ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Upgrading to Oracle Identity Governace 12.2.1.3.0

Technical Overview

ORACLE WHITE PAPER | AUGUST 2017

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, HIPPA and GDPR). 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 Governance (hereafter OIG) 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 Governance which is 12c PS3 (12.2.1.3.0) and upgrade process in general.

Benefits of Upgrading to OIG 12cPS3

Organizations that upgrade to OIG 12cPS3 can leverage the benefits of the Oracle Identity Governance Platform. With this platform you get a single rationalized solution through which you can deliver simplified application on boarding, access request and access review capabilities. These capabilities will be delivered from a single technology stack and will enable organization to

- Simplify their deployments, upgrade
- Reduce their total cost of ownership
- Accelerate their return on investment
- Reduce time to go live

What's new in 12cPS3

- Simplified wizard based application on-boarding process which enables business users to on-board applications in OIG without knowing lots of technical jargons. It allows users to create and manage applications, templates, and instances of applications, and clone applications from self service UI.
- Enables to define own custom access reviewer and group review for user certifications and provides real-time certification purging solution
- Improved access policies which can be enforced at inherited access grants.
- Simple, three steps wizard based deployment manager flow.
- SCIM resources are secured by custom Oracle Web Services Manager (OWSM) policy, custom request headers, and a origin whitelist.
- Oracle Identity Governance provides a JSON Web Token (JWT) service to simplify the use of Oracle Identity Governance SCIM-REST service. See Using the JSON Web Token (JWT) Service.
- Oracle Identity Governance provides policy sets containing attached OWSM policies on application path that make Restful and SOAP services secure.

» Complete Identity Governance Platform

An enterprise will get a single solution through which they can easily on board new applications and do both access request and access review from a single converged solution. The application on boarding features offer very easy wizard based configurations of applications and in-build editor for the customization logic e.g. transformation and validation business logic.

Organizations can now design certification campaigns for customer reviews and group reviewers base on their business requirements, through which both business and IT can collaborate to make an access review decision.

Significant enhancements have also been made to provide a more user friendly and navigation friendly UI for certification dashboard. The Certification Dashboard enables sorting and listing the certifications by the percentage completion of the certifications. Group or certifier assignments must be claimed by a user to take actions on it and released by the user for other users in the group to view the actions taken.

New option to *"Include entitlements provisioned by access policy"* has been introduced for creating an entitlement certification definition which will enable business users to certify the access which is granted by policy. Now, OIG provides a new real-time certification purging solution.

Policies has been improved significantly and now OIG supports inheriting the access granted via access policies from the parent role to child role. Access policy can be created and managed from Self Service UI.

We have also further simplified the In Identity System Administration; the Import and Export options for incremental migration of deployments by using the Deployment Manager have a new interface and flow. Its just simple three steps wizard based approach and very easy to use.

SCIM and REST services has been enhanced and more security has been added to REST and SCIM services. SCIM and REST resources are now secured by OWSM JWT token. Now, OIG provides better administration of the keys, File based store has been replaced by key store services and TLS support has been added for various TLS Ciphers.

» Full Lifecycle Management

Oracle Identity Governance 12cPS3 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, customer users and support for service account with customization.

» Business Friendly Application on Boarding

Access Oracle Identity Governance provides a quick and convenient way to on-board applications (AOB) using the Applications option to business users. It quickly on boards the application into the OIG system and save the time and cost to bring one application on board. The wizard based simple approach allows business users to step through basic configuration to complete the application on boarding process. It just asks for the minimum details to on board an application.

This offers an interface to write business logic for validation and transformation business logic capabilities which need not to be complied and plugged in with binaries. It offers the application template creation and import export options by which one application can be easily import/export form one environment to other environment. Application on-boarding offers capability in Oracle Identity Self Service to create and manage applications,

templates and instances of applications and clone applications. AOB templates cover most of the features offered by design console.

An application templates is just the xml representation of the application with some pre-filled values, with the help of application templates you can create any numbers of applications.

» Easy & Accurate Identity Certifications

Identity Certifications in OIG 12cPS3 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. OIG supports time or event based certification campaigns with quick closed loop remediation. Certifications can also be completed in offline mode and reviewers can customized.

» Rapid and Scalable Fulfillments

OIG 12cPS3 supports both automated and manual fulfillment processes. Identity Connector Framework automates the provisioning to popular on-premise and cloud apps. OIG 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.

