Sun Java™ System Identity Manager Release Notes

Version 7.1 Update 1 November 2007

Part Number 820-2952-10

These Release Notes contain important information available at the time of release of Sun Java System Identity Manager 7.1 Update 1. New features and enhancements, known issues and limitations, and other information are addressed here. Read this document before you begin using Identity Manager 7.1 Update 1.

These Release Notes are organized into the following sections:

Third-party URLs are referenced in this document and provide additional, related information.

NOTE Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Introduction

This section of the Identity Manager 7.1 Update 1 Release Notes provides information about

- Supported Software and Environments
- Upgrade Paths and End of Service Life
- Redistributable Files
- How to Report Problems and Provide Feedback
- Sun Welcomes Your Comments
- Additional Sun Resources

Supported Software and Environments

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

- Operating Systems
- Application Servers
- Repository Database Servers
- Sun Identity Manager Gateway
- Supported Resources
- Web Servers
- Browsers
- Discontinued Software

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

This release of Identity Manager supports the following operating systems:

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 or higher
- Microsoft Windows 2003
- Solaris 8, 9, 10 Sparc and x86
- 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). Identity Manager requires JDK 1.4.2 or higher.

- Apache® Tomcat
  - Version 4.1.x (with JDK 1.4.2)
  - Version 5.0.x (with JDK 1.4.2)
  - Version 5.5.x (with JDK 1.5)
- BEA WebLogic® Express 8.1 (with JDK 1.4.2 or higher)
- BEA WebLogic® Server™ 8.1 (with JDK 1.4.2 or higher)
- BEA WebLogic® Server™ 9.1, 9.2
- IBM WebSphere® 6.0, 6.1
- IBM WebSphere® Application Server - Express Version 5.1.1 (with JDK 1.4.2)
- JBoss Application Server 4.0.*x*
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8.1, 8.2, 9.*x*

- Sun Java™ System Application Server Enterprise Edition 8.1, 8.2, 9.*x*
- Sun Java™ System Application Server Standard Edition 8.2

NOTE

- If your current application server does not support JDK 1.4.2 or higher, please check with your vendor to examine the implications of upgrading to one that does before installing Identity Manager 7.1
- You can run Identity Manager 7.1 and later on BEA WebLogic application servers with all WebLogic-supported 1.4.2 and 1.5 JVMs.

Repository Database Servers

Identity Manager supports the following repository database servers:

- IBM® DB2® Universal Database for Linux, UNIX®, and Windows® (Version 7.*x*, 8.1, 8.2)
- Microsoft SQL Server™ 2000, 2005
- MySQL™ 4.1, 5.0

NOTE Identity Manager supports MySQL in a development environment only. MySQL is not supported in a production environment.

- Oracle 9i® and Oracle Database 10g, 10g Release 1 and 10g Release 2®

NOTE Oracle RAC (Real Application Cluster) is supported in a two-node active-passive configuration. That is, a configuration where the `active_instance_count` parameter is set to 1. Used in conjunction with connection failover for the JDBC driver, this provides failover capability for the repository. (Refer to Oracle documentation for how to configure this in your environment)

Oracle RAC is not currently supported in any other configuration.

Sun Identity Manager Gateway

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

NOTE The Novell GroupWise adapter is deprecated, and will be discontinued in the next major Identity Manager release. However, the NetWare NDS adapter supports GroupWise accounts, and can be used instead.

Supported Resources

Identity Manager software supports these resources:

- Customer Relationship Management (CRM)
- Databases
- Directories
- Enterprise Resource Planning (ERP)
- Help Desk
- Message Platforms
- Miscellaneous
- Operating Systems
- Role Management System
- Security Managers
- Web Access Control

Customer Relationship Management (CRM)

- Siebel version 6.2, 7.0.4, 7.7, 7.8 CRM software

Databases

- Generic database table
- 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, 2005
- MySQL™ 4.1.*x*, 5.*x*

NOTE The MySQL™ 4.1.*x* database server is deprecated, and will be discontinued in the next major Identity Manager release.

- Oracle Database 9i®, 10g Release 1®, 10g Release 2®
- Sybase Adaptive Server® 12.*x*
- Scripted JDBC (manages resources using JDBC 3.0 drivers or later)

Directories

- LDAP v3
- RACF LDAP
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory 8.7.1, 8.8
- Novell NetWare® 5.1, 6.0, and 6.5
- Open LDAP
- Sun™ ONE Directory Server 4.*x*
- Sun Java™ System Directory Server 5.*x*, 6.*x*

NOTES

- While Identity Manager is tested on Sun Java™ System 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)

- MySAP ERP 2005 (ECC 6.0) Kernel version 7.00
- Oracle E-Business Suite on Oracle Applications 11.5.9, 11.5.10, 12
- Peoplesoft® PeopleTools 8.1 through 8.4.2
- Peoplesoft PeopleTools HRMS 8.0 through 8.8, 9.0
- 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)
- SAP® Governance, Risk, and Compliance (GRC) Access Enforcer 5.2

Help Desk

- BMC Remedy Action Request System Server 6.0, 6.3, and 7.0
- BMC Remedy Service Desk Application 7.0

NOTES Identity Manager 7.1 Update 1 supports Remedy versions 6.3 and 7.0. However, there are many substantial differences between these versions in terms of their sample data, defaults, and out-of-the-box configuration. For example, the name of the "ticket" schema in version 6.3 is *HPD:HelpDesk*, while in 7.0 it has been changed to *HPD:Help Desk*.

Message Platforms

- Blackberry RIM Enterprise Server 4+ (uses generic Windows script adapter)

  NOTE The BlackberryResourceAdapter and BlackBerry Enterprise Server scripts are deprecated and will not be supported in the next major Identity Manager release. Future implementations requiring resource adapters for Blackberry Enterprise Server Version 4+ should be based on the ScriptedGatewayResourceAdapter. The Blackberry Enterprise Server scripts will continue to be shipped with Identity Manager as sample scripts, but customers will be responsible for maintaining these scripts.

- Sun Java System Messaging and Calender Service Java Enterprise System 2005Q1 and later

- Lotus Notes® (Domino) 5.0, 6.5, 7.0
- Microsoft® Exchange 2000, 2003
- Novell® GroupWise 6.0, 6.5, and 7.0 (using the Novell NDS adapter)

NOTE
- Microsoft Exchange 2000 and 2003 are managed through the Microsoft Windows Active Directory 2000 and 2003 resources.
- The Novell GroupWise adapter is deprecated and will be discontinued in the next major Identity Manager release. However, the NetWare NDS adapter supports GroupWise accounts, and can be used instead.

Miscellaneous

- Flat files
- JMS Message Queue Listener (manages any JMS 1.0b or later compliant queue)
- Generic UNIX Shell Script

NOTE The Generic UNIX Shell Script adapter runs scripts in supported shell types on supported UNIX operating systems.

- Generic Windows Script Adapter

NOTE The Generic Windows Script adapter runs scripts in the `cmd` shell on supported Windows operating systems that host the Sun Identity Manager Gateway.

Operating Systems

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L, 5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- 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

NOTE If you manage NIS accounts on Solaris, install patch 126632-01 on the resource to improve the performance of the logins command and the Solaris adapter.

Role Management System

- BridgeStream SmartRoles 2.7

Security Managers

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- eTrust CA-Top Secret® Security 5.3
- IBM RACF®
- INISafe Nexess 1.1.5
- Natural

NOTE The Natural adapter is deprecated, and will be discontinued in the next major Identity Manager release.

- RSA ClearTrust 5.5.2, 5.5.3
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® for UNIX 5.1, 6.0
- Scripted Host

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 (Realms supported as of 2005Q4), 7.1

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

Browsers

Identity Manager supports the following browsers:

- Microsoft Internet Explorer 6.x and later
- Safari 2.0 and later for Mac OS X 10.3.3 and later
- Firefox 1.5 and later (with JRE 1.5)

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.

Software Category	Software Package
Operating Systems	• IBM AIX 4.3.3
Application Servers	• Apache Tomcat 4.1.x
	• BEA Weblogic Express 8.1
	• BEA Weblogic Server 8.1
	• IBM Websphere Application Server - Express Version 5.1.1
	• IBM Websphere 6.0
	• Sun ONE Application Server 7
Repository Database Servers	• MySQL 4.1
	• Microsoft SQL Server 2000
Resources	• ActivCard 5.0
	• Blackberry RIM Enterprise Server 4+ (uses generic Windows script adapter) and Blackberry Enterprise Server scripts
	• Lotus Notes (Domino) 5.0, 6.5, 7.0
	• Microsoft Windows NT 4.0
	• Sun Identity Manager Gateway running on Microsoft Windows NT 4.0
	• MySQL 4.1
	• Natural
	• Novell® GroupWise 5.x, 6.0, 6.5
	• Novell® eDirectory on Novell NetWare 5.1, 6.0
	• Oracle 8*i* (through the Oracle resource adapter)
	• Red Hat Linux 8.0
	• Remedy® Help Desk 4.5, 5.0.
	• SAP R/3 v4.5, v4.6
	• Siebel 6.2
	• Sun ONE Identity Server 6.0

The following dependent software will no longer be supported in Identity Manager 7.1 or 7.1 Update 1:

Software Category	Software Package
Repository Database Servers	• Oracle 8*i* • IBM DB2 Universal Database for Linux, UNIX, and Windows 7.0
Operating Systems	• Solaris 7, Microsoft Windows NT 4.0
Resources	• Microsoft Exchange 5.5 • IBM DB2 7.0 • Novell® GroupWise 5.x

API Support

The Identity Manager 7.1 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
Report	com.waveset.report.BaseReportTask

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.*
	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 you will be required to migrate to a supported class.

Deprecated APIs

The "Deprecated APIs" section in these Release Notes lists all Identity Manager Application Programming Interfaces (APIs) deprecated in this release and their replacements (if available).

Upgrade Paths and End of Service Life

This section provides information about the upgrade paths you should follow when upgrading Identity Manager, and describes Identity Manager's End of Service Life (EOSL) policy for the products software support.

Identity Manager Upgrade Paths

Use the following to determine the upgrade path you must follow when upgrading to a newer version of Identity Manager.

Current Identity Manager Version	Target Version					
	5.0	**2005Q3M1**	**2005Q4M3**	**7.0**	**7.1**	**7.1 Update 1**
Waveset Lighthouse 4.1 SP*x*	5.0	5.0 > 2005Q3M1	5.0 > 2005Q4M3	5.0 > 2005Q4M3 > 7.0	5.0 > 2005Q4M3> 7.0 > 7.1	7.1 Update 1
Identity Manager 5.0 SP*x*		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	7.1 Update 1
Identity Manager 2005Q1M3 Identity Auditor 1.0		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	7.1 Update 1
Identity Manager 2005Q3M1 Identity Manager 5.5			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	7.1 Update 1
Identity Manager 2005Q3M3 Identity Manager SPE 1.0			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1	7.1 Update 1
Identity Manager 2005Q4M3 (6.0)				7.0	7.1	7.1 Update 1
Identity Manager 7.0					7.1	7.1 Update 1
Identity Manager 7.1						7.1 Update 1

NOTE

- When upgrading Identity Manager, you do not have to install Updates (*formerly called Service Packs or SPs*) within a major release to upgrade to the next major release. For example, when upgrading from Identity Manager 5.0 to 6.0, you do not have to install any of the 5.0 Service Packs.
- Updates for a major release are cumulative. After upgrading to the major release, you can install the latest Update without having to install all of the Updates (or Service Packs) for that release. For example, if you upgraded to Identity Manager 5.0, installing SP6 gives you all of the functionality provided in SP1 through SP5.

Updates to the Identity Manager documentation are provided as follows:

- **For Every release** (including Service Packs): Release Notes are provided to describe bug fixes, product enhancements, new functionality, and other important information.
- **For Major releases** (*x*.0): The complete Identity Manager documentation set is updated and republished.
- **For Minor releases and updates**: Individual publications are updated and republished or Documentation Addendum are provided.

End of Service Life for Software Support

During the End of Service Life (EOSL) period, Identity Manager software support is offered in two phases:

- *Phase 1: Full Support*
- *Phase 2: Limited Support*

NOTE The length of the Full Support Phase varies by product.

Full Support Phase

During the Full Support Phase, Sun Microsystems, Inc. provides software 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, when a software product's EOL date is announced, customers will no longer have access to software updates and upgrades for that software product.

Limited Support Phase

During the Limited Support Phase, Sun Microsystems, Inc. provides software 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 are not entitled to submit bugs or to receive new patches from Sun Microsystems, Inc. As with Full Support Phase, when a software product's EOL date is announced, customers will no longer have access to software updates and upgrades for that software product.

The following table provides information about the EOSL and EOL dates for older versions of Identity Manager.

Product Name	Product Status	Last Ship Date	Phase 1 End Date	Phase 2 End Date (EOSL)	EOL Announcement
Sun Java System Identity Manager 7.0	Post-RR				
Sun Java System Identity Manager 6.0 2005Q4	Post-RR	05/25/2007	05/25/2008	05/2012	11/20/06
Sun Java System Identity Auditor 1.0 2005Q1	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager Service Provider Edition 1.0 2005Q3	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager 5.0 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.0 SP*x* 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.5	EOL	08/11/2006	08/2007	08/2011	02/07/06
Waveset Lighthouse 4.1			03/2006	03/2010	

Redistributable Files

Sun Java System Identity Manager 7.1 Update 1 does not contain any files that you can redistribute.

How to Report Problems and Provide Feedback

If you have problems with Sun Java System Identity Manager, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
  http://www.sun.com/service/sunone/software

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to http://docs.sun.com and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is Sun Java System Identity Manager November 2007 Release Notes, and the part number is 820-2952-10.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Documentation for Sun Java™ System Identity Manager
  http://docs.sun.com/app/docs/prod/ident.mgr#hic
- Sun Java System Documentation
  http://docs.sun.com/prod/java.sys
- Sun Java System Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Java System Software Products and Service
  http://www.sun.com/software
- Sun Java System Software Support Services
  http://www.sun.com/service/sunone/software
- Sun Java System Support and Knowledge Base
  http://www.sun.com/service/support/software
- Sun Support and Training Services
  http://training.sun.com
- Sun Java System Consulting and Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Java System Developer Information
  http://developers.sun.com
- Sun Developer Support Services
  http://www.sun.com/developers/support
- Sun Java System Software Training
  http://www.sun.com/software/training
- Sun Software Data Sheets
  http://wwws.sun.com/software

Identity Manager 7.1 Update 1 Features

This section of the Identity Manager 7.1 Update 1 Release Notes provides information about

- What's New in This Release
- Bugs Fixed in This Release
- Known Issues

What's New in This Release

This section provides additional information about the new features provided in Identity Manager 7.1, and the information is organized into the following sections:

- Administrator and User Interfaces
- Auditing
- Identity Manager Integrated Development Environment (IDE)
- Password Synchronization
- Resources
- Security

Administrator and User Interfaces

- Identity Manager's User Extended Attributes now fully supports multi-valued attributes. (ID-14863)

NOTE An attribute condition that refers to a multi-valued extended attribute will evaluate correctly for a user object *only* after that user object has been re-serialized. If you want such an attribute condition to evaluate correctly for all user objects, then you must re-serialize all user objects.

Instructions for re-serializing users are provided "Upgrade Issues" on page 47.

- A Return to Main Menu button was added to the Launch Requests form to take users back to the Identity Manager Home page. (ID-15957)

  The Launch Requests form (EndUserRequestMenu) is preserved during an upgrade, so you must manually add this button to the End User interface by referring to the default `UserForm` object in `sample/enduser.xml`.

- Identity Manager supports the Microsoft Internet Explorer 7 browser. (ID-16708)

- When upgrading from previous Identity Manager versions to version 7.1 Update 1, the Forgot Your User ID? feature on the Log In to Identity Manager page is disabled by default. (ID-16715)

  To enable this feature so users can retrieve forgotten user IDs, you must modify the following attributes in the System Configuration object:

  ```
  ui.web.user.disableForgotUserId = false

  ui.web.admin.disableForgotUserId = false
  ```

- Call timer and tracing functions are now related, and Call Timing statistics can only be collected when tracing is enabled. This change affects the Identity Manager Debug pages. For more information see "Identity Manager Tuning, Troubleshooting, and Error Messages" on page 178 in *Documentation Additions and Corrections*. (ID-17106)

Auditing

- Audit records for role creation now provide additional information about the role (such as assigned resources, sub roles, super roles, and role attributes) in the Change section of the Audit report. (ID-16327)

Identity Manager Integrated Development Environment (IDE)

- You can use the new Identity Manager Profiler to troubleshoot performance problems in forms, Java, rules, workflows, and XPRESS. (ID-14311)

  For more information about this new tool, see "Identity Manager Tuning, Troubleshooting, and Error Messages" on page 178.

- The Netbeans embedded application server now automatically shuts down whenever you perform any of the following project operations (ID-16738):
  - Clean Project
  - Create Delta Distribution
  - Create Jar
  - Debug Project
  - Manage Embedded Repository
  - Profile Project
  - Run Project
- Identity Manager IDE's Manage Embedded Repository feature can now import your customizations as well as default `init.xml` as long as you select the Initialize Repository or Automatically publish IDM objects repository settings. (ID-16749)
- The following changes have been made to the CBE shipped with Identity Manager (ID-16812):
  - Performance enhancements include:
    - Incremental XML validation (Identity Manager only validates files that have changed since the last build)
    - Incremental pattern substitution and copying (Identity Manager only applies pattern substitutions and copies files that have changed since the last build).
    - The Build Project action no longer creates a WAR in it's warred form. There is now a separate Create IDM War action that builds the WAR.
  - Target names in `build.xml` have been simplified and are now consistent with the project actions. For more information, refer to "Ant Targets" in the "Core CBE (Configuration Build Environment)" section of the `README.txt` provided.
  - You can now safely run ant targets by right-clicking `build-netbeans.xml`.
  - JSP validation has been cleaned up, and the "Setup JSP Validation" section of the `README.txt` describes best practices for enabling JSP validation.
  - Documentation improvements include, an improved overview of the CBE in the `README.txt` and more inline comments in `build.xml` and `build-netbeans.xml`.
  - A single `CLASSPATH` variable in `build.xml` now controls the `CLASSPATH` for both the purposes of building and for auto-completion in the JSP and Java editors. For more information, see the new "How to Add a New JAR Dependency" section provided in the `README.txt`.

- In the `build-config.properties` file, `install.includes` has been replaced by `install.pattern.substitution.excludes` and `install.excludes`.
- The ant property names were changed, and they now use the standard "." ant convention instead of "-". In addition, `lighthouse*` property names were changed to `idm*`.
- XML validation is now run both before and after pattern substitutions are applied.
- For Identity Manager 7.1 Update 1, it was necessary to change the following files in the Identity Manager project:
  - `build.xml nbproject/project.xml`
  - `build-netbeans.xml`
  - `custom-init.incremental.xml`
  - `build-config.properties`
  - `custom-init-common.xml`
  - `custom-init-full.xml`

  If you have modified any of these files, you must manually merge the changes. See "Upgrading Version 7.1 Projects to Version 7.1 Update 1" on page 144 for more information.

NOTE The `build.xml`, `build-netbeans.xml`, and `nbproject/project.xml` files are subject to change from release to release — you should avoid changing theses files if at all possible.

Password Synchronization

- PasswordSync uses a newly created servlet to provide support for 64-bit Windows. This servlet goes in to the `web.xml` file and should be configured as follows (ID-15660):

```
<servlet>
    <servlet-name>PasswordSync</servlet-name>
    <servlet-class>com.waveset.rpc.PasswordSyncServlet</servlet-class>
    <init-param>
     <param-name>parameter</param-name>
     <param-value>value</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
  </servlet>

  <servlet-mapping>
    <servlet-name>PasswordSync</servlet-name>
    <url-pattern>/servlet/PasswordSync</url-pattern>
  </servlet-mapping>
```

Resources

New Resource Versions

The following new resource versions have been added this release:

- The Identity Manager NDSResourceAdapter now supports NetWare 6.5 with eDirectory 8.8. (ID-10612)
- The Identity Manager MySAP adapter now supports MySAP ERP 2005 (ECC 6.0) Kernel version 7.00 on SAP. (ID-15205)
- Identity Manager now supports Sun Access Manager 7.1. (ID-16365)
- Identity Manager now supports SAP GRC Access Enforcer 5.2. (ID-16642)

Resource Adapter Updates

- MySQL resource adapter now supports account iteration. The adapter discards duplicate usernames and skips null usernames. (ID-6204)
- The RACF adapter now allows you to control dataset rules directly, rather than have Identity Manager administer them. This feature enables you to create dataset rules different from the rules that are native to Identity Manager. (ID-10446)

  The following example after create rule creates a dataset rule of *user id*`.test1.**`, rather than the Identity Manager default of *user id*`.**`.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE ResourceAction PUBLIC 'waveset.dtd' 'waveset.dtd'>
<ResourceAction name='create after action'>
   <ResTypeAction restype='RACF'>
      <act>
         var TSO_PROMPT = " READY";
         var TSO_MORE = " ***";
         var cmd1 = "addsd '"+identity+".test1.**' owner('"+identity+"')[enter]";
         var result1 = hostAccess.doCmd(cmd1, TSO_PROMPT, TSO_MORE);
      </act>
   </ResTypeAction>
</ResourceAction>
```

  The new "`use Datasets`" flag controls whether Identity Manager administers dataset rules itself (`"use Datasets" = true`) or defers control strictly to `before` and `after` actions.
- The resource used for the Service Provider master repository can now have multiple variables in the identity template. (ID-14290)
- You can now configure the Database Table adapter to skip past rows that failed during Active Sync processing so that the next poll will not repeatedly process failed rows. (ID-15147)
- The RACF LDAP resource adapter now supports pass-through authentication. (ID-15251)
- The Access Enforcer Resource adapter now supports the change password feature. (ID-15403)

  A new Resource Attribute (`Use IDM Password on Create`) has been added to configure the behavior for a `create` operation. Access Enforcer generates a password for the create operation and sends an email containing the generated password to the newly created user. You cannot prevent this email from being sent, but if you want Identity Manager to set the password to the one sent to the adapter, set this attribute to **`true`** and Identity Manager will set the password to the desired value.

In addition, the following attributes are available from the SAP Resource adapter:

- `Use SAP Temporary Passwords`
- `Return SAP Temporary Passwords on Failure`

- The SAP Adapter now supports the Rename feature. For more information, see "Renaming Accounts" on page 104 in *Documentation Additions and Corrections*. (ID-15582)
- The `rethrowAllSQLExceptions` parameter has been added to the Database Table adapter. (ID-16419)
  - If you select this option, exceptions with **`0`** ErrorCodes result.
  - If you do not select this option, SQL statements that cause SQLExceptions with a **`0`** ErrorCode will catch and suppress the exception.
- The Oracle ERP adapter now has an `npw_number` account attribute to support contingent workers. The `npw_number` account attribute functions in the same manner as `employee_number`, but the `employee_number` attribute and `npw_number` attribute are mutually exclusive. If both are entered on create, `employee_number` takes precedence. (ID-16507)
- Support for accessing Remedy servers has changed. The Sun Identity Manager Gateway no longer depends on version 4.5 of the Remedy API libraries. Now, you must put Remedy libraries in the Gateway directory (the Remedy libraries are located on the Remedy server). For more information, see "Remedy" on page 104 in *Documentation Additions and Corrections*. (ID-16551)
- It is now possible to specify the domain for an Active Directory resource in the resource authentication properties. This makes it possible to limit a login module to authenticate against just one domain. In a multi-domain AD environment, this prevents accounts from being locked out due to failed login attempts. (ID-16603) To implement this feature, add the following authentication property in the resource XML within the `<AuthnProperties>` element:

  ```
  <AuthnProperty name='w2k_domain' dataSource='resource attribute' value='MyDomainName'/>
  ```

- Identity Manager can now use the Attachmate Adapter for Sun Java System Identity Manager product to connect to mainframe resources. (ID-16631)
- The `checkIfUserExists` method now takes a `JCO.Client` argument, which gives you the option of creating a new connection or using an existing one. A new connection is necessary in cases where this method is not the first method performed on the connection. The use of an existing connection is still provided for backward compatibility. In the current version, only the rename operation uses this new functionality. (ID-16902)

Security

- Identity Manager now provides a new, built-in ObjectGroup/organization called *End User* that, initially, has no member objects. The End User ObjectGroup/organization enables users to view several types of objects, including tasks, rules, roles, and resources. This ObjectGroup/organization is implicitly assigned to all users. For more information, see "Chapter 5, Administration" in *Documentation Additions and Corrections*. (ID-14630)
- When defining an AdminRole, you can now select an Exclude All Controlled Child Organizations and Contained Objects checkbox to exclude all controlled child organizations and their contained objects from the user's scope of control. Clear this checkbox to grant the user assigned the AdminRole the associated Capabilities on all child organizations and their contents. (16859)
- The Text display component can now render `autocomplete="off"` on input fields where the `autocomplete` attribute of the `display` property has been set to **`off`**. Specifying `autocomplete="off"` prevents browsers from offering to store the user's credentials on their computer. (ID-17045)

  You can make this customization in XPRESS by adding the display property. Using a value other than **`off`** prevents the `autocomplete` attribute from being rendered (which is the same as not setting the property).

  To enable this feature for the Identity Manager `login.jsp`, `continueLogin.jsp`, `user/login.jsp`, and `user/continueLogin.jsp` login pages, change the `ui.web.disableAutocomplete` system configuration object to **`true`**.

  Other Identity Manager login forms are generated from XPRESS, so you must modify the following forms (located in the `sample` directory) to use the new display property:

  - Anonymous User Login
  - Question Login Form
  - End User Anonymous Enrollment Validation Form
  - End User Anonymous Enrollment Completion Form
  - Lookup Userid

  The `display` property has been added to the preceding forms, but the property is commented out by default.

NOTE According to the support article provided at the following location,

`http://support.microsoft.com/default.aspx?scid=kb;en-us;329156`

`AutoComplete` does not work in Internet Explorer if you use JavaScript to submit the form.

Bugs Fixed in This Release

This section describe the bugs fixed in Identity Manager 7.1 Update 1, and the information is organized as follows:

Administrator and User Interfaces

- Clicking Edit on the User Results page before specifying a user to edit no longer causes a 404 File Not Found error. Now an error message appears, indicating you must select a user. (ID-10944)
- The View Dashboards page now displays the Dashboard Summary column in localized text. (ID-11544)
- The confirmation forms that display when you perform actions on multiple users or on organizations from the Accounts list or Find Users results can now be fully localized. (ID-12248)

- The Summary column on the Run Reports page now displays correctly localized text. (ID-12393)
- The Resource List Group view on the Resource tab now displays the Resource Group list in the order that it was saved instead of sorting the list. (ID-14117)
- The synchronization mechanism for the legacy `role` and current `roles` attribute can now clear the legacy `role` attribute when roles are removed. (ID-14568)
- When you unassign resource accounts from a user using the Edit User functionality, the accounts' SITUATION in the account index are now properly updated in all cases. (ID-15310)
- Clicking a form's Refresh button (not the browser page Refresh) after changing a user's role assignments no longer generates approvals for roles that have already been approved. (ID-15500)
- The JavaScript functions used by the Selector display component no longer cause errors in Internet Explorer. (ID-15540)
- Dashboard graph names are now consistently localized on the Dashboard Edit page. (ID-16008)
- Identity Manager now properly updates sub/super roles during a SaveAs action. (ID-16010)
- Combining the Users Organization search option with other search options no longer causes an empty find users result. (ID-16076)
- The session is now correctly set during expansions and derivation while processing resource account creations in bulk action. (ID-16181)
- If a delegate is deleted, then any work items (such as approvals) that were supposed to be delegated are now assigned to the next person up the path of existing delegators. In addition, Identity Manager records the event in the System Log. (ID-16417)
- When creating or editing a user, Administrators can now assign a manager who is outside the Administrator's scope of control. (ID-16452)
- Identity Manager now properly sorts Extended User Attributes in the User Account treetable. (ID-16488)
- Performance related to the caching of organizations has been improved. You should see improved concurrency for processes that access organization data, such as user creation and editing. (ID-16543)
- When delegating future work items to users, the list of users to whom you can delegate will consist of users who are in scope for the user whom delegation is being defined; regardless of whether they are defined by the user or by an administrator on their behalf. (ID-16561)

- You can now edit and save current or previous workItem delegations. (ID-16564)
- When delegating future work items for a user, if the user does not have an Identity Manager manager or cannot access any other users or `DelegateWorkItemsRules`, that user is no longer allowed to create new delegations, edit existing delegations, or edit previous delegations. (ID-16566)
- TaskDefinitions containing `ManualActions` will now run correctly from the End User interface. (ID-16694)
- You can now use the Dynamic Tabbed User Form to assign multiple resource accounts. (ID-16711)
- Server tasks are now sorted by start time. (ID-16783)
- During a Search action, the `RuleDrivenMembersCache` now returns a unique list of `ObjectGroupRefs` so the same user cannot be returned multiple times for the same organization. (ID-16795)
- The Status column no longer displays on Results pages when the status column is not populated with data. (ID-16889)
- Opening a field-level help (iHelp) window in WebKit-based browsers (such as Safari in Mac OS X) no longer yields an empty (blank) window. (ID-16927)
- A null pointer exception no longer occurs when users try to change their own passwords through the End User interface. (ID-16942)
- Using `continueLogin.jsp` from the Administrator interface no longer causes JavaScript errors. (ID-16989)
- Administrators with improper permissions can no longer delete objects from the debug pages. (16991)
- The `continueLogin.jsp` page now contains a Forgot User ID? button. (ID-16992)
- You can now clear the DatePicker field type value on forms. To clear this field, all three parts of the multi-field property (day, month and year) must be empty. (ID-17022)
- A cross-site scripting vulnerability was identified and fixed in the following pages (ID-17241):
  - task/taskLaunch.jsp
  - user/processLaunch.jsp
  - user/requestLaunch.jsp

Auditing

- Now, when you launch a periodic access review and then go to the Access Reviews page, you no longer have to manually refresh the page to see your scan displayed in the list. (D-14169, 16570)
- The Identity Manager Compliance features provide tasks, policies, and rules that you can use as is. (ID-16127, 16571)

  Identity Manager initially creates these objects in either the Top or All object groups as appropriate. For deployments that use delegated administration with administrators that do not control the Top object group, you may want to add some or all Auditor objects to other object groups. Identity Manager provides a script that lists and adds or removes object groups from the Auditor objects. (For a complete list of Auditor objects, see `$WSHOME/sample/scripts/AuditorObjects.txt`.)

  NOTE In the following scripts, the expected form of *idm-url* is [*http://*]*hostname*:*port*[*/idm/servlet/rpcrouter2*], where at least *hostname*:*port* are required. You can omit the Identity Manager server if it is bound to the default URL path.

  - To list objects:

    ```
    cd $WSHOME/sample/scripts
    beanshell.sh objectGroupUpdate.bsh -u Configurator -p Configurator's password -h
    idm-url -action list -data AuditorObjects.txt
    ```

  - To add the 'All' object group to all objects:

    ```
    cd $WSHOME/sample/scripts
    beanshell.sh objectGroupUpdate.bsh -u Configurator -p Configurator's password -h
    idm-url -action add -data AuditorObjects.txt -groups
    ```

  - To remove the 'All' object group from all objects:

    ```
    cd $WSHOME/sample/scripts beanshell.sh objectGroupUpdate.bsh -u
    Configurator -p Configurator's password -h idm-url -action remove -data
    AuditorObjects.txt -groups All
    ```

  NOTE You can use object groups Top and All with their friendly names, but almost all other object groups require you to use the object group ID with this utility.

- Continuous compliance is now enforced on all subtabs on the User Edit page. (ID-16934)
- When you end a delegation in the user interface and then run an Audit Log report, the changes are now captured in the audit report. (ID-17103)

Installation and Upgrade

- For an example of how to create the required database structure on SQL Server 2005 SP2, refer to the comments provided in the sample database creation script (`sample/create_waveset_tables.sqlserver`). (ID-17021)

Identity Manager Integrated Development Environment (IDE)

- You can now test rules in a rule library by selecting the rule node in tree view or by right-clicking within the `<Form>/<Rule>` element in the XML. (ID-14093, 14842)

  NOTE You can use the rule tester to edit and test a rule library, but navigation and property support for rule libraries is not currently implemented.

- Locked objects can now be unlocked when you check in or close a view. (ID-14797, 16573)

  Now, when you check in a view, the view becomes read-only. You can then right-click Repository > Checkout View and select Unlock View from the pop-up menu to check out and make the view writable again. Also, when you close the view window, the view is implicitly unlocked.

  For 7.0 compatibility, you must remove `com.waveset.rpc.SimpleRpcHandler` from `web.xml` to prevent the unlocking problem. Now, when you are setting up a full-featured project, Identity Manager IDE automatically checks the `web.xml` and asks if you want `com.waveset.rpc.SimpleRpcHandler` removed.

- The Identity Manager IDE Debugger's Attach dialog has been fixed and it now works in Netbeans 5.5.1. (ID-16731)

Password Synchronization

- The Password Synchronization `dll` now shows the correct error messages for connection failures instead of the `There was a soap client error: -2147467259` message. This change also fixes possible handle leaks during connection failures. (ID-15451)
- Computer object changes in Active Directory no longer cause a handle leak in the PasswordSync `dll`. (ID-16495)
- Booting the AD domain controller in `Directory Service Restore` mode with Password Synchronization installed no longer causes a continuous reboot cycle if Password Synchronization crashes. (ID-16695)
- If you use JMS to synchronize a Windows Active Directory user password for a user who does not exist in Identity Manager, an appropriate message will be logged in the trace. (ID-16920)

Reconciliation

- Losing the `Start Reconcile` TaskEvent no longer causes the Reconciler to become stuck in a Pending state. (ID-14555)

Reports

- You can now select a resource name for the y-axis of a usage report, and the value will be used in the query. (ID-12035)
- Changes to user's authentication questions are now logged in the audit logs. (ID-13082)
- Identity Manager logs an error when it deletes a non-existent user and now create an audit event for reporting. (ID-13284)

NOTE	In versions 6.0 SP4 and later, the delete event is recorded in the system logs instead of the audit log report.

- HTML `<b></b>` tags are now removed from the following PDF reports (ID-15408):
  - All Admin Roles
  - All Administrators
  - All Roles

- Identity Manager now supports the CLOB datatype for `acctAttrChanges` when using an Oracle database as the Identity Manager repository. (ID-15326)

  The advantage of using CLOB (instead of using the default `VARCHAR(4000)` datatype) is that it allows a much larger set of changes to be logged; however, it also makes this column more difficult to query, due to the proprietary nature of the CLOB access routines.

  To enable a larger set of changes, you must change the `log.acctAttrChanges` column type to `CLOB` (from `VARCHAR(4000)`) and adjust the `maxLogAcctAttrChangesLength` attribute of the `RepositoryConfiguration` Configuration Object correspondingly.

- Received email no longer contains garbage HTML tags in the message body. Email headers are now processed through `processMessage` instead of `processImage`, and they are checked for empty strings as well as nulls. (ID-15745)

- The Password Change Chart and other usage reports now require the operand value before submitting the form. (ID-15777)

- When editing reports, you can now click the Run button to execute a report without saving the report changes. Use the Save button to save any changes made to the report. (ID-17212)

Resources

- The SecurID UNIX adapter now uses the Resource User Attribute name to resolve the schema attribute name (LHS value) for read/modify. (ID-10521)

- The SecurID ACE/Server adapters now enforce the RSA requirement that a “default login” can only be comprised of single-byte English characters. (ID-13805)

- You can now use the Mutex Acquire Timeout resource attribute for UNIX adapters to specify how much time (in seconds) certain operations will wait for the scripting mutex. (ID-14234)

- Identity Manager 7.1 Update 1 supports Remedy versions 6.3 and 7.0. However, there are many substantial differences between these versions in terms of their sample data, defaults, and out-of-the-box configuration. For example, the name of the “ticket” schema in version 6.3 is *HPD:HelpDesk*, while in 7.0 it has been changed to *HPD:Help Desk*. (ID-14611)

- The Audit Log has been updated to more accurately reflect what has happened to resource attributes during the creation or modification of a resource account. (ID-15323)

  The log now contains three columns for resource account attributes:

  - The first column (old value) shows the value before modification.
  - The second column (attempted value) shows the requested change.
  - The third column (new value) shows how the value was actually set. If an error occurs, the requested value will not be the same as the actual value set.

- If a Resource Affinity account on a RACF resource has insufficient privileges to list a user, Identity Manager will now provide an appropriate error message. (ID-15331)
- When deleting RACF accounts, the system now queries the user's (using a search mask) data set profiles, enumerates over the data set, and deletes the individual data sets (instead of trying to remove them all using a `DELDSD .**` command) (ID-15413)
- All Oracle ERP responsibilities are now listed in the default Oracle ERP User Form's Responsibilities drop-down list. This list will include Oracle ERP Responsibilities currently not assigned to any user. (ID-15492)
- The Oracle ERP adapter no longer returns a `java.lang.IndexOutOfBoundsException` when trying to retrieve a responsibility that does not exist in Oracle ERP. The adapter now returns a null value. (ID-15493)
- The FlatFileActiveSync `processLine` now returns normal processing errors for use in `AllowedErrorCount` calculations. (ID-15662)
- Before and after actions now operate correctly on the HP OpenVMS adapter. (ID-15920)
- Deadlocks no longer occur when you use Active Sync with a PeopleSoft resource. (ID-16109)
- The SAP adapter now supports updating the `ALIAS` field in SAP. The attribute mapping in the schema configuration is `ALIAS->USERALIAS`. (ID-16320)
- A null pointer exception no longer results in the Database Table resource adapter when the database is down or the resource is misconfigured. (ID-16358)
- The `WF_ACTION_ERROR` workflow variable is now set when there is a error in the Remedy resource adapter. (ID-16360)

- The attribute names on left-hand side of the SAP adapter schema map have been changed as follows: (ID-16399)

Old Name	New Name
title	titleP
nameSupplement	titleSupplement
communicationTypeCUA	communicationType
personName	addressName
personName2	addressName2
personName3	addressName3
personName4	addressName4
cityPostalCode2	poBoxPostalCode
cityPostalCode3	companyPostalCode
poBoxCityNumber	poBoxCityCode
streetCode	streetNumber

- The Oracle ERP adapter no longer erases previous values for responsibilities during a single user load. A Default value clause has been added to the form to initialize the responsibilities correctly. (ID-16414, 16654)
- The Default RACF ListUser AttrParse now supports RACF versions 1.6 and 1.8 by allowing for differences in formatting in the `DEFAULT-GROUP` line, and by making the `PHRASEDATE` optional. (ID-16580)
- The SAP adapter schema map attribute names were changed to more closely represent the SAP semantics of the attribute. (ID-16634)
- The gateway can now return the correct value when accounts are locked due to an expired password, which enables Identity Manager to allow users to change their password. (ID-16681)
- Resource adapters that use the IBM Host on Demand software, can now properly load HoD JAR files. (ID-16690).
- Now, when you set the AIX Resource Adapter `Completely Remove User` attribute to `true`, the attribute can now properly add the `-p` argument to the `rmuser` command emitted by the adapter. (ID-16706)
- The XmlParser now correctly strips `DOCTYPE` declarations from XML strings. (ID-16909)

- When using Attachmate libraries to access a mainframe, Identity Manager uses the port specified in the resource instead of always using the default TCP port (23). (ID-17046)
- The sample `AccessEnforcerUserForm` now handles cases where an Access Enforcer user's role assignment only contains a single SAP role. (ID-17161)

Roles

- Rules used to calculate resource attributes from roles are no longer applied when a user logs in to the End User page. (ID-13338)
- The Approvers list on Roles > Find Roles is now sorted. (ID-16392)

Scheduler

- Scheduled tasks will no longer be processed by multiple servers for a given scheduled start time. (ID-16318)

Security

- Approvers who do not control TOP cannot see their previously approved or rejected approvals. (ID-15271)

Server

- You can now use a customized `emailTemplate` for forwarded approvals. You must specify the `emailTemplate` in the Approval subprocesses, by ID. (ID-16468)

SPE

- For the SPE Sync task, transaction retries no longer fail before reaching the specified maximum number of retries. If a target resource is down and you execute a `delete` operation against the source resource with Transaction Retries enabled, the `delete` operation will not fail until the number of transaction retries exceeds the specified maximum. (ID-16120)
- SPE can now use SPE user naming attributes other than `accountId` to access users through the Forgot Your Password form. Although `accountId` is the default attribute, you can now configure user look-up from within the SPE configuration to use other look-up attribute names. (ID-16918)

Workflow

- You can no longer edit expired work items. Identity Manager now returns an error indicating the work item is invalid. (ID-15439)
- Configuring a large number of users with the same email address no longer causes an `OutOfMemory` error for a Notify action. (ID-16386)

Additional Defects Fixed

9940, 11690, 14489, 15073, 15906,16382, 16395, 16500, 16536, 16560, 16586, 16596, 16610, 16656, 16680, 16770, 16870, 16930, 17044, 17055

Known Issues

This section of the Identity Manager 7.1 Update 1 Release Notes lists known issues and workarounds:

- If you edit a user while you are also running Active Sync as a different administrator, an Active Sync exception occurs. Because the user is locked by another administrator, Active Sync cannot retry the process. (ID-11255)

  Workaround: To enable Active Sync retry for a resource, update the resource XML to include these two additional resource attributes, in the following format:

  ```
  <ResourceAttribute name='syncRetryCountLimit' type='string' multi='false'
  facets='activesync' value='180'/>

  <ResourceAttribute name='syncRetryInterval' type='string' multi='false'
  facets='activesync' value='10000'/>
  ```

  Where:

  - **syncRetryCountLimit** is the number of times to retry the update.
  - **syncRetryInterval** is the number of milliseconds to wait between retries.

  Subsequently, these values will appear as custom resource settings when you configure Active Sync. Specifying a `displayName` is advisable; using a custom catalog key if localization is necessary.

- A regression causes Identity Manager password synchronization to fail when used with Sun Java™ System Directory Server Enterprise Edition 6.0, 6.1, and 6.2. The failure will be corrected in the Directory Server 6.3 release. If versions 6.0, 6.1, or 6.2 are required to work with Identity Manager, please request a Directory Server hotfix from Support, referencing Directory Server bug 6604342. (ID-14895)

- When you expand the resource objects of a Sun Java™ System Access Manager 7.0 resource from the Resources tab, you might see the following error: (ID-15525)

  ```
  Error listing objects. ==> com.waveset.util.WavesetException: Error trying to get
  attribute value for attribute 'guid'. ==> java.lang.IllegalAccessError: tried to access
  method com.sun.identity.idm.AMIdentity.getUniversalId()Ljava/lang/String; from class
  com.waveset.adapter.SunAccessManagerRealmResourceAdapter
  ```

  This error occurs on Access Manager 7.0 resources that have not had any patches applied. To fix this problem, you must apply at least Patch 1 of Access Manager, and then rebuild and redeploy the Access Manager client SDK.

- The default `LocalFiles` repository does not work with Sun Java™ System Application Server 9.*x*. You must use one of the supported databases (listed in the "Supported Software and Environments" section of these Release Notes) or MySQL during development. Some individuals have had success disabling the SecurityManager for the particular container and setting the memory higher, but neither action is a definitive fix for this issue. (ID-15589)

- Some of the words on the tab of "Edit User" screen could wrap around in multi-language mode. (ID-16054)

  Workaround: To ensure words in tabs are displayed without being wrapped, add the following to `$WSHOME/styles/customStyle.css`:

  ```
  table.Tab2TblNew td
  {background-image:url(../images/tabs/level2_deselect.jpg);background-repeat:repeat-x;b
  ackground-position:left top;background-color:#C4CBD1;border:solid 1px
  #8f989f;white-space:nowrap}
  ```

  ```
  table.Tab2TblNew td.Tab2TblSelTd
  {border-bottom:none;background-image:url(../images/tabs/level3_selected.jpg);backgroun
  d-repeat:repeat-x;background-position:left
  bottom;background-color:#F2F4F3;border-left:solid 1px #8f989f;border-right:solid 1px
  #8f989f;border-top:solid 1px #8f989f;white-space:nowrap}
  ```

- Due to interoperability issues between WebSphere data sources and Oracle JDBC drivers, Oracle customers who want to use a WebSphere data source with Identity Manager must use Oracle 10g R2 and the corresponding JDBC driver. (The Oracle 9 JDBC driver will not work with a WebSphere data source and Identity Manager.) (ID-16167)

If you have a version of Oracle prior to 10g R2 and cannot upgrade Oracle to 10g R2, then configure the Identity Manager repository so that it connects to the Oracle database using Oracle's JDBC Driver Manager (and not a WebSphere data source).

See the following URL or more information:

http://www-1.ibm.com/support/docview.wss?uid=swg21225859

- Numbers display in the Priority and Severity columns of the Violation Summary Report instead of text descriptions. (ID-16932)
- The Violation Summary Report does not show Corrected or Remediating violations. (ID-16933)
- The Violation State column in the Violation Summary Report should be localized. (ID-17011)
- Add an EXEMPTED option to the Possible States drop-down menu in the Violation Summary Report. (ID-17042)
- The Identity Manager installer does not run with a 64-bit JDK. (ID-17104)

  Workarounds:

  - Install manually.
  - Use a 32-bit version JDK to run the installer.
  - Set `os.arch="x86"` by setting `JAVA_OPTS` (used by `install.bat`) to get through the install. For example,

    ```
    set JAVA_OPTS=-Dos.arch="x86"

    install.bat
    ```

- If you are provisioning GroupWise users through an Identity Manager gateway running in single-threaded mode (for example, an `ExclusiveNDSContext` registry key was created with a value of **`1`**), an error similar to the following may result when you attempt to update a GroupWise user: (ID-17144)

  ```
  XPRESS  exception ==> com.waveset.util.WavesetException: Can't call method
  getResourceObject on class com.waveset.ui.FormUtil ==>
  com.waveset.util.WavesetException: Error connecting to the GroupWise domain
  (cn=7GWDOM.o=6idmtest): Error occurred opening the database. Check the path.
  ```

  Workaround: If you are provisioning GroupWise users, run the gateway in multi-threaded mode. To run in multi-threaded mode, either delete the `ExclusiveNDSContext` registry key or set the `ExclusiveNDSContext` registry key's value to **`0`**, then stop and restart the gateway.

- All Inactive Account Scan reports do not display their results on the View Risk Analysis page. To view the result from these reports, go to the Server Tasks page. (ID-17255)

- When installing Password Synchronization, be sure to use the binary that is appropriate for the operating system on which you are installing. The binary for 32-bit Windows is called `IdmPwSync_x86.msi` and the binary for 64-bit Windows is called `IdmPwSync_x64.msi`. If you install the wrong binary, it may appear to succeed, but Password Synchronization will not operate properly. (ID-17290)

  When uninstalling Password Synchronization, use the Windows Add or Remove Programs feature from the Control Panel to ensure correct removal.

- Identity Manager's round robin account policy might not generate sequential order assignment of authentication questions. (ID-17295)

- A Sealing violation exception might occur when you use Identity Manager 7.1 or 7.1 Update 1 with Oracle 10g on Sun Java™ System Application Server Enterprise Edition 8.2. The problem can be caused by having more than one Oracle JDBC JAR file in the `CLASSPATH` or by having an incompatible version of the JDBC JAR file in the `CLASSPATH`. (ID-17311)

  Be sure there is only one Oracle JDBC JAR file in the `CLASSPATH` and that it is a compatible version, such as the JAR file supplied during the Oracle install.

- WRQ looks though the `classpath` to discover its own entry. From that entry, WRQ computes the directory where the `JAR` is stored, and then uses that directory to read the `.JAW` (licensing file). However, both BEA and WebSphere use non-standard protocol names (BEA uses `zip`, and WebSphere uses `wsjar`) rather than the standard `JAR`, which is the protocol the WRQ code assumes exists. (ID-17319)

  Workaround: Add the following option to the `java` command in the `startWeblogic.sh` file:

  `-Dcom.wrq.profile.dir="<`*dir containing JAW file*`>"`

- Before creating a new resource, be sure to enable the resource type in the list of configured types. Otherwise, the newly created resource object may not have all the required fields. (ID-17324)

- When editing or updating a user, if you try to assign an idmManager that does not yet exist (for example, the idmManager is missing), you will see the following error message and the change cannot be saved. (ID-17339)

  ```
  'Item User:[idmManager that doesn't exist] was not found in the repository, it may have been deleted in another session'
  ```

  You do not see this problem when creating a new user.

- Report configurations are not preserved when upgrading from 7.1 to 7.1 Update 1. Please save the report configuration objects prior to upgrading. (ID-17363)

- When executing `Load From Resource`, and the resource supports `ACCOUNT_CASE_INSENSITIVE_IDS`, if the user's accountId differs in case from the accountId stored in Identity Manager's `ResourceInfo` user object, a second `ResourceInfo` will be added to the user object with the accountId in the same case as reported by the resource.

  Workaround: Ensure that the accountId in the Identity Manager `ResourceInfo` object in the user object is the same case as that reported by the resource. (ID-17377)

Installation and Update Notes

This section provides information related to installing or updating, and the information is organized as follows:

- Installation Notes
- Upgrade Notes

A schema change occurs with most major Identity Manager releases. You must update your schema before upgrading to a new Identity Manager version. To upgrade to Identity Manager 7.1, run one of following schema upgrade scripts, depending on the version from which you are upgrading: (ID-15392 and ID-15722)

- From Identity Manager 6.0, run the appropriate `upgradeto71from60` script.
- From Identity Manager 7.0, run the appropriate `upgradeto71from70` script.

NOTES

- When upgrading Identity Manager, be sure to review the installation section for your application server in *Sun Java™* System *Identity Manager Installation* for application server-specific instructions.
- For more detailed information and instructions about upgrading, see *Sun Java™* System *Identity Manager Upgrade*.
- 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.

Installation Notes

The following information relates to the product installation process:

- You must manually install Identity Manager on HP-UX.
- The Identity Manager 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.

- Running the Sun Identity Manager Gateway on a Windows NT system requires the Microsoft Active Directory Client extension. The DSClient can be found at the following location:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358

NOTE Refer to the *Sun Java™* System *Identity Manager Installation* publication for detailed product installation instructions.

- On UNIX/Linux, there are two additional installation requirements (ID-8403):
  - For 5.0 - 5.0 SP1:
    - `/var/tmp` must exist
    - `/var/tmp` must be writable by the user that executed the install
  - For 5.0 SP2 and later:
    - `/var/opt/sun/install` must exist
    - `/var/opt/sun/install` must be writable by the user that executed the install
- The steps for installing Identity Manager for Sun ONE Application Server 7 and for Sun Java System Application Server have been revised. (ID-16600)

  You must edit the `server.policy` file after installing the Identity Manager software or Identity Manager will not run. Consequently, you must perform the installation steps in the following order:
  - Step 1: Install the Sun ONE Application Server Software
  - Step 2: Install the Identity Manager Software
  - Step 3: Edit the server.policy File
  - Step 4. Deploy Identity Manager into Sun ONE Application Server
  - Step 5. Install the Sun Identity Manager Gateway

Upgrade Notes

This section summarizes the tasks you must perform to upgrade Identity Manager from version 6.0 or version 7.0 to version 7.1. (See "Identity Manager Upgrade Paths" on page 14 for information about which versions can be upgraded to Identity Manager 7.1.)

The information in this section is organized as follows:

Upgrade Issues

- After upgrading, the `changedFileList` and `notRestoredFileLists` will contain the following files. These files should not display, and no action is required. (ID 9228)

