ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Upgrading to Oracle Identity Manager 11.1.2.3.0

Technical Overview

ORACLE WHITE PAPER | AUGUST 2015

ORACLE

Table of Contents

.

Executive Overview

Application proliferation has created identity fragmentation as user identities are inconsistently managed across applications in the enterprise, increasing risk and cost. Enterprises need to ensure users have sufficient access privileges to perform their job functions, but for compliance and security reasons it's also important to constrain such access. Accordingly, enterprises must make it easy for users to acquire and provision access, and also easy for managers, resource owners, and system administrators to review and revoke access. Oracle's Identity Governance solution is designed to help enterprises balance these objectives of access, security, and compliance.

Business user experience tends to drive key Identity Governance initiatives for enterprises today. A simple, persona oriented end user experience enables business users to complete key Identity Governance tasks seamlessly while truly understanding the task they are performing or taking action on. Today, Identity Governance solutions are no longer geared solely towards administrative users, but for business users to complete key self-service tasks.

For large organizations, getting users the access they require can be a frustrating and time consuming task. Manual processes used to on-board users, link identities and terminate users are often times, inefficient and error prone. In addition, privileged account access is poorly managed, creating unnecessary risk. New users have little exposure to IT jargon that would enable them to request privileges by name. New users often resort to requesting the same kinds of access as their peers, who may have privileges that new users shouldn't. And as employees and contractors work on a variety of projects, transfer departments and locations, change their job functions, and get promoted, their requirements for access change. At a deeper level, system administrators require access to privileged, shared accounts that allow them to perform business-critical and administrative functions. Often, these accounts are "root-level" accounts that don't use administrators' named accounts, so it becomes critical to grant access to the right individuals in a timely manner. For all of these scenarios, Oracle provides identity governance solutions to simplify access grants by enabling users to request access in simple, web-based catalogs, and by routing these requests to appropriate approvers. The solution also provides privileged account management, which controls access to shared, root-level or admin accounts.

Similarly, access certification is an ongoing challenge for most enterprises, but necessary for compliance with regulations such as Sarbanes Oxley (SOX). The need to perform multiple, difficult tasks—such as certifying user access rights, enforcing security policies, and automatically revoking unnecessary access rights—is compounded by the reliance on slow, error-prone manual processes to

handle them. These issues, coupled with the lack of a comprehensive, cohesive approach to compliance and auditing, make it nearly impossible to address the challenge in an effective and cost-efficient manner. As a result, enterprises are obliged to commit significant resources to compliance efforts. Oracle simplifies certification challenges by automating the review cycle. Oracle's Identity Governance solution automatically detects user privileges, segregation of duties violations and orphan accounts, notifies the appropriate stakeholders of any action they need to take, applies risk scores to help stakeholders prioritize their certification tasks, and makes changes to privileges and accounts once a decision is reached.

Oracle Identity Manager (hereafter OIM) is a key component in the Oracle Identity Governance suite. This white paper outlines the benefits of upgrading to the latest path set of Oracle Identity Manager which is 11g R2 PS3 (11.1.2.3.0) and upgrade process in general.

Benefits of Upgrading to OIM 11gR2 PS3

Organizations that upgrade to OIM 11gR2 PS3 can leverage the benefits of the Oracle Identity Governance Platform. With this platform you get a single rationalized solution through which you can deliver access request and access review capabilities. These capabilities will be delivered from a single technology stack and will enable organization to

- Simplify their deployments
- Reduce their total cost of ownership
- Accelerate their return on investment

» Complete Identity Governance Platform

An enterprise will get a single solution through which they can do both access request and access review from a single converged solution. The Access Request module and the Access Review module now leverage the same data model, glossary data and catalog data to provide the much needed consistency in business context across both access request and access review. These two modules are now deployed on a single technology stack which reduces the number of application servers or databases instance that an organization needs to deploy thereby simplifying an Identity Governance deployment.

Organizations can now design certification campaigns through which both business and IT can collaborate to make an access review decision. The new automated workflows eliminate the need for manual tasks such as consolidation, correlation and distribution of access review decisions which are time consuming and error prone.

Significant enhancements have also been made to provide a more user friendly and navigation friendly UI. Rich Inline analytics such as graphs and charts have been stitched into the UI to give a reviewer an at a glance view of the complete risk and risk summary associated with each user and their access. Advanced filtering, sorting, drill down and saved search capabilities coupled with the innovative risk engine gives a reviewer the tools through which he/she can slice and dice data to identify high risk profiles and hone in on high risk access items that require immediate remediation.

The converged provisioning, access request and access review solution available in OIM ensures that you get the most effective closed loop remediation tracking and enforcement solution in the industry. We have also added a provision through which the end users can become involved in the remediation process and challenge a revoke decision if it prevents them from completing their job.

Additionally integration of access review with MS™ EXCEL provides a solution that accelerates and simplifies large scale certification campaigns. Exporting certifications tasks to EXCEL gives a reviewer the luxury and flexibility to complete their access review task in an offline mode. The need to be continuously connected to an online system is eliminated. The fact that EXCEL is a very common tool used by almost every business user and it provides intuitive and user friendly navigation and filtering capabilities makes it an excellent tool through which a reviewer can complete their access review task and with a simple click can upload decisions to the online server.

We have also further simplified reporting by stitching the certification reporting module right into the certification dashboard. A business user or auditor can now leverage the point and click reporting capabilities to generate certification reports from the same console through which access review and access request is done.

» Full Lifecycle Management

Oracle Identity Manager 11gR2 PS3 manages full lifecycle of an identity. It includes complete HR-driven automation of employee lifecycle, from hire to retire for enterprise, mobile and cloud application. Along with employee, it also manages other identities like guest users, contractors, affiliates and customer users.

» Business Friendly Access Request

Access request module is now more business friendly. It enables end-users to get the access they need via Self-Service Application On-boarding and administration. It is easier to search and browse through various catalog entities along with the recommendations for the requestor. Policy checks are now inline to prevent violations.

Access catalog now has more advanced search form where in UDFs which are marked as searchable will automatically be part of advance search form. You can customize the search form. Attributes can be used to search catalog items.

There is end to end visibility of the user data into the approval and fulfillment process which helps the approver in making quick and correct decisions

» Easy & Accurate Identity Certifications

Identity Certifications in OIM 11gR2PS3 rely on live data. Certification leverage analytics to expedite low and highlight high risk. It also highlights provisioning context so that more informed decisions can be made. OIM supports time or event based certification campaigns with quick closed loop remediation. Certifications can also be completed in offline mode.