OIG has huge numbers of connectors; with the help of these connector automatic provisioning/de-provisioning happens immediately. OIG connector stacks includes:-

Business Applications: Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP

LDAP stores: Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory

Security systems: RSA, RACF, Top Secret, ACF2

Collaboration Suites: Exchange/Domino and GroupWise

Operating systems: OEL, Red Hat Linux, HP-UX, AIX, Solarix, AS/400 and Windows

Ticket Management systems: BMC Remedy

Cloud Connectors: Oracle CRM On- demand, Google Apps, Office 365, Salesforce, ServiceNow, Concur, Box, DropBox, GoToMeeting, WebEx and SuccessFactors

Databases: Oracle, MySQL, SQL Server, DB2, Sybase

Technology Integrations: SSH, Telnet, Flat File, JDBC, LDAP V3, SOAP, Generic Scripting Connector(BeanShell, Groovy and JS), REST and SCIM

» Flexible and Modular Architecture

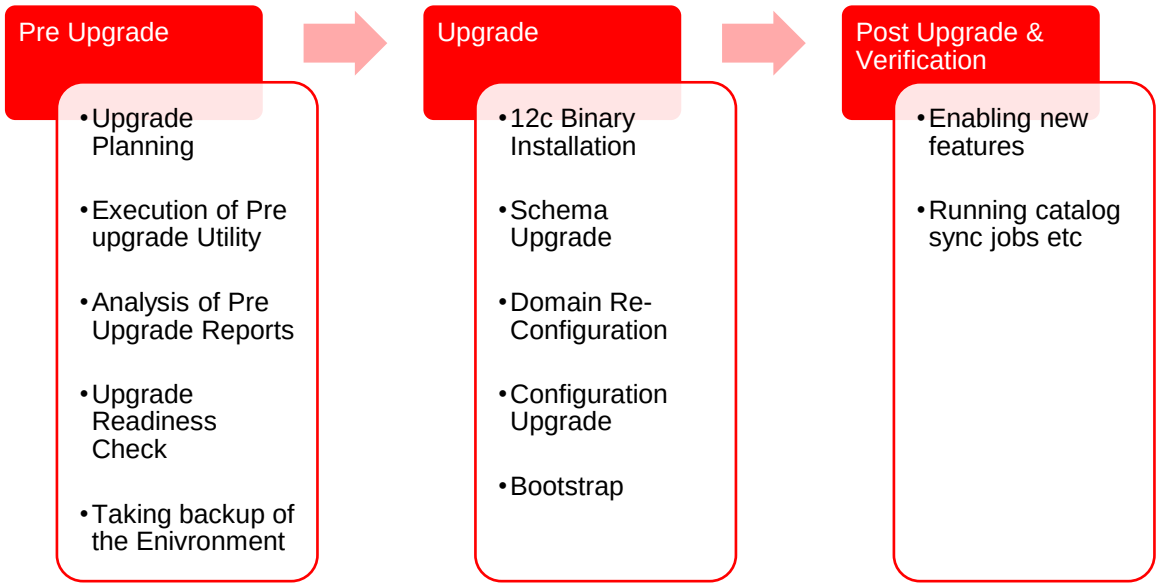
OIM 12cPS3 has flexible modular architecture which fits with your governance requirements. It has single data store for all phases of identity governance. You can easily customize and model your identity governance projects. There are multiple points of entry to begin like building an access catalog to enable request process, automating access certification and automating provisioning to key applications.

Upgrading Oracle Identity Governance

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.

OIG 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 OIG 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.

In pre-upgrade phase you also need to upgrade the server wallet and DB wallet to remove MD5 algorithm. Please go through upgrade guide for more details.

» Phase 2: Upgrade

In this phase, the actual upgrade happens. It will update the whole FMW stack and the OIG server. The whole upgrade process is offline process. But, there are certain tasks which OIG performs online. After FMW stack upgrade, when OIG server starts first times; it performs certain upgrade related task in online manner when bootstrap task get invoked. In 12cPS3 upgrade, domain upgrade is in place upgrade and middleware is out of place upgrade.

12cPS3 Quick Start Installer will install all the binaries i.e. OIG, SOA and WebLogic etc. Then Schema will get updated and domain reconfiguration will take place and it will upgrade the configurations of each components. Then bootstrap task will perform online task which are mandatory for OIG upgrade.