```
bin/winnt/nspr4.dll
bin/winnt/jdic.dll
bin/winnt/MozEmbed.exe
bin/winnt/IeEmbed.exe
bin/winnt/AceApi.dll
bin/winnt/DominoAPIWrapper.dll
bin/winnt/DotNetWrapper.dll
bin/winnt/gateway.exe
bin/winnt/lhpwic.dll
bin/winnt/msems.inf
bin/winnt/pwicsvc.exe
bin/winnt/remedy.dll
bin/solaris/libjdic.so
bin/solaris/mozembed-solaris-gtk2
bin/linux/librfccm.so
bin/linux/libsapjcorfc.so
bin/linux/libjdic.so
bin/linux/mozembed-linux-gtk2
```

- Identity Manager's User Extended Attributes now fully supports multi-valued attributes. (ID-14863)

  NOTE You can add a multi-valued user extended attribute to the accounts list table, and it will render the list without error. However, attempting to sort on that column will yield the following error:

  ```
  java.lang.ClassCastException: java.util.ArrayList
  ```

  An attribute condition that refers to a multi-valued extended attribute will evaluate correctly for a user object *only* after that user object has been re-serialized. If you want such an attribute condition to evaluate correctly for all user objects, then you must re-serialize all user objects.

  There are three ways to re-serialize existing users:

  - Modifying an individual User object during normal operations.

    For example, opening a user account through the user interface and saving it with or without modifications.

    Disadvantage: This method is time-consuming, and the administrator must be meticulous to ensure all existing users are re-serialized.

  - Using the `lh refreshType` utility to re-serialize all users. The `refreshType` utility's output is a refreshed list of users.

    ```
    lh console

    refreshType User
    ```

    Disadvantage: Because the `refreshType` utility runs in the foreground and not the background, this process can be time-consuming. If there are a lot of users, re-serializing them all will take a long time.

- Using the Deferred Task Scanner.

  NOTE Before running the Deferred Task Scanner process, you must edit the `System Configuration` object using the Identity Manager Integrated Development Environment (Identity Manager IDE) or some other method.

  Search for `'refreshOfType'` and remove the attributes for `'2005Q4M3refreshOfTypeUserIsComplete'` and `'2005Q4M3refreshOfTypeUserUpperBound'`.

  After editing the `System Configuration` object, you must import it to repository for your changes to be present.

  Disadvantage: This method causes the next Deferred Task Scanner run to take a long time because it examines and re-writes almost every User object. However, subsequent Deferred Task Scanner runs should execute at normal speed and duration.

- If you are upgrading from a 6.x installation to version 7.0 or 7.1, and you want to start using the new Identity Manager end-user pages, you must manually change the system configuration ui.web.user.showMenu to true for the horizontal navigation bar to display. (ID-14901)

  Also, if you want the new end user dashboard to display on the end-user home page, you must manually change the end user form mapping for Form Type 'endUserMenu'. Go to Configure -> Form and Process Mapping -> for Form Type 'endUserMenu' change the Form Name Mapped To to be 'End User Dashboard'.

  You should also update the mapping for Form Type 'endUserWorkItemListExt'. Change the Form Name Mapped To to be 'End User Approvals List'.

- If you are upgrading from 6.0 or 7.0 to version 7.1, and using `LocalFiles`, you must export all of your data before upgrading and then re-import the data after doing a clean installation of 7.1. (ID-15366)

- When you are upgrading to Identity Manager 7.1 from a previous release, the `WEB-INF/speConfiguration.xml` file is not removed during the upgrade process. This file, however, is no longer used by the Service Provider feature and can safely be removed. Similarly, the `spe.enableServer` property might still appear in the `Waveset.properties` file. This property is also no longer used in the Identity Manager 7.0 or 7.1 releases. (ID-15765)

- If your installation contains a Remedy resource, you must place Remedy API libraries in the directory where the Gateway is installed. These libraries can be found on the Remedy server.

Table 1 Remedy API Libraries

Remedy 4.x and 5.x	Remedy 6.3	Remedy 7.0
• `arapi`*XX*`.dll` • `arrpc`*XX*`.dll` • `arutl`*XX*`.dll` where *XX* matches the version of Remedy. For example, `arapi45.dll` on Remedy 4.5.	• `arapi63.dll` • `arrpc63.dll` • `arutl63.dll` • `icudt20.dll` • `icuin20.dll` • `icuuc20.dll`	• `arapi70.dll` • `arrpc70.dll` • `arutl70.dll` • `icudt32.dll` • `icuin32.dll` • `icuuc32.dll`

- Report configurations are not preserved when upgrading from 7.1 to 7.1 Update 1. Please save the report configuration objects prior to upgrading. (ID-17363)

Using the Identity Manager Upgrade Program

This section describes the steps for upgrading Identity Manager using the Identity Manager installation and upgrade program.

NOTES

- A schema change occurs with most major Identity Manager releases. You must update your schema before upgrading to a new Identity Manager version. To upgrade to Identity Manager 7.1, run one of following schema upgrade scripts, depending on the version from which you are upgrading: (ID-15722)
  - From Identity Manager 6.0, run the appropriate `upgradeto71from60` script.
  - From Identity Manager 7.0, run the appropriate `upgradeto71from70` script.

  For more information, see the *Sun Java™* System *Identity Manager Upgrade*.
- In some environments, including on HP-UX, you may be required or prefer to follow the alternate, manual update procedures. If so, skip to "Upgrading Manually" on page 54.
- For UNIX environments, make sure that an `install` directory exists in one of the following locations, and that you can write to it:
  - **For Linux/HP-UX**: `/var/opt/sun/install`
  - **For Solaris**: `/var/sadm/install`
- During update, you will need to know the location where your application server is installed.
- Any previously installed hotfixes will be archived to the following directory:

  `$WSHOME/patches/`*`HotfixName`*
- 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 upgrade Identity Manager:

1. Shut down the application server.
2. If you are upgrading to Identity Manager *6.0* or Identity Manager *7.0*, you must upgrade the repository database schema, as follows:
   - **Identity Manager 6.0** introduces a schema change that provides new tables for tasks, groups, orgs, and the syslog table. You must create these new table structures and move your existing data.
   - Identity Manager 6.0 stores user objects in two tables. You can use the sample scripts provided in the `db_scripts` directory to make schema changes. Refer to the `db_scripts/upgradeto2005Q4M3.`*DatabaseName* script to upgrade your repository tables.

     NOTE
     - Before updating your repository schema, make a full backup of your repository tables.
     - The upgrade of MySQL databases is highly involved. Refer to `db_scripts/upgradeto2005Q4M3.mysql` for more information.

   - **Identity Manager 7.0** introduces new tables for user entitlements.
     You must create these new table structures and move your existing data. You can use the sample scripts provided in the `db_scripts` directory to make schema changes.

     NOTE
     - Before updating the repository schema, make a full backup of your Repository tables.
     - Refer to the `db_scripts/upgrade7.0.`*DBMSName* script for more information.

3. If you are running Sun Identity Manager Gateway on the Identity Manager server, use the following command to stop the Gateway service:

   ```
   net stop "Sun Identity Manager Gateway"
   ```

4. Use either of the following methods to start the installer:
   - To use the GUI installer, run the `install.bat` (for Windows) or `install` (for UNIX).

     The installer displays the Welcome panel.

- To activate the installer in `nodisplay` mode, change to the directory where the software is located, and enter the following command:

  ```
  install -nodisplay
  ```

  The installer displays the Welcome text, and then presents a list of questions to gather installation information in the same order as the GUI installer.

  NOTE
  - If no display is present, the installer defaults to the `nodisplay` option.
  - The installer will not install an older version of the software over a newer version. In this situation, an error message displays and the installer exits.

5. On the Welcome panel, click Next.
6. On the Install or Upgrade? panel, select Upgrade, and then click Next.
7. On the Select Installation Directory panel, select the directory where the earlier Identity Manager version is located and click Next.

   The installer displays progress bars for the pre- and post-upgrade processes and then proceeds to Installation Summary panel.
8. For detailed information about the installation, click Details, view the log file, and click Close to exit the installer.
9. Remove all of the compiled Identity Manager files from the work directory of the application server.
10. If you are running Gateway on a remote system, upgrade it by using the following steps.
    a. Log in to the Windows system, and change to the directory where Gateway is installed.
    b. Stop the Gateway service by running the command:

       ```
       gateway -k
       ```

    c. If using Windows 2000 or later, exit all instances of the Services MMC plug-in.
    d. Use the following command to remove the Gateway service:

       ```
       gateway -r
       ```

    e. Back up and delete the existing Gateway files.

f. Extract the new Gateway files.

If you are installing the newly upgraded Gateway on a system that is not the Identity Manager server, then copy the `gateway.zip` file from the Identity Manager Installation CD.

g. Unpack the `gateway.zip` file into the directory where Gateway was installed.

h. Run the following command to install the Gateway service:

```
gateway -i
```

i. Run the following command to start the Gateway service:

```
gateway -s
```

Upgrading Manually

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

NOTE

- Be sure you 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.

On a Windows Platform

Use the following steps to upgrade Identity Manager manually on a supported Windows platform:

1. Stop the application server and Sun Identity Manager Gateway.
2. Update the Identity Manager database. (See Step 2 on page 52 for detailed instructions.)
3. Enter the following commands to set your environment:

```
set ISPATH=Path to install software
set WSHOME=Path to Identity Manager Installation OR Staging Directory
set TEMP=Path to Temporary Directory
```

4. Run pre-process:

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

5. Install software:

```
cd %WSHOME%
jar -xvf %ISPATH%\IDM.WAR
```

6. Run post-process:

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

NOTE The installer supports upgrading installations that have renamed, deleted, or disabled the default Configurator account.

The installer prompts you for user name and password to import the `update.xml` during the upgrade post process. If the user or password is entered incorrectly, you will be prompted (up to three times) to enter the correct password. The error will be displayed in the text box behind it.

For manual installation you must provide the `-U` *username* `-P` *password* flags to pass the credentials to the `UpgradePostProcess` procedure.

7. If you installed into a staging directory, create a `.war` file for deployment to your application server.
8. Remove the Identity Manager files from the application server work directory.
9. If the upgrade process did not do so already, move any hotfix class files from the `WEB-INF\classes` directory to the `$WSHOME\patches\`*HotfixName* directory.
10. Start the application server.
11. Upgrade and then restart Sun Identity Manager Gateway. (See Step 10 on page 53 for detailed instructions.)

On a UNIX Platform

Use the following steps to upgrade Identity Manager manually on a supported UNIX platform:

1. Stop the application server and Sun Identity Manager Gateway.
2. Update the Identity Manager database. (See Step 2 on page 52 for instructions.)
3. Enter the following commands to set your environment:

   ```
   export ISPATH=Path to Install Software
   export WSHOME=Path to Identity Manager Installation OR Staging Directory
   export TEMP=Path to Temporary Directory
   ```

4. Run pre-process:

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

5. Install software:

   ```
   cd $WSHOME
   jar -xvf $ISPATH/idm.war
   ```

6. Run post-process:

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

NOTE The installer supports upgrading installations that have renamed, deleted, or disabled the default Configurator account.

The installer prompts you for user name and password to import the `update.xml` during the upgrade post process. If the user or password is entered incorrectly, you will be prompted (up to three times) to enter the correct password. The error will be displayed in the text box behind it.

For manual installation you must provide the `-U` *username* `-P` *password* flags to pass the credentials to the `UpgradePostProcess` procedure.

7. Change directory to `$WSHOME/bin/solaris` or `$WSHOME/bin/linux`, and then set permissions on the files in the directory so that they are executable.
8. If you installed into a staging directory, create a `.war` file for deployment to your application server.
9. Remove the Identity Manager files from the application server work directory.
10. If the upgrade process did not do so already, move any hotfix class files from the `WEB-INF/classes` directory to the `$WSHOME/patches/`*HotfixName* directory.
11. Start the application server.
12. Upgrade and then restart Sun Identity Manager Gateway. (See Step 10 on page 53 for instructions.)

Deprecated APIs

This section lists all Identity Manager Application Programming Interfaces (APIs) deprecated since Identity Manager 6.0 2005Q4M3 and their replacements (if available). This information is organized into the following sections:

- Deprecated Constructors and Classes
- Deprecated Methods and Fields

Deprecated Constructors and Classes

The following table lists the deprecated constructors and classes and their replacements, when available.

Deprecated	Replacement
com.sun.idm.idmx.IDMXContext	com.waveset.object.LighthouseContext
com.sun.idm.idmx.IDMXContextFactory	com.waveset.session.SessionFactory
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AIXResourceAdapter.BlockAcctIter	References to this class should be replaced with an AccountIterator based on the Supplier model. For example BufferedAccountQueue(new AIXAccountSupplier).
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	References to this class should be replaced with an AccountIterator based on the Supplier model. For example BufferedAccountQueue(new LinuxAccountSupplier).
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.LinuxResourceAdapter.BlockAcctIter	
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter

Deprecated	Replacement
com.waveset.adapter.ResourceAdapterBase.SimpleAccountIterator	Users of this class should switch to using the supplier model for account iteration. A direct replacement for this class would be: new BufferedAccountQueue(new SimpleAccountSupplier(accounts));
com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter	References to this class should be replaced with an AccountIterator based on the Supplier model. For example BufferedAccountQueue(new SVIDAccountSupplier).
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError
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.AuditEvent.setAccountAttributesBlob (List)	Use one of the other forms of setAccountAttributesBlob (to allow for new, attempted, or old values).
com.waveset.object.AuditEvent.setAccountAttributesBlob (Map, Map)	Put the list of attributes into name=value;; format, which in turn will be stored in a blob. The delimiter ;; will be filtered.
com.waveset.object.AuditEvent.setAccountAttributesBlob (Map, Map, Set)	Use one of the other forms of setAccountAttributes Blob (to allow for new, attempted, or old attribute values).
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.object.Syntax.getDescription()	
com.waveset.object.ViewMaster()	
com.waveset.object.ViewMaster.ViewMaster(String,String)	
com.waveset.object.ViewMaster.ViewMaster(Subject,String)	
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

Deprecated	Replacement
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.ConnectionPool.getConnection(String, String, String, String, String, boolean)	getConnection(String driverClass, String driverPrefix, String url, String user, String password, boolean checkConnection, String validationSql)
com.waveset.util.CSVParser	com.waveset.util.ConfigurableDelimitedFileParser
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.PooledConnection.isValid()	isValid(String SQL)
com.waveset.util.ITrace	com.sun.idm.logging.Trace
com.waveset.util.PipeDelimitedParser	com.waveset.util.ConfigurableDelimitedFileParser

Deprecated Methods and Fields

The tables in this section list deprecated methods and fields. 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 or Field	Replacement
handlePDException(Exception)	handlePDException(PDException)

com.waveset.adapter.ACF2ResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ActiveSync

Deprecated Method or Field	Replacement
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Deprecated Method or Field	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 or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.AuthSSOResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

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

com.waveset.adapter.DB2ResourceAdapter

Deprecated Method or Field	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 or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

r

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

com.waveset.adapter.HostConnPool

Deprecated Method or Field	Replacement
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	
putFree(IHostAccess)	putAffinityFree

com.waveset.adapter.iapi.IAPIFactory

Deprecated Method or Field	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 or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

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

com.waveset.adapter.NaturalResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

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

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Deprecated Method or Field	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 or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

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

com.waveset.adapter.RequestResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

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

com.waveset.adapter.ResourceAdapterBase

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

com.waveset.adapter.ResourceManager

Deprecated Method or Field	Replacement
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

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

com.waveset.adapter.SAPResourceAdapter

Deprecated Method or Field	Replacement
reverseMapMultiAttr(String, Object, WSUser)	
setUserField(JCO.Function, String)	Function#setUserField(String)
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

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

com.waveset.adapter.ScriptedHostResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

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

com.waveset.adapter.SybaseResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Deprecated Method or Field	Replacement
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)
login(IHostAccess hostAccess)	#login(IHostAccess hostAccess, ServerAffinity affinity)

com.waveset.adapter.VerityResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Deprecated Method or Field	Replacement
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

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

com.waveset.object.AccountAttributeType

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

com.waveset.object.AuditEvent

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

com.waveset.object.Constants

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

com.waveset.object.LoginConfig

Deprecated Method or Field	Replacement
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

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

com.waveset.object.RepositoryResult

Deprecated Method or Field	Replacement
get(int)	
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext()
	next()
sort()	

com.waveset.object.RepositoryResult.Row

Deprecated Method or Field	Replacement
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Deprecated Method or Field	Replacement
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Deprecated Method or 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 or Field	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 or Field	Replacement
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.WSUser

Deprecated Method or Field	Replacement
getApproverDelegate()	getWorkItemDelegate(String workItemType)
getDelegateHistory()	getWorkItemDelegateHistory()
setApproverDelegate(WSUser.Delegate)	addWorkItemDelegate(Delegate workItemDelegate)
setDelegateHistory(List)	etWorkItemDelegateHistory(List workItemDelegateHistory)

com.waveset.session

Subclass	Deprecated Method or Field	Replacement
LocalSession	getAdministrators(Map)	com.waveset.view.WorkItemUtil#getAdministrators
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 or Field	Replacement
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Deprecated Method or Field	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)

Deprecated Method or Field	Replacement
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)
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)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)

Deprecated Method or Field	Replacement
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 or Field	Replacement
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Deprecated Method or Field	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 or Field	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 or Field	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)
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)
getLocalHostName()	#getServerId() (to get a unique server identifier)

com.waveset.workflow.WorkflowContext

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

Deprecated Method or Field	Replacement
getApproverDelegate()	
setApproverDelegate()	
getDelegateHistory()	
setDelegateHistory()	

Documentation Additions and Corrections

This section contains new and corrected information that was required after the Identity Manager 7.1 documentation set was published. This information is organized as follows:

Identity Manager Installation

This section provides new information and documentation corrections related to *Sun Java*™ System *Identity Manager Installation*.

- The following information should be added to the Note provided in the "Set Up a Java Virtual Machine and Java Compiler" section found in Chapter 1, Before You Install. (ID-17131)

  You can run Identity Manager 7.1 and later on BEA WebLogic application servers with all WebLogic-supported 1.4.2 and 1.5 JVMs.

- The Exchange 5.5 resource adapter is not supported. Ignore any references to this adapter.

- The installation steps in Chapter 6, "Installing Identity Manager for Sun ONE Application Server 7" and Chapter 7, "Installing Identity Manager for Sun Java System Application Server" have been revised because you must edit the `server.policy` file after installing the Identity Manager software or Identity Manager will not run. Consequently, you must perform the installation steps in the following order (ID-16600):

  - Step 1: Install the Sun ONE Application Server Software
  - Step 2: Install the Identity Manager Software

- Step 3: Edit the server.policy File
- Step 4. Deploy Identity Manager into Sun ONE Application Server
- Step 5. Install the Sun Identity Manager Gateway

- Specific version numbers should be removed from the "Supported Software and Environments" section in Chapter 1, "Before You Install" and the following note will be added: (ID-16687)

NOTE Because software product developers frequently ship new versions, updates, and fixes to their software, the software and environment versions supported by Identity Manager changes often. Review the "Supported Software and Environments" section of the *Identity Manager Release Notes* before proceeding with installation.

Identity Manager Upgrade

This section provides new information and documentation corrections for *Sun Java™* System *Identity Manager Upgrade*.

- Before upgrading, it is important to back up both the directory where Identity Manager is installed and the database that Identity Manager is using. You can use third-party back up software or a back up utility supplied with your system to back up the Identity Manager file system. To back up your database, refer to the database documentation for recommended back up procedures. (ID-2810)

  When you are ready to create your backups, you must first shutdown (or idle) Identity Manager. Then, use your backup utilities to back up your database and the file system where you installed Identity Manager.

- The AD Active Sync resource has been deprecated and replaced by the AD resource. Perform the following steps to migrate to the AD Active Sync to newer releases: (ID-11363)
  - Export the existing AD Active Sync resource object to an xml file (either from the command line or debug pages).
  - Delete the existing resource (this will not affect Identity Manager users or resource account users)
  - Create a new AD resource that is Active Sync.
  - Export this new resource object to an XML file.

- Edit this file and change the value of the id attribute and the value of the name attribute to match the values from the OLD resource object saved in step 1. These attributes are in the <Resource id='*idnumber*' name='AD' ...> tag.
- Save the changes to the file.
- Import the modified object back into Identity Manager using either the Configure->Import Exchange File page or the command line.

- Updated the Other Custom Repository Objects section to include instructions for using Identity Manager's SnapShot feature to create a baseline or "snap shot" of the customized repository objects in a deployment. (ID-14840)

Other Custom Repository Objects

Record the names of any other custom repository objects that you created or updated. You might have to export these objects from your current installation and then re-import them to the newer version of Identity Manager after upgrading.

- Admin group
- Admin role
- Configuration
- Policy
- Provisioning task
- Remedy configuration
- Resource form
- Resource form
- Role
- Rule
- Task definition
- Task template
- User form

You can use Identity Manager's SnapShot feature to create a baseline or "snap shot" of the customized repository objects in your deployment, which can be very useful when you are planning an upgrade.

SnapShot copies the following, specific object types from your system for comparison:

- AdminGroup
- AdminRole
- Configuration
- EmailTemplate
- Policy
- ProvisionTask
- RemedyConfig
- ResourceAction
- Resourceform
- Role
- Rule
- TaskDefinition
- TaskTemplate
- UserForm

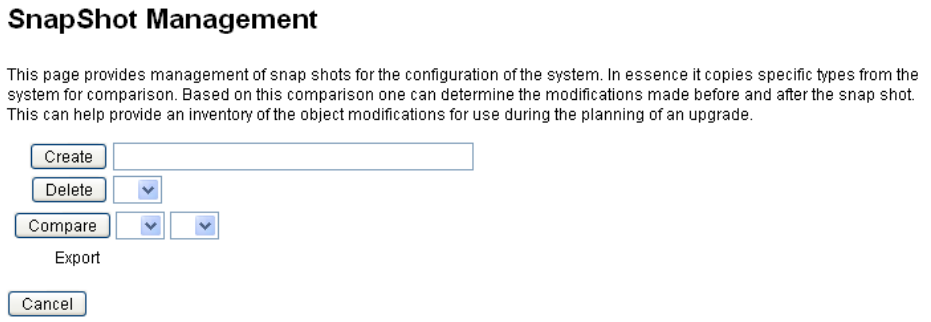
You can then compare two snapshots to determine what changes have been made to certain system objects before and after upgrade.

NOTE This feature is not intended for detailed, on-going XML diffs — it is only a minimal tool for “first-pass” comparisons.

To create a snapshot:

1. From the Identity Manager Debug page (Figure 1), click the SnapShot button to view the SnapShot Management page.

Figure 1 SnapShot Management Page



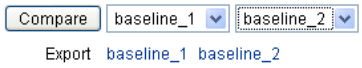
2. Type a name for the snapshot in the Create text box, and then click the Create button.

   When Identity Manager adds the snapshot, the snapshot's name displays in the Compare menu list and to the right of the Export label.

To compare two snapshots:

1. Select the snapshots from each of the two Compare menus (Figure 2).

Figure 2 SnapShot Management Page



2. Click the Compare button.
   - If there are no object changes, then the page indicates that no differences were found.
   - If object changes were found, then the page displays the object type and name, and whether an object is different, absent, or present.

     For example, if an object is present in baseline_1, but is not present in baseline_2, then the baseline_1 column indicates `Present` and the baseline_2 column indicates `Absent`.

You can export a snapshot in XML format. Click the snapshot name to export the snapshot file.

To delete a snapshot, select the snapshot from the Delete menu, and then clicking the Delete button.

- Added the following paragraph to the Modified JSPs section to include information about using the `inventory -m` command to identify modified JSPs in a deployment: (ID-14840)

  You can use the `inventory -m` command (described on the previous page) to identify any JSP modifications made in your deployment.

- If you are upgrading from a 6.*x* install to version 7.0 or 7.1, and you want to start using the new Identity Manager end-user pages, you must manually change the system configuration `ui.web.user.showMenu` to **`true`** for the horizontal navigation bar to display. (ID-14901)
- If you are upgrading from 6.0 or 7.0 to version 7.1, and using `LocalFiles`, you must export all of your data before upgrading and then re-import the data after doing a clean installation of 7.1. (ID-15366)
- Upgrading from 6.0 or 7.0 to version 7.1 requires a database schema upgrade. (ID-15392)
  - If you are upgrading from 6.0 to 7.1, you must use the `upgradeto71.*` script appropriate to the type of RDBMS you are using.
  - If you are upgrading from 7.0 to 7.1, you must use the `upgradeto71from70.*` script appropriate to the type of RDBMS you are using.
- During the upgrade process, Identity Manager analyzes all roles on the system and then updates any missing subroles and super roles links using the `RoleUpdater` class. (ID-15734)

  To check and upgrade roles outside of the upgrade process, import the new `RoleUpdater` configuration object that is provided in `sample/forms/RoleUpdater.xml`. For example:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
   <ImportCommand class='com.waveset.session.RoleUpdater' >
      <Map>
         <MapEntry key='verbose' value='true' />
         <MapEntry key='noupdate' value='false' />
         <MapEntry key='nofixsubrolelinks' value='false' />
   v</Map>
   </ImportCommand>
</Waveset>
```

  Where:

  - **verbose**: Provides verbose output when updating roles. Specify **`false`** to enable a silent update of roles.
  - **noupdate**: Determines whether the roles are updated. Specify **`false`** to get a report that only lists which roles will be updated.
  - **nofixsubrolelinks**: Determines whether super roles are updated with missing subrole links. This value is set to false by default and links will be repaired.
- If you have a space in the path to the Identity Manager installation directory, you must specify the `WSHOME` environment variable without double quotes (`"`), as shown in the following example (ID-15470):

NOTE Do not use trailing slashes (\) when specifying the path, even if the path contains no spaces.

```
set WSHOME=c:\Program Files\Apache Group\Tomcat 5.5\idm
```

or

```
set WSHOME=c:\Progra~1\Apache~1\Tomcat~1\idm
```

The following path will not work:

```
set WSHOME="c:\Program Files\Apache Group\Tomcat 5.5\idm"
```

Identity Manager Administration Guide

This section provides new information and documentation corrections for *Sun Java™* System *Identity Manager Administration*.

