Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.5.4000

Part No. E55699-01

July 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E55699-01

Primary Author: David Christie

Contents

Release Notes

Release Notes

Oracle Enterprise Governance, Risk and Compliance (GRC) is a set of components that regulate activity in business-management applications:

- Oracle Application Access Controls Governor (AACG) and Oracle Enterprise Transaction Controls Governor (ETCG) enable users to create models and "continuous controls," and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk. These applications are two in a set known collectively as "Oracle Advanced Controls."
- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk and complying with regulatory requirements.
- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM, AACG, and ETCG.

These GRC components run as modules in a shared platform. AACG and ETCG run as a Continuous Control Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create custom EGRCM modules to address other areas of the company's business. A customer may license only EGRCM, only AACG, or only ETCG; any combination of them; or all of them.

Resolved Issues

Issues resolved by version 8.6.5.4000 include the following:

- Issue 19154094: In an access model, a condition is a filter that excludes objects from analysis. When a model contained two conditions, it returned results for objects that should have been excluded (although when the model contained either condition by itself, results were correctly excluded).
- Issue 19144640: Data synchronization is a process that copies data from a datasource (business application) into GRC for analysis by models and controls. Distinct processes synchronize transaction and access data. Transaction synchronization jobs stopped before completion.
- Issue 19032476: The Manage Controls page loaded slowly. During attempts to scroll through the list of existing controls, the page was slow to fetch data.

- Issue 19005133: While creating an access condition, a user selects an attribute value (an item that the condition will exclude from analysis). A popup window should display values appropriate for the datasource subject to analysis. A custom connector can link GRC to a datasource other than PeopleSoft or