» 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 OIG upgrade guide for information related to post upgrade steps.

Upgrading from 11gR2PS3 (Manual Deployment) releases

Supported starting point for is upgrading Oracle Identity and Access Management to 12c (12.2.1.3.0) is Oracle Identity and Access Management 11g Release 2 PS3 (11.1.2.3.0).

If you are not using the 11.1.2.3.0 version of Oracle Identity and Access Management, you must upgrade to 11.1.2.3.0 before you move to 12c (12.2.1.3.0).

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 OIG 12cPS3 that are relevant for organizations upgrading from 11g R2PS3 releases. Refer to the product documentation for a detailed description of the new capabilities.

Below diagram provides the overview of the steps involved in upgrade process from 11.1.2.3.0 to 12.2.1.3.0

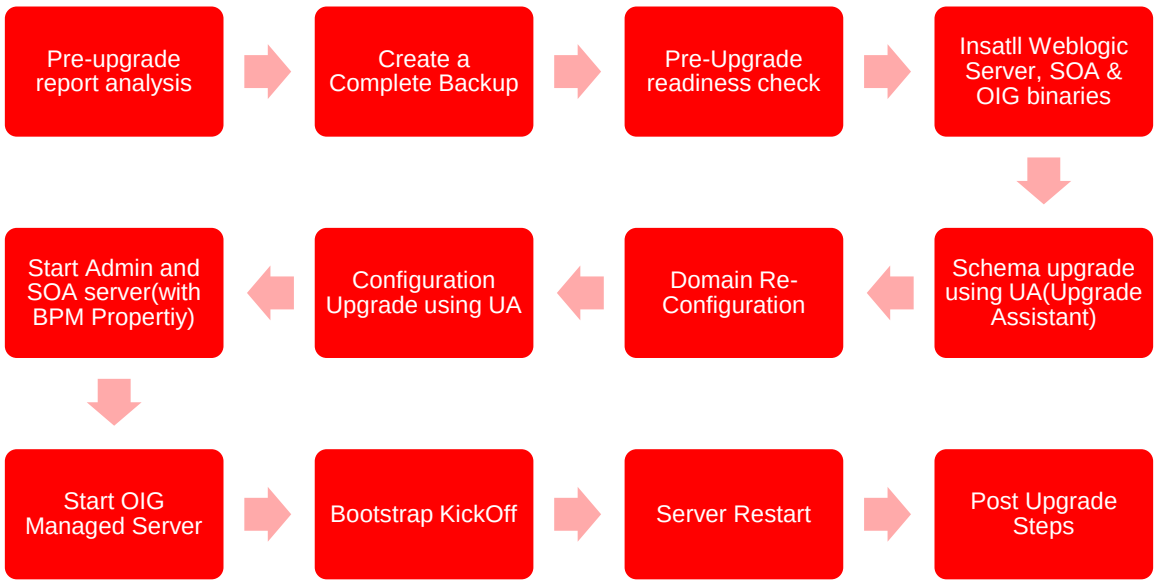


Figure 1: Upgrade steps from 11.1.2.3.0 to 12.2.1.3.0

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 domain home. In the event of any incident you may need to do a quick restore of the database and the domain home.
3. In 12c PS3 features quick start installer, which installs WebLogic, IDM and SOA binaries in one go.
4. Upgrade the OIG database schema. Use the Upgrade Assistant to upgrade OIG and dependent component schemas. The Upgrade Assistant automatically create required 12c schema and identifies dependent schemas and upgrades them.
5. Domain re-configuration utility will upgrade 11gR2PS3 domain to 12cPS3 domain
6. Upgrade the OIG configuration using the upgrade assistant. The Upgrade Assistant automatically identifies dependent products configuration and upgrades them.
7. Start Admin Sever, SOA Server (With BPM Property) and OIG managed Server. Bootstrap task will be kicked off to perform online upgrade tasks
8. Restart all the servers after successful bootstrap
9. Review the release notes to identify any patches that you may need to apply.
10. BI Publisher needs to be installed and configured separately.

Upgrading from 11gR2PS3 (LCM Tool Deployment) releases

Upgrading from 11g R2PS3 goes through a different process as LCM tool created one private and shared domain. Upgrade assistance will run all the upgrade utilities on the shared domain and then will takes backups from the private domain and delete the private domain. It will then pack the shared domain on private domain.

