Sun Java™ System

Identity Installation Pack 2005Q4M3 SP2 Release Notes

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-6120-10

Contents

Contents

Notes about Identity Installation Pack 2005Q4M3 SP2

Identity Installation Pack 2005Q4M3 SP2 Features

Previous Features and Bug Fixes

Notes on Installation and Update

Documentation Additions and Corrections

Deprecated APIs

Notes about Identity Installation Pack 2005Q4M3 SP2

Before installing or upgrading the Sun Java™ System Identity Installation Pack software, review the Notes on Installation and Update section of these release notes and any documentation provided.

Installation

Use Identity Installation Pack 2005Q4M3 to install Sun Java™ System Identity Manager, Sun Java™ System Identity Auditor, and Sun Java™ System Identity Manager Service Provider Edition (SPE) in a new environment or as an update.

You can update Identity Manager, Identity Auditor, and Identity Manager SPE from Identity Manager v5.0 or any of its service packs up to 5.0 SP6. If you have an older version of Identity Manager, you must first upgrade to Identity Manager v5.0.

Refer to *Identity Manager Upgrade* and *Identity Install Pack Installation* for detailed product installation instructions.

Note The minimum supported Java version is 1.4.2.

Supported Software and Environments

This section lists software and environments that are compatible with Identity product software:

- Operating Systems
- Application Servers
- Browsers
- Database Servers
- Java Runtime Environment
- Sun Identity Manager Gateway
- Supported Resources
- Web Servers

Note Because software product developers frequently ship new versions, updates, and fixes to their software, the information published here changes often. Review the release notes for updates before proceeding with installation.

Operating Systems

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 or above
- Microsoft Windows 2003
- Solaris 8, 9, 10 Sparc and x86d
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Novell SuSE Linux Enterprise Server 9 SP1

Application Servers

The application server you use with Identity Manager must be Servlet 2.2-compliant and installed with the included Java platform (unless noted as follows):

- Apache Tomcat
  - Version 4.1.x (with JDK 1.4.2)
  - Version 5.0.x (with JDK 1.4.2)
- BEA WebLogic® Express 8.1 (with JDK 1.4.2)
- BEA WebLogic® Server™ 8.1 (with JDK 1.4.2)
- IBM WebSphere® 6.0
- IBM WebSphere® Application Server - Express Version 5.1.1 (with JDK 1.4.2)
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8
- Sun Java™ System Application Server Platform Edition and Enterprise Edition 8.1

Note If your current application server does not support JDK 1.4.2, please check with your vendor to examine the implications of upgrading to one that does before installing Identity Installation Pack 2005Q4M3 SP2.

Browsers

- Microsoft Internet Explorer 5.x and later
- Safari v2.0 and later for Mac OS X 10.3.3 and later
- Mozilla 1.78 (with JRE 1.5)
- Firefox 1.04, 1.05, 1.06 (with JRE 1.5)

Repository Database Servers

- IBM® DB2® Universal Database for Linux, UNIX®, and Windows® (Version 7.x, 8.1, 8.2)
- Microsoft SQL Server™ 2000
- MySQL™ 4.1
- Oracle 9i® and Oracle Database 10g, 10gR1 and 10gR2®

Sun Identity Manager Gateway

If you plan to set up Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, Lotus Domino or RSA ACE/Server resources, you should install the Sun Identity Manager Gateway.

Supported Resources

Identity product software supports these resources.

Customer Relationship Management (CRM)

- Siebel 6.2, 7.0.4, 7.7, 7.8

Databases

- IBM® DB2® Universal Database for Linux, UNIX®, and Windows® (7.x, 8.1, 8.2)
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000
- MySQL™ 4.1.x, 5.x
- Oracle 8i®
- Oracle 9i®
- Oracle Database 10g Release 1®
- Sybase Adaptive Server® 12.x

Directories

- LDAP v3
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory on Novell NetWare 5.1, 6.0
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

Notes

- While Identity Manager is tested on Sun™ ONE Directory Server and Open LDAP, LDAP servers that are v3-compliant may work without any changes to the resource adapter.
- Sun Java™ System Directory Server 5 2005Q1 requires a patch to the Directory Server retro changelog plugin if you are using Active Sync. This patch is required for “regular” replication only (not for MMR replication).

Enterprise Resource Planning (ERP)

- Oracle Financials on Oracle Applications 11.5.9, 11.5.10
- Peoplesoft® PeopleTools 8.1 through 8.4.2 with HRMS 8.0 through 8.8
- SAP® R/3 v4.5, v4.6
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
- SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)

Help Desk

- Remedy® Help Desk 4.5, 5.0

Message Platforms

- Blackberry RIM Enterprise Server 4+ (uses generic Windows script adapter)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0, 6.5, 6.5.4 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 5.x, 6.0

Note Microsoft Exchange 2000 and 2003 are managed through the Microsoft Windows Active Directory 2000 and 2003 resources.

Message Queue

- JMS Message Queue Listener

Operating Systems

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L v5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- Generic Windows Script Adapter (uses Gateway
- Red Hat Linux 8.0, 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

Security Managers

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Scripted Host
- INISafe Nexess 1.1.5
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 for UNIX
- eTrust CA-Top Secret® Security 5.3

Web Access Control

- IBM Tivoli® Access Manager 4.x, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2

- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4

Web Servers

Note Integration between an application server and Web server is not required for Identity Manager. You may choose to use a Web server for better load balancing and for increased security (through the https protocol).

- Apache 1.3.19
- iPlanet 4.1
- Microsoft Internet Information Server (IIS) 4.0, 5.0
- Sun™ ONE Web Server 6

Discontinued Software

Identity Manager will discontinue support for the following software packages that are used as application servers, database repositories and managed resources. Support will continue until the next major release of Identity Manager. Please contact your Customer Care representative or Customer Support if you have questions about moving to newer versions of these software packages.

Database Servers

- Oracle 8*i*
- IBM DB2 Universal Database for Linux, UNIX, and Windows 7.0

Operating Systems

- Solaris 7

Resources

- Microsoft Exchange 5.5
- IBM DB2 7.0

Official support of the NT4 Resource Adapter

As we continue in our progress to deliver new and improved functionality in our latest releases, please accept this as the End-of-Life (EOL) notice for older versions. Plans for EOL are based on Microsoft's drop of the NT4 operating system support. Sun is discontinuing support of the NT operating system but not the rest of the NT adapter functionality. Sun is committed to continued support for customers using the NT operating system until late 2006.

API Support

The Identity Manager v6.0 Application Programming Interface (API) includes any public class (and any public or protected method or field of a public class) listed in the following table.

API Type	**Class Names**
Session	com.waveset.msgcat.* com.waveset.util.* com.waveset.object.* com.waveset.exception.* com.waveset.expression.* com.waveset.config.* com.waveset.session.SessionUtil com.waveset.session.ScriptSession com.waveset.session.SessionFactory com.waveset.session.Session com.waveset.session.UserViewConstants
Adapter	com.waveset.adapter.* com.waveset.util.Trace
Policy	com.waveset.policy.PolicyImplementation com.waveset.policy.StringQualityPolicy

Task	com.waveset.task.Executor com.waveset.task.TaskContext
UI	com.waveset.ui.FormUtil com.waveset.ui.util.RequestState com.waveset.ui.util.html.*
Workflow	com.waveset.provision.WorkflowServices com.waveset.session.WorkflowServices com.waveset.workflow.WorkflowApplication com.waveset.workflow.WorkflowContext

Identity Manager SPE additionally includes the public classes listed in the following table.

API Type	Class Names
SPE	com.sun.idm.idmx.api.IDMXContext com.sun.idm.idmx.api.IDMXContextFactory com.sun.idm.idmx.auditor.* com.sun.idm.idmx.txn.TransactionPersistentStore com.sun.idm.idmx.txn.TransactionQuery com.sun.idm.idmx.txn.TransactionSummary

These classes are the only classes that are officially supported. If you are using classes that do not appear in these tables, contact Customer Support to determine whether it will be required to migrate to a supported class.

Deprecated API

Deprecated APIs lists all Identity Manager Application Programming Interfaces (APIs) deprecated in this release and their replacements (if available).

End of Life

We are committed to evolving our products to meet the standards of quality that our customers require. As we continue in our progress to deliver new and improved functionality in our latest release, Identity Manager v6, please accept this as the End-of-Life notice for older versions. We encourage you to begin your migration plans as soon as possible in order to avoid running on releases that are no longer on a maintenance plan.

End of Service Life (EOSL) for Software Support

During the EOSL Period, support is offered in two phases, the Full Support Phase and the Limited Support Phase. The length of the Full Support Phase will vary by Product. See Table 1 below for a list of Full and Limited Support Phases by Product.

Full Support Phase

During the Full Support Phase, Sun will provide Customers with support in accordance with the Customer's support contract with Sun (including the applicable Service Listing) as set forth at: http://www.sun.com/service/servicelist/. However, upon announcement of EOL of a Software Product, Customers will not have access to software updates and upgrades for that Software Product.

Limited Support Phase

During the Limited Support Phase, Sun will provide Customers with support in accordance with the Customer's support contract with Sun (including the applicable Service Listing) as set forth at: `http://www.sun.com/service/servicelist/.` However, Customers will not be entitled to submit bugs or to receive new patches from Sun. As during the Full Support Phase, upon announcement of EOL of a Software Product, Customers will not have access to software updates and upgrades for that Software Product.

End of Service Life Notes for Identity Manager Products

Specific dates are listed below. Please contact your Customer Care representative or Customer Support for assistance in planning for your upgrade to Identity Manager 6.0 (2005Q4M3).

- Identity Manager 2005Q3M1, which includes Identity Manager 5.5 and Identity Auditor 1.5, (including all service packs) will have Full Support until August 11, 2007, with Limited Support continuing through August 11, 2011.
- Identity Manager 5.0 (including all service packs) will have Full Support until August 11, 2007, with Limited Support continuing through August 11, 2011.
- Identity Manager 2005Q3M3 will be supported until October 2006, with no additional service packs.
- Identity Manager 2005Q1M3 will be supported until March 2006, with no additional service packs.
- Lighthouse 4.1 (including all service packs) will be supported until March 2006, with no additional service packs.
- Lighthouse 4.0, including SP1, support ended in September 2004.
- Lighthouse 3.1 (including all service packs) support ended in September 2005.
- Lighthouse 2.0 (including all patch levels) support ended in May 2004.
- Lighthouse 1.x (including 1.6) support ended in May 2004.

Identity Installation Pack 2005Q4M3 SP2 Features

Before installing or upgrading the Sun Java™ System Identity Installation Pack software, review the Notes on Installation and Update section of these release notes and any documentation provided with the most recent Identity Manager 2005Q4M3 service pack.

New Features and Defects Fixed in This Release

This section contains a summary and details new features for Identity Installation Pack 2005Q4M3 SP2. See the individual sections in this chapter for details.

Installation and Update

- The `waveset.serverId` system attribute has been added. Use this attribute to set unique server names when your deployment includes multiple Identity Manager instances that point to one repository on a single physical server.. (ID-11578)
- The installer now supports upgrading installations that have renamed, deleted, or disabled the default Configurator account. The installer now prompts for the proper user name and password that can import the update.xml during the upgrade post process. If the incorrect user or password is entered, the user is prompted up to three times to enter the correct password. The error should be displayed in the text box behind it. (ID-13006)

  For manual installation you must provide the `-U` <*`username`*> `-P` <*`password`*> flags to pass the credentials to UpgradePostProcess procedure.
- Identity Manager installs correctly on machines without a graphics card. (ID-14258)

Administrator Interface

- When you click on Reset Query in the Find Users screen, the name drop down and the results limit are now reset to their initial state.(ID-8961)
- MultiSelect objects now sort the available values when the `noApplet=true` and `sorted=true` properties are set. (ID-12823)
- Changes to a configuration object containing a static list did not get detected by the accounts Treetable. For example, an administrator's controlled organizations were determined by a rule which fetched a static list from a

configuration object. Before, the server would have to be rebooted to detect changes to the configuration object. Now the treetable changes to configuration objects after users log out of their current session and log in again. (ID-14442)

- The DatePicker can now have a date range set to allow for only certain dates to be picked from the calendar.(ID-10100)
- The Server Configuration and Modify Email Templates have been modified to allow the administrator to determine if SSL or authentication should be done on the SMTP server. (ID-12465)
- The continueLogin.jsp page now displays message correctly. (ID-13193)
- Fixed an issue where an organization object would not be unlocked when a user with insufficient rights tried to delete it. (ID-14942)

Forms

- In a form, using `<set>` within `<Expansion>` now works correctly. (ID-9617)
- Verification rule messages now appear in the locale of the client, not the server. (ID-12780)

Identity Auditor

- An Audit Policy can now be configured to scan only a restricted set of resources. (ID-9127)
- Database Table and Microsoft Identity Information Server now uses the custom forms specified for these two resources.(ID-10302)
- The title of the User Access Report displays correctly. (ID-11538)
- The Access Scan task now works on dynamic organizations. (ID-12437)
- The user view option CallViewValidators (UserViewConstants.OP_CALL_VIEW_VALIDATORS) can be set to the string "true "or "false" to enable or disable (respectively) audit policy checking during provisioning. (ID-12757)
- The upgrade process no longer overwrites the Access Review Notice email template (ID-13216)

Identity Manager SPE

- Identity Manager SPE now resumes processing transactions when the service is shutdown ungracefully (for example, the application server exits with an out-of-memory error). (ID-14579)

- Identity Manager SPE transactions can now support configurable user update consistency levels. Existing transaction store databases will need to be modified to add an additional column, `userId VARCHAR(N)` where `N` is large enough to contain the maximum length expected for a Identity Manager SPE user DN, plus an additional 8 characters. This database change does not occur automatically when running the upgrade scripts. (ID-13830)

Localization

- Message keys used as authentication questions now display correctly in the results page. (ID-13076)

Logging

- Active Sync events are now recorded in the system log. (ID-12446)
- Changing the user's authentication questions are now logged in the audit logs. (ID-13082)
- Direct and indirect method subcalls can now be traced. (ID-13436) This can be useful in debugging problems known to happen at some level below a specific entry method. To enable this feature, set the trace level for a scope with the `subcalls` modifier, as in the following example:

  ```
  trace 4,subcalls=2
  com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
  ```

  This will trace the `reconcileAccount()` method at level 4 and all subcalls at level 2.
- Errors that occur in Scheduler are now written to the system log, rather than preserved in the TaskSchedule object. (ID-14261)

Reconciliation

- The Notify Reconcile Finish task definition completes successfully when it is specified as the Post-Reconciliation Workflow (ID-9259)
- When a large number of Account objects exist (these are created as a result of reconciliations and provisions), reconciliation and provisioning performance can decrease drastically.

  To address this, an index should be created on the "name" column of the "account" table in the repository. Some scripts to aid in this have been provided under the sample directory. `account_index.sqlserver` is for Microsoft SQL Server; `account_index.sql` is for all other databases. (ID-14478)

Reports

- The Resource User Report now generates CSV and PDF files correctly. (ID12509, 13701)
- User Reports now show the resource accountId for all the accounts on the resource in a semicolon separated list.(ID-12820) Accounts and resources indirectly assigned, via a role or resource group, are also listed. If there is only one resource account, the accountId will be displayed only if it is not equal to the Identity Manager accountId.

Resources

New Resources

- Siebel 7.8
- OS/400 v4r5, v5r2, v5r3, and v5r4 (5.2, 5.3, and 5.4).

General

- The RACF adapter now includes search filter support for `listAllObjects`. (ID-10895)
- The LDAP adapter no longer creates an illegal distinguished name (DN) for a new account. (ID-10951)

  The escape method in `com.sun.idm.util.ldap.DnUtil` can now be used in forms to escape values to be inserted into identity templates of resource adapters with the LDAP DN format. Alternatively, an accountId policy with the “Required LDAP DN format” option checked can be used to validate LDAP distinguished names entering Identity Manager via input such as user input, ActiveSync, and reconciliation.
- The `isPickListAttribute` method within the Siebel adapter is no longer misidentified as `isMVGAttribute` in the tracing system. (ID-11471)
- For SecurId resources, the clients attribute is now treated as an optional attribute. (ID-11509)
- The default for the **Objectclasses to synchronize** Active Sync attribute on LDAP resources now defaults to inetorgperson. (ID-11644)
- Added multiple attributes to the Oracle ERP adapter to support auditing features. (ID-11725) *Oracle ERP Adapter* on page 95 for more details.
- The maximum number of Active Sync logs configured on an Active Sync resource are now honored correctly. (ID-11848)

- Solaris and Linux adapters now return a year on the last login information. (ID-12182)
- The Oracle ERP adapter no longer fails to close Oracle data base cursors. Previously, the failure caused the following error: (ID-12222)

  ```
  ORA-01000: maximum open cursors exceeded
  ```
- For the Domino adapter, concurrent updates of HTTPPassword with several users with the `NSFNoteComputeWithForm()` API call no longer result in a "-551" gateway error. (ID-12466)
- The Flat File Active Sync adapter now provides a warning message in the Active Sync log (if enabled) whenever an error occurs preventing a `diff` action for synchronization. (ID-12484)
- Modifications to AttrParse objects can now take effect without restarting Identity Manager. (ID-12516)
- The SAP and SAP HR adapters now provide three new resource attributes that provide the parameters for a retry of an SAP operation when a network failure occurs.(ID-12579) These attributes are:
  - SAP BAPI Retry Count - The number of times to retry the operation
  - SAP Connection Retry Count - The number of times to attempt to re-connect to the SAP server
  - SAP Connection Retry Wait Time - The number of milliseconds to wait before attempting to re-connect to the SAP server.
- The Database Table wizard no longer permits you to configure tables you cannot access. (ID-12643)
- When viewing account information from a Solaris resource configured with NIS, group membership information is displayed with the group name, instead of the numeric group ID. (ID-12667)
- The Siteminder LDAP Adapter now performs the following operations correctly, even when the Siteminder user is locked due to failed login attempts: (ID-12824)
  - enable
  - disable
  - expire password (with enable/disable)
  - unexpire password (with enable/disable)
- The RACF adapter no longer searches a large string once for every user retrieved in `listAllObjects`, which usually results in better performance in this function for a large number of users. (ID-12829)
- Changing LDAP group membership now uses single adds and removes instead of rewriting the entire group (that is, replacing the entire uniqueMember attribute). (ID-13035)

- Identity Manager now clears Admin privileges, if any, before attempting to delete a Secure ID user. (ID-13053)
- A VLV Sort is now configurable. The VLV sort attribute (`vlvSortAttribute`) has been added the to the LDAP resource. If the attribute is set, that value is used for the sort, but if it is not set, the “uid” value is used. (ID-13321)
- Passwords can now be set as not expired when using CUA mode on an SAP resource. (ID-13355)
- Performance improvements have been made to `AttrParse`. Normal parsing no longer throws and catches an exception for every character in a parsed buffer. (ID-13384)
- Corrected a problem encountered when performing a reconciliation on VMS. (ID-13425)
- The SecurID for UNIX adapter now performs UTF-8 character encoding and decoding when interoperating with RSA. (ID-13451)
- The Shell Script adapter can now detect errors generated from a ResourceAction during user create and update functions.(ID-13465)
- When creating account on a Windows NT resource through the Windows NT resource adapter, the following error message is no longer displayed in the Create user result page: “Error requiring password: put_PasswordRequired(): 0X80004005:E_FAIL”. (ID-13618)
- The Active Directory `PasswordNeverExpires` attribute can now be set during an update. (ID-13710)
- A new resource configuration parameter, enableEmptyString, has been added to the Database Table adapter to allow writing an empty string, instead of a NULL value, in character-based columns defined as not-null in the table schema. This option does not influence the way strings are written for Oracle-based tables. (ID-13737)
- Updating an Oracle ERP account's responsibility using the Oracle ERP adapter no longer causes other responsibilities associated with the account to be updated. (ID-13889) As a result, only the Oracle ERP audit timestamp for the responsibility modified is updated. The Oracle ERP audit timestamps for the other account responsibilities remain unchanged.
- The NDS Active Sync adapter no longer polls for changes based on the User object's lastModifiedTimeStamp. This attribute was getting updated when ever a user logged in/out. To remedy this issue, the last modified value is now calculated based on the lastModifiedTimestamp of a user's attributes defined in the schema map. If an attribute's lastModifiedTimestamp is greater than the highwater mark presented by the adapter, the gateway will send this user back to the server as modified.(ID-13896)
- Corrected a problem that caused newly-created NDS users to be unable to access their home directories. (ID-14208)

- The Shell Script adapter now supports the rename, disable and enable functions. (ID-14472)
- Active Directory data retrieval timeouts will no longer cause a premature end to reconcilations.(ID-14564)
- Corrected a problem that caused Active Directory Active Sync adapter to hang due to connections to the gateway not getting closed. (ID-14597)
- The Scripted JDBC adapter now correctly updates an attribute in which the original value was null but is being set to a non-null value. (ID-14655)
- The SAP adapter will no longer throw a JCO_ERROR_FUNCTION_NOT_FOUND exception when the SAP system does not contain the PASSWORD_FORMAL_CHECK function module. (ID-14663)
- Added the person_fullname account attribute to the schema map for the Oracle ERP adapter. In the Oracle ERP user form, this attribute is used to display the Person Name field. This field is read-only and will show the user’s fullname if an Oracle ERP account is linked to the Oracle HR system using the employee number. (ID-14675)
- The SAP adapter now properly reports the status of Disabled accounts. (ID-14834)
- The LDAP adapter permits the `nsaccountlock` activation short cut to use logic based on value presence/absence when determining if an LDAP user is disabled. (ID-14925) See *Disabling and Enabling Accounts* on page 92 for more information
- The Oracle ERP adapter now prevents the unlinking of resource accounts if the Oracle ERP Resource is inaccessible during full reconciliation. (ID-14960) (The resource could be inaccessible for many reasons including incorrect resource connection configuration.)