Chapter 2, Getting Started with Identity Manager

- The section titled, Forgotten User ID describes how to use the Forgot Your User ID? button on the Log In to Identity Manager page to retrieve a forgotten user ID. However, when upgrading from previous Identity Manager versions to version 7.1 Update 1, the Forgot Your User ID? feature is disabled by default. (ID-16715)

  To enable this feature, you must modify the following attributes in the System Configuration object:

  ```
  ui.web.user.disableForgotUserId = false
  ```

  ```
  ui.web.admin.disableForgotUserId = false
  ```

Chapter 3, User and Account Management

- In the section titled Disable Users (User Actions, Organization Actions), the note has been amended.:

> **NOTE** If an assigned resource does not have native support for account disabling, but does support password changes, then Identity Manager can be configured to disable user accounts on that resource through the assignment of new, randomly generated passwords. This configuration requires that you enable the resource Disable and Password account features by using the Identity System Parameters page in the Resource Wizard. See Chapter 4, Configuration, for more information.

- In the section titled Enable Users (User Actions, Organization Actions), the note has been added:

> **NOTE** If an assigned resource does not have native support for account enabling, but does support password changes, then Identity Manager can be configured to enable user accounts on that resource through password resets. This configuration requires that you enable the resource Enable and Password account features by using the Identity System Parameters page in the Resource Wizard. See Chapter 4, Configuration, for more information.

- In the section title User Authentication, a description of the authentication question policies has been added.

  The authentication question policy determines what happens when a user clicks on the **Forgot Password** button on the login page or when accessing the Change My Answers page. The following table describes each option:

Table 2 Authentication Question Policy options

Option	Description
Round Robin	Identity Manager selects the next question from the list of configured questions and assigns this question to the user. The first user is assigned the first question in the list of authentication questions, and the second user is assigned the second question. This pattern continues until the number of questions is exceeded. At that point, questions are assigned to users in sequential order. For example, if there are 10 questions, the 11th and 21st users are assigned the first question. The selected question is the only one that is displayed. If you want the user to answer a different question every time, use the Random policy and set the number of questions to 1. This option does not allow users to define their own authentication questions.

Table 2 Authentication Question Policy options *(Continued)*

Option	Description
Random	This option allows the administrator to specify how many questions the user must answer. Identity Manager randomly selects and displays the specified number of questions from the list of questions defined in the policy as well as those the user has defined. The user must answer all questions displayed.
Any	Identity Manager displays all policy-defined and user-defined questions. You must specify how many questions the user must answer.
All	The user must answer all policy-defined and user-defined questions.

Chapter 5, Administration

- In the section titled "Delegating Work Items," the following note has been added.

  NOTE After setting up delegation, any work items created during the effective delegation period are added to your list and the delegate's list. If you end delegation, then the delegated work items are recovered; this may result in duplicate work items. When you approve or reject one, then the duplicate is automatically removed from your list.

- In the section titled "Managing Work Items," the following information has been added.

  ### *Delegations to Deleted Users*

  If you have delegated a work item to a user who is later deleted from Identity Manager, then the deleted user is indicated in the Current Delegations list in parentheses. If you subsequently edit or create a delegation that includes the deleted user, then the action fails. Additionally, any user create or update work items that are delegated to a deleted user will fail.

  You can recover work items that are delegated to a deleted user by ending the delegation.

- In the table titled Identity Manager Capabilities Descriptions, the End User Administrator capability has been added. Any user assigned this capability can view and modify the rights to object types specified in the End User capability, as well as the contents of the end User Controlled Organizations rule. By default, this capability is assigned to Configurator.

- In the section titled "Scope of Control," the following information should be added: (17187)

  Identity Manager allows you to control which users are within an end user's scope of control.

You can use the `EndUserControlledOrganizations` rule to define whatever logic is necessary to ensure the right set of users are available for delegating, based on your organizational needs.

If you want the scoped list of users to be the same for administrators, whether they are logged into the Administrator interface or the End User interface, you must change the `EndUserControlledOrganizations` rule as follows:

Modify the rule to first check whether the authenticating user is an administrator, and then configure the following:

- If the user is not an administrator, return the set of organizations that should be controlled by an end user, such as the user's own organization (for example, `waveset.organization`).
- If the user is an administrator, do not return any organizations so the user only controls organizations that are assigned because that user is an administrator.

For example:

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- The following information should be added to the "Understanding and Managing Capabilities" section. (ID-14630, 15614)

  Identity Manager provides a built-in ObjectGroup/organization called *End User* that, initially, has no member objects. The `End User` ObjectGroup/organization is implicitly assigned to all users, and enables them to view several types of objects, including tasks, rules, roles, and resources.

  Previously, when users logged into the End User interface, they were automatically granted rights to object types specified in the `EndUser` capability (such as `AdminRole`, `EndUserConfig`, and `EndUserTask`). Now when users log in to the End User interface, Identity Manager also automatically gives them control of the new `EndUser` ObjectGroup. In addition, Identity Manager evaluates a new, built-in `End User Controlled Organizations` rule. Any ObjectGroup/organization names returned by this rule will also be automatically controlled by the user logging into the End User interface.

  The authenticating user's view is the input argument to the `End User Controlled Organization` rule. Identity Manager expects the rule to return one (a string) or more (a list) organizations which the user logging into the End User interface will control. A new `End User Administrator` capability was added that enables users to manage these new objects. Users who are assigned the `End User Administrator` capability can view and modify rights to object types specified in the `EndUser` capability and to the contents of the `End User Controlled Organization` rule.

  The `End User Administrator` capability is assigned to `Configurator` by default. Any changes made to the list or to organizations returned by the evaluation of the `End User Controlled Organization` rule will not be reflected dynamically for logged in users. These users must log out and then log in again to see the changes.

  If the `End User Controlled Organization` rule returns an invalid organization (for example, the organization that does not exist in Identity Manager), the problem will be logged in the System Log. You can correct the problem by logging into the Administrator user interface and fixing the rule.

  The `End User` ObjectGroup/organization is a member of `Top` and cannot have child organizations. This ObjectGroup/organization is not displayed in the tree table on the Accounts tab of the Administrator user interface. However, when editing objects (such as `Roles`, `AdminRoles`, `Resources`, `Policy`, `Tasks`, and so forth), you can make any object available to the `End User` ObjectGroup/organization from the Administrator user interface.

  Use this new best practice method (instead of using `End User Tasks`, `End User Resources`, `System Configuration:EndUserAccess`, and `End User` authTypes) to give end users access to Identity Manager configuration objects such as Roles, Resources, Tasks, and so forth. Although the `End User Tasks`, `End User Resources`, `System Configuration:EndUserAccess`, and `End User` authTypes methods will continue to be supported for backward compatibility.

Chapter 8, Task Templates

- The following information should be added to this chapter, in the Configuring the Audit Tab section: (ID-16797)

  The Audited Attribute Report can report attribute-level changes to Identity Manager users and accounts. However, standard audit logging does not generate enough audit log data to support a full query expression.

  Standard audit logging *does* write the changed attributes to the `acctAttrChanges` field in the audit log, but the changed attributes are written in a way that the report query can only match records based on the changed attribute's name. The report query cannot accurately match the attribute's value.

  You can configure this report to match records containing changes to the attribute `lastname`, by specifying the following parameters:

  ```
  Attribute Name = 'acctAttrChanges'

  Condition = 'contains'

  Value = 'lastname'
  ```

  NOTE Using `Condition='contains'` is necessary because of the way data is stored in the `acctAttrChanges` field. This field is not multi-valued. Essentially, it is a data structure that contains the `before/after` values of all changed attributes in the form `attrname=value`. Consequently, the preceding settings allow the report query to match any instances of `lastname=`*xxx*.

  It is also possible to capture only those audit records that have a specific attribute with a specific value, but some additional configuration is required. Use the following instructions:

  a. Open and log in to the Identity Manager Administrator interface:

  `http://`*server-name:port*`/idm`

  b. Select the Server Tasks tab.

  c. Select the Configure Tasks tab.

  d. Click the Update User Template task (for example).

  e. Select the Audit tab.

  You should see Audit Controls for the selected task, which performs auditing when a user update occurs.

  f. Select the Audit entire workflow box to activate the workflow auditing feature.

g. Click the Add Attribute button (located in the Audit Attributes section) to select the attributes you want to record for reporting purposes.

h. When the Select an attribute menu displays in the Audit Attributes table, select an attribute from the list. (For example: Select `user.global.email` from the drop-down menu).

i. Click Save.

j. You must now enable the configuration as follows:

I. Select Server Tasks > Configure Tasks.

II. Click the Update User Template's Enable button.

III. Do not change the default value in the Select Process Types list.

Performing this step actually causes the workflow engine to emit the necessary logging information.

IV. Click Save again.

The workflow can now provide audit records that are suitable for matching both the attribute name and the value. Although turning on this level of auditing provides much more information, be aware that there is a significant performance cost and your workflows will run slower.

Chapter 11, Identity Auditing

The following information has been added to this chapter:

Continuous Compliance

The information in this section currently states that any provisioning operations performed on a user will cause user- and organization-assigned policies to be evaluated. This information should be corrected to read as follows: (ID-17416)

Continuous compliance means that an audit policy is applied to all provisioning operations, such that an account cannot be modified in a way that does not comply with current policy.

You enable continuous compliance by assigning an audit policy to an organization, a user, or both. Any provisioning operations performed on a user will cause the user-assigned policies to be evaluated. Any resulting policy failure will interrupt the provisioning operation.

Resolving Auditor Capabilities Limitations

By default, capabilities needed to perform auditing tasks are contained in the Top organization (object group). As a result, only those administrators who control Top can assign these capabilities to other administrators.

You can resolve this limitation by adding the capabilities to another organization. Identity Manager provides two utilities, located in the `sample/scripts` directory, to assist with this task.

1. Run the following command to list all capabilities (AdminGroups) and their associated organizations (object groups):

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
   ```

   This command captures the output to a comma-separated value (CSV) file.

2. Edit the CSV file to adjust the capabilities organizational locations as desired.

3. Run this command to update Identity Manager.

   ```
   beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
   ```

Adding Rules

Added the following Note to this section (ID-16604, 16831):

NOTE Identity Manager does not support the control of rule nesting. In addition, using the Audit Policy Wizard to create policies with Boolean expression nesting can produce unpredictable results.

For complex Rule expressions, use an XML editor to create a separate XPRESS rule that references all of the rules you want to use.

Create the Rule Expression

Changed the Note in this section to read as follows (ID-16604, 16831):

NOTE Identity Manager does not support the control of rule nesting. In addition, using the Audit Policy Wizard to create policies with Boolean expression nesting can produce unpredictable results.

For complex Rule expressions, use an XML editor to create a separate XPRESS rule that references all of the rules you want to use.

Chapter 13, Service Provider Administrator

The section titled “Configure Synchronization” should state the default synchronization interval for Service Provider synchronization tasks defaults to 1 minute.

All Chapters

The release date noted in the chapter footers should be 7.1 not 7.0. (ID-16968)

Identity Manager Resources Reference

This section contains new information and documentation corrections for the *Sun Java™* System *Identity Manager Resources Reference*:

General

- The Exchange 5.5 resource adapter is not supported. Ignore any references to this adapter.

Active Directory

The following information should be added to the Active Directory resource adapter documentation.

Specifying a Domain for Pass-Through Authentication

In a default configuration, pass-through authentication is accomplished by sending the user ID and password only. These two attributes are configured in the `AuthnProperties` element in the resource object's XML as `w2k_user` and `w2k_password`. Without a domain specification, the gateway searches all known domains and tries to authenticate the user in the domain that contains the user.

In a trusted multi-domain environment, there can be two possible situations:

- All domains contain a synchronized user/password combination
- The user/password combination is domain dependent.

  When the user/password combination is synchronized, configure your Active Directory resources so that they are common resources. See *Identity Manager Administration* for more information about setting up common resources.

  If the user/password combination is domain-dependent, and if users can be expected to know the domain information, you can allow users to enter the domain information on the login screen. This option can be used in combination with common resources.

  To allow the user to enter the domain on the login page, add the following property to the `<AuthnProperties>` element in the resource object's XML:

```
<AuthnProperty name='w2k_domain' displayName='Domain:' formFieldType='text'
dataSource='user' doNotMap='true'/>
```

In an environment with multiple trusted domains and Active Directory forests, the authentication can fail using any of these configurations because the Global Catalog does not contain cross-forest information. If a user supplies a wrong password, it could also lead to account lockout in the user's domain if the number of domains is greater than the lockout threshold.

User management across forests is only possible when multiple gateways, one for each forest, are deployed. In this case, you can configure the adapters to use a predefined domain for authentication per adapter without requiring the user to specify a domain. To accomplish this, add the following authentication property to the `<AuthnProperties>` element in the resource object's XML:

```
<AuthnProperty name='w2k_domain' dataSource='resource attribute' value='MyDomainName'/>
```

Replace *MyDomainName* with the domain that will authenticate users.

Login failures will occur in domains if the user exists in the domain and the password is not synchronized.

It is not possible to use multiple data sources for the domain information in one Login Module Group.

Correction

In the Active Directory documentation, the "Managing ACL Lists" procedure of this guide contains the following step: (ID-16476)

3. Edit the user in Identity Manager and on the Edit User form.

Replace this sentence with the following:

3. Edit the user in Identity Manager on the Edit User form.

Database Table

- In the Database Table adapter documentation, the example for the Last Fetched Predicate is invalid. It should be defined as follows:

  ```
  lastMod > '$(lastmod)'
  ```

Flat File Active Sync

- The Flat File Active Sync adapter discusses setting the sources.hosts property in the Waveset.properties file. This configuration should now be accomplished using synchronization policy.

Gateway Adapters

The Domino Gateway, Active Directory, Novell NetWare and other gateway adapters allow you to use the RA_HANGTIMEOUT resource attribute to specify a timeout value, in seconds. This attribute controls how long before a request to the gateway times out and is considered hung.

You must manually add this attribute to the Resource object as follows:

```
<ResourceAttribute name='Hang Timeout'
displayName='com.waveset.adapter.RAMessages:RESATTR_HANGTIMEOUT' type='int'
description='com.waveset.adapter.RAMessages:RESATTR_HANGTIMEOUT_HELP' value='NewValue'>
</ResourceAttribute>
```

The default value for this attribute is 0, indicating that Identity Manager will not check for a hung connection.

Mainframe Adapters

A step is missing in the Identity Manager Installation Notes section for the ACF2, Natural, RACF, RACF-LDAP, Scripted Host, and Top Secret adapters. Add the following step after step 3.

4. When the Attachmate libraries are installed into a WebSphere Application Server, add the property com.wrq.profile.dir=*LibraryDirectory* to the WebSphere/AppServer/configuration/config.ini file.

This allows the Attachmate code to find the licensing file.

Microsoft SQL Server

The following information should be added to the Usage Notes section:

Windows authentication mode for the SQL Server resource adapter can only be configured on the Microsoft SQL Server adapter if the Identity Manager server is running on a Windows machine that is included in the same Windows security/authentication framework as the SQL Server server instance.

The JDBC driver supports the use of Type 2 integrated authentication on Windows operating systems through the integratedSecurity connection string property. To use integrated authentication, copy the sqljdbc_auth.dll file to a directory on the Windows system path on the computer where the JDBC driver is installed.

The sqljdbc_auth.dll files are installed in the following location:

InstallationDirectory\sqljdbc_*Version**Language*\auth\

On a 32-bit processor, use the `sqljdbc_auth.dll` file in the x86 folder. On a 64-bit processor, use the `sqljdbc_auth.dll` file in the x64 folder.

For more information, see:

`http://msdn2.microsoft.com/en-us/library/ms378428.aspx`

NetWare

- The NDS adapter has improved support for GroupWise:
  - The adapter can now manage post offices in secondary domains.
  - GroupWise users can subscribe to any known distribution list.
  - A post office can be deleted without specifying a “delete pattern”.
- The NetWare adapter documentation incorrectly states that the Login Script, NRD:Registry Data, and NRD:Registry Index attributes are unsupported. These attributes are supported. (ID-16813)

Oracle

- In the Oracle adapter documentation, the description for the `oracleTempTSQuota` account attribute should be as follows: (ID-12843)

  The maximum amount of temporary tablespace the user can allocate. If the attribute appears in the schema map, the quota is always set on the temporary tablespace. If the attribute is removed from the schema map, no quota will be set on the temporary tablespace. The attribute must be removed for adapters that communicate with Oracle 10gR2 resources.

Oracle ERP

- The Oracle ERP adapter now has an `npw_number` account attribute to support contingent workers. (ID-16507)

Resource User Attribute	Data Type	Description
npw_number	string	Contingent worker number. It represents an npw_number from the per_people_f table. 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 npw_number is entered on create, no linking is attempted. If you enter an npw_number on create and that number is not found, then the adapter throws an exception. The adapter will try to return the npw_number on a getUser, if npw_number is in the adapter schema. **Note:** The employee_number attribute and npw_number attribute are mutually exclusive. If both are entered on create, employee_number takes precedence.

- The Oracle ERP adapter supports Oracle E-Business Suite (EBS) version 12. It is no longer necessary to edit or comment out sections the OracleERPUserForm, depending on version of ERP installed as described in the *Identity Manager Resources Reference*. (16705, 16713)

  The FormRef attribute now supports the following properties:

  - RESOURCE_NAME — Specifies the ERP resource name
  - VERSION - Specifies the version of the ERP resource. Allowed values are 11.5.9, 11.5.10, 12.
  - RESP_DESCR_COL_EXISTS — Defines whether the description column exists in the fnd_user_resp_groups_direct table. This property is required if Version is 11.5.10 or 12. Allows values are TRUE and FALSE.

  These properties should be entered on wherever the user form is being referenced from. For example, the Tabbed User Form may need to be modified in a manner similar to the following to support Release 12.

```
<FormRef name='Oracle ERP User Form'>
   <Property name='RESOURCE_NAME' value='Oracle ERP R12'/>
   <Property name='VERSION' value='12'/>
   <Property name='RESP_DESCR_COL_EXISTS' value='TRUE'/>
</FormRef>
```

Remedy

You must place multiple Remedy API libraries in the directory where the Gateway is installed. These libraries can be found on the Remedy server.

Table 3 Remedy API Libraries

Remedy 4.x and 5.x	Remedy 6.3	Remedy 7.0
• `arapi`*XX*`.dll` • `arrpc`*XX*`.dll` • `arutl`*XX*`.dll` where *XX* matches the version of Remedy. For example, `arapi45.dll` on Remedy 4.5.	• `arapi63.dll` • `arrpc63.dll` • `arutl63.dll` • `icudt20.dll` • `icuin20.dll` • `icuuc20.dll`	• `arapi70.dll` • `arrpc70.dll` • `arutl70.dll` • `icudt32.dll` • `icuin32.dll` • `icuuc32.dll`

SAP

General Notes

The note in step 1 in the Identity Manager Installation Notes procedure is unclear. The wording should be

NOTE Make sure that the JCo toolkit you download matches the bit version of Java your application server runs on. For example, JCo is available in only in the 64-bit version on the Solaris x86 platform. Therefore, your application server must be running the 64-bit version on the Solaris x86 platform.

Renaming Accounts

The SAP adapter now supports renaming accounts. The adapter performs this function by copying an existing account to a new account and deleting the original. SAP discourages renaming accounts, but provides the option in the user management application (Transaction SU01 from the SAP GUI). Therefore, Identity Manager also supports the option. Be aware that SAP may not support the rename feature in future releases.

The SAP GUI uses a different method to perform the rename because it has access to non-public APIs and to the SAP kernel. The following steps provide a high-level description of how the adapter performs the rename operation:

1. Get the user information for the existing user.
2. Save the ALIAS attribute, if one exists.
3. Create the new user.
4. Set the Activity Groups on the new user. (If in CUA mode, get the old user's Activity Groups)
5. Set the Profiles on the new user. (If in CUA mode, get the old user's Profiles.)
6. Get the old user's Personalization Data.
7. Set the new user's Personalization Data.
8. Delete the old user.
9. Set the Alias on the new user if one was set on the old user.

If an error occurs during steps 1-3, the operation fails immediately. If an error occurs during steps 4-7, the new user is deleted and the whole operation fails. (If the new user cannot be deleted, a warning is placed into the WavesetResult). If an error occurs during steps 8-9, a warning is added to the WavesetResult, but the operation succeeds.

The Rename operation requires that a new password be set on the new user. This is most easily accomplished by customizing the Rename User Task to invoke the Change User Password Task.

Sun Java System Access Manager

- The procedure described in the “Policy Agent” section in the Sun Java System Access Manager documentation is outdated. Use the following procedure instead.

  1. From the Identity Manager Administrator Interface menu bar, select **Security**.
  2. Click the **Login** tab.
  3. Click the **Manage Login Module Groups** button, located at the bottom of the page.
  4. Select the Login Module to modify. For example, select Default Identity System ID/Pwd Login Module Group.
  5. In the Assign Login Module select box, select Sun Access Manager Login Module or Sun Access Manager Realm Login Module.

6. When a new Select option displays next to the Assign Login Module option, select the appropriate resource.
7. When the Modify Login Module page displays, edit the displayed fields as needed, and then click **Save**. The Modify Login Module Group is displayed again.
8. Specify Sun Access Manager Login Module as the first resource in the module group, and then click **Save**.

- A step is missing in the procedure listed under the heading "Sun Java System Access Manager Realm Resource Adapter. After you have copied the `amclientsdk.jar` file to the **`InstallDir`**`/WEB-INF/lib` directory (step 4), you must restart Identity Manager's application server.
- References to Policy Agent 2.1 should be changed to Policy Agent 2.2.

Sun Java System Access Manager Realm

The *Identity Manager Resources Reference* contains outdated links. Use the following links instead:

- Policy agent downloads: `http://wwws.sun.com/software/download/inter_ecom.html#dirserv`
- Policy agent documentation: `http://docs.sun.com/app/docs/coll/1322.1`

In the Installation Notes section, the procedure for configuring the Sun Java System Access Manager Realm Resource Adapter has been updated as follows:

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`
5. Add the `amclientsdk.jar` file to the server class path.
6. Restart the Identity Manager application server.

7. After copying the files, you must add the Sun Java System Access Manager Realm resource to the Identity Manager resources list. Add the following value in the Custom Resources section of the Configure Managed Resources page.

   ```
   com.waveset.adapter.SunAccessManagerRealmResourceAdapter
   ```

The procedure described in the "Policy Agent" section is outdated. Use the following procedure instead.

1. From the Identity Manager Administrator Interface menu bar, select **Security**.
2. Click the **Login** tab.
3. Click the **Manage Login Module Groups** button, located at the bottom of the page.
4. Select the Login Module to modify. For example, select Default Identity System ID/Pwd Login Module Group.
5. In the Assign Login Module select box, select Sun Access Manager Login Module or Sun Access Manager Realm Login Module.
6. When a new Select option displays next to the Assign Login Module option, select the appropriate resource.
7. When the Modify Login Module page displays, edit the displayed fields as needed, and then click **Save**. The Modify Login Module Group is displayed again.
8. Specify Sun Access Manager Realm Login Module as the first resource in the module group, and then click **Save**.

UNIX Adapters

The documentation for the AIX, HPUX, Solaris, and Linux adapters previously stated that if you are using sudo, the NOPASSWORD option must be specified for each command the adapter uses. This is incorrect.

Synchronizing LDAP Passwords

Identity Manager now supports LDAP password synchronization Directory Server 5.2 SP5 and later. The Configure Password Synchronization page contains a new field, **Directory Server version**, which allows you to specify whether your Directory Server instance is 5.2 P4 or earlier, or 5.2 P5 or later.

Note the following documentation changes:

- In the procedure “Step 2: Enable Password Synchronization Features”, a new numbered step should be added between steps 6 and 7 that states you must select an option from the **Directory Server version** pull-down menu.
- The section titled “Installing the Password Capture Plugin” should be re-titled to “Installing and Configuring the Password Capture Plugin.” The first sentence in the first note in that section should end with “then the plugin must be installed and configured on each master replica.”

  Step 2 in this section should begin “For Directory Server version 5.2 P4 or earlier only, place the plugin binary (`idm-plugin.so`) on the host where the Directory Server is running.”
- The following paragraph and note should be added to the end of the “Installing and Configuring the Password Capture Plugin” section:

  After the Password Capture plugin is enabled, clients must have the MODIFY right to both the `userPassword` and the `idmpasswd` attribute to make password changes. Adjust the access control information settings in your directory tree accordingly. This is usually necessary if administrators other than the directory manager have the ability to update the password of other users.

  NOTE Directory Server must be restarted whenever you make changes to the plugin configuration.

Identity Manager Technical Deployment Overview

This section contains new information and documentation corrections for *Sun Java™* System *Identity Manager Technical Deployment Overview*:

- You can use CSS to set column widths in the User list and Resource list tables to a fixed pixel or percentage value. To do so, add the following style classes (commented out by default) to `customStyle.css`. You can then edit the values to meet the user's requirements.