Below diagram provides the overview of the steps involved in upgrade process from 11gR2PS3 LCM tool deployment to 12.2.1.3.0.

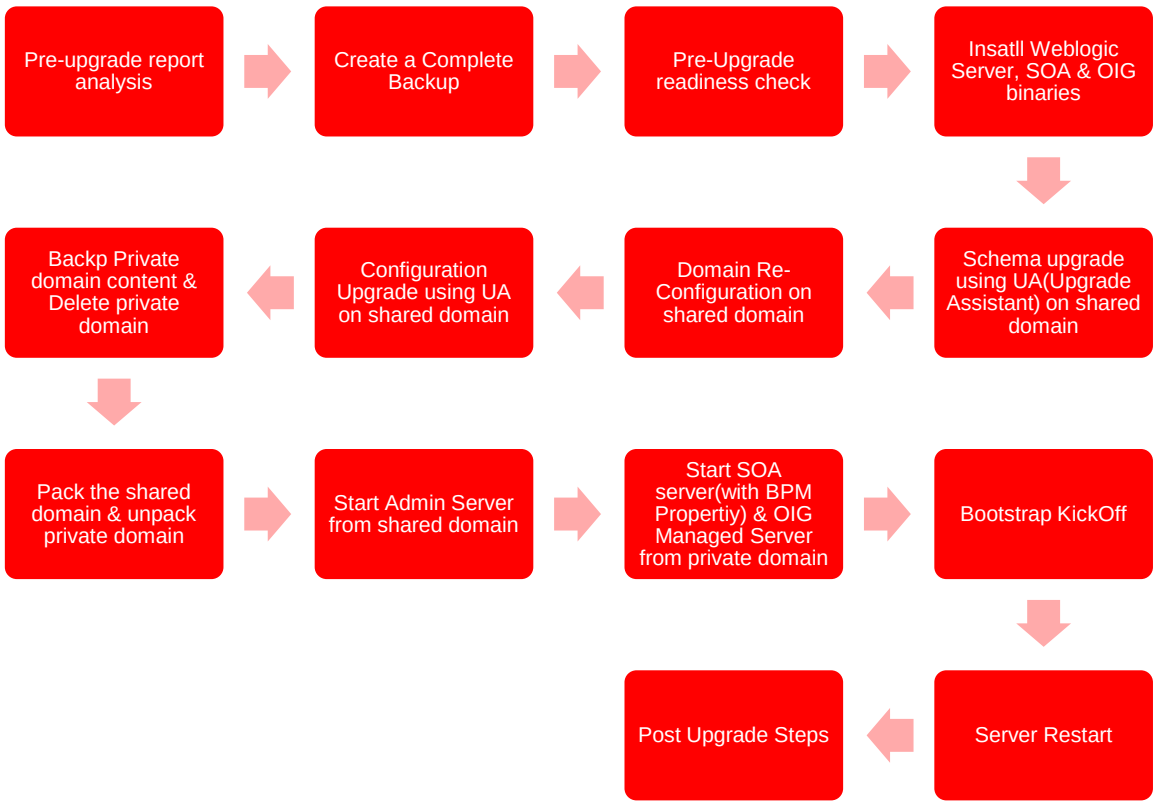


Figure 2: Upgrade from 11.1.x.x. to 11.1.2.3.0

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 domain home. In the event of any incident you may need to do a quick restore of the database and the domain home.
3. In 12c PS3 features quick start installer, which installs WebLogic, IDM and SOA binaries in one go.
4. Upgrade the OIG database schema on shared domain. Use the Upgrade Assistant to upgrade OIG and dependent component schemas. The Upgrade Assistant automatically create required 12c schema and identifies dependent schemas and upgrades them.
5. Run Domain re-configuration utility on shared domain, it will upgrade 11gR2PS3 domain to 12cpPS3 domain
6. Upgrade the OIG configuration using the upgrade assistant on shared domain. The Upgrade Assistant automatically identifies dependent products configuration and upgrades them.
7. Backup the private domain and delete the content of private domain
8. Pack shared domain and unpack onto empty private domain
9. Start Admin Sever from shared domain, SOA Server (With BPM Property) and OIG managed Server on private domain. Bootstrap task will be kicked off to perform online upgrade tasks

10. Restart all the servers after successful bootstrap
11. Review the release notes to identify any patches that you may need to apply.
12. BI Publisher needs to be installed and configured separately.