Reports

- The generation of `TaskTemplate` names that were too long (greater than MAX_NAME_LENGTH) has been corrected. (ID-13790)
- Column names are now displayed correctly in PDF reports. (ID-12794)

Repository

- IDM Repository now initializes more quickly. (ID-14937)

Security

- End user password changes initiated by administrators, via SPML or otherwise, will not get added to password history. This fix introduces both a System Configuration option and a View (form) option that will allow an administrator to toggle the desired behavior. The View option will always override any system configuration setting. In the System Configuration, an administrator may toggle based on login application. This will provide a greater amount of flexibility since admins may not desire a behavior that affects all applications. (ID-13029)

Server

- TaskInstance subobjects, like approvals, are now deleted properly when terminating the task. (ID-3258)
- Identity Manager now requires access to the `tmp` directory. (ID-7804) In order to accommodate this, if your application server uses a security policy, you need to add the following permission:

```
permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- In a clustered environment, a failed login on the end-user pages no longer generates a serialization-related exception. (ID-10556)
- A server no longer triggers failover mechanism on itself and terminates its own tasks if the server takes too long to process task information. (ID-10920)
- User Extended Attributes are now deleted from user objects correctly. (ID-11721)
- Corrected the condition that caused a "no cache error" on the All Tasks page for users in sub-organizations that do not have admin access to parent organizations. (ID-12288)
- Delimiter processing is now suppressed between brackets. Consequently, all characters found within bracket sets will now be treated as either an index or as a filter. Note: there currently isn't a mechanism to escape the closing bracket "]". (ID-12384)
- Task instance terminate actions are now audited as Terminate actions instead of Modify. (ID-12791)
- User actions can be performed on users after deleting a resource directly assigned to them. (ID-14806)

SOAP

- The SPML server now returns errors for requests containing filters that use operators that are not yet implemented. (ID-11343)

Workflow

- Invalid checkReference warning are no longer returned when running workflows. (ID-10802)
- If `notification.redirect` is used to redirect messages to a file, that file is now written using the `emailNotifier.contentCharset`, just as the message would, if it were emailed. This allows the file to contain non ISO-8859-1 characters. (ID-10331, 14984)
- More information is added to a workflow message when an approver is attempting to approve or reject a workitem that has already been approved or rejected. (ID-11045)
- Assigned the RoleAdminTask authType to the Manage Role TaskDefinition and assigned the ResourceAdminTask authType to the Manage Resource TaskDefinition. (ID-12768)

Additional Defects Fixed

10235, 10475, 13434, 14044, 14178, 14792, 14874

Known Issues

- By default, when a user types an answer to an authentication question, the characters are masked with asterisks (*). However, this practice disables the ability of some input method editors (IMEs) to create complex characters, such as those used in Japanese kanji.

  To allow users to use an IME to answer authentication questions, use the Debug page to change the `secret` Property value to `false` in the Question Login Form UserForm.

  ```
  <Property name='secret' value='false'/>
  ```

  Note: Setting this value to false is a security risk because answers to authentication questions are now human-readable on the screen. The answers are still stored encrypted. (ID-7424)
- Some configuration options that appear in the Identity Manager Administrator interface are not used with Identity Manager SPE. (ID-10843). Among these are:
  - Resource wizard configuration options: exclude accounts rule, approvers, and organizations
  - Role attributes

- FireFox 1.5 does not display some Identity Manager forms correctly. For example, on the Tabbed User form, the browser does not wrap labels, which pushes everything to the right. (ID-13109)
- The "Report only users whose user name" checkbox is listed twice in the User and User Question Reports. One checkbox has i-help, but the other checkbox does not. Either checkbox, used individually, will return the correct data. (ID-13155)
- If logging into the SPE end user pages produces an HTTP Status 500 error, this could indicate that there are multiple EncryptionKeys in the SPE configuration. This could be caused by a new one being generated in Identity Manager during the upgrade process.

  The workaround is to delete the EncryptionKeys from the SPE config directory and re-export from Identity Manager. (ID-13162)
- Once a value has been set for a user's email attribute, it cannot be removed. The value can be changed, but cannot be set back to null. (ID-13164)
- If you edited the Access Review Notice email template in Identity Manager version 6.0, you must either save the template before upgrading Identity Manager or edit the template after you upgrade. (The upgrade process overwrites the template with the default values.) (ID-13216)
- The help page for the Email Template tab of the Edit Server Settings page is incomplete. Refer to the Guidance help details about new fields added this release. (ID-14899)
- An approver who does not control the Top organization cannot view previously approved/rejected approvals.(ID-15271)

Previous Features and Bug Fixes

Previous Features

This section contains a summary and details features added for previous service packs for Identity Installation Pack 2005Q4M3.

Installation and Update

- If you use SQL Server 2000 SP4 as a repository and are using Microsoft's JDBC driver, you must use the SQL Server 2000 Driver for JDBC SP3 driver. (ID-9917)
- Identity Manager now supports Oracle Database 10g Release2® as a repository. (ID-12908)

Administrator and User Interfaces

- The **Configure > Servers > Edit Server Settings/Edit Default Server Settings** panels now include an Email Templates tab. This tab includes the default/per server SMTP host variable that all email templates with the `$(smtpHost)` variable will use as their default. This tab also uses the server configuration variable if the SMTP host field is blank. (ID-3574)
- The Change User Password and Reset User Password pages in the Identity Manager Administrator Interface now contain menu options for search type. These dropdown options include **starts with**, **contains**, and **is** as operands to search for user whose password needs changing or resetting. (ID-8965)
- The Debug page now provides **export default** and **export all** options. These options operate similar to console options, except that the Debug page options do not provide a choice for the exported file name. Instead, Identity Manager creates a file named `export<`***date***`>.xml` that you can save from the Debug page. (ID-9270)
- Importing an email template that contains a "cc" address is now supported. (ID-9768)
- The Identity Attributes page now displays a Passwords section, which describes the status of password generation with respect to the Identity attributes. You can configure Identity Manager to assign passwords to new users based on a default value, a rule, or by assigning an Identity System Account Policy that generates passwords. (ID-10274, 12560)
- Revised error messages associated with policy editing. (ID-12187)

- Identity Manager now includes a default Manager attribute, which provides support for a built manager-employee relationship. This information is stored on the Identity Manager user object. For more information, see the *Documentation Additions and Corrections* section of these release notes. (ID-12416)
- You can now configure Identity Attributes based on recent changes to resources (either edit or create operations). (ID-12678) If resources have changed since the last time the Identity Attributes were saved in the Identity Manager Administrator Interface, the Identity Attributes page displays this message: "One or more resources have been modified since the Identity Attributes were last saved. If these changes affect the Identity Attributes, they should be assimilated through the Configure Identity Attributes from Resource Changes page." Identity Manager provides a link to the Configure Identity Attributes from Resource Changes page that allows selecting which attributes from the modified resources' schema maps should be used as sources or targets for the Identity Attributes.

  After saving a resource from the Resource Wizard or the Account Attributes page, Identity Manager displays a page asking whether you wish to configure Identity Attributes based on recent resource changes. Select **Yes** to forward to the Configure Identity Attributes from Resource Changes page. Select **No** to return to the resource list.

  To disable this page, select **Do not ask me again**. This disable the page by setting the `idm_showMetaViewFromResourceChangesPage` property on the logged-in user to false.

Gateway

- The Gateway now runs on both Windows 2000 SP4 and Windows 2003 SP1 vmware images. (ID-12826)

HTML Display Components

- The DatePicker display class has the new `strict` property. If set, this property causes manually entered dates to be validated. (ID-11037)
- You can now disable the forced regeneration of the End User Menu by adding of the `doNotRegenerateEndUserMenu` property on the End User Menu form. (ID-11327)
- The SortingTable component now respects the `align`, `valign`, and `width` properties of the children components that comprise the table when rendering to HTML. An InlineAlert component is also available to display error, warning, success, and informational messages in forms. (ID-12560)

- The treetable component now supports adjustable columns. You can now set column widths in the user list and resource list tables via CSS to a fixed pixel or percentage value. You can also resize the columns using the mouse by clicking and dragging the right border of the column header. (ID-11474)

Note In Firefox/Mozilla and other Gecko-based browsers, resizing a column can cause browser text to be selected. This does not occur with Internet Explorer or Safari, as the onselectstart DHTML behavior can be suppressed.

Identity Manager SPE

Identity Manager SPE 2005Q4M3 SP1 introduces the following new features. For detailed information about these features, see *Identity Manager Service Provider Edition Administration Addendum* and *Identity Manager SPE Deployment*.

Enhanced End User Pages

Enhanced end user pages are now available. The example pages include the following features:

- Login (and logout) including authentication via challenge questions
- Registration and enrollment
- Password and user name changing
- Challenge questions and notification address editing
- Forgotten password and user name handling
- E-mail notification
- Auditing

The pages can be customized for your deployment. You can customize the following:

- Branding
- Configuration options (for example, the number of failed login attempts)
- Adding and removing pages

Password and Account ID Policy

There are now account ID and password policies for Identity Manager SPE and resource accounts. These policies are implemented with the same policy infrastructure as Identity Manager. (ID-12556)

Active Sync and Identity Manager SPE Sync Co-existence

You can now run Active Sync and SPE Synchronization on the same Identity Manager server. Do not run both on the same resource. (ID-12178)

Separate LDAP User and Configuration Directories

User and configuration information can now be stored on separate LDAP instances. These instances are selected during initial configuration. (ID-12548)

Access Manager Integration

You can now use Sun Java System Access Manager 7 2005Q4 for authentication on Identity Manager SPE end user pages. Access Manager ensures that only authenticated users can access the end user pages.

Reports

- Identity Manager now creates audit events when Capabilities are created and modified. (ID-9734).
- By default, the following reports are now automatically scoped to the set of organizations controlled by the logged-in administrator, unless explicitly overridden by selecting one or more organizations against which the report should be run. (ID-12116)
  - Admin Role Summary
  - Administrator Summary
  - Role Summary
  - User Questions Summary
  - User Summary

  To support this feature, the organization scope component has been changed from a single `Select` to a `MultiSelect` component.
- Identity Manager now provides a new Roles option named in the **Select which Identity Manager attributes you would like to display for each user** field. Selecting this option for new and existing reports results in the display of a comma-separated list of roles in the report. (ID-9777)
- You can now specify a list of attributes to display on their own column in .csv and .pdf reports. If you do not specify the list, all attributes are shown in a single column named Auditable attributes. (ID-10468)

- Two new reports support the introduction of built-in support for manager-employee relationships: My Direct Reports Summary, My Direct Employee Summary, My Direct and Indirect Employee Summary, and My Direct Reports Individual. (ID-12416, ID-12689)
- User Report now contains a search attribute to facilitate running a report based on User's manager. (ID-12689)

Repository

- Identity Manager now supports Oracle Database 10g Release2® as a repository. (ID-12908)

Resources

New Resources

Support for the following resources has been added since Identity Manager 2005Q4M3: See the *Identity Manager Resources Reference Addendum* for more information.

- HP OpenVMS (ID-8556)
- BridgeStream SmartRoles (ID-12262)
- Shell Script (ID-11906, ID-9866)
- Scripted JDBC (ID-7540)
- Realm support in Sun Java System Access Manager (ID-12414)

General

- Identity Manager now supports storing binary account attributes The following adapters support this feature: (ID-8851, 12665)
  - Active Directory
  - LDAP
  - Flat File Active Sync
  - Database Table
  - Scripted JDBC

- Sun Java System Communications Services

  Active Directory now supports the `thumbnailPhoto` (Windows 2000 Server and greater) and `jpegPhoto` (Windows 2003) binary attributes. The other adapters now support attributes such as `jpegPhoto`, `audio`, and `userCertificate`.

  Identity Manager throws an exception if you attempt to send binary or complex attributes to a resource that does not support binary attributes.

  Binary attributes should be kept as small as possible. If you load a binary attribute that is too large (for example, 200 KB), you might encounter an error message that states that you have exceeded the maximum allowed packet size. Contact Customer Support for guidance if you need to manage larger-sized attributes.

- Agent resource adapters now provide an optional resource attribute that supports the retention of connections during block operations: RA_HANGTIMEOUT. This attribute specifies the timeout value, in seconds, before a request to the gateway times out and is considered hung. The default value for this is 0, which indicates not to check for a hung connection.
  (ID- 12455)

Active Sync

- The Active Sync Wizard is now more fully internationalized. (ID-10504)

Domino

- You can now create a Domino user without an ID file or email address, but with only an entry in the Domino directory. (ID-11201)
- On Domino 6.x resources, you can now disable accounts without providing a Deny Groups list. When no Deny Groups are specified, Identity Manager uses the CheckPassword attribute for enabling and disabling on the Domino resource. A value of 2 disables the account. (ID-12088)

LDAP

- Identity Manager now provides a more scalable mechanism for editing large list-valued resource object attributes. Example forms for using this approach to manage LDAP groups are provided in `sample/forms/LDAPgroupScalable.xml`. (ID-9882)

- LDAP Resource Adapter now directly uses JSSE Provider. (ID-9958) The minimum supported Java version on Identity Manager is now 1.3, which allows third-party security providers to be used for SSL communication in case of the Domino, LDAP and NDS SecretStore resource adapters. You can register third-party security provider libraries using the standard java.security file.

  For more information, see http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#ProviderInstalling

- You can now edit LDAP groups whose names contain forward slashes. (ID-9872)

  The `ldapJndiConnectionFactory.alwaysUseNames` configuration attribute has been added to the `Waveset.properties` file.

  By default, this property is enabled. When enabled, all String names will be parsed into a Name using the NameParser of the context. This helps to avoid JNDI escaping issues. This option is meaningful only if the `ldapJndiConnectionFactory.wrapUnpooledConnections` option is set to true.

  Relying on the default value (true) or explicitly setting this value to true requires a 1.4 or later JVM. Due to a problem with JNDI, in earlier JVM's, some rename operations can fail when this option is enabled.

UNIX

- UNIX-based adapters now contain a Home Base Directory resource attribute. When present, this attribute overrides the setting of the home directory on the native resource for the account being created. The setting is the value set on this attribute appended with the `accountID`. If you set the user's home directory in the account attributes, then that setting will take precedence over the Home Base Directory. (ID-8587)
- You can now set timeout defaults via Resource Type Policy. In addition, you can also use the `maxWaitMilliseconds` property to control the polling frequency that Identity Manager’s scripted adapter uses when waiting for the resource to complete a task. (ID-11906)

Other Adapters

- You can now create and update objects in Siebel that require parent/child business component navigation. See *Documentation Additions and Corrections* in these release notes for more information. (ID-11427)
- You can now configure the SAP HR adapter to process IDOCs of any message type. Previously, only IDOCs of type HRMD_A could be processed. (ID-12120)

- The SAP HR Active Sync adapter now supports mySAP ERP ECC 5.0 (SAP 5.0) (ID-12408)
- If you are configuring Identity Manager to provision to a RSA Clear Trust 5.5.2 resource, additional libraries are not required for SSL communication as with previous Clear Trust versions. (ID-12499)
- In forms for Oracle ERP adapters, the `listResourceObjects` method in the `com.waveset.ui.FormUtil` class can now return a user's specific responsibilities and can be filtered to return all responsibilities, or active responsibilities only. (ID-12629)

  The options passed in are:

  - `key id` - (String) Identifies the resource identity whose responsibilities are returned
  - `activeRespsOnly` - (String) true or false. This value defaults to false if not sent.
- Identity Manager's Oracle ERP adapter now provides a `sysdate` or `SYSDATE` keyword. You use this keyword with `to_date` to specify an expiration date for a responsibility with the local time of an Oracle E-Business Suite (EBS) server. (ID-12709)
- Identity Manager's Oracle ERP adapter now provides a new `employee_number` account attribute. This attribute represents an `employee_number` from the `per_people_f` table. See the *Documentation Additions and Corrections* section of these release notes for more information. (ID-12710).

Roles

- Roles and resource groups now provide the ability, both singly and in combination, to assign users multiple accounts on a resource. See the *Documentation Additions and Corrections* section of these release notes for more information. (ID-6684)

Security

- Users with approver capabilities can now delegate their future approval requests to one or more users, who themselves are not Identity Manager approvers, for a specified period of time. Users can delegate from three interfaces: (ID-8485)
  - End User Main Menu - "Delegate Approvals" link
  - Admin Approvals Tab - "Delegate My Approvals" Subtab
  - Admin Create/Edit/View User - Security section

- Password generation now works correctly, and fails as expected when passwords are not correctly generated. (ID-12275)
- Identity Manager now provides the end user EndUserLibrary authorization type (authType). The EndUser capability (AdminGroup) now has List and View access to Libraries whose authType is EndUserLibrary. (ID-12469)

  To give end users access to the contents of a Library, set `authType='EndUserLibrary`' and ensure the Library's MemberObjectGroup is All.
- An Identity Manager user can have concurrent login sessions. However, you can limit concurrent sessions to one per login application by changing the value of the security.authn.singleLoginSessionPerApp configuration attribute in the System Configuration object. This attribute is an object that contains one attribute for each login application name (for example, the Administrator Interface, User Interface, or BPE). Changing the value of this attribute to true enforces a single login session for each user. (ID-12778)

  If enforced, then a user can log in to more than one session. However, only the last logged-in session remains active and valid. If the user performs an action on an invalid session, then he is automatically forced off the session and the session terminates.

Server

- The Find User page now handles deeply nested hierarchies of many organizations. (ID-10352)
- The ResourceConnectionManager is now notified of pending shutdowns. Consequently, the server no longer has to wait for SSH connections to timeout before it can exit. (ID-12214)

SOAP

- SPML support has been extended to cover roles and resource groups in addition to persons. (ID-8850)
- The new SPMLAccess capability allows account administrators access to the SPML interface. (ID-10854)
- The Identity Manager SPML interface provides a `login` ExtendedRequest that allows callers to log in as an administrator. As of this release, the SPML interface also provides a `loginUser` ExtendedRequest that allows the caller to get a session for user self-provisioning. This `loginUser` ExtendedRequest supports logging in with a password or with answers to security questions. (ID-12103)

Views

- The User view now provides the following control attribute: (ID-4383)

  `accounts[`***resname***`].waveset.forceUpdate`

  where ***resname*** represents the name of the resource. The value of this attribute is a list of resource account attributes that will always be sent to the resource for update when a user is modified.
- The Resource Account views (DeprovisionViewer, DisableViewer, EnableViewer, PasswordViewer, RenameUserViewer, ReprovisionViewer, and UnlockViewer) now support two new options to fetch resource account attributes for the user: (ID-10176)
  - `fetchAccounts` - a Boolean that causes the view to include account attributes for the resources assigned to the user
  - `fetchAccountResources` - a List of resource names to fetch from. If this is not specified, Identity Manager uses all assigned resources.

Workflow

- Identity Manager now provides the `auditPolicyScan` workflow service. You can use this workflow service call to scan a user for Audit Policy Violations based on the policies assigned to the user. If no policy is assigned to the user, a policy assigned to the organization, if exists, is used. See the *Documentation Additions and Corrections* section of these release notes for more information. (ID-12589)

Defects Fixed in Previous Releases

This section details defects fixed since Identity Installation Pack 2005Q4M3.

Administrator Interface

- When you configure a new User Action for the User Applet menu, text keys are now displayed correctly. (ID-8400)
- Identity Manager now correctly handles help displays that triggered errors when they contained special characters. (ID-8747)
- When a login application's singleLoginSessionPerApp attribute is set to true, Identity Manager behaves as follows: a user can log in to the same application more than once. However, the last session the user logged in as will be the only active, valid session. If the user tries to perform a task during another logged-in session as the same Identity Manager user, he is automatically forced off, and the session is terminated. (ID-9543)
- When a user is directly assigned to an organization, and a UserMemberRule also assigns this user to the same organization, the user will no longer be duplicated in the list. (ID-10410)
- The session timeout login page can now be localized and will be displayed in the language specified by the user locale. (ID-10571)
- The sample LDAP Password Sync form (sample/forms/LDAPPasswordActiveSyncForm.xml) now sets the `waveset.password` field instead of `password.password` and `password.confirmpassword`. (ID-11660)
- The Identity Manager Administrator Interface no longer generates errors when search results include a user name that contains a single quote, and that name is used in a link for a subsequent command. (ID-11123)
- MultiSelect components now correctly display single strings. (ID-11979)
- Identity Manager now displays the correct error message when you attempt to edit a resource object type that does not support update. (ID-12242)
- When using the tree table to list resources, nodes with names containing underscore characters now expand properly. (ID-12478)
- Online help now displays the correct help pages when non-Wizard options are selected from the ActiveSync configuration submenu. (ID-12597)
- You can now successfully delete users when using the French language locale. (ID-12642)
- The treetable, Account page, and Find Results page now display an unresolved Manager attribute as the Identity Manager manager's name wrapped in parentheses. Each time the user is updated, Identity Manager tries to resolve

the unresolved Manager attribute. If it resolves the attribute, Identity Manager strips off the parentheses, and performs constraint checking on the new value. (ID-12726)

- The inbox link for anonymous user login now points to the new end user work item list table. (ID-12816)
- You can now position TabPanel component buttons. (ID-12797)
- Identity Manager now converts the email templates that have the default mail.example.com to the new server config variable functionality. (ID-12720)
- Password fields are now conditionally displayed when the Identity Manager User Interface does not include the LH login module, and the user is assigned an AdminRole. (ID-12692)

Business Process Editor

- You can display and edit negative values (in seconds) for manual action timeouts. (ID-9715)
- Selecting **Store attribute in Identity Manager repository** when editing a MetaView attribute now works as planned. (ID-12396)

Forms

- Identity Manager provides new sample LDAP Create and Update Group forms to allow non-unique member names. (ID-8831)
- MultiSelect components now correctly handle items with identical labels (display names). (ID-10964)
- The Text component default maxlength is now unlimited (changed from 256 characters) (ID-11995).
- NTForm and NDSUserForm Groups fields now correctly implement the ListObjects rule. (ID-12301)
- Host adapter resource wizards now manage affinityAdmin fields better, preventing duplicates and null entries. (ID-12024)
- LDAP Update Group form no longer ignores edits when net membership remains the same. (ID-12162)

Identity Auditor

- Policy checking during user creation no longer results in the creation of extra task instances. (ID-10489)

Identity Manager SPE

- When creating a resource account, if that resource is down, Identity Manager SPE remembers the resource attribute values. The next time that user is edited in Identity Manager SPE, the account will be created on the resource if it is available. (ID-11168)
- You can now disable Tracked Events in SPE by unselecting "Enable tracked event collection" on the **Service Provider > Edit Main Configuration** page. You can also selectively disable from the same page Collecting Tracked Event data for each Time Scale. Like with all settings on this page, the modified configuration objects must be exported to the SPE master directory before they take effect. (ID-12033)
- The SPE IDMXContext deleteObjects method now correctly deletes objects from the directory store. (ID-11251)
- Service Provider Edition auditing subsystem no longer throws a null pointer exception at container shutdown. (ID-12845)
- IDMXUserViewer used to throw a null pointer exception if the form associated with the view-specified properties other than include or targets and the option map passed to the view handler methods (create/checkin/checkout/refresh) was null. (ID-12861)

Login

- Launching a custom task during login no longer slows down login excessively. (ID-12377)
- Identity Manager now correctly logs failed administrator log-in attempts for users that do not possess capabilities, organizations, or capabilities/organizations. (ID-12497)

Reports

- Windows 2000 Active Directory Inactive Account Scan (a task that resides under the Risk Analysis top menu bar) now completes successfully. (ID-11148)
- You can now use the Resource User Report with more than one user. (ID-11420)
- When a delegated administrator runs a User Report, users that are members of an organization due to a UserMembersRule are now included. (ID-11871)

- By default, the following reports will be automatically scoped to the set of organizations controlled by the logged in administrator, unless explicitly overridden by selecting one or more organizations against which the report should be run. To support this, the organization scope component has been changed from a single Select component to a MultiSelect. (ID-12116)
- Identity Manager now correctly audits modifications of LDAP group membership. (It now includes both old and new values.) (ID-12163)

Repository

- The Identity Manager Repository now performs Oracle-proprietary handling for BLOB columns. The sample scripts for Oracle now define the xml column as data type BLOB (rather than LONG VARCHAR). For new installations, all tables will be created with BLOB xml columns. During an upgrade, only new tables will have a BLOB xml column, but the remaining tables can be converted to BLOBs by making the changes noted in the upgrade script (For large deployments, this upgrade process can take several hours). You should upgrade to the latest Oracle JDBC driver to get the best performance with BLOBs. (ID-11999)
- The Identity Manager repository has been changed to avoid a deadlock that is specific to Microsoft SQL Server 2000. The repository now uses the ID (rather than the name) of the LAST_MOD_ITEM when it selects the last modified value for a Type. (ID-12297)

Resources

Gateway

- The gateway no longer crashes when using Identity Manager APIs directly without going through the Identity Manager interface. (ID-12481)

General

- You can safely use single quotes in passwords. (ID-10043)
- Host adapter resource wizards now manage affinityAdmin fields better, which prevents duplicates and null entries. (ID-12024)
- Active Sync processes that are running on a Websphere cluster using "Automatic with Failover" startup no longer hang. (ID-12540)

Directories

- The Active Directory resource adapter now throws an exception if an invalid encryption type is specified. Valid values are nothing (empty), "none", "kerberos" and "ssl". (ID-9011)
- Identity Manager now pools LDAP connections. (ID-10219)
- Managing Out of Office attributes of a mail-enabled Active Directory (Exchange) user will no longer fail if `msExchHideFromAddressLists` is set to true. In addition, the sample Active Directory user form has been updated to prevent Identity Manager from displaying Out of Office attributes when `msExchHideFromAddressLists` is enabled. (ID-12231)
- LDAP Changelog Active Sync processing now handles MODIFY changetype that have no values. (ID-12298)

Mainframe

- In the RACF adapter, a change to DFLTGRP now results in adding (if necessary) DFLTGRP to the GROUPS to ensure that the DFLTGRP can be set as the new default group. (ID-9987)
- Mainframe resource adapter connections are correctly pooled and no longer cause mainframe operations to hang. (ID-12388)
- The terminal emulation now used to create a NaturalResourceAdapter account permits an 8-character user name that does not use a tab to select the Copy Links attribute. (ID-12503)

Oracle and Oracle ERP

- During a session with the OracleResource adapter, all Oracle cursors are closed, even when exceptions occur. (ID-10357)
- For the Oracle and Oracle ERP resource adapters connecting to Oracle RAC environments using a thin driver, use the following format: (ID-10875)

  jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=PROD)))
- The Oracle ERP can optionally limit accounts returned by the account iterator and listObjects interfaces by setting the resource attribute `activeAccountsOnly` to TRUE. The default is FALSE. When set to FALSE, all accounts on the resource are returned. When TRUE, only accounts with START_DATE and END_DATE spanning SYSDATE (now) are returned. (ID-12303)

- Oracle ERP adapters have been updated to close PreparedStatements more consistently, reducing the number of open cursors. (ID-12564)

SAP

- The SAP adapter now handles cases where duplicate Activity Groups are returned from listAllObjects(). (ID-7776)
- The SAP adapter provides the capability to return the temporary, generated password in the WavesetResult object if the adapter was unable to set a password as unexpired. This occurs only under the following conditions:
  - an administrator password change is requested and expirePassword = false
  - the desired password fails SAP password policy

  Failure most likely occurs when the desired password is already in the SAP password history.

  The `Return SAP Temporary Passwords on Failure` resource attribute was created to enable this capability, but the attribute does not work at this time. (ID-12185)
- The SAP adapter now more robustly checks a user's password against his current password when the request is an Administrator password change and the `expirePassword` flag is false. This prevents an error condition when the desired password and the user's current password are the same. (ID-12447)

UNIX

- The UNIX adapters provide basic `sudo` initialization and reset functionality. However, if a resource action is defined and contains a command in the script that requires `sudo` authorization, then you must specify the `sudo` command along with the UNIX command. (For example, you must specify `sudo useradd` instead of just `useradd`.) Commands requiring `sudo` must be registered on the native resource. Use `visudo` to register these commands. (ID-10206)
- The Red Hat Linux and SuSE Linux adapters now populate the primary group, secondary group, and last login fields during bulk list processes such as Load from Resource and Export to File. (ID-11627)

  If the schema map indicates that the last login field is to be tracked, then the bulk list process can slow down considerably, because the adapter must individually request the last login information for each user.
- You can now map the `time_last_login resource` attribute on Solaris, HP-UX, and Linux adapters to an attribute name other than the default (Last login time). (ID-11692)

Other

- If you have a PeopleSoft Component Active Sync resource that is using the LH_AUDIT_RANGE_COMP_INTF component interface, you must make changes to the resource if you wish to continue using the LH_AUDIT_RANGE_COMP_INTF component interface. (ID-11226)

  Confirm that your resource has an `auditLegacyGetUpdateRows` resource attribute set to true.