```
th#UserListTreeContent_Col0 {
            width: 1px;
}

th#UserListTreeContent_Col1 {
            width: 1px;
}

th#UserListTreeContent_Col2 {
            width: 50%;
}

th#UserListTreeContent_Col3 {
            width: 50%;
}

th#ResourceListTreeContent_Col0 {
            width: 1px;
}

th#ResourceListTreeContent_Col1 {
            width: 1px;
}

th#ResourceListTreeContent_Col2 {
            width: 33%;
}

th#ResourceListTreeContent_Col3 {
            width: 33%;
}

th#ResourceListTreeContent_Col4 {
            width: 33%;
}
```

You can also resize table columns by clicking and dragging the right border of the column header. If you mouse over the right border of the column header, the cursor will change to a horizontal resize arrow. Left-click and drag the cursor will resize the column. (Resizing ends when you release the mouse button.)

- Customers who want to use custom JavaScript functions specifically in the end user navigation bar (tabs) must reference that form using `endUserNavigation`. For example, `document.forms['endUserNavigation'].elements`. (ID-13769)
- The System Configuration object now contains the `security.delegation.historyLength` attribute, which controls the number of previous delegations that are recorded.
- The Access Review Dashboard and Access Review Detail Report both show instances of reviews that are recorded in the audit logs. Without database maintenance, the audit logs are never trimmed, and the list of reviews grows. Identity Manager provides the ability to limit the reviews shown to a certain age range. To change this limit, you must customize `compliance/dashboard.jsp` (for the dashboard) and `sample/auditortasks.xml` (for the Details report). (The default is to show only reviews that are less than 2 years old.)

  To restrict the reviews included in the Access Review Dashboard, customize `compliance/dashboard.jsp` as follows:

  a. Open `compliance/dashboard.jsp` in either the Identity Manager IDE or editor of your choice:

  b. Change the line: `form.setOption("maxAge", "2y");` to `form.setOption("maxAge", "6M");` to limit the list to reviews run in the last 6 months. The qualifiers are:

  - m - minute
  - h - hour
  - d - day
  - w - week
  - M - month
  - y - year

  To show all reviews that still exist in the audit logs, comment out this line.

  To restrict the reviews included in the Access Review Detail Report,

  a. Open sample/auditortasks.xml in either the IDE or editor of your choice.

  b. Change the following line as indicated:

```
<s>maxAge</s>
  <s>2y</s>
```

to

```
<s>maxAge</s>
  <s>6M</s>
```

to limit reviews to the last 6 months. The same qualifiers as above apply.

Each Periodic Access Review includes a set of UserEntitlement records that were created when the review was run. These records, which accumulate over time, provide valuable historical information about accounts. However, to conserve database space, consider deleting some records. You can delete a record by executing **Server Task > Run Task > Delete Access Review**. Deleting a review adds new audit log entries that indicate the review is deleted, and deletes all UserEntitlement records associated with the review, which conserves database space.

- In the section "Changing Background Image on the Login Page", the third line of code should read:

  ```
  url(../images/other/login-backimage2.jpg)
  ```

- Code Example 5-5 contains information that should appear in Code Example 5-4. Code Example 5-4 should be as follows:

Code Example 5-4 Customizing Navigation Tabs

```
/* LEVEL 1 TABS */
.TabLvl1Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#333366;
    padding:6px 10px 0px;
}
a.TabLvl1Lnk:link, a.TabLvl1Lnk:visited  {
    display:block;
    padding:4px 10px 3px;
    font: bold 0.95em sans-serif;
    color:#FFF;
    text-decoration:none;
    text-align:center;
}
table.TabLvl1Tbl td {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#666699;
    border:solid 1px #aba1b5;
}
table.TabLvl1Tbl td.TabLvl1TblSelTd {
    background-color:#9999CC;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
```

Code Example 5-4 Customizing Navigation Tabs *(Continued)*

```
    border-bottom:none;
}

/* LEVEL 2 TABS */
.TabLvl2Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#9999CC;
    padding:6px 0px 0px 10px
}
a.TabLvl2Lnk:link, a.TabLvl2Lnk:visited{
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    text-decoration:none;
    text-align:center;
}
table.TabLvl2Tbl div.TabLvl2SelTxt {
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    font-weight:normal;
    text-align:center;
}
table.TabLvl2Tbl td {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#CCCCFF;
    border:solid 1px #aba1b5;
}
table.TabLvl2Tbl td.TabLvl2TblSelTd {
    border-bottom:none;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#FFF;
    border-left:solid 1px #aba1b5;
    border-right:solid 1px #aba1b5;
    border-top:solid 1px #aba1b5;
```

Code Example 5.5 should be as follows:

Code Example 5-5 Changing Tab Panel Tabs

```
table.Tab2TblNew td
{background-image:url(../images/other/dot.gif);background-repeat:repeat-x;background-positi
on:left top;background-color:#CCCCFF;border:solid 1px #8f989f}
table.Tab2TblNew td.Tab2TblSelTd
{border-bottom:none;background-image:url(../images/other/dot.gif);background-repeat:repeat-
x;background-position:left bottom;background-color:#FFF;border-left:solid 1px
#8f989f;border-right:solid 1px #8f989f;border-top:solid 1px #8f989f}
```

- In the Identity Manager End User Interface, the horizontal navigation bar is driven by the End User Navigation UserForm in `enduser.xml`. (ID-12415)

  `userHeader.jsp`, which is included in all the end user pages, includes another JSP named `menuStart.jsp`. This JSP accesses two system configuration objects:

  - `ui.web.user.showMenu` - Toggles the display of the navigation menu on/off (default: true)
  - `ui.web.user.menuLayout` - Determines whether the menu is rendered as horizontal navigation bar with tabs (the default: `horizontal`) or a vertical tree menu (`vertical`)

  The CSS style classes that determine how the menu is rendered are in `style.css`.

- Identity Manager now calls the **Lighthouse** account the **Identity Manager** account. You can override this name change through the use of a custom catalog. (ID-14918) See *Enabling Internationalization* in *Identity Manager Technical Deployment Overview* for information on custom catalogs.

  The following catalog entries control the display of the product name:

  PRODUCT_NAME=Identity Manager

  LIGHTHOUSE_DISPLAY_NAME=[PRODUCT_NAME]

  LIGHTHOUSE_TYPE_DISPLAY_NAME=[PRODUCT_NAME]

  LIGHTHOUSE_DEFAULT_POLICY=Default [PRODUCT_NAME] Account Policy

- Identity Manager now provides a new configuration object (`WorkItemTypes` configuration object) that specifies all supported work item type names, extensions, and display names. (ID-15468) This configuration object is defined in `sample/workItemTypes.xml`, which is imported by `init.xml` and `update.xml`.

The `extends` attribute allows for a hierarchy of work item types (`workItem` Types). When Identity Manager creates a work item, it delegates the work item to the specified users if its `workItem` type is:

- the type delegated
- one of the subordinate `workItem` types of the type being delegated.

workItem Type	Description	Display Name
Approval	extends WorkItem	Approval
OrganizationApproval	extends Approval	Organization Approval
ResourceApproval	extends Approval	Resource Approval
RoleApproval	extends Approval	Role Approval
Attestation	WorkItem	Access Review Attestation
review	WorkItem	Remediation
accessReviewRemediation	WorkItem	Access

- The code sample included in the section titled “Changing Masthead Appearance” incorrectly lists the first line as “MstDiv”. This line should read “.MstDiv”. (ID-16072)
- The section titled Customizing the Browser bar has been revised as follows: (ID-16073)

  You can now replace the product name string in the browser title bar with a localizable string of your choice.

1. Import the following XML file:

Code Example 1 XML to Import

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Configuration name='AltMsgCatalog'>
 <Extension>
 <CustomCatalog id='AltMsgCatalog' enabled='true'>
 <MessageSet language='en' country='US'>
 <Msg id='UI_BROWSER_TITLE_PROD_NAME_OVERRIDE'>Override Name</Msg>
    </MessageSet>
 </CustomCatalog>
</Configuration>
</Extension>
```

2. Using the Identity Manager IDE, load the System Configuration object for editing. Add a new top-level attribute:

   ```
   Name = customMessageCatalog

   Type = string

   Value = AltMsgCatalog
   ```

3. Open the ui.web Generic Object and look for the `browserTitleProdNameOverride` attribute. Set this value to true.

4. Save this change to the System Configuration object, and restart your application server.

- By default, Identity Manager's anonymous enrollment processing generates values for `accountId` and `emailAddress` by using user-supplied first (`firstName`) and last names (`lastName`) as well as `employeeId`. (ID-16131)

  Because anonymous enrollment processing can result in the inclusion of non-ASCII characters in email addresses and account IDs, international users should modify EndUserRuleLibrary rules so that Identity Manager maintains ASCII account IDs and email addresses during anonymous enrollment processing.

  To maintain account ID and email address values in ASCII during anonymous enrollment processing, follow these two steps:

1. Edit the following three rules within the EndUserRuleLibrary as indicated below:

Edit this rule	To make this change...
`getAccountId`	To use `employeeId` only (and remove `firstName` and `lastName`)
`getEmailAddress`	To use `employeeId` only (remove `firstName`, `lastName`, and ".")
`verifyFirstname`	To change length check from 2 to 1 to allow for single character Asian first names

2. Edit the End User Anon Enrollment Completion form to remove the `firstName` and `lastName` arguments from calls to the getAccountId and getEmailAddress rules.

- The discussion of how to customize the login pages in Chapter 5 “Private Labeling of Identity Manager” should include the following information about message keys. (ID-16702)

JSP or Identity Manager Component	Interface Affected	Message Key
Login Page TITLE	Administrator and User	UI_LOGIN_TITLE_TO_RESOURCE
		UI_LOGIN_CHALLENGE
Login Page SUBTITLE	Administrator and User	Select a key depending on the login mode: Forgot Password, Forgot User ID, Login Challenge.
		UI_LOGIN_WELCOME3
		UI_LOGIN_WELCOME4
		UI_LOGIN_WELCOME5
		UI_LOGIN_WELCOME6
		UI_LOGIN_CHALLENGE_INFO
staticLogout.jsp and user/staticUserLogout.jsp	Administrator and User	UI_LOGIN_TITLE
continueLogin.jsp	Administrator	UI_LOGIN_IN_PROGRESS_TITLE
		UI_LOGIN_WELCOME

The following keys are no longer used:

- UI_LOGIN_TITLE_LONG
- UI_LOGIN_WELCOME2.

Identity Manager Workflows, Forms, and Views

This section contains new information and documentation corrections for *Sun Java™* System *Identity Manager Workflows, Forms, and Views*.

- You can turn off policy checking in your user form by adding the following field to the form: (ID-13346)

```
<Field name='viewOptions.CallViewValidators'>
  <Display class='Hidden'/>
    <Expansion>
        <s>false</s>
    </Expansion>
</Field>
```

  This field overrides the value in the OP_CALL_VIEW_VALIDATORS field of `modify.jsp`.

- The Identity Manager User Interface pages include a second XPRESS form that implements the navigation bar. As a result, the rendered page contains two `<FORM>` tags, each with a different name attribute:

  `<form name="endUserNavigation">` and `<form name="mainform">`

  To avoid potential confusion between these two `<FORM>` elements, make sure you use the `name` attribute as follows to distinguish which `<FORM>` you are referencing: `document.mainform` or `document.endUserNavigation`.

Chapter 1, Identity Manager Workflow

- Identity Manager provides the following new sample Access Review workflow in /sample/workflows. (ID-15393)

  Test Auto Attestation

  Use to test new Review Determination rules without creating Attestation work items. This workflow does not create any work items, and simply terminates shortly after it starts. It leaves all User Entitlement objects in the same state that they were created in by the access scan. Use the Terminate and Delete options to clean up the results from access scans run with this workflow.

You can import this stub workflow as needed. (Identity Manager does not import it automatically.)

- Identity Manager Compliance uses workflows as integration and customization points for the application. The default compliance-related workflows are described below. (ID-15447)

Workflow Name	Purpose
Remediation	Remediation for a single Remediator working with a single Compliance Violation
Access Review Remediation	Remediation for a single remediator working with a single UserEntitlement
Attestation	Attestation for a single Attestor working with a single UserEntitlement
Multi Remediation	Remediation for a single Compliance Violation and multiple remediators
Update Compliance Violation	Mitigates a Compliance Violation
Launch Access Scan	Launch an Access Scan task from an Access Review task
Launch Entitlement Rescan	Launch a rescan of an Access Scan for a single user
Launch Violation Rescan	Launch a rescan of an Audit Policy Scan for a single user

- The description of the maxSteps property has been revised as follows: (ID-15618)

  Specifies the maximum number of steps allowed in any workflow process or subprocess. Once this level is exceeded, Identity Manager terminates the workflow. This setting is used as a safeguard for detecting when a workflow is stuck in an infinite loop. The default value set in the workflow itself is 0, which indicates that Identity Manager should pull the actual setting value from the global setting stored in the SystemConfiguration object's `workflow.maxSteps` attribute. The value of this global setting is 5000.

- This chapter now contains the following description of the Scripted Task Executor task. (ID-15258)

  Executes Beanshell or JavaScript based on the script provided. As a task, it can be scheduled to run periodically. For example, you can use it to export data from the repository to a database for reporting and analysis. Benefits include the ability to write a custom task without writing custom Java code. (Custom Java code requires a re-compile on every upgrade and must be deployed to every server because the script is embedded in the task there is no need to recompile or deploy it.)

Chapter 2, Workflow Services

- The Arguments table of the `createView` Session Workflow Service is incorrect. The following table describes the arguments available in this service.(ID-14201)

Table 1

Name	Required	Valid Values	Description
`op`	yes	`createView`	
`viewId`	yes		Specifies the type of view to create.
`options`	no		Specifies view-specific options. The values you can pass are specific to the view being used. The most common is the User view. Options can be found in `session.UserViewConstants`. The simpler views should declare their option constants in the `Viewer.java` file. Probably the second most common view used from workflow is ProcessViewer, followed by PasswordViewer, DisableViewer, EnableViewer, and RenameViewer. These have comparatively few options

- The description of the `disableUser` Workflow Service should clarify that the default behavior of this service is to disable the Identity Manager account as well as the resource account. (ID-14572) If you do not want to disable the Identity Manager account, pass the following argument:

```
<Argument name='doWaveset' value='false'/>
```

The discussion of this method's arguments should read as follows:

Name	Required	Valid Values	Description
op	yes	disableUser	
accountId	yes		Identifies the Identity Manager user to disable accounts for.
doWaveset	no	true/false	If `true`, the Identity Manager account is disabled for this user. If not supplied, it defaults to `true`, and the account is disabled.
services	no		Identifies a list of resources to disable. If this argument is not supplied, all of the user's resource accounts will be disabled.

- This document incorrectly represents the `viewId` attribute of the `checkoutView` and `createView` methods as "*viewid*". Note that the correct spelling of this parameter is *viewId*. (ID-15411)
- This chapter now contains the following description of the lock and unlock workflow services.(ID-17070)

lock Provisioning Workflow Service

Use to lock an object.

Argument	Required	Description
subject	no	Indicates the effective subject for the call. If not supplied, Identity Manager uses the task's *subject*. If the value of this argument is none, Identity Manager performs no authorization.
options	no	(Map) A value map of option name/option value pairs. If not supplied, specific arguments below are used. If supplied, any specific arguments below will override the same argument contained in this options map.
accountId	no	(String) Identifies the name of the Identity Manager user to lock.
adminName	no	(String) Indicates the name of the administrator performing the operation.
loginAppName	no	(String) Specifies the login application name.
op	yes	Valid value is *unlock*

This method returns a null value.

unlock Workflow Service

Use to unlock a locked object.

Table 1

Argument	Required	Description
subject	no	(String) Indicates the effective subject for the call. If not supplied, the task's subject is used. If the value of this argument is none, then no authorization is performed.
options	no	(Map) A value map of option name/option value pairs. If not supplied, Identity Manager uses the specific arguments below. If supplied, any specific arguments below will override the same argument contained in this options map.
accountId	no	(String) Identifies the name of the Identity Manager user to unlock.

Table 1

Argument	Required	Description
adminName	no	(String) Indicates the name of the administrator performing the operation
loginAppName	no	(String) Specifies the login application name.
doLighthouse	no	(Boolean) Indicates whether or not to unlock the Identity Manager account.
doResources	no	(Boolean) Indicates whether or not to unlock the user's resources.
doAuthenticators	no	(Boolean) If true, unlocks all pass-through authentication.
op	yes	Valid value is *unlock.*

This method returns a WavesetResult with the result of the operation.

- The description of the removeDeferredTask session workflow service has been revised as follows: (ID-17302)

  Used to remove a deferred task from an Identity Manager object. Identity Manager will ensure that the administrator that launched the workflow is authorized to remove the object.

Table 2 removeDeferredTask Method Arguments

Name	Required	Valid Values	Description
type	no	valid values are the list of types	Specifies the type of the object that the deferred task will be removed from. If not supplied, the type is defaulted to *user.*
name	yes		Specifies the name of the object that the deferred task will be removed from.
task			Specifies the name of the TaskDefinition to remove.

Chapter 3, Identity Manager Forms

- This chapter now contains the following description of forms used in auditing and compliance procedures. (ID-15447, 16240)

  Identity Manager auditing and compliance forms provide a feature unique among Identity Manager forms: You can assign a form on a per-user and per-organization basis. Forms assigned on a per-user basis can boost the efficiency of attestation and remediation processing.

  For example, you can specify the user form that Identity Manager displays for editing a user in the context of an access review, remediation or a compliance violation remediation. You can specify this user form at the level of user or organization. When Identity Manager re-scans a user in context of an access review re-scan or access review remediation, the re-scan will respect the audit policies as defined in the AccessScan. You can define this to include the continuous compliance audit policies.

  NOTE To configure auditing components, you must be an Identity Manager administrator with the Configure Audit and Auditor Administrator capabilities.

Related Information

- See *Identity Manager Administration* for a discussion of the concepts that support Identity Manager auditing and compliance features as well as the basic procedures for implementing the default auditing and compliance features.
- See Identity Manager Rules in *Identity Manager Deployment Tools* for a general discussion of rules as well as specific information about remediation rules.

About Auditing-Related Form Processing

Much like `userForm` and `viewUserForm`, you can set the form on a specific user, or on an organization, and the user (or all users in the organization) will used that form. If you set a form on both user and organization, the form set on the user takes precedence. (When looking up the form, Identity Manager searches organizations upwards.)

Auditing-related forms behave the same way that the User Form and View User Form work: Each user can designate a specific form to use, and the resolution of which form a specific user should use will honor the user's organization.

Specifying User Forms

The Audit Policy List and Access Scan List forms support a `fullView` property that causes the form to display a significant amount of data about the elements in the list. Set this policy to `false` to improve the performance of the list viewer.

The Access Approval List form has a similar property named `includeUE`, and the Remediation List form uses the `includeCV` property.

Default Auditing-Related Forms

The following table identifies the default auditing-related forms that ship with Identity Manager.

Table 2

Form Name	Mapped Name	Per-User Control	General Purpose
Access Approval List	accessApprovalList		Display the list of attestation workitems
Access Review Delete Confirmation	accessReviewDeleteConfirmation		Confirm the deletion of an access review
Access Review Abort Confirmation	accessReviewAbortConfirmation		Confirm the termination of an access review
Access Review Dashboard	accessReviewDashboard		Show the list of all access reviews
Access Review Remediation Form	accessReviewRemediationWorkItem	Yes	renders each UE-based remediation workitem
Access Review Summary	accessReviewSummary		Show the details of a specific access review
Access Scan Form	accessScanForm		Display or edit an access scan
Access Scan List	accessScanList		Show the list of all access scans
Access Scan Delete Confirmation	accessScanDeleteConfirmation		Confirm the deletion of an access scan
Access Approval List	attestationList	Yes	Renders the list of all pending attestations.
Attestation Form	attestationWorkItem	Yes	Renders each attestation work item
UserEntitlementForm	userEntitlementForm		Display the contents of a UserEntitlement
UserEntitlement Summary Form	userEntitlementSummaryForm		

Table 2

Form Name	Mapped Name	Per-User Control	General Purpose
Violation Detail Form	violationDetailForm		Show the details of a compliance violation
Remediation List	remediationList	Yes	Show a list of remediation work items
Audit Policy List	auditPolicyList		Show a list of audit policies
Audit Policy Delete Confirmation Form	auditPolicyDeleteConfirmation		Confirm the deletion of an audit policy
Conflict Violation Details Form	conflictViolationDetailsForm		Show the SOD violation matrix
Compliance Violation Summary Form	complianceViolationSummaryForm		
Remediation Form	reviewWorkItem	Yes	Renders a compliance violation.

Why Customize These Forms?

Attestors and remediators can specify forms that show exactly the detail they need to more efficiently attest and remediate. For example, a resource attestor could show specific resource-specific attributes in the list form to allow them to attest without looking at each specific work item. Because this form would differ depending on the resource type (and thus attributes) involved, customizing the form on a per-attestor basis makes sense.

During attestation, each attestor can look at entitlements from a unique perspective. For example, the `idmManager` attestor may be looking at the user entitlement in a general way, but a resource attestor is interested only in resource-specific data. Allowing each attestor to tailor both the Attestation-list form and the AttestationWorkItem form to retrieve and display only the information they need can boost the efficiency of the product interface.

Scan Task Variables

The Audit Policy Scan Task and Access Scan Task task definitions both specify the forms to be used when initiating the task. These forms include fields that allow for most, but not all, of the scan task variables to be controlled.

Variable Name	Default Value	Purpose
`maxThreads`	5	Identifies the number of concurrent users to work at one time for a single scanner. Increase this value to potentially increase throughput when scanning users with accounts on very slow resources.
`userLock`	5000	Indicates time (in mS) spent trying to obtain lock on user to be scanned. If several concurrent scans are scanning the same user, and the user has resources that are slow, increasing this value can result in fewer lock errors, but a slower overall scan.
`scanDelay`	0	Indicates time (in mS) to delay between issuing new scan threads. Can be set to a positive number to force Scanner to be less CPU-hungry.

- The description of the Disable element has been revised as follows: (ID-14920)

  Calculates a Boolean value. If true, the field and all its nested fields will be ignored during current form processing.

  Do not create potentially long-running activities in Disable elements. These expressions run each time the form is recalculated. Instead, use a different form element that will not run as frequently perform this calculation.

- The section titled “Inserting Javascript into a Form” incorrectly states that you can include JavaScript in your form with a `<JavaScript>` tag (ID-15741). Alternatively, include JavaScript as follows:

```
<Field>
   <Expansion>
      <script>
.............
```

NOTE The display.session and display.subject variables are not available to Disable form elements.

- You can now insert WARNING), error (ERROR), or informational (OK) alert messages into an XPRESS form. (ID-14540, ID-14953)

NOTE Although this example illustrates how to insert a Warning `ErrorMessage` object into a form, you can assign a different severity level.

1. Use the Identity Manager IDE to open the form to which you want to add the warning.
2. Add the `<Property name='messages'>` to the main EditForm or HtmlPage display class.
3. Add the `<defvar name='msgList'>` code block from the following sample code.
4. Substitute the message key that identifies the message text to be displayed in the Alert box in the code sample string:

   `<message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE >`
5. Save and close the file.