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 OIG Managed server logs that are generated when you start the OIG 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.
- Remote Manager and Design Console have not been supported in 12c release. So, will not get upgraded as part of 12cPS3 upgrade.

Connector Considerations

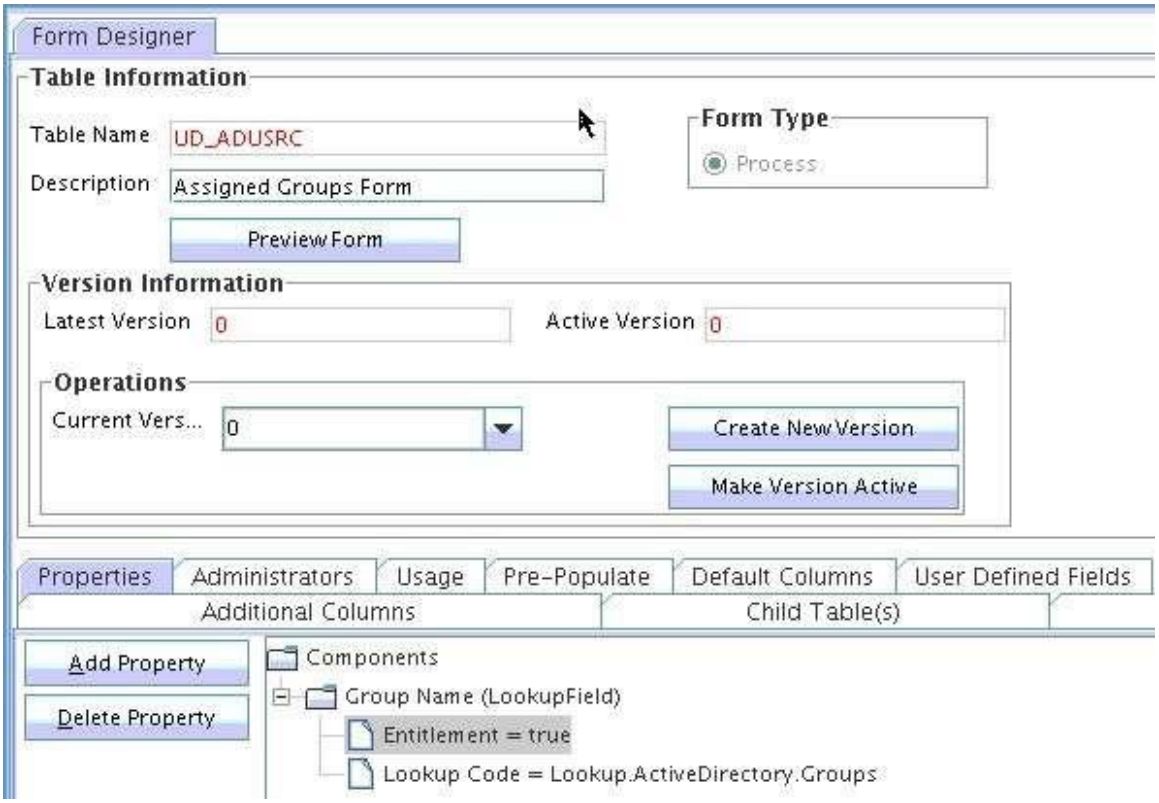
This section is relevant for Release Upgrades. Organizations upgrading from 9.x or 11.1.1.x will need to ensure that certain connector specific properties are set, most out of the box connectors already have these properties set. If these properties are not set new capabilities such as the Catalog, Identity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