```
<ResourceAttribute name='auditLegacyGetUpdateRows'
    value='true'
    displayName='Use Legacy Get Update Rows'
    type='boolean'
    multi='false'
    facets='activesync' >
</ResourceAttribute>
```

- You can now delete Sun Access Manager Organization objects from the Identity Manager resources applet. (Identity Manager subsequently deletes all child objects without confirmation.) (ID-11516)
- When managing SecurId users, Identity Manager now supports three tokens per user. (ID-11723)
- For the Database Table adapter, database connections are now closed as soon as possible during iteration and polling, which prevents unused connections from being held unnecessarily. (ID-11986)
- The JMS Listener adapter no longer fails on Websphere 6.0. A change from asynchronous to synchronous message processing now permits JMS Listener to work on J2EE servers that prohibit asynchronous JMS message processing within a web application. The polling frequency should now be defined for JMS Listener resources. (ID-12654)

Reconciliation

- Setting a ControlledOrganizationRule on the User AdminRole no longer prevents the Reconciler daemon from starting. (ID-12695)

Repository

- Error messages of the form, `com.waveset.util.InternalError: Summary String length (2185) exceeds maximum (2048)` no longer occur when saving users or other objects. (ID-12492)

Roles

- Role names that contain apostrophes are no longer truncated during Role edit. (ID-8806)
- Identity Manager now correctly handles the addition and subtraction of assigned groups through role attributes. (ID-10832)
- Roles that were created in Identity Manager 5.0 and were sub-roles of other roles now include links to their super roles. (ID-11477)
- If a resource is renamed, Role Attributes will now correctly continue to reference the appropriate resource. (ID-11689)

Security

- You can suppress the detailed debugging information that is hidden in HTML comments by setting the `ui.web.disableStackTraceComments` property in the `Waveset.properties` file to true. If you are upgrading from a previous version of Identity Manager, you will need to add this property to config/Waveset.properties. The property is ignored (equivalent to setting the property to false) if it is not present in the properties file.(ID-10499)
- Anonymous users can now access various object types, such as rules, without setting the deprecated `endUserAccess` attribute in the System Configuration object. (ID-11248)
- To configure this release to provision to a Clear Trust 5.5.2 resource, you must install the `ct_admin_api.jar` from the Clear Trust 5.5.2 installation CD. You do not need additional libraries for SSL communication. (ID-12449)
- During AdminRole creation, Identity Manager now correctly handles the inclusion and exclusion of all object types. (ID-12491)
- Administrators with the following capabilities now have access to the List Resources page: (ID-12647)
  - Resource Password Administrator
  - Change Resource Password Administrator
  - Reset Resource Password Administrator
  - Change Active Sync Resource Administrator
  - Control Active Sync Resource Administrator
  - Reconcile Administrator
  - Reconcile Request Administrator

Server

- The application server no longer crashes when using Oracle OCI drivers with SSL (ID-7109)
- You no longer receive a null pointer exception when attempting to log in to the End User Menu if the Identity Manager user has a role on a resource in which the user does not exist. (ID-12379)

SOAP

You can now monitor SPML 1.0 calls through the `debug/callTimer.jsp` facility. The outermost call, the `doRequest()` method of com.waveset.rpc.SpmlHandler, is most useful for determining SOAP/SPML performance. The individual SPML methods (for example, `addRequest`) are also timed for monitoring convenience. (ID-8463)

Documentation

The following books have been updated because they have either been significantly updated or contain substantial amounts of new information.

- *Identity Manager Resources Reference Addendum*
- *Identity Manager Service Provider Edition Administration Addendum*
- *Identity Manager SPE Deployment*
- *Configuring PasswordSync with a Sun JMS Server*

See also *Documentation Additions and Corrections* in these release notes for updates to the 2005Q4M3 documentation set.

Additional Defects Fixed

6496, 8586, 8739, 8958, 8960, 9936, 10483, 10832, 11232, 12135, 12234, 12464,12483, 12611, 11642, 11767, 11979, 12203, 12274, 12368, 12377, 12510, 12614, 12673, 12967, 13054

Notes on Installation and Update

Installation Notes

- You must manually install Identity Install Pack on HP-UX.
- The Identity Install Pack installation utility can now install or update to any installation directory name. You must create this directory prior to starting the installation process, or select to create the directory from the setup panel.
- To run Identity Manager under Tomcat 4.1.x, download the JSSE jar files from Sun Web site, http://java.sun.com/products/jsse/index-103.html, and place them in the idm\WEB-INF\lib directory.
- Running the Sun Identity Manager Gateway on a Windows NT system requires the Microsoft Active Directory Client extension. The DSClient can be found at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358.
- The following jars were removed because of licensing issues. (ID-9338) These jars are required for the following resource adapter. Each is labeled below with information on how to obtain the jars from the vendor.

Adapter:	OS400ResourceAdapter
URL:	http://jt400.sourceforge.net
Project:	JTOpen
JAR:	jt400.jar
Version:	2.03
Adapter:	ONTDirectorySmartAdapter
URL:	http://my.opennetwork.com
Project:	Directory Smart
JARs:	dsclass.jar, DSUtils.jar
Version:	N/A

Update Notes

When updating Identity Manager, review the installation section for your application server for application server-specific instructions. This section includes a summary of upgrade tasks for upgrading from Identity Manager version 6.0 to 6.0 SP2. For more information, see *Identity Manager Upgrade*.

Identity Install Pack 2005Q4M3 SP2 can be updated from the following previous versions:

- Identity Manager 6.0 (any service pack level)
- Identity Auditor 1.7 (any service pack level)

Note If your current Identity Manager installation has a large amount of custom work, you should contact Sun Professional Services to assist in planning and executing your upgrade.

Use the following information and procedures to update Identity Manager.

Note In some environments, including HP-UX, you may be required or prefer to follow the alternate, manual update procedures. If so, skip to the section titled *Update Identity Manager Manually*.

Note Identity Manager 6.0 involves a schema change that introduces new tables for tasks, groups, organizations, and the syslog table. You must create these new table structures and move your existing data. See *Step 2: Update the Repository Database Schema* on page 5-60 in the *Documentation Additions and Corrections* section of this document.

Note If you edited the Access Review Notice email template in Identity Manager version 6.0, you must either save the template before upgrading Identity Manager or edit the template after you upgrade. (The upgrade process overwrites the template with the default values.) (ID-13216)

Step 1: Update the Identity Manager Software

Use the following information and procedures to update Identity Manager.

Notes:

- In some environments, including on HP-UX, you may be required or prefer to follow the alternate, manual update procedures. If so, skip to the section titled *Update Identity Manager Manually*.
- For UNIX environments, make sure that the `/var/opt/sun/install` directory exists and that you can write to it.
- During update, you will need to know the location where your application server is installed.
- Any previously installed hotfixes will be archived to the `$WSHOME/patches/`*`HotfixName`* directory.
- Commands shown in the following steps are specific to a Windows installation and Tomcat application server. The commands you use may differ depending on your specific environment.

To update Identity Manager:

1. Shut down the application server.
2. If you are running the Sun Identity Manager Gateway on the Identity Manager server, stop the gateway service with this command:

   ```
   gateway -k
   ```
3. Run the `install` command to start the installation process.

   Identity Manager displays the Welcome panel.
4. Click **Next**. Identity Manager displays the Select Installation Directory panel. Select Upgrade and click Next.
5. Enter a location for (or click **Browse** to locate) the Identity Manager installation directory, and then click **Next**.
6. Click **Next** to begin update.

   Identity Manager displays the Installation Summary Panel.

Note For detailed information about the installation, click **Details**. Depending on the amount of information captured during the installation process, not all messages will be displayed here. View the log file (identified in details) for more information. When finished, click **Close** to exit the installer.

7. Remove all of the compiled Identity Manager files from the application server work directory.

8. If the update process did not do so already, move any hotfix class files from the `WEB-INF/classes` directory to the `patches/`*`HotfixName`* directory.

Step 2: Update the Sun Identity Manager Gateway

If you are running the Sun Identity Manager Gateway on a remote system, use the following steps to update it:

1. Log in to the Windows 2000 system where the Sun Identity Manager Gateway is installed.
2. Change to the directory where the gateway is installed.
3. Stop the gateway service by running the command:

   ```
   gateway -k
   ```
4. If using Windows 2000 or later, exit all instances of the Services MMC plug-in.
5. Delete the existing gateway files.
6. If the newly updated gateway is installed on a system that is not the Identity Manager server, then copy the `gateway.zip` file from the location the installation image was unpacked.
7. Unpack the `gateway.zip` file into the directory where the gateway was installed.
8. Run the following command to start the gateway service:

   ```
   gateway -s
   ```

You can also start and stop the gateway by following these steps:

1. Open the Windows Control Panel.
2. Open Services. (In Windows 2000, Services is located in Administrative Tools.)
3. Select Sun Identity Manager Gateway.
4. Click **Start** or **Stop**.

Update Identity Manager Manually

In some environments, you may need to perform the update steps manually instead of using the Identity Manager installation and upgrade program.

Notes:

- Make sure you have set the `JAVA_HOME` environment variable.
- Make sure that the `bin` directory in the `JAVA_HOME` directory is in your path.
- Any previously-installed hotfixes will be archived to the `$WSHOME/patches/`*`HotfixName`* directory.

- Before upgrading, restore the built-in Configurator account so that it is named Configurator and has the Import capbility. In addition, the password for this account must configurator. After the upgrade, revert the Configurator account to its state before the upgrade. If necessary, rename this account and change the password before deploying in your production environment.

Follow these steps to update Identity Manager manually:

1. Stop the application server and the Sun Identity Manager Gateway.
2. Enter the following series of commands:

   On Supported Windows Platforms

   a. Set your environment:

   ```
   set SPPATH=Path to Service Pack Files
   set WSHOME=Path to Identity Manager Installation
   OR Staging Directory
   set TEMP=Path to Temporary Directory
   ```

   b. Run pre-process:

   ```
   mkdir %TEMP%
   cd /d %TEMP%
   jar -xvf %SPPATH%\IDPAK2005Q4M3_SP2.jar \
   WEB-INF\lib\idm.jar \ WEB-INF\lib\idmcommon.jar \
   WEB-INF\lib\idmformui.jar
   set TMPLIBPTH=%TEMP%\WEB-INF\lib
   set CLASSPATH=%TMPLIBPTH%\idm.jar;\
   %TMPLIBPTH%\idmcommon.jar;%TMPLIBPTH%\idmformui.jar
   java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
      com.waveset.install.UpgradePreProcess
   ```

   c. Install software:

   ```
   cd %WSHOME%
   jar -xvf %SPPATH%\IDM.jar
   ```

   d. Run post-process:

   ```
   java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
     com.waveset.install.UpgradePostProcess
   ```

On Supported UNIX Platforms

a. Set your environment:

```
export SPPATH=Path to Extracted Service Pack Files
export WSHOME=Path to Identity Manager Installation
OR  Staging Directory
export TEMP=Path to Temporary Directory
```

b. Run pre-process:

```
mkdir $TEMP
cd $TEMP
jar -xvf $SPPATH/IDPAK2005Q4M3_SP2.jar \
WEB-INF/lib/idm.jar WEB-INF/lib/idmcommon.jar \
WEB-INF/lib/idmformui.jar
CLASSPATH=$TEMP/WEB-INF/lib/idm.jar:\
$TEMP/WEB-INF/lib/idmcommon.jar:\
$TEMP/WEB-INF/lib/idmformui.jar
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME \
com.waveset.install.UpgradePreProcess
```

c. Install software:

```
cd $WSHOME
jar -xvf $SPPATH/IDM.jar
```

d. Run post-process:

```
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME
  com.waveset.install.UpgradePostProcess
```

3. Change directory to `$WSHOME/bin/solaris` or `$WSHOME/bin/linux`, then set permissions on the files in the directory so that they are executable.
4. If you installed into a staging directory, create a `.war` file for deployment to your application server.

Note Refer to the appropriate chapter in *Sun Java™ System Identity Manager Installation* for application server-specific instructions.

5. Remove the Identity Manager files from the application server work directory.
6. If the update process did not do so already, move any hotfix class files from the `WEB-INF/classes` directory to the `patches/`*`HotfixName`* directory.
7. Start the application server.
8. Update the Identity Manager database. Refer to the earlier section titled *Step 2: Update the Sun Identity Manager Gateway* for detailed instructions.
9. Update and then restart the Sun Identity Manager Gateway. Refer to the earlier section titled *Step 2: Update the Sun Identity Manager Gateway* for detailed instructions.

Documentation Additions and Corrections

About the Identity System Software Guides

Identity system software documentation is arranged in multiple guides, which are provided in Acrobat (`.pdf`) format on the Identity Install Pack CD. The release includes the following guides.

Identity System Software

Install Pack Installation (`Identity_Install_Pack_Installation_2005Q4M3.pdf`) — Describes how to install and update Identity system software.

Identity Manager

- *Identity Manager Administration* (`IDM_Administration_2005Q4M3.pdf`) — Provides an introduction to the Identity Manager Administrator and User interfaces.
- *Identity Manager Upgrade* (`IDM_Upgrade_2005Q4M3.pdf`) — Provides information to assist in planning for and executing upgrades.

Note For this release, *Identity Manager Technical Deployment* and *Identity Manager Technical Reference* were reorganized into the following publications:

- *Identity Manager Technical Deployment Overview* (`IDM_Deployment_Overview_2005Q4M3.pdf`) — Conceptual overview of the Identity Manager product (including object architectures) with an introduction to basic product components.
- *Identity Manager Workflows, Forms, and Views* (`IDM_Workflows_Forms_Views_2005Q4M3.pdf`) — Reference and procedural information that describe how to use the Identity Manager workflows, forms, and views — including information about the tools you need to customize these objects.
- *Identity Manager Deployment Tools* (`IDM_Deployment_Tools_2005Q4M3.pdf`) — Reference and procedural information that describe how to use different Identity Manager deployment tools; including rules and rules libraries, common tasks and processes, dictionary support, and the SOAP-based Web service interface provided by the Identity Manager server.

- *Identity Manager Resources Reference* (`IDM_Resources_Reference_2005Q4M3.pdf`) — Reference and procedural information that describe how to load and synchronize account information from a resource into Sun Java™ System Identity Manager. Additional adapters are documented in `ResourcesRef_Addendum_2005Q4M3SP1.pdf`
- *Identity Manager Audit Logging* (`IDM_Audit_Logging_2005Q4M3.pdf`) — Reference and procedural information that describe how to load and synchronize account information from a resource into Sun Java™ System Identity Manager.
- *Identity Manager Tuning, Troubleshooting, and Error Messages* (`IDM_Troubleshooting_2005Q4M3.pdf`) — Reference and procedural information that describe Identity Manager error messages and exceptions, and provide instructions for tracing and troubleshooting problems you might encounter as you work.

Identity Auditor

Identity Auditor Administration (`IDA_Administration_2005Q4M3.pdf`) - Provides an introduction to the Identity Auditor Administrator interface.

Identity Manager Service Provider Edition

- *Identity Manager Service Provider Edition Administration Addendum* (`SPE_Administration_Addendum_2005Q4M3SP1.pdf`) - Introduces Identity Manager SPE features.
- *Identity Manager Service Provider Edition Deployment* (`SPE_Deployment_2005Q4M3_SP1.pdf`) - Provides Identity Manager SPE deployment information.

Navigating the Online Guides

Use the Acrobat Bookmarks feature to navigate the guides. Click a section name in the bookmark panel to jump to that section location in the document.

The Identity Manager documentation set can be seen from any Identity Manager installation by navigating to `idm/doc` in your web browser.

Install Pack Installation

Corrections

Preface

Removed the erroneous cross reference to Appendix H from How to Find Information in this Guide. (ID-12369)

Chapter 1: Before You Install

- Removed Microsoft Exchange 5.5 as a Supported Resource from the Supported Resources table. It has been deprecated. (ID-12682)
- Added Lotus Notes® 6.5.4 (Domino) as a Supported Resource to the Supported Resources table. (ID-12226)
- Added JDK 1.5 as a supported Java version in multiple instances. (ID-12984)
- Modified the ERP Systems SAP information in the Supported Resources table to: (ID-12635)
  - SAP® R/3 v4.5, v4.6
  - SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
  - SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
  - SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- Modified the Red Hat information in the Supported Resources table to:
  - Red Hat Linux Advanced Server 2.1
  - Red Hat Linux Enterprise Server 3.0, 4.0
- Added the section Repository Database Servers and the following information under Supported Software and Environments: (ID-12425)
  - IBM® DB2® Universal Database for Linux, UNIX®, and Windows® (Version 7.x, 8.1, 8.2)
  - Microsoft SQL Server™ 2000
  - MySQL™ 4.1
  - Oracle 9i® and Oracle Database 10g, 10gR1 and 10gR2®

Chapter 2: Installing Identity Install Pack for Tomcat

The chapter now supports Apache Tomcat application server, Versions 4.1.x or 5.0.x.

Chapter 4: Installing Identity Install Pack for WebSphere

- The chapter now deals with installing Websphere 5.1 express and 6.0. (ID-12655, 12656) The following notes and information have been added at the points indicated:

Note The following step is not necessary when installing Identity Install Pack 6.0 or later.

4. Change to the staging directory, and delete the following files, if they exist:

```
WEB-INF\lib\cryptix-jce-provider.jar
WEB-INF\lib\cryptix-jce-api.jar
```

25. Download the latest `jlog package` from WebSphere at:

```
http://www.alphaworks.ibm.com/tech/loggingtoolkit4j
```

Note The `jlog package` is now incorporated in WebSphere’6.0. Download this only for earlier versions.

- Because you must install JDK 1.4.2 for this release, the section *For JDK 1.3.x:* is no longer applicable. In the same chapter, the section *For JDK 1.4* should be changed to *For JDK 1.4.2*.

Chapters 7/8: Installing Identity Install Pack for Sun ONE/Sun Java System Application Server 7/8

- Added the following corrected information under Installation Steps > Step 5: Edit the server.policy File > example permissions: (ID-12292)

```
permission java.io.FilePermission
"/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/
idm/config/trace1.log", "read,write,delete";

permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- Added the following information under Installation Steps > Step 5: Edit the server.policy File > example permissions:

  If you want to run with Identity Manager Service Provider Edition, add the following permission to the above server.policy file entries.

```
permission java.lang.RuntimePermission "shutdownHooks";
```

Chapter 14: UnInstalling Applications

Removed `_Version_` from the syntax example under Remove the Software > On UNIX > Step 3. (ID-7762)

Chapter 15: Installing The Applications (Manual Installation)

Corrected syntax example under Installation Steps > Step 3: Configure the Identity `Install Pack Index Database Connection > Non-Xwindows Environments > Step 3 to:` (ID-5821)

3. Set your license key with the following commands:

```
cd idm/bin
./lh license set -f LicenseKeyFile
```

Appendix A: Index Database Reference

Changed syntax example under table entry SQL Server to: (ID-12784)

```
URL:
“sqlserver://host.your.com:1433;
DatabaseName=dbname;SelectMethod=Cursor”
```

Appendix C: Configuring Data Sources for Identity Manager

- Multiple IIOP URLs are not supported. (ID-12499) Removed the following incorrect information under Configuring a WebSphere Data Source for Identity Manager > Configuring a Websphere 5 Data Source > Configure the DataSource in a Websphere Cluster:

  If the application servers do not have the same port specified in the **BOOTSTRAP_ADDRESS** property, the java.naming.provider.url can specify multiple URLs, for example:

```
iiop://localhost:9812,iiop://localhost:9813.
```

- All j2c.properties which were used in WebSphere version 5 are now part of the resources.xml file in WebSphere version 6. Added information about Configuring a Websphere 5.1/6.x Data Source and Configuring the 6.x Authentication Data. Removed Configuring a Websphere 4.x Data Source information. (ID-12767) Changes involved the following sections:

Configuring a JDBC Provider

Use WebSphere's administration console to configure a new JDBC Provider.

1. Click the **Resources** tab in the left pane to display a list of resource types.
2. Click **JDBC Providers** to display a table of configured JDBC providers.
3. Click the **New** button above the table of configured JDBC providers.
4. Select from the list of JDBC database types, jdbc type and implementation type. Click Next.

   Oracle, Oracle JDBC Drive, and Connection pool Data Source will be used for this example.
5. Continue configuring general properties.
   - Specify the name.
   - Specify the path to the JAR that contains the JDBC driver in the **Classpath** field. For example, to specify the Oracle thin driver, specify a path similar to the following:

   ```
   /usr/WebSphere/AppServer/installedApps/idm/idm.ear/idm.war/WEB-
   INF/lib/oraclejdbc.jar
   ```

Note You can use the administration console to specify the path to the JAR that contains the JDBC Driver. From the menu labeled **Environment**, select the **WebSphere Variable** menu item. On that pane, first choose the **cell**, **node**, and **server** for which to define this environment variable. Then specify the path to the JAR as the value of this variable.

   - Specify the fully qualified name of the JDBC Driver class in the **Implementation ClassName** field.
     - For the Oracle thin driver, this value is `oracle.jdbc.pool.OracleConnectionPoolDataSource`.
     - For db2 jcc driver, this value is com.ibm.db2.jcc.DB2ConnectionPoolDataSource
   - You may also change the name or description of the provider to anything you choose.

     When you are finished, click the **OK** button at the bottom of the table. The right pane should display the provider you added.

To configure a data source that uses this JDBC provider, see “Point the Identity Manager Repository to the Data Source.”

Configuring a Websphere JDBC Data Source

1. Use WebSphere's Administrative Console to define a data source with an existing JDBC Provider. If you need to define a new JDBC Provider for use with Identity Install Pack, see “Configuring a JDBC Provider.”

Before you can finish configuring the data source, you must configure authentication data. These aliases contain credentials that are used to connect to the DBMS.

Configure the 5.1 Authentication Data

1. Click on the **Security** tab in the left pane to display a list of security configuration types.
2. Click on the **JAAS Configuration** tab in the left pane to display a list of JAAS configuration types.
3. Click on the **J2C Authentication Data** tab in the left pane. The right pane displays a table of authentication data entries.
4. Click the **New** button above the table of authentication data entries. The right pane displays a table of general properties that can be configured.
5. Configure the general properties for the new authentication data entry. Note the following:
   - **Alias** is the name that will be shown in the selection list whenever someone configures the DBMS credentials for a Data Source.
   - **UserID** is the name used to connect to the DBMS.
   - **Password** is the password used to connect to the DBMS.

Next, configure the data source.

Configure the 6.x Authentication Data

1. Click **Security > Global security**.
2. Under Authentication, click **JAAS configuration > J2C authentication data**. The **J2C Authentication Data Entries** panel is displayed.
3. Click **New**.
4. Enter a unique alias, a valid user ID, a valid password, and a short description (optional).
5. Click **OK** or **Apply**. No validation for the user ID and password is required.
6. Click **Save**.

Note The newly created entry is visible without restarting the application server process to use in the data source definition. But the entry is only in effect after the server is restarted.

Configure the Data Source

Note If configuring a data source in a Websphere 5.x cluster, see “Configure the DataSource in a Websphere Cluster” for more information.

1. Click the **Resources** tab in the left pane to display a list of resource types.
2. Click **JDBC Providers** to display a table of configured JDBC providers.
3. Click on the name of a JDBC provider in the table. The right pane displays a table of general properties configured for the selected JDBC provider.
4. Scroll down to a table of additional properties. Click on **Data Sources**. The right pane displays a table of data sources configured for use with this JDBC provider.

Note Be aware of the **Scope** field at the top of the frame in the WebSphere administration console. Ensure that **Node** and **Server** are blank so that the cell information is presented for configuration underneath the **New** and **Delete** buttons.

5. Click the **New** button above the table of data sources. The right pane displays a table of general properties to configure.
6. Configure the general properties for the new data source. Note the following:
   - The **JNDI Name** is the path to the DataSource object in the directory service. You must specify this same value as the `-f` argument in `setRepo -t`*`dbms`*` -i`*`initCtxFac`*` -f`*`filepath`*.
   - **Container-managed persistence** should be left unchecked. Identity Install Pack does not use Enterprise Java Beans (EJBs).
   - **Component-managed Authentication Alias** points to the credentials that will be used to access the DBMS (to which this DataSource points).
   - Select from the drop-down list the alias that contains the appropriate set of DBMS credentials. See *Configure the 5.1 Authentication Data* for more information.
   - **Container-managed Authentication Alias** is not used. Set this value to `(none)`. Identity Install Pack makes its own connection to the DBMS (to which this DataSource points).
   - Click **OK** when you have configured this panel. The Data Sources page is displayed.
7. Click the DataSource you created. Then scroll down to the table of Additional Properties near the bottom. Click the **Custom Properties** link.

   The right pane displays a table of DBMS-specific properties.
8. Configure the custom properties for this DataSource. Click on the link for each property to set its value. Note the following:

- **URL** is the only required property. This database URL identifies the database instance and contains driverType, serverName, portNumber and databaseName.You may also specify some of these as individual properties.
- **driverType** in this example is thin.
- **serverName** is a host name (or an IP address).
- **databaseName** is usually a short database name.
- **portNumber** is 1521 by default for Oracle.
- **preTestSQLString** may be worth configuring to a value such as SELECT 1 FROM USEROBJ. This SQL query confirms that the USERJOB table exists and is accessible.

9. From the table of Additional Properties, you may also click the **Connection Pool** link if you wish to configure these properties for performance tuning.

Appendix E: Configuring JCE

A note should appear as follows:

Note Because you must install JDK 1.4.2 for this release, all supported environments should now have a JCE 1.2 included and information in this appendix is no longer applicable.

Additions

Chapter 1: Before You Install

- Added the following note under Setup Task Flow > Bullet Install and configure the Identity Install Pack software: (ID-8431)

Note On Unix or Linux systems:

- When installing Identity Install Pack versions 5.0 - 5.0 SP1 `/var/tmp` must exist and be writable by the user running the installer.
- When installing Identity Install Pack versions 5.0 SP2 and higher `/var/opt/sun/install` must exist and be writable by the user running the installer.

- Added the following note to Prerequisite Tasks > Set Up an Index Database > Setting Up SQL Server > step 3b: (ID-11835)

Note The following files that need to be in the `$WSHOME/WEB-INF/lib` directory:

```
db2jcc
db2jcc_license_cisuz.jar or db2jcc_license_cu.jar
```

- Added the following note under Supported Software and Environments > Application Servers: (ID-12385)

Note Your current application server container must support UTF-8.

Chapter 2: Installing Identity Install Pack for Tomcat

- Added the following step to Installation Steps > Step 1: Install the Tomcat Software > Installing on UNIX: (ID-12487)

  2. Add the Java `mail.jar` and `activation.jar` files to the `./tomcat/common/lib` directory. The mail and activation jar files can be found at:

```
http://java.sun.com/products/javamail
http://java.sun.com/products/beans/glasgow/jaf.html
```

- Added the following steps to Installation Steps > Step 1: Install the Tomcat Software > Installing on UNIX: (ID-12462)

  3. When configuring Tomcat to support UTF-8, add the `URIEncoding="UTF-8"` attribute to the *connector* element in the *TOMCAT DIR*`conf/server.xml` file, for example:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on the port
specified during installation -->
<Connector port="8080"
             maxThreads="150"
             minSpareThreads="25"
             maxSpareThreads="75"
             enableLookups="false" redirectPort="8443"
             acceptCount="100" debug="0" connectionTimeout="20000"
             disableUploadTimeout="true"
             URIEncoding="UTF-8" />
```

  4. When configuring Tomcat to support UTF-8, also add -Dfile.encoding=UTF-8 in your java vm options.

Chapter 13: Updating Identity Manager

Added a cross reference to Identity Manager Upgrade to assist users in finding complete upgrade information. (ID-12366)

Chapter 15: Installing The Applications (Manual Installation)

Added the following note under Installation Steps > Step 2: Install the Application Software: (ID-8344)

Note As of the 5.0 SP3 release the adapter classes are now contained in the `idmadapter.jar` file. If you have a custom adapter, you might need to update your class path.

Appendix B: Configuring MySQL

Added the following information under Configuring MySQL > step 3 Start the MySql process: (ID-12461)

If this process has not been started, then use the following steps to register and start MySQL.
On Windows, if you are installing in a directory other than `c:\mysql` then create a file called `c:\my.cnf` with the following content:

```
[mysqld]
basedir=d:/mysql/
default-character-set=utf8
default-collation=utf8_bin
```

On Windows, install and start the service:

```
cd <MySQL_Install_Dir>/bin
mysqld-nt --install
net start mysql
```

Appendix C: Configuring Data Sources for Identity Manager

Added the following information under Configuring a WebSphere Data Source for Identity Manager > Point the Identity Manager Repository to the Data Source: (ID-12071)

8. Point the repository to the new location. For example:

```
lh -Djava.ext.dirs=$JAVA_HOME/jre/lib/ext:$WAS_HOME/lib setRepo
-tdbms -iinitCtxFac
-ffilepath -uiiop://localhost:bootstrap_port
-Uusername
```

```
-Ppassword
-toracle icom.ibm.websphere.naming.WsnInitialContextFactory -
fDataSourcePath
```

In the above example the *DataSourcePath* might be `jdbc/jndiname`. The `bootstrap_port` is the WebSphere server bootstrap address port.

The `-Djava.ext.dirs` option adds all of the JAR files all of the JAR files in WebSphere's `lib/` and `java/jre/lib/ext/` directories to the CLASSPATH. This is necessary in order for the setrepo command to run normally.

Change the `-f` option to match the value you specified for the **JNDI Name** field when configuring the data source. See setrepo Reference for more information about this command.

Identity Manager Upgrade

Additions

Chapter 1: Upgrade Overview

Added the following item to the section *Example Upgrade*: (ID-12467)

Use care when editing the super role field in the Role Form. The super role itself may be a nested role. The super and sub roles fields indicate a nesting of roles and their associated resources or resource groups. When applied to a user, the super role includes the resources associated with any designated sub role. The super role field is displayed to indicate the roles that include the displayed role.

Chapter 3: Develop the Upgrade Plan

Added the following to the section Upgrade the Environment Upgrade From Identity Manager 5.x to 6.x. (ID-12361)

Step 2: Update the Repository Database Schema

Identity Manager 6.0 involves a schema change that introduces new tables for tasks, groups, organizations, and the syslog table. You must create these new table structure and move your existing data.

Note Before updating the repository schema, make a full backup of your Repository tables.

1. Identity Manager uses two tables to store user objects. Sample scripts (in the `sample` directory) can be used to make schema changes.

   Refer to the `sample/upgradeto2005Q4M3.`*`DatabaseName`* script to update your repository tables.

Note The update of MySQL databases is highly involved. Refer to `sample/upgradeto2005Q4M3.mysql` for further details.

Identity Manager Administration Guide

Additions

- If sunrise is configured, creating a user creates a work item that can be viewed from the **Approvals** tab. Approving this item overrides the sunrise date and creates the account; rejecting the item cancels account creation.
- When scheduling reconciliation, you can now provide the name of a Rule to be used to customize the schedule. For example, the Rule can push Reconciliations scheduled for a Saturday to the following Monday. (ID-11391)

Chapter 4: Administration

- Added information about approval delegation feature. (ID-12754)

Delegating Approvals

If you have approver capabilities, then you can delegate your future approval requests to one or more users (delegates) for a specified period of time. Users do not need approver capabilities to be delegates.

The delegation feature applies only to future approval requests. Existing requests (those listed under the Awaiting Approval tab) are forwarded through the forwarding feature.

To set up delegation, select the **Delegate My Approvals** tab in the **Approvals** area.

Notes

- Access to the delegation feature is available if you are assigned any capability that grants you the Delegate right to either WorkItem or any authType extension of WorkItem, including Approval, OrganizationApproval, ResourceApproval, and RoleApproval; or any custom subtype that extends WorkItem or one of its authTypes.
- You also can delegate approvals from the Security form tab of the Create/Edit/View User pages, and from the User Interface main menu.

Delegates can approve any requests during the effective delegation period on your behalf. Delegated approval requests include the name of the delegate.

Audit Log Entries for Requests

Audit log entries for approved and rejected approval requests include your (the delegator’s) name if the request was delegated. Changes to a user's delegate approver information will be logged in the detailed changes section of the audit log entry when a user is created or modified.

Chapter 5: Configuration

- Added information about configuring Identity Attributes when a resource is created or updated. (ID-12606)

Configuring Identity Attributes from Resource Changes

Identity Attributes define how attributes on resources relate to each other. When you create or modify a resource, it can affect these attribute relationships.

When you save a resource, Identity Manager displays the Configure Identity Attributes? page. From here, you can choose to:

- Continue to the Configure Identity Attributes from Resource Changes page and configure attributes. Click **Yes** to continue.
- Return to the resource list. Click **No** to return.
- Disable this page for future resource updates. Click **Do not ask me again** to disable the page.

Note **Do not ask me again** button is visible only to users with capabilities to modify the MetaView.

Re-enabling the Configure Identity Attributes? Page

If this page is disabled, then use one of these methods to re-enable it:

- Use the Identity Manager debug facility to edit the logged-in user's WSUser object. Change the value of the `idm_showMetaViewFromResourceChangesPage` property to a value of `true`.
- Add a field similar to the following sample to the user form (for example, the Tabbed User Form), and then use the Edit User page to change the value of this setting:

```
<Field name='accounts[Lighthouse].properties.displayMetaViewPage'>
  <Display class='Checkbox'>
    <Property name='label' value='Display Meta View?'/>
  </Display>
</Field>
```

Configuring Attributes

Use the Configure Identity Attributes from Resource Changes page to select attributes from the schema maps of modified resources to be used as sources and targets for the Identity Attributes. In some cases, you cannot select attributes in the Source and Target columns. You cannot select an attribute as a source if:

- It is marked as encrypted in the schema map
- It is marked as write-only in the schema map

You cannot select an attribute as a target if:

- There is an Identity Attribute stored globally with the same name. For example, if there is a global Identity Attribute named "firstname", then the firstname target option is selected and cannot be de-selected.
- The attribute is marked as read-only in the schema map.
- The resource's create and update account features are disabled or not supported by the resource.

Chapter 7: Security

- Added information about concurrent login session limitations. (ID-12778)

Limiting Concurrent Login Sessions

By default, an Identity Manager user can have concurrent login sessions. However, you can limit concurrent sessions to one per login application by changing the value of the `security.authn.singleLoginSessionPerApp` configuration attribute in the system configuration object. This attribute is an object that contains one attribute for each login application name (for example, the Administrator Interface, User Interface, or BPE). Changing the value of this attribute to `true` enforces a single login session for each user.

If enforced, then a user can log in to more than one session; however, only the last logged-in session remains active and valid. If the user performs an action on an invalid session, then he is automatically forced off the session and the session terminates.

Chapter 8: Reporting

In the section titled Summary Reports, the description of user report now includes ability to search for users by manager: (ID-12690)

- **User** – View users, the roles to which they are assigned, and the resources they can access. When defining a user report, you can select which users to include by name, assigned manager, role, organization, or resource assignment.

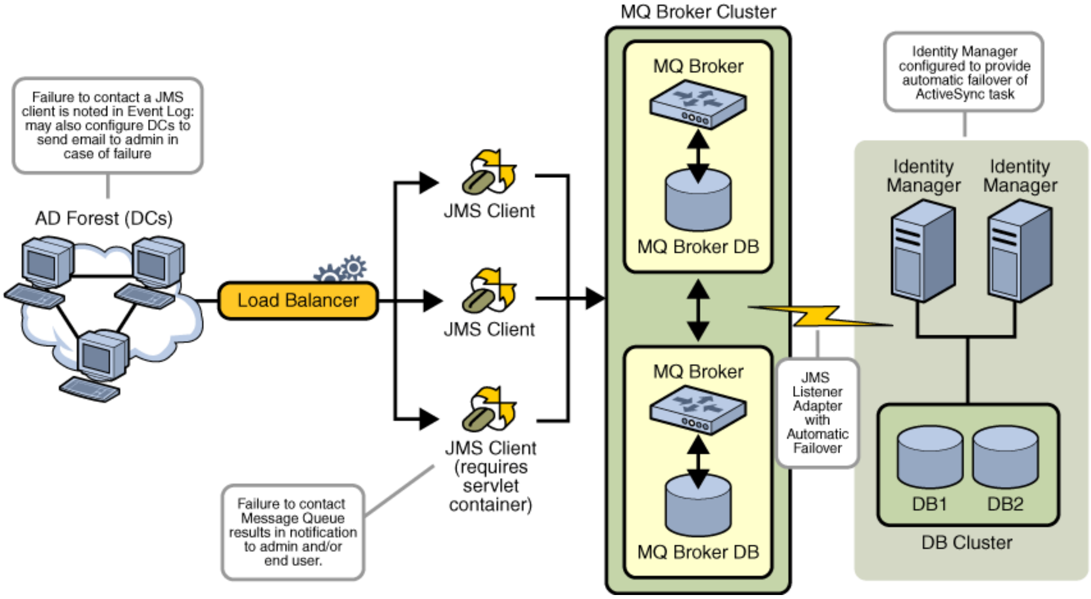
Chapter 10: PasswordSync

- Added instructions for configuring Windows PasswordSync with a Sun JMS server. See the *Configuring PasswordSync with a Sun JMS Server* document that accompanies these release notes. (ID-11788)
- Added the following new section to describe High Availability architecture with failover for PasswordSync. (ID-12634)
- Added a section that describes how to implement PasswordSync without using a Java Messaging Server. (ID-14974)

Failover Deployment for Windows PasswordSync

PasswordSync's architecture provides for the elimination of any single point of failure in the Windows password synchronization deployment for Identity Manager.

If you configure each Active Directory Domain Controller (ADC) to connect to one in a series of JMS clients through a Load Balancer (see the following figure), the JMS clients can send messages to a Message Queue Broker cluster, which ensures that no messages will be lost if any Message Queue fails.


MQ Broker Cluster
Failure to contact a JMS client is noted in Event Log: may also configure DCs to send email to admin in case of failure
AD Forest (DCs)
Load Balancer
JMS Client
JMS Client
JMS Client (requires servlet container)
Failure to contact Message Queue results in notification to admin and/or end user.
MQ Broker
MQ Broker DB
MQ Broker
MQ Broker DB
Identity Manager configured to provide automatic failover of ActiveSync task
Identity Manager
Identity Manager
JMS Listener Adapter with Automatic Failover
DB1
DB2
DB Cluster

Note Your Message Queue cluster will probably require a database for persistence of messages. (Instructions for configuring a Message Queue broker cluster should be provided in your vendor's product documentation.)

The Identity Manager server that is running the JMS Listener adapter configured for automatic failover will contact the Message Queue broker cluster. Although the adapter executes on only one Identity Manager at a time, if the primary ActiveSync server fails, the adapter will begin polling for password-related messages on a secondary Identity Manager server and propagating password changes out to downstream resources.

Implementing PasswordSync without a Java Messaging Service

To implement PasswordSync without a JMS, launch the configuration application with the following flag:

```
Configure.exe -direct
```

When the `-direct` flag is specified, the configuration application displays the User tab. Configure PasswordSync using the procedures described in “Configuring PasswordSync”, with the following exceptions:

- Do not configure the JMS Settings and JMS Properties tabs.
- In the User tab, specify the account ID and password that will be used to connect to Identity Manager.

If you implement PasswordSync without a JMS, you do not need to create a JMS Listener adapter. Therefore, you should omit the procedures listed in “Deploying PasswordSync”. If you want to set up notifications, you may need to alter the Change User Password workflow.

Note If you subsequently run the configuration application without specifying the `-direct` flag, PasswordSync will require a JMS to be configured. Relaunch the application with the `-direct` flag to bypass the JMS again.

Corrections

Chapter 5: Resources

In the custom resource class table, the custom resource class for the ClearTrust resource adapter is corrected as follows: (ID-12681)

```
com.waveset.adapter.ClearTrustResourceAdapter
```

Chapter 10: PasswordSync

In the section titled Configuring PasswordSync, under JMS Settings Dialog, the following description of Queue Name is corrected as follows:

- **Queue Name** specifies the Destination Lookup Name for the password synchronization events. (ID-12621)

lh Reference

Command syntax has been updated to correctly indicate a space after specified options. (ID-12798)

When using the -p option, for security reasons, *Password* should be specified as a path to a text file containing a password, rather than specified directly at the command line.

Examples

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console –u $user –p` *`PathtoPassword`*`.txt`
- `lh setup -U` *`Administrator`* `-P` *`PathtoPassword`*`.txt`
- `lh setRepo –c -A` *`Administrator`* `-C` *`PathtoPassword`*`.txt`
- `lh setRepo –t` *`LocalFiles`* `–f $WSHOME`

license command

Usage

`license [options] { status | set {parameters} }`

Options

- `-U` *`username`* (if Configurator account renamed)
- `-P` *`PathtoPassword`*`.txt` (if Configurator password changed)

Parameters for the `set` option must be in the form `-f` *File*.

Identity Manager Workflows, Forms, and Views

Chapter 1: Workflows

The discussion of manual actions in this chapter should contain the following information:

If a work item's `itemType` is set to wizard, the work item will, by default, bypass getting forwarding approvers when checking out the WorkItem view. If the itemType is anything other than wizard, then Identity Manager still fetches the forwarding approvers unless `CustomUserList` is set to true as a property of the form that is being used with the manual action. (ID-10777)

To do this, include the following code in the form:

```
<Form>
   <Properties>
      Property name='CustomUserLists' value='true'/>
   </Properties>
```

Chapter 2: Workflow Services

Identity Manager provides the `checkStringQualityPolicy` Workflow Service method, which checks the value of a designated string against string policy. (ID-12428, 12440)

Name	Required	Valid Values	Description
policy	yes		Identifies the policy (String)
map	no		Provides a map of the data that the string must not contain (Map). `returnNull` -- (Optional) If set to true, the method return a null object upon success.
value	yes		Specifies the value of the string to be checked. (Object)
pwdhistory	no		Lists user's previous passwords in uppercase, encrypted format.
owner	yes		Identifies the user whose string value is being checked.

The method returns a `checkPolicyResult` object. A value of `true` indicates that the string passes the policy test. If the string does not pass the policy test, the method returns an error message. If you have set the `returnNull` option to true on the `map` parameter, the method returns a null object upon success.

Chapter 3: Forms

Identity Manager can identify in the display whether an attribute in a resource's schema map is required. Edit User form identifies these attributes by a * (asterisk). By default, Identity Manager displays this asterisk after the text field that follows the attribute name. (ID-10662)

To customize the placement of the asterisk, follow these steps:

1. Using the Identity Manager BPE or your XML editor of choice, open the Component Properties configuration object.
2. Add `EditForm.defaultRequiredAnnotationLocation=left` to the `<SimpleProperties>` tag.

   Valid values for `defaultRequiredAnnotationLocation` include left, right, and none.
3. Save your changes, and restart your application server.

Chapter 4: FormUtil Methods

- Identity Manager provides the new `checkStringQualityPolicy` FormUtil method, which checks the value of a designated string against string policy. (ID-12428, 12440)

  checkStringQualityPolicy(LighthouseContext s, String policy, Object value, Map map, List pwdhistory, String owner)

Parameter	Description
LighthouseContext	Specifies the current user's Lighthouse context.
policy	(Required) Specifies the name of the policy that the string will be tested against.
value	(Required) Identifies the string value to check.
map	(Optional) Provides a map of the data that must not be contained in the string. `returnNull` -- (Optional) If set to `true`, the method return a null object upon success
pwdhistory	(Optional) Lists user's previous passwords in uppercase, encrypted format.
owner	(Required) Identifies the user whose string value is being checked.

  This method returns a value of true indicates that the string passes the policy test. If the string does not pass the policy test, the method returns an error message. If you have set the `returnNull` option to true on the `map` parameter, the method returns a null object upon success.

- Identity Manager now provides the `controlsAtLeastOneOrganization` FormUtil method. (ID-9260)

  controlsAtLeastOneOrganization(LighthouseContext s, List organizations)

  throws WavesetException {

  Determines whether a currently authenticated user controls any of the organizations specified on a list of one or more organization (ObjectGroup) names. The supported list of organizations include those returned by listing all objects of type ObjectGroup.

Parameter	Description
s	Specifies current user's Lighthouse context (session).
organizations	Specifies a list of one or more organization names. The supported list of organizations include those returned by listing all objects of type ObjectGroup.

This method returns:

`true` – Indicates that the current authenticated Identity Manager user controls any one of the organizations in the list.

`false` – Indicates that the current authenticated Identity Manager user does not control any organizations in the list.

Chapter 5: Views

Account Types

This release of Identity Manager provides support for assigning users multiple accounts on a resource with *account types*. (ID-12697) You can now optionally assign an account type on a resource when assigning resources to a user, with the following limitations:

- Every account on a resource can be of one (and only one) type.
- Users typically have only one account of a given type.

An administrator must first define an account type on a resource before you can associate it with a resource. An IdentityRule must also be defined. (See samples/identityRules.xml for examples of Identity rules.)

Identity Manager uses the IdentityRule subtype to associate a rule with an account type. This rule generates `accountIds` as needed. (These rules function similarly to the Identity Template, but are implemented in XPRESS and have access to the LighthouseContext API).

Consult *Identity Manager Administration* for a discussion on how to use the Identity Manager Administrator Interface to assign account types to resources.

Omitting the Account Type

If you omit an account type on a resource, Identity Manager assigns the default account type, which provides backwards compatibility. However, if no resource has an account type defined, this function is disabled.

The default account type uses the Identity Template. However, you can also specify that the default type use a specified rule instead of the Identity Template.

The default account type is unique in that a user can assign multiple accounts of that type. However, best practice suggests not assigning multiple accounts of the same type.

View-Related Changes

The following changes to Identity Manager views support account types.

- The Resource view now has an `accountType` attribute (List). Each entry is an object with an `identityRule` attribute, which names the rule used to generate `accountIds` for this type.

- The `resources` attribute of both the Role and Application views now allow the use of qualified resource assignments. The syntax for these qualified assignments is `<resource name>|<account type>`.

- The User view now contains the `waveset.resourceAssignments` attribute, which takes qualified resource assignments. (`waveset.resources` contains only unqualified references.) You can change either attribute, but best practice suggests using only `waveset.resourceAssignment` for updates and `waveset.resources` for read-only purposes.)

  How you access the objects in the User view `accounts` attribute has not changed with the addition of this new feature. Use qualified resource names to index the `accounts` list (for example, `accounts[resource|type]` selects the resource account for that resource and type combination. If you are not specifying a type, you can still access these objects through `accounts[resource]`.)
- Related views, including Deprovision and Change Password, also use this type of addressing. The objects in this list also now have a new attribute `accountType`, which specifies the account type of the resource account.

Delegate Approvers View

Use this view to assign one or more Identity Manager users as delegate approvers to an existing approver. This enables an approver to delegate his approval capabilities for a specified period of time to users who may not be approvers themselves.High-level attributes include: (ID-12754)

Note The User view contains these same attributes, (with the exception of the name attribute). These new attributes are contained within the accounts[Lighthouse]. namespace.

name

Identifies the user who is delegating approvals.

delegateApproversTo

Specifies to whom the user is delegating approvals where valid values include manager, selectedUsers, or delegateApproversRule.

delegateApproversSelected

- If `selectedUsers` is the value of `delegateApproversRule`, lists the selected user names.
- If `delegatedApproversRule` is the value of `delegateApproversTo`, identifies the selected rule.
- If `manager` is the value of `delegateApproversTo`, this attribute has no value.

delegateApproversStartDate

Specifies the date on which to start approval delegation. By default, the selected start date’s hours and minutes are 12:01 am of that day.

delegateApproversEndDate

Specifies the date to end approval delegation. By default, the selected end date’s hours and minutes are 11:59 pm of that day

The Role view documentation has been updated as follows. (ID-12390)

Role View

Used to define Identity Manager role objects.

When checked in, this view launches the Manage Role workflow. By default, this workflow simply commits the view changes to the repository, but it also provides hooks for approvals and other customizations.

The following table lists the high-level attributes of this view.

Attribute	Editable?	Data Type	Required
`name`	Read/Write	String	Yes
`resources`	Read/Write	List	No
`applications`	Read/Write	List	No
`roles`	Read/Write	List	No
`assignedResources`	Read/Write	List	No
`notifications`	Read/Write	List	No
`approvers`	Read/Write	List	No
`properties`	Read/Write	List	
`organizations`	Read/Write	List	Yes

Table 1. Role View Attributes

name

Identifies the name of the role. This corresponds to the name of a Role object in the Identity Manager repository.

resources

Specifies the names of locally assigned resources.

applications

Specifies the names of locally assigned applications (Resource Groups).

roles

Specifies the names of locally assigned roles.

assignedResources

Flattened list of all assigned resources via resources, applications, and roles.

Attribute	Editable?	Data Type
`resourceName`		String
`name`		String
`attributes`		Object

resourceName

Identifies the name of the assigned resource.

name

Identifies the resource name or ID (preferably ID).

attributes

Identifies the characteristics of the resource. All subattributes are strings and are editable.

Attribute	Description
`name`	Name of resource attribute
`valueType`	Type of value set for this attribute. Allowed values include Rule, text, or none.
`requirement`	Type of value set by this attribute. allowed values include Rule, Text, None, Value, Merge with Value, Remove with Value, Merge with Value clear existing, Authoritative set to value. Authoritative merge with value, Authoritative merge with value clear existing.
`rule`	Specifies rule name if value type is Rule.
`value`	Specifies value if rule type is Text.

Table 2. attribute Options (Role View)

- `notifications` -- Lists the names of administrators that must approve the assignment of this role to a user.
- `approvers` -- Specifies the names of the approvers that must approve the assignment of this role to a user.

- `properties` -- Identifies the user-defined properties that are stored on this role.
- `organizations` -- Lists organizations of which this role is a member.
- The Resource Account views (Deprovision view, Disable view, Enable view, Password view, Rename User view, Reprovision view, and Unlock view) now support two new view options that you can use to fetch resource account attributes for the user. (ID-12482)
  - `fetchAccounts` – (Boolean) Causes the view to include account attributes for the resources assigned to the user
  - `fetchAccountResources` – Lists resource names to fetch from. If unspecified, all assigned resources will be used.

  You can most easily set these options as form properties. (For more information, see the discussion of the WorkItem List view in the Views chapter of this guide).

Chapter 6: XPRESS Language

- The `instanceOf` function is not currently documented in the XPRESS language chapter. This function identifies whether an object is an instance of the type specified in the `name` parameter. (ID-12700)

  `name` – identifies the object type you are checking against.

  This function returns 1 or 0 (true or false) depending on whether the sub expression object is an instance of the type specified in the `name` parameter.

  The following expression returns 1 because ArrayList is a List

```
<instanceof name='List'>
   <new class='java.util.ArrayList'/>
</instanceof>
```

Chapter 8: HTML Display Components

- The description of the SortingTable component has been revised as follows:

  Use to create a table whose contents can be sorted by column header. Child components determine the content of this table. Create one child component per column (defined by the `columns` property). Columns are typically contained within a FieldLoop.

  This component respects the `align`, `valign`, and `width` properties of the children components when rendering the table cells. (ID-12606)

- Identity Manager now provides the InlineAlert display component. (ID-12606)

  Displays an error, warning, success, or informative alert box. This component is typically located at the top of a page. You can display multiple alerts in a single alert box by defining child components of type `InlineAlert$AlertItem`.

  Properties for this display component include:

  - `alertType` – Specifies the type of alert to display. This property determines the styles and images to use. Valid values are error, warning, success, and info. The value of this property defaults to info. This property is valid only for `InlineAlert`.
  - `header` – Specifies the title to display for the alert box. This can be either a string or a message object. This property is valid for `InlineAlert` or `InlineAlert$AlertItem`.
  - `value` – Specifies the alert message to display. This value can either be a string or a message object. This property is valid for `InlineAlert` or `InlineAlert$AlertItem`.
  - `linkURL` – Specifies an optional URL to display at the bottom of the alert. This property is valid for `InlineAlert` or `InlineAlert$AlertItem`.
  - `linkText` – Specifies the text for the `linkURL`. This can be either a string or a message object. This property is valid for `InlineAlert` or `InlineAlert$AlertItem`.
  - `linkTitle` – Specifies the title for the `linkURL`. This can be either a string or a message object. This property is valid for `InlineAlert` or `InlineAlert$AlertItem`.

Examples

Single alert message

```
<Field>
   <Display class='InlineAlert'>
      <Property name='alertType' value='warning'/>
      <Property name='header' value='Data not Saved'/>
      <Property name='value' value='The data entered is not yet saved.
          Please click Save to save the information.'/>
   </Display>
</Field>
```

Multiple alert messages

Define `alertType` only within the `InlineAlert` property. You can define other properties in the `InlineAlert$AlertItems`.

