Oracle® Fusion Middleware

Release Notes for Oracle Identity Analytics

11g Release 1, Patch Set 1 (11.1.1.5)

E23379-01

August 2011

This document contains release notes for Oracle Identity Analytics 11g Release 1 Patch Set 1 (Release 11.1.1.5). It contains the following sections:

1 Announcements and Notices

OIA has Dropped Support for MySQL, IBM DB2, and Microsoft SQL Server

Oracle Identity Analytics has dropped support for the MySQL, IBM DB2, and Microsoft SQL Server database servers.

OIA has Dropped Support for Provisioning Servers From IBM and CA

Oracle Identity Analytics has dropped support for IBM Tivoli Identity Manager and CA eTrust Identity Access Management.

OIA has Dropped Support for LDAP Authentication and Intellitactics Security Manager

Oracle Identity Analytics no longer supports authenticating with LDAP. OIA has also dropped support for Intellitactics Security Manager (ISM).

OIA has Dropped Support for the JBoss and GlassFish Application Servers

Oracle Identity Analytics has dropped support for the JBoss and the GlassFish application servers, including both the Oracle GlassFish Application Server and the GlassFish Server Open Source Edition.

Third-Party Libraries Now Need to be Downloaded Separately

The following third-party files are no longer included with Oracle Identity Analytics. Third-party files may be downloaded separately and included in the `rbacx.war` deployment file during installation.

- CloverETL - OIA uses CloverETL for data import and export transformations.
- `jxl-2.5.9.jar` - OIA uses the Java-Excel API to import data from an Excel spreadsheet file.

- `wsdl4j-1.6.1.jar` - Oracle Identity Analytics Web Services requires the use of this JAR file.

For details, see the *Installation and Upgrade Guide for Oracle Identity Analytics*.

The Workflow Tab on the Identity Warehouse Pages in now Hidden by Default

The Workflow page displays three approver fields that are populated with data if OIA has been integrated with the CA Identity Manager provisioning server. This page is now hidden by default. To enable the Workflow tab, see the steps in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the Oracle Identity Analytics User Interface" chapter, "Enabling Hidden Pages in the UI" section.

The Exclusion Roles Tab on the Identity Warehouse Pages is now Hidden by Default

The Exclusion Roles page lists roles that are in conflict with one another from a segregation of duties standpoint. This page is now hidden by default. To enable the Exclusion Roles tab, see the steps in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the Oracle Identity Analytics User Interface" chapter, "Enabling Hidden Pages in the UI" section.

There has been no change to the Exclusion Policies page in this release.

The System now Prompts you to Change the rbacxadmin Account Password

Upon logging in to Oracle Identity Analytics for the first time, the system now automatically expires the default password for the rbacxadmin account and prompts the administrator to create a new password.

The Oracle Identity Analytics Product Documentation has Changed

The *Business Administrator's Guide* and the *System Administrator's Guide* have been combined into a single *Administrator's Guide*. Part one of the Administrator's Guide contains information for business administrators, and part two contains information for system administrators.

The product documentation for this release is not posted to a wiki. It is available in PDF and HTML formats.

2 Features and Enhancements Added in This Release

The following features and enhancements were added in this release.

Risk Properties Now Available During Identity Certification

A number of risk properties have been added to Identity Warehouse objects. You can directly assign high, medium, and low risk levels to roles, resources, and resource-attribute values (entitlements), as well as to certain predefined risk factors. A risk-aggregation job calculates Risk Summaries for the remaining higher-order data objects that are needed to support the OIA Identity Certification feature. These objects include every User, User-Role assignment, Account, and Account-Attribute value in the Identity Warehouse. During identity certification, reviewers can now search for certification items based on a calculated Risk-Summary value and other risk properties.

For detailed information about risk, see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Identity Warehouse" chapter, "Understanding How Risk Summaries are Calculated."

An Advanced Search and Filtering Feature has Been Added to the Identity Certification Module

A new Filter-data-by feature has been added to Identity Certification pages. The Filter-data-by menu allows certifiers to filter items within a certification by various criteria, such as risk level, certification status, and so on. Certifiers who have a large number of records to review can quickly create expressions with multiple criteria to find records of interest.

The Filter-data-by feature is documented in the *User's Guide for Oracle Identity Analytics*, "Identity Certification" chapter, "Understanding the Certification Pages."