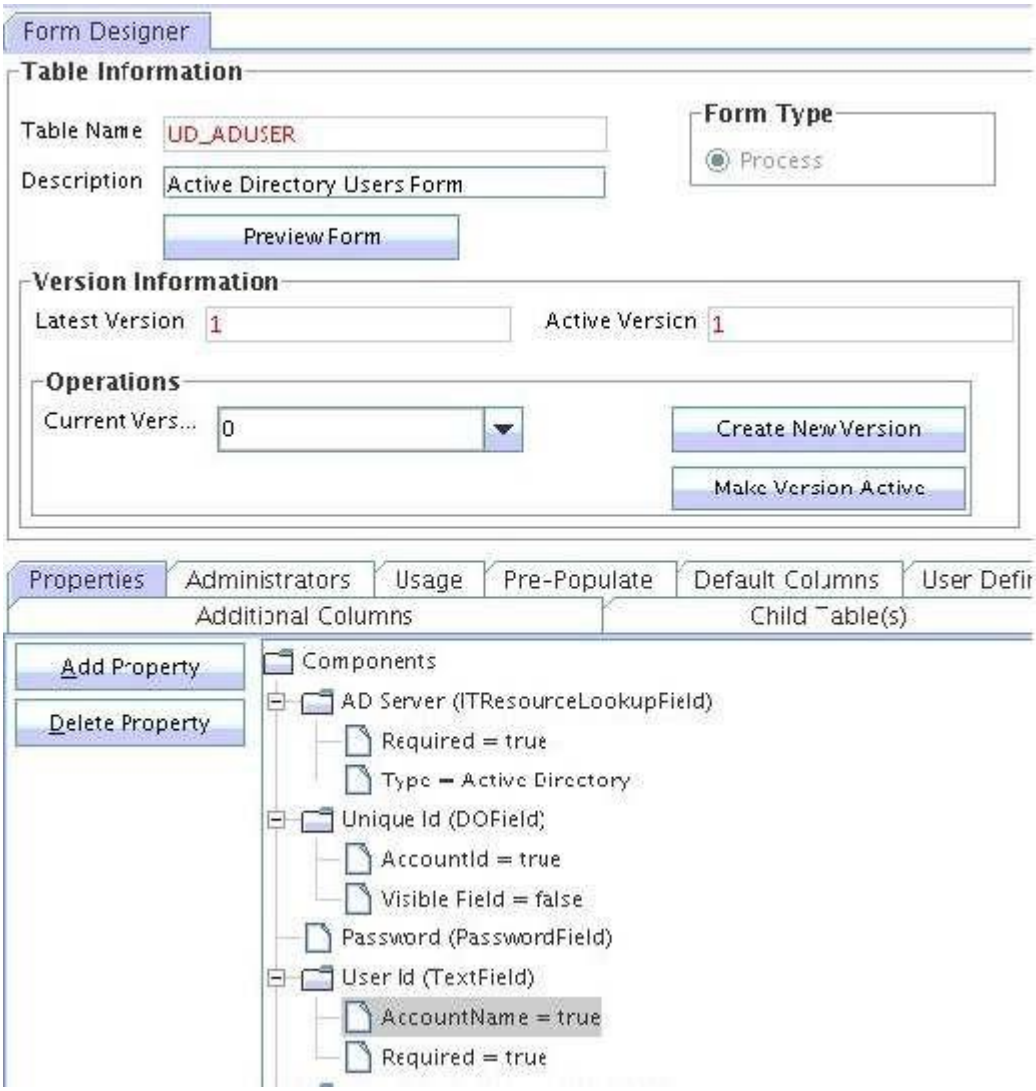
Screenshot 1: Setting Entitlement Property

» 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



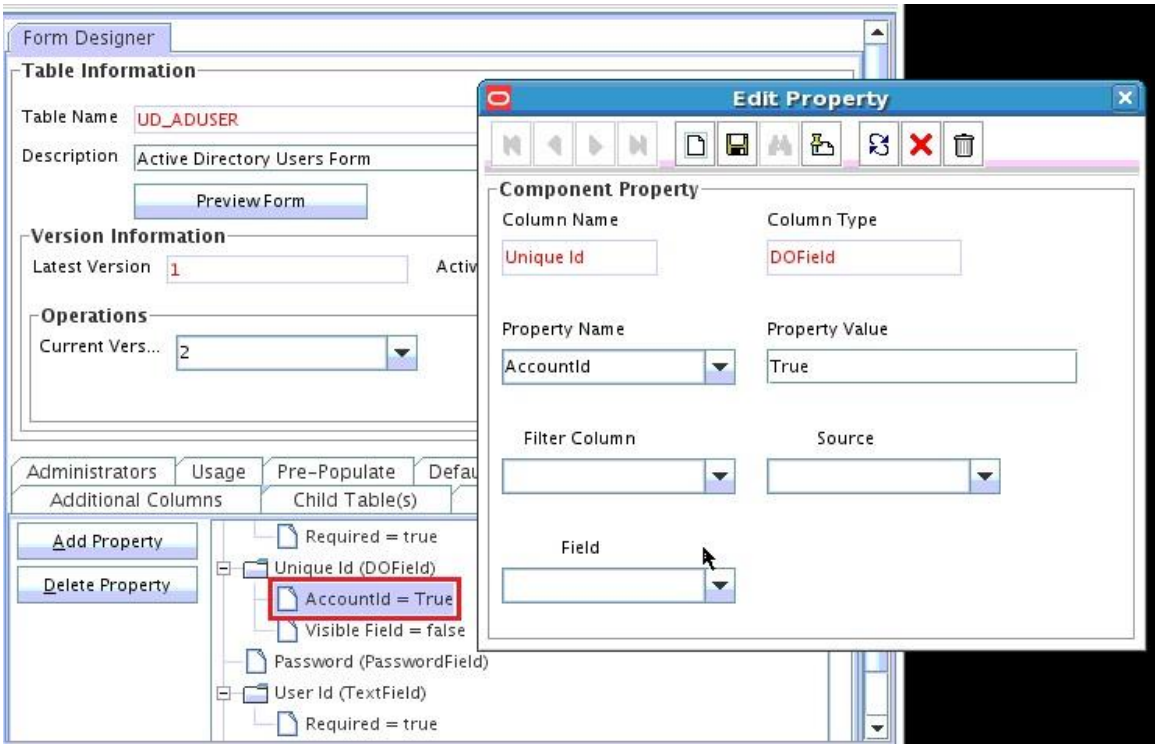
Screenshot 2: Setting Account Name property