» Rapid and Scalable Fulfillments

OIM 11gR2PS3 supports both automated and manual fulfillment processes. Identity Connector Framework automates the provisioning to popular on-premise and cloud apps. OIM now has browser based, simplified application on-boarding & management. Oracle is the only vendor to feature a comprehensive, end-to-end strategy to manage Oracle Applications

» Flexible and Modular Architecture

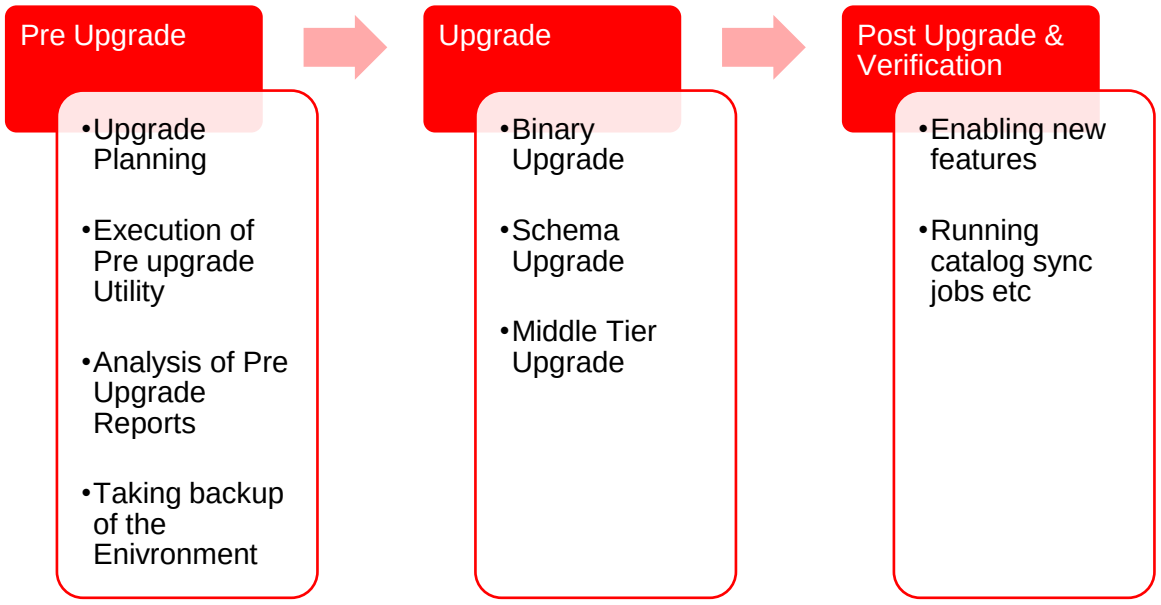
OIM 11gR2PS3 has flexible modular architecture which fits with your governance requirements. It has single data store for all phases of identity governance. You can easily customize and model your identity governance projects. There are multiple points of entry to begin like building an access catalog to enable request process, automating access certification and automating provisioning to key applications.

Upgrading Oracle Identity Manager

Before doing an actual upgrade, it is recommended that you refer to the Upgrade planning guide and Release notes to understand new capabilities, identify the supported upgrade paths, and review the best practices.

OIM Upgrade Process

Typically an OIM upgrade is a three phase process and each phase consists of multiple steps. The diagram below depicts the phases of an OIM upgrade



» Phase 1: Pre Upgrade

In this phase, you plan for your upgrade. It is recommended that you refer to the Upgrade Planning guide and define an upgrade project plan according to your organization's requirements. Once you have decided to go for an upgrade, you should run the pre upgrade utility which analyzes your existing OIM environment, and provides information about the mandatory prerequisites that you must complete before upgrading your environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before the upgrade, cyclic groups in LDAP directory, deprecated authorization policies, and potential issues in creating application instance.

Once you have taken the prerequisite steps mentioned in the reports, take a backup of your environment so that you can revert to your original environment in case any errors or failures occur during the upgrade. This phase is completed offline.

» Phase 2: Upgrade

In this phase, the actual upgrade happens wherein binaries, various OIM schemas and Middle tier components are upgraded. In this process new stored procedures are loaded, new scheduler jobs are seeded and domain specific

changes are done. This phase is completed in both offline and online mode. Binary and Schema upgrades are offline steps whereas middle tier upgrade is done in both offline and online mode.

» Phase 3: Post Upgrade & Verification

This is the last phase where you verify your environment after the upgrade. Also, you perform various post upgrade steps depending on your requirements, like enabling new features etc. Refer to the OIM upgrade guide for information related to post upgrade steps.

Upgrading from 11gR2x releases

Completing a Patch Set upgrade is a very simple task and all 11.1.2.x.x customers are encouraged to move to the latest and the greatest patch set which is 11.1.2.3.0.

Organizations should review and become familiar with the new capabilities before moving into the upgrade execution phase. Following is a summary of the key new capabilities added in OIM 11gR2 PS3 that are relevant for organizations upgrading from 11g R2x releases. Refer to the product documentation for a detailed description of the new capabilities.

TABLE 1: FEATURE COMPARISION

S.No	Oracle Identity Manager 11gR2x	Oracle Identity Manager 11gR2PS3
1	Oracle Identity Manager 11.1.2.0 and 11.1.2.1.0 uses the Fusion Fx skin where as 11.1.2.2.0 uses Skyros skin which is a light weight skin.	Oracle Identity Manager 11gR2PS3 uses Alta skin which is business (mobile, cloud) friendly .OIM now has a new Home page, new my profile page with a user-friendly inbox. Most UI customizations will need to be re done to match the look and feel of 11gR2PS3
2	In Oracle Identity Manager 11.1.2, the Access Catalog was introduced to provide meaningful and contextual information to end users during the request and access review. The Access Catalog allows you to associate meaningful metadata against any request able entity. Also, you can enable the display of hierarchical attributes of entitlements to requesters, approvers, and certifiers to view technical glossary in the catalog detail screen.	Oracle Identity Manager 11gR2PS3 has a new advanced search catalog where UDFs that are marked as searchable will automatically be part of the advanced search form. You can also customize the search form. Attributes can be used to search catalog items and the catalog now includes enhanced pagination and categories to simply resource searches.
3	In Oracle Identity Manager 11.1.2.1.0, certification was introduced and the workflow supported one level of access in each phase. Certification workflow in 11.1.2.2.0 enables business to define more robust processes for compliance, enabling more granular oversight of "who has access to what". Certification reviews can mirror access request workflow, where they can be reviewed or approved by multiple sets of business and IT owners before they are deemed complete in each phase. This ensures improved visibility of user access privileges, and all review decisions are captured in a comprehensive audit trail that is recorded live during the certification as well as in reports	Certification feature of Oracle Identity Manager 11gR2PS3 also uses the Alta UI and has been enhanced to provide inline SoD violation checks.
4	Till Oracle Identity Manager 11.1.2.2.0, BI publisher was a separate standalone managed server	Oracle Identity Manager 11.1.2.3.0 has embedded BI Publisher, hence all BI reports are embedded in OIM. A business user now can launch a custom report from within OIM Self Service Console.