```
<Field>
   <Display class='InlineAlert'>
```

```
      <Property name='alertType' value='error'/>
   </Display>
   <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Server Unreachable'/>
        <Property name='value' value='The specified server could not
       be contacted.  Please view the logs for more information.'/>
        <Property name='linkURL' value='viewLogs.jsp'/>
        <Property name='linkText' value='View logs'/>
        <Property name='linkTitle' value='Open a new window with
           the server logs'/>
     </Display>
   </Field>
   <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Invalid IP Address'/>
        <Property name='value' value='The IP address entered is
       in an invalid subnet.  Please use the 192.168.0.x subnet.'/>
     </Display>
   </Field>
</Field>
```

- Identity Manager now provides the Selector display component. (ID-12729)

  Provides a single- or multi- valued field (similar to Text or ListEditor components, respectively) with search fields below. After a search is executed, Identity Manager displays results beneath the search fields and populates the results into the value field.

  Unlike other container components, `Selector` has a value (the field we are populating with `search` results). The contained fields are typically search criteria fields. `Selector` implements a property to display the contents of the search results.

  Properties include:

  - `fixedWidth` – Specifies whether the component should have a fixed width (same behavior as Multiselect). (Boolean)
  - `multivalued` – Indicates whether the value is a List or a String. (The value of this property determines whether a ListEditor or Text field is rendered for the value). (Boolean)
  - `allowTextEntry` – Indicates whether values must be selected from the supplied list or can be entered manually. (Boolean)
  - `valueTitle` – Specifies the label to use on the `value` component. (String)
  - `pickListTitle` – Specifies the label to use on the `picklist` component. (String)
  - `pickValues` – the available values in the picklist component (if null, the picklist is not shown). (List)

- pickValueMap – a map of display labels for the values in the picklist. (Map or List)
- sorted – Indicates that the values should be sorted in the picklist (if multivalued and not ordered, the value list will also be sorted). (Boolean)
- clearFields – Lists the fields that should be reset when the Clear button is selected. (List)

The following properties are valid only in a multi-valued component:

- ordered – Indicates that the order of values is important. (Boolean)
- allowDuplicates – Indicates whether the value list can contain duplicates. (Boolean)
- valueMap– Provides a map of display labels for the values in the list. (Map)

These properties are valid only in a single-valued component:

- nullLabel – Specifies a label to use to indicate a value of null. (String)

- The descriptions of the Select and MultiSelect components have been revised as follows to include discussion of the caseInsensitive property. (ID-13364)

MultiSelect Component

Displays a multi-selection object, which Identity Manager displays as two side-by-side text selection keys in which a defined set of values in one box can be moved to another box. Values in the left box are defined by the allowedValues property, values are often obtained dynamically by calling a Java method such as FormUtil.getResources. The values displayed in the right multi-selection box are populated from the current value of the associated view attribute, which is identified through the field name.

You can set the form titles for each box in this multi-selection object through the availabletitle and selectedtitle properties.

If you want a MultiSelect component that does not use an applet, set the noApplet property to true.

Note If you are running Identity Manager on a system running the Safari browser, you must customize all forms containing MultiSelect components to set the noApplet option. Set this option as follows:

```
<Display class='MultiSelect'>
      <Property name='noApplet' value='true'/>
 ...
```

Properties for this display component include:

- availableTitle – Specifies the title of the available box.
- selectedTitle – Specifies the title of the selected box.

- `ordered` – Defines whether selected items can be moved up or down within the list of items in the text box. A `true` value indicates that additional buttons will be rendered to permit selected items to be moved up or down.
- `allowedValues` – Specifies the values associated with the left box of the multi-selection object. This value must be a list of strings. **Note**: The `<Constraints>` element can be used to populate this box, but its use is deprecated.
- `sorted` – Specifies that the values in both boxes will be sorted alphabetically.
- `noApplet` – Specifies whether the MultiSelect component will be implemented with an applet or with a pair of standard HTML select boxes. The default is to use an applet, which is better able to handle long lists of values. See preceding note for information on using this option on systems running the Safari browser.
- `typeSelectThreshold` – (Available only when the `noApplet` property is set to true.) Controls whether a type-ahead select box appears under the `allowedValue` list. When the number of entries in the left select box reaches the threshold defined by this property, an additional text entry field appears under the select box. As you type characters into this text field, the select box will scroll to display the matching entry if one exists. For example, if you enter **w**, the select box scrolls to the first entry that begins with **w**.
- `width` – Specifies the width of the selected box in pixels. The default value is 150.
- `height` – Specifies the width of the selected box in pixels. The default value is 400.
- `caseInsensitive` -- Use to perform case-insensitive comparisons.

Select Component

Displays a single-selection object. Values for the list box must be supplied by the `allowedValues` property.

Properties for this display component are:

- `allowedValues` – Specifies the list of selectable values for display in the list box.
- `allowedOthers` – When set, specifies that initial values that were not on the `allowedValues` list should be tolerated and silently added to the list.
- `autoSelect` – When set to `true`, this property causes the first value in the `allowedValues` list to be automatically selected if the initial value for the field is null.
- `caseInsensitive` -- Use to perform case-insensitive comparisons.

  - `multiple` – When set to `true`, allows more than one value to be selected.
  - `nullLabel` – Specifies the text that displays at the top of the list box when no value is selected.
  - `optionGroupMap` – Allows the selector to render options in groups using the `<optgroup>` tag. Format the map such that the keys of the maps are the group labels, and the elements are lists of items to be selectable. (Values must be members of `allowedValues` in order to render.)
  - `size` – (Optional) Specifies the maximum number of rows to display. If the number of rows exceeds this size, a scroll bar is added.
  - `sorted` – When set to `true`, causes the values in the list to be sorted.
  - `valueMap` – Maps raw values to displayed values.

  The component supports the `command` and `onChange` properties.

- The discussion of the `DatePicker` component should describe the following new properties. (ID-14802)

  The `DatePicker` HTML component now permits you to select discrete dates. You can specify a date range set that allows for particular dates to be picked from the calendar.

  `DatePicker` implements the following two new properties:

  `SelectAfter` -- Limits the selectable dates that are displayed in the calendar to dates on or after the entered date. This property value can be a date string or a Java Date object.

```
<Property name='SelectAfter' value='**/**/****'/>
```

  `SelectBefore` -- Limits the selectable dates displayed in the calendar to dates on or before the entered date. This property value can be a date string or a Java Date object.

```
<Property name='SelectBefore' value='**/**/****'/>
```

  Wherever you use a form that implements the `<Display class='DatePicker'>` tag, add these variables to the form to set up the date range. If you do not set these properties, the calendar will not be limited in the dates that can be selected.

Identity Manager Technical Deployment Overview

The following discussion of associated workflows, forms, and JSPs belongs to the architectural overview of the *Identity Manager Technical Deployment Overview* (ID-7332).

Process Execution

When a user enters data into a field on a page and clicks Save, view, workflow and form components work together to execute the processes necessary to process the data.

Each page in Identity Manager has a view, workflow and form associated with it that performs the necessary data processing. These workflow, view, and form associations are listed in the following two tables.

Identity Manager User Interface Processes

The following tables indicate the forms, views and workflows that are involved in processes initiated from the following Identity Manager User Interface pages:

User Interface Page	Form	View	Workflow
Main menu	• endUserMenu • default End User Menu	User View is read-only. No modifications can be made on this page	none
Change Password	• endUserChangePassword • default Change Password Form	Password	• changeUserPassword • default Change User Password
Change Other Account Attributes	• endUserForm • default End User Form	User	Update User
Check Process Status	• endUserTaskList • default End User Task List	List View includes information on TaskInstance objects launched by the user	none
Process Status Page is generated by the TaskViewResults class	none	none	none

User Interface Page	Form	View	Workflow
Available Processes	• endUserLaunchList • default End User Launch List	List View includes information on TaskDefinition objects accessible to the user	none
Launch Process Launches a selected TaskDefinition	Defined by the TaskDefinition	Process	none
Change Answers to Authentication Questions	• changeAnswers • default Change User Answers Form	ChangeUserAnswers	none
Self Discovery Can link to existing resource accounts only	• selfDiscovery • default Self Discovery	User	Update User
Inbox	• endUserWorkItemList • default End User Work Item List	List View contains information about WorkItems directly owned by the current user	none
Inbox Item Edit	Specified by WorkItem or auto-generated	WorkItem	none

Administrator Interface Processes

The following tables identify the forms, views, workflows, and JSPs that are involved in processes initiated from these Identity Manager Administrator Interface pages:

Administrator Interface Page	Form	View	Workflow
Create Organization and Edit Organization	System Configuration mapping Depending upon context, can be one of several forms, including: • Organization Form • Organization Rename Form • Directory Junction Form • Virtual Organization Form • Virtual Organization Refresh Form	Org	none
Create User	• userForm • default Tabbed User Form	User	• createUser • default Create User
Update User	• userForm • default Tabbed User Form	User	• updateUser • default Update User
Disable User's Resource Accounts	• disableUser • default Disable User	Disable	• disableUser • default Disable User
Rename User	• renameUser • default Rename User Form	RenameUser	• renameUser • default Rename User
Update User's Resource Accounts	• reprovisionUser • default Reprovision Form	Reprovision	• updateUser • default Update User
Unlock User's Resource Accounts	• unlockUser • default Unlock User	Unlock	• unlockUser • default Unlock User
Delete User's Resource Accounts	• deprovisionUser • default Deprovision Form	Deprovision	• deleteUser • default Delete User

Administrator Interface Page	Form	View	Workflow
Change User Password Uses same workflow as end-user GUI, but different form	• changePassword • default Change User Password Form	ChangeUser Password	• changeUserPassword • default Change User Password
Reset User Password	• resetPassword • default Reset User Password Form	ResetUserPassword	• changeUserPassword • default Change User Password
Change My Password Same view, form, and workflow as End-User Change Password but different JSP	• endUserChangePassword • default Change Password Form	Password	• changeUserPassword • default Change User Password
Change My Answers Same view, form as End-User Change Answers but different JSP	• changeAnswers • default Change User Answers Form	ChangeUserAnswers	none
Approvals	• workItemList • default Work Item List • default form includes Work Item Confirmation	WorkItemList	none
Edit WorkItem Check in of the WorkItem view results in the resumption of the workflow that created it, but no workflow is created just to process the work item checkin	Specified by WorkItem, or auto-generated	WorkItem	none
Launch Task Launches a selected TaskDefinition	Defined by the TaskDefinition	Process	none

Administrator Interface Page	Form	View	Workflow
Create and Update Scheduled Tasks	no System Configuration mapping, default Task Schedule Form, merged with TaskDefinition form This form is generated by combining the TaskDefinition form with Task Schedule Form as a wrapper	TaskSchedule	none
Create Role and Edit Role	no System Configuration mapping The default Role Form and Role Rename Form depend on context	Role	• manageRole • default Manage Role
Edit Resource	no System Configuration mapping, depends on context, forms include: • Change Resource Account Password Form • Reset Resource Account Password Form • Edit Resource Policy Form • Resource Rename Form • Resource Wizard <resource type> • Resource Wizard. Allows type-specific wizard forms, default to Resource Wizard	Resource	• manageResource • default Manage Resource
Edit Capability	changeCapabilities, default Change User Capabilities Form	ChangeUserCapabilities	none

Java Server Pages (JSPs) and Their Role in Identity Manager

The following tables describe the JSPs that are shipped with the system as well as their Administrator and User Interface pages.

JSPs for Identity Manager User Interface

Page	Associated JSP
Main Menu	user/main.jsp
Change Password	user/changePassword.jsp
Change Other Account Attributes	user/changeAll.jsp
Check Process Status	user/processStatusList.jsp
Process Status	user/processStatus.jsp
Available Processes	user/processList.jsp
Launch Process	user/processLaunch.jsp
Change Answers to Authentication Questions	user/changeAnswers.jsp
Self Discovery	user/selfDiscover.jsp
Inbox	user/workItemList.jsp
Inbox Item Edit	user/workItemEdit.jsp

JSPs for Admin Interface

Page	Associated JSP
Create Organization and Edit Organization	security/orgedit.jsp
Create User	account/modify.jsp
Update User	account/modify.jsp
Disable User’s Resource Accounts	account/resourceDisable.jsp
Rename User	account/renameUser.jsp
Update User’s Resource Accounts	account/resourceReprovision.jsp
Unlock User’s Resource Accounts	admin/resourceUnlock.jsp
Delete User’s Resource Accounts	account/resourceDeprovision.jsp
Change User Password	admin/changeUserPassword.jsp

Page	Associated JSP
Reset User Password	admin/resetUserPassword.jsp
Change My Password	admin/changeself.jsp
Change My Answers	admin/changeAnswers.jsp
Approvals	approval/approval.jsp
Edit WorkItem	approval/itemEdit.jsp
Launch Tasks	task/taskLaunch.jsp
Create and Update Scheduled Tasks	task/editSchedule.jsp
Create Role and Edit Role	roles/applicationmodify.jsp
Edit Resource	resources/modify.jsp
Edit Capability	account/modifyCapabilities.jsp

Identity Manager 6.0 Resources Reference

- The list of Supported Account Attributes under Resources Reference > Active Directory > Account Attributes > Account Attribute Support is more current in the PDF version of the document than the HTML version. Please refer to the PDF version. (ID-12630)
- The Identity Manager 6.0 Resources Reference 2005Q4M3 top level node at the following URL does not contain a link to the section titled Domino: (ID-12636)

```
http://docs.sun.com/app/docs/doc/819-4520
```

Please find the Domino section by opening Contents at this node or at the following URL:

```
http://docs.sun.com/source/819-4520/Domino_Exchange.html#wp999317
```

Access Manager Adapter

Step 5 in the procedure “General Configuration” should state the following:

5. Add the following lines to the `java.security` file, if they do not already exist:

```
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.net.ssl.internal.ssl.Provider
```

The number that follows security.provider in each line specifies the order in which Java consults security provider classes and should be unique. The sequence numbers may vary in your environment. If you already have multiple security providers in the java.security file, insert the new security providers in the order given above and renumber any existing security providers. Do not remove the existing security providers and do not duplicate any providers. (ID-12044)

Active Directory Adapter

Active Directory now supports the `thumbnailPhoto` (Windows 2000 Server and greater) and `jpegPhoto` (Windows 2003) binary attributes.

BridgeStream SmartRoles Adapter

Identity Manager now provides a BridgeStream SmartRoles resource adapter that provisions users in SmartRoles. This adapter places users in the appropriate organizations within SmartRoles so that SmartRoles can determine which business roles those users should have.

When retrieving a user from SmartRoles, the adapter retrieves the user's business roles. These business roles can be used within Identity Manager to determine the Identity Manager roles, resources, attributes, and access that user should be assigned.

Additionally, SmartRoles can be a source of user changes using Active Sync. You can load SmartRoles users into Identity Manager and reconcile them.

For detailed information about this adapter, see the *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-12714)

ClearTrust Adapter

- The ClearTrust resource adapter now supports the 5.5.2 version of ClearTrust.
- Steps 2 and 3 in the Identity Manager Installation Notes procedure should state the following (ID-12906):

1. Copy the `ct_admin_api.jar` file from your Clear Trust installation CD to the `WEB-INF\lib` directory.
2. If using SSL, copy the following files to the `WEB-INF\lib` directory.

Note If you are provisioning to an RSA Clear Trust 5.5.2 resource, additional libraries are not required for SSL communication.

- `asn1.jar`
- `certj.jar`
- `jce1_2-do.jar`
- `jcert.jar`
- `jnet.jar`
- `jsafe.jar`
- `jsaveJCE.jar`
- `jsse.jar`
- `rsajsse.jar`
- `sslj.jar`

Database Table Adapter

This adapter supports binary data types, including BLOBs, in Oracle. The corresponding attributes must be marked as binary on the schema map. Sample binary attributes include graphics files, audio files, and certificates.

Flat File Active Sync Adapter

- The administrative user must have read and write access to the directory that contains the flat file. This user must also have delete access if the **Process Differences Only** Active Sync parameter is enabled.

  In addition, the administrator account must have read, write, and delete permissions on the directory specified in the Active Sync **Log File Path** field. (ID-12477)
- If the flat file format is LDIF, then binary attributes, such as graphics files, audio files, and certificates may be specified. Binary attributes are not supported for CSV and pipe-delimited files.

HP OpenVMS Adapter

Identity Manager now provides an HP OpenVMS resource adapter that supports VMS version 7.0 and later. For detailed information about this adapter, see the *Sun Java™ System Identity Manager Resources Reference Addendum*. (ID-8556)

JMS Listener Adapter

The JMS Listener adapter now supports synchronous message processing instead of asynchronous processing. As a result, the second paragraph in the Connections section of the Usage Notes should read as follows:

The JMS Listener adapter operates in synchronous mode. It establishes a synchronous message consumer on the queue or topic destination specified by the **JNDI name of Destination** field. During each poll interval, the adapter will receive and process all available messages. Messages can be (optionally) additionally qualified by defining a valid JMS message selector string for the **Message Selector** field.

The Message Mapping section should contain the following:

When the adapter processes a qualified message, the received JMS message is first converted to a map of named values using the mechanism specified by the **Message Mapping** field. Refer to this resulting map as the *message value map*.

The message value map is then translated to the Active Sync map using the account attributes schema map. If the adapter has account attributes specified, the adapter searches the message value map for key names that also appear as a resource user attribute in the schema map. If present, the value is copied to the Active Sync map, but the entry name in the Active Sync map is translated to the name specified in the Identity system user attribute column in the schema map.

If the message value map has an entry that cannot be translated using the account attributes schema map, then the entry from the message value map is copied unaltered to the Active Sync map.

LDAP Adapter

Binary Account Attribute Support

The following binary account attributes from the inetOrgPerson object class are now supported:

Resource User Attribute	LDAP Syntax	Description
audio	Audio	An audio file.
jpegPhoto	JPEG	An image in JPEG format.
userCertificate	certificate	A certificate, in binary format.

Other binary accounts might be supported, but they have not been tested.

Disabling and Enabling Accounts

The LDAP adapter provides several ways to disable accounts on an LDAP resource. Use one of the following techniques to disable accounts.

Change the password to an unknown value

To disable accounts by changing the password to an unknown value accounts, leave the **Activation Method** and **Activation Parameter** fields blank. This is the default method for disabling accounts. The account can be re-enabled by assigning a new password.

Assign the `nsmanageddisabledrole` role

To use the `nsmanageddisabledrole` LDAP role to disable and enable accounts, configure the LDAP resource as follows:

1. On the Resource Parameters page, set the **Activation Method** field to `nsmanageddisabledrole`.
2. Set the **Activation Parameter** field to *`IDMAttribute`*`=CN=nsmanageddisabledrole,`*`baseContext`*. (*`IDMAttribute`* will be specified on the schema in the next step.)
3. On the Account Attributes page, add *IDMAttribute* as an Identity System User attribute. Set the Resource User attribute to `nsroledn`. The attribute must be of type string.
4. Create a group named nsAccountInactivationTmp on the LDAP resource and assign `CN=nsdisabledrole,`*`baseContext`* as a member.

LDAP accounts can now be disabled. To verify using the LDAP console, check the value of the `nsaccountlock` attribute. A value of `true` indicates the account is locked.

If the account is later re-enabled, the account is removed from the role.

Set the `nsAccountLock` attribute

To use the nsAccountLock attribute to disable and enable accounts, configure the LDAP resource as follows:

1. On the Resource Parameters page, set the **Activation Method** field to `nsaccountlock`.
2. Set the **Activation Parameter** field to the name of the attribute that you will define in the next step. Also assign a value to test for. For example, `accountLockAttr=true`.

3. On the Account Attributes page, add the value specified in the Activation Parameter field as an Identity System User attribute. Set the Resource User attribute to `nsaccountlock`. The attribute must be of type string.

LDAP accounts can now be disabled. To verify using the LDAP console, check the value of the `nsaccountlock` attribute. A value of `true` indicates the account is locked.

If the account is later re-enabled, the attribute is removed.

Disable accounts without the `nsmanageddisabledrole` and `nsAccountLock` attributes

If the `nsmanageddisabledrole` and `nsAccountLock` attributes are not available on your directory server, but the directory server has a similar method of disabling accounts, enter one of the following class names into the **Activation Method** field. The value to enter in the **Activation Parameter** field varies, depending on the class.

Class Name	When to Use:
com.waveset.adapter.util. ActivationByAttributeEnableFalse	The directory server enables an account by setting an attribute to false, and disables an account by setting the attribute to true. Add the attribute to the schema map. Then enter the Identity Manager name for the attribute (defined on the left side of the schema map) in the **Activation Parameter** field.
com.waveset.adapter.util. ActivationByAttributeEnableTrue	The directory server enables an account by setting an attribute to true, and disables an account by setting the attribute to false. Add the attribute to the schema map. Then enter the Identity Manager name for the attribute (defined on the left side of the schema map) in the **Activation Parameter** field.
com.waveset.adapter.util. ActivationByAttributePullDisablePushEnable	Identity Manager should disable accounts by pulling an attribute/value pair from LDAP and enable accounts by pushing an attribute/value pair to LDAP. Add the attribute to the schema map. Then enter the attribute/value pair in the **Activation Parameter** field. Use the Identity Manager name for the attribute, as defined on the left side of the schema map.

Class Name	When to Use:
com.waveset.adapter.util.ActivationByAttributePushDisablePullEnable	Identity Manager should disable accounts by pushing an attribute/value pair to LDAP and enable accounts by pulling an attribute/value pair from LDAP. Add the attribute to the schema map. Then enter the attribute/value pair in the **Activation Parameter** field. Use the Identity Manager name for the attribute, as defined on the left side of the schema map.
com.waveset.adapter.util.ActivationNsManagedDisabledRole	The directory uses a specific role to determine the account status. If an account is assigned to this role, the account is disabled. Add the role name to the schema map. Then enter a value in the **Activation Parameter** field, using the following format: `IDMAttribute=CN=roleName,baseContext` `IDMAttribute` is the Identity Manager name for the role, as defined on the left side of the schema map.

Oracle/Oracle ERP Adapters

The Oracle/Oracle ERP chapter in the *Identity Manager Resources Reference* was divided into two separate chapters for this release. See the *Sun Java™ System Identity Manager Resources Reference Addendum* to view these two new chapters. (ID-12758)

Oracle Adapter

- Support for Oracle 8i was erroneously removed from the adapters table and from the Oracle adapter section in Chapter 1 of the Identity Manager Resources Reference. Identity Manager still supports Oracle 8*i* as a resource. (ID-13078)
- The `updateableAttributes` section name was corrected to *`updatableAttributes`* in step one of the Cascade Deletes section of this chapter, as follows (ID-13075):

The noCascade account attribute indicates whether to perform cascade drops when deleting users. By default, cascade drops are performed. To disable cascade drops:

1. Add an entry to `updatableAttributes` section of System Configuration Object:

Oracle ERP Adapter

The Oracle ERP adapter now provides an `employee_number` account attribute that represents an `employee_number` from the `per_people_f` table (ID-12796):

- When you enter a value on create, the adapter tries to lookup a user record in the `per_people_f` table, retrieve the `person_id` *into* the create API, and insert the `person_id` into the `fnd_user` table's `employee_id` column.
- If no employee_number is entered on create, no linking is attempted.
- If you enter and employee_number on create and that number is not found, then the adapter throws an exception.
- The adapter will try to return the `employee_number` on a `getUser`, if `employee_number` is in the adapter schema.

Auditing Responsibilities

Added multiple attributes to the Oracle ERP adapter to support auditing features. (ID-11725)

To audit the sub-items (such as forms and functions) of responsibilities assigned to users, add the `auditorObject` to the schema map. `auditorObject` is a complex attribute that contains a set of responsibility objects. The following attributes are always returned in a responsibility object:

- responsibility
- userMenuNames
- menuIds
- userFunctionNames
- functionIds
- formIds
- formNames
- userFormNames
- readOnlyFormIds
- readWriteOnlyFormIds
- readOnlyFormNames
- readOnlyUserFormNames
- readWriteOnlyFormNames

- readWriteOnlyUserFormNames
- functionNames
- readOnlyFunctionNames
- readWriteOnlyFunctionNames

Note readOnly and ReadWrite attributes are identified by querying the PARAMETERS column in the fnd_form_functions table for one of the following:

- QUERY_ONLY=YES
- QUERY_ONLY="YES"
- QUERY_ONLY = YES
- QUERY_ONLY = "YES"
- QUERY_ONLY=Y
- QUERY_ONLY="Y"
- QUERY_ONLY = Y
- QUERY_ONLY = "Y"

If the **Return Set of Books and/or Organization** resource parameter is set to TRUE, the following attributes are also returned:

- setOfBooksName
- setOfBooksId
- organizationalUnitName
- organizationalUnitId

With the exception of the responsibility, setOfBooksName, setOfBooksId, organizationalUnitId, and organizationalUnitName attributes, the attribute names match account attribute names that may be added to the schema map.The account attributes contain an aggregate set of values that are assigned to the user. The attributes that are contained in the `responsibility` objects are specific to the responsibility.

The auditorResps[] view provides access to the responsibility attributes. The following form snippet returns all the active responsibilities (and their attributes) assigned to a user .