Role Owners Can Now Certify Users Who Have a Role Assigned

When completing a Role Entitlement Certification, role owners can now review a list of users who have the role assigned and then take action to certify or revoke each user's role access.

For details see the *User's Guide for Oracle Identity Analytics*, "Identity Certification" chapter, "Understanding the Certification Pages," "Role Entitlement Certification Help," "Role Entitlement Certification - Members Detail Page."

Multiple Certifiers Can Now Review the Same Certification

It is now possible to assign multiple certifiers to the same certification. Certifiers can review the same certification simultaneously.

When Importing Records From an External System you can now Import Details About how Roles and Entitlements are Assigned

Oracle Identity Analytics can be configured to capture provisioning and assignment information about the roles, accounts, and entitlements that are assigned to a user. This information needs to originate from authoritative sources, such as Oracle Identity Manager and file-based imports. Provisioning method categories include Reconciliation from target system, Direct provisioning by administrator, Access request, Provisioned by access policy, and Rule-based role-assignment. Assign a high, medium, or low risk values to each provisioning method category. For example, you might configure a risk level of High for objects that are provisioned directly by an administrator, and a risk level of Low for objects that are provisioned based on Policies that are tied to Roles. The OIA risk-aggregation job processes these risk levels when it calculates Risk Summaries for objects in the Identity Warehouse.

You can now Prevent Self-Certification During the Identity Certification Process

A "Disallow self-certification" option has been added to the Identity Certification Settings page. Select this option to prevent managers from being able to certify their own access. The certification is assigned to an alternate reviewer designated by the certification creator instead.

For more information see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Configuration and Settings" chapter, "Identity Certification Configuration" section.

Note: By default, self-certification is allowed for Oracle Identity Analytics customers who upgrade to version 11.1.1.5.0. Self-certification is not considered a best practice, however, and upgrade customers are encouraged to select the **Disallow Self-Certification** option.

You can now Prevent Self-Remediation During the Identity Audit Process

A "Prevent Self-Remediation" option has been added to the Identity Audit configuration page. Select this option to prevent users from being able to remediate their own violations if their attributes, roles, or entitlements are causing a segregation of duties violation.

For more information see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Configuration and Settings" chapter, "Identity Audit Configuration" section.

Note: By default, self-remediation is allowed for Oracle Identity Analytics customers who upgrade to version 11.1.1.5.0. Self-remediation is not considered a best practice, however, and upgrade customers are encouraged to select the **Prevent Self-Remediation** option.

3 Known Issues and Workarounds

This section describes known issues in Oracle Identity Analytics Release 11.1.1.5.

The Login Page Displays `???login.streamlineAccessControl???` After Upgrading OIA (Bug 12662090)

To fix this issue, clean out the web server's cached directories. Refer to your server's documentation for further instructions.

The UI Defaults to the Server Locale Instead of English When the Browser is set to a Language That OIA Does not Support (Bug 10310571)

If a user's browser is set to a language that OIA does not support, for example Arabic (ar-AE), the UI defaults to the language configured in the server's locale settings instead of English.

To work around this issue, change the server's locale to output English.

Exported CSV Files With UTF-8 Encoding are Garbled in Excel (Bug 9998221)

When an exported `.csv` file is opened in Microsoft Excel, the multibyte characters become unrecognizable. This is because Oracle Identity Analytics uses a UTF-8 encoding for exported `.csv` files, and Microsoft Excel cannot properly open UTF-8 encoded files.

To work around this issue, either open the `.csv` file in Oracle Open Office Calc, or, if using Excel, follow these steps:

1. Save the `.csv` file to a local folder.
2. Open Microsoft Excel and from the menu choose **Data >Import CSV file**.
3. Select `65001: Unicode (UTF-8).`

WebSphere Exception Error Messages in CSV Files are Garbled When Server is Running in a Locale That is not UTF-8 (Bug 12610885)

WebSphere honors the server locale when outputting exception error text. When this text is included in an exported CSV file, the text is rendered as garbage characters if the server locale is not UTF-8.

Currently there is not a workaround for this issue.

Report Elements are Displayed in English Instead of Being Translated (Bug 9998287)

Report elements such as labels, column headers, and the report name are displayed in English instead of being displayed in the configured local language.

Currently there is not a workaround for this issue.

Multibyte Characters Become Garbage or are not Displayed at all in a PDF Report (Bug 10209447)

To work around this issue, export your report to a `.csv` file or `.xls` file and format the report in a desktop application that is capable of editing these file types (for example, Oracle Open Office Calc or Microsoft Excel). From your desktop application, save the file as a PDF.

Active Certifications Require Special Processing to be Compatible with OIA Version 11.1.1.5.0 (Bug 12671056)

If your environment includes any incomplete certifications, enable the Identity Certification Migration Job (`idcMigrationJob`) after completing the upgrade process. This job updates active certification data to be compatible with version 11.1.1.5. This job only needs to run successfully one time in your environment, after which it can be disabled.

For more information, see the following topics in the *Installation and Upgrade Guide for Oracle Identity Analytics*:

- "Enable the Identity Certification Migration Job in a Test Environment," located in the "Upgrading Oracle Identity Analytics in a Test Environment" chapter
- "Enable the Identity Certification Migration Job in a Production Environment," located in the "Upgrading Oracle Identity Analytics in a Production Environment" chapter

A Custom Report Cannot be Created Unless the OIA Host (or its Domain) is Added to the Local Intranet Group in the Browser Security Options (Bug 10295505)

This issue affects Safari 5 and Internet Explorer 8. To work around this issue, open the browser security options, edit the Local Intranet Group settings, and add either the host computer or the domain the host computer is a member of.

Some Identity Certification Pop-ups Show Snapshot Data and Others Show Real-Time Data (Bug 12774833)

Clicking a More-Info link during the certification process will open either a Details pop-up or a Meta-Information pop-up that displays additional detail about roles, accounts, attributes, policies, and so on. Some pop-ups show snapshot data (that is, the data details as they existed at the moment that the Identity Certification was created), while others show real-time data (the data details as they exist in the Identity Warehouse at the moment that the More-Info link is clicked). Displaying real-time data in a pop-up may be confusing to users completing identity certifications (which use snapshot data) because the real-time data and snapshot data may not match.

The following pop-ups show *snapshot* data:

- On the "Data Owner Certification - Summary" page, the Attribute-Values Detail pop-up, and the Value pop-up (which is displayed if there is a Glossary value)
- On the "User Entitlement Certification - Entitlements Detail" page, the Value pop-up (which is displayed if there is a Glossary value)
- On the "Role Entitlement Certification - Policies Detail" page, the Value pop-up (which is displayed if there is a Glossary value)
- On the "Resource Entitlement Certification - Summary" page, the resource details pop-up (which displays if you click a resource)
- On the "Resource Entitlement Certification - Accounts and Entitlements Detail" page, the Value pop-up (which is displayed if there is a Glossary value)

All other Identity Certification pop-ups show *real-time* data.

The "Attribute" Meta-Information Pop-up Does not Report a Risk Summary Value (Bug 12762577)

When you open the "Attribute" meta-information pop-up from the User Entitlement Certification - Entitlements Detail page, it displays a blank Risk Summary value. To work around this issue, view the Risk Summary value on the Entitlements Detail page.

The Resource Name and Resource Type Labels are Reversed on the Resource Certification Summary Page (Bug 12848092)

On the Resource Entitlement Certification Summary page, the resource name and resource type column labels are switched. The values listed under resource name are actually the resource types and the values listed under resource type are actually the resource names.

OIA Does not Display a Confirmation Message When you Start a Role Mining Task (Bug 12540231)

On the Role Mining page, when you click Run to start a role mining task, OIA does not display a message informing you that the role mining task has started. To work around this issue, click View Results to view the task status.

OIA Does not Display a Confirmation Message When you add or Remove a Role on the Identity Warehouse > Users > Roles page (Bug 10207138)

When one or more roles are assigned or removed from the Identity Warehouse > Users > Roles page, OIA does not display a message informing you that the approval workflow process has started. The lack of immediate feedback may be confusing to new users.

OIA Displays an Inadequate Confirmation Message When you add a Role to a Policy (Bug 11901765)

When you add a role to a policy and click Save, OIA displays a message that says "role was requested for a policy," but the message does not tell the end-user what to do next. End-users need to click "Send to approval" to add the role to the policy.

In the UI, the Main Menu Does Not Hide the "Administration > Settings" Option From OIA Users who Lack the Required Access Privileges to View its Contents (Bug 12717036)

OIA users who are limited to the "Configure Resource Type Definitions" system privilege can see the Administration > Settings option on the main menu even though the menu is empty. Because these users do not have the required access privileges to view the menu, the Settings option should be hidden from view.

OIA Returns Inactive Users When Running or Previewing a Role Management Rule (Bug 12653762)

When searching for users prior to running or previewing a role-management rule, OIA returns both active users and inactive users, even though a role-management rule can only assign roles to active users.

The Number of Imported Accounts may not be Reported on the Import/Export > Completed Jobs Page (Bug 12544912)

In a clustered environment, if an import is triggered by another member of the cluster, the Status column on the Administration > Import/Export > Completed Jobs page will not show the total number of imported accounts.

Certain Identity Certification Pages may Have an Excessive Amount of White Space in Internet Explorer 7 and Internet Explorer 8 (Bug 11892866)

Some Identity Certification pages may have an excessive amount of vertical white space between the "Actions" button bar and the table of certification data. This is a cosmetic defect only.

In Internet Explorer 8, the UI Page Elements Overlap Slightly on the "Identity Warehouse > Users > Account" Page (Bug 12388034)

On the "Identity Warehouse > Users > Account" page, the **Cancel** button slightly overlaps the footer menu when viewed in Internet Explorer 8. This is a cosmetic defect only.

In Internet Explorer 9, the Left Side of the "Word Balloon" That Displays Glossary Pop-ups is not Rendering Properly (Bug 12764533)

When you click a Glossary value link in Internet Explorer 9, two of the image pieces that make up the "Word Balloon" image are not spaced properly. This is a cosmetic defect only. The Glossary information is still legible.

In Safari 5, the UI Buttons on the "My Requests > Pending Requests" Page are Askew (Bug 12644276)

On the "My Requests > Pending Requests" Page, the buttons are askew by one pixel when viewed in Safari 5.0. This is only a cosmetic defect.

The Add and Remove Buttons are not Grayed out for Decommissioned Roles in Firefox and Safari (Bug 12716784)

Because decommissioned roles cannot be edited, the Add and Remove buttons should be grayed out in the user interface. In Internet Explorer the buttons are grayed out, however, in Firefox and Safari they are not. The button functionality is properly disabled regardless of which browser is used.

The Search Button on the Resource > Data Management Page is not Grayed out in Firefox and Chrome (Bug 12634852)

If you have not selected an attribute on the Resource > Data Management page, Firefox and Google Chrome do not gray out the Search button even though the button is not active. Internet Explorer properly disables and grays out the Search button if you have not selected an attribute.

An Unnecessary Feedback Message About Object HTMLDivElement is Displayed (Bug 12825688)

If using Chrome or Safari, the text "[object HTMLDivElement]" briefly displays at the top of the page when you navigate to the Identity Warehouse > Business Structures > Rules page.

Feedback Messages on Some Pages are not Displaying in Firefox, Safari, and Chrome (Bug 12854009)

Certain feedback messages that normally display in response to user actions are not displaying in Firefox, Safari, and Google Chrome. The affected feedback messages include the message that displays upon saving a role that you edited, and the message that displays when creating or sending a role-management rule for approval. These messages display properly in Internet Explorer.

If Running Safari on Windows Server 2008, the Drop-Down Menu Buttons are Missing the Arrow (Bug 12825713)

This issue is limited to Safari 5.0.5 on Windows Server 2008. The drop-down menus still function properly, but the drop-down button is blank.

In Chrome and Safari, a Specific Menu Overflows the Page Boundary When the Browser is Resized (Bug 12826545)

In Chrome and Safari, part of the menu on the Identity Warehouse > Roles page overflows the page boundary instead of wrapping when the window is re-sized to a smaller size. This is only a cosmetic defect.

4 Related Documentation

The Oracle Identity Analytics documentation library includes the following titles:

- *Installation and Upgrade Guide for Oracle Identity Analytics*
- *User's Guide for Oracle Identity Analytics*
- *Administrator's Guide for Oracle Identity Analytics*
- *System Integrator's Guide for Oracle Identity Analytics*
- *API Guide for Oracle Identity Analytics*

Documentation for other Oracle Identity and Access Management products (version 11.1.1.5.0) can be found here:

`http://download.oracle.com/docs/cd/E21764_01/im.htm`

5 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Oracle Fusion Middleware Release Notes for Oracle Identity Analytics 11g Release 1, Patch Set 1 (11.1.1.5)

Copyright © 2010, 2011 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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