5	Oracle Identity Manager 11.1.2.0.0 has to be integrated with Oracle Identity Analytics(OIA) to leverage advanced access review capabilities. In Oracle Identity Manager 11.1.2.1.0 and 11.1.2.2.0, the advanced access review capabilities of OIA are converged into OIM to provide a complete identity governance platform that enables an enterprise to do enterprise grade access request, provisioning, and access review from a single product	OIA functionality is now ported into OIG. Customers can define and manage identity audit policies based on IDA rules. Customers can define owners and remediators for a policy , which can be a specific user, a list of users or an OIM role Customers can use preventive and detective scan capabilities which can create actionable policy violations. Oracle Identity Manager 11gR2PS3 has comprehensive role lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI. It also includes detailed Role Analytics to aid with the composition and modifications of roles.
6	Till Oracle Identity Manager 11.1.2.2.0, policies are implemented and customized using OIM plug-in and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies	Oracle Identity Manager 11gR2PS3 has introduced declarative policies that enable customers to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.
7	Existing certification feature provides certifier selection based on User Manager, Organization Manager, Catalog Owner and Selected User.	Oracle Identity Manager 11gR2PS3 introduced additional certifier selection where role can be used to define certifiers. All members of a certifier role can see the certification in their inbox, but the first member who 'claims' the certification will be the primary reviewer for that certification.
8	In Oracle Identity Manager 11.1.2.x.x, concept of request profile is introduced. You can draft and save the request. Request has to go through two levels of approval process	Oracle Identity Manager 11gR2PS3 includes a number of enhancements to the request workflow. Temporal grants allow the requester to specify the start and end date (grant duration) of the role, account and entitlements at the time of assignment. Administrators can configure approvals by creating workflow policy rules instead of approval policies. It also supports role requests (create , modify, delete etc).Also, now enabling SOA is optional.
9	Till Oracle Identity Manager 11.1.2.2.0, only out-of-the box admin roles were available	Oracle Identity Manager 11gR2PS3, provides a fine grained authorization engine to help you create various admin roles, for example, using attributes to define membership, you can restrict an administrator to managing home organization members only.

Below diagram provides the overview of the steps involved in upgrade process from 11.1.2.0.0, 11.1.2.1.0 and 11.1.2.2.0 to 11.1.2.3.0.

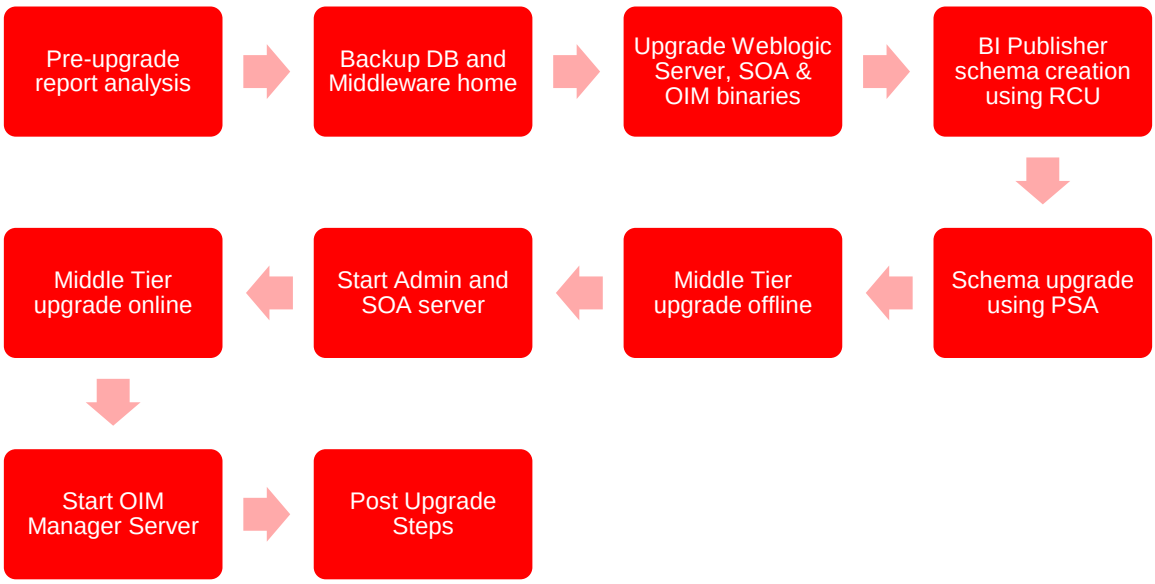


Figure 1: Upgrade steps from 11.1.2.x.x to 11.1.2.3.0

1. Run pre upgrade utility and analyze the generated report. It is mandatory to follow the instructions mentioned in the reports before initiating the upgrade.
2. Backup the database and the Middleware home. In the event of any incident you may need to do a quick restore of the database and the middleware home.
3. OIM 11g R2 PS3 requires Weblogic Server 10.3.
4. OIM 11g R2 PS3 requires SOA Suite 11.1.1.9, download the SOA 11.1.1.9 binaries from edelivery.oracle.com and upgrade your existing SOA suite to 11.1.1.9. Refer to OIM release notes to identify and apply SOA patches.
5. Download the IAM 11.1.2.3 (11g R2 PS3) binaries from edelivery.oracle.com and install the new binaries in the existing Middleware home. This step copies the new binaries to the Middleware home folder.
6. BI Publisher is embedded in OIM 11g R2PS3, create schema of BI Publisher using RCU
7. Upgrade the OIM database schema. Use the patch set assistant to upgrade OIM and dependent component schemas. The patch set assistant automatically identifies dependent schemas and upgrades them.
8. New capabilities are enabled by running the OIM Upgrade utility in both offline and online mode, which deploys new artifacts such as SOA Composites, Scheduled Jobs, CSF Credentials, etc.
9. Review the documentation and complete the steps to upgrade other components such as the Design Console and Remote Manager. Review the release notes to identify any patches that you may need to apply.

Upgrading from 11gR1x releases

Upgrading from 11g R1 releases to 11g R2 PS3 requires a thorough assessment of new capabilities, changes to authorization and request model as well UI customizations.

Organizations should review and become familiar with the new capabilities before moving into the upgrade execution phase. Following is a summary of the key new capabilities added in OIM R2 PS3 that are relevant for organizations upgrading from 11g R1 Releases. Refer to the product document for a detailed description of the new capabilities.