```
<defvar name='audObj'>
   <invoke name='get'>
      <ref>accounts[Oracle ERP 11i VIS].auditorObject</ref>
   </invoke>
</defvar>
<!-- this returns list of responsibility objects -->
```

```
<defvar name='respList'>
   <invoke name='get'>
      <ref>audObj</ref>
      <s>auditorResps[*]</s>
   </invoke>
</defvar>
```

For example:

- `auditorResps[0].responsibility` returns the name of the first responsibility object.
- `auditorResps[0].formNames` returns the formNames of the first responsibility object.

SAP Adapter

- In the Account Attributes section, the table describing the default iDoc infotypes supported by the SAP HR Active Sync adapter was corrected. The supported subtype listed for the 0105 Communication infotype was changed from EMAIL to *MAIL* as follows (ID-12880):

  By default, the following infotypes are supported:

Infotype	Name	Supported Subtypes
0000	Actions	Not applicable
0001	Organizational Assignment	Not applicable
0002	Personal Data	Not applicable
0006	Addresses	01 (permanent residence), 03 (home residence)
0105	Communication	MAIL (email address), 0010 (internet address)

The SAPHRActiveSyncAdapter now supports mySAP ERP ECC 5.0 (SAP 5.0). As a result, the following changes were made to Resource Configuration Notes (ID-12769):

SAP Resource Adapter

The following resource configuration notes are applicable to the SAP resource adapter only.

To enable the ability for a user to change his or her own SAP password, perform the following steps:

1. Set the **User Provides Password On Change** resource attribute.
2. Add **`WS_USER_PASSWORD`** to both sides of the schema map. You do not need to modify the user form or other forms.

SAP HR Active Sync Adapter

The following resource configuration notes are applicable to the SAP HR Active Sync adapter only.

The SAP Application Link Enabling (ALE) technology enables communication between SAP and external systems, such as Identity Manager. The SAP HR Active Sync adapter uses an outbound ALE interface. In an outbound ALE interface, the base logical system becomes the sender for outbound messages and the receiver of inbound messages. A SAP user will likely be logged into the base logical system/client when making changes to the database (for example, hiring an employee, updating position data, terminating an employee, etc.) A logical system/client must also be defined for the receiving client. This logical system will act as the receiver of outbound messages. As for the message type between the two systems, the Active Sync adapter uses a `HRMD_A` message type. A message type characterizes data being sent across the systems and relates to the structure of the data, also known as an IDoc type (for example, `HRMD_A05`).

The following steps provide the configurations required on SAP for the Active Sync adapter to receive authoritative feeds from SAP HR:

Note You must configure the SAP system parameters to enable Application Link Enabling (ALE) processing of `HRMD_A` IDocs. This allows for data distribution between two application systems, also referred to as *messaging*.

Creating a Logical System

Depending on your current SAP environment, you might not need to create a logical system. You might only need to modify an existing Distribution Model by adding the `HRMD_A` message type to a previously configured Model View. It is important, however, that you follow SAP's recommendations for logical systems and configuring your ALE network. The following instructions assume that you are creating new logical systems and a new model view.

1. Enter transaction code **`SPRO`**, then display the SAP Reference IMGproject (or the project applicable to your organization).
2. Based on the SAP version you are using, perform one of the following:

- For SAP 4.6, click **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
- For SAP 4.7, click **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
- For SAP 5.0, click **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Define Logical System**.

3. Click **Edit** > `New Entries`.
4. Enter a name and a description for the logical system you want to create (IDMGR).
5. Save your entry.

Assigning a Client to the Logical System

1. Enter transaction code SPRO, then display the SAP Reference IMGproject (or the project applicable to your organization).
2. Based on the SAP version you are using, perform one of the following:
   - For SAP 4.6, click **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
   - For SAP 4.7, click **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
   - For SAP 5.0, click **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Assign Client to Logical System.**
3. Select the client.
4. Click **GOTO > Details** to display the Client Details dialog box.
5. In the Logical System field, enter the logical system you want to assign to this client.
6. In the Changes and Transports for Clients section, click **Automatic Recording of Changes**.
7. Save your entry.

Creating a Distribution Model

To create a distribution model:

1. Verify that you are logged on to the sending system/client.
2. Enter transaction code `BD64`. Ensure that you are in Change mode.
3. Click **Edit > Model View > Create**.
4. Enter the short and technical names for your view, as well as the start and end date, then click **Continue**.
5. Select the view you created, then click **Add Message Type**.
6. Define the sender/logical system name.
7. Define the receiver/server name.
8. In the Protection Client Copier and Comparison Tool section, click **Protection Level: No Restriction**.
9. Define the Message Type you want to use (HRMD_A), then click **Continue**.
10. Click **Save**.

Registering the RFC Server Module with the SAP Gateway

During initialization, the Active Sync adapter registers with the SAP Gateway. It uses “IDMRFC” for its ID. This value must match the value set in the SAP application. You must configure the SAP application so that the RFC Server Module can create a handle to it. To register the RFC Server Module as an RFC destination:

1. In the SAP application, go to transaction SM59.
2. Expand the TCP/IP connections directory.
3. Click **Create (F8)**.
4. In the RFC destination field, enter the name of the RFC destination system. (IDMRFC).
5. Set the connection type to **T** (Start an external program via TCP/IP).
6. Enter a description for the new RFC destination, and then click **Save**.
7. Click the Registration button for the Activation Type.
8. Set the Program ID. We recommend that you use the same value as the RFC destination (IDMRFC), and then click Enter.
9. If the SAP system is a Unicode system, the port must be configured for Unicode. Click the **Special Options** tab, and look for the Character Width In Target System section. There is a setting for unicode and non-unicode.
10. Using the buttons at the top - **Test Connection** and **Unicode Test** - test the connection to the Identity Manager resource. You must have the adapter started for the test to pass.

Creating a Port Definition

The port is the communication channel to which IDocs are sent. The port describes the technical link between the sending and receiving systems. You should configure an RFC port for this solution. To create a port definition:

1. Enter transaction code **`WE21`**.
2. Select Transactional RFC, then click the **Create** icon. Enter **`IDMRFC`** for the RFC Destination.
3. Save your changes.

Modifying the Port Definition

When you generated a partner profile, the port definition might have been entered incorrectly. For your system to work properly, you need to modify the port definition.

1. Enter transaction code **`WE20`**.
2. Select **Partner Type LS**.
3. Select your receiving partner profile.
4. Select **Outbound Parameters**, then click **Display**.
5. Select message type **`HRMD_A`**.
6. Click **Outbound Options**, then modify the receiver port so it is the RFC port name you created (IDMGR).
7. From the Output Mode, select **Transfer IDoc Immediately** to send IDocs immediately after they are created.
8. From the IDoc Type section, select a basictype:
    - For SAP 4.6, select **HRMD_A05**
    - For SAP 4.7 or 5.0, select **HRMD_A06**
9. Click **Continue**/**Save**.

Scripted JDBC Adapter

Identity Manager now provides a Scripted JDBC resource adapter to support management of user accounts in any database schema and in any JDBC-accessible database. This adapter also supports Active Sync to poll for account changes in the database. For detailed information about this adapter, see the Sun Java™ System *Identity Manager Resources Reference Addendum*. (ID-12506)

Shell Script Adapter

Identity Manager now provides a Shell Script resource adapter to support management of resources controlled by shell scripts that are running on the system hosting the resource. This adapter is a general purpose adapter, and is therefore highly configurable.

Siebel CRM Adapter

Siebel objects that require parent/child business component navigation can now be created and updated. This is an advanced feature that is not typically implemented in Identity Manager.

The advanced navigation feature allows you to optionally specify the following information needed to create and update child business components:

- business object name
- parent business component name
- parent search attribute
- target business component
- target search attribute
- in scope attributes (which attributes of the business component should be set/updated)
- optional co-action

An advanced navigation rule can be used during create and update actions. It cannot be used for other types of actions.

To implement the advanced navigation feature of the Siebel CRM adapter, you must perform the following tasks:

- Add an attribute to the schema map in which the Resource User Attribute (right hand side) is named PARENT_COMP_ID.
- Use the debug page to manually add the following ResourceAttribute to your resource's XML

```
<ResourceAttribute name='AdvancedNavRule'
   displayName='Advanced Nav Rule'
   value='MY_SIEBEL_NAV_RULE'>
</ResourceAttribute>
```

  Replace *MY_SIEBEL_NAV_RULE* with a valid rule name.

- Write the advanced navigation rule. The rule should expect two variables to be present:

  `resource.action` — The value must be either `create` or `update`.

  `resource.objectType` — For normal account maintenance, this value will be `account`.

  The rule must return a map with one or more of the following name/value pairs:

Attribute	Definition
`busObj`	The name of the business object.
`parentBusComp`	The name of the parent business component for `busObj`. The context of the business object is updated by moving to the first qualified (see `parentSearchAttr`) record of this business component
`parentSearchAttr`	The attribute to use as the search field in the `parentBusComp`. The value to search for is expected to be present as the value for the attribute whose Resource User Attribute name is PARENT_COMP_ID.
`busComp`	The name of final business component to create or update. If creating, then a new record of this business component will be created in the business object. If updating, then the business component record to update is selected by moving to the first qualified (see `searchAttr`) record of this business component.
`searchAttr`	The attribute to use as the search field in the `busComp`. The value to search for is the user's account ID.
`attributes`	A list of strings that specifies the set of fields in the `busComp` that will be set or updated. This list overrides the attributes defined in the resource's schema map for the action being performed.
`coAction`	If the requested action (`resource.action`) is `create`, then specify a `coAction` value of `update` to instruct the adapter to also perform an update immediately following the create. This may be necessary if the create cannot set all the necessary fields, and therefore an update must also occur to logically complete the create. This attribute will be ignored unless `resource.action` is `create` and `coAction` is set to `update`.

  An example navigation rule is provided in `$WSHOME/sample/rules/SiebelNavigationRule.xml`.

Sun Java System Access Manager Adapter

- This adapter supports legacy mode only for Access Manager 7 and later. Realms are not supported.

Installing and Configuring Sun Java System Access Manager (Versions Prior to Access Manager 7.0)

Steps 4 and 8 in the "Installing and Configuring Sun Java System Access Manager" procedure should read as follows (ID-13087):

1. Create a directory to place files that will be copied from the Sun Java System Access Manager server. This directory will be called *CfgDir* in this procedure. The location of the Sun Java System Access Manager will be called *AccessMgrHome*.
2. Copy the following files from *AccessMgrHome* to *CfgDir*. Do not copy the directory structure.
   - `lib/*.*`
   - `locale/*.properties`
   - `config/serverconfig.xml`
   - `config/SSOConfig.properties` (Identity Server 2004Q2 and later)
   - `config/ums/ums.xml`
3. On UNIX, it may be necessary to change the permissions of the jar files in the *CfgDir* to allow universal read access. Run the following command to change permissions:

   ```
   chmod a+r CfgDir/*.jar
   ```
4. Prepend the JAVA classpath with the following:
   - **Windows**: `CfgDir;CfgDir/am_sdk.jar;CfgDir/am_services.jar;CfgDir/am_logging.jar`
   - **UNIX**: `CfgDir:CfgDir/am_sdk.jar:CfgDir/am_services.jar:CfgDir/am_logging.jar`
5. If you are using version 6.0, set the Java system property to point to your *CfgDir*. Use a command similar to the following:

   ```
   java -Dcom.iplanet.coreservices.configpath=CfgDir
   ```
6. If you are using version 6.1 or later, add or edit the following lines in the `CfgDir/AMConfig.properties` file:

   ```
   com.iplanet.services.configpath=CfgDircom.iplanet.security.
   SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFact
   oryImpl

   com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.
   factory.JSSESocketFactory

   com.iplanet.security.encryptor=com.iplanet.services.util.
   JCEEncryption
   ```

   The first line sets the `configpath`. The last three lines change security settings.

7. Copy the `CfgDir/am_*.jar` files to `$WSHOME/WEB-INF/lib`. If you are using version 6.0, also copy the `jss311.jar` file to the `$WSHOME/WEB-INF/lib` directory.
8. If Identity Manager is running on Windows and you are using Identity Server 6.0, copy `IdServer\lib\jss\*.dll` to *CfgDir* and add *CfgDir* to your system path.

Note In an environment where Identity Manager is installed on a different system from Sun Java System Access Manager check the following error conditions. If an error java.lang.ExceptionInInitializerError, followed by java.lang.NoClassDefFoundError, on subsequent attempts, is returned when attempting to connect to the Sun Java System Access Manager resource, then check for incorrect or missing configuration data.

Also, check the jar file for the class indicated by the `java.lang.NoClassDefFoundError`. Prepend the classpath of the jar file containing the class to the JAVA classpath on the application server.

Installing and Configuring Sun Java System Access Manager (Versions 7.0 and Later in Legacy Mode)

Use the following steps io install and configure the resource adapter for legacy mode.

1. Follow the instructions provided in the *Sun Java™ System Access Manager 7 2005Q4 Developer's Guide* to build the client SDK from the Sun Access Manager installation.
2. Extract the `AMConfig.properties` and `amclientsdk.jar` files from the `war` file that is produced.
3. Put a copy of the `AMConfig.properties` in the following directory:

   `InstallDir/WEB-INF/classes`
4. Place a copy of `amclientsdk.jar` in the following directory:

   `InstallDir/WEB-INF/lib`

Sun Java System Communications Services Adapter

- The sample script that could be run on the proxy resource after creating a user is listed incorrectly. The following script should be used instead: (ID-12536)

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -c -P user/%WSUSER_accountId%.*
```

- The following binary account attributes from the inetOrgPerson object class are now supported:

Resource User Attribute	LDAP Syntax	Description
audio	Audio	An audio file.
jpegPhoto	JPEG	An image in JPEG format.
userCertificate	certificate	A certificate, in binary format.

  Other binary accounts might be supported, but they have not been tested.

Top Secret Adapter

The *Identity Manager Resources Reference* incorrectly states that the Top Secret adapter supports renaming accounts. The adapter does not support renaming Top Secret accounts.

Identity Manager Tuning, Troubleshooting, and Error Messages

Additions

- You can now use the standard tracing facility on com.waveset.task.Scheduler to trace the task scheduler if a task is having problems.

  See *Tracing the Identity Manager Server* in *Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages* for more information.

- To debug a problem that is occuring at a level below a specific entry method, consider tracing at the method level. Identity Manager now provides the ability to trace only a method and its direct and indirect subcalls. (ID-14967)

  To enable this feature, set the trace level for a scope with the `subcalls` modifier, as shown below:

```
trace 4,subcalls=2
com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
```

  This will trace the `reconcileAccount()` method at level 4 and all subcalls at level 2.

  See *Defining a Trace Configuration* in *Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages* for more information.

Corrections

Because you must install JDK 1.4.2 for this release, the instruction to remove the Cryptix jars (`cryptix-jceapi.jar` and `cryptix-jce-provider.jar`) from the `idm\WEB-INF\lib` directory in Chapter 1: *Performance Tuning, Optimizing the J2EE Environment*, no longer applies (unless you are upgrading from a previous version of Identity Manager).

Identity Manager Deployment Tools

Corrections

Chapter 7: Using Identity Manager Web Services

The launchProcess example provided in the ExtendedRequest Examples section was corrected as follows (ID-13044):

launchProcess

The following example, shows a typical format for `launchProcess` request. (View — Process view).

```
ExtendedRequest req = new ExtendedRequest();
req.setOperationIdentifier("launchProcess");
req.setAsynchronous(false);
req.setAttribute("process", "Custom Process Name");
req.setAttribute("taskName", "Custom Process Display Name");
SpmlResponse res = client.request(req);
```

Using helpTool

With the Identity Manager 6.0 release, a new feature has been added that allows you to search the online help and documentation files, which are in HTML format. The search engine is based on the SunLabs “Nova” search engine technology.

