feature Does Not Support Special Characters for Column Name \(Bug 5373011\)"](#)
- [Section 5.2.3, "Default Tasks Not Added to Resource Object After Changing Its Process Definition Type \(Bug 5637994\)"](#)
- [Section 5.2.4, "Cannot Delete User Defined Fields When the Required and Visible Properties are Set to True \(Bug 5486223\)"](#)
- [Section 5.2.5, "Cannot Save Multiple Rules Simultaneously \(Bug 5457386\)"](#)
- [Section 5.2.6, "Toolbars in Creating New Task Window May Be Disabled When Multiple Creating New Task Windows Are Open \(Bug 5514864\)"](#)
- [Section 5.2.7, "Error Thrown When the Caret \(^\) Character Is Encountered in a Challenge Question"](#)
- [Section 5.2.8, "Error Messages Displayed on the Password Policies Form Are Concatenated \(Bug 6444500\)"](#)
- [Section 5.2.9, "User Group Name Attribute for Reconciliation Mapping \(Bug 6608943\)"](#)
- [Section 5.2.10, "Single Quotation Mark Cannot Be Included in IT Resource Instance Name \(Bug 6643202\)"](#)
- [Section 5.2.11, "Passwords As Child Table Fields Are Not Supported \(Bug 6703251\)"](#)

5.2.1 Invoking FVC Utility on IBM WebSphere May Display "Realm/Cell is Null" Error (Bug 5563654)

When attempting to use the FVC utility in IBM WebSphere deployments, a dialog box with the error message `Realm/cell is Null` may be displayed. You can close the dialog box and ignore this error message to continue.

To avoid this issue entirely, change the properties in the `WEBSHERE_HOME\AppClient\properties\sas.client.props` file to the following:

Note: `WEBSHERE_HOME` represents the location where IBM WebSphere is installed.

Change the existing values to the following:

- `Com.ibm.CORBA.loginSource = properties`
- `Com.ibm.CORBA.loginTimeout = 300`
- `Com.ibm.CORBA.securityEnabled = true`
- `Com.ibm.CORBA.loginUserid = xelsysadm`
- `Com.ibm.CORBA.loginPassword = xelsysadm`

5.2.2 Form Designer Feature Does Not Support Special Characters for Column Name (Bug 5373011)

The Form Designer form in the Design Console will not save entries that contain any of the following special characters in the Column Name field:

`;/ % = | + , \ ' " < >`

5.2.3 Default Tasks Not Added to Resource Object After Changing Its Process Definition Type (Bug 5637994)

In the Design Console, after changing the Process Definition type for a Resource Object from Approval to Provisioning, or from Provisioning to Approval, the Resource Object is not updated with the default tasks associated with each type of Process Definition. To avoid this issue, do not change the Process Definition type after setting it initially.

5.2.4 Cannot Delete User Defined Fields When the Required and Visible Properties are Set to True (Bug 5486223)

Attempting to delete User Defined Fields in the Design Console when the **Required** and **Visible** properties are set to **true** causes an error message to be displayed. To avoid this issue, first delete the properties and then delete the User Defined Column.

5.2.5 Cannot Save Multiple Rules Simultaneously (Bug 5457386)

The Rule Designer feature in the Design Console cannot save multiple rules simultaneously. To avoid this issue, save each rule before creating additional rules.

5.2.6 Toolbars in Creating New Task Window May Be Disabled When Multiple Creating New Task Windows Are Open (Bug 5514864)

Toolbars in the **Creating New Task** window may be disabled after adding event handlers or adapters from the **Integration** tab when using the same **Create New Task** window for a second time to add a task (by clicking the **New Form** icon). To avoid this issue, close the **Creating New Task** window before creating another task.

5.2.7 Error Thrown When the Caret (^) Character Is Encountered in a Challenge Question

While setting challenge questions in the `Lookup.WebClient.Questions` lookup definition, you must not include the caret (^) character in the text of the questions. The Design Console does not stop you from entering this character, but the Administrative and User Console will throw an error when this character is encountered.

5.2.8 Error Messages Displayed on the Password Policies Form Are Concatenated (Bug 6444500)

An error message is displayed if there is conflicting input on the Password Policies form. For example, an error message is displayed if the minimum password length

specified is greater than the maximum length. If there is more than one set of conflicting input, then the errors messages that are displayed are concatenated.

5.2.9 User Group Name Attribute for Reconciliation Mapping (Bug 6608943)

While defining reconciliation field mappings for trusted sources, you must not use the User Group Name user attribute.

5.2.10 Single Quotation Mark Cannot Be Included in IT Resource Instance Name (Bug 6643202)

Single quotation marks are not supported in the name of an IT resource. If a single quotation mark is included in the Name field on the IT Resources form, then a system error message is displayed.

5.2.11 Passwords As Child Table Fields Are Not Supported (Bug 6703251)

Although you can use the Design Console to mark child table fields as password fields, Oracle Identity Manager does not support passwords as child table fields.

5.3 Reports Known Issues

This section describes known issues related to reporting functionality in Release 9.1.0.2. This section contains the following topics:

- [Section 5.3.1, "Group Membership History Report Does Not Differentiate Between Active and Deleted Groups \(Bug 5249535\)"](#)
- [Section 5.3.2, "User Disabled and User Unlocked Reports Display Current Values \(Bug 6371878\)"](#)
- [Section 5.3.3, "Resource Name Lookup Window on the Input Parameters Page for Some Reports May Incorrectly Display Organization Resources \(Bug 5493332\)"](#)
- [Section 5.3.4, "Reports May Not Differentiate Between Information for Deleted Users and Information for Users Created with the Same User IDs As the Deleted Users \(Bug 5741951\)"](#)
- [Section 5.3.5, "java.lang.ClassNotFoundException or java.lang.NullPointerException May Be Encountered When You Run the GenerateSnapshot.sh or GenerateGPASnapshot.sh Script on Oracle WebLogic Server \(Bugs 7655637 and 7658820\)"](#)
- [Section 5.3.7, "tcDataAccessException Encountered on Generating the Password Reset Success Failure Report on an Oracle Identity Manager Installation Using Microsoft SQL Server \(Bug 7654516\)"](#)
- [Section 5.3.8, "Results Might Note Be Generated If UDF Is Added to the Resource Access List Report \(Bug 6887926\)"](#)
- [Section 5.3.9, "classnotfoundexception Exception Encountered While Running the UpgradeAttestation Script on an Oracle Identity Manager Installation Using Microsoft SQL Server \(Bug 7699259\)"](#)
- [Section 5.3.10, "Error Encountered When the UpgradeAttestation Script Is Run Twice on the Same Oracle Identity Manager Installation That Is Using Microsoft SQL Server \(Bug 7758475\)"](#)
- [Section 5.3.11, "Report Not generated If a UDF Is Added to the ResourceAccessList Report \(Bug 6887926\)"](#)

- Section 5.3.12, "System Error Encountered on Running the Policy List Report with a Wildcard Character on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7654460)"
- Section 5.3.13, "CORBA.NO_PERMISSION Exception Might Be Encountered on Running the Generatesnapshot or GenerateGPASnapshot Script (Bugs 8428517 and 8474392)"
- Section 5.3.14, "ora-01858 Exception Might Be Encountered On Generating an Entitlement Report in a Non-English Locale (Bug 8499200)"
- Section 5.3.15, "Error Encountered on Trying to Modify a Resource Through the Resource Management Feature (Bug 8495892)"
- Section 5.3.16, "BI Publisher Reports Do Not Work on Microsoft SQL Server (Bug 8421216)"

5.3.1 Group Membership History Report Does Not Differentiate Between Active and Deleted Groups (Bug 5249535)

When you run a Group Membership History report, the report results do not differentiate between active and deleted groups.

5.3.2 User Disabled and User Unlocked Reports Display Current Values (Bug 6371878)

The User Profile columns in the User Disabled and User Unlocked reports display current values instead of historical values.

5.3.3 Resource Name Lookup Window on the Input Parameters Page for Some Reports May Incorrectly Display Organization Resources (Bug 5493332)

In the Administrative and User Console, clicking the **Resource Name** lookup icon on the **Input Parameters** page for various reports will display a lookup window. This lookup window may incorrectly display Organization resources in addition to User resources for the following reports:

- Resource Access List
- Entitlement Summary
- Resource Access List History
- Resource Password Expiration
- Account Activity in Resource
- Task Assignment History
- Rogue Accounts By Resource
- Fine Grained Entitlement Exceptions By Resource

Ignore the Organization resources listed in the lookup window. Running these reports for Organization resources will return no data.