TABLE 2: FEATURE COMPARISION

S.No	Oracle Identity Manager 11gR1x	Oracle Identity Manager 11gR2PS3
1	Oracle Identity Manager 11gR1x provided separate interfaces for end user self-service and delegated administration. UI relied on the classic UI customization model where developers would edit the back end code then deploy it to an application server and finally validate the changes from a browser. This was required for minor changes such as changes to logos, label, font, button, etc.	In Oracle Identity Manager 11gR2PS3, the end user self-service and delegated administration consoles are unified into a single self-service console to simplify administration and self service. 11gR2PS3 uses the Alta skin which is business (mobile, cloud) friendly .OIM now has new Home page, new my profile page with user friendly inbox. UI customization is simplified using Sandboxing and web composer. Most UI customizations will need to be re done to match the look and feel of 11gR2PS3
2	In Oracle Identity Manager 11gR1x, administrators configured request templates to control what an end user could request. End users have to navigate through a series of menus to select entitlement before they can submit and access request. An end user's access to request templates was controlled by his/her role memberships.	Oracle Identity Manager 11gR2PS3 provides a new user interface with a shopping cart-type request model through which end users can search and browse through the catalog and directly request any item such as roles, entitlements, or applications, without having to navigate through a series of menus. In addition to this, several business-friendly metadata such as description, audit objective, tags, owner, approver, technical glossary, and so on can be associated to each access item, to display business-friendly and rich contextual information to a business user at the time of self service access request and access review. UDFs which are marked as searchable will automatically be part of advance search form. You can customize the search form. Attributes can be used to search catalog items. Catalog is the single point for managing access.
3	Oracle Identity Manager 11gR1x has to be integrated with Oracle Identity Analytics(OIA) to leverage advanced access review capabilities.	OIA functionality is now ported into OIG. Customers can define and manage identity audit policies based on IDA rules. Customers can define owners and remediators for a policy , which can be a specific user, a list of users or an OIM role Customers can use preventive and detective scan capabilities which can create actionable policy violations. Oracle Identity Manager 11gR2PS3 has comprehensive role lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI. It also includes detailed Role Analytics to aid with the composition and modifications of roles.
4	In Oracle Identity Manager 11gR1x, Resource and IT resource names tend to be named in a manner such that it	Oracle Identity Manager 11gR2PS3 provides an abstraction entity called Application Instance. It is a combination of IT

	is easy for the IT users to manage them. The problem with this approach is that if a business user has to request access the resource name will not make sense to him/her. These incomprehensible Resource and IT resource names make the access request process non intuitive	resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business friendly names to Application instances and map them to corresponding IT resources and Resource Objects. End users who request for accounts through the catalog will search for an account by providing the business friendly Application Instance Name. Application instances are automatically created as part of the Upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to request for access to the application.
5	In Oracle Identity Manager 11gR1x, authorization policies are used to control a user's access to the functions within Oracle Identity Manager. Policy administration was done through a UI that was built specifically for Oracle Identity Manager	Oracle Identity Manager 11gR2PS3, provides a fine grained authorization engine to help you create various admin roles, for example, using attributes to define membership, you can restrict an administrator to managing home organization members only.
6	Introduced SOA based approval workflows in Oracle Identity Manager 11gR1x. Request templates are provided to create various request.	Oracle Identity Manager 11gR2PS3 includes a number of enhancements to the request workflow. Temporal grants allow the requester to specify the start and end date (grant duration) of the role, account and entitlements at the time of assignment. Administrators can configure approvals by creating workflow policy rules instead of approval policies. It also supports role requests (create , modify, delete etc).Also, now enabling SOA is optional.
7	Existing certification feature provides certifier selection based on User Manager, Organization Manager, Catalog Owner and Selected User.	Oracle Identity Manager 11gR2PS3 introduced additional certifier selection where role can be used to define certifiers. All members of a certifier role can see the certification in their inbox, but the first member who ‘claims’ the certification will be the primary reviewer for that certification.
8	Till Oracle Identity Manager 11gR1x, policies are implemented and customized using OIM plug-in and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies	Oracle Identity Manager 11gR2PS3 has introduced declarative policies that enable customers to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.

Below diagram provides the overview of the steps involved in upgrade process from 11.1.1.x.x to 11.1.2.3.0.

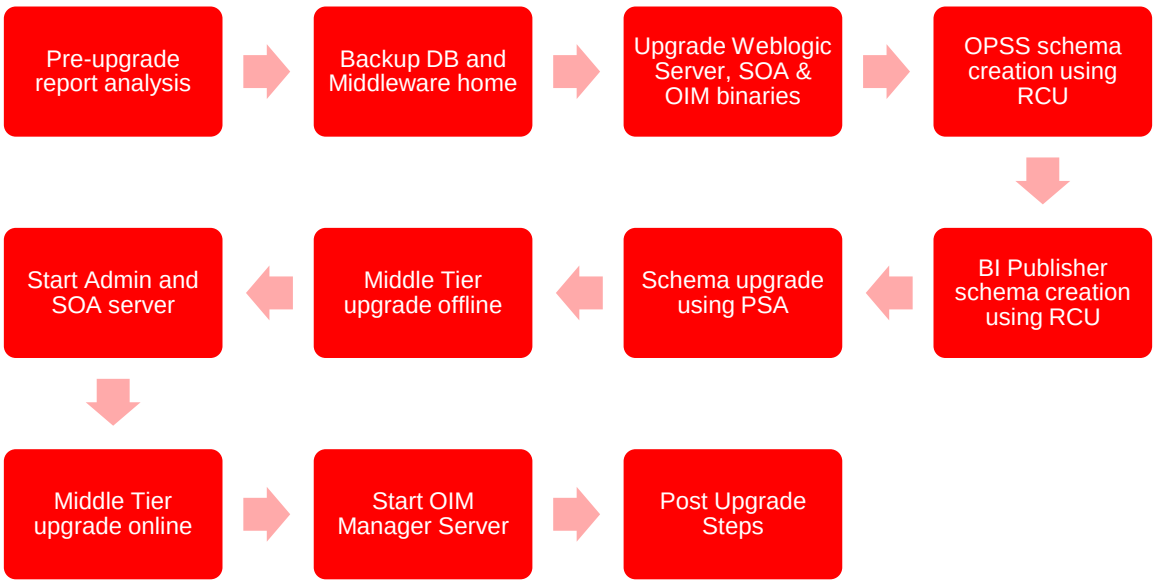


Figure 2: Upgrade from 11.1.x.x. to 11.1.2.3.0

1. First step involves tasks like generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report. The Pre-Upgrade Report utility analyzes your existing OIM environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before upgrade, cyclic groups in LDAP directory, deprecated authorization policies and potential issues in creating application instance.
2. Backup the database and the Middleware home. In the event of any incident you may need to do a quick restore of the database and the middleware home.
3. OIM 11g R2 PS3 requires Weblogic Server 10.3.6
4. OIM 11g R2 PS3 requires SOA Suite 11.1.1.9, download the SOA 11.1.1.9 binaries from edelivery.oracle.com and upgrade your existing SOA suite to 11.1.1.9. Refer to OIM release notes to identify and apply additional SOA patches.
5. Download the Identity and Access Management 11.1.2.3 (11g R2 PS2) binaries from edelivery.oracle.com and install the new binaries in the existing Middleware home. This step copies the new binaries to the Middleware home folder.
6. OIM 11g R2 PS3 uses Oracle Platform Security Services (OPSS). OPSS is the underlying security platform that provides security to Oracle Fusion Middleware including products like WebLogic Server, SOA, WebCenter, ADF, OES to name a few. To enable OPSS the first step is to use the Repository Creation Utility (RCU) and create the underlining OPSS database schemas.
7. Create BI Publisher schema using RCU. OIM 11.1.2.3.0 has embedded BI Publisher
8. Upgrade the OIM database schema. Use the patch set assistant(PSA) to upgrade OIM and dependent component schemas. The patch set assistant automatically identifies dependent schemas and upgrades them.
9. New capabilities are enabled by running the OIM Upgrade utility in both offline and online mode. This deploys new artifacts such as SOA Composites, Scheduled Jobs, CSF Credentials, etc.

10. Review the documentation and complete additional post upgrade steps.
11. Review the documentation and complete the steps to upgrade other components such as the Design Console and Remote Manager. Review the release notes to identify any patches that you may need to apply.

Upgrading from 10g releases

Upgrading from 9.1.0.x releases to 11g R2 PS3 is not direct. OIM 9.1.x should be upgraded to 11gR2PS2 first and then to 11gR2PS3. This requires a thorough assessment of new capabilities. Changes to authorization and request model needs to be assessed. Custom artifacts such as Entity adapters and any code that invokes legacy API's needs to be transformed into artifacts that align with 11g R2 PS3 design paradigms and orchestration. A number of functional and architectural enhancements have been introduced post 9.1.0.x to solve current and future business requirements such as scalability, performance and business friendly end user interfaces. Post upgrade customer can leverage these new capabilities to solve and address current and future business requirements.

Organizations should review and become familiar with the new capabilities before moving into the upgrade execution phase. Following is a summary of the key new capabilities added in OIM 11g R2 PS3 that are relevant for organizations upgrading from 9.1.0.x Releases. Refer to the product document for a detailed description of the new capabilities.

TABLE 3: FEATURE COMPARISION

S.No	Oracle Identity Manager 10g	Oracle Identity Manager 11gR2PS3
1	The Oracle Identity Manager 9.1.x.x User Interface is built on the struts framework. It provides basic self service interfaces.	Oracle Identity Manager 11gR2PS3 uses Alta skin which is business (mobile, cloud) friendly .OIM now has a new Home page, new my profile page with a user-friendly inbox. Most UI customizations will need to be re done to match the look and feel of 11gR2PS3
2	Oracle Identity Manager 9.1.x.x provides basis self service capabilities such as password reset and account request.	Oracle Identity Manager 11gR2PS3 provides a new user interface with a shopping cart-type request model through which end users can search and browse through the catalog and directly request any item such as roles, entitlements, or applications, without having to navigate through a series of menus. In addition to this, several business-friendly metadata such as description, audit objective, tags, owner, approver, technical glossary, and so on can be associated to each access item, to display business-friendly and rich contextual information to a business user at the time of self service access request and access review. UDFs which are marked as searchable will automatically be part of advance search form. You can customize the search form. Attributes can be used to search catalog items. Catalog is the single point for managing access.
3	Oracle Identity Manager 9.1.0.x provided Identity Attestation to periodically review a user's access. For advanced access review capabilities such as role or data owner certification, OIM 9.1.0.x had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities that OIA provided.	OIA functionality is now ported into OIG. Customers can define and manage identity audit policies based on IDA rules. Customers can define owners and remediators for a policy , which can be a specific user, a list of users or an OIM role Customers can use preventive and detective scan capabilities which can create actionable policy violations. Oracle Identity Manager 11gR2PS3 has comprehensive role

		lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI. It also includes detailed Role Analytics to aid with the composition and modifications of roles. lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI. It has now detailed Role Analytics to aid the composition of a role.
4	In Oracle Identity Manager 9.1.0.x, users are assigned to organizations by specifying an organization name in the Organization attribute of the user details. This is a static organization membership. A user can only be a member of one organization.	In Oracle Identity Manager 11gR2PS3, in addition to the existing feature, you can dynamically assign users to organizations based on user-membership rules, which you can define in the Members tab of the organization details page. All users who satisfy the user-membership rule are dynamically associated with the organization, irrespective of the organization hierarchy the users statically belong to. With this new capability, a user can gain membership of one home organization via static membership and multiple secondary organizations via user-membership rules that are dynamically evaluated.
5	Oracle Identity Manager 9.1.0.x Resource and IT resource names tend to be named in a manner such that it is easy for the IT users to manage them. The problem with this approach is that if a business user has to request access the resource name will not make sense to him/her. These incomprehensible Resource and IT resource names make the access request process non intuitive.	Oracle Identity Manager 11gR2PS3 provides an abstraction entity called Application Instance. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business friendly names to Application instances and map them to corresponding IT resources and Resource Objects. End users who request for accounts through the catalog will search for an account by providing the business friendly Application Instance Name. Application instances are automatically created as part of the Upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to request for access to the application.
6	In Oracle Identity Manager 9.1.x, policies are implemented and customized using OIM plug-in and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies	Oracle Identity Manager 11gR2PS3 has introduced declarative policies that enable customers to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.

Below diagram provides the overview of the steps involved in upgrade process from 9.1.x.x to 11.1.2.2.0 and then refer figure 1 for the upgrade process from 11.1.2.2.0 to 11.1.2.3.0.

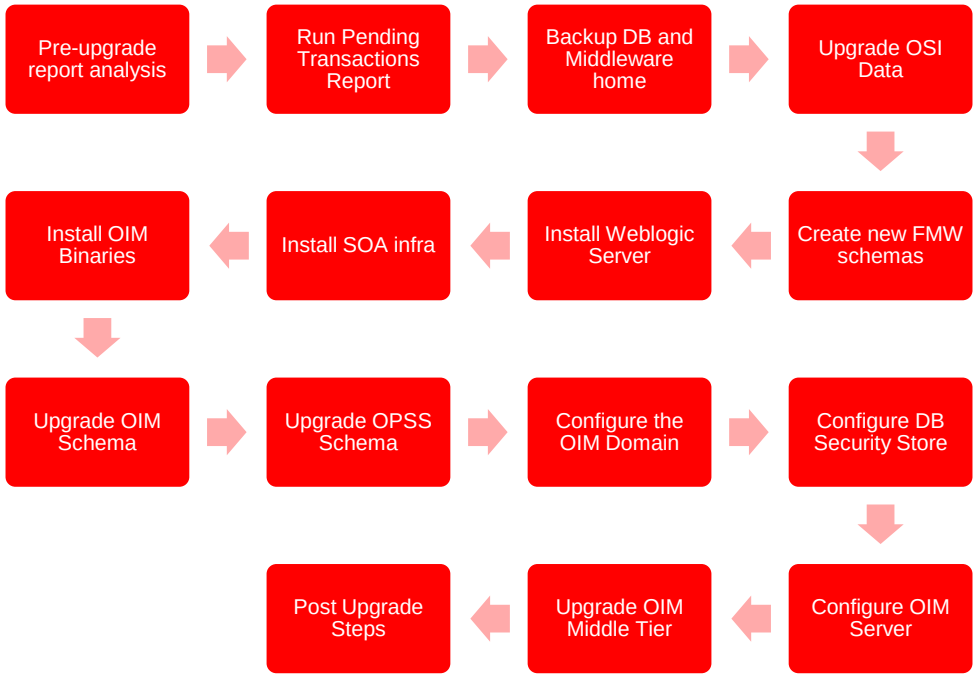


Figure 3: Upgrade steps from 9.x to 11.1.2.2.0

1. First step involves tasks like generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report. The Pre-Upgrade Report utility analyzes your existing OIM environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before upgrade, cyclic groups in LDAP directory, deprecated authorization policies and potential issues in creating application instance.
2. Run the pending transactions report. This report facilitates identification of pending transactions, e.g. pending Approval tasks, pending Off-line Provisioning Tasks, pending Audit Tasks, etc in the environment. Organization should complete on all the identified pending items which otherwise will become orphan post upgrade.
3. Backup the database and the Middleware home. In the event of any incident you may need to do a quick restore of the database and the middleware home.
4. The format of values stored in the internal column osi_note which contains transient values used in processes, is different in Oracle Identity Manager 11.1.2.2.0 when compared to Oracle Identity Manager 9.1.x.x. As the format of the values is incompatible, you must clean the existing values using the OSI Data Upgrade utility before you proceed with the upgrade. The OSI Data Upgrade utility upgrades the OSI data.
5. Using the Repository creation utility create database schemas for dependent Oracle FMW components.
6. OIM 11g R2 PS2 requires Weblogic Server 10.3.6. Install Weblogic Server 10.3.6.
7. OIM 11g R2 PS2 requires SOA Suite 11.1.1.7, download the SOA 11.1.1.7 binaries from edelivery.oracle.com and upgrade your existing SOA suite to 11.1.1.7. Refer to OIM release notes to identify and apply additional SOA patches.
8. Download the Identity and Access Management 11.1.2.2 (11g R2 PS2) binaries from edelivery.oracle.com and install the new binaries in the Middleware home. This step copies the new binaries to the Middleware home folder
9. Using the upgrade assistant (UA) upgrade the OIM schemas from version 9.0.1.x to 11.1.2.2.

10. The OPSS Schemas created by the Repository Creation Utility (RCU) are of version 11.1.1.7. There are additional security and performance fixes in version 11.1.1.7.2. To uptake these enhancement you need to run the Patch Set Assistant (PSA) and update the OPSS database schemas.
11. Create a WebLogic domain for Oracle Identity Manager 11.1.2.2 by running the configuration wizard from the Oracle Identity Manager 11.1.2.2 home.
12. Configure the OPSS Security Store. The OPSS security store is the repository for system and application-specific policies, credentials, and keys. While configuring choose the database based security store.
13. Configure the Oracle Identity Manager 11.1.2.2.0 Server using the configuration wizard.
14. New capabilities are enabled by running the OIM Upgrade utility. This deploys new artifacts such as SOA Composites, Scheduled Jobs, CSF Credentials, etc.
15. Review the documentation and complete the steps to upgrade other components such as the Design Console and Remote Manager. Review the release notes to identify any patches that you may need to apply.

General Guidelines

- Refer to the product documentation to collect log files for each step.
- Ensure you follow the sequence of steps mentioned in the documentation.
- Pay special attention to the server startup/shutdown instructions before executing each step.
- Save OIM Managed server logs that are generated when you start the OIM server for the first time after completing upgrade.
- At any point if there is a failure it is recommended to restore the environment from the backups and go through the upgrade procedure.
- To leverage new features refer to the User, Admin and Developer Guides that are included with the product documentation.

Connector Considerations

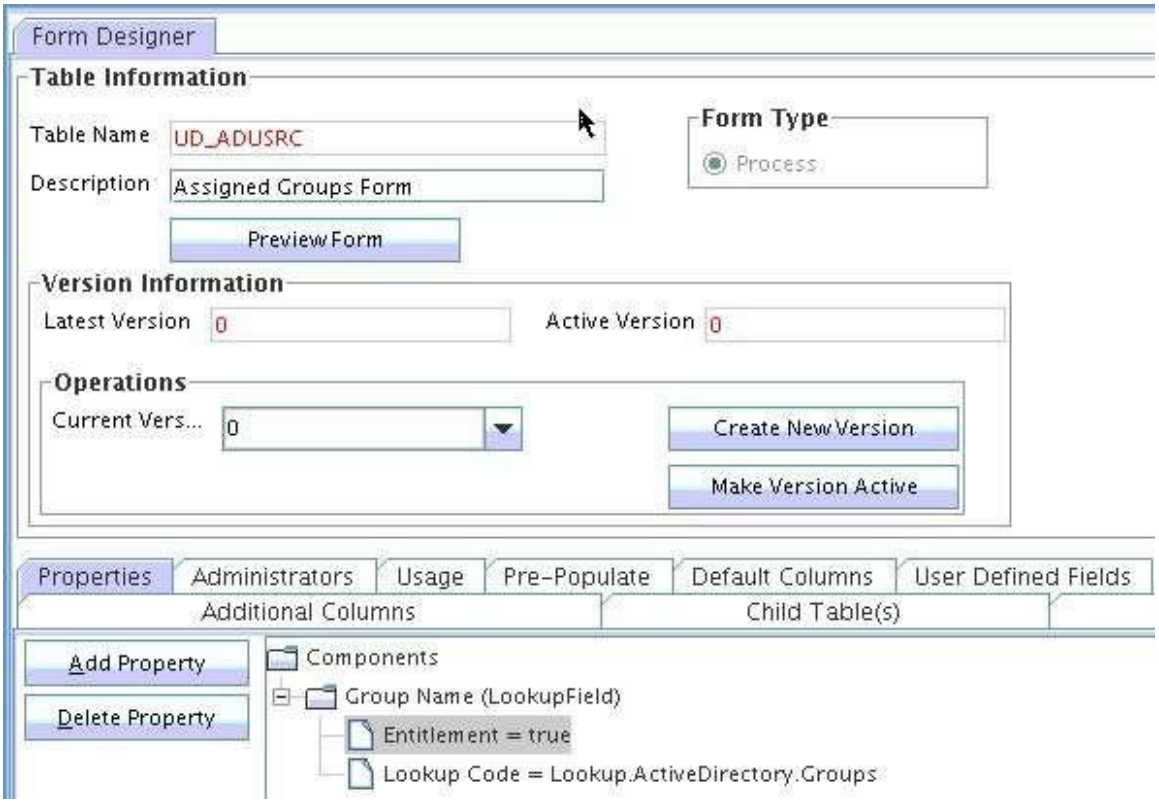
This section is relevant for Release Upgrades. Organizations upgrading from 9.x or 11.1.1.x will need to ensure that certain connector specific properties are set, most out of the box connectors already have these properties set. If these properties are not set new capabilities such as the Catalog, Identity Certification, etc will not work as designed.

- **Entitlements Tagging**

The child form attributes which are provisioned as an entitlement has to be specifically tagged.

Impact: If the attribute is not tagged as an entitlement it won't show up in catalog and end users will not be able to request for the entitlement from the cart. Also Identity certification will not work.

Action: All entitlement attributes should be tagged with “Entitlement = true” field property.



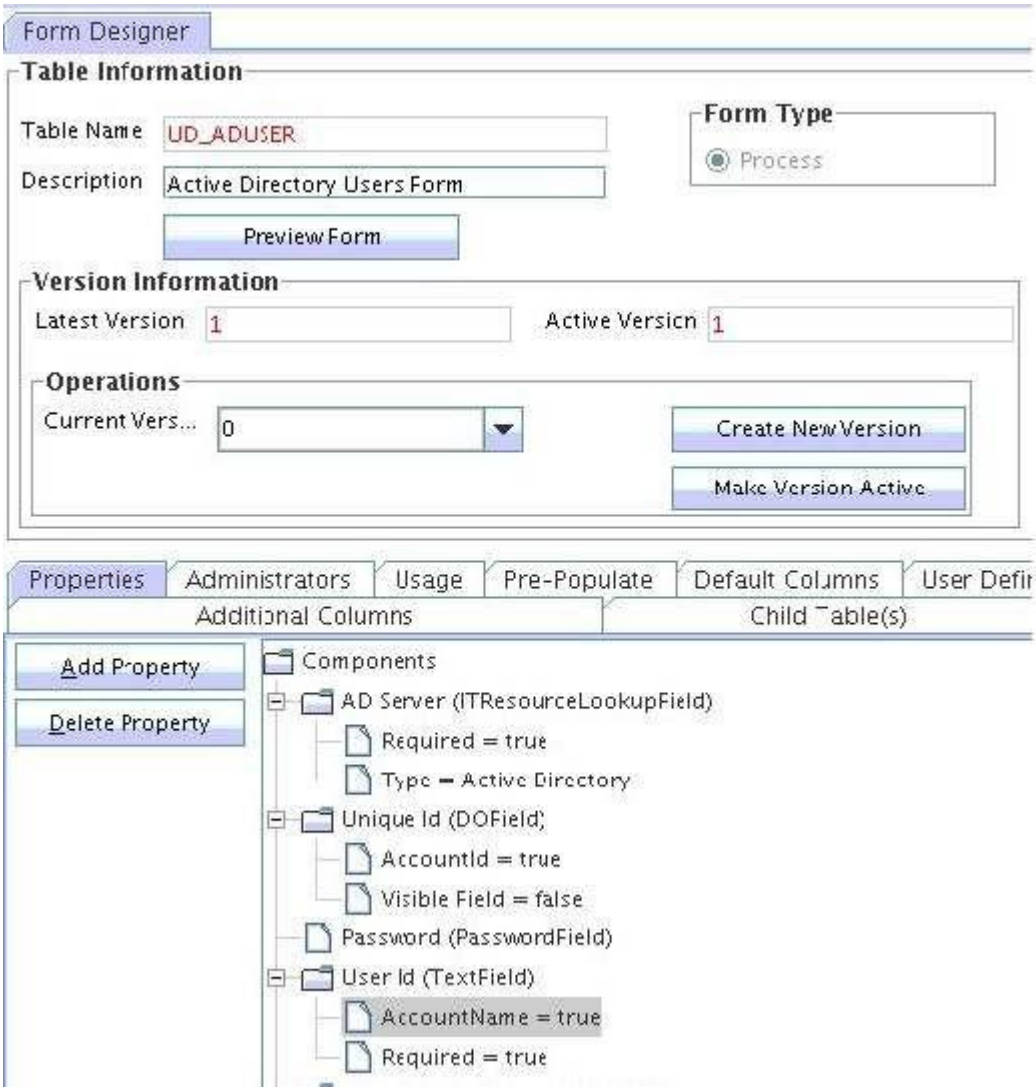
Screenshot 1: Setting Entitlement Property

» Account Tagging

One of the unique attributes of the process form should be tagged as account name, which will be displayed on the Resource UI, and hence will help the user differentiate various accounts.

Impact: If this is not present, the account name field in “My Accounts” will show the DB numeric key which does not make sense from the end user perspective. Also Identity certification will not work.

Action: Tag one of the unique attributes of the process form with “AccountName =true” field property



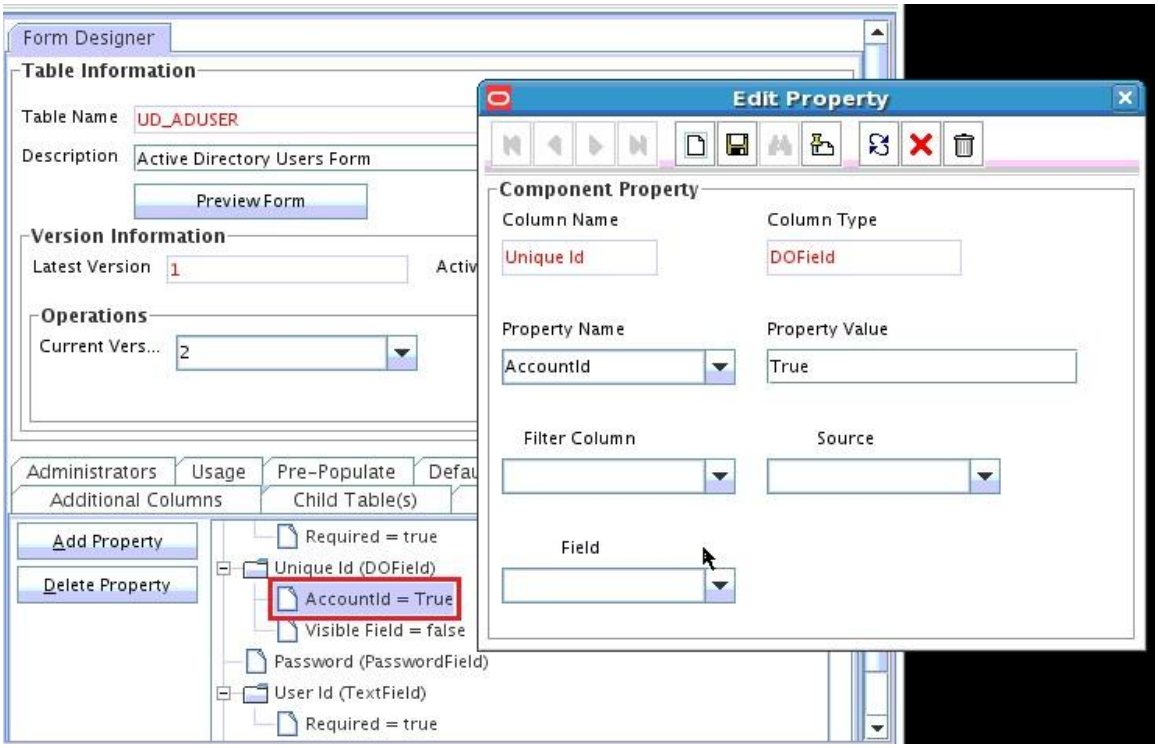
Screenshot 2: Setting Account Name property

» Account ID Tagging

The field that is tagged as AccountId represents the immutable GUID of the specific account (if one exists).

Impact: Identity Certification will not work.

Action: Tag the GUID field of the process form with “AccountId = true” field property. If no such field is present, tagging can also be done to Login Name/Login ID field which uniquely identifies the account on the target.



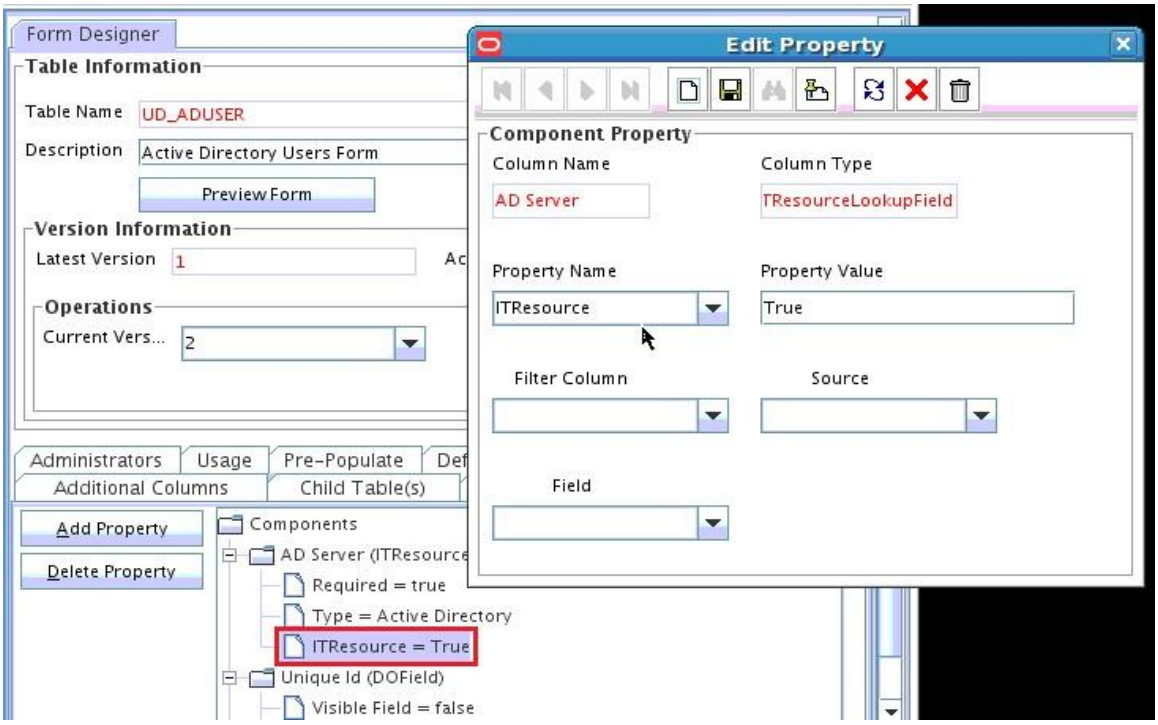
Screenshot3: Setting Account ID property

» IT Resource Tagging

The IT Resource field of the process form should be tagged with IT Resource property. Note if you are using a connector for reconciliation the IT Resource field needs to be tagged in the reconciliation field mappings as well.

Impact: Identity Certification will not work. Account reconciliation will not work.

Action: Tag the IT Resource field of the process form with “ITResource = true” field property. Tag the IT Resource field in the reconciliation mappings.



Screenshot 4: Setting ITResource Property

» Lookup by Query

OIM 9.1.x and 11.1.1.x supported lookups of type Lookup by query. OIM 11.1.2.x does not support lookups of type Lookup by query.

Action: Any such lookup needs to be converted to Lookup of type Lookup Code.

» Pre-populate Adapters

In OIM 11.1.2.x Pre-populate adapters associated with the forms do not auto populate forms at the time of an end user request. The pre-populated values will not be displayed on screen at the time of request.

Action: 11g Plug-ins must be developed and mapped to form fields to auto populate a form at the time of end user request.

» Localizing Field Labels in UI Forms

Post upgrade to OIM 11.1.2.3 perform the procedure described in the section Localizing Field Labels in UI Forms of each connector's documentation if you need to localize UI form field labels.

» Connector Upgrades

Organizations should upgrade to the versions supported by OIM 11g R2 PS3. They can make use of the Connector Lifecycle Management feature that automates Connector upgrades.

Upgrade Best Practices

- Read the release notes to identify known issues and workarounds.
- Do not ignore sizing. Based on new processes and capabilities that you plan to uptake you may need to add more compute capacity.
- Test upgrade in Development environment first, then staging and finally production.
- Test plan should include post upgrade functional tests and performance tests as well.
- Ensure you have run the pre-upgrade report and have completed all “to-do” actions flagged in the reports.
- The documentation is your best friend; make sure you are familiar with the steps.
- Validation instructions are provided in the documentation for most upgrade steps, after each upgrade step go through the validation instruction to ensure that there are no errors.
- Become familiar with new functionality such as Catalog, Entity and Organization Publishing, OES Authorizations, Plug-ins, ADF UI customization and SOA Approval workflows before starting the upgrade.
- In the event of upgrade issue, refer to the product documentation to identify and capture diagnostics logs, create a Service Ticket and attach the logs along with a description of the issue and your environment.
- Get a commitment from all stakeholders.

Conclusion

Organizations that upgrade to OIM R2 PS3 can leverage the benefits of the Oracle Identity Governance Platform. With this platform you get a single rationalized solution through which you can deliver access request and access review capabilities. These capabilities will be delivered from a single technology stack and will enable organization to simplify their deployments, reduce their total cost of ownership and accelerate their return on investment.

For further information on Oracle Identity Manager and the Oracle Identity and Access Management platform, please visit: http://www.oracle.com/identity

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together

White Paper Title
August 2015
Author: Niharika
Contributing Authors: [OPTIONAL]