There are two stages to using the Nova engine: *indexing* and *retrieval*. During the indexing stage, the input documents are analyzed and an index is created which is used during the retrieval stage. During retrieval, it is possible to pull “passages” that consist of the context in which the query terms were found. The passage retrieval process requires the original HTML files to be present, so these files must exist in a location in the file system accessible by the search engine.

helpTool is a Java program that performs two basic functions:

- Copies the HTML source files into a location known to the search engine
- Creates the index used during the retrieval stage

You execute helpTool from the command line, as follows:

```
$ java -jar helpTool.jar
usage: HelpTool
 -d    Destination directory
 -h    This help information
 -i    Directory or JAR containing input files, no wildcards
 -n    Directory for Nova index
 -o    Output file name
 -p    Indexing properties file
```

Rebuilding/Re-creating the Online Help Index

The HTML files for online help are packaged in a JAR file. You must extract these files to a directory for the search engine. Use the following procedure:

1. Unpack the helpTool distribution to a temporary directory. (Details TBD)

   In this example, we will extract the files to `/tmp/helpTool`.

2. In a UNIX shell or Windows command window, change directory to the location where the Identity Manager application was deployed to your web container.

   For example, a directory for Sun Java System Application Server might look like the following:

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Change your current working directory to the `help/` directory.

Note It is important to run helpTool from this directory or the index will not build correctly. In addition, you should remove the old index files by deleting the contents of the `index/help/` subdirectory.

4. Gather the following information for your command line arguments:

• **Destination directory**:	`html/help/en_US` **Note**: Use the locale string appropriate for your installation.
• **Input files**:	`../WEB-INF/lib/idm.jar`
• **Nova index directory**:	`index/help`
• **Output file name**:	`index_files_help.txt` **Note**: The name of the file is not important – but the tool will exit if this file already exists.
• **Indexing properties file**:	`index/index.properties`

5. Run the following command:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/help/en_US -i ../
WEB-INF/lib/idm.jar -n index/help -o help_files_help.txt -p
index/index.properties
Extracted 475 files.
[15/Dec/2005:13:11:38] PM Init index/help AWord 1085803878
[15/Dec/2005:13:11:38] PM Making meta file: index/help/MF: 0
[15/Dec/2005:13:11:38] PM Created active file: index/help/AL
[15/Dec/2005:13:11:40] MP Partition: 1, 475 documents, 5496 terms.
[15/Dec/2005:13:11:40] MP Finished dumping: 1 index/help 0.266
[15/Dec/2005:13:11:40] IS 475 documents, 6.56 MB, 2.11 s, 11166.66
MB/h
[15/Dec/2005:13:11:40] PM Waiting for housekeeper to finish
[15/Dec/2005:13:11:41] PM Shutdown index/help AWord 1085803878
```

Rebuilding/Re-creating the Documentation Index

Use the following procedure to rebuild or re-create the documentation index:

1. Unpack the helpTool distribution to a temporary directory. (Details TBD)

   In this example, we will extract the files to `/tmp/helpTool`.

2. In a UNIX shell or Windows command window, change directory to the location where the Identity Manager application was deployed to your web container.

   For example, a directory for Sun Java System Application Server might look like:

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Change your current working directory to the `help/` directory.

Note You must run helpTool from this directory or the index will not build correctly. In addition you should remove the old index files by deleting the contents of the `index/docs/` subdirectory.

4. Gather the following information for your command line arguments:

• **Destination directory**:	`html/docs`
• **Input files**:	`../doc/HTML/en_US` **Note**: The tool will copy the `en_US/` directory and subdirectories to the destination.
• **Nova index directory**:	`index/docs`
• **Output file name**:	`index_files_docs.txt` **Note**: The name of the file is not important – but the tool will exit if this file already exists.
• **Indexing properties file**:	`index/index.properties`

5. Run the following command:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/docs -i
../doc/HTML/en_US -n index/docs -o help_files_docs.txt -p
index/index.properties
Copied 84 files.
Copied 105 files.
Copied 1 files.
Copied 15 files.
Copied 1 files.
Copied 58 files.
Copied 134 files.
Copied 156 files.
Copied 116 files.
Copied 136 files.
Copied 21 files.
Copied 37 files.
Copied 1 files.
Copied 13 files.
Copied 2 files.
Copied 19 files.
Copied 20 files.
Copied 52 files.
Copied 3 files.
Copied 14 files.
Copied 3 files.
Copied 3 files.
Copied 608 files.
[15/Dec/2005:13:24:25] PM Init index/docs AWord 1252155067
[15/Dec/2005:13:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:13:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:13:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:13:24:29] MP Finished dumping: 1 index/docs 0.617
```

```
[15/Dec/2005:13:24:29] IS 192 documents, 14.70 MB, 3.81 s, 13900.78
MB/h
[15/Dec/2005:13:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```

Deprecated APIs

This chapter lists all Identity Manager Application Programming Interfaces (APIs) deprecated in Identity Manager 6.0 2005Q4M3 SP1and their replacements (if available). This chapter is divided into the following sections:

- Deprecated Constructors (on page 6-113)
- Deprecated Methods and Fields (on page 6-114)

Deprecated Constructors

The following table lists the deprecated constructors and the replacement constructors, when available.

Deprecated Constructor	Replacement
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	
com.waveset.adapter.DblBufIterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError

Deprecated Constructor	Replacement
com.waveset.exception.IOException	com.waveset.util.IOException
com.waveset.exception.XmlParseException	com.waveset.util.XmlParseException
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManageView
com.waveset.security.authn.LoginInfo	com.waveset.object.LoginInfo
com.waveset.security.authn.SignedString	com.waveset.util.SignedString
com.waveset.security.authn.Subject	com.waveset.object.Subject
com.waveset.security.authz.Permission	com.waveset.object.Permission
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.ITrace	com.sun.idm.logging.Trace

Deprecated Methods and Fields

The tables in this section list all methods and fields that were deprecated in this release. The methods and fields are sorted by class name.

The data in the **Replacement** column may contain the following types of information:

- If the column is blank, then there is no replacement for the deprecated method or field.
- If no class name is listed, then the replacement method or field is defined in the same class as the deprecated method or field.
- If the replacement method or field is defined in a different class as the deprecated method or field, the replacement is listed using Javadoc syntax. For example, the `getBaseContextAttrName()` method in the

com.waveset.adapter.ADSIResourceAdapter class has been deprecated. Its replacement is listed as `com.waveset.adapter.ResourceAdapter#ResourceAdapter()`

where:

- `com.waveset.adapter` is the package name.
- `ResourceAdapter` is the class name.
- `ResourceAdapter()` is the method and argument list.

com.waveset.adapter.AccessManagerResourceAdapter

Deprecated Method	Replacement
handlePDException(Exception)	handlePDException(PDException)

com.waveset.adapter.ACF2ResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ActiveSync

Deprecated Field	Replacement
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Deprecated Method	Replacement
getLogFileFullPath()	

com.waveset.adapter.ADSIResourceAdapter

Deprecated Method or Field	Replacement
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.AgentResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.AIXResourceAdapter.BlockAcctIter

Deprecated Method	Replacement
BlockAcctIter(AIXResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.AuthSSOResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

Deprecated Field	Replacement
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.DB2ResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.DominoResourceAdapter

Deprecated Method or Field	Replacement
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.DominoResourceAdapterBase

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

Deprecated Method	Replacement
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)

com.waveset.adapter.HostConnPool

Deprecated Method	Replacement
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	

com.waveset.adapter.iapi.IAPIFactory

Deprecated Method	Replacement
getIAPIProcess(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIProcess(Element)	
getIAPIUser(Element)	
getIAPIUser(Map,Map,String,Map)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIUser(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)

com.waveset.adapter.IDMResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

Deprecated Method or Field	Replacement
addUserToGroup(LDAPObject,String,String)	addUserToGroup(String,String,String)
buildBaseUrl()	
buildBaseUrl(String)	

Deprecated Method or Field	Replacement
buildEvent(UpdateRow)	
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
getGroups(Name,String,Vector,Vector)	getGroups(String,String,Vector,Vector)
getLDAPAttributes(String,DirContext[],String)	getLDAPAttributes(String,DirContext,String,String[])
getLDAPAttributes(String,DirContext[])	getLDAPAttributes(String,DirContext,String,String[])
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
removeNameFromAttribute(DirContext,Name,Attribute)	removeNameFromAttribute(DirContext,String,boolean,Attribute)
removeUserFromAllGroups(Name,String,WavesetResult)	removeUserFromAllGroups(String, boolean,String,WavesetResult)
removeUserFromGroup(DirContext,Name,String,String,Attributes)	removeUserFromGroup(DirContext, String,boolean,String,String,Attributes)
removeUserFromGroups(Name,Vector,String, WavesetResult)	removeUserFromGroups(String, boolean,Vector,String,WavesetResult)

com.waveset.adapter.MySQLResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.NaturalResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

Deprecated Method	Replacement
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter

Deprecated Method or Field	Replacement
DEFAULT_AUDIT_STAMP_FORMAT	
DEFAULT_AUDIT_STAMP_START_DATE	
getAccountAttributes(String)	
getUpdateRows(UpdateRow)	getUpdateRows(UpdateRow)
RA_AUDIT_STAMP_FORMAT	

com.waveset.adapter.RACFResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

Deprecated Method	Replacement
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

com.waveset.adapter.RedHatLinuxResourceAdapter.BlockAcctIter

Deprecated Method	Replacement
BlockAcctIter(int,CaptureList)	BlockAcctIter(SVIDResourceAdapter,CaptureList)

com.waveset.adapter.RequestResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceAdapterBase

Deprecated Method	Replacement
getAccountAttributes(String)	
getAdapter(Resource,LighthouseContext)	getAdapterProxy(Resource,LighthouseContext)
getAdapter(Resource,ObjectCache,WSUser)	getAdapterProxy(Resource,ObjectCache)
getAdapter(Resource,ObjectCache)	getAdapterProxy(Resource,LighthouseContext)
getBaseContextAttrName()	getBaseContexts()
isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)
isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy #isExcludedAccount(String, Map,ResourceOperation,Rule)

com.waveset.adapter.ResourceAdapterProxy

Deprecated Method	Replacement
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceManager

Deprecated Method	Replacement

getResourceTypes()	getResourcePrototypes()
	getResourcePrototypes(ObjectCache,boolean)

getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

Deprecated Field	Replacement
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.SAPResourceAdapter

Deprecated Method	Replacement
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

Subclass	Deprecated Method	Replacement
Script	hasNextToken()	
Script	nextToken()	
ScriptedConnection	disConnect()	com.waveset.adapter.ResourceConnection #disconnect()
ScriptedConnection Factory	getScriptedConnection(String,HashMap)	com.waveset.adapter.ScriptedConnectionPool#getConnection(HashMap,String,long,boolean)
SSHConnection	disConnect()	disconnect()
TelnetConnection	disConnect()	disconnect()

com.waveset.adapter.ScriptedHostResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter

Deprecated Method or Field	Replacement
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(SVIDResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.SybaseResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Deprecated Method	Replacement
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)

com.waveset.adapter.VerityResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Deprecated Method	Replacement
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

Deprecated Method	Replacement
getMessage(String,Object[],Locale)	format (Locale,String,Object[])
getMessage(Locale,String,Object[])	format (Locale,String,Object[])
getMessage(Locale,String)	format (Locale,String)
getMessage(String,Locale)	format (Locale,String)
getMessage(String,Object[])	format (Locale,String,Object[])

com.waveset.object.Account

Deprecated Method	Replacement
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

com.waveset.object.AccountAttributeType

Deprecated Method	Replacement
getAttrType()	getSyntax()

setAttrType(String)	setSyntax(String)
	setSyntax(Syntax)

com.waveset.object.Attribute

Deprecated Method or Field	Replacement
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	
STARTUP_TYPE_AUTO	com.waveset.object.Resource#STARTUP_TYPE_AUTO
STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource#STARTUP_TYPE_AUTO_FAILOVER
STARTUP_TYPE_DISABLED	com.waveset.object.Resource#STARTUP_TYPE_DISABLED
STARTUP_TYPE_MANUAL	com.waveset.object.Resource#STARTUP_TYPE_MANUAL
STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource#STARTUP_TYPES_DISPLAY_NAMES

com.waveset.object.AttributeDefinition

Deprecated Method	Replacement
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

com.waveset.object.AuditEvent

Deprecated Method	Replacement
setAttributeMap(Map)	setAuditableAttributes(Map)
addAuditableAttributes(AccountAttributeType[ ],WSAttributes)	setAuditableAttributes(Map)
getAttributeMap()	getAuditableAttributes()
getAttributeValue(String)	getAuditableAttributes()
setAccountAttributesBlob(Map)	setAccountAttributesBlob(Map,Map)
setAccountAttributesBlob(WSAttributes,List)	setAccountAttributesBlob(WSAttributes,WSAttributes,List)

com.waveset.object.CacheManager

Deprecated Method	Replacement
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

com.waveset.object.Constants

Deprecated Field	Replacement
MAX_SUMMARY_STRING_LENGTH	

com.waveset.object.EmailTemplate

Deprecated Method or Field	Replacement
setToAddress(String)	setTo(String)
getFromAddress()	getFrom()
getToAddress()	getTo()
setFromAddress(String)	setFrom(String)
VAR_FROM_ADDRESS	VAR_FROM
VAR_TO_ADDRESS	VAR_TO

com.waveset.object.Form

Deprecated Method or Field	Replacement
EL_HELP	com.waveset.object.GenericObject#toMap(int)
getDefaultDataType()	getDefaultSyntax()
getType()	getSyntax()
setType(String)	setSyntax(Syntax)

com.waveset.object.GenericObject

Deprecated Method	Replacement
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

com.waveset.object.LoginConfig

Deprecated Method	Replacement
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

Deprecated Method	Replacement
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayName(LighthouseContext,String)

com.waveset.object.RepositoryResult

Deprecated Method	Replacement
get(int)	next()
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	

seek(int)	hasNext()
	next()

sort()	

com.waveset.object.RepositoryResult.Row

Deprecated Method	Replacement
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Deprecated Method	Replacement
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Deprecated Field	Replacement
DATE_FORMAT	com.waveset.util.Util#stringToDate(String,String) com.waveset.util.Util#getCanonicalDate(Date) com.waveset.util.Util#getCanonicalDate(Date,TimeZone) com.waveset.util.Util#getCanonicalDate(long)

VAR_RESULT_LIMIT	setResultLimit(int)
	getResultLimit()

VAR_TASK_STATUS	

com.waveset.object.TaskTemplate

Deprecated Method	Replacement
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

com.waveset.object.Type

Deprecated Method or Field	Replacement
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	
REPORT_COUNTER	
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

com.waveset.object.UserUIConfig

Deprecated Method	Replacement
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	

Deprecated Method	Replacement
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.ViewMaster

Deprecated Method	Replacement
ViewMaster()	ViewMaster(LighthouseContext)
ViewMaster(String,String)	ViewMaster(LighthouseContext)
ViewMaster(Subject,String)	ViewMaster(LighthouseContext)

com.waveset.session

Subclass	Deprecated Method or Field	Replacement
Session	listApprovers()	getAdministrators(Map)
	listControlledApprovers()	getAdministrators(Map)
	listSimilarApprovers(String adminName)	getAdministrators(Map)
SessionFactory	getApp(String)	getLoginApp(String)
	getApps()	getLoginApps()
WorkflowServices	ARG_TASK_DATE	com.waveset.object.Attribute#DATE

com.waveset.task.TaskContext

Deprecated Method	Replacement
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Deprecated Method	Replacement
getAdministrators(Session,List)	getUsers(LighthouseContext,Map)
getAdministrators(Session,Map)	getUsers(LighthouseContext,Map)
getApplications(LighthouseContext,List)	getApplications(LighthouseContext,Map)
getApplications(LighthouseContext)	getApplications(LighthouseContext,Map)
getApproverNames(Session,List)	getUsers(LighthouseContext,Map)
getApproverNames(Session)	getUsers(LighthouseContext,Map)
getApprovers(Session,List)	getUsers(LighthouseContext,Map)
getApprovers(Session)	getUsers(LighthouseContext,Map)
getCapabilities(LighthouseContext,List,Map)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,List)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String, String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List)	getObjectNames(LighthouseContext,String,Map)

Deprecated Method	Replacement
getObjectNames(LighthouseContext,Type,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getOrganizations(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getSimilarApproverNames(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApproverNames(Session)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session)	getUsers(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)

Deprecated Method	Replacement
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,Map)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,List,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String)	getUnassignedResources(LighthouseContext,Map)

com.waveset.ui.util.html

Subclass	Deprecated Method or Field	Replacement
Component	isNoWrap()	
	setHelpKey(String)	
	setNoWrap(boolean)	
HtmlHeader	NORMAL_BODY	
MultiSelect	isLockhart()	
	setLockhart(boolean)	
WizardPanel	setPreviousLabel(String)	setPrevLabel(String)

com.waveset.util.JSSE

Deprecated Method	Replacement
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Deprecated Method	Replacement
render(Element,boolean,String,OutputStream)	render(Element,boolean,String,OutputStream ,String,boolean)
render(Element,boolean,String)	render(Element,boolean,String,String,boolean)
render(Report,boolean,String,OutputStream)	render(Report,boolean,String,OutputStream, String,boolean)
render(Report,boolean,String)	render(String,boolean,String,String,boolean)

com.waveset.util.Quota

Deprecated Method	Replacement
getQuota()	

com.waveset.util.ReportRenderer

Deprecated Method or Field	Replacement
renderToPdf(Report,boolean,String,OutputStream)	renderToPdf(Report,boolean,String,OutputStream,String,boolean)
renderToPdf(Report,boolean,String)	renderToPdf(Report,boolean,String,String,boolean)

com.waveset.util.Trace

Deprecated Method	Replacement
data(long,Object,String,byte[])	com.sun.idm.logging.trace.Trace#data(long,String,byte[])
entry(long,Object,String,Object[])	com.sun.idm.logging.trace.Trace#entry(long,String,Object[])
entry(long,Object,String,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
entry(long,Object,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
exception(long,Object,String,t)	com.sun.idm.logging.trace.Trace#throwing(long,String,Throwable) com.sun.idm.logging.trace.Trace#caught(long,String,Throwable)
exit(long,Object,String,boolean)	com.sun.idm.logging.trace.Trace#exit(long,String,boolean)
exit(long,Object,String,int)	com.sun.idm.logging.trace.Trace#exit(long,String,int)
exit(long,Object,String,long)	com.sun.idm.logging.trace.Trace#exit(long,String,long)
exit(long,Object,String,Object)	com.sun.idm.logging.trace.Trace#exit(long,String,Object)
exit(long,Object,String)	com.sun.idm.logging.trace.Trace#exit(long,String)
getTrace()	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(Class)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(String)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
level1(Class,String)	com.sun.idm.logging.trace.Trace#level1(String)
level1(Object,String)	com.sun.idm.logging.trace.Trace#level1(String)
level2(Class,String)	com.sun.idm.logging.trace.Trace#level2(String)
level2(Object,String)	com.sun.idm.logging.trace.Trace#level2(String)
level3(Class,String)	com.sun.idm.logging.trace.Trace#level3(String)
level3(Object,String)	com.sun.idm.logging.trace.Trace#level3(String)

Deprecated Method	Replacement
level4(Class,String)	com.sun.idm.logging.trace.Trace#level4(String)
level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)
variable(long,Object,String,String,boolean)	com.sun.idm.logging.trace.Trace#variable(long,String,String,boolean)
variable(long,Object,String,String,int)	com.sun.idm.logging.trace.Trace#variable(long,String,String,int)
variable(long,Object,String,String,long)	com.sun.idm.logging.trace.Trace#variable(long,String,String,long)
variable(long,Object,String,String,Object)	com.sun.idm.logging.trace.Trace#variable(long,String,String,Object)
void info(long,Object,String,String)	com.sun.idm.logging.trace.Trace#info(long,String,String)

com.waveset.util.Util

Deprecated Method or Field	Replacement

DATE_FORMAT_CANONICAL	stringToDate(String,String)
	getCanonicalDate(Date)
	getCanonicalDate(Date,TimeZone)
	getCanonicalDate(long)

debug(Object)	

getCanonicalDateFormat()	stringToDate(String,String)
	getCanonicalDate(Date)
	getCanonicalDate(Date,TimeZone)
	getCanonicalDate(long)

getOldCanonicalDateString(Date,boolean)	getCanonicalDateString(Date)
rfc2396URLPieceEncode(String,String)	com.waveset.util.RFC2396URLPieceEncode #encode(String,String)
rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode #encode(String)

com.waveset.workflow.WorkflowContext

Deprecated Field	Replacement
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED