ORACLE

Oracle Identity Governance (12.2.1.3)
Overview and Frequently Asked Questions
August 2017

Overview

These frequently asked questions serve as a supplement to the product documentation and answer the most commonly asked questions for the 12c PS3 release of Oracle Identity Governance.

General Questions

1. What is Oracle Identity Governance (OIG)?

   Oracle Identity Governance is a highly flexible and scalable enterprise identity administration system that provides operational and business efficiency by providing centralized administration & complete automation of identity and user provisioning events across enterprise as well as extranet applications. It manages the entire identity and role lifecycle to meet changing business and regulatory requirements and provides essential reporting and compliance functionalities.

   Note: - Oracle Identity Manager and Oracle Identity Governance are synonyms and used interchangeably.

2. What are the new features in Oracle Identity Governance 12.2.1.3?

   - Simplified quick installer
   - Simplified install and upgrade experience
   - Improved Access Policies
   - Simplified Application On-Boarding Process
   - Group reviewer for the certifications
   - Custom group reviewer access certification
   - Improved Jet based UI for Test to Production(Deployment Manager)
   - Policy linking for multiple application instance
   - Enhanced REST/SCIM API and Security

3. What's not included in Oracle Identity Governance 12.2.1.3?

   - Oracle Identity Analytics:- Role mining is not part of OIG 12.2.1.3
   - Oracle Privileged Account Manager
   - Full Test To Production migration is not supported in 12c PS3
   - LDAP Synch during fresh installation is not supported.

4. What are the various features which has been deprecated/de-supported features in Oracle Identity Governance 12.2.1.3?

   - OMSS Integration
   - Embedded BI Publisher Reports
   - Post Install configuration UI
   - Remote manager
   - OAACG integration with SOD
   - Diagnostics dashboard.

   For more details, please go through release notes.

5. Where to find more information about Oracle Identity Governance?

   Outbound and inbound collateral for Oracle Identity Governance is available on the internal Oracle IdM Sales Enablement Portal.

   http://my.oracle.com/site/pd/fmw/products/idm/mobile-security/index.html

   Outbound collateral is also available on Oracle Technology Network and Oracle.com/identity.
   http://www.oracle.com/technetwork/middleware/id-mgmt/overview/default-2099033.html

   Download Oracle Identity Governance at
   https://edelivery.oracle.com/

6. What is the current version of Oracle Identity Governance?

   The current version is OIG 12c PS3 (12.2.1.3) in line with other existing Identity management products.

Upgrades, migrations, major releases, minor release and bundle patches

7. How should customers plan for major releases, minor releases (aka patchsets) and bundle patches?

   Oracle recommends customers to plan for major Oracle Identity Governance releases every 12-18 months, minor releases every 6-12 months, and Bundle Patches (BP) every 2-3 months. This strategy allows customers to remain on the latest possible version, thus enabling faster and smoother delivery of bug fixes as well as easier uptake of newer features as they are introduced by Oracle. Additionally, it should be noted that BPs are cumulative of all previous BPs for a particular minor release. Customers are thus strongly recommended to apply the latest BP after upgrading or installing a particular Oracle Identity Governance version.

8. Are OIG interfaces accessibility compliant?

   The OIG 12.2.1.3 consoles are accessibility compliant. For more info, refer to the published VPAT.

9. 12c PS3 can be directly upgraded from which OIM version?

   You can upgrade from 11gR2PS3 to 12c PS3, prior release versions can't be directly upgraded to 12cPS3

10. Is 11gR2PS3 to 12cPS3 upgrade is in-place upgrade?

    Domain upgrade is in-place upgrade, FMW middleware upgrade is out of the place upgrade. Please refer to the upgrade guide.

11. Can 11gR2PS3 LCM installation be directly updated to 12cPS3?

    Yes. There are addition steps. Please refer to the upgrade guide.

12. Can 11gR2PS3 manual installation be directly updated to 12cPS3?

    Yes. Please refer to the upgrade guide.

13. As 12cPS3 won't support embedded BI, what will happen to BI during upgrade process?

    Embedded UI configuration will deactivated and it will remain intact and new BI publisher need to be installed and configured. Please refer to the upgrade guide.

14. IS OMSS supported with 12c OIG?

    No, it's not supported.

15. Do the OIG interfaces support internationalization?

    The end-user (self service) interface supports all 27 languages (English, French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, Traditional Chinese, Arabic, Czech, Danish, Dutch, Finnish, Greek, Hebrew, Hungarian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Swedish, Thai, Turkish) as defined by Fusion Middleware guidelines. However the support is limited to only 10 languages (English, French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, Traditional Chinese) for the System Administration console.

Pricing and packaging

16. What happened to Oracle Identity Analytics?

    With 12c PS3, Oracle Identity Analytics features, excluding Role Mining, have been converted into Oracle Identity Governance. Oracle will not be enhancing or selling Oracle Identity Analytics as a standalone product. Customers who are using Oracle Identity Analytics for Role Lifecycle Management, Identity Certification and Segregation of Duties, should move to 12c PS3. Customers who are using Role Mining, or who have Role Mining needs, can continue to use Oracle Identity Analytics.

17. What is Identity Auditor?

    Identity Auditor is a licensing option in the Oracle Identity Governance Suite. It comprises of the features provided by Oracle Identity Analytics and includes the following components:

    - Role Lifecycle Management

    - Segregation of Duties

    - Role Mining

    - Identity Certification

18. How can customers be licensed for Identity Auditor?

    Customers need to upgrade their Oracle Identity Governance or Oracle Waveset licenses to the Governance Suite.

19. How can customers make use of Identity Auditor features?

    Customers can enable Identity Auditor features by enabling a configuration option.

20. Does OIG include a license for Weblogic application server, BI Publisher, SOA BPEL or Oracle database?

    OIG includes an Application Specific Usage license for Oracle WebLogic Server, BI Publisher and SOA. More details can be found here:

http://download.oracle.com/docs/cd/E14571_01/doc.1111/e14860/im_options.htm#CIHEJCBD

OIG does not include any license for Oracle database.

21. Is the provisioning product modular (i.e. can the individual components such as password management, audit, self-service, workflow, etc. be purchased standalone)?

    Individual components of OIG cannot be purchased standalone. However, given the modular architecture of OIG, customers can choose to implement only a subset of features initially and then gradually expand their deployment to leverage the remaining features.

22. How are connectors sold? Is any connector license included with OIG license?

    Connectors are licensed separately using different licenses. Each license grants access to one or more connector packages. OIG Connector related information found at here.

23. Where can I find the latest price list? Does OIG provide a separate pricing model for internal and external users?

    Refer to the latest Technology Price List available here:

Certifications

24. What Application Servers does Oracle Identity Governance run on?

    Oracle Identity Governance runs only on Oracle WebLogic Server.

25. What platforms does Oracle Identity Governance run on?

    Please refer to the certification matrix.

26. Are all editions of Oracle DBs (Enterprise, Standard, Standard One and Express) certified?

    OIG supports Oracle DB 12.12.1.0.1+, 11.2.0.4+ 12.2.0.1+ Enterprise Edition.

27. What is the supported version of Oracle SOA with OIG?

    12.2.1.3.0.

28. What is the supported version of Weblogic with OIG?

    12.2.1.3.0.

29. Does this product run in a virtualized environment?

    OIG follows the Oracle Fusion Middleware support guidelines available here

    http://www.oracle.com/technetwork/middleware/ias/oracleas-supported-virtualization-089265.html.

30. Which are the certified browsers for the product?

    Currently tested on Internet Explorer, Chrome, and Safari. Please refer to the FMW Certification Matrix.

Security

31. How does OIG secure itself from attacks?

    All Oracle products including Oracle Identity Governance follow Oracle Security Assurance Process that includes the design, development and testing guidelines for SQL injections.

    Oracle has formal secure coding standards and a compliance program that ensures that all development, QA and Product Management staff and other people who need to, are educated about this and attend the training/course. Additionally, Oracle also has formal vulnerability handling policies to deal with any problems discovered. This provides a consistent, cohesive way of analyzing security issues and providing fixes. The details of the Oracle Security Assurance Process are also available at:

    http://www.oracle.com/us/support/assurance/index.html

    Additionally, Oracle Identity Governance provides the following security-related features:

    • Out-of-the-box certification with web access management tools for SSO and protection of Oracle Identity Governance's web UI.

    • Support for multiple encryption algorithms & keys as well as automatic rotation of encryption keys

• Hardened against SQL & XML injection attacks through special character filtering on the user input and API parameters

• Audit data can be stored in Oracle Audit Vault to ensure tamper proofing

• Sensitive data can be protected from unauthorized access through out-of-the-box Oracle DB Vault realms

• Secure from password sniffers as client applications authorize using signature-based login instead of traditional passwords

• Support for mutual authentication and transport encryption in all connectors

• No dependence on anonymous logins

32. What are the various encryption algorithms used by OIG?

• Database encryption (symmetric):

AES (128 bytes)

• Configuration file encryption (symmetric):

AES (128 bytes)

NOTE: Starting OIM 11gR1, there is no config file on stored on the server anymore. All 'password' entries are moved to Credential Store.

• Certificate:

For 12c/11g – RSA (1024 bytes), Signature: SHA1WithRSA

•KSS Support:

File based key store has been replaced with KSS (Key Store Service)

•TLS Support:

Support for various TLS 1.2 Ciphers

Segregation of Duties (SoD)

33. What is meant by Segregation of Duties (SoD) policies?

SoD can be broadly defined as a way of preventing a user from acquiring a set of entitlements that are not in conformance with applicable business policies. This set of entitlements, also referred as "toxic" combination in some literature, could allow a user to potentially perform fraudulent or undesirable activities by circumventing certain commonly established checks and controls. SoD checks thus ensure that a single individual is not given enough authority to perpetrate a fraud on his/her own.

34. What types of SoD policies are typically defined?

SoD policies are typically defined and managed in an IT system known as the SoD engine. The choice of the SoD engine depends on the granularity of access that the policy controls. Enterprise IT and ERP application are two commonly used levels of granularity.

a) Enterprise IT SoD policies are defined by business users based on enterprise roles and access policies. Additionally, these policies can be used to provide SoD capabilities for entitlements in individual IT systems that lack a dedicated SoD engine of their own. Examples of such entitlements include LDAP groups and Database roles. Identity management products are best suited to offer Enterprise IT SoD engines because they already manage the enterprise roles and access policies are needed to define such policies. Oracle Identity Governance 12.2.1.3 provides an Enterprise IT SoD engine that can define policies on the enterprise roles managed in identity management products, both Oracle and non-Oracle.

b) ERP application SoD policies are defined in the context of ERP business applications by the administrators assigned to those applications. Examples of the ERP entitlements used in such policies include Oracle E-Business Suite (EBS) responsibilities and SAP roles. Since these entitlements roll up lower level ERP security contexts such as menu hierarchies, function security & data security, defining these SoD policies require deep knowledge of the security best practices of the ERP. Hence, these policies are documented, managed and remediated in a SoD engine that is dedicated to the business application.

OIG integrates with SAP GRC Risk Analysis and Remediation (RAR) by enabling real-time SoD validation checks. This integration invokes standard web services available in the RAR module (formerly known as Compliance Calibrator) of SAP GRC Access Controls Suite and is certified with SAP GRC Access Controls versions 5.3 or later. Additionally, OIG's SAP provisioning connector is pre-configured to invoke SAP GRC so that SoD violations are detected in the pre-provisioning phase. Customers are also able to configure non-SAP connectors to invoke SAP GRC.

SPML, SCIM and REST Support

35. What is Oracle Identity Governance stance on SPML?

    SPML 2.0 (XSD profile only) support exists only for backward compatibility purpose and will be dropped in a future release of OIG. SPML-DSML is only supported for internal communication between the Active Directory Password Synchronization Agent and Oracle Identity Governance.

36. What identity services does OIG provide?

    Oracle Identity Governance provides REST services using the Simplified Cloud Identity Management (SCIM) protocol. This is the recommended and strategic approach for customers to develop their own applications. REST and SCIM interfaces secured by OWSM JWT Security tokens.

Oracle Identity Governance (OIG) & Oracle Access Management (OAM) integration

37. Is LDAP Synch required?

    LDAP Synchronization (or LDAP Synch) is a capability in Oracle Identity Governance that provides real-time synchronization of users, user passwords and state information between Oracle Identity Governance and a Directory.

38. What are the out-of-the-box integration use cases between OIG 12c and OAM 12c?

    LDAP synchronization is not supported in Oracle Identity Governance 12c (12.2.1.3.0).

    LDAP synchronization works when Oracle Identity Governance is integrated with Oracle Access Management (OAM). But OAM-OIG integration using IDMConfigTool is not supported in this release.

    Workaround: - If you have upgraded from Release 11.1.2.3 to Release 12.2.1.3, then you can continue with LDAP synchronization, as described in Enabling LDAP Synchronization in Oracle Identity Governance in Integration Guide for Oracle Identity Management Suite for Release 11.1.2.3.

Oracle Identity Governance FAQ
(12.2.1.3)

Oracle Corporation
Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
Worldwide Inquiries
Phone: +1.650.506.7000
+1.800.ORACLE1
Fax: +1.650.506.7200
oracle.com

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

Hardware and Software, Engineered to Work Together