

Sun Java™ System Identity Manager Release Notes

Version 7.1 May 2007

Part Number 820-0815-10

These Release Notes contain important information available at the time of release of Sun Java System Identity Manager 7.1. 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.

These Release Notes are organized into the following sections:

- [Introduction](#)
- [Identity Manager 7.1 Features](#)
- [Known Issues](#)
- [Installation and Update Notes](#)
- [Deprecated API](#)
- [Documentation Additions and Corrections](#)

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 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 above
- 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

- Sun Java™ System Application Server Platform Edition and Enterprise Edition 8.1
- Sun Java™ System Application Server Enterprise 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

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™ 2005
- MySQL™ 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 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](#)
- [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
- Oracle 9i®
- Oracle Database 10g Release 1®

- Sybase Adaptive Server® 12.x
- Scripted JDBC

Directories

- LDAP v3
- RACF LDAP
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory on Novell NetWare 5.1, 6.0, and 6.5
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

NOTES

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

Enterprise Resource Planning (ERP)

- Oracle E-Business Suite on Oracle Applications 11.5.9, 11.5.10
- Peoplesoft® PeopleTools 8.1 through 8.48 with HRMS 8.0 through 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

Help Desk

- Remedy Help Desk 4.5, 5.0.
- BMC Remedy Action Request System Server 6.0, 6.03, and 7.0
- BMC Remedy Service Desk Application 7.0

Message Platforms

- Blackberry RIM Enterprise Server 4+ (uses generic Windows script adapter)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0 6.5, 6.5.4, 7.0 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 6.0, 6.5, and 7.0 (using the Novell NDS adapter)

NOTES

- Microsoft Exchange 2000 and 2003 are managed through the Microsoft Windows Active Directory 2000 and 2003 resources.
 - The BlackBerryResourceAdapter will not be supported in a future release. Future implementations that require resource adapters for Blackberry Enterprise Server Version 4+ should be based on the ScriptedGatewayResourceAdapter.
 - 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

Operating Systems

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

- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

Role Management System

- BridgeStream SmartRoles

Security Managers

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Scripted Host
- INISafe Nexess 1.1.5
- RSA ClearTrust 5.5.2, 5.5.3
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 for UNIX
- eTrust CA-Top Secret® Security 5.3

Web Access Control

- IBM Tivoli® Access Manager 4.x, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2
- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4 (Realms supported as of 2005Q4)

Web Servers

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

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

Browsers

Identity Manager supports the following browsers:

- Microsoft Internet Explorer 5.x and later
- Safari v2.0 and later for Mac OS X 10.3.3 and later
- Mozilla 1.78 (with JRE 1.5)
- Firefox 1.0x, 1.5 (with JRE 1.5), 2.0 and later

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	<ul style="list-style-type: none"> • IBM AIX 4.3.3

Software Category	Software Package
Application Servers	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • MySQL 4.1 • Microsoft SQL 2000
Resources	<ul style="list-style-type: none"> • ActivCard 5.0 • Lotus Notes (Domino) 5.0.x, 6.0.x • Microsoft Windows NT 4.0 • Sun Identity Manager Gateway running on Microsoft Windows NT 4.0 • MySQL 4.1 • Novell® GroupWise 5.x, 6.0, 6.5 • Novell® eDirectory on Novell NetWare 5.1, 6.0 • Oracle 8i (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:

Software Category	Software Package
Repository Database Servers	<ul style="list-style-type: none"> • Oracle 8i • IBM DB2 Universal Database for Linux, UNIX, and Windows 7.0
Operating Systems	<ul style="list-style-type: none"> • Solaris 7, Microsoft Windows NT 4.0
Resources	<ul style="list-style-type: none"> • 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 API](#)” 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 Version	Target Version				
	5.0	2005Q3M1	2005Q4M3	7.0	7.1
Waveset Lighthouse 4.1 SPx	5.0	5.0 > 2005Q3M1	5.0 > 2005Q4M3	5.0 > 2005Q4M3 > 7.0	5.0 >2005Q4M3 > 7.1
Identity Manager 5.0 SPx		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q1M3 Identity Auditor 1.0		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M1 Identity Manager 5.5			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q3M3 Identity Manager SPE 1.0			2005Q4M3	2005Q4M3 > 7.0	2005Q4M3 > 7.1
Identity Manager 2005Q4M3 Identity Manager 6.0				7.0	7.1
Identity Manager 7.0					7.1

-
- NOTE**
- When upgrading Identity Manager, you do not have to install Service Packs 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.
 - Service Packs for a major release are cumulative. After upgrading to the major release, you can install the latest service pack without having to install all of the 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 service packs**: 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 SPx 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 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 May 2007 Release Notes, and the part number is 820-0815-10.

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/coll/1514.1>
- **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://www.sun.com/software>

Copyright © 2007 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

SUN PROPRIETARY/CONFIDENTIAL.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Portions may be derived from Berkeley BSD systems, licensed from U. of CA.

Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

Copyright © 2007 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou des brevets des applications de brevet en attente aux Etats - Unis et dans les autres pays.

Propriété de SUN/CONFIDENTIEL.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.

Identity Manager 7.1 Features

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

- [What's New in This Release](#)
- [Bugs Fixed in This Release](#)

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:

- [Installation and Update](#)
- [Administrator and User Interfaces](#)
- [Auditing](#)
- [Forms](#)
- [Identity Manager Integrated Development Environment \(IDE\)](#)
- [Identity Manager SPE](#)
- [Repository](#)
- [Resources](#)
- [Roles](#)
- [Security](#)
- [Server](#)

Installation and Update

- Use the `waveset.serverId` system attribute to set unique server names when your deployment includes multiple Identity Manager instances that point to one repository on a single physical server. (ID-11578)
- Install and update can be run on a system without a display. (ID-14258)
- A script for creating a Identity Manager Service Provider transaction database for MySQL is now provided at `sample/create_spe_tables.mysql`. (ID-14666)

MySQL is not supported as a Service Provider transaction database. The script is intended to be used for demonstration purposes only.

- For localization: The `RAMessage_l10n.jar` previously required for the Upgrade Pre-Process procedure has been removed and you must download translations for the adapters. (ID-16272)

You can download a language pack from the Sun Download Center, which is part of the Online Support Center (<http://www.sun.com/download>). A registered account name and password is required to access the download center.

For more information, see Identity Manager 7.1 Installation and the Identity Manager L10n Readme, which can be found in every IDM language pack.

Administrator and User Interfaces

- When a user forgets their user ID, they can now click **Forgot My User ID** on the `login.jsp` or `user/login.jsp` to open a new **Lookup User ID** page. From this page, the user can provide a notification email address and some additional identity attribute values (such as phone number, first and last name, employee ID, etc.) and Identity Manager will try to find a single user who matches the specified identity attribute values. (ID-4924)
 - If successful, Identity Manager sends an email containing the user's Identity Manager user ID to the notification email address specified. (A new **User ID Recovery Email Template** was created for this purpose. The subject and body of this template are message keys, so that they can be customized and internationalized.)
 - If unsuccessful, an error message reports that Identity Manager could not locate a user matching the specified information or that it found more than one user who matched the specified information.

This feature is enabled by default, but it can be disabled.

- Now, when editing a **Resource Login Module (non-Identity System User ID/Pwd Login Module)** within the scope of a **Login Module Group** (from the **Security > Login** subtab) you can select a **Login Correlation Rule** to map login information provided by the user to an Identity Manager user.

Identity Manager uses the logic specified in the **Login Correlation Rule** to search for an Identity Manager user. The rule must return a list of one or more `AttributeConditions`, and then search for an Identity Manager user that matches these conditions.

For example, it might be sufficient to just correlate on the Identity Manager user ID. Alternatively, if the Identity Manager users have an LDAP resource accountID, you could search for the accountID and the Identity Manager users would not need a Sun Access Manager resource link. The `authType` of the Login Correlation Rule must be `LoginCorrelationRule`. (ID-8577)

- Synchronization status is no longer provided in the Description column of the resource tree table. The Status column now provides a combined status for reconciliation and synchronization. (ID-12465, ID-14005)
- The server configuration and email templates have been modified to allow the administrator to determine if SSL or authentication should be done on the SMTP server. (ID-14899)

For more information see, the *Sun Java™ System Identity Manager Administration*.

Auditing

- You can now prioritize policy violations by assigning them a priority, severity, or both. Prioritize violations from the remediations page. For more information, see “Prioritizing Policy Violations” in *Identity Manager Administration*. (ID-11703)
- Audit policy scans now scan members of dynamic organizations. (ID-12437)
- Audit policy scans can now be scheduled. (ID-12474)
- Audit scans now have a test mode, which disables remediation and deletes all violations upon completion of the scan. (ID-12522)
- The Violation Summary Report has been extended to allow selection of violations to be made by the violation state. The report can be configured to only report violations that are in one or more of the possible states. (ID-12612)
- Audit log entries that are related to access review approvals, rejections, and remediations can now be digitally signed. (ID-13264)
- After launching a periodic access review, if you go to the access review page, you will not see your scan displayed on the list until you click the refresh button. (D-14169)
- Directory junctions and virtual organizations now support audit policy assignment. (ID-14591)
- You can now define the Access Scan user scope based on assigned resources. (ID-14654)
- You can now quickly show Identity Manager Compliance by installing the demonstration environment. (ID-14970)

You can install the Compliance demo environment by importing `sample/auditordemo.xml` or by creating your own demonstration environment using the tools provided in the Compliance/RuleBuilder. See `Compliance/RuleBuilder/README.txt` for more information.

- Attestors and remediators can now specify forms that show exactly the detail they need to increase efficiency when attesting and remediating. For more information, see the Documentation Additions and Changes section of these Release Notes. (ID-14973)
- During remediation, you can now re-evaluate a compliance violation to determine if it is still in effect. You can edit a user so that the audit policy won't be violated again. (ID-15019)
- Pending access review entitlements can now be refreshed with current entitlement data. (ID-15027)
- An access review remediator can edit (re-provision) a user directly using a new Edit button on the remediation form. (ID-15172)
- A compliance review remediator can edit (re-provision) a user directly using a new Edit button on the remediation form. (ID-15173)
- An access review can now alter user entitlements either of these ways: (ID-15180)
 - The access review attestor requests a rescan by clicking Rescan, which causes the user entitlement to be refreshed and re-evaluated.
 - The access review remediator clicks Remediated, which causes the user entitlement to be refreshed and re-evaluated.
- A user entitlement created in the REMEDIATING state now automatically creates a remediation work item. (ID-15423)

For more information, see Chapter 2, “Working with Rules,” in *Identity Manager Deployment Tools*.

Upgrade Consideration: After an upgrade, the Bulk Attestation Notice and all email templates are preserved. However, the Bulk Attestation Notice in the `auditorwfs.xml` file shows how the new access review remediation work item notification variables can be implemented.

- Auditor scans can now specify target resources more explicitly for multi-account resources. (ID-15485)
- The management page for Audit Policy objects is now form-based and customizable. You can now select either the “full view -- an information-dense display -- or restrict the level of detail to a partial view. For more information, see the Documentation Addendum of these Release Notes. (ID-15486)
- The management page for Access Scans is now form-based and customizable. For more information, see the Documentation Addendum of these Release Notes. (ID-15515)

- Audit log reports now show the details of role modifications. (ID-15587)
- By default, only the following user entitlement events are logged (ID-15735):
 - Attestor Approved
 - Attestor Rejected
 - Remediation Requested
 - Rescan Requested
 - Terminate

Forms

- The `TabPanel` display class now supports the execution of validation expressions on a per-tab basis. If you set the `validatePerTab` display property to `true`, Identity Manager performs validation expressions as soon as the user switches to a different tab. (ID-12442)
- A sample VMS form is now provided in the `sample/forms` folder. (ID-12835)

Identity Manager Integrated Development Environment (IDE)

The Identity Manager Integrated Development Environment (Identity Manager IDE) is Java application that enables you to view, customize, and debug Identity Manager objects in your deployment.

The following new features have been added to (or changed in) the Identity Manager IDE for the Identity Manager 7.1 release:

NOTE For more information about these features, see *Identity Manager Deployment Tools*

- The Identity Manager IDE now supports `GenericObjects`. (ID-12952, 12991)
- There is now an IdM menu on the NetBean's top level menu bar from which you can select actions that are appropriate for selected object nodes. (ID-13158)
- The Identity Manager IDE 7.0 project has been replaced with the following two project types, both of which are NetBeans ant projects: (ID-14587)

- **Identity Manager Project:** Used as the primary development environment for deployers as it is the most fully featured project type, including:
 - Java/JSP editing, building, debugging
 - Ability to launch Identity Manager in a Netbeans' embedded application server
 - Ability to manage an embedded repository

This project type provides a simple repository that you can use for testing in your sandbox. When you create this project type, you can specify an embedded repository for the project. In addition, you can enable a Manage Embedded Repository option to re-initialize the repository. The Identity Manager IDE provides an auto-publish feature that automatically loads the embedded repository anytime you run or debug the project.

- A sample CBE (Configuration Build Environment) and import file generator. For more information about the CBE, refer to the `README.txt` file provided with the Identity Manager project.
- **Identity Manager Project (Remote):** Used for making small changes and for debugging a remote project on an external server. A lightweight, quick set-up project type has all the editing functionality of the Identity Manager project, but lacks the build environment and the ability to launch the `war` file.

- The Identity Manager IDE now provides version independence. (ID-14723)

The 7.1 version of the Identity Manager IDE `.nbm` has been decoupled from the Identity Manager classes. The version 7.1 `.nbm` supports Identity Manager 7.0 and 7.1, and it is planned to support Identity Manager 6.0 SP3.

Each Identity Manager IDE project is tied to a specific Identity Manager version, and the Identity Manager IDE now requires a compatibility bundle (`ide-bundle.zip`) that provides Identity Manager `jar` files and some XML registries containing version-specific information for each supported Identity Manager version. The compatibility bundle is specified when you create a project:

- For **Identity Manager Projects:** The compatibility bundle is included in the `idm.war` file, and Identity Manager IDE automatically accesses this file during project setup.
- For **Identity Manager Projects (Remote):** Because you do not specify a `war` file location for remote projects, you must provide the compatibility bundle's location, which is:

Identity Manager install root/sample/ide-bundle.zip

NOTE Identity Manager version 7.0 did not provide an IDE Compatibility Bundle, but you can download this file from the Identity Manager 7.0 download site.

- Library objects have been added to the list of object types displayed in the Explorer window, and these objects have Property Sheets, Palette features, and navigation nodes. (ID-14817)
- The Identity Manager IDE plugin now requires JDK 1.5 and Netbeans 5.5. (ID-14950)
- You can now compare (diff) a single object or a folder of objects (recursively) in a local directory with those in the repository. You can use this feature to view the differences between your local copies and those on the server. In addition, you can use this feature to upload and reload one or more modified objects. (ID-15151, 15206)
- When you select Design view for a Rule object, an Expression Builder now displays in the Editor window to make it easier for you to see the logical structure of a rule and to modify the rule's properties. (ID-15104)
- Features and functionality were added to the Identity Manager IDE Expression Builder dialogs. You can now do the following:
 - Edit simple data types (integers and strings) directly in the Expression Builder table. (ID-15528)
 - View JavaDoc for Identity Manager API methods when defining XPRESS invoke statements (static or instance) in the Expression Builder dialogs. (ID-12961)

When you select classes or methods from Class Name and Method Name menus in the Expression Builder, the related JavaDoc displays in a pop-up alongside the dialog. (ID-12960)
 - Edit property values that support expressions and primitive values (such as strings) directly in a property table. (ID-13763)
 - Create a specific expression rather than first creating a BLOCK and then changing it to the expression you want. (ID-15932)
 - Include or “wrap” an expression element in another element, which enables you to build expressions from the inside out.
 - Change an element's expression type using a new Change To button and dialog. (ID-15933)
- The Identity Manager IDE now provides separate nodes for files, persistent objects, and extensions to better reflect the actual underlying XML content. In addition, you can re-order nodes and insert nodes into other locations (before, after, or into other nodes in the Project tree). (ID-14689)
- You can now delete objects from the Identity Manager IDE repository. (ID-14081, 15031)
- You can now upload an object in the Identity Manager IDE to an Identity Manager 7.0 server and manually assign an ID to the object. (ID-15474)

- To facilitate moving objects from one repository to another, you can now configure Identity Manager IDE to remove all auto-generated repository IDs before it downloads objects from the repository. (ID-15307, 15347)

Identity Manager IDE locates and removes all object IDs and objectRef IDs that conform to a specified expression — without removing any hard-coded, predefined IDs.

- Now, when editing forms you can follow references to forms and fields. In addition, when editing workflows, you can follow external processes. The Identity Manager IDE opens the referenced file and finds the reference. (ID-14428, 15406)
- You can now specify a root context, by leaving the Context field blank when you create the project. (ID-15912)

Identity Manager SPE

- Identity Manager Identity Manager SPE now supports link correlation and link confirmation rules. (ID-10500) For more information, see the description of bug 15760 in the Documentation Addendum of these Release Notes.
- Authentication answers for Service Provider users can now be edited in the administrative interface. (ID-12781)
- LDAP deleted attributes are now propagated after a downed resource is once again available. (ID-15471)

Reports

- You can now globally control the font used when generating reports by editing the settings on the Configure > Reports page. You can override this by editing the configuration for each report. By default, only fonts available to all PDF viewers are shown.

Add additional fonts to the system by copying font definition files into `WEB-INF/fonts` directory under the directory where IDM is deployed (for example, `/var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm/WEBINF/fonts`). You must then restart the server. Accepted font definition formats include `.ttf`, `.ttc`, `.otf`, and `.afm`. If one of these fonts is selected, then the same font must be available at the machine where the report is viewed or the font must be embedded in the report.

Since the default set of fonts does not support all character sets (for example, Asian characters), you must install an additional font in the `fonts/` directory and select it in the configuration pages to generate reports that can display alternate character sets. (ID-10641/14376)

NOTE TrueType fonts are licensed with different levels of possible embedding. The font that you have selected to generate the PDF with must be licensed to allow the font to be embedded for printing and previewing in the PDF. If the font is not correctly licensed for embedding in the PDF, the PDF will be generated with a standard font. This will cause the content of the PDF to be corrupted. Identity Manager currently does not log a failure to alert you to this issue.

Repository

- Information about repository object size is now available. You can access this information through the web pages and from the console command line. (ID-9896)

NOTE For upgrades, existing objects will report a size of 0 until they have been updated or otherwise refreshed.

Resources

New Resource Adapters

The following adapters have been added this release:

- RACF-LDAP
- SAP Governance, Risk, and Compliance (GRC) Access Enforcer

See the *Identity Manager Resources Reference* for details about these resource adapters.

Resource Adapter Updates

- You should now configure servers that will run ActiveSync in the synchronization policy for the resource. The use of `waveset.properties` has been deprecated, but can still be used. Migration to configuring in the synchronization policy is strongly encouraged. (ID-10167)
- Configuring the Flat File Active Sync adapter has been simplified; especially for delimited files. (ID-11678)
- Active Sync can be terminated before all updates have been processed on the LDAP adapter. (ID-13695)
- Identity Manager now provides PeopleSoft HRMS 9.0 support. (ID-14195)

- The Domino adapter now supports setting the explicit policy attribute for Domino 7.0 resources. (ID-14315)
- The Oracle ERP resource adapter now supports before and after actions. (ID-14659)
- The default RACF List User `AttrParse` mechanism has been extended to handle large numbers of “CLASS AUTHORIZATIONS” and template users with group entries such as “GROUP SYS1 USER CONNECTION NOT INDICATED”. (ID-15021)
- Two resource attributes, Default Primary Group and Login Shell, have been added to the Solaris, AIX, HP-UX, Red Hat Linux, and SuSE Linux resource adapters. (ID-15034)
- The NDS adapter has improved support for GroupWise:
 - The adapter can now manage post offices in secondary domains. (ID-15122)
 - GroupWise users can subscribe to any known distribution list. (ID-15707)
 - The adapter no longer uses the **Delete Pattern** parameter as its mechanism for signifying that a post office should be removed from a GroupWise user. The new method requires that the post office field merely be set to "" (two double quotation marks). If you have legacy forms or workflows that programmatically remove post offices, change them to set the field to "". (ID-15970)
- The Domino resource adapter supports roaming users for Domino 7.0 servers. (ID-15157)
- Activity groups (roles) and profiles in a CUA environment can now be updated with a start and end date. (ID-15613)

For roles, map the `activityGroups` attribute in the adapter to:

```
CUA->directLocalActivityGroupObjects
```

For Profiles, map “profiles” to:

```
CUA->directLocalProfileObjects
```

- The ACF2 adapter supports ACF2 8.0 SP2. (ID-15833)
- The sample `NDSUserForm` includes working examples of all seven techniques for fetching post offices and distribution lists. (ID-15872)
- The PeopleSoft Component Interface adapter now supports specifying separate keys for GET, FIND, and CREATE operations on a component interface. (ID-16055)
- The PeopleSoft Component Interface adapter now supports PeopleTools 8.1 through 8.48. (ID-16128)
- The Top Secret resource adapter now correctly handles `ASUSPEND`, `PSUSPEND`, `VSUSPEND` and `XSUSPEND` when enabling and disabling users. (ID-16295)

Roles

- When you import roles containing links to back to existing super roles, Identity Manager now updates the existing roles with links back to the newly imported roles. (ID-15482)

Identity Manager detects and creates links from existing super roles back to the subroles that reference them. During upgrade, Identity Manager invokes the `RoleUpdater` class used to repair the roles.

You can update roles outside the upgrade process by importing a new `RoleUpdater.xml` file found in `sample/forms/RoleUpdater.xml`. By default, Identity Manager adds the subrole links during upgrade or when you import `RoleUpdater.xml`.

To disable this new functionality, set the `RoleUpdater` attribute `nofixsubrolelinks` to `true`. For example,

```
<MapEntry key='nofixsubrolelinks' value='true' />
```

See ID-15053 described in “[Known Issues](#)” for related information about automatically updating roles during import.

- The delegation model is changed as follows: (ID-15440)
 - If you are editing a user who has delegated to one or more users or a rule that has been deleted after the delegation was originally established, the user or rule delegated to is now be displayed enclosed in parentheses, indicating that it has been deleted. For example: “(auser)”
 - If the user's delegate to list is changed but still includes the deleted delegate, an exception will be thrown and the save will fail. If the user's delegate to list is not changed but other attributes of the user are changed, the save will succeed, because there is no change to the delegate info.
 - If you are creating or updating a user and the approver has delegated to a user who no longer exists, a create or update will fail with a message indicating that the approval work item could not be delegated as configured because the delegate was deleted.
 - Work items that were delegated to a user who was subsequently deleted can still be recovered by the delegating user. The delegating user can then end the delegation to the deleted user.

For more information, see the *Sun Java™ System Identity Manager Administration*.

Security

- Identity Manager now allows users to define different delegation configurations for different work item types (such as attestations, remediations, approvals, and so forth). (ID-14152)
- A new, built-in ObjectGroup/Organization called End User has been added to Identity Manager. (ID-14630)

This new ObjectGroup/Organization is a member of Top. Initially, it does not have any memberobjects. This ObjectGroup/Organization is not displayed in the tree table under the Accounts tab in the Administrator user interface, and it cannot have child organizations. However, you can make any object available to the End User ObjectGroup/Organization using the Administrator user interface when you are editing objects (such as Roles, AdminRoles, Resources, Policy, or Tasks).

Previously, when users logged into the End User interface, they were automatically assigned the rights to object types specified in the EndUser capability (such as AdminRole, EndUserConfig, or EndUserTask). Now, Identity Manager also automatically assigns them control of the new EndUser ObjectGroup and evaluates a built-in End User Controlled Organizations rule. If any organization names are returned, Identity Manager automatically gives those users control of those organizations as well. Identity Manager uses the authenticating user's view as the input argument to the End User Controlled Organizations rule. The rule can return one organization (as a string) or more organizations (as a list) for which the user logging into the End User Interface will have the EndUser capability.

In addition, a new End User Administrator capability has been added to manage the new objects. Users with this capability can view and modify the rights to object types specified in the EndUser capability and to the contents of the End User Controlled Organizations rule. This capability is assigned to Configurator by default. Any changes to the list, or to the organizations returned by evaluation of the End User Controlled Organizations rule, will not be dynamically reflected for logged in users. These users must log off and then login again to view the changes.

You should consider this new ObjectGroup/Organization as the best practice method for giving end users access to Identity Manager configuration objects such as Roles, Resources, Tasks, and so forth.

In future, you should use this method instead of using End User Tasks, End User Resources, System Configuration:EndUserAccess, and End User authTypes; however, these methods are still supported for backward compatibility.

- You can now add passwords to a user's password history when creating a user. (ID-15179)

- When listing objects (such as roles or resources) and there are more than six `memberOfObjectGroups` for any of the returned objects, Identity Manager no longer filters out the truncated `memberOfObjectGroups` from the results. (ID-15181)

NOTE This behavior does not apply to the `USER` type because it can be a member of only one `ObjectGroup`.

- If a user who owns any pending work items is deleted, Identity Manager now ensures that the work items are not lost, as follows: (ID-15868)
 - If a pending work item was delegated and the delegator has not been deleted, the pending work item is returned to the delegator, and the delegator will then be the new work item owner.
 - If a pending work item was delegated and the delegator has also been deleted or if a pending work item was not delegated, the delete attempt fails until the user's pending work item has been either resolved or forwarded to another user.

Server

- You can now configure tracing to trace a method *and* all of its subcalls (both direct and indirect), which can be useful if you are debugging problems known to happen at some level below a specific entry method. (ID-13436)

To enable this feature, set the trace level for a scope with the `subcalls` modifier, as in the following example:

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

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

- The following methods have been added to `WSUser`. See the JavaDoc shipped in the REF kit for more information on this class. (ID-15468/14152)

WSUser Object Methods

Method	Description
<code>getWorkItemDelegates()</code>	Returns the current set of Delegate objects for the specified user
<code>getWorkItemDelegate(String workItemType)</code>	Returns a Delegate object of the requested workItem type from <code>_delegates</code>

WSUser Object Methods

Method	Description
<code>addWorkItemDelegate(Delegate delegate)</code>	Adds a Delegate object of the specified work item type to <code>_workItemDelegates</code> . If one of the specified <code>workItemType</code> types already exists, it will be replaced
<code>removeWorkItemDelegate(String workItemType)</code>	Removes the specified <code>workItemType</code> from the set of work item Delegate objects
<code>setWorkItemDelegates(Map workItemDelegates)</code>	Sets the set of work item delegate objects for this user
<code>getWorkItemDelegateHistory()</code>	Returns the specified user's list of Delegate history objects
<code>setWorkItemDelegateHistory(List workItemDelegateHistory)</code>	Sets the specified user's list of Delegate history objects

Work Items

- When an Attestation WorkItem is forwarded, any comments provided by the forwarding Attestor are included in WorkItem such that when the WorkItem is finally attested, the comments from other Attestors will be included. (ID-14643)

Bugs Fixed in This Release

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

- [Administrator and User Interfaces](#)
- [Auditing](#)
- [Integrated Development Environment \(IDE\)](#)
- [MetaView](#)
- [Password Synchronization](#)
- [Reconciliation](#)
- [Reports](#)
- [Repository](#)
- [Resources](#)
- [Security](#)
- [Server](#)
- [Workflow](#)
- [Additional Defects Fixed](#)

Administrator and User Interfaces

- On the debug pages, ObjectGroups no longer appears in the dropdown list of item types that can be bulk deleted. (ID-13324)
- You can now unlock an organization object that becomes locked after a user with insufficient rights tries to delete it. (ID-14942)
- Custom end-user tasks that need to checkout the view of the logged-in user no longer get an error about the account being unavailable because the account is locked. (ID-15040)
- You can now find Roles with lots of Organizations from the Find Roles page without an ObjectGroup error being displayed. (ID-15303)
- The Roles tab > Find Roles > Approvers menu can now show users with the "Role Approver" capability. (ID-15373)

- If you use a `customEdit.jsp` form for your own custom edit form, you no longer get a page with no navigation bar and two copies of your custom form. (ID-15460)
- Internet Explorer 6 or 7 with security update 912812 users are no longer required to double click a multi-select box to highlight the box or double click an item to move it. (ID-15824)
- When you specify `true` for `IAPI.cancel` (which cancels any pending updates detected for the user being processed) on the ActiveSync Input form, the user's view no longer remains locked after being processed. (ID-15912)
- Editing a user in the Top organization, which is the result of a user list search, now works correctly without generating an error. (ID-15977)
- The default rules provided to support access scans are all members of the Top organization by default. If your deployment wants to allow administrators edit access scans or audit policies without controlling the Top organization, you must add the following rules to the other organizations: (ID-15996)
 - Review Everyone
 - Review Changed Users
 - Reject Changed Users
 - Default Remediator
 - Default Attestor
 - Default Escalation
 - AttestorAll
 - Non-Administrators
 - All Administrators
 - Users Without a Manager

Auditing

- A new policy, the IDM Role Comparison audit policy, is available for checking that users' resource attributes match the role attributes defined in their assigned roles. If there isn't a match, a compliance violation is created when a non-compliant user is scanned using this new policy. (ID-11225)
- An error is no longer displayed when you edit an Access Review Detail Report in which the specified access review target has been deleted. (ID-14805)

- For a new Identity Manager 7.1 installation, the default Auditor Report for All Compliance Violations now uses the `resourceNames` display attribute to allow compliance violations to reflect more than one resource. Previously, this report used the `resourceName` attribute, which generated a warning message. (ID-15915)

Upgrade Consideration: This problem is fixed only for a new Identity Manager 7.1 installation. If you are upgrading Identity Manager, you must manually fix this problem by specifying `resourceNames` and not `resourceName` in the default report task (and any other reports configured from the Violation Summary Report task definition).

- The Audit Policy wizard GUI allows the specification of 3 remediators, and an escalation period between them. If you specified the period, you must specify the remediator. Otherwise, the remediation will be deleted. (ID-14198)
- You can now perform an Audit Scan or Access Review with the user scope set to a dynamic org. (ID-14886)
- Audit log reports show the details of role modifications (ID-15587)
- The Identity Manager Compliance features provide tasks, policies and rules that you can use as is. (ID-16127) Identity Manager initially creates these objects in either the Top or All object groups as appropriate. For deployments that choose to 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 add or remove object groups from the Auditor objects. (For a complete list of Auditor objects, see `$WSHOME/sample/scripts/AuditorObjects.txt`.)

- To list objects:

```
cd $WSHOME/sample/scripts
beanshell.sh objectGroupUpdate.bsh -action list -data AuditorObjects.txt
```

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

```
cd $WSHOME/sample/scripts
beanshell.sh objectGroupUpdate.bsh -action add -data AuditorObjects.txt
-groups
```

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

```
cd $WSHOME/sample/scripts beanshell.sh objectGroupUpdate.bsh -action remove
-data AuditorObjects.txt -groups All
```

- The Identity Manager auditing component provides workflows that you can use directly and that are potentially long-running. (ID-16173) To allow an upgrade from 7.0 to 7.1, you must rename any suspended TaskInstances of these workflows.

Identity Manager provides a script that you can run before the 7.1 upgrade to perform this rename operation automatically. These scripts are in the `util_scripts` directory of the installation image. To execute the scripts, you must change to the directory that contains them, and the Identity Manager server must be running. Specify the `-h idm-url` option, even if running the script locally on the Identity Manager server. The expected form of `idm-url` is required. If the Identity Manager server is bound to the default URL path, you can omit this. This script changes the Identity Manager repository, so it only needs to be run on a single Identity Manager server.

- To list the tasks that need to be renamed

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h idm-url
-action list
```

- To perform the rename operation

```
./beanshell.sh taskUpdate.bsh -u Configurator -p configurator -h idm-url
-action rename
```

The renamed TaskDefinition objects will have the form `old-name-7.1-update[N]`

- When terminating or deleting an Access Review, termination or deletion tasks might encounter errors that prevent the tasks from completing. If that happens, the Access Review will be put into the TERMINATE ERROR or DELETE ERROR state. To see the specific error information, you will need to look at the Task results from System Tasks -> All Tasks (ID-16211)

Integrated Development Environment (IDE)

- Most nodes have an associated property sheet in the Properties windows, and most of these nodes have a Name property for managing the value of the name. If you rename a particular object via its node, either by right-clicking and selecting Rename, or by clicking the node and typing text over the label, the node's label is updated and the XML changes. However, the property sheet fails to update. You can click another node and then re-click the renamed node and the property sheet updates to reflect the new name. You can also click the title of the property sheet to update to the correct values. (ID-13696)
- Rule Libraries are not currently supported other than to perform basic XML editing and testing in the rule tester. Navigation and property support is not currently implemented. (ID-14093)
- Form property values cannot be set with the property editor if the data type is Integer or Boolean. (ID-14128)

Workaround: Edit the value to the property directly in the XML.

- Downloading, uploading or reloading an object causes a lock to be placed on the object in the repository. Consequently, attempts to access the object by users other than the one given in the project settings within the lock's time of expiration may fail. (ID-14132)
- Renaming an object from the context menu in NetBeans requires the change to be saved. After making the change, the user can save the change from File ->Save without opening the file. If the file is open, use File ->Save, or close the file and select to save the changes when prompted. (ID-14420)
- When setting the displayClass for a field to InlineAlert, if the field has a name the value property of the InlineAlert will not display. (ID-14456)
- Checking out a user view in Identity Manager IDE puts a lock on the object. Checking in the view or closing the view does not release the lock. The lock will be released automatically after 5 minutes. You can also release the lock by logging in to Identity Manager as the administrator that checked the view out in IDM IDE and viewing the user. (ID-14797)
- It is now possible to specify a root context, by leaving the **Context** field blank on project creation. (ID-15925)

Identity Manager SPE

- You can now terminate the SPE Synchronization task prior to processing all updates. (ID-15077)
- You can now configure SPE to use an SSL-enabled End User Directory. (ID-15773)
- The Identity Manager SPE configuration page no longer allow you to set non-SPE account policies. (ID-14833)

MetaView

- The `idmManager` attribute is now stored properly in the user attribute when using MetaView. (ID-14445)

Password Synchronization

- The password synchronization configuration application (`Configure.exe`) no longer truncates the JMS properties at an equal sign (=) when reading from the repository. (ID-12658)

- Passwords intercepted with characters outside of the 7-bit ASCII range are now correctly encoded as UTF-8 before encryption. (ID-15829)

Reconciliation

- Reconciliations no longer stop when resources have duplicate users. (ID-14949)
- Some ambiguous account matches during reconcile are now considered a preferred match to avoid unnecessary reconciliation errors. (ID-14965)
- Reconciliations no longer stop when user normalizations remove all resource information from a user. (ID-15028)
- Using the `checkDynamicallyAssignedAdminRolesAtLoginTo` option no longer causes Reconcile Policy Editor errors when updating the reconcile schedule. (ID-15338)

Reports

- Audit logging is now supported for the creation, modification, and deletion of admin roles. (ID-12514)
- User Reports show the resource `accountID` for all accounts on the resource in a semicolon-separated list. Accounts and resources that are indirectly assigned through a role or resource group are also listed. If there is only one resource account, the `accountID` will display only if it is not equal to the Identity Manager `accountID`. (ID-12820)
- Changes to a user's authentication questions are now logged in the audit logs. (ID-13082)
- The **User Compliance Violation Log** should not be displayed in the Reports menu under the Auditor Reports selector. This is the **Default Compliance Audit Report** task and should be hidden. (ID-14721)
- If you customized the form Conflict Violation Details Form in an earlier release, you should export the form before upgrading to 7.0. Re-import the saved form if you prefer after upgrade. (ID-14772)
- Emailed PDF reports now honor the font and font embedding settings specified at any level. (ID-15328)

Repository

- The `ObjectSource.OP_ALLOW_NOT_FOUND` (`allowNotFound`) option is now honored correctly in calls to `getView` and `checkoutView` for an `IDMXUserView`, and in calls to `getObject` through a `LighthouseContext` in Identity Manager. (ID-11900)
- The Identity Manager Repository now closes (rolls back) an active database connection whenever the repository encounters a Java Error (that is, an instance of `java.lang.Error`). Previously, the repository closed the active database connection whenever it caught a declared Exception or a Runtime Exception (but not an Error). This change guards against leaving an open (uncommitted) transaction when the Java Virtual Machine throws an error (such as an `OutOfMemoryError`). (ID-14411)
- The `setRepo` command's `-n` option now correctly prevents checking for the current repository location. The `-n` option allows the `setRepo` command to succeed when the current repository location is invalid (or the database instance at the current location is unavailable). This change fixes a regression that was introduced in Identity Manager 2005Q4M3 (Identity Manager 6.0). (ID-14809)
- The Identity Manager repository now initializes faster because the `RelationalDataStore` now generates an SQL statement that executes faster against larger database tables. (ID-14937)
- Slow Oracle database systems can no longer cause suspended tasks to execute on more than one Scheduler simultaneously. (ID-15372)
- Removing a role from one user in a similar group of users no longer affects the repository entries of the other users, and no longer prevents you from finding those users when searching by role. (ID-15584)

Resources

- Added the **Failover Servers** resource parameter field for the LDAP resource adapter. This field allows the user to list multiple servers for failover if the preferred server fails. The LDAP Resource adapter uses JNDI to maintain the connection to the LDAP directory. JNDI therefore will automatically attempt to connect to each server in order until a connection is found. Once a connection is found, JNDI will continue to use this server until it fails and then the process will be repeated. Replication across all of the failover servers is the responsibility of the customer. (ID-10889)
- The `LDAPActiveSync` search filter that searches for changes in the changelog has been optimized for performance. The filter part (`objectClass=changelogEntry`) has been removed from the default search filter. (ID-11722)

You can restore the old behavior by adding the `Remove objectClass` from Search Params Filter resource attribute directly to the resource definition with a value of `false`, as follows:

```
<ResourceAttribute name='Remove objectClass from Search Params Filter'  
  displayName='Remove objectClass from Search Params Filter' facets='activesync'  
  value='false'>  
</ResourceAttribute>
```

NOTE You cannot change this setting from the GUI.

- The NDS Resource Adapter now allows you to merge groups contained in the NDS Template with those groups not defined in the NDS Template. This action is performed from the user interface with user form changes. See `NDSUserForm.xml` for details. (ID-12083)
- Linux adapters can now return a year on last login. (ID-12182)
- In order to use a view from a different Oracle user, you must establish an alias, so that the view can be referred to without qualifying it with a user name. Identity Manager did not detect this, and allowed you to specify such a view in the resource adapter. Identity Manager now detects the error, and provides a message. (ID-12643)
- When viewing users on a Solaris NIS resource, the setting for the primary group is now displayed as the group name. (ID-12667)
- You can now set passwords to not expired when using CUA mode on the SAP resource. (ID-13355)
- The VMS resource adapter now has reconcile abilities. (ID-13425)
- Provisioning now recognizes when an error from a `ResourceAction` script has been captured during user create and update functions. (ID-13465)
- Identity Manager now provides a resource configuration parameter called `enableEmptyString`. You can use this parameter to write an empty string (instead of a `NULL` value) in character-based columns defined as not-null in the table schema. The `enableEmptyString` parameter does not influence the way strings are written for Oracle-based tables. (ID-13737)

The default for this parameter is `OFF` or `FALSE` (existing behavior). To write an empty string, change the parameter to `ON` or `TRUE`.

- Using the Oracle ERP Resource Adapter to update an Oracle ERP account's responsibility no longer causes all of the account's other responsibilities to be updated. (ID-13889)

Only the Oracle ERP audit timestamp for the modified responsibility is updated. The Oracle ERP audit timestamps for all other account responsibilities will remain unchanged.

- NDS adapter Active Sync no longer polls for changes based on the User object's `lastModifiedTimeStamp`. Previously, this attribute was updated whenever a user logged in or logged out. Now, the last modified value is calculated based on the `lastModifiedTimeStamp` of a user's attributes that are defined in the Identity Manager schema. If an attribute's `lastModifiedTimeStamp` is greater than the high-water mark presented by the adapter, the gateway sends this user back to the server as modified. (ID-13896)
- The Shell Script adapter now supports the rename, disable and enable functions. (ID-14472)
- Resolved an issue where Active Directory Active Sync would hang because connections to the gateway were not being closed. Connections would grow to the maximum, and open connections would stay in `CLOSED_WAIT` state. Once the maximum number of connections is met and are connections all in the `CLOSED_WAIT` state, Active Sync will halt until these connections are cleaned up. (ID-14597)
- The attributes map that the adapter sends to the customer's update script will now contain an entry for the null-ed attribute, and the map entry value will be null. Specifically, this condition (an empty value in the attribute map) means that an attribute is being cleared. (ID-14655)
- For some resource adapters, exclusion rules are now applied before users are fetched during reconciling, which allows specific users to be excluded, prevents errors generated by the resource, and can improve performance for a large number of users. (ID-14436)
- Writing SAP activity groups and profiles in a Central User Administration (CUA) environment no longer splits a new table row into two rows when the information is separated by a colon. (ID-14371)
- The LDAP resource adapter will again use the VLV control when listing and searching user accounts, if the LDAP server supports the VLV control and the server is correctly configured. (ID-14526)
- The Oracle ERP User Form now has a Person Name field. This read-only field shows the Oracle HR person's fullname if an Oracle ERP account is linked to the Oracle HR system using the employee number. (ID-14675)
- The SAP adapter now properly reports Disabled status. (ID-14834)
- The `nsaccountlock` activation shortcut can now use logic based on value presence/absence to determine whether an LDAP user is disabled. (ID-14925)
- Identity Manager now honors the Supported Features *deny, ignore* combination setting for a resource. If you select `ignore` the action will not be performed, but in some circumstances it could be shown as a message in the GUI. (ID-14948)
- The Oracle ERP resource adapter now prevents the unlinking of resource accounts if the Oracle ERP resource is inaccessible during full reconciliation. (ID-14960)

- Passwords with characters outside of the 7-bit ASCII range are now set correctly by the gateway (create and update) when Identity Manager is deployed with Tivoli Access Manager and Active Directory. (ID-15006)
- If common resources are configured in System Configuration for use by login, and a common resource login fails, logins no longer fail when there is another resource in the login module stack that is not a common resource and it requires different authentication properties than any of the previous login module resources. (ID-15047)
- If you do a Create Resource Object for a Solaris NIS server resource, select multiple accounts in Users, and then click Save, all of the accounts are now added to the group file in the NIS password source directory in the managed NIS server. Previously, this operation worked only if one account was selected. (ID-15085)
- The ADSIResourceAdapter now closes connections when querying for resource objects. (ID-15098)
- ACF2 connection properties (such as a wider and deeper virtual screen size) can now be specified. (ID-15158) To implement this feature you must import your own an `update.xml` script that contains:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <ImportCommand class='com.waveset.session.ResourceUpdater' >
    <Map>
      <MapEntry key='updateAttributes' value='true' />
    </Map>
  </ImportCommand>
</Waveset>
```

Once the updater has run, the application server needs to be stopped and restarted.

To increase screen size to a model 5 terminal type, the following properties needs to be added:

```
Enable TN3270E: 1
Session Properties: SESSION_PS_SIZE <newline> 5
```

Note the `<newline>` should be interpreted as the `SESSION_PS_SIZE` and 5 parameter go on two separate lines.

- There is a new corresponding Oracle ERP schema resource attribute: `person_fullname`. The sample `$WSHOME/sample/other/CreateLHERPAdminUser.oracle` script has been updated to include an ICX* table and to provide views to the synonyms created for the non-APPS user. (ID-15188)

- The example JDBC scripts did not close ResultSets and Statements when they were no longer needed. In a large application, this could lead to some resource leakage. The example scripts have been modified to close such objects when they are no longer needed. (ID-15254)
- Identity Manager now “traps” and reports output from Delete scripts that overtly return with an error. (ID-15340)
- A storage allocation issue involving character translations has been resolved. (ID-15341)
You must use UTF-8 uniformly on the gateway, and you should configure your windows gateway with a default ANSI code page that is compatible with your application data. In other words, use a windows character encoding that is capable of representing all of the Unicode characters in the data that you manage with Identity Manager.
- The temporary file names that are used when running shell scripts for resource actions have been changed to be more unique over time. (ID-15348)
- For Solaris NIS, Identity Manager no longer adds the `netid` target, which was not required and caused error messages in the traces. (ID-15503)
- For Solaris NIS, Identity Manager no longer prevents use of the `sudo` command if the directory containing Solaris NIS `passwd`, `shadow`, and `group` template files are read-protected from the admin user. (ID-15505)
- For Solaris NIS, an account is no longer partially created if the default primary group is either missing entirely or is a name not found in the group file. (ID-15509)
- A bug has been corrected that caused Solaris NIS user or group ID generation to fail when beginning with an environment with no users or groups, and template `passwd` and `group` files are in a directory other than `/etc`. (ID-15510)
- For Solaris NIS, if two accounts are created in a row and a shell is specified for the first account but not the second (either it is not defined in the `defadduser` file or there is no `defadduser` file), the second account no longer is created with the first account's shell. (ID-15511)
- For Solaris NIS, `defgname` in the `/usr/sadm/defadduser` file is now used to set the default primary group instead of `defgroup`, as an optional source for default values for newly created accounts. (ID-15512)
- Identity Manager no longer stores the Solaris NIS and HP-UX NIS encrypted passwords in both the `passwd` and `shadow` NIS template files when an account is updated. Now, the placeholder value “x” is stored in the `passwd` file. (ID-15593)
- Active Sync no longer continues running when Create Unmatched Accounts is set to true and the Allowed Error Count is exceeded. (ID-15662)
- The PeopleSoft Component Interface adapter can now report disabled status. (ID-15674)

- Identity Manager no longer reads write-only account attributes from an LDAP directory or Active Directory. (ID-15838)
- The Scripted Gateway resource adapter can now correctly capture non-zero return codes from scripts and report an error. (ID-15860)
- Clearing a RACF attribute in a form did not cause Identity Manager to clear the attribute on the user when the form was submitted, it was a noop. Identity Manager now clears the attribute. (ID-15971)
- The NDS Template Resource Attribute now displays the pop-up help (i-Help) rather than the NDS_TEMPLATE_HELP message key. (ID-15986)
- The Enable and Disable resource actions are now supported for the Scripted Gateway resource adapter. (ID-16066)
- The ScriptedGateway resource adapter now passes Resource Attributes to the scripts implementing the getInfo and listAllObjects actions. (ID-16149)
- The GroupWise resource adapter has been deprecated. The NDS adapter should be used instead to manage GroupWise users. (ID-16308)

Scheduler

- Suppressed the output of the syslog entry, 'EVNT00', LockedByAnother error. This caused excessive output into the syslog in a clustered environment. (ID-15714)

Security

- End user password changes initiated by administrators (through SPML or otherwise) are now added to the password history if it is enabled. This fix introduces both a System Configuration option and a View (form) option that enables administrators to toggle the desired behavior. (ID-13029)
 - Administrators can toggle the System Configuration option, based on the login application, which provides a greater amount of flexibility because administrators may not want a behavior that affects all applications.
 - The View option always overrides any system configuration setting.
- A delegated administrator with only report administrator capability can no longer remove out-of-scope organizations (which are being reported on) from a report. (ID-14765)
- An audit log for an organization now includes organizational approvers who are added to or deleted from the organization. (ID-15232)

- An Admin Role administrator now has sufficient privileges to create an Admin Role. When creating a new Admin Role or Capability, the creator might be required to select one or more users who can assign the Admin Role or Capability to other users. This situation occurs when a creator is not authorized to assign Admin Roles or Capabilities. The set of users from which the creator can select assigners is not subject to Identity Manager authorization scoping, since the creator might need to choose one or more users outside their scope of control. The set of available users will now have been granted the “Assign Capability” right. (ID-15980)

Server

- The SPML server now returns errors if requests contain filters using operators that are not yet implemented. (ID-11343)
- Dropping attributes from the "User Extended Attributes" Configuration object did not cause them to be dropped from the WSUser's attributes; old values were retained in the XML. This has been corrected, and the values are now removed from the XML. (ID-11721)
- When you are specifying commands or users for bulk operations via the input area of the GUI, the operation no longer fails with the “An object name must be specified.” even though you actually did specify a user name. (ID-15112)
- The problems that caused OutOfMemory errors when processes intensively accessed a resource (such as reconciliation) have been addressed. (ID-16222)
- To return a workItem-specific list of delegates, Identity Manager now provides the following new public methods, which take the *workItemType* argument. (ID-15787/14152)

```
DelegateUtil#checkWorkItemDelegates()
```

```
DelegateUtil#getWorkItemDelegates()
```

Tasks

When editing a scheduled task, the start date must be re-entered using MM/DD/YYYY format (ID-5675).

Workflow

- Identity Manager’s sample Notify Reconcile Finish task definition now completes and sends email notification upon completion (ID-9259).

Additional Defects Fixed

8691, 8961, 9913, 10100, 10802, 11538, 12509, 12571, 12585, 12872, 13223, 13251, 13258, 13701, 13741, 13965, 14282, 14334, 14459, 14564, 14663, 14748, 14893, 15036, 15098, 15234, 15345, 15424, 15746, 15798, 15851, 15864, 16041, 16087, 16121, 16171, 16177, 16215, 16288,

Known Issues

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

- [Identity Manager](#)
- [Service Provider Edition](#)

Identity Manager

This section describes known issues and workarounds for Identity Manager, and the information is organized as follows:

- [General](#)
- [Install and Update](#)
- [Account Management](#)
- [Approvals](#)
- [Auditing](#)
- [Integrated Development Environment \(IDE\)](#)
- [Login Configuration](#)
- [Organizations](#)
- [Policies and Capabilities](#)
- [Reconcile and Import Users](#)
- [Reports](#)
- [Resources](#)
- [Resource Object Management](#)
- [Resource Groups](#)
- [Security](#)
- [Servers](#)
- [Sun Identity Manager Gateway](#)
- [Tasks](#)
- [Workflow, Forms, Rules, and XPRESS](#)

General

- Required fields set on the resource schema map are only checked when a user account is created (ID-220). If a field is to be required on user updates, then the user form should be configured to ensure that the field is required.
- No checking is done on organization name, administrator name, account name, user attribute name (left hand side of schema map), or task names for invalid characters (ID-1145, 1206, 1679, 1734, 1767, 2413, 3331). You cannot use a dollar (\$), a comma (,), a period (.), an apostrophe ('), an ampersand (&), a left bracket ([), a right bracket (]), or a colon (:) in the name for these types of objects.
- A misleading error message is given on the account page if you try to perform an action after your session has timed out (ID-1223).
- The calendar object is not fully viewable if the browser is using large fonts (ID-2120).
- The Select All checkbox on the Find Results page and the List Task page does not become un-selected if one of the items in the list is un-selected (ID-5090). The selectAll checkbox is ignored during the resulting action if not all of the members in the list have their checkbox selected.
- If you make a change to a custom message catalog, it is necessary to restart the server in order to see your changes. (ID-6792)
- The current mechanism for detecting a failed Server assumes that all the systems in an Identity Manager cluster are synchronized with respect to time. (ID-7064) With the default failure interval of five minutes, if one server is five minutes out of sync with another, the server that is ahead will declare the server that is behind to be dead, causing unpredictable results.

Workaround: Maintain better time synchronization or increase the failover interval.

- On Windows, if you are logging in as a user whose name contains double-byte characters and the default encoding for the machine only supports single-byte characters, you must set the USER_JPI_PROFILE environment variable to an existing directory whose name contains only single byte characters. (ID-8540)
- If an expanded node contains less than one page of data and you insert a new child of that node (for example, if you are creating a User in the organization) *before* the first record on the page, Identity Manager will insert a page with one item before the current page on the subsequent refresh. (ID-12151)

Workaround: To *realign* the pages, click the First Page button.

- If you modify a Role form to change the `showSuperAndSubRoles` variable from 0 to 1, and then import a super role object definition file containing existing subroles from the Configure tab; those subroles will not be modified to include the <SuperRoles> section. However, if you use the Identity Manager graphic user interface to create a super role, the subroles referenced by that super role will be updated. (ID-15053)

This issue can occur with roles created outside Identity Manager that have references to existing roles (either subroles or super roles) already in the system.

When importing these roles, the roles that already exist in the system are not updated to reflect the new relationships; for example, referential integrity is not maintained. Use the RoleUpdater to check and correct the referential integrity if roles are imported in this way.

Workaround: See ID-15482, described in “Roles” on page 29.

- You must update the JDK on which you run your application server to JDK 1.4.2_13 to support the new Daylight Savings Time (DST) beginning in 2007. (ID-15475)

To update, perform these steps:

- a. Update the gateway hosting time functions from

<http://www.microsoft.com/windows/timezone/dst2007.mspx>

(Identity Manager obtains gateway hosting time functions from the Windows operating system.)

- b. Upgrade to a compliant version of Java on the application server. *Identity Manager Installation* provides directions for shutting down, upgrading, and restarting your application server.
- c. Review the list of tasks scheduled to start within the new extended periods of DST (see the following for more details about when these periods occur).

After applying the DST patches, you must reschedule any items that are scheduled to start within this time frame. Any recurrent items that run at least once after you have applied the DST patch, and before the beginning of these periods, will run at their expected times.

Refer to Java upgrades or use the *tzupdater* tool

(<http://java.sun.com/developer/technicalArticles/Intl/USDST/>) to address DST issues.

Also see Sun Alert for Java.

Daylight Savings Time (DST) in the United States and Canada has been extended to begin earlier and end later than in previous years. These extended periods of DST are from the second Sunday of March to the first Sunday of April, and from the last Sunday of October to the first Sunday of November. For 2007, these periods are from March 11th to April 1st, and from October 28th to November 4th. Issues caused by non-compliant software will continue indefinitely until the software is made compliant.

NOTE Failure to implement the preceding steps might have the following effects:

- Some scheduled tasks (including reconciliation and Active Sync) might run one hour off-schedule, depending upon specific scheduling parameters.
 - Reports might include or exclude events up to an hour outside the specified range.
 - Customer modifications with date dependencies might show erroneous results.
-

- The menu in the end user interface that allows an approval work item to be forwarded to another approver from the list of work items is not populated correctly. (ID-15935)

Workaround: Insert the following field into the form after the `userIds` field, replacing the "user*" strings with the desired list of `accountIds`:

```
<Field name='forwardingUsers'>
  <Derivation>
    <list>
      <s>user1</s>
      <s>user2</s>
    </list>
  </Derivation>
</Field>
```

- If you modify settings (such as adding additional column attributes) on an existing changelog, these modifications might not appear in a pre-existing changelog CSV file. (ID-15973)
- Strings that are displayed in the tabs of the TabPanel display component (used, for example, in the Tabbed User Form) will wrap if they contain spaces. To change this behavior so that the strings do not wrap, the following two lines should be added 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}
```

- While in a localized Identity Manager session, users might encounter partial localization (a mix of English and the selected language) in Process Diagram applets. (ID-16139)

- When editing a role, if a second role is included as both a super role and a sub-role, a circular reference will exist, possibly resulting in a `StackOverflowError`. (ID-16326)
- Direct-mode password synchronization requires `SimpleRpcHandler` to be configured in the `web.xml` file. By default, this handler is not provided as a handler for the `rpcrouter2` servlet. (ID-16469) To use direct-mode password synchronization, set the handlers initialization parameter in the following way:

```
<init-param>
  <param-name>handlers</param-name>
  <param-value>com.waveset.rpc.SimpleRpcHandler,com.waveset.rpc.PasswordSyncHandler</param-value>
</init-param>
```

Note that `SimpleRpcHandler` is known to interfere with certain `RemoteSession` calls. If you plan on using `RemoteSession` as well as direct-mode password synchronization, configure a separate servlet for handling `RemoteSession` calls.

Install and Update

NOTE For issues that affect only this release, see [“Installation and Update Notes” on page 69](#).

- If you update from a 6.x install, but want to start using the new end-user pages, you must manually change the system configuration `ui.web.user.showMenu` to `true` to get the horizontal navigation bar to appear. (ID-14900, 16401)

You must also manually change the system configuration end user form mapping so that it looks like this:

```
<Attribute name='endUserMenu' value='End User Dashboard' />
```

- WebLogic 9.0 is not supported because a compiler error affects several pages.

Workaround: Use WebLogic 9.1 or 9.2 instead. (ID-16002)

- There is no database upgrade script for the Service Provider transaction store. When upgrading from Identity Manager 5.6 (Service Provider Edition 1.0) or Identity Manager 6.0 to 7.0 or 7.1, a new column (`userId`) has to be added to the existing table. The sample database scripts (`create_spe_tables.*`) in this release show the expected type and the default maximum value length of this column. (ID-16423)

- While upgrading, under rare circumstances the following error may be seen when attempting to run `update.xml`:

```
com.waveset.util.InternalError: Reserved item
'ComplianceViolation:LastModified' name is already in use by existing item
'ComplianceViolation:LastModified'.
```

If this occurs, delete the offending item from the repository with the following SQL:

```
delete from object where type='ComplianceViolation' and name='LASTMODIFIED'
```

After this, you can resume the upgrade at the point at which it failed, importing `update.xml` again. (ID-16437)

Account Management

- It is possible to create NT accounts that have account names longer than 20 characters and that the NT native tools cannot manage (ID-710).
- An administrator cannot save resources or roles that contain organizations that he does not manage (ID-839).
- Sorting the columns on the Provisioning Results page adds additional empty rows to the results (ID-1105).
- Approvals of several hundred user accounts take a considerable amount of time (ID-1149).

Workaround: Approve user account records in smaller groups.

- Approval records owned by an administrator who no longer has approval capability cannot be approved (ID-1150).

Workaround: Remove the administrator from resources, roles, and organizations in which he has approval rights, then approve any outstanding approval records prior to removing the administrator or the approval capability for that administrator.

- Updating a user without making any modifications does not show detailed results page (ID-2327).
- When creating a new user or adding a resource to an existing user, if the distinguished name for the user is incorrect, the incorrect value is cached until the administrator logs out (ID-2508). Attempts to re-create the user after fixing the distinguished name are not successful until after the administrator logs out.

- Windows Active Directory requires the gateway to run as an administrator who can create directories (ID-2919). Identity Manager can create home directories on Windows 2000 systems. The home directory account creation is being performed by the user the gateway process is running as, instead of the administrator specified in the resource definition.

Workaround: Change the user that the gateway is running as from Local System to an account that has permission to create remote shares and set permissions on those shares. This account will also need Bypass traverse checking and Act as operating system privileges.

- The Windows NT resource incorrectly throws a warning message instead of an error message when errors occur when disabling a user account (ID-3222).
- A `java.lang.NullPointerException` may be seen when removing all the resources from a user via the edit user page (ID-4811).

Workaround: Use the user delete page to either unlink or delete these resource accounts from the user.

- If an Identity Manager user is created and assigned to a Windows Active Directory resource where the user account already exists, the user will be created without a GUID attribute in the resource info (ID-5114). This GUID is used to detect changes to the user's organization or name in the Directory. Running reconcile from the resource will fix this problem.
- When creating a user, a warning is given if you add a Role to the user that contains a resource that is directly assigned (ID-5385).
- A "Forward To" administrator cannot be specified when a user is being created. This option can only be set when editing the user (ID-5695).

Approvals

- When updating a user and selecting to run the update in the background, an approval activity appears on the task results page (ID-3301). This approval can be ignored.
- Approval records for an administrator do not show up after the user is renamed (ID-3386).

Workaround: Resolve all outstanding approvals before renaming the user.

- Previously approved or previously rejected approval records cannot be viewed by an administrator if the user being approved belongs to an organization that the approver does not control (ID-3494).
- Resource retries tasks appear in the pending approval list for Configurator (ID-3508).

Auditing

- During a scan, there is no support for retrying user accounts that could not be fetched from resources, or where other failures occur. These failures are reported when the scan is complete, but there is no automated way to rescan the accounts. (ID-9112)
- Identity Auditor attempts to keep users in compliance between policy scans by enforcing policy whenever the user is edited. If editing a user that has assigned audit policies and also is in violation of a policy, you cannot save changes to the user, even if the change is as simple as moving a user to another organization. (ID-9504)

Workaround: Use the right-click move (or find then move) functionality on the user applet, or temporarily disable the audit policy checks.

To disable the auditor policy checks, edit the system configuration and remove `userViewValidators` property. This property which has a value of a List of strings is added during the import of `init.xml` or `upgrade.xml`.

- In the AuditPolicy, Resource and Organization Violation History reports, implementing logarithmic scaling for a STACK chart type may result in unusual display behavior. (ID-9522)
- Currently, the Auditor Access Scan Report administrator cannot schedule an Audit Policy Scan. An error, Error message: Create access denied to Subject auditadmin on type TaskSchedule is displayed. To schedule any task, administrators must have create privileges for the TaskSchedule authType. (ID-14713)

Workaround: Edit the administrator to assign the create privilege for the TaskSchedule, or specify a user with at least the Auditor Administrator or Waveset Administrator capabilities.

- If you have created Audit Policy Scan reports in previous versions of Identity Auditor, these reports will not be visible when you upgrade to Identity Manager 7.0. To correct this, an administrator with the Auditor Report Administrator capability (or higher) can edit these specific reports and change the visibility to **run**. (ID-14881)
- When running Audit Scans that produce multiple violations, Auditor might create a remediation workflow to manage processing of the violations. The default MySQL setting for `max_allowed_packet` (1M) is too small for a workflow with dozens of violations. If this limit is reached, Auditor will not start the remediation workflow.

Workaround: For heavy use of Auditor, this value should be much larger. To address this issue, add `max_allowed_packet = 32M` to the MySQL configuration file (`my.cnf`) and restart the database server. (ID-15830)

- Audit policy names cannot contain these characters: ' (apostrophe), . (period), | (line), [(left bracket),] (right bracket), , (comma), : (colon), \$ (dollar sign), " (double quote), = (equals sign). (ID-16078)
- Changing severity and priority values for Compliance Violation remediations can be misleading. The initial values in the form are *not* the current values of the Compliance Violations. They are the last values set when making a change. It is important that you know what severity/priority value you want while still viewing the list view, because you cannot determine the current values when on the page that lets you change the values. (ID-16040)
- ComplianceViolations created before the IdM 7.1 upgrade will not allow the severity or priority to be set. The error message returned indicates that the Compliance Violation no longer exists, but this is incorrect. The violation does exist, but IdM is unable to set the severity or priority. (ID-16420)

Integrated Development Environment (IDE)

- Renaming objects using Identity Manager IDE should be done through the right-click context menu in the Projects explorer, instead of editing the XML using the editor. (ID-13828)
- The XML Navigator has been disabled in IDM IDE. Windows ->Navigator opens the Navigator panel and <No view available> is displayed. (ID-13390)
- Project delete functionality is not supported. (ID-14013)
- When closing a project, the Discard All option does not work properly. If you wish to discard your changes to an object, you must close the editor window and select Discard. This is a known issue with NetBeans (bug 84236). (ID-14164)
- If you are working with the standard Identity Manager IDE project, start the bundled Tomcat instance, and the Tomcat Manager dialog displays, it generally indicates one of the following conditions: (ID-15546)
 - Multiple Tomcat instances are running.
 - A credentials mismatch has occurred.

This is a known NetBeans issue.

Workaround: You must insure that only one Tomcat instance is running on the host machine and configured to listen on the same port as the bundled Tomcat.

The credentials stored as part of the bundled Tomcat server must match those stored on the Server Manager's Username and Password fields. For more information about these field values, go to the following website:

<http://wiki.netbeans.org/wiki/view/FaqInstallationDefaultTomcatPassword>

To check the port number of the bundled Tomcat and the stored credentials:

- a. Select the Identity Manager IDE Runtime tab and expand the Servers and Bundled Tomcat nodes.
 - b. Right-click the Bundled Tomcat node and select Properties from the pop-up menu.
 - c. When the Server Manager dialog displays, check the Server Port, Username, and Password field values.
- The Clone Document feature does not work. (ID-15725)
 - If you perform a diff action on a document and do not save your changes, the diff action will not show any results. Currently, there is no warning message to indicate this situation. the Identity Manager IDE can only perform a diff action against the file contents, and not what is shown in the Editor window. (ID-15952)
 - If you perform a diff action on a directory containing unsaved files, no results will display in the Diff Output window. (ID-15955)
 - When using the expression builder to create an invoke statement, a window is opened that displays the Javadoc for the selected method. Currently, you cannot use the scroll bars to scroll through the document. This means that for some methods, the window will not display the entire Javadoc. (ID-16093)

Workarounds:

- Once you have selected the method the java doc will be transferred temporarily to the bottom of the expression window. You will be able to scroll through the entire java doc here, however this is only a temporary copy and once you click away into another expression element or a different expression entirely it will not be restored.
 - Use the regular Javadoc, which is provided in the *Image/REF/javadoc* directory of the installation media.
- A null pointer exception will be thrown when you check validation in the design view. (ID-16168)

Workaround: Perform validation from the XML (source view).

Login Configuration

- Pass-through authentication module does not work for the Domino resource (ID-1646).

- Changes made to the Administrator Login Setup and User Login Setup pages are not visible to other administrators logged in (ID-3487). To see the changes, the other administrators will need to log out of the Administrator Interface and log back in.
- If an Administrator logs in and selects Change My Password, and then selects another tab, their account is locked until the lock expires. (ID-3705)

If another Administrator attempts to edit that locked Administrator, the following message displays:

```
com.waveset.util.WavesetException: Unable to access account #ID#Configurator at this time. Please try again later.
```

If that Administrator clicks OK, the workflow process diagram from the last action is displayed.

Organizations

- When deleting multiple organizations, if the delete fails on one organization, all the remaining organizations are not deleted (ID-517).
- Renaming an organization when there are provisioning requests pending that have users belonging to the organization will cause the provision request to fail (ID-564).

Workaround: Ensure there are no outstanding requests before renaming an organization.

- When creating a new organization, if the User Member Rules option is selected before specifying an org name, when the page is refreshed, an organization ID will appear in the Organization name field (ID-6302). The name can still be set prior to saving the new organization.

```
( ) - Warning: Parenthesized values in field 'Approvers' do not match any of the allowed values.
```

Policies and Capabilities

- The Identity Manager account policy attribute Reset Notification Option has a value option of “administrator” that has no effect (ID-944). The only viable options are “immediate” and “user”.
- When deleting multiple roles, if an error is encountered, the entire operation will stop instead of continuing to the other roles (ID-1168).

- The minimum number of questions a user must answer can be set to a value greater than the number of defined questions (ID-1834). If this situation occurs, the user will not be able to log in using the “Forgot My Password” option.
- The Default Lighthouse Account Policy cannot be cloned by editing the policy, changing the name, and selecting to create a new object (ID-5147).

Workaround: Create a new account policy.

Reconcile and Import Users

- Importing users from a CSV file does not update resource attributes if the user already exists in Identity Manager (ID-2041).
- Comma-separated-value (CSV) file that is loaded with single quotes (') in the account IDs are translated to question marks (?) (ID-2100).
- Scheduled tasks will not show up in a search on the "Find Tasks" page when using the "Is Scheduled" option (ID-5001).
- Reconciliation fails when run against a Red Hat version 8 resource (ID-6087).
- Reconciliation of an Oracle ERP resource will complete with errors if connection pooling on the resource is enabled (ID-6386). Workaround is to turn off connection pooling during reconciliation.

Reports

- Security administrators cannot run or create reports (ID-1217).
- Risk analysis reports can be viewed by administrators other than report administrators (ID-1224).

Workaround: Give administrators Report Administrator capability.

- Report results that are emailed with the plain text option are not formatted (ID-2191).
- Audit Log entries may not be recorded for large results (ID-5050).
- The ticker will not display when selected if there are organizations with apostrophes (') in their name (ID-5653).

- If you attempt to run an Administrator Report and select to Report only Administrators which belong to a specific organization which has no administrators, a `java.lang.NullPointerException` error is returned (ID-5722).

Resources

- Resource test button does not test all fields (ID-51).
- Resource port assignments can be set to values greater than 65535 (ID-59).
- Bad error message displayed when setting incorrect Active Directory group name (ID-393). If you attempt to set an Active Directory group name to “groupname” instead of “cn=groupname,cn=builtin,dc=waveset,dc=com” an error message stating “array index out of bounds” is displayed.
- Required account attributes are sometimes ignored if there is another resource with the same account attribute name that does not have the required flag set (ID-1161).
- If an administrator attempts to add an organization to a resource that he does not have rights over, an error will appear. The edit of the resource must then be canceled and the resource edited again to make any other changes to the resource (ID-1274).
- The error message when a resource account password or username is not correct on a PeopleSoft resource is not clear (ID-2235). The error message states:

```
bea.jolt.ApplicationException: TPESVCFAIL - application level service failure
```

- Windows Active Directory resource actions that use the `%DISPLAY_INFO_CODE%` exit status cause the action to fail with errors (ID-2827).
- Windows NT resource actions that return a non-zero exit code do not cause the action to fail (ID-2828).
- Setting a user's primary group ID on Active Directory cannot be done when creating the user (ID-3221).

Workaround: Create the user without setting the primary group ID, then edit the user and set the value. The primary group ID is also set by number and not by the distinguished name (DN) of the group.

- Resource IP addresses are cached in the JVM after the hostname is resolved to an IP address. If a resource IP address is changed, the application server must be restarted for Identity Manager to detect the change (ID-3635). This is a setting in the Sun JDK (version 1.3 and higher) and can be controlled with the `sun.net.inetaddr.ttl` property, which is typically set in `jre/lib/security/java.security`.
- You cannot create multiple accounts for a single user on Oracle resources (ID-3832).

- End-users cannot use the self-discovery feature for Domino resource accounts (ID-4775).
- If a user is moved from or to a sub-container within the Active Directory organization, the Active Sync adapter will detect the change, but when you view the user on the edit page, (or make a change and view the confirmation page) the user's accountId is still displayed as the original DN (distinguished name) (ID-4950). Because we use GUID to modify the user, this will not cause any operational problems. Running a reconcile against the resource will fix the problem.
- If a user is moved from an Organization (OU) to a sub-organization, the LDAP ChangeLog adapter will not recognize the change and assumes the user has been deleted. The user object is then locked in Identity Manager (if that is the current setting), and a new account is not created for the moved account (ID-4953).
- The pooled connections used by the UNIX resource adapters can be left in an undetermined state if an error occurs while executing a command or script (ID-5406).
- NDS organizations can be created in the top level of the tree only by setting the Base Context for the resource to "[ROOT]" (ID-5509).
- On NDS, if you edit a field (such Grace Login Limit) on the initial provision, and do not provide values for the boolean fields, all the boolean fields are set to false (ID-6770). This prevents you from setting the other fields on the restriction tab which require certain check box values to be true. To avoid this, always ensure all your boolean fields are true when you expect them to be, so they are properly pushed when editing other fields.
- If you change the password for a UNIX machine using the Manage Connection --> Change Resource Password feature, the task name that appears is:

```
_FM_PASSWORD_CHANGING_TASK null:null
```

A user-friendly name should be displayed. (ID-6947)
- You cannot use the manage connection feature for UNIX resources that use NIS (ID-6948). An error is thrown because the password you are trying to change is for root, but NIS does not manage the root account.
- When updating users by selecting update from an Identity Manager organization, users with a Sun One ID Server account will get an error if those users were created natively and loaded into Identity Manager (ID-7094). The work around is to update those users individually.
- Identity Manager still contains the following deprecated classes:
 - com.waveset.object.IAPI
 - com.waveset.object.IAPIProcess
 - com.waveset.object.IAPIUser

Custom adapter classes should no longer refer to these classes, and should instead refer to the corresponding classes in package `com.waveset.adapter.iapi`. (ID-8246)

- An error occurs when trying to delete a user who has an account on the PeopleSoft Component Interface resource. This resource currently does not support account deletions. (ID-9000)
- If you leave the New Resource Object wizard without clicking the **Save** or **Cancel** button, the abandoned form may not be destroyed and may interfere with the creation of subsequent new resource objects. (ID-11033) This leads to an error that says

No resource form id found in options or view.

Workaround: Always use the Cancel button to abandon the New Resource Object wizard.

- Temporary tablespaces do not honor quota settings and if attempted from Oracle 10gR2, a SQL exception occurs. (ID-12843)

Until now, the resource adapter would set a quota on a temporary tablespace — even if the `oracleTempTSQuota` attribute was not mapped. This behavior has changed. If you map the `oracleTempTSQuota` attribute, the old behavior is maintained (no change), but if you remove the mapping, no quota will be set on the temporary tablespace.

Workaround: For Oracle 10gR2 installations, remove the `oracleTempTSQuota` attribute from the resource adapter.

- There are two known issues with the Remedy Integration template editor. (ID-14729)
 - The default Remedy Schema value "HPD:HelpDesk" is not appropriate for later versions of BMC Remedy. Later versions do contain a schema "HPE:Help Desk".
 - The Choices columns is not displayed for some fields. This does not affect the ability to use Remedy templates.
- NDS/Groupwise users created by Identity Manager that possess the Access and AccountID fields can appear to not have their corresponding values saved when inspected by certain viewers within the NDS Console 1 application (for example, by selecting user's properties and then selecting the Groupwise tab).

However, if the user's Groupwise Diagnostic -> Display Object "viewer" is used instead, the field are then seen. Updates made by Identity Manager to the aforementioned fields do not seem to be affected by this "viewer" bug. (ID-16330)

- The IS_DELETE rule (used to configure the PeopleSoft Active Sync adapter) is not displayed in the pull-down menu of known rules. (ID-16398)

Workaround: Edit the `$WSHOME/sample/rules/PeopleSoftRules.xml` file and change to the text below. Then re-import the file using Configuration->Import Exchange File.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Waveset PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Waveset>
  <Rule name='IS_DELETE'>
    <Description>Should the active sync event delete the user?</Description>
    <or>
      <eq><ref>activeSync.Status</ref><s>T</s></eq>
      <eq><ref>activeSync.Status</ref><s>L</s></eq>
    </or>
  </Rule>
</Waveset>
```

- The Oracle ERP adapter erases previous values for responsibilities during a single user load. The user's current responsibility description, start_date, and end_date are not formatted into form properly on getUser(). This could cause responsibility data to get corrupted. (ID-16414)

Workaround: Edit the includeResponsibilities field in the sample user form OracleERPUserForm.xml to include a default value. Then re-import the file using Configuration->Import Exchange File.

```
<Field name='includeResponsibilities'>
  <Display class='Checkbox' action='true'>
    <Property name='title' value='Add Direct Responsibilities' />
  </Display>
  <Default>
    <cond>
      <gt>
        <length>
          <ref>global.responsibilities</ref>
        </length>
        <i>0</i>
      </gt>
      <s>true</s>
    </cond>
  </Default>
  <Disable>
    <not>
      <ref>global.showOracleERPFields</ref>
    </not>
  </Disable>
</Field>
```

—OR—

Select the **Load** button when on attributes page to load the user a second time.

Resource Object Management

- A Windows Active Directory object (Group, Organizational Unit, or Container) cannot be renamed on the List Resources page (ID-3329).
- Cannot create new LDAP groups if there are users with multi-valued CNs (ID-3848).

Workaround: Manage the members of the group by DN instead of CN which is configured in the LDAP Create Group Form.

Resource Groups

- Using the return key on the Create or Edit Resource Group page clears the changes made on the page (ID-3430).
- Resource Group reports cannot be saved as a CSV file. (ID-8001)

Security

- Identity Manager no longer issues a `java.lang.StackOverflowError` exception when the following conditions occur: (ID-15035)
 - a. At least one dynamic (rule driven user members) org is defined under Identity Manager
 - b. The user form includes a `<Field>` that calls `getObject` on `Type.USER`

The `StackOverflowError` was caused by an infinite loop resulting from the Expansion permission evaluation.

This issue was resolved by adding two new User View boolean options:

- `NoFormDerviation` (Default true)
- `NoFormExpansion` (Default true)

These options will always be passed when you request a User View be passed to a rule. Setting these options to `true` prevents form derivation and expansion from occurring.

NOTE

When you set these options to `true`, and form field Derivation or Expansion are needed within the rule, they will have to be done as part of the rule logic.

See "Setting View Options in Forms" in *Identity Manager Workflows, Forms, and Views* for more information about how to set View Options.

Servers

- Customers using Identity Manager 4.x should be sure that their hosting server is not using an ambiguous time zone. For example, EST can be used in either Australia or the United States. However, using GMT+10 or GMT-6 is unambiguous. (ID-8297)
 - The `com.waveset.rpm.SimpleRpcHandler` class has been deprecated as of 7.1 (ID-14756)
1. Add the following servlet definition to the deployment descriptor

```
<servlet>
  <servlet-name>rpcrouter3</servlet-name>
  <display-name>OpenSPML SOAP Router</display-name>
  <description>no description</description>
  <servlet-class>
    org.openspml.server.SOAPRouter
  </servlet-class>

  <init-param>
    <param-name>handlers</param-name>
    <param-value>com.waveset.rpc.PasswordSyncHandler</param-value>
  </init-param>

  <init-param>
    <param-name>spmlHandler</param-name>
    <param-value>com.waveset.rpc.SpmlHandler</param-value>
  </init-param>

  <init-param>
    <param-name>rpcHandler</param-name>
    <param-value>com.waveset.rpc.RemoteSessionHandler</param-value>
  </init-param>
</servlet>
```

2. Add the following servlet mapping to the deployment descriptor:

```
<servlet-mapping>
  <servlet-name>rpcrouter3</servlet-name>
  <url-pattern>/servlet/rpcrouter3</url-pattern>
</servlet-mapping>
```

To use `createView` with `RemoteSession`, you need to use the `rpcrouter3` servlet. To access the `rpcrouter3` servlet, you need to use the `RemoteSession(URL, String, EncryptedData)` constructor.

- Microsoft SQL Server 2000's locking characteristics can cause deadlock errors under certain heavy load conditions in Sun Identity Manager. (ID-16068)

Workaround: Upgrade from Microsoft SQLServer 2000 to Microsoft SQLServer 2005 using native mode.

Microsoft SQLServer 2005 (which has new functionality called *Snapshot Isolation*) has been tested with Identity Manager under heavy load, and does not exhibit the same deadlocking problems as SQLServer 2000.

Some customers also found it useful to alter their database to use `READ_COMMITTED_SNAPSHOT` as follows:

```
ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON
```

</quote>

- If you deploy Identity Manager in the Sun Application Server and pass the `--precompile` option, JSP precompilation fails because Identity Manager uses JSP fragments but does not name them as a `.jspxf`. (ID-16373)

Workaround: Rename these files with a `.jspxf` extension.

Sun Application Server 8.2 and 9.0 now provide an option to ignore precompilation errors due to `.jspx` fragments. For more information, see

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6393940

Sun Identity Manager Gateway

- The Sun Identity Manager Gateway occasionally will not stop when the Stop button is pressed on the NT Services screen. (ID-590)

Workaround: Cancel the stop service request (if it is still hanging) and stop the service again, or exit the NT services dialog and re-enter and attempt the stop operation again.

- Users cannot be added to groups in an NT domain if the gateway is in a remote trusted domain (ID-711).
- The gateway occasionally will not stop when using `'net stop "Sun Identity Manager Gateway"` (ID-2337).

Tasks

- Administrators with Identity Manager Administrator privileges cannot view the manage tasks page if there is a Risk Analysis task in the list of tasks (ID-1225).
- Administrators who do not control Top cannot create Discovery or ResourceScanner scheduled tasks (ID-1414).

- The Find Task page does not display the number of tasks matching the search criteria (ID-5152).
- Delegated administrators who do not control Top can schedule tasks and view the task results, but cannot view the task after it has been created (ID-6659). The scheduled task was placed in Top and the delegated administrator does not have rights to view the object.
- A field named Deferred Tasks was added to the library. It provides the ability to list deferred tasks on a user. To implement this field, the following line must be added the Tabbed User Form and Tabbed View User Form (ID-7660).

```
<FieldRef name='Deferred Tasks' />
```

Workflow, Forms, Rules, and XPRESS

- You cannot use the XPRESS `<eq>` function to compare Boolean values to TRUE or FALSE strings or to the integers 1 or 2 (ID-3904).

Workaround: Use the following

```
<cond>
  <isTrue><ref>Boolean_variable</ref></isTrue>
  <s>True action</s>
  <s>False action</s>
</cond>
```

- Path expressions do not work when iterating a list of generic objects via a dolist (ID-4920).

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <ref>genericObj.name</ref>
</dolist>
```

Workaround: Use `<get>` / `<set>` as shown:

```
<dolist name='genericObj'>
  <ref>listOfGenericObjects</ref>
  <get><ref>genericObject</ref><s>name</s>
</dolist>
```

- If you use `global.attrname` variables for fields in your user form, and the attribute is shared among more than one resource, you should also define a Derivation rule (ID-5074). Otherwise, if the attribute has been changed natively on one of the resources, the attribute may or may not be picked up and propagated to the other resources.
- Cannot use special strings beginning with `&` in HTML components of forms. For example, ` ` will no longer appear as a space. This issue was introduced because of a change to support special characters (`&\<>`) in Select lists (ID-5548).

- Form, workflow and rule comments contained in `<Comment>` tags have `
` strings in them representing the line feed character (ID-6243). These characters are only seen when viewing the XML for these objects; the Identity Manager server and Business Process Editor will process these characters properly.
- If you use the delete templates with bulk actions, they will override the bulk action behavior with no indication that this action occurred. (ID-10320)
- If you use the Resource Table User Form for editing users, when editing a user's resource, the resource attributes are not fetched when the form first appears.

Workaround: Click the Refresh button, which will fetch the attribute data. (ID-10551)

Service Provider Edition

This section describes known issues and workarounds for Identity Manager SPE.

- Identity Manager SPE and Sun Java System Portal Server may not be compatible; there is a problem related to the encrypted libraries. (ID-10744)

This problem may be corrected by setting the following values in Portal Server's `/etc/opt/SUNWam/config/AMConfig.properties` file, and then restarting the web container:

```
com.ipanet.security.encryptor=com.ipanet.services.util.JCEEncryption
com.ipanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.
    JSSESocketFactory
com.ipanet.security.SecureRandomFactoryImpl=com.ipanet.am.util.
    SecureRandomFactoryImpl
```

- When working with SPE dashboards: If graphs take several minutes to load the first time, then you should verify that your browser is not configured to use the Microsoft Java Virtual Machine (MSJVM). Identity Manager SPE does not support using MSJVM to run browser applets. (ID-10837)
- Some configuration options that appear in the Identity Manager Administrator interface are not used with Identity Manager SPE. (ID-10843). Among these are:
 - Resource options: exclude accounts rule, approvers, and the organization that the resource is assigned to.
 - Role attributes

- By default, auditing is not performed when using the `checkinObject` and `deleteObject` IDMXContext API calls. Auditing has to be explicitly requested by setting the `IDMXContext.OP_AUDIT` key to true in the option map passed to these methods. The `createAndLinkUser()` method in the `ApiUsage` class shows how to request auditing. (ID-11261)
- Dashboard graph name changes do not work properly. Although the new name is displayed when editing the graph, the graph is not referenced by the new name on any other pages. (ID-11690)
- The default Service Provider login module group expects the Service Provider resource to be named 'SPE End-User Directory'. If the name of the resource is different, then the Service Provider end-user login page will not function properly. The page will not show the login related fields. (ID-14891)

Workaround: Update the resource name in the `UI_LOGIN_MOD_GRP_DEFAULT_SPE_PWD` `LoginModGroup` object to reference the correct resource name.

- The SPE Sync task is a scheduled task, so stopping it from the Tasks page will not stop synchronization. To stop it, you can disable the schedule itself. (ID-16000)

Workaround: The preferred method of starting and stopping is either through the product interface on the Resource page, or programmatically (for example, from a workflow) through the `SessionUtil` methods to start and stop SPE Sync. To prevent SPE Sync from starting automatically whenever an Identity Manager server instance is started, you must disable it from the Synchronization Policy for the resource. Stopping SPE Sync through the UI or `SessionUtil` method will merely stop synchronization until another Identity Manager server instance is started.

- A `javax.servlet.UnavailableException` occurs when you use the Identity Manager SPE End User Login page in WebSphere, and a 404 error displays in the browser. (ID-16001)

Workaround: You must set the following properties in the IBM 1.5 JDK:

- a. In the `was-install/java/jre/lib` directory, rename the `jaxb.properties.sample` to `jax.properties` and uncomment these two lines:

```
javax.xml.parsers.SAXParserFactory=
    org.apache.xerces.jaxp.SAXParserFactoryImpl
javax.xml.parsers.DocumentBuilderFactory=
    org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
```

- b. Save the file and restart the application server.

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

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 13 for information about which versions can be upgraded to Identity Manager 7.1.)

The information in this section is organized as follows:

- [Upgrade Issues](#)
- [Using the Identity Manager Upgrade Program](#)
- [Upgrading Manually](#)

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

```

- 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)

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 75](#).
 - 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	<ul style="list-style-type: none"> • Before updating your repository schema, make a full backup of your repository tables. • The upgrade of MySQL databases is highly involved. Refer to <code>db_scripts/upgradeto2005Q4M3.mysql</code> 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	<ul style="list-style-type: none"> • Before updating the repository schema, make a full backup of your Repository tables. • Refer to the <code>db_scripts/upgrade7.0.DBMSName</code> 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 73](#) 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 TEMPLIBPTH=%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 74](#) 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 73](#) 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 74](#) for instructions.)

Deprecated API

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: <code>new BufferedAccountQueue(new SimpleAccountSupplier(accounts));</code>
com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter	References to this class should be replaced with an AccountIterator based on the Supplier model. For example <code>BufferedAccountQueue(new SVIDAccountSupplier)</code> .
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.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.SourceAdapterManagerView
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
com.waveset.security.authz.Right	com.waveset.object.Right
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.ITrace	com.sun.idm.logging.Trace
com.waveset.util.PipeDelimitedParser	com.waveset.util.ConfigurableDelimitedFileParser

Deprecated Methods and Fields

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

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

- If the column is blank, then there is no replacement for the deprecated method or field.
- If no class name is listed, then the replacement method or field is defined in the same class as the deprecated method or field.
- If the replacement method or field is defined in a different class as the deprecated method or field, the replacement is listed using JavaDoc syntax. For example, the `getBaseContextAttrName()` method in the `com.waveset.adapter.ADSIResourceAdapter` class has been deprecated. Its replacement is listed as `com.waveset.adapter.ResourceAdapter#ResourceAdapter()`

where:

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

`com.waveset.adapter.AccessManagerResourceAdapter`

Deprecated Method or Field	Replacement
<code>handlePDEException(Exception)</code>	<code>handlePDEException(PDEException)</code>

`com.waveset.adapter.ACF2ResourceAdapter`

Deprecated Method or Field	Replacement
<code>getAccountAttributes(String)</code>	

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#getAPI(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
getAPIProcess(Map,Map,String,Resource)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIProcess(Element)	
getAPIUser(Element)	
getAPIUser(Map,Map,String,Map)	getAPI(Map,Map,String,ResourceAdapterBase)
getAPIUser(Map,Map,String,Resource)	getAPI(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()

Deprecated Method or Field	Replacement
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)

Deprecated Method or Field	Replacement
unexpirePassword(WUser,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()

Deprecated Method or Field	Replacement
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)

Deprecated Method or Field	Replacement
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)

Deprecated Method or Field	Replacement
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()

Deprecated Method or Field	Replacement
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)	setWorkItemDelegateHistory(List workItemDelegateHistory)

com.waveset.session

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

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

com.waveset.task.TaskContext

Deprecated Method 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)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)

Deprecated Method or Field	Replacement
<code>getObjectNames(LighthouseContext, String, List)</code>	<code>getObjectNames(LighthouseContext, String, Map)</code>
<code>getObjectNames(LighthouseContext, String, String, String, List, Map)</code>	<code>getObjectNames(LighthouseContext, String, Map)</code>
<code>getObjectNames(LighthouseContext, String, String, String, List)</code>	<code>getObjectNames(LighthouseContext, String, Map)</code>
<code>getObjectNames(LighthouseContext, Type, String, String, List, Map)</code>	<code>getObjectNames(LighthouseContext, String, Map)</code>
<code>getObjectNames(LighthouseContext, Type, String, String, List)</code>	<code>getObjectNames(LighthouseContext, String, Map)</code>
<code>getOrganizations(LighthouseContext, boolean, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizations(LighthouseContext, boolean)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizations(LighthouseContext, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizations(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsDisplayNames(LighthouseContext, boolean, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsDisplayNames(LighthouseContext, boolean)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsDisplayNames(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsDisplayNamesWithPrefixes(LighthouseContext, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsDisplayNamesWithPrefixes(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsWithPrefixes(LighthouseContext, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getOrganizationsWithPrefixes(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getSimilarApproverNames(Session, String)</code>	<code>getUsers(LighthouseContext, Map)</code>
<code>getSimilarApproverNames(Session)</code>	<code>getUsers(LighthouseContext, Map)</code>
<code>getUnassignedOrganizations(LighthouseContext, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getUnassignedOrganizations(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getUnassignedOrganizationsDisplayNames(LighthouseContext, List)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getUnassignedOrganizationsDisplayNames(LighthouseContext, Map)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>
<code>getUnassignedOrganizationsDisplayNames(LighthouseContext)</code>	<code>getOrganizationsDisplayNames(LighthouseContext, Map)</code>

Deprecated Method or Field	Replacement
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](#)
- [Identity Manager Upgrade](#)
- [Identity Manager Administration Guide](#)
- [Identity Manager Resources Reference](#)
- [Identity Manager Technical Deployment Overview](#)
- [Identity Manager Workflows, Forms, and Views](#)
- [Identity Manager Deployment Tools](#)
- [Identity Manager Tuning, Troubleshooting, and Error Messages](#)
- [Identity Manager Service Provider Edition Deployment](#)
- [Using helpTool](#)

Identity Manager Installation

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

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

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

SnapShot Management

This page provides management of snap shots for the configuration of the system. In essence it copies specific types from the system for comparison. Based on this comparison one can determine the modifications made before and after the snap shot. This can help provide an inventory of the object modifications for use during the planning of an upgrade.

The screenshot shows the SnapShot Management interface. It features a 'Create' button followed by a text input field. Below this is a 'Delete' button with a dropdown arrow. The 'Compare' button is followed by two dropdown arrows. An 'Export' label is positioned below the Compare buttons. At the bottom is a 'Cancel' button.

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

The screenshot shows the SnapShot Management interface with the 'Compare' button selected. The two dropdown menus are now populated with 'baseline_1' and 'baseline_2'. The 'Export' label now displays 'baseline_1 baseline_2'.

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' />
    </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 4.1\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 4.1\idm"
```

Identity Manager Administration Guide

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

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.

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.

Chapter 11, Identity Auditing

The following information has been added to this chapter.

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
```

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.

Identity Manager Resources Reference

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

- The Exchange 5.5 resource adapter is not supported. Ignore any references to this adapter.
- In the Database Table adapter documentation, the example for the Last Fetched Predicate is invalid. It should be defined as follows:

```
lastMod > '${lastmod}'
```

- 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.

- 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 “Managing ACL List” 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.

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.)

- 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;
}
```

Code Example 5-4 Customizing Navigation Tabs (Continued)

```

table.TabLvl1Tbl td {
    background-image:url(..images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#666699;
    border:solid 1px #abab5;
}
table.TabLvl1Tbl td.TabLvl1TblSelTd {
    background-color:#9999CC;
    background-image:url(..images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    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 #abab5;
}
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 #abab5;
    border-right:solid 1px #abab5;
}

```

Code Example 5-4 Customizing Navigation Tabs (Continued)

```
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-position: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 (`workItemTypes`). 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.

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

- 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:

- Edit the following three rules within the `EndUserRuleLibrary` as indicated below:

Edit this rule	To make this change...
getAccountId	To use <code>employeeId</code> only (and remove <code>firstName</code> and <code>lastName</code>)
getEmailAddress	To use <code>employeeId</code> only (remove <code>firstName</code> , <code>lastName</code> , and <code>"."</code>)
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.

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:

```
<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 2, 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 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 rescans 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 use 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.

Form Name	Mapped Name	Per-User Control	General Purpose
Access Approval List	<code>accessApprovalList</code>		Display the list of attestation workitems
Access Review Delete Confirmation	<code>accessReviewDeleteConfirmation</code>		Confirm the deletion of an access review
Access Review Abort Confirmation	<code>accessReviewAbortConfirmation</code>		Confirm the termination of an access review
Access Review Dashboard	<code>accessReviewDashboard</code>		Show the list of all access reviews
Access Review Remediation Form	<code>accessReviewRemediationWorkItem</code>	Yes	renders each UE-based remediation workitem
Access Review Summary	<code>accessReviewSummary</code>		Show the details of a specific access review
Access Scan Form	<code>accessScanForm</code>		Display or edit an access scan
Access Scan List	<code>accessScanList</code>		Show the list of all access scans

Form Name	Mapped Name	Per-User Control	General Purpose
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		
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:

- o `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`.

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?
<code>orgName</code>	Read	String	System-Generated
<code>orgDisplayName</code>	Read/Write	String	Yes
<code>orgType</code>	Read/Write	String	No
<code>orgId</code>	Read	String	System-Generated
<code>orgAction</code>	Write	String	No
<code>orgNewDisplayName</code>	Write	String	No
<code>orgParentName</code>	Read/Write	String	No
<code>orgChildOrgNames</code>	Read	List	System-Generated
<code>orgApprovers</code>	Read/Write	List	No
<code>allowsOrgApprovers</code>	Read	List	System-Generated
<code>allowedOrgApproverIds</code>	Read	List	System-Generated
<code>orgUserForm</code>	Read/Write	String	No
<code>orgViewUserForm</code>	Read/Write	String	No
<code>orgPolicies</code>	Read/Write	List	No
<code>orgAuditPolicies</code>	Read/Write	List	No
<code>renameCreate</code>	Read/Write	String	No

Name	Editable?	Data Type	Required?
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?
<code>orgContainerId</code>	Read	String	System-generated
<code>orgContainerTypes</code>	Read	List	System-generated
<code>orgContainers</code>	Read	List	System-generated
<code>orgParentContainerId</code>	Read	String	System-generated
<code>orgResource</code>	Read/Write	String	yes, if directory junction or virtual organization

Name	Editable?	Data Type	Required?
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 <i>Identity Manager Technical Deployment Overview</i> 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.
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?
<code>name</code>		String	Yes
<code>status</code>		String	Yes
<code>user</code>		String	Yes
<code>userId</code>		String	Yes
<code>attestorHint</code>		String	No
<code>userView</code>		GenericObject	Yes
<code>reviewInstanceId</code>		String	Yes
<code>reviewStartDate</code>		String	Yes
<code>scanId</code>		String	Yes
<code>scanInstanceId</code>		String	Yes
<code>approvalWorkflowName</code>		String	Yes
<code>organizationId</code>		String	Yes
<code>attestorComments.name</code>		String	No
<code>attestorComments.attestor</code>		String	No
<code>attestorComments.time</code>		String	No
<code>attestorComments.timestamp</code>		String	No
<code>attestorComments.status</code>			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.

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>
```

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 contains new information and documentation corrections for the *Sun Java™ System Identity Manager Deployment Tools*:

What's New?

Substantial information was added to the following chapters in the *Identity Manager Deployment Tools* book:

- Chapter 1, “*Using the Identity Manager IDE*,” was updated to provide information about the following new features and functionality:
 - The process for creating and working with Identity Manager IDE projects was updated to provide two project types (ID-14587):
 - Identity Manager Project is a fully featured, primary development environment for developers.

- Identity Manager Project (Remote) is used to make small modifications and perform debugging on an external server.
- Identity Manager IDE projects are now integrated with a Configuration Build Environment (CBE) (ID-14980)
- There is now an IdM menu on the NetBean's top level menu bar from which you can select actions that are appropriate for selected object nodes. (ID-14787)
- Library objects were added to the list of object types displayed in the Explorer window, and these objects have Property Sheets, Palette features, and navigation nodes. (ID-14817)
- When you select Design view for a Rule object, an Expression Builder now displays in the Editor window to make it easier for you to see the logical structure of a rule and to modify the rule's properties. (ID-15104)
- You can now compare (diff) objects in a local directory with those in the repository. (ID-15206)
- The process for testing forms and rules was modified. The Form *Previewer* option was renamed to Form *Tester*. (ID-15325)
- Features and functionality were added to the Identity Manager IDE Expression Builder dialogs, including:
 - You can now edit simple data types (integers and strings) directly in the Expression Builder table. (ID-15528)
 - You can now create a specific expression rather than first creating a BLOCK and then changing it to the expression you want. (ID-15932)
 - A new Change To button and dialog were created that enable you to change an element's expression type. (ID-15933)
 - You can now edit property values that support an expression and a primitive value (such as a string) directly in a property table. (ID-15528)
 - When defining instance or static XPRESS invoke statements in the Expression Builder, you can view the related JavaDoc information for the Identity Manager API methods. You access this JavaDoc by running your cursor over the methods listed in the Method Name menus. A pop-up window displays with the information.
- The Identity Manager IDE plugin now requires JDK 1.5 and Netbeans 5.5. (ID-14950)
- You can now delete objects from the Identity Manager IDE repository. (ID-15031)

- You can now upload an object in the IDE to an Identity Manager 7.0 server and manually assign an ID to the object. (ID-15474)
- You can now right-click nodes in the Project tree and open objects to which certain references refer (such as ObjectRefs, FormRefs, FieldRefs and Workflow Subprocesses). (ID-15406)
- Other, minor user interface and process changes.
- The “*Auditor Rules*” section in Chapter 2, “*Working with Rules*,” was updated to provide more detailed information about Identity Auditor rules. (ID-15367, 15496, 15609, 15934, 16166, 16263, and 16292)
- Chapter 7, “*Using SPML 1.0 with Identity Manager Web Services*,” was updated to include information about the SPE SPML interface. (ID-14458)
- The “*Using Trace in SPML*” section in Chapter 7, “*Using SPML 1.0 with Identity Manager Web Services*,” was updated to provide additional information about how to enable trace output so you can log Identity Manager’s SPML traffic and diagnose problems. (ID-15346)
- The “*Using Trace in SPML*” section in Chapter 8, “*Using SPML 2.0 with Identity Manager Web Services*,” was updated to provide additional information about how to enable trace output so you can log Identity Manager’s SPML traffic and diagnose problems. (ID-15346)

Updates

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

- The “*Palette Window*” and “*Properties Window*” sections in Chapter 1, “*Using the Identity Manager IDE*,” 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.

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

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	<code>getServerInternalContext()</code>	Returns a fully authorized context without any authentication.
Local authenticated	<code>getSPESession(String user, EncryptedData password)</code>	Constructs a session for the Service Provider user interface.
Local authenticated	<code>getSPESession(Map credentials)</code>	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	<code>getSPEPreAuthenticatedSession(String user)</code>	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	<code>getSession(URL url, String user, EncryptedData pass)</code>	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:

- o **Destination directory** — `html/docs`
- o **Input files** — `../doc/HTML/en_US`

NOTE The tool will copy the `en_US/` directory and subdirectories to the destination.

- o **Nova index directory** — `index/docs`
- o **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.

- o **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
```