Code Example

```
<Display class='EditForm'>
   <Property name='componentTableWidth' value='100%'/>
   <Property name='rowPolarity' value='false'/>
   <Property name='requiredMarkerLocation' value='left'/>
   <Property name='messages'>
     <ref>msgList</ref>
   </Property>
</Display>
<defvar name='msgList'>
  <cond>
    <and>
      <notnull>
        <ref>username</ref>
      </notnull>
      <isnull>
        <ref>userview</ref>
      </isnull>
    </and>
    <list>
      <new class='com.waveset.msgcat.ErrorMessage'>
        <invoke class='com.waveset.msgcat.Severity' name='fromString'>
           <s>warning</s>
        </invoke>
        <message name='UI_USER_REQUESTS_ACCOUNTID_NOT_FOUND_ALERT_VALUE'>
          <ref>username</ref>
        </message>
      </new>
    </list>
  </cond>
</defvar>
```

To display a severity level other than warning, replace the <s>warning</s> in the preceding example with either of the these two values:

- error -- Causes Identity Manager to render an InlineAlert with a red "error" icon.
- ok -- Results in an InlineAlert with a blue informational icon for messages that can indicate either success or another non-critical message.

Identity Manager renders this as an InlineAlert with a warning icon

```
<invoke class='com.waveset.msgcat.Severity' name='fromString'>
   <s>warning</s>
</invoke>
```

where warning can also be error or ok.

- This chapter now contains the following description of the Hidden display component:

  The Hidden display class corresponds to the <input type=hidden'/> HTML component. This component supports only single-valued data types because there is no way to reliably serialize and deserialize multi-valued data types. (ID-16904)

  If you have a List that you want to render it as a string, you must explicitly convert it to a string. For example:

Code Example 0-1 Rendering Multi-Value Data Type with the Hidden Display Component

```
<Field name='testHiddenFieldList' >
     <Display class='Hidden'/ >
     <Derivation>
          <invoke name='toString'> <List> <String>aaaa</String> <String>bbbb</String>
</List> </invoke>
     </Derivation>
</Field>
```

- You can now set the RequiresChallenge property in the End User Interface Change Password Form to require users to reenter their current password before changing the password on their account. For an example of how to set this property, see the Basic Change Password Form in enduser.xml. (ID-17309)

Chapter 4, Identity Manager Views

- The description of the Org view has been updated as follows: (ID-13584)

  Used to specify the type of organization created and options for processing it.

Common Attributes

The high-level attributes of the Org view are listed in the following table.

Name	Editable?	Data Type	Required?
orgName	Read	String	System-Generated
orgDisplayName	Read/Write	String	Yes
orgType	Read/Write	String	No
orgId	Read	String	System-Generated
orgAction	Write	String	No
orgNewDisplayName	Write	String	No
orgParentName	Read/Write	String	No
orgChildOrgNames	Read	List	System-Generated
orgApprovers	Read/Write	List	No
allowsOrgApprovers	Read	List	System-Generated
allowedOrgApproverIds	Read	List	System-Generated
orgUserForm	Read/Write	String	No
orgViewUserForm	Read/Write	String	No
orgPolicies	Read/Write	List	No
orgAuditPolicies	Read/Write	List	No
renameCreate	Read/Write	String	No
renameSaveAs	Read/Write	String	No

orgName

Identifies the UID for the organization.This value differs from most view object names because organizations can have the same short name, but different parent organizations.

orgDisplayName

Specifies the short name of the organization. This value is used for display purposes only and does not need to be unique.

orgType

Defines the organization type where the allowed values are `junction` or `virtual`. Organizations that are not of types `junction` or `virtual` have no value.

orgId

Specifies the ID that is used to uniquely identify the organization within Identity Manager.

orgAction

Supported only for directory junctions, virtual organizations, and dynamic organizations. Allowed value is `refresh`. When an organization is a directory junction or virtual organization, the behavior of the refresh operation depends on the value of `orgRefreshAllOrgsUserMembers`.

orgNewDisplayName

Specifies the new short name when you are renaming the organization.

orgParentName

Identifies the full pathname of the parent organization.

orgChildOrgNames

Lists the Identity Manager interface names of all direct and indirect child organizations.

orgApprovers

Lists the Identity Manager administrators who are required to approve users added to or modified in this organization.

allowedOrgApprovers

Lists the potential user names who could be approvers for users added to or modified in this organization.

allowedOrgApproverIds

Lists the potential user IDs who could be approvers for users added to or modified in this organization.

orgUserForm

Specifies the `userForm` used by members users of this organization when creating or editing users.

orgViewUserForm

Specifies the view user form that is used by member users of this organization when viewing users.

orgPolicies

Identifies policies that apply to all member users of this organization. This is a list of objects that are keyed by type string: Each policy object contains the following view attributes, which are prefixed by `orgPolicies[<type>].` `<type>` represents policy type (for example, Lighthouse account).

- `policyName` -- Specifies name
- `id` -- Indicates ID
- `implementation` -- Identifies the class that implements this policy.

orgAuditPolicies

Specifies the audit policies that apply to all member users of this organization.

renameCreate

When set to true, clones this organization and creates a new one using the value of `orgNewDisplayName`.

renameSaveAs

When set to true, renames this organization using the value of `orgNewDisplayName`.

Directory Junction and Virtual Organization Attributes

Name	Editable?	Data Type	Required?
orgContainerId	Read	String	System-generated
orgContainerTypes	Read	List	System-generated
orgContainers	Read	List	System-generated
orgParentContainerId	Read	String	System-generated
orgResource	Read/Write	String	yes, if directory junction or virtual organization
orgResourceType	Read	String	System-generated
orgResourceId	Read	String	System-generated
orgRefreshAllOrgsUserMembers	Write	String	No

orgContainerId

Specifies the dn of the associated LDAP directory container (for example, cn=foo,ou=bar,o=foobar.com).

orgContainerTypes

Lists the allowed resource object types that can contain other resource objects.

orgContainers

Lists the base containers for the resource used by the Identity Manager interface to display a list to choose from.

orgParentContainerId

Specifies the dn of the associated parent LDAP directory container (for example, ou=bar,o=foobar.com).

orgResource

Specifies the name of the Identity Manager resource used to synchronize directory junction and virtual organizations (for example, West Directory Server).

orgResourceType

Indicates the type of Identity Manager Resource from which to synchronize directory junction and virtual organizations (for example, LDAP).

orgResourceId

Specifies the ID of the Identity Manager resource that is used to synchronize directory junctions and virtual organizations.

orgRefreshAllOrgsUserMembers

If `true` and if the value of `orgAction` is `refresh`, synchronizes Identity organization user membership with resource container user membership for the selected organization and all child organizations. If `false`, resource container user membership will not be synchronized, only the resource containers to Identity organizations for the selected organization and all child organizations.

Dynamic Organization Attributes

Name	Editable?	Data Type	Required?
orgUserMembersRule	Read/Write	String	No
orgUserMembersRuleCacheTimeout	Read/Write	String	No

orgUserMembersRule

Identifies (by name or UID) the rule whose `authType` is UserMembersRule, which is evaluated at run-time to determine user membership.

orgUserMembersCacheTimeout

Specifies the amount of time (in milliseconds) before the cache times out if the user members returned by the orgUserMembersRule are to be cached. A value of 0 indicates no caching.

The discussion of the User view now includes the following discussion of the `accounts[Lighthouse].delegates` attributes: (ID-15468)

accounts[Lighthouse].delegates

Lists delegate objects, indexed by `workItemType`, where each object specifies delegate information for a specific type of work item

- If `delegatedApproversRule` is the value of `delegateApproversTo`, identifies the selected rule.
- If `manager` is the value of `delegateApproversTo`, this attribute has no value.

accounts[Lighthouse].delegatesHistory

Lists delegate objects, indexed from 0 to *n*, where *n* is the current number of delegate history objects up to the delegate history depth

This attribute has one unique attribute: `selected`, which is a Boolean that indicates the currently selected delegate history object.

accounts[Lighthouse].delegatesOriginal

Original list of delegate objects, indexed by `workItemType`, following a get operation or checkout view operation.

All `accounts[Lighthouse].delegates*` attributes take the following attributes:

Attributes of accounts[Lighthouse].delegate* Attributes	**Description**
`workItemType`	Identifies the type of `workItem` being delegated. See the description of the Delegate Object Model in the *Identity Manager Technical Deployment Overview* section of this Documentation Addendum for a valid list of `workItem` types.
`workItemTypeObjects`	Lists the names of the specific roles, resources, or organizations on which the user is delegating future `workItem` approval requests. This attribute is valid when the value of `workItemType` is `roleApproval`, `resourceApproval`, or `organizationApproval`. If not specified, this attribute by default specifies the delegation of future `workItem` requests on all roles, resources, or organizations on which this user is an approver.

Attributes of accounts[Lighthouse].delegate* Attributes	Description
toType	Type to delegate to. Valid values are: manager delegateWorkItemsRule selectedUsers
toUsers	Lists the names of the users to delegate to (if toType is selectedUsers) .
toRule	Specifies the name of the rule that will be evaluated to determine the set of users to delegate to (if toType is delegateWorkItemsRule).
startDate	Specifies the date when delegation will start.
endDate	Specifies the date when delegation will end.

Referencing a DelegateWorkItems View Object from a Form

The following code sample illustrates how to reference a DelegateWorkItems view delegate object from a form:

```
<Field name='delegates[*].workItemType'>
<Field name='delegates[*].workItemTypeObjects'>
<Field name='delegates[*].toType'>
<Field name='delegates[*].toUsers'>
<Field name='delegates[*].toRule'>
<Field name='delegates[*].startDate'>
<Field name='delegates[*].endDate'>
```

where supported index values (*) are workItemType values.

- This chapter now contains the following description of the User Entitlement view:

  Use to create and modify UserEntitlement objects.

  This view has the following top-level attributes:

Name	Editable?	Type	Required?
name		String	Yes
status		String	Yes

Name	Editable?	Type	Required?
user		String	Yes
userId		String	Yes
attestorHint		String	No
userView		GenericObject	Yes
reviewInstanceId		String	Yes
reviewStartDate		String	Yes
scanId		String	Yes
scanInstanceId		String	Yes
approvalWorkflowName		String	Yes
organizationId		String	Yes
attestorComments.name		String	No
attestorComments.attestor		String	No
attestorComments.time		String	No
attestorComments.timestamp		String	No
attestorComments.status			No

name

Identifies the User Entitlement (by a unique identifier).

status

Specifies the state of User Entitlement object. Valid states include PENDING, ACCEPTED, REJECTED, REMEDIATING, CANCELLED.

user

Identifies the name of the associated WSUser for this entitlement.

userId

Specifies the ID of the associated WSUser.

attestorHint

Displays the (String) hint to the attestor that is provided by the Review Determination Rule. This hints acts as “advice” from the rule to the attestor.

userView

Contains the User view that is captured by User Entitlement scanner. This view contains zero or more resource accounts depending on the configuration of the Access Scan object.

reviewInstanceId

Specifies the ID of the PAR Task instance.

reviewStartDate

Indicates the (String) start date of the PAR task (in canonical format).

scanId

Specifies the ID of AccessScan Task definition.

scanInstanceId

Specifies the ID of AccessScan Task instance.

approvalWorkflowName

Identifies the name of workflow to be run for approval. This value comes from the Access Scan Task definition.

organizationId

Specifies the ID of the WSUser's organization at the time of the scan.

attestorComments

Lists attestation records for the entitlement. Each attestation record indicates an action or statement made about the entitlement, including approval, rejection, and rescan.

attestorComments[timestamp].name

Timestamp used to identify this element in the list.

attestorComments[timestamp].attestor

Identifies the WSUser name of the attestor making the comment on the entitlement.

attestorComments[timestamp].time

Specifies the time at which the attestor attested this record. May differ from the timestamp.

attestorComments[timestamp].status

Indicates the status assigned by the attestor. This can be any string, but typically is a string that indicates the action taken by the attestor -- for example, approve, reject, rescan, remediate.

attestorComments[name].comment

Contains comments added by attestor.

- The following User view attributes have been deprecated. (ID-15468)
- `accounts[Lighthouse].delegateApproversTo`
- `accounts[Lighthouse].delegateApproversSelected`
- `accounts[Lighthouse].delegateApproversStartDate`
- `accounts[Lighthouse].delegateApproversEndDate`
- The Delegate Approvers view has been deprecated, but still works for editing Delegate objects whose `workItemType` is `approval`.

  The existing User View `accounts[Lighthouse].delegate*` attributes are deprecated and no longer available via the User View. Use the new `accounts[Lighthouse].delegates` view.

Chapter 6, XPRESS Language

- This chapter has been substantially updated. See the.pdf titled XPRESS in the same directory as these Release Notes.
- The description of the isTrue function should be revised as follows: (ID-17078)

  Used when referencing Boolean values that are represented with the strings true and false rather than the numbers 0 and 1. Takes one argument.

  - `0` – the argument is logically false. The following are considered true: the string `true`, a Boolean true, and a non-zero integer. (Anything else is considered false.)
  - `1` – the argument is logically true.

  Example

  The following expression returns 0.

```
<isTrue>
   <s>false</s>
</isTrue>
```

Chapter 8, HTML Display Components

- The following discussion about an alternative to the MultiSelect component has been added to this chapter:

  It can be unwieldy to display many admin roles using the MultiSelect component (either the applet or HTML version). Identity Manager provides a more scalable way of displaying and managing admin roles: the `objectSelector` field template. (ID-15433)

  The Scalable Selection Library (in `sample/formlib.xml`) includes an example of using an `objectSelector` field template to search for admin role names that a user can select.

Code Example Example of objectSelector Field Template

```
<Field name='scalableWaveset.adminRoles'>
  <FieldRef name='objectSelector'>
     <Property name='selectorTitle' value='_FM_ADMIN_ROLES'/>
     <Property name='selectorFieldName' value='waveset.adminRoles'/>
     <Property name='selectorObjectType' value='AdminRole'/>
     <Property name='selectorMultiValued' value='true'/>
     <Property name='selectorAllowManualEntry' value='true'/>
     <Property name='selectorFixedConditions'>
       <appendAll>
         <new class='com.waveset.object.AttributeCondition'>
           <s>hidden</s>
           <s>notEquals</s>
           <s>true</s>
         </new>
         <map>
           <s>onlyAssignedToCurrentSubject</s>
           <Boolean>true</Boolean>
         </map>
       </appendAll>
     </Property>
     <Property name='selectorFixedInclusions'>
       <appendAll>
         <ref>waveset.original.adminRoles</ref>
       </appendAll>
     </Property>
  </FieldRef>
</Field>
```

How to Use the objectSelector Example Code

1. From the Identity Manager IDE, open the Administrator Library UserForm object.
2. Add the following code to this form:

```
<Include>
   <ObjectRef type='UserForm' name='Scalable Selection Library'/>
</Include>
```

3. Select the `accounts[Lighthouse].adminRoles` field within the `AdministratorFields` field.
4. Replace the entire `accounts[Lighthouse].adminRoles` with the following reference:

```
<FieldRef name='scalableWaveset.adminRoles'/>
```

5. Save the object.

   When you subsequently edit a user and select the Security tab, Identity Manager displays the customized form. Clicking ... opens the Selector component and exposes a search field. Use this field to search for admin roles that begin with a text string and set the value of the field to one or more values.

   To restore the form, import `$WSHOME/sample/formlib.xml` from **Configure > Import Exchange File**.

   See the Scalable Selection Library in `sample/formlib.xml` for other examples of using the `objectSelector` template to manage resources and roles in environments with many objects.

- The discussion of the `TabPanel` component now contains the following description of the `validatePerTab` property: (ID-15501)

  `validatePerTab` -- When set to true, Identity Manager performs validation expressions as soon as the user switches to a different tab.

- The discussion of the MultiSelect component now contains the following description of the `displayCase` property: (ID-14854)

  `displayCase` – Maps each of the allowedValues to their uppercase or lowercase equivalents. Takes one of these two values: upper and lower.

- The following discussion of the Menu component has been added to this chapter: (ID-13043)

  Consists of three classes: `Menu`, `MenuBar`, and `MenuItem`.

  - `Menu` refers to the entire component.
  - `MenuItem` is a leaf, or node, that corresponds to a tab on the first or second level.
  - `MenuBar` corresponds to a tab that contains `MenuBars`, or `MenuItems`.

  `Menu` contains the following properties:

  - `layout` - A String with value `horizontal` or `vertical`. A value of `horizontal` generates a horizontal navigation bar with tabs. A value of `vertical` causes the menu to be rendered as a vertical tree menu with typical node layout.
  - `stylePrefix` - String prefix for the CSS class name. For the Identity Manager End User pages, this value is `User`.

  `MenuBar` contains the following properties:

  - `default` - A String URL path that corresponds to one of the MenuBar's MenuItem URL properties. This controls which subtab is displayed as `selected` by default when the `MenuBar` tab is clicked.

  `MenuItem` contains the following properties:

  - `containedUrls` - A List of URL path(s) to JSPs that are "related" to the MenuItem. The current MenuItem will be rendered as "selected" if any of the `containedUrls` JSPs are rendered. An example is the request launch results page that is displayed after a workflow is launched from the request launch page.

  You can set these properties on either a `MenuBar` or `MenuItem`:

  - `title` - Specifies the text String displayed in the tab or tree leaf as a hyperlink
  - `URL` - Specifies the String URL path for the title hyperlink

The following XPRESS example creates a menu with two tabs. The second tab contain two subtabs:

Code Example Implementation of Menu, MenuItem, and MenuBar Components

```
<Display class='Menu'/>
<Field>
   <Display class='MenuItem'>
     <Property name='URL' value='user/main.jsp'/>
     <Property name='title' value='Home' />
   </Display>
</Field>
<Field>
    <Display class='MenuBar' >
      <Property name='title' value='Work Items' />
     <Property name='URL' value='user/workItemListExt.jsp' />
   </Display>
    <Field>
       <Display class='MenuItem'>
         <Property name='URL' value='user/workItemListExt.jsp'/>
         <Property name='title' value='Approvals' />
        </Display>
     </Field>
    <Field>
      <Display class='MenuItem'>
         <Property name='URL' value='user/otherWorkItems/listOtherWorkItems.jsp'/>
          <Property name='title' value='Other' />
       </Display>
    </Field>
 </Field>
```

- The following discussion of the ListEditor component has been added to this chapter: (ID-16518)

ListEditor

Renders an editable list of strings.

Table 3 Properties of the ListEditor Component

Property	Description
`listTitle`	(String) Specifies the label that Identity Manager places next to the ListEditor graphical representation.
`pickListTitle`	(String) Specifies the label to use on the `picklist` component.
`valueMap`	(Map) Specifies a map of display labels for the values in the list.
`allowDuplicates`	(Boolean) A value of `true` indicates that Identity Manager allows duplicates in the managed list

Table 3 Properties of the ListEditor Component

Property	Description
`allowTextEntry`	(Boolean) A value of `true` indicates that Identity Manager displays a text entry box, along with an add button.
`fixedWidth`	(Boolean) A value of `true` indicates that the component should be of fixed width (same behavior as `Multiselect` component).
`ordered`	(Boolean) A value of `true` indicates that the order of values is important.
`sorted`	(Boolean) A value of `true` indicates that the values should be sorted in the pick list. If values are multi-valued and not ordered, Identity Manager also sorts the value list.
`pickValueMap`	(List or Map) Specifies a map of display labels for the values in the pick list.
`pickValues`	(List) Specifies the available values in the `picklist` component. If null, the `picklist` is not shown
`height`	(Integer) Specifies preferred height.
`width`	(Integer) Specifies the preferred width. Can be used by the Container as a property of the table cell in which this item is rendered

Example

The following example from the Tabbed User Form shows a form field that uses the ListEditor display class:

```
<Field name='accounts[Sim1].Group'>
     <Display class='ListEditor' action='true'>
        <Property name='listTitle' value='stuff'/>
        <Property name='allowTextEntry'>
            <Boolean>true</Boolean>
        </Property>
        <Property name='ordered'>
            <Boolean>true</Boolean>
        </Property>
     </Display>
     <Expansion>
         <ref>accounts[Sim1].Group</ref>
     </Expansion>
</Field>
```

This code snippet creates a field where the customer can add groups to or remove them from a user.

NOTE This display class typically requires a List of Strings as input. To coerce a single String into a List of Strings:

```
<Expansion>
   <appendAll><ref>accounts[Sim1].Group</ref></appendAll>
</Expansion>
```

- The `Text` display component contains the new `autocomplete` property. (ID-17310) Setting the `autocomplete` property to `off` prevents browsers from offering to store the user's credentials on their computer.

  You can implement this feature in input fields in XPRESS by adding this display property. Any value other than `off` prevents Identity Manager from rendering the `autocomplete` attribute in the rendered HTML from (which is the same as not setting the property).

Enabling autocomplete for Identity Manager Login Pages

You can enable this feature for the Identity Manager login pages by changing the `ui.web.disableAutocomplete` system configuration object to `true`. Identity Manager login pages include `login.jsp`, `continueLogin.jsp`, `user/login.jsp`, and `user/continueLogin.jsp`.

Identity Manager login forms other than the preceding ones are generated from XPRESS, and you must edit these forms to use the new display property. These forms, which reside in the sample directory, include this property commented out by default.

- Anonymous User Login
- Question Login Form
- End User Anonymous Enrollment Validation Form
- End User Anonymous Enrollment Completion Form
- Lookup Userid

Appendix A, Form and Process Mappings

- An updated version of this appendix, titled Form and Process Mappings, is included in the same directory as these Release Notes.
- You can access compliance-specific tasks through the mapped names. (ID-15447)

Process Name	Mapped Name	Description
Access Review	accessReview	Performs an access review
Access Scan	accessReviewScan	Performs an access scan
Access Review Rescan	accessReviewRescan	Performs an access rescan
Audit Policy Rescan	auditPolicyRescan	Performs an audit policy rescan
Abort Access Review	abortAccessReview	Terminates an access review
Delete Access Review	deleteAccessReview	Deletes an access review
Recover Access Review	recoverAccessReview	Recovers missing access review status objects from audit logs

Identity Manager Deployment Tools

This section provides corrections and additions to the *Identity Manager Deployment Tools* documentation:.

Chapter 1, Using the Identity Manager IDE

- The "Palette Window" and "Properties Window" sections should include GenericObjects in the list of elements provided in the first paragraph of both sections, as follows: (ID-14817)
  - The Palette window (such as Figure 1-11) enables you to "drag-and-drop" elements into Email Template, Form, *GenericObjects*, Library, Workflow Process, or Workflow Subprocess objects displayed in the Editor windows — without having to type XML.
  - The Identity Manager IDE Properties window consists of a properties sheet for XML elements associated with Email Template, Form, *GenericObjects*, Library, Rule, Workflow Process, and Workflow Subprocess objects. You can use this properties sheet to view and edit a selected object's properties; including the object name, file sizes, modification times, result information, and so forth.

- Several files in the Identity Manager project were changed for 7.1 Update 1; and if you modified any of these files, you must manually merge the changes when you upgrade from the Identity Manager IDE plugin version 7.1 to version 7.1 Update 1.

  The following instructions describe the "best practices" for upgrading Identity Manager IDE Plugin version 7.1 projects to version 7.1 Update 1 (and later). (ID-16850)

Upgrading Version 7.1 Projects to Version 7.1 Update 1

This section describes the "best practices" procedure for upgrading the Identity Manager IDE Plugin 7.1 version of the Identity Manager Project to Version 7.1 Update 1 (and later).

NOTE The instructions in this section only describe how to upgrade the *Identity Manager IDE Plugin* version. They do not explain how to upgrade Identity Manager, which is a much more involved process.

To upgrade your current Identity Manager version, refer to the instructions provided in *Identity Manager Upgrade*.

The following Identity Manager project files were changed for Identity Manager version 7.1 Update 1:

- `build.xml`
- `nbproject/project.xml`
- `build-netbeans.xml`
- `custom-init.incremental.xml`
- `build-config.properties`
- `custom-init-common.xml`
- `custom-init-full.xml`

If you modified any of these files, you must manually merge the changes when you upgrade the Identity Manager IDE plugin from version 7.1 to version 7.1 Update 1 (or later).

NOTE The `build.xml`, `build-netbeans.xml`, and `nbproject/project.xml` files are subject to change from release to release, so avoid changing theses files if at all possible.

This section describes the "best practices" procedure for upgrading the Identity Manager IDE Plugin version of the Identity Manager project.

NOTE The procedures in this section describe how to upgrade the *Identity Manager IDE Plugin* version only. They do not explain how to upgrade Identity Manager, which is a much more involved process.

For example, if you want to use a project created with the 7.1 version of the Identity Manager IDE plugin with the version 7.1 Update 1 plugin, use the following instructions.

Your Identity Manager version will remain at 7.1 unless you upgrade using instructions provided in *Identity Manager Upgrade*.

This upgrade procedure assumes that your project is checked in to source control, and the instructions are divided into two sections:

- Steps to be Performed by One Deployment Team Member
- Steps to be Performed by Other Deployment Team Members

Steps to be Performed by One Deployment Team Member

One person on your deployment team should perform the following steps:

1. Shut down NetBeans.
2. Delete the `.netbeans` directory.
3. Install the new `nbm`.
4. Start NetBeans.
5. Open the project.

   A message displays to inform you that several project files (such as `build.xml` and `build-netbeans.xml` must be upgraded, and provides `merge needed` indicators if any of the files have been modified.
6. Note which files have merge needed indicators, and then click Yes.

   A message displays to let you know that the upgrade was successful.
7. If you have any `merge needed` files, manually merge those files.

   Your copy of each file will be named `<filename>.bak` and so you can `diff` it with the new file version to determine what needs to be merged.
8. When you are finished, and everything is back up and working, check all of the files you changed or added into source control.

NOTE For a complete list of the files that should be checked into source control, read the "CVS Best Practices" section provided in the `README.txt`.

Steps to be Performed by Other Deployment Team Members

After someone upgrades the new Identity Manager IDE 7.1 Update 1 plugin `nbm` file and merges the necessary project files, the remaining members of the deployment team should perform the following steps:

1. Perform a full source control update of the project.
2. Shut down NetBeans.
3. Delete the `.netbeans` directory.
4. Install the new `nbm`.
5. Start NetBeans.
6. Open the project.

- The "Unable to Delete Errors" troubleshooting information provided in the "Troubleshooting Identity Manager IDE" section is no longer applicable. Now, the Netbeans embedded application server automatically shuts down whenever you perform any of the following project operations (ID-16851, 16738):
  - Clean Project
  - Create Delta Distribution
  - Create Jar
  - Debug Project
  - Manage Embedded Repository
  - Profile Project
  - Run Project

- Identity Manager now provides a Profiler utility to help you troubleshoot performance problems with forms, Java, rules, workflows, and XPRESS in your deployment. The following section should be added to Chapter 1, Using the Identity Manager IDE (ID-16764):

Using the Profiler to Troubleshoot Performance Problems

Identity Manager provides a Profiler utility to help you troubleshoot performance problems with forms, Java, rules, workflows, and XPRESS in your deployment.

Forms, Java, rules, workflows, and XPRESS can all cause performance and scale problems. The Profiler profiles how much time is spent in different areas of your forms and workflows, enabling you to determine if these forms or workflows are contributing to performance and scale problems and, if so, which parts of these objects are causing the problems.

This section explains how to use Identity Manager's Profiler and provides a tutorial to help you learn how to troubleshoot performance issues in your deployment. The information is organized as follows:

Overview

The section provides an overview of the Identity Manager's Profiler's features and functionality. The information is organized as follows:

Main Features

You can use the Profiler utility to

- Create "snapshots" of profiling data.

  A *snapshot* is the cumulative result of profiling since the last time you reset all of your collected profile results.

- You an display snapshot results in four, different data views:

- **Call Tree view** provides a tree table showing the call timing and invocations counts throughout the system.
- **Hotspots view** provides a flattened list of nodes that shows the aggregate call timings regardless of parent.
- **Back Traces view** provides an inverted call stack showing all the call chains from which that node (known as the *root node*) was called.
- **Callees view** provides an aggregate call tree of the root node, regardless of its parent chain.

- Specify what kinds of information to include in your snapshot:
  - You can include every element of form, workflow, and XPRESS or restrict the content to a set of specific elements.
  - You can pick specific Java methods and constructors to include or exclude from the instrumentation. Instrumentation of Identity Manager classes and custom classes is supported.
- Manage your project snapshots as follows:
  - Save the snapshot in your project's `nbproject/private/idm-profiler` directory or to an arbitrary location outside of your project.

    NOTE You can view a list of all saved snapshots in the Saved Snapshots section of the IDM Profiler view.

  - Open snapshots from your project or load them from an arbitrary location outside your project.
  - Delete snapshots.
- Search for specific nodes, by name.

How the Profiler Locates and Manages Source

This section describes how the Profiler looks up and manages the source for the following Identity Manager objects:

- For Forms, Rules, Workflows, and XPRESS Objects
- For Java Source

TIP In Call Tree view or Hotspots view, you can double-click any node that corresponds to a Java method, workflow, form, rule, or XPRESS to view the source for that node.

For Forms, Rules, Workflows, and XPRESS Objects

When you take a snapshot with the Profiler, the server evaluates all of the profiling data and discovers on which sources the data depends. The server then fetches all of these sources from the repository and includes them in the snapshot. Consequently, you can be sure that the Identity Manager objects displayed in the snapshot are accurately reflecting the point at which the snapshot was captured.

This process adds to the size of the snapshot, but the source size is actually a relatively small fraction of the total size. As a result, you can send a snapshot to Sun's Customer Support without having to send your source files separately.

For Java Source

NOTE In a Java source snapshot, do not assume the source is up-to-date with the server or always available.

When you take a snapshot of Java source, the client downloads the snapshot and then goes through the snapshot to capture all referenced Java sources from the project. When you save the snapshot, the client zips the sources and attaches them to the end of the snapshot.

Then, when you view the snapshot and go to the Java source, the client first checks the content of the snapshot. If the client cannot find the content there, it checks the project's content. This process allows you to send a snapshot containing profiling data from both your custom Java code and Identity Manager code.

Statistics Caveats

The following sections contain information to consider when you evaluate results provided by the Profiler:

- Self Time Statistics
- Constructor Calls
- Daemon Threads

Self Time Statistics

To compute a root node's Self Time statistic, the Profiler subtracts the times of all children nodes from the root node's total time.

Consequently, an uninstrumented child node's time is reflected in the root node's self time. If a root node has a significant self time, you should certainly investigate why. You might not have the proper methods instrumented and so you are looking in the wrong place.

For example, assume method A calls method B.

Method A takes a total time of 10 seconds (where total time includes the call to B) and the call to B takes a total time of 10 seconds.

If both A and B are instrumented, the call stack reflects that information. You will see that A has a self-time of 0 seconds and that B has a self-time of 10 seconds (where 10 seconds was actually spent in B). If, however, B is not instrumented, you only see that the call to A takes 10 seconds and that A's self-time is 10 seconds. Consequently, you might assume the problem lies directly in A rather than in B.

In particular, you might notice large self times on JSPs during their initial compile. If you reset the collected results and then redisplay the page, the self time value will be much less.

Constructor Calls

Because there are limitations in the Java instrumentation strategy, initial calls to `this()` or `super()` will appear as a sibling to the constructor call, rather than as a child. See the following example:

```
class A
{
   public A()
   {
      this(0);
   }
   public A(int i)
   {
   }
}

and:

class B
{
   public static void test()
   {
      new A();
   }
}
The call tree will look like this:
B.test()
   -A.<init>(int)
   -A.<init>()
Rather than this:
B.test()
   -A.<init>()
      -A.<init>(int)
```

Daemon Threads

Do not be mislead by the seemingly large amount of time spent in a number of Identity Manager's daemon threads, such as `ReconTask.WorkerThread.run()` or `TaskThread.WorkerThread.run()`. Most of this time is spent sleeping, while waiting for events. You must explore these traces to see how much time is actually spent when they are processing an event.

Getting Started

This section describes how to start the profiler and how to work with various features of the Profiler's graphical user interface. This information is organized as follows:

Before You Begin

Because the Profiler is very memory intensive, you should significantly increase the memory for both your server and the Netbeans Java Virtual Machine (JVM).

- To increase your server's memory,
  a. Open the Netbeans window and select the Runtime tab.
  b. Expand the Servers node, right-click Bundled Tomcat, and select Properties from the menu.
  c. When the Server Manager dialog displays, clear the Enable HTTP Monitor box on the Connection tab.
  d. Select the Platform tab, and then set VM Options to **`-Xmx1024M`**.
  e. Click Close.
- To increase the Netbeans JVM memory,
  a. Open the *netbeans-installation-dir*`\etc\netbeans.conf` file and locate the following line:

     ```
     netbeans_default_options="-J-Xms32m -J-Xmx ...
     ```

  b. Change the `-J-Xmx` value to `-J-Xmx`**`1024M`**.
  c. Save, and then close the file.

When you are finished, you can start the Profiler as described in the next section.

Starting the Profiler

You can use any of the following methods to start the Profiler:

- Click the Start Identity Manager Profiler on Main Project icon  located on the menu bar.

NOTE	The Start Identity Manager Profiler on Main Project icon is enabled when the main Identity Manager project is version 7.1 Update 1 or later.

- Select Window > IDM Profiler from the menu bar.

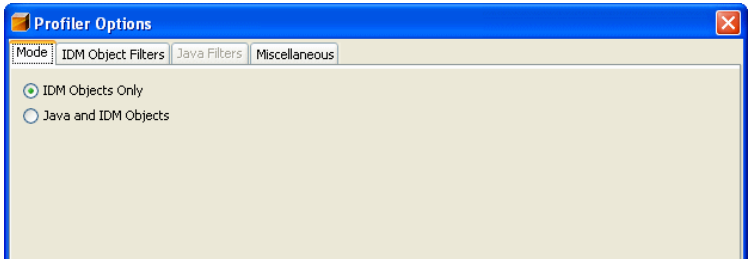
  The Identity Manager Profiler window appears in the Explorer. From this window, select an Identity Manager project from Current Project drop-down menu, and then click the Start Identity Manager Profiler icon located in the Controls section.

- Right-click a project in the Projects window, and then select Start Identity Manager Profiler from the pop-up menu.

- Select a project in the Projects window, and then select IdM > Start Identity Manager Profiler from the menu bar.

When you start the Profiler, the Profiler Options dialog displays so you can specify which profiling options you want to use.

Figure 3 Profiler Options Dialog



See "Specifying the Profiler Options" for information about setting these options.

Using the Profiler

This section describes the features of the Profiler graphical user interface, and how to use these features. The information is organized as follows:

Specifying the Profiler Options

The Profiler Options dialog consists of the following tabs:

- Mode
- IDM Object Filters
- Java Filters
- Miscellaneous

Use the options on these tabs to indicate which objects to profile and which elements to display in the profile.

After specifying the Profiler options, click OK to start the Profiler. Depending on your project configuration, the Profiler does one of two things:

- If you are using a regular Identity Manager project with an *Embedded* Identity Manager Instance, the Profiler performs a full build, deploys into the NetBean's application server, and starts the Profiler.
- If you are using a regular Identity Manager project with an *External* Identity Manager Instance or the remote Identity Manager project, the Profiler attaches to the Identity Manager instance configured for the project.

NOTE You can select IdM > Set Identity Manager Instance to control the Identity Manager Instance action for the project.

Mode

The Mode tab provides the following options:

- **IDM Objects Only**: Select to profile form, rule, workflow, and XPRESS objects. Excludes Java objects from the profile.
- **Java and IDM Objects**: Select to profile form, Java, rule, workflow, and XPRESS objects.

NOTE

- The Java and IDM Objects option is not available if you are using a regular Identity Manager project with an *external* Identity Manager instance or using a remote Identity Manager project.
- You cannot change the Mode option while the Profiler is running. You must stop the Profiler to change the option.

IDM Object Filters

The IDM Object Filters tab provides the following options:

- **Show IDM Object details**:
  - Select this box to include every executed form, workflow, and XPRESS element in the snapshot.
  - Clear this box to include only the following elements in the snapshot:
    - `<invoke>`
    - `<new>`
    - `<Rule>`
    - `<Form>`
    - `<WFProcess>`
    - `<ExScript>`
    - `<ExDefun>`
    - `<FieldRef>`
    - `<Action>` (for workflow application callouts)
- **Include Anonymous Sources**:

NOTE	*Anonymous sources* are forms (or portions of a form) that are generated on the fly (such as Login forms and MissingFields forms) and do not correspond to a persistent form that resides in the Identity Manager repository.

  - Select this box to include Anonymous sources in the snapshot.
  - Clear this box to exclude Anonymous sources from the snapshot.

Java Filters

Select the Java Filters tab to

- Include or exclude Java filters
- Create new filters
- Delete existing filters
- Restore the default filters

Java filters are given in terms of method patterns, and they are expressed in patterns that include or exclude based on *canonical method name*. Where a canonical method name is:

fully-qualified-class-name.method-name(*parameter-type-1*, *parameter-type-2*, ...)

NOTE For constructors, *method-name* is `<init>`.

Here are a few examples:

- To exclude all constructors, enable the Exclude box and add the following filter:

  ```
  *.<init>(*)
  ```

- To exclude all constructors with a single `org.w3c.dom.Element` parameter, enable the Exclude box and add the following filter:

  ```
  *.<init>(org.w3c.dom.Element)
  ```

- To exclude all Identity Manager classes, enable the Exclude box and add the following filters:

  ```
  "com.waveset.*"
  ```

  ```
  "com.sun.idm.*"
  ```

- To instrument your custom code only, disable the Exclude box, remove the initial `* include` filter, and then add the following filter:

  ```
  "com.yourcompany.*"
  ```

  NOTE The last two examples are currently equivalent because the filters are applied only to your custom classes and Identity Manager classes.

If necessary, you can instrument other JARs by modifying the following lines in `build.xml` as appropriate. For example,

```
<instrument todir="${lighthouse-dir-profiler}/WEB-INF"
verbose="${instrumentor.verbose}" includeMethods="${profiler.includes}"
excludeMethods="${profiler.excludes}">
           <fileset dir="${lighthouse-dir}/WEB-INF">
               <include name="lib/idm*.jar"/>
               <include name="classes/**/*.class"/>
           </fileset>
</instrument>
```

By default, the configuration includes all your custom classes and most Identity Manager classes. A number of Identity Manager classes are forcibly excluded — because enabling them would break the Profiler.

For example, classes from the workflow, forms, and XPRESS engines are excluded or the Profiler would produce an unintelligible snapshot when profiling Java and Identity Manager objects.

Note that Java filters provide much more filtering granularity than IDM Object Filters. Java instrumentation adds *significant* overhead to the execution time, which can drastically skew the profiling results. Because Identity Manager objects are interpreted rather than compiled, the instrumentation overhead is negligible. So for example, there is basically no reason to exclude workflow A and include workflow B, and so forth.

NOTE You cannot modify Java filters while the Profiler is running. You must stop the Profiler before changing Java filters.

Miscellaneous

The Miscellaneous tab provides the following options:

- **Prune snapshot nodes where execution time is 0**:
  - Disable this option (default) if you want the snapshot to include invocation information for all executed entities — even those whose execution time is zero.

    It might be useful to have the number of invocations, even for nodes where there is no execution time.
  - Enable this option to remove these nodes, which allows you to focus on the most relevant profiling data. In addition, enabling this option can provide a large savings in Profiler snapshot size.
- **Automatically Open Browser Upon Profiler Start**:
  - Enable this option (default) when you launch the Profiler to automatically open a browser that points to the Identity Manager instance being profiled.
  - Disable this option if you do not want to open a browser.
- **Include Java Sources in Snapshot**:
  - Enable this option (default) to include Java sources for any Java methods referenced by the profiling data in the Snapshot. You should always use this setting for snapshots in the field. Custom Java is relatively small and it is very valuable to have for support.

- Disable this option only if you are profiling Identity Manager and have the complete Identity Manager source available.

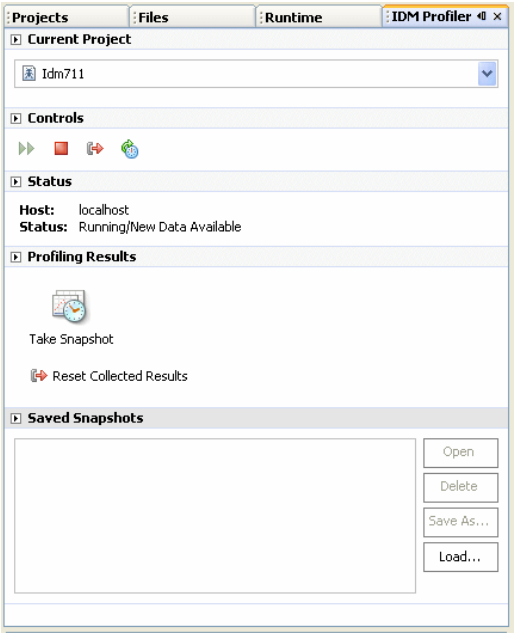
  In this situation, you do not want to include the Identity Manager source because it can create extremely large snapshots. (See "How the Profiler Locates and Manages Source" on page 148 for more information.)

Working with the IDM Profiler View

The IDM Profiler view (Figure 3) consists of the following areas:

- Current Project Area
- Controls Area
- Status Area
- Saved Snapshots Area

Figure 4 IDM Profiler View



Current Project Area

The Current Project area consists of a drop-down menu that lists all of your current projects. Use this menu to select the project you want to profile.

Controls Area

The Controls area contains four icons:

Table 4 Controls Area Icons

Icon		Purpose
	Start Identity Manager Profiler	Starts the Profiler and opens the Profiler Options dialog.
	Stop Identity Manager Profiler	Stops the Profiler.
	Reset Collected Results	Resets all of the profile results you collected to this point.
	Modify Profiling	Re-opens the Profiler Options dialog so you can change any of the settings to modify your current profile results.

Status Area

The Status area reports whether you are connected to the Host and provides Status information as the Profiler is starting up, running, and stopping.

Profiling Results Area

The Profiling Results area contains two icons:

Table 5 Profiling Results Area Icons

Icon		Purpose
	Start Identity Manager Profiler	Starts the Profiler and opens the Profiler Options dialog.
	Reset Collected Results	Resets all of the profile results you collected to this point.

Saved Snapshots Area

The Saved Snapshots area provides a list of all saved snapshots. In addition, you can use the following buttons to manage these snapshots:

- **Open**: Click to open saved snapshots in the Snapshot View window.

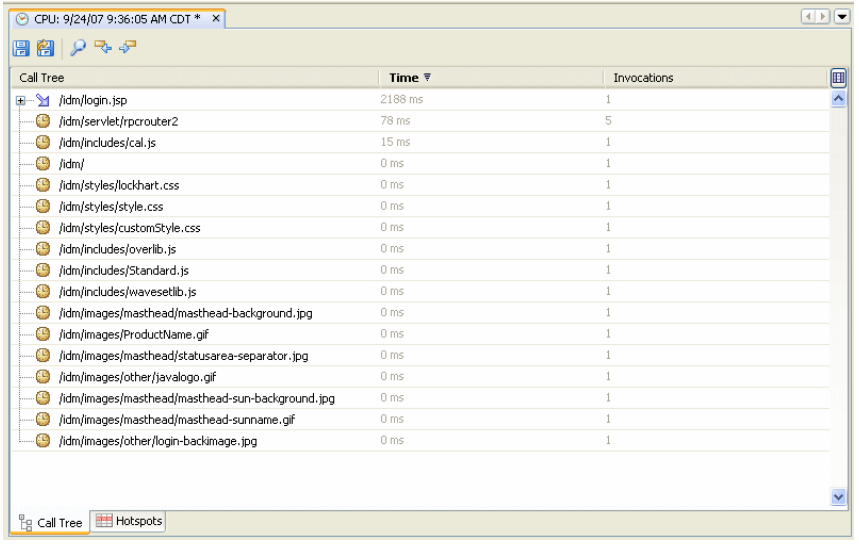
TIP	You can also double-click a snapshot in the Saved Snapshots list to open that snapshot.

- **Delete**: Select a snapshot in the Saved Snapshots list, and then click this button to delete the selected snapshot.
- **Save As**: Select a snapshot in the list and then click this button to save that snapshot externally to an arbitrary location.
- **Load**: Click to open a snapshot from an arbitrary location into the Snapshot View window.

Working with the Snapshot View

When you open a snapshot, the results display in the Snapshot View window, located on the upper right side of Identity Manager IDE.

Figure 5 Snapshot View Window



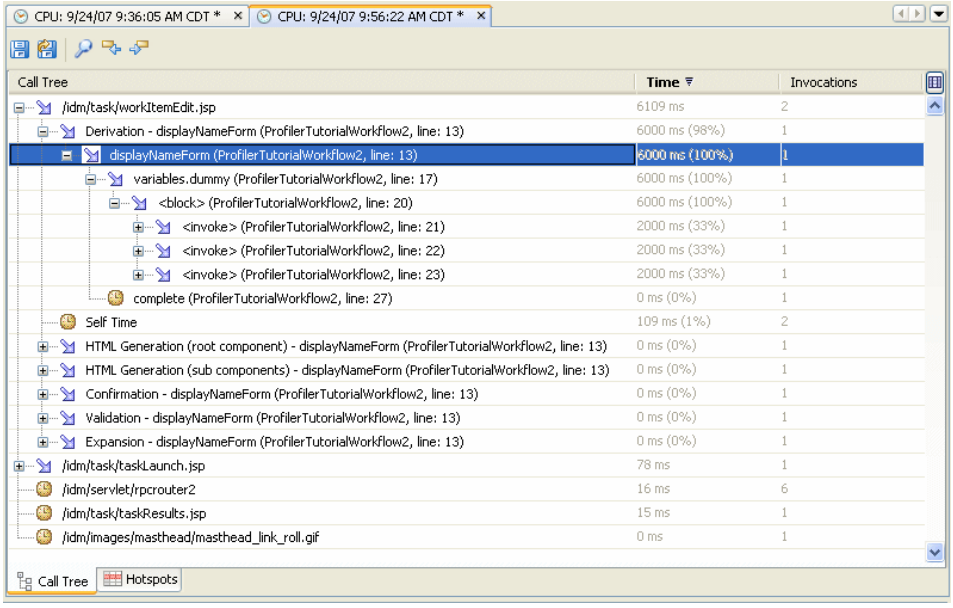
A snapshot provides several views of your data, which are described in the following sections:

- Call Tree View
- Hotspots View
- Back Traces View
- Callees View

Call Tree View

Call Tree view (Figure 5) consists of a tree table showing the call timing and invocation counts throughout your system.

Figure 6 Example Call Tree View



This tree table contains three columns:

- **Call Tree column**: Lists all nodes, where the top-level nodes are one of the following:
  - `Thread.run()` methods for various background threads in the system.

    For example, if you enable Java profiling, you will see the `ReconTask.WorkerThread.run()` method.
  - Request timings

    For example, if you view the `idm/login.jsp` URL, you will see a top-level entry for `idm/login.jsp`. For this entry, the data displayed in the Time column represents the total time for that request (or requests), and the data displayed in the Invocations column represents the total number of invocations to that page. You can explore further into that data to see what calls contributed to its time.

NOTE The Call Tree also contains Self Time nodes. Self Time values represent how much time was spent in the node itself. (For more information, see "Self Time Statistics" on page 150.)

- **Time column**: Lists the time spent in each node when that node was called from its parent. The percentages are given relative to parent time.
- **Invocations column**: Lists how many times each node was invoked from its parent.

Hotspots View

Hotspots view provides a flattened list of nodes that shows aggregate call timings regardless of parent.

This view contains the following columns:

- **Self Time**: Lists the total amount of time spent in each node.
- **Invocations**: Lists the total number of times each node was invoked from its parent.
- **Time**: Lists the total amount of time spent in each node and in all of its children.

Back Traces View

Back Traces view provides an inverted call stack showing all the call chains from where each node was called.

You can use these statistics to answer the question — How much time would I save if I eliminated this particular call chain from this node?

You can access the Back Traces view from any of the other snapshot views by right-clicking a node (known as the *root node*) and selecting Show Back Traces from the pop-up menu.

NOTE The Time and Invocations data values mean something different in Back Traces view:

- **Time**: The values in this column represent the time spent in the root node when it is called from a given call chain.
- **Invocations**: The values in this column represent how many times the root node was invoked from a given call chain.

Callees View

Callees view provides an aggregate call tree for a node (known as the *root node*), regardless of its parent chain.

These statistics are helpful if you have a problem area that is called from many places throughout the master call tree and you want to see the overall profile for that node.

You can access the Callees view from any of the other snapshot views by right-clicking a node (known as the *root node*) and selecting Show Callees from the pop-up menu.

NOTE The Time and Invocations data values used in Callees view have the same meaning as those used in Call Tree view.

Using the Pop-Up Menu Options

Right-click any node in Call Tree view or in Hotspots view and a pop-up menu displays with the options described in Table 6:

Table 7 Profiler Pop-Up Menu Options

Menu Options	Description
GoTo Source	Select this option to view the XML source for a node that corresponds to a Java method, workflow, form, rule, or XPRESS. For detailed information about this view, see "How the Profiler Locates and Manages Source" on page 148.
Show Back Traces	Select this option to access the Back Traces view. For detailed information about this view, see "Back Traces View" on page 162.
Show Callees	Select this option to access the Callees view. For detailed information about this view, see "Callees View" on page 163.

Table 7 Profiler Pop-Up Menu Options *(Continued)*

Menu Options	Description
Find In Hotspots	Select this option to find a node in the Hotspots view. For detailed information about this view, see "Hotspots View" on page 162.
List Options > Sort >	Select this option to • None • Call Tree • Time • Invocations • Ascending • Descending
List Options > Change Visible Columns	Select this option to change the columns displayed in the Call Tree or Hotspots list. When the Change Visible Columns dialog displays, you can select one or more of the following options: • Call Tree: Call Tree • Invocations: Invocations • Time: Time

Searching a Snapshot

Use the Search icon  , located at the top of the Snapshot View window to search for nodes by name the Call Tree view or Hotspots tree.

Alternatively, right-click any node in Call Tree view or Hotspots view and select Find in Call Tree or Find in Hotspots (respectively) from the pop-up menu to search for a node.

Saving a Snapshot

The Profiler provides several options for saving a snapshot. See Table 7 for a description of these options:

Table 8 Save Icons

Icon		Purpose
	Save the Snapshot in the Project icon (located at the top of the Snapshot View window)	Saves the snapshot in the `nbproject/private/idm-profiler` directory of your project. Snapshots saved in your project are listed in the Saved Snapshots section of the Profiler view.
	Save the Snapshot Externally icon (located at the top of the Snapshot View window)	Saves a snapshot to an external, arbitrary location.
	Save As button (located in the Saved Snapshots area)	Saves a snapshot to an external, arbitrary location.

Tutorial: Troubleshooting Performance Problems

Identity Manager provides a tutorial (`profiler-tutorial.zip`) to help you learn how to use the Profiler to troubleshoot forms, Java rules, workflows, and XPRESS.

Step 1: Create an Identity Manager Project

Follow these steps to create an Identity Manager project:

1. Select File > New Project.
2. When the New Project wizard displays, specify the following, and then click Next:
   a. In the Categories list, select Web to indicate what type of project you are creating.
   b. In the Projects list, select Identity Manager Project.

> **NOTE** You must create a regular Identity Manager project for a fully featured development environment. Do not select the Identity Manager Project (Remote) option.

3. Complete the following fields on the Name and Location panel, and then click Next:
   - **Project Name**: Enter **`Idm711`** as the project name.
   - **Project Location**: Use the default location or specify a different location.
   - **Project Folder**: Use the default folder or specify a different folder.
4. When the Identity Manager WAR File Location panel displays, enter the location of the Identity Manager 7.1 Update 1 `war` file. Typically, this file is located in the `waveset\images` directory.

   NOTE Currently, version 7.1 Update 1 is the only Identity Manager version that supports profiling.

5. Click Next to continue to the Repository Setup panel.

   You should not have to change the default settings on this panel, just click Finish. When you see the `BUILD SUCCESSFUL` message in the Identity Manager IDE Output window, you can extract the Profiler tutorial files. See "Step 2: Unzip the Profiler Tutorial" for instructions.

Step 2: Unzip the Profiler Tutorial

Unzip `profiler-tutorial.zip` in the project root. The extracted files include:

project root`/custom/WEB-INF/config/ProfilerTutorial1.xml`

project root`/custom/WEB-INF/config/ProfilerTutorial2.xml`

project root`/src/org/example/ProfilerTutorialExample.java`

project root`/PROFILER_TUTORIAL_README.txt`

You are now ready to start the Profiler.

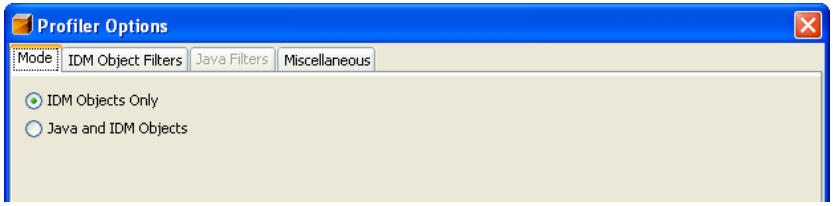
Step 3: Starting the Profiler

To start the Profiler,

1. Use the instructions provided in "Before You Begin" on page 152 to increase the memory for your server and Netbeans JVM.
2. Use any of the methods described in "Overview" on page 147 to start the Profiler.
3. When the Profiler Options dialog displays (Figure 8), you can specify profiling options.

4. Continue to "Step 4: Setting the Profiler Options."

Figure 9 Profiler Options Dialog



Step 4: Setting the Profiler Options

NOTE For detailed information about all of the different Profiler options, see "Specifying the Profiler Options" on page 154.

For the purposes of this tutorial, specify the following Profiler options:

1. On the Mode tab, select Java and IDM Objects to profile form, Java, rule, workflow, and XPRESS objects.
2. Select the Java Filters tab.

   Use the following steps to disable all Identity Manager Java classes *except* your custom Java classes (in this case, `org.example.ProfilerTutorialExample`):

   a. Click New and a new, blank field appears at the bottom of the Filter column.

   b. Enter **`com.waveset.*`** into the new field, and then select the Exclude box.

   c. Click New again.

   d. Enter **`com.sun.idm.*`** into the new field, and then select the Exclude box.
3. Click OK to run the Profiler.

   NOTE The Profiler takes a few minutes to complete the first time you run it on a project or if you have recently performed a `Clean Project` action.

   When the Profiler finishes processing, you are prompted to Log In.
4. Enter the password **`configurator`**, select the Remember Password box, and then click OK to continue.

5. When the Identity Manager window displays, log in.

NOTE	Typically, you should log in to Identity Manager as a different user instead of logging in as `configurator` again. You are already logged into the Profiler as configurator, and the Identity Manager session pool only allows one entry per user. Using multiple entries can result in the appearance of a broken session pool and might skew your profiling results for finer-grained performance problems. However, for this simple example the session pool is of no consequence so you can login as `configurator/configurator`.

6. In Identity Manager, select Server Tasks > Run Tasks, and then click ProfilerTutorialWorkflow1.

   The tutorial might take a few moments to respond.

7. Although you could take a snapshot now; you are going to reset your results instead, run the Profiler, run it again, and then take a snapshot.

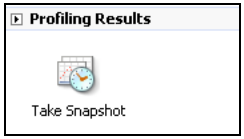
NOTE	It is a best practice to run the Profiler a couple of times before taking a snapshot to be sure all the caches are primed, all the JSPs are compiled, and so forth. Running the Profiler several times enables you to focus on actual performance problems. The only exception to this practice is if you are having a problem populating the caches themselves.

   a. Return to the IDM Profiler view in the Identity Manager IDE. Click the Reset Collected Results icon in the Profiling Results section (or in the Controls section) to reset all of the results collected so far.

   b. In Identity Manager, select Server Tasks > Run Tasks again, and click ProfilerTutorialWorkflow1.

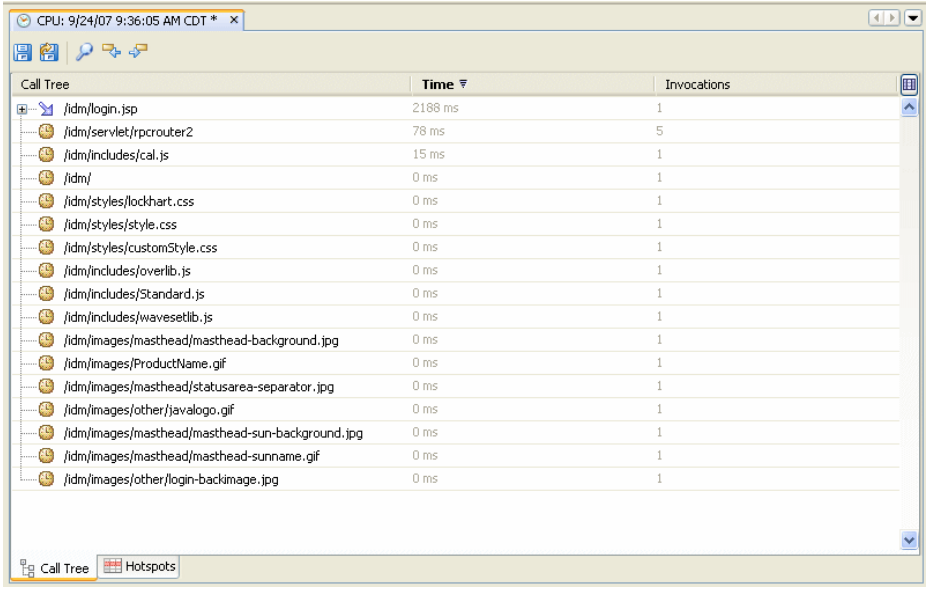
c. When the Process Diagram displays, return to the Identity Manager IDE and click Take Snapshot in the Profiling Results section.

Figure 10



8. The Identity Manager IDE downloads your snapshot and displays the results on the right side of the window.

Figure 11 Call Tree Results



This area is the *Call Tree* view. At the top of the Call Tree, you should see a `/idm/task/taskLaunch.jsp` with a time listed in the Time column. The time should indicate that the entire request took six+ seconds.

9. Expand the `/idm/task/taskLaunch.jsp` node, and you can see that ProfilerTutorialWorkflow1 took six seconds.

10. Expand the `ProfilerTutorialWorkflow1` node. Note that `activity2` took four seconds and `activity1` took two seconds.

11. Expand `activity2`.

    Note that `action1` took two seconds and `action2` took two seconds.

12. Expand `action1` and note that the `<invoke>` also took two seconds.

13. Double-click the `<invoke>` to open `ProfilerTutorialWorkflow1.xml` and highlight the following line:

    ```
    <invoke name='example' class='org.example.ProfilerTutorialExample'/>
    ```

    You should see that a call to the `ProfilerTutorialExample` method took two seconds.

> **NOTE** You are actually browsing XML source that was captured in the snapshot, rather than source in the project. Snapshots are completely self-contained. (For more information, see "How the Profiler Locates and Manages Source" on page 148.)

14. Select the CPU:<*date*><*time*> tab to return to your snapshot.

15. Expand the `<invoke>` node, and note that the Profiler spent two seconds in the Java `ProfilerTutorialExample.example()` method.

16. Double-click the method name to open the `ProfilerTutorialExample.java` source and highlight the following line:

    ```
    Thread.sleep(2000);
    ```

    There's the problem! This method contains a two-second thread sleep.

17. If you return to the Call Tree, you can see that all of the two second paths lead to this method. (You should see three paths; for a total of six seconds.)

18. Select the Hotspots tab (located at the bottom of the Call Tree area) to open the Hotspots view. Notice that `ProfilerTutorialExample.example()` has a total self time of six seconds.

    (For more information about Hotspots, see "Hotspots View" on page 162.)

19. Right-click `ProfilerTutorialExample.example()` and select Show Back Traces from the pop-up menu.

    A new Back Traces tab displays at the bottom of the area.

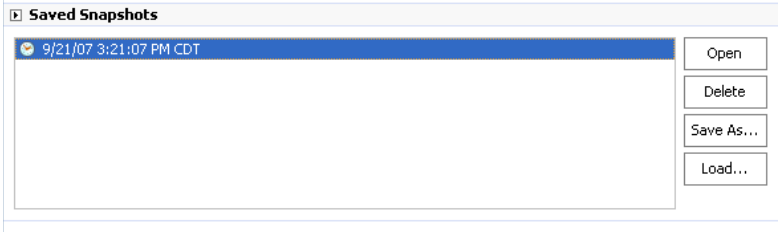
20. Expand the `ProfilerTutorialExample.example()` node on the Back Traces tab to see that this method was called from three places, and that the method took two seconds when it was called from each place.

    (For more information about Back Traces, see "Back Traces View" on page 162.)

21. Click the Save the snapshot in the project icon to save your snapshot and close it.

    If you check the Saved Snapshots section on the IDM Profiler tab, you should see your snapshot. (You might have to scroll down.)

Figure 12 Saved Snapshots List



22. Select the saved snapshot, and then click Open to re-open it.

NOTE	You can use the Save As button to save your snapshots externally and use the Load button to load a snapshot from outside your project.

23. Close the snapshot again.

Using the Profiler on a Workflow ManualAction

The next part of this tutorial illustrates how to profile a workflow ManualAction.

1. In Identity Manager, select Server Tasks > Run Tasks, and then click ProfilerTutorialWorkflow2.

   After a few moments, an empty form displays.

2. Click Save and the process diagram displays.
3. Select Server Tasks > Run Tasks again.
4. Return to the Identity Manager IDE IDM Profiler view and click the Reset Collected Results icon in the Profiling Results section.
5. Now click ProfilerTutorialWorkflow2 in Identity Manager.
6. When the blank form displays again, click Save.

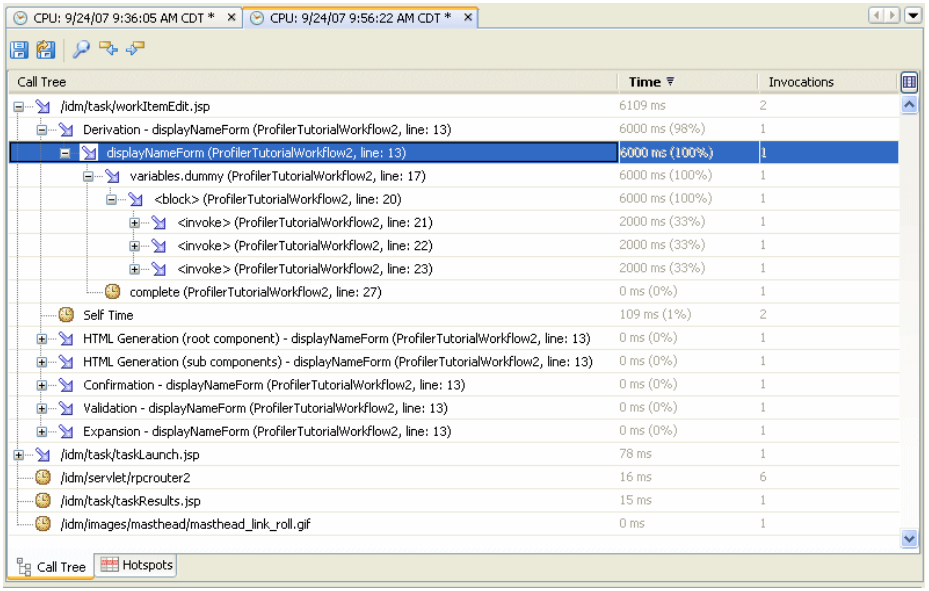
7. In the IDM Profiler view, click Take Snapshot.

   After a few seconds, a snapshot should display in the Call Tree area. You should see that `/idm/task/workItemEdit.jsp` took six+seconds. (This result corresponds to the manual action in the workflow.)

8. Expand the `/idm/task/workItemEdit.jsp` node and note that running all Derivations in the ManualAction form took a total of six seconds.

9. Expand the `Derivation`, `displayNameForm`, `variables.dummy`, and `<block>` nodes.

Figure 13 ProfilerTutorialWorkflow2 Snapshot Results



You should see that the `<block>` took six seconds and, of that time, the Profiler spent two seconds in each of the three invokes to the `ProfilerTutorialExample.example()`. method.

10. You can double-click `<block>` to view the source.

- The following information should be provided as a Frequently Asked Questions (FAQ) section at the end of Chapter 1, Using the Identity Manager IDE: (ID-16739)

Identity Manager IDE Frequently Asked Questions (FAQ)

This FAQ answers some commonly asked questions related to using the Identity Manager Integrated Development Environment (Identity Manager IDE). The information is organized into these categories:

Using NetBeans

Q: Which version of Netbeans should I use?

A: Use the Netbeans version referenced in the Identity Manager product documentation provided for the Netbeans plugin version you are using.

NOTE	Always use the *exact* version referenced because even patch releases can cause major functionality to break.

Q: The Netbeans plugin was working, I did something, and now it is no longer working. What could be causing this problem?

A: This problem is commonly caused by a corrupt file in your `.netbeans` directory. Generally, deleting your `.netbeans` directory and re-installing the NetBeans plugin resolves the problem. (Deleting the `.netbeans` directory effectively uninstalls the NetBeans plugin. You lose all of your user settings, but the contents of your project will be safe.)

The steps are as follows:

1. Shutdown NetBeans.
2. Delete the .netbeans directory.
3. Start NetBeans.
4. Install the NetBeans plugin.
5. Restart NetBeans.

Working with Projects

Q: Building and running a project is taking a very long time, and the Identity Manager IDE seems to be copying a lot of files. What could be causing this problem?

A: This problem can occur for the following reasons:

- You are using the Identity Manager IDE 7.0 or 7.1 plugin.

  Use the Identity Manager IDE 7.1 Update 1 plugin.
  Several adjustments were made to the Identity Manager IDE 7.1 Update 1 Configuration Build Environment (CBE) to improve performance.

- You might be using the `Clean` commands unnecessarily.

  When you use `Clean Project` or `Clean And Build Project`, the Identity Manager IDE deletes the entire `image` directory, which contains several thousand files. Identity Manager IDE must copy all of these files from `idm-staging` during the next build.

  To use the Identity Manager IDE efficiently, you must understand when to use the `Clean` commands. Refer to the "When to Use Clean" section in the Identity Manager IDE `README.txt` file for more information.

Q: Now that I have created an Identity Manager project, what files should be checked into source control?

A: See the "CVS Best Practices" section in the Identity Manager IDE `README.txt` for information.

Q: What are the best practices for using project management in CVS?

A: See the "CVS Best Practices" section in the Identity Manager IDE `README.txt` for information.

Q: When are objects imported into the repository?

A: See "Working with the Repository" on page 174 for information.

Q: How do I add a new JAR to the project?

A: See the "How to add a new JAR dependency" section in the Identity Manager IDE `README.txt`.

Working with the Repository

Q: Which repository should I use for my sandbox repository?

A: Use the embedded repository for your sandbox — particularly if you are using Identity Manager 7.1 (or higher), which has an HsSQL repository available. You lose functionality if you do not use the embedded repository.

Refer to the "Working with the Repository" section in the Identity Manager IDE `README.txt` for more information.

Q: When are objects imported automatically?

A: You have to configure Identity Manager IDE to import objects automatically.

The steps are as follows:

1. Select Repository > Manage Embedded Repository from the IdM menu.
2. Enable the Automatically Publish Identity Manager Objects option on the Manage Embedded Repository dialog.

NOTE	This option is not available for Identity Manager Project (Remote) or if you specify your own repository.

3. Select Project > Run Project or Project > Debug Project.

   The Identity Manager IDE automatically imports all objects that have changed since the last time you ran the project.

NOTE	Automatically publishing Identity Manager objects increases the time needed to start the server. To minimize server start time, disable this option and explicitly upload objects to the repository.

Q: What is the most effective way to upload objects?

A: Use one of the following methods to upload modified objects:

- Right-click one or more edited objects in the project tree and select Upload Object from the pop-up menu.

TIP	To upload multiple objects, press and hold the Control key as you select objects from the list.

- Select one or more edited objects, and then select Repository > Upload Objects from the IdM menu. A dialog is displayed so you can select the objects to upload.

Either method uploads the object(s) directly to the server, so there is no cache latency issue and it is much faster than using Run Project or Debug Project. The Upload Objects feature is available regardless of which repository you are using.

Using the Identity Manager IDE Debugger

Q: The Identity Manager IDE Debugger is sluggish. What could be causing this problem?

A: To improve the Debugger's performance:

- Always disable Tomcat's HTTP Monitor, as follows:
  1. Select the Identity Manager IDE Runtime Tab.
  2. Expand the Servers node and right-click Bundled Tomcat > Properties.
  3. Disable the Enable HTTP Monitor option, and then close the dialog.

     The next time you start Tomcat, the HTTP Monitor will be disabled.
- If you are not debugging Java, select Project > Run Project, and then select Attach Debugger > Identity Manager XML Object Debugger to use just the XPRESS Debugger.

  Selecting Project > Debug Project for a non-remote Identity Manager IDE project starts both the XPRESS Debugger *and* Java Debugger, and the Java Debugger adds substantial overhead.

Q: I cannot set a breakpoint in the Debugger. What could be causing this problem?

A: The following conditions might prevent you from setting a breakpoint:

- You just installed the NBM, but did not restart Netbeans.
- Your XML contains a `<Waveset>` wrapper element.

  The Identity Manager IDE basically ignores any file that starts with a `<Waveset>` wrapper element because the Identity Manager IDE parses that element as a multi-object file.

  The following features do not work on multi-object files:

  - Debugger
  - Rule Tester
  - Form Previewer
  - Any of the editors
  - Import file generator
  - Upload Object
  - Diff Object

  Basically, all you can do with multi-object files is import them. The only files that should contain `<Waveset>` wrapper elements are your project's top-level import files.

Q: I set a breakpoint in the Debugger and it is not suspending on the breakpoint. What could be causing this problem?

A: There are two things to check:

- Be sure the object name does not contain a CBE replacement string (`%%`). CBE replacement strings are not allowed in object names.
- Verify that the code you think is being executed is actually being executed. Try adding a trace and see if anything prints out.

Working with Rules

Q: When developing rules in Netbeans, why is design mode not available for a Rule Library?

A: The design mode functionality is available from the explorer tree in Projects view. Use the following steps:

1. Expand the library node and right-click a rule.
2. When the pop-up menu displays, select Properties and then click Body.

Chapter 4, Developing Adapters

- If you create an adapter that implements the AsynchronousResourceAdapter class, then note that this adapter may be working with users that are partially initialized. (These users are created outside Identity Manager, but not fully populated with attributes.) The Provisioner will not automatically convert a Create operation to an Update operation if the WSUser already exists on the Resource. Your resource adapter must distinguish this case. (ID-16829)

Identity Manager Tuning, Troubleshooting, and Error Messages

This section provides new information and documentation corrections for *Sun Java™* System *Identity Manager Tuning, Troubleshooting, and Error Messages*.

- Information about the size of repository objects (in characters) is now available. You can use this information to detect problematically large objects that might affect your system. (ID-9896, ID-15239)

  You can access this information through the debug/Show_Sizes.jsp web page or from the console command line by typing:

  `showSizes [<type> [<limit>]]`

  NOTE For upgrades, existing objects will report a size of 0 until they have been updated or otherwise refreshed.

- Some tasks have been moved from the adapter to the task package. Update these paths if you have tracing enabled for any of the following tasks, or if you have customized task definitions referencing these packages.

Old Package Name	New Package Name
com.waveset.adapter.ADSyncFailoverTask	com.waveset.task.ADSyncFailoverTask
com.waveset.adapter.ADSyncRecoveryCollectorTask	com.waveset.task.ADSyncRecoveryCollectorTask
com.waveset.adapter.SARunner	com.waveset.task.SARunner
com.waveset.adapter.SourceAdapterTask	com.waveset.task.SourceAdapterTask

- Call timer and Tracing functions are now related, and Call Timing statistics can only be collected when tracing is enabled. (ID-17106)

  The following information should be added to “Show Timings” in the “Debugging Performance Issues” section in “Chapter 1: Performance Tuning.”

Show Timings

The Show Timings page provides a list of methods and their aggregate call timer statistics (*not broken down by caller*) that can help you track bottlenecks to specific methods and invoked APIs.

NOTE Call timing statistics are only collected while trace is enabled.

You can use the options on this page to start timing and tracing, stop timing and tracing, clear the timing statistics, and import or export call timer metrics. In addition, click any of the method names to see which methods they call.

Identity Manager Service Provider Edition Deployment

This section provides new information and documentation corrections for *Sun Java™* System *Identity Manager SPE Deployment*.

Chapter 5, Other Objects in Identity Manager SPE

Identity Manager Identity Manager SPE now supports link correlation and link confirmation rules.

Link Correlation Rule

The `linkTargets` IDMXUser view option allows the caller to specify the list of resources that should be targeted for linking. When using forms, the list can be provided as a form property with the same name. Form properties are assimilated into view options when the IDMXUser view is checked in.

A link correlation rule selects resource accounts that the user might own. Given the view of the user, a link correlation rule returns an identity, a list of identities, or an option map.

If the rule returns an option map, then the view handler uses the map to look for resource accounts and obtains a list of identities that satisfy these options. For example, the `searchFilter` option of the `getResourceObjects` FormUtil method can be used to pass a search filter to an LDAP resource adapter.

A link correlation rule must have the `authType` attribute set to `SPERule` with the `subtype` set to `SUBTYPE_SPE_LINK_CORRELATION_RULE`.

Link Confirmation Rule

A link confirmation rule eliminates any resource accounts from the list of potential accounts that the link correlation rule selects. Given the view of the user and the list of candidate resource accounts, a link confirmation rule selects at most one resource account from the candidate list. The view of the user is visible under the 'view' path, while the list of candidates is available under the 'candidates' path.

If the link correlation rule selects no more than one resource account, the link confirmation rule is optional.

NOTE Unlike Identity Manager confirmation rules, a link confirmation rule is invoked only once during the linking process.

A link confirmation rule must have the `authType` attribute set to `SPERule` with the `subtype` set to `SUBTYPE_SPE_LINK_CONFIRMATION_RULE`.

LighthouseContext API

Several convenience methods have been added to the `SessionFactory` class. The table on page 16 should be updated as follows.

Connection Type	Method	Description
Local anonymous	getServerInternalContext()	Returns a fully authorized context without any authentication.
Local authenticated	getSPESession(String user, EncryptedData password)	Constructs a session for the Service Provider user interface.
Local authenticated	getSPESession(Map credentials)	Constructs a session for the Service Provider user interface. The map specifies the credentials of the user, including the values of the user and password keys.
Local pre-authenticated	getSPEPreAuthenticatedSession(String user)	Constructs a pre-authenticated session for the Service Provider user interface.
Remote anonymous	Not applicable	This connection type is only available through SPML.
Remote authenticated	getSession(URL url, String user, EncryptedData pass)	Returns an authenticated session.

Localization Scope

Historically, Identity Manager does not localize resource objects and functions, primarily because they are mostly samples that get loaded (through `init.xml`) during initialization of Identity Manager, and because the attributes of object types can vary between actual customer deployments, depending on the level of customizations. Following is a list of areas where users might encounter English: (ID-16349)

- Default user forms and process mapping
  - **Example**: Edit User > Security > User Form pull-down menus
  - **Example**: Configure > Form and Process Mappings
- Configuration object attribute names

  Example: Configure > User Interface, concatenated names such as `displayPasswordExpirationWarning`
- Default tasks
  - Task templates

    Example: Server Tasks > Configure Tasks > available task template names in table
  - Task type labels

    Example: Server Tasks > Run Tasks > second column items from Available Tasks table
  - Task definitions

    Example: Server Tasks > Find Tasks > second pull-down menu to select Task Definition
- Default report names

  Example: Report names found under Reports > Run Reports > Report Table
- Default policy names

  Example: Compliance > Manage Policies > audit policy names and descriptions
- Default capability names

  Example: Edit User > Security > Available Capabilities
- Default report & graph names
- Process/workflow diagram applets

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 file** — `../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
```