5.3.4 Reports May Not Differentiate Between Information for Deleted Users and Information for Users Created with the Same User IDs As the Deleted Users (Bug 5741951)

Reports may not differentiate between information for a deleted user and information for a user that was created with the same user ID as the deleted user, regardless of whether or not the User ID Reuse property is enabled.

5.3.5 `java.lang.ClassNotFoundException` or `java.lang.NullPointerException` May Be Encountered When You Run the `GenerateSnapshot.sh` or `GenerateGPASnapshot.sh` Script on Oracle WebLogic Server (Bugs 7655637 and 7658820)

When you run the `GenerateSnapshot.sh` or `GenerateGPASnapshot.sh` script on Oracle WebLogic Server, the `java.lang.ClassNotFoundException` or `java.lang.NullPointerException` may be encountered. If this happens, then first verify the value of the `SQL_SERVER_DRIVER_DIR` variable in the script. Then, change the value of the `CLASSPATH` environment variable in the script file from:

```
%CLASSPATH%;%SQL_SERVER_DRIVER_DIR%\msbase.jar;%SQL_SERVER_DRIVER_DIR%\mssqlserver.jar;%SQL_SERVER_DRIVER_DIR%\msutil.jar;
```

To one of the following:

For Microsoft SQL Server:

```
%CLASSPATH%;%SQL_SERVER_DRIVER_DIR%\sqljdbc.jar;WL_HOME\server\lib\wlclient.jar
```

For Oracle Database

```
%CLASSPATH%;WL_HOME\server\lib\wlclient.jar
```

5.3.6 `java.lang.ClassNotFoundException` Might Be Encountered When You Run the `GenerateSnapshot.sh` or `GenerateGPASnapshot.sh` Script on JBoss Application Server (Bug 7833924)

When you run the `GenerateSnapshot.sh` or `GenerateGPASnapshot.sh` script on JBoss Application Server, the `java.lang.ClassNotFoundException` might be encountered. If this happens, then:

Remove the following entries from the `CLASSPATH` variable in the script:

- `;%XEL_EXT%\log4j-1.2.8.jar`
- `msbase.jar`
- `mssqlserver.jar`
- `msutil.jar`

Add the `sqljdbc.jar` and `JBOSS_HOME/client/log4j.jar` entries to the `CLASSPATH` variable in the script.

5.3.7 `tcDataAccessException` Encountered on Generating the Password Reset Success Failure Report on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7654516)

While generating the Password Reset Success Failure report on an Oracle Identity Manager installation using Microsoft SQL Server, a system error might be encountered when you select the Weekly option from the Aggregation Frequency list.

5.3.8 Results Might Not Be Generated If UDF Is Added to the Resource Access List Report (Bug 6887926)

If Oracle Identity Manager is using Microsoft SQL Server, then results might not be generated if you add a UDF to the Resource Access List report.

5.3.9 classnotfoundexception Exception Encountered While Running the UpgradeAttestation Script on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7699259)

The classnotfoundexception exception might be encountered while running the UpgradeAttestation script on an Oracle Identity Manager installation using Microsoft SQL Server. If this exception is encountered, then open the UpgradeAttestation script in a text editor and implement the following changes:

1. Change ; \$CLASS_PATH to : \$CLASSPATH.

Note: Ensure that the semicolon (;) at the start of the text is replaced with a colon (:).

2. Ensure that the sqljdbc.jar file from the Microsoft SQL Server driver is included in the CLASSPATH.

5.3.10 Error Encountered When the UpgradeAttestation Script Is Run Twice on the Same Oracle Identity Manager Installation That Is Using Microsoft SQL Server (Bug 7758475)

The UpgradeAttestation script is meant to be run only one on a particular Oracle Identity Manager installation that is using Microsoft SQL Server. If you run the script twice on the same Oracle Identity Manager installation, then the following error is thrown and attestation would not work after the upgrade:

```
com.microsoft.sqlserver.jdbc.SQLServerException: Column names in each table must be unique. Column name 'APD_ATTESTATION_DEFINITION' in table 'APD' is specified more than once
```

5.3.11 Report Not generated If a UDF Is Added to the ResourceAccessList Report (Bug 6887926)

If you run the ResourceAccessList report after adding a UDF, then a blank page is displayed.

5.3.12 System Error Encountered on Running the Policy List Report with a Wildcard Character on an Oracle Identity Manager Installation Using Microsoft SQL Server (Bug 7654460)

If you try to run the Policy List Report with a wildcard character, then a system error might be encountered. This issue is encountered only on an Oracle Identity Manager installation using Microsoft SQL Server.

5.3.13 CORBA.NO_PERMISSION Exception Might Be Encountered on Running the Generatesnapshot or GenerateGPASnapshot Script (Bugs 8428517 and 8474392)

On an Oracle Identity Manager installation running on IBM WebSphere Application Server and using Microsoft SQL Server, you might encounter the CORBA.NO_PERMISSION exception when you run the Generatesnapshot or GenerateGPASnapshot script. To address this issue, map roles to user groups as follows:

1. Log in to the WebSphere Administrative Console.
2. Expand **Applications**, select **Enterprise Applications**, select **Xellerate**, and then select **Security role to user/group mapping**.

3. Select **Everyone**.
4. Click **OK**, and then click **Save**.
5. Restart the application server.
6. Rerun the `GenerateSnapshot` or `GenerateGPASnapshot` script.

5.3.14 ora-01858 Exception Might Be Encountered On Generating an Entitlement Report in a Non-English Locale (Bug 8499200)

The ora-01858 exception might be encountered on generating an entitlement report in a non-English locale.

5.3.15 Error Encountered on Trying to Modify a Resource Through the Resource Management Feature (Bug 8495892)

An error encountered on trying to modify a resource through the resource management feature. You can work around this error by clicking **OK** and closing the error message.

5.3.16 BI Publisher Reports Do Not Work on Microsoft SQL Server (Bug 8421216)

The BI Publisher reports do not work on Microsoft SQL Server.

5.4 Globalization Known Issues

This section describes known issues in Release 9.1.0.2 related only to globalization or translation. This section contains the following topics:

- [Section 5.4.1, "Installer Programs for Non-English Languages May Contain Some English Text \(Bug 5232751\)"](#)
- [Section 5.4.2, "Some Administrative and User Console Windows Display Text for Default Locale Setting After Timing Out \(Bug 5545626\)"](#)
- [Section 5.4.3, "Notes Field on the Task Details Page Not Localized For Reconciliation Tasks \(Bug 5512136\)"](#)
- [Section 5.4.4, "English Characters Required for Some Attributes"](#)
- [Section 5.4.5, "Some Information in Workflow Visualizer May Be Displayed as Box Characters \(Bug 5704436\)"](#)
- [Section 5.4.6, "Report in Non-English Environments Requires English Values for Filter Parameters \(Bug 5511190\)"](#)
- [Section 5.4.7, "Deployment Manager Import and Export Features Include an Untranslatable String \(Bug 5501127\)"](#)
- [Section 5.4.8, "Names of Log Files for Oracle Identity Manager Utilities Do Not Include Time Stamp for Some Non-English Locales \(Bug 5850607\)"](#)
- [Section 5.4.9, "Pre-Populate Adapter Error Messages Do Not Support Localized Display of Date and Time"](#)
- [Section 5.4.10, "Some Asian Languages Not Displayed Correctly With Sun JDK 1.4 \(Bug 6314961\)"](#)
- [Section 5.4.11, "Names of IT Resource Parameters Displayed in the Administrative and User Console Are Not Localized \(Bug 6455617\)"](#)

- Section 5.4.12, "Inconsistent Ordering of Names in Columns of Some Reports in Non-English Environments (Bugs 5557974 and 6457618)"
- Section 5.4.13, "Error Message Displayed While Trying to Delete Menu Items Is Not Localized (Bug 6503868)"
- Section 5.4.14, "Localization to the Chinese (Simplified), Chinese (Traditional), and Portuguese (Brazilian) Languages Not Supported (Bug 6728226)"
- Section 5.4.15, "Group Name Field Is Displayed in English (Bug 6816544)"
- Section 5.4.16, "Resource Bundle Entry for SoD Not Localized (Bugs 8303480 and 8504055)"
- Section 5.4.17, "UI Text on Generic Technology Connector Pages of Administrative and User Console Is Not Localized for the Arabic Language (Bug 8516213)"

5.4.1 Installer Programs for Non-English Languages May Contain Some English Text (Bug 5232751)

The Installer programs for non-English languages may contain some untranslated text that is displayed in English.

5.4.2 Some Administrative and User Console Windows Display Text for Default Locale Setting After Timing Out (Bug 5545626)

In the Administrative and User Console, if the Export and Import pages of the Deployment Manager or the Workflow Visualizer page are open and the session times out, then the text on these pages may be displayed in the language of the default locale of the system where Oracle Identity Manager is installed. After closing the session timeout window and clicking any of the Administrative and User Console menu options, the Oracle Identity Manager Logout page is displayed and may also be displayed in the language of the default locale of the system where Oracle Identity Manager is installed.

5.4.3 Notes Field on the Task Details Page Not Localized For Reconciliation Tasks (Bug 5512136)

In the Administrative and User Console, some text in the **Notes** field on the **Task Details** page may be displayed in English in non-English environments. Task instances that have the following names may encounter this issue:

- Reconciliation Update Received
- Reconciliation Insert Received
- Reconciliation Delete Received

5.4.4 English Characters Required for Some Attributes

Release 9.1.0.2 requires that you use only English characters for the following:

- Installation paths and directory names (Bug 5397854)
- Host names (Bug 5360993)
- E-mail addresses (Bug 5397105)
- If used, external certificate names and certificate content (Bug 5387397)
- The Administrative and User Console requires that you use only English characters for the E-mail Address fields on the **Create/Edit User**, **Account Profile**, and **Self-Registration** pages. In addition, when installing the Remote Manager,

you must use only English characters for the Service Name on the **Configuration** page (Bug 5460100).

Refer to *Oracle Identity Manager Globalization Guide* for detailed information about the character restrictions for various components and attributes.

5.4.5 Some Information in Workflow Visualizer May Be Displayed as Box Characters (Bug 5704436)

Some information may be displayed as box characters in the Workflow Visualizer of the Administrative and User Console due to a known limitation with Java Applets and globalized characters. The browser JVM displays only those characters that are in the current locale of the system where Oracle Identity Manager is installed. Globalized characters are displayed correctly in applets only if you set the browser to the same locale as the system where Oracle Identity Manager is installed.

5.4.6 Report in Non-English Environments Requires English Values for Filter Parameters (Bug 5511190)

In non-English environments, the following report requires that the given filter parameter use only English values:

Report: Entitlement Summary

Filter parameter: Account Status

For example, filtering on Account Status in the Entitlement Summary report in non-English environments and using a translated version of the status *Active* will return nothing. You must use the English value *Active*.

5.4.7 Deployment Manager Import and Export Features Include an Untranslatable String (Bug 5501127)

The Administrative and User Console's Deployment Manager import and export features use the Java AWT file dialog box that shows the All Files (*.*) string in the dialog box filter. The All Files (*.*) string is not translated for any locale and is displayed in English. This limitation is caused by the Java implementation, and the string cannot be translated. For more information, refer to the Sun Microsystems report for Bug ID 4152317 at

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4152317

5.4.8 Names of Log Files for Oracle Identity Manager Utilities Do Not Include Time Stamp for Some Non-English Locales (Bug 5850607)

When you use the Reconciliation Archival utility or Task Archival utility, or Oracle Identity Manager Database Validator, the name of the log files for some non-English environments may not include the time stamp. For example, for the Reconciliation Archival utility, you may see a log file that looks something like Arch_Recon____15_56.log instead of Arch_Recon_Wed_31_2007_03_31.log.

5.4.9 Pre-Populate Adapter Error Messages Do Not Support Localized Display of Date and Time

The server-side date and time displayed in the error message on the Administrative and User Console when a pre-populate adapter error is encountered are not localized.

5.4.10 Some Asian Languages Not Displayed Correctly With Sun JDK 1.4 (Bug 6314961)

Some Asian languages may not be displayed correctly with Sun JDK 1.4 on the Deployment Manager if you launch it on a non-Asian Windows computer in spite of installing a language package on the client host. If you encounter this issue, install SUN Java Plug-in 1.5.

5.4.11 Names of IT Resource Parameters Displayed in the Administrative and User Console Are Not Localized (Bug 6455617)

The names of IT resource parameters displayed on the "Manage IT Resources" pages of the Administrative and User Console are not localized.

5.4.12 Inconsistent Ordering of Names in Columns of Some Reports in Non-English Environments (Bugs 5557974 and 6457618)

In non-English environments, the ordering of first and last names in some reports does not correspond to the browser locale of the logged in user. [Table 4](#) lists the reports and their columns in which first and last names may be displayed in inconsistent order. You can modify the display of first and last names by modifying the stored procedures for these reports.

Table 4 Reports and Columns in Which First and Last Names May Be Inconsistently Ordered

Report	Sectional Header	Sectional Table	Display Format
Attestation Requests by Process	Reviewer	NA	FirstName LastName
Attestation Process List	NA	Reviewer	FirstName LastName
Policy List	NA	Created By	FirstName MiddleName LastName
Policy Detail	Created By	NA	FirstName LastName
Organization Structure	NA	Manager Name	FirstName MiddleName LastName
Requests Initiated	NA	Requester	FirstName MiddleName LastName
Requests Details by Status	Requester	NA	FirstName MiddleName LastName
Group Membership	Group Created By	NA	FirstName LastName
Task Assignment History	NA	Assigner User Name	FirstName LastName
Account Activity in Resource	NA	Manager Name	FirstName LastName
User Resource Access History	NA	Manager Name, Provisioned By	FirstName LastName
Group Membership History	Group Created By	NA	FirstName LastName

5.4.13 Error Message Displayed While Trying to Delete Menu Items Is Not Localized (Bug 6503868)

While trying to delete a menu item, you may encounter an error message that is not localized.

5.4.14 Localization to the Chinese (Simplified), Chinese (Traditional), and Portuguese (Brazilian) Languages Not Supported (Bug 6728226)

If Oracle Single Sign-On is used to provide authentication service to Oracle Identity Manager, then localization to the Chinese (Simplified), Chinese (Traditional), and Portuguese (Brazilian) languages is not supported. This is due to a known bug (6728226) in the Oracle Single Sign-On Plug-in deployed on Oracle HTTP Server.

5.4.15 Group Name Field Is Displayed in English (Bug 6816544)

The Group Name Field label is always displayed in English, regardless of the locale you set.

Note: Changes made in the resource bundles are listed in the ["Customizations"](#) section.

5.4.16 Resource Bundle Entry for SoD Not Localized (Bugs 8303480 and 8504055)

The following label in the resource bundle is displayed in English on the console even when you use a locale other than English:

```
global.xmlmetadata.request.object.SoDResult=SOD Result
```

In addition, the TopologyName IT resource parameter label has not been translated.

5.4.17 UI Text on Generic Technology Connector Pages of Administrative and User Console Is Not Localized for the Arabic Language (Bug 8516213)

UI text on the Generic Technology Connector pages of the Administrative and User console is not localized for the Arabic language.

6 Customizations

The following sections list all the Oracle Identity Manager user interface (UI) related files that have been modified:

- [Section 6.1, "Customizations in Release 9.1.0.2"](#)
- [Section 6.2, "Customizations in Release 9.1.0.1"](#)

6.1 Customizations in Release 9.1.0.2

The following sections list items customized in release 9.1.0.2:

- [Section 6.2.1, "JavaServer Pages"](#)
- [Section 6.2.2, "Java Files"](#)
- [Section 6.2.3, "Properties File"](#)

6.1.1 JavaServer Pages

The following JavaServer pages have been added or modified in release 9.1.0.2:

SystemVerificationWeb\pages\FilterErrorPage.jsp
SystemVerificationWeb\error.jsp
SystemVerificationWeb\Login.jsp
SystemVerificationWeb\welcome.jsp
SystemVerificationWeb\index.jsp
web\tiles\common\tjspFooter.jsp
web\tiles\common\tjspHeader.jsp
web\tiles\util\CIWGenCstUtil.jsp
web\tiles\util\DualListComponent.jsp
web\tiles\util\ReportFormFieldsDisplay.jsp
web\tiles\util\TableGenerator.jsp
web\tiles\util\TablePagingLinks.jsp
web\tiles\util\tcGenerateCreateITResourceForm.jsp
web\tiles\util\tjspForm.jsp
web\tiles\util\tjspGenerateCreateForm.jsp
web\tiles\util\tjspGenerateCreateOrganizationForm.jsp
web\tiles\util\tjspGenerateCreateUserForm.jsp
web\tiles\util\tjspGenerateEditForm.jsp
web\tiles\util\tjspGenerateSchTaskEditForm.jsp
web\tiles\AccessPoliciesSearchResultsTiles.jsp
web\tiles\AccessPolicyAllChildFormsFooterTiles.jsp
web\tiles\AccessPolicyChildFormFooterTiles.jsp
web\tiles\AccessPolicyDetailsTiles.jsp
web\tiles\AccessPolicyEditPopupChildFormTilesInclude.jsp
web\tiles\AccessPolicyEditPopupFormTilesInclude.jsp
web\tiles\AccessPolicyEditSequencePopupChildFormTilesInclude.jsp
web\tiles\AccessPolicyFinalStepFooterTiles.jsp
web\tiles\AccessPolicyFirstStepFooterTiles.jsp
web\tiles\AccessPolicyFormChildTablesTiles.jsp
web\tiles\AccessPolicyFormsNoticeWizardFooterTiles.jsp
web\tiles\AccessPolicyObjectFormTilesInclude.jsp
web\tiles\AccessPolicyObjProcFormsWizardFooterTiles.jsp
web\tiles\AccessPolicyProcessFormTilesInclude.jsp
web\tiles\AccessPolicyProvideChildDataTilesInclude.jsp
web\tiles\AddNotesForTaskTiles.jsp
web\tiles\ApprovalTaskHistoryTiles.jsp

web\tiles\ApprovalTasksAssignedToManagedUsersTiles.jsp
web\tiles\ApprovalTasksReassignToGroupTiles.jsp
web\tiles\ApprovalTasksReassignToUserTiles.jsp
web\tiles\AssignAdminUsersTiles.jsp
web\tiles\AssignResourceAdministratorsTiles.jsp
web\tiles\AssignResourceAuditObjectivesTiles.jsp
web\tiles\AssignResourceAuthorizersTiles.jsp
web\tiles\AssociatedOrganizationsForResourceTiles.jsp
web\tiles\AssociatedUsersForResourceTiles.jsp
web\tiles\AttestationAdminAclTiles.jsp
web\tiles\AttestationAssignAdministratorsTiles.jsp
web\tiles\AttestationDashboardTiles.jsp
web\tiles\AttestationEditDetailsTilesInclude.jsp
web\tiles\AttestationEditUserScopeTiles.jsp
web\tiles\AttestationExecuteRequestDetailsTiles.jsp
web\tiles\AttestationResourceScopeEditTilesInclude.jsp
web\tiles\AttestationSearchResultsTiles.jsp
web\tiles\AttestationUpdateAdministratorsTiles.jsp
web\tiles\AttestationUserScopeEditTilesInclude.jsp
web\tiles\AttestationViewAttRequestDetailsTiles.jsp
web\tiles\AttestationViewDelegationPathTiles.jsp
web\tiles\AttestationViewDetailsTiles.jsp
web\tiles\AttestationViewExecutionDelegationPathTiles.jsp
web\tiles\AttestationViewRequestDetailsTiles.jsp
web\tiles\AttestationWizardConfirmationTiles.jsp
web\tiles\AttestationWizardExitTiles.jsp
web\tiles\AttestationWizardFinalStepFooterTiles.jsp
web\tiles\AttestationWizardFirstStepFooterTiles.jsp
web\tiles\AttestationWizardFirstTiles.jsp
web\tiles\AttestationWizardResourceScopeTilesInclude.jsp
web\tiles\AttestationWizardScheduleTilesInclude.jsp
web\tiles\AttestationWizardSuccessPageTiles.jsp
web\tiles\AttestationWizardUserScopeTilesInclude.jsp
web\tiles\AttestExecuteHistoryTiles.jsp
web\tiles\changePasswordTiles.jsp
web\tiles\CIWAssignAccessPermissionITResourceTiles.jsp

web\tiles\CIWAssignGroupITResourceTiles.jsp
web\tiles\CIWConfirmDeleteAttributeTiles.jsp
web\tiles\CIWConfirmScheduleTaskTiles.jsp
web\tiles\CIWConInstallTiles.jsp
web\tiles\CIWCreateITResIncludeTiles.jsp
web\tiles\CIWCreateITResourceConnectionTestTiles.jsp
web\tiles\CIWCreateITResourceParametersTiles.jsp
web\tiles\CIWCreateScheduledTaskIncludeTiles.jsp
web\tiles\CIWEditITResourceTiles.jsp
web\tiles\CIWITResourceDependenciesTiles.jsp
web\tiles\CIWManageITResourceTiles.jsp
web\tiles\CIWManageScheduledTaskTiles.jsp
web\tiles\CIWPreInstallStepsTiles.jsp
web\tiles\CIWSchTaskAttributesTiles.jsp
web\tiles\CIWSelectConTiles.jsp
web\tiles\CIWSetITAccessPermissionTiles.jsp
web\tiles\CIWStatusBarTiles.jsp
web\tiles\CIWUpdatePermissionsTiles.jsp
web\tiles\CIWVerifyITResCreationTiles.jsp
web\tiles\CIWVerifyScheduleTaskTiles.jsp
web\tiles\CIWViewITResourceTiles.jsp
web\tiles\CIWViewScheduledTaskTiles.jsp
web\tiles\ConfigureFormDataFlowTiles.jsp
web\tiles\ConfigureReconDataFlowTiles.jsp
web\tiles\ConfirmManualCompleteTasksTiles.jsp
web\tiles\ConfirmReassignTasksTiles.jsp
web\tiles\ConfirmReassignTaskTiles.jsp
web\tiles\ConfirmResponsesForTasksTiles.jsp
web\tiles\ConfirmRetryTasksTiles.jsp
web\tiles\CreateAccessPolicyDetailTiles.jsp
web\tiles\CreateAccessPolicySuccessTiles.jsp
web\tiles\CreateAccessPolicyTiles.jsp
web\tiles\CreateConnectorExitTiles.jsp
web\tiles\CreateGenConTiles.jsp
web\tiles\DelegateEntityWizardFooterTiles.jsp
web\tiles\DenyResourcesByAccessPolicyDetailTiles.jsp

web\tiles\DenyResourcesByAccessPolicyTiles.jsp
web\tiles\detailTasksReassignToGroupTiles.jsp
web\tiles\detailTasksReassignToUserTiles.jsp
web\tiles\DirectProvisionOrganizationWizard_ExitTiles.jsp
web\tiles\DirectProvisionOrganizationWizard_ProvideChildProcessDataTilesInclude.jsp
web\tiles\DirectProvisionOrganizationWizard_ProvideChildResourceDataTilesInclude.jsp
web\tiles\DirectProvisionOrganizationWizard_ProvideParentProcessDataTilesInclude.jsp
web\tiles\DirectProvisionOrganizationWizard_ProvideParentResourceDataTilesInclude.jsp
web\tiles\DirectProvisionOrganizationWizard_VerifyProcessDataTiles.jsp
web\tiles\DirectProvisionOrganizationWizard_VerifyResourceDataTiles.jsp
web\tiles\DirectProvisionUserWizard_ExitTiles.jsp
web\tiles\DirectProvisionUserWizard_ProvideChildProcessDataTilesInclude.jsp
web\tiles\DirectProvisionUserWizard_ProvideChildResourceDataTilesInclude.jsp
web\tiles\DirectProvisionUserWizard_ProvideParentProcessDataTilesInclude.jsp
web\tiles\DirectProvisionUserWizard_ProvideParentResourceDataTilesInclude.jsp
web\tiles\DirectProvisionUserWizard_VerifyProcessDataTiles.jsp
web\tiles\DirectProvisionUserWizard_VerifyResourceDataTiles.jsp
web\tiles\DisplayPasswordPolicyTiles.jsp
web\tiles\MyProxyConfirmProxyAssignTiles.jsp
web\tiles\MyProxyConfirmProxyRemoveTiles.jsp
web\tiles\MyProxyNoProxyDefinedTiles.jsp
web\tiles\MyProxyViewProxyAssignTilesInclude.jsp
web\tiles\MyProxyViewTiles.jsp
web\tiles\OpenTasksTiles.jsp
web\tiles\OrgResourceProfileConfirmRetryTasksTiles.jsp
web\tiles\OrgResourceProfileProvisioningTasksTiles.jsp
web\tiles\ProvideProvisioningDataNoticeTiles.jsp
web\tiles\ProvisionedResourcesForUserTiles.jsp
web\tiles\ProvisionResourcesByAccessPolicyDetailTiles.jsp
web\tiles\ProvisionResourcesByAccessPolicyTiles.jsp
web\tiles\ReportDisplayTiles.jsp
web\tiles\ReportTabularDisplayTiles.jsp
web\tiles\requestApprovalDetailTiles.jsp
web\tiles\requestCommentAddTiles.jsp

web\tiles\requestCommentTiles.jsp
web\tiles\requestDetailTiles.jsp
web\tiles\requestEntityDetailTilesInclude.jsp
web\tiles\requestEntityTiles.jsp
web\tiles\requestHistoryTiles.jsp
web\tiles\requestMoreInfoObjectTiles.jsp
web\tiles\requestMoreInfoRequestTiles.jsp
web\tiles\requestOrganizationProvisionDetailTiles.jsp
web\tiles\requestProvisionDetailTiles.jsp
web\tiles\requestResourceResolutionTiles.jsp
web\tiles\requestResourceTiles.jsp
web\tiles\requestTrackTiles.jsp
web\tiles\requestTrackTilesInclude.jsp
web\tiles\ResourceAdministratorsTiles.jsp
web\tiles\ResourceAuditObjectivesTiles.jsp
web\tiles\ResourceAuthorizersTiles.jsp
web\tiles\ResourceProfileConfirmRetryTasksTiles.jsp
web\tiles\ResourceProfileProvisioningTasksTiles.jsp
web\tiles\ResourceWorkflowsTiles.jsp
web\tiles\SearchGroupTiles.jsp
web\tiles>SelectGroupsForAccessPolicyDetailTiles.jsp
web\tiles>SelectGroupsForAccessPolicyTiles.jsp
web\tiles\SetResponseForSingleTaskTiles.jsp
web\tiles\SpecifyAdminPermissionsTiles.jsp
web\tiles\SpecifyGroupAliasTiles.jsp
web\tiles\SpecifyResponsesForTasksTiles.jsp
web\tiles\TaskDetailsTiles.jsp
web\tiles\TaskHistoryTiles.jsp
web\tiles\TaskShowAllStatusTiles.jsp
web\tiles\TasksReassignToGroupTiles.jsp
web\tiles\TasksReassignToUserTiles.jsp
web\tiles\tjspAccessPolicyExitTiles.jsp
web\tiles\tjspAccountOptionsTiles.jsp
web\tiles\tjspAddResourceObjectTiles.jsp
web\tiles\tjspAddTargetUserErrorTiles.jsp
web\tiles\tjspAddTargetUserTiles.jsp

web\tiles\tjspAssignConfirmContentTiles.jsp
web\tiles\tjspAssignConfirmTiles.jsp
web\tiles\tjspAssignListContentTiles.jsp
web\tiles\tjspAssignListTiles.jsp
web\tiles\tjspChallengeQuestionTiles.jsp
web\tiles\tjspChangeChallengeQuestionsTiles.jsp
web\tiles\tjspChangePasswordCompleteTiles.jsp
web\tiles\tjspChangePasswordTiles.jsp
web\tiles\tjspCompleteDraftRequestTiles.jsp
web\tiles\tjspConfirmAssignOrganizationAdministratorsStep1Tiles.jsp
web\tiles\tjspConfirmAssignOrganizationResourceObjectsStep1Tiles.jsp
web\tiles\tjspConfirmMoveSubOrganizationsStep1Tiles.jsp
web\tiles\tjspConfirmUpdateOrganizationAdministratorsStep1Tiles.jsp
web\tiles\tjspConformationLogoffTiles.jsp
web\tiles\tjspCreateGroupTilesInclude.jsp
web\tiles\tjspCreateOrganizationTilesInclude.jsp
web\tiles\tjspCreateRequestHomeTiles.jsp
web\tiles\tjspCreateRequestTiles.jsp
web\tiles\tjspCreateUserIncludeTiles.jsp
web\tiles\tjspCustomLookupFormTiles.jsp
web\tiles\tjspDisplayCommentTiles.jsp
web\tiles\tjspDisplayTrackSearchTiles.jsp
web\tiles\tjspEditGroupTilesInclude.jsp
web\tiles\tjspEditOrganizationConfirmationTilesInclude.jsp
web\tiles\tjspEditUserTilesInclude.jsp
web\tiles\tjspListOfTasksTiles.jsp
web\tiles\tjspLoginHelpTiles.jsp
web\tiles\tjspLogoffTiles.jsp
web\tiles\tjspLogoffTimeoutTiles.jsp
web\tiles\tjspLogonTiles.jsp
web\tiles\tjspLookupFormTiles.jsp
web\tiles\tjspModifyProfileSavedTiles.jsp
web\tiles\tjspModifyProfileTilesInclude.jsp
web\tiles\tjspMoveOrganizationUsersConfirmationTiles.jsp
web\tiles\tjspPasswordExpiredTiles.jsp
web\tiles\tjspProvideChallengeAnswersConfirmTiles.jsp

web\tiles\tjspProvideChallengeAnswersTiles.jsp
web\tiles\tjspProvideDataChildFormTilesInclude.jsp
web\tiles\tjspProvideDataParentFormTilesInclude.jsp
web\tiles\tjspRegistrationHelpTiles.jsp
web\tiles\tjspRemoveTargetUserConfirmationTiles.jsp
web\tiles\tjspRequestActResourceVerificationTiles.jsp
web\tiles\tjspRequestAdditionalInformationTilesInclude.jsp
web\tiles\tjspRequestCommentTiles.jsp
web\tiles\tjspRequestEditCommentTiles.jsp
web\tiles\tjspRequestMoreInfoTiles.jsp
web\tiles\tjspRequestScheduleFooterTiles.jsp
web\tiles\tjspRequestScheduleTilesInclude.jsp
web\tiles\tjspRequestSelectResourceTiles.jsp
web\tiles\tjspRequestSelectTargetTiles.jsp
web\tiles\tjspRequestShowResolutionTiles.jsp
web\tiles\tjspRequestSubmitErrorTiles.jsp
web\tiles\tjspRequestSubmitTiles.jsp
web\tiles\tjspRequestTargetTypeTiles.jsp
web\tiles\tjspRequestVerificationTiles.jsp
web\tiles\tjspRequestWizardAdminTiles.jsp
web\tiles\tjspRequestWizardExitTiles.jsp
web\tiles\tjspRequestWizardFooterTiles.jsp
web\tiles\tjspRequestWizardResourceTiles.jsp
web\tiles\tjspResetPasswordCompleteTiles.jsp
web\tiles\tjspResetPasswordTiles.jsp
web\tiles\tjspSearchGroupResultsTiles.jsp
web\tiles\tjspSearchUserResultsTiles.jsp
web\tiles\tjspSelfRegistrationNotAllowedTiles.jsp
web\tiles\tjspSelfRegistrationResultTiles.jsp
web\tiles\tjspSelfRegistrationTiles.jsp
web\tiles\tjspSelfRegTrackRequestTiles.jsp
web\tiles\tjspSetChallengeAnswersConfirmTiles.jsp
web\tiles\tjspSetChallengeAnswersTiles.jsp
web\tiles\tjspSetChallengeQuestionsTiles.jsp
web\tiles\tjspShowFormTilesInclude.jsp
web\tiles\tjspTaskApprovalDetailsTiles.jsp

web\tiles\tjspTaskApprovalViewTasksTiles.jsp
web\tiles\tjspTrackRequestTilesInclude.jsp
web\tiles\tjspUserMemberOfAssignTiles.jsp
web\tiles\tjspUserMemberOfDeleteTiles.jsp
web\tiles\tjspUserMemberOfTiles.jsp
web\tiles\tjspVerifyPasswordTiles.jsp
web\tiles\tjspVerifyUserIdTiles.jsp
web\tiles\tjspViewAdministratorsOrganizationDetailsTiles.jsp
web\tiles\tjspViewGroupDetailsTiles.jsp
web\tiles\tjspViewOrganizationDetailsTiles.jsp
web\tiles\tjspViewProfileTiles.jsp
web\tiles\tjspViewResourceProfileOrganizationDetailsTiles.jsp
web\tiles\tjspViewResourcesAllowedOrganizationDetailsTiles.jsp
web\tiles\tjspViewSubOrganizationDetailsTiles.jsp
web\tiles\tjspViewUsersOrganizationDetailsTiles.jsp
web\tiles\tjspWebAdminHomeTiles.jsp
web\tiles\tjspWizardFooterTiles.jsp
web\tiles\tjspWizardHeaderTiles.jsp
web\tiles\tUpdateResourceAdministratorsTiles.jsp
web\tiles\tUserDefinedChildFormEditTilesInclude.jsp
web\tiles\tUserDefinedFormEditTilesInclude.jsp
web\tiles\tUserGroupAdministratorsAssignTiles.jsp
web\tiles\tUserGroupAdministratorsTiles.jsp
web\tiles\tUserGroupAdministratorsUpdatePermissionsTiles.jsp
web\tiles\tUserGroupAssignMembershipRulesTiles.jsp
web\tiles\tUserGroupAssignMenuItemsTiles.jsp
web\tiles\tUserGroupAssignReportsTiles.jsp
web\tiles\tUserGroupConfirmAssignMembershipRulesTiles.jsp
web\tiles\tUserGroupConfirmDeleteMembershipRulesTiles.jsp
web\tiles\tUserGroupMembershipRulesTiles.jsp
web\tiles\tUserGroupMembersTiles.jsp
web\tiles\tUserGroupMenuItemsTiles.jsp
web\tiles\tUserGroupPermissionsTiles.jsp
web\tiles\tUserGroupPoliciesTiles.jsp
web\tiles\tUserGroupReportsTiles.jsp
web\tiles\tUserGroupUnassignedPermissionsTiles.jsp

web\tiles\UserGroupUnassignedPoliciesTiles.jsp
web\tiles\UserGroupUpdatePermissionsTiles.jsp
web\tiles\UserProxyConfirmProxyAssignTiles.jsp
web\tiles\UserProxyConfirmProxyRemoveTiles.jsp
web\tiles\UserProxyNoProxyDefinedTiles.jsp
web\tiles\UserProxyViewProxyAssignTilesInclude.jsp
web\tiles\UserProxyViewTiles.jsp
web\tiles\VerifyAdminUsersTiles.jsp
web\tiles\VerifyInfoForAccessPolicyTiles.jsp
web\pages\FilterErrorPage.jsp
web\layouts\tjspClassicLayout.jsp
web\layouts\tjspMenuNoStruts.jsp
web\layouts\tjspPopUpLayout.jsp
web\gc\ConnectorConfigurationTiles.jsp
web\gc\ConnectorImagePopUpTiles.jsp
web\gc\ConnectorMappingTiles.jsp
web\gc\CreateConnectorBasicTiles.jsp
web\gc\CreateConnectorExitTiles.jsp
web\gc\CreateConnectorSuccessPageTiles.jsp
web\gc\GenConnectorPopUpLayout.jsp
web\gc\GenConnectorTableGenerator.jsp
web\gc\manageConnectorExitTiles.jsp
web\gc\ModifyConnectorAddEditValidationsTiles.jsp
web\gc\ModifyConnectorConfirmationTiles.jsp
web\gc\ModifyConnectorFieldInfoTiles.jsp
web\gc\tjspPopUpLayout.jsp
web\gc\tjspWizardFooterTiles.jsp
web\gc\tjspWizardHeaderTiles.jsp
web\gc\ValidateFormConnectorTiles.jsp
web\dm\dmImportConfirmation.jsp

6.1.2 Java Files

The following Java files have been modified in release 9.1.0.2:

src\com\thortech\xl\webclient\actions\ApprovalsAction.java
src\com\thortech\xl\webclient\actions\AssociatedEntitiesForResourceAction.java
src\com\thortech\xl\webclient\actions\AttestationWizardAction.java
src\com\thortech\xl\webclient\actions\ConnectorInstallProcessAction.java

src\com\thortech\xl\webclient\actions\Constants.java
src\com\thortech\xl\webclient\actions\CreateAccessPolicyAction.java
src\com\thortech\xl\webclient\actions\CreateConnectorAction.java
src\com\thortech\xl\webclient\actions\CreateConnectorPopUpAction.java
src\com\thortech\xl\webclient\actions\DelegateEntityAction.java
src\com\thortech\xl\webclient\actions\DirectProvisionUserAction.java
src\com\thortech\xl\webclient\actions\ManageAccessPoliciesAction.java
src\com\thortech\xl\webclient\actions\ManageAccessPoliciesForm.java
src\com\thortech\xl\webclient\actions\ManageAttestationAction.java
src\com\thortech\xl\webclient\actions\ManageAttestationDashboardAction.java
src\com\thortech\xl\webclient\actions\ManageAttestationTaskAction.java
src\com\thortech\xl\webclient\actions\ManageITResourceAction.java
src\com\thortech\xl\webclient\actions\ManageScheduledTaskAction.java
src\com\thortech\xl\webclient\actions\MyProxyAction.java
src\com\thortech\xl\webclient\actions\MyRequestAction.java
src\com\thortech\xl\webclient\actions\OpenTasksAction.java
src\com\thortech\xl\webclient\actions\OrgResourceProfileProvisioningTasksAction
.java
src\com\thortech\xl\webclient\actions\ProvisionedResourcesForUserAction.java
src\com\thortech\xl\webclient\actions\RegistrationHelpPageAction.java
src\com\thortech\xl\webclient\actions\RequestAction.java
src\com\thortech\xl\webclient\actions\RequestApprovalDetailAction.java
src\com\thortech\xl\webclient\actions\RequestCommentAction.java
src\com\thortech\xl\webclient\actions\RequestProvisionDetailAction.java
src\com\thortech\xl\webclient\actions\RequestStatusHistoryAction.java
src\com\thortech\xl\webclient\actions\RequestTrackAction.java
src\com\thortech\xl\webclient\actions\RequestTrackForm.java
src\com\thortech\xl\webclient\actions\ResourceAdministratorsAction.java
src\com\thortech\xl\webclient\actions\ResourceAuthorizersAction.java
src\com\thortech\xl\webclient\actions\ResourceProfileProvisioningTasksAction.jav
a
src\com\thortech\xl\webclient\actions\SearchGroupAction.java
src\com\thortech\xl\webclient\actions\TaskDetailsAction.java
src\com\thortech\xl\webclient\actions\tcChangePasswordAction.java
src\com\thortech\xl\webclient\actions\tcForgetPasswordAction.java
src\com\thortech\xl\webclient\actions\tcLogonAction.java
src\com\thortech\xl\webclient\actions\tcLookupFieldAction.java

src\com\thortech\xl\webclient\actions\tcManageGroupAction.java
src\com\thortech\xl\webclient\actions\tcManageOrganizationAction.java
src\com\thortech\xl\webclient\actions\tcManageUserAction.java
src\com\thortech\xl\webclient\actions\tcRequestActResourceAction.java
src\com\thortech\xl\webclient\actions\tcRequestUserProvisionResourceAction.java
src\com\thortech\xl\webclient\actions\tcRequestWizardAction.java
src\com\thortech\xl\webclient\actions\tcSearchOrganizationAction.java
src\com\thortech\xl\webclient\actions\tcSearchUserAction.java
src\com\thortech\xl\webclient\actions\tcSelfRegistrationAction.java
src\com\thortech\xl\webclient\actions\tcSelfRegTrackRequestAction.java
src\com\thortech\xl\webclient\actions\tcSetChallengeQuestionsAction.java
src\com\thortech\xl\webclient\actions\tcTaskApprovalDetailsAction.java
src\com\thortech\xl\webclient\actions\tcTrackRequestAction.java
src\com\thortech\xl\webclient\actions\tcUserMemberOfAction.java
src\com\thortech\xl\webclient\actions\tcWebAdminHomeAction.java
src\com\thortech\xl\webclient\actions\tcWebAdminHomeForm.java
src\com\thortech\xl\webclient\actions\UserDefinedFormAction.java
src\com\thortech\xl\webclient\actions\UserGroupAccessPoliciesAction.java
src\com\thortech\xl\webclient\actions\UserGroupAdministratorsAction.java
src\com\thortech\xl\webclient\actions\UserGroupAdministratorsForm.java
src\com\thortech\xl\webclient\actions\UserGroupMembersAction.java
src\com\thortech\xl\webclient\actions\UserGroupMembershipRulesAction.java
src\com\thortech\xl\webclient\actions\UserGroupMembershipRulesForm.java
src\com\thortech\xl\webclient\actions\UserProxyAction.java

6.1.3 Properties File

The following properties have been introduced to support localization of text in release 9.1.0.2:

Properties Added in xldd.properties

global.security.filter=<\s*,<\s*/\s*,\s*>,\s*/\s*>,\s*;

global.label.filterErrorPage=Filter Error Page

global.image.clientlogo=/images/client_logo.gif

global.image.xelleratologo=/images/xellerate-trans-grey.gif

global.image.spacer=/images/spacer.gif

global.error.illegalInput=Illegal Script Tag or Characters

global.image.error=/images/reject.gif

global.error.illegalInputDesc=The User Input Field contains script tags or special characters that are not allowed.

global.label.back=Back
global.label.indicatesrequiredfield=Indicates required field
global.label.button.login=Login
global.label.button.clear=Clear
global.label.asterisk=*
global.label.mandatoryField=Indicates Required Field
global.label.loginErrorPage=Login Error Page
global.error.invalidInput=Invalid Username or Password
global.error.message=Please Contact Administrator
global.label.retry=Try Relogin
logon.message.toLogin=To log in, enter your User ID and password.
logon.label.userid=User ID:
logon.label.password=Password:
logon.label.button.login=Login
logon.label.button.clear=Clear
logoff.link=LOGOUT

Properties Added in xlWebadmin.properties

button.exit=Exit
global.label.offlineprovisioning=Off-line Provisioning
global.label.trustedsource=Trusted Source
global.label.sequencerecon=Sequence Recon
global.error.searchAdviceMaxCount=Please refine your search criteria. The search results reached the max account {0}.
global.xlmetadata.request.object.SoDResult=SOD Status
createuser.error.endDateBeforeCurrentDate=User End Date Error
createuser.error.endDateBeforeCurrentDateDesc=User End date cannot be past or today.
attestation.message.instruction=1. Select the search criteria to use by clicking the appropriate option.
2. Enter the search parameter values.
3. Click the Search button.
(New)trackrequest.message.instruction=1. Select the search criteria to use by entering values in the appropriate search fields .
 2. Enter the search parameter value(s).
 3. Enter comma separated values for searching multiple Request IDs and Resource Names .
 4. Select multiple status by pressing Ctrl button and selecting appropriate values of status.
 5. Click the Search button.
(Old)trackrequest.message.instruction=1. Select the search criteria to use by clicking the appropriate option.
2. Enter the search parameter values.
3. Click the Search button.
(Old)trackrequest.error.select=Specify the search criteria to use by selecting an option.
(new)trackrequest.error.select=Select atleast one search criteria.

users.provisionedResources.text.resourceOfflineStatus.provision=Provisioning In Queue

users.provisionedResources.text.resourceOfflineStatus.enable=Enable In Queue

users.provisionedResources.text.resourceOfflineStatus.disable=Disable In Queue

users.provisionedResources.text.resourceOfflineStatus.revoke=Revoke In Queue

(New)requestWizard.label.mustselect.resource.instanceForEachUserOrg=You must select at least one resource instance of each resource for each user or organization.

(Old)requestWizard.label.mustselect.resource.instanceForEachUserOrg=You must select at least one resource instance for each user or organization.

request.requestDetail.text.processedOfflineStatus.pending.provision=Provisioning In Queue

request.requestDetail.text.processedOfflineStatus.pending.enable=Enable In Queue

request.requestDetail.text.processedOfflineStatus.pending.disable=Disable In Queue

request.requestDetail.text.processedOfflineStatus.pending.revoke=Revoke In Queue

request.button.deletecomment=deleteComment

requests.requestComments.message.delete=Delete

generic.dualList.error.badResourceSelection=Bad Resource Selection made

generic.dualList.error.badUserSelection=Bad User Selection made

(New)UserGroupMembers.error.noGroupMembersGroupsFound=There are no member groups in this group.

(Old)UserGroupMembers.error.noGroupMembersGroupsFound=There are member groups in this group.

global.error.invalidLookupValue=Invalid lookup value

UserGroupMembershipRules.label.filterByRuleName=Filter By Rule Name

UserGroupMembershipRules.button.SearchByRuleName=Search

UserGroupMembershipRules.button.SearchByUnassignedRuleName=Find

UserGroupAdministrators.error.cannotDeleteGroupWithMemberUsersSubgroups=Delete only if there are no users/group. Remove the users/group associated with the group, and then try again.

UserGroupAdministrators.error.cannotDeleteGroupWithAccessPolicy=Delete only if there are no access policy associated with the group. Remove the group from associated access policy, and then try again.

(New)passwordPolicy.message.complexPassword=<p>Password must meet the following complexity criteria:Must be at least six characters long.Must belong to at least three out of five categories.Uppercase alphabetic characters (A-Z)Lowercase alphabetic characters (a-z)Numerals (0-9)Non-alphanumeric characters (for example: !, \$, #, or %)Unicode charactersMust not contain any of user ID, first name or last name when their length is larger than 2.</p>

(Old)passwordPolicy.message.complexPassword=<p>Password must meet the following complexity criteria:Must be at least six characters long.Must belong to at least three out of five

categories.

- Uppercase alphabetic characters (A-Z)
- Lowercase alphabetic characters (a-z)
- Numerals (0-9)
- Non-alphanumeric characters (for example: !, \$, #, or %)
- Unicode characters

Must not contain three or more continuous characters from the user ID or full name.

tooltip.request.deleteRequestComments=Delete Request Comment

orm.integrated.feature.disabled=Feature available on ORM Console

Properties Added in xlDefaultAdmin.properties

global.locales.ar=ar

global.request.groups.selectedListDisplayFields.labels=

global.request.groups.selectedListDisplayFields=

global.emailValidate.filter=([\w!#\$%&'*+~/=?^_`{|}~])+[@](\w|[-]|[.])+([a-zA-Z0-9])+

request.requestTrack.defaultFromDays=30

Properties Added in xlRichClient.properties

dm.import.message.substitutionFailed.ObjectDoesNotSupport=Object {0} {1} does not support substitutions.

6.2 Customizations in Release 9.1.0.1

The following sections list items customized in release 9.1.0.1:

- [Section 6.2.1, "JavaServer Pages"](#)
- [Section 6.2.2, "Java Files"](#)
- [Section 6.2.3, "Properties File"](#)

6.2.1 JavaServer Pages

The following JavaServer pages have been modified in release 9.1.0.1:

ModifyConnectorFieldInfoTiles.jsp

tjspMenuNoStruts.jsp

DualListComponent.jsp

ReportFormFieldsDisplay.jsp

tjspForm.jsp

tjspGenerateEditForm.jsp

AssignResourceAdministratorsTiles.jsp

CIWAssignGroupITResourceTiles.jsp

CIWEditITResourceTiles.jsp

CIWViewITResourceTiles.jsp

CIWViewScheduledTaskTiles.jsp

ConfigureReconDataFlowTiles.jsp

DirectProvisionUserWizard_ProvideChildProcessDataTilesInclude.jsp

DirectProvisionUserWizard_ProvideParentProcessDataTilesInclude.jsp
MyProxyViewProxyAssignTilesInclude.jsp
OrgResourceProfileProvisioningTasksTiles.jsp
requestDetailTiles.jsp
requestTrackTilesInclude.jsp
ResourceAdministratorsTiles.jsp
ResourceAuthorizersTiles.jsp
ResourceProfileProvisioningTasksTiles.jsp
SearchGroupTiles.jsp
SelectGroupToAssignToTaskTiles.jsp
SelectUserToAssignToTaskTiles.jsp
tjspConfirmAssignOrganizationAdministratorsStep1Tiles.jsp
tjspConfirmUpdateOrganizationAdministratorsStep1Tiles.jsp
tjspLogoffTimeoutTiles.jsp
tjspLogonTiles.jsp
tjspProvideChallengeAnswersConfirmTiles.jsp
tjspSearchOrganizationTiles.jsp
tjspSearchUserTiles.jsp
tjspSelfRegTrackRequestTiles.jsp
tjspSetChallengeAnswersConfirmTiles.jsp
tjspSetChallengeAnswersTiles.jsp
tjspSetChallengeQuestionsTiles.jsp
tjspUserMemberOfTiles.jsp
tjspVerifyUserIdTiles.jsp
tjspViewAdministratorsOrganizationDetailsTiles.jsp
UpdateResourceAdministratorsTiles.jsp
UserDefinedChildFormEditTilesInclude.jsp
UserDefinedFormEditTilesInclude.jsp
UserGroupAdministratorsAssignTiles.jsp
UserGroupAdministratorsTiles.jsp
UserGroupAdministratorsUpdatePermissionsTiles.jsp
UserGroupPermissionsTiles.jsp
UserGroupPoliciesTiles.jsp
UserGroupReportsTiles.jsp
UserGroupUnassignedPermissionsTiles.jsp
UserGroupUpdatePermissionsTiles.jsp

UserProxyNoProxyDefinedTiles.jsp
UserProxyViewProxyAssignTilesInclude.jsp

6.2.2 Java Files

The following Java files have been modified in release 9.1.0.1:

AssociatedEntitiesForResourceAction.java
CreateConnectorAction.java
CreateConnectorPopUpAction.java
CreateConnectorPopUpForm.java
DirectProvisionOrganizationAction.java
DirectProvisionUserAction.java
LoadDeploymentUtilityAction.java
ManageAccessPoliciesAction.java
ManageAttestationAction.java
ManageAttestationTaskAction.java
ManageITResourceAction.java
ManageITResourceForm.java
ManageScheduledTaskAction.java
ManageScheduledTaskForm.java
OpenTasksAction.java
OrgResourceProfileProvisioningTasksAction.java
OrgResourceProfileProvisioningTasksForm.java
ProvisionedResourcesForUserAction.java
RegistrationHelpPageAction.java
RequestAction.java
RequestTrackAction.java
ResourceAdministratorsAction.java
ResourceAdministratorsForm.java
ResourceAuthorizersAction.java
ResourceAuthorizersForm.java
ResourceProfileProvisioningTasksAction.java
ResourceProfileProvisioningTasksForm.java
ResourceWorkflowsAction.java
SearchGroupAction.java
SearchResourceAction.java
tcAction.java
tcChangePasswordAction.java

tcForgetPasswordAction.java
tcITResourceLookupFieldAction.java
tcLogonAction.java
tcLogonForm.java
tcLookupFieldAction.java
tcManageGroupAction.java
tcManageOrganizationAction.java
tcManageOrganizationForm.java
tcManageUserAction.java
tcModifyProfileAction.java
tcRequestProvisionResourceAction.java
tcRequestUserProvisionResourceAction.java
tcRequestWizardAction.java
tcSearchOrganizationAction.java
tcSearchUserAction.java
tcSelfRegistrationAction.java
tcSelfRegTrackRequestAction.java
tcSetChallengeQuestionsAction.java
tcUserMemberOfAction.java
tcUserMemberOfForm.java
UserDefinedFormAction.java
UserGroupAccessPoliciesAction.java
UserGroupAdministratorsAction.java
UserGroupAdministratorsForm.java
UserGroupMembersAction.java
UserGroupMembershipRulesAction.java
UserGroupMenuItemsAction.java
UserGroupPermissionsAction.java
UserGroupPermissionsForm.java
UserGroupReportsAction.java
UserGroupReportsForm.java

6.2.3 Properties File

Note: If you have modified any of the properties files on your Oracle Identity Manager installation, then create a backup of those files before you overwrite the files with the ones from the PATCH directory. After you copy the files, make the same modifications in the newly copied files.

The following properties have been modified in the resource bundle for the Diagnostic Dashboard:

xladd.vdtest.xlSQL_display1=One or more 'Microsoft SQL Server Driver for JDBC' files were not found.

xladd.dftest.tValidateSQLServerDefinition_description=Oracle Identity Manager requires 'Microsoft SQL Server Driver for JDBC' to work with Microsoft SQL Server. This test verifies if these JDBC drivers are available to the application server.

xladd.dftest.sqlServer_description=Oracle Identity Manager requires 'Microsoft SQL Server Driver for JDBC' to work with Microsoft SQL Server. This test verifies if these JDBC drivers are available to the application server.

xladd.vdtest.driverNotFound=One or more 'Microsoft SQL Server Driver for JDBC' files were not found.

xladd.bctest.errors.itResourceName=The IT Resource Instance is not available. Enter a valid IT Resource Instance Name.

The following properties have been modified in the resource bundle for Oracle Identity Manager:

global.label.calendar=Select to access date picker

global.error.duplicateFormData=The entered form data already exists.

global.error.duplicateFormDataAdvice=Please select another field value.

user.label.filterByGroupName=Filter By Group Name

user.button.searchMemberGroupName=Search

UserGroupPolicies.error.noPermsToDelete=No Permission To Delete

UserGroupPolicies.error.noPermsToDeleteDescription=You don't have rights to Delete one or more selected Access policies.

label.atetstation.comment=Reassigning Attestation Process as Grace Period has expired. the reviewer for this Process was

trackrequest.error.selectUser=Please Specify Username.

AboutXl.message.header=© Oracle Corporation

resourceMgmt.resourceAdministrators.error.noAdminFoundWithSearchCriteria=No Administrator found with given search criteria

resourceMgmt.resourceAdministrators.button.searchAssignedGroup=Find

resourceMgmt.resourceAdministrators.button.searchUpdateGroup=Go

resourceMgmt.resourceAuthorizers.button.searchAssignedGroup=Find

resourceMgmt.resourceWorkflows.label.removeKeyCaseInsensitiveField=Click to remove the setting of case insensitive

resourceMgmt.resourceWorkflows.label.addKeyCaseInsensitiveField=Click to add the setting of case insensitive

UserGroupPermissions.message.FilterByPermissionName=Filter by Permission Name:

UserGroupPermissions.message.button.searchAssignedPermissionName=Find

UserGroupPermissions.message.button.searchUpdatePermissionName=Search

UserGroupPermissions.message.button.searchUnAssignedPermissionName=Go

manageOrganization.label.filterByGroupName=Filter By Group Name

manageOrganization.button.searchAssignedGroup=Search

manageOrganization.button.searchUnassignedGroup=Find

manageOrganization.button.searchUpdatePermissionGroup=Go

UserGroupReports.error.noPermsToDelete=No Permission to Delete.

UserGroupReports.error.noPermsToDeleteDescription=You have no permission to delete one or more selected reports.

UserGroupMembershipRules.error.noPermsToDelete=No Permission to Delete.

UserGroupMembershipRules.error.noPermsToDeleteDescription=You don't have rights to Delete one or more Rules.

UserGroupAdministrators.label.filterByGroupName=Filter By Group Name

UserGroupAdministrators.button.SearchByGroupName=Search

UserGroupAdministrators.button.SearchByUnassignedGroupName=Find

UserGroupAdministrators.button.SearchByUpdatePermissionGroupName=Go

UserGroupAdministrators.error.cannotDeleteGroup=Can not delete this group.

UserGroupAdministrators.error.noPermsToDelete=No Permission to Delete.

UserGroupAdministrators.error.noPermsToDeleteDescription=You don't have rights to Delete one or more selected Administrative Groups.

global.FormInfoDesc.Lookup.Change-self-password-menu-item=Change Self Password menu item

global.FormInfoDesc.Lookup.Create-generic-connector=Create Generic Technology Connector menu item

global.FormInfoDesc.Lookup.Manage-generic-connector=Manage Generic Technology Connector menu item

modifyConnector.label.caseInsensitive=Case-Insensitive

global.button.stopexecution=Stop Execution

manageITResource.resourceAdministrators.button.search=Search Group

manageITResource.resourceAdministrators.button.find=Find Group

manageITResource.resourceAdministrators.button.go=Filter Group

manageITResource.resourceAdministrators.label.filterByGroupName=Filter By Group Name

manageITResource.resourceAdministrators.error.adminNotFound=There are no administrators associated with this It Resource

global.resultSet.Form~Information.Description.Create~generic~connector=Create Generic Technology Connector menu item

global.resultSet.Form~Information.Description.Manage~generic~connector=Manage Generic Technology Connector menu item

global.resultSet.Form~Information.Description.Change~self~password~menu~item=Change Self Password menu item

7 Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for Release 9.1.0.2.

8 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> if you are hearing impaired.

Oracle Identity Manager Readme, Release 9.1.0.2
E14764-06

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following

notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.