» 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.



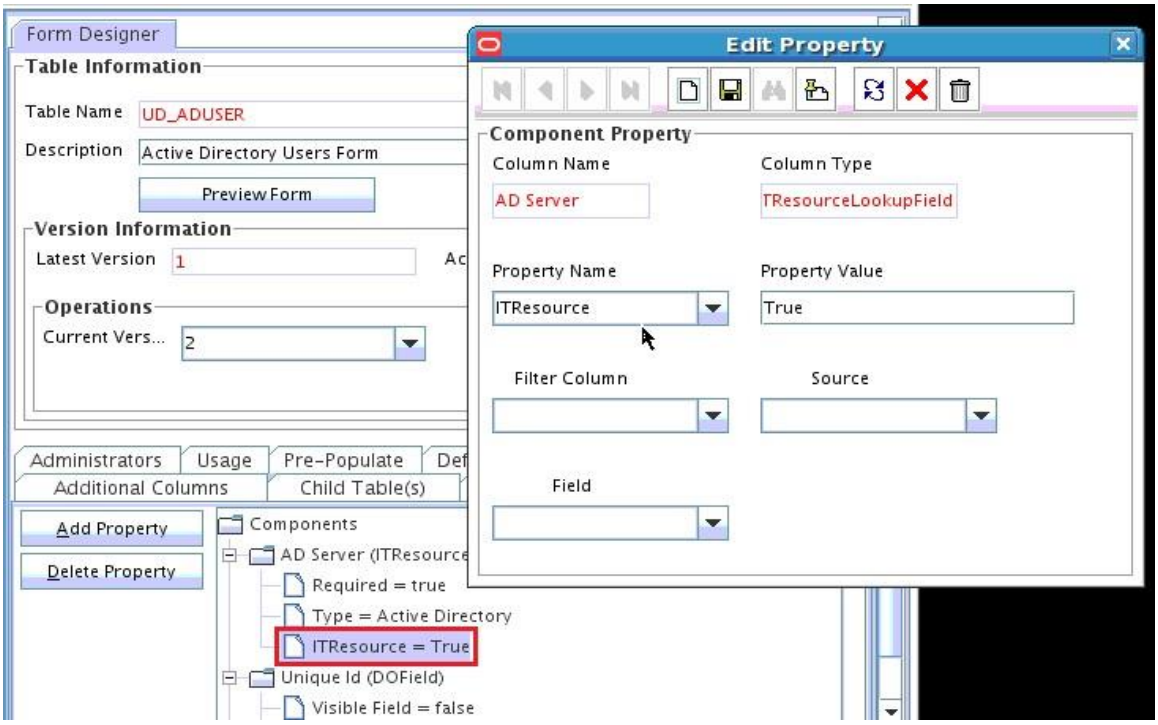
Screenshot3: Setting Account ID property

» 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 OIG 12.2.1.3 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 OIG 12c 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, OPSS 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 OIG 12c 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 Governance 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 2017
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]


Oracle is committed to developing practices and products that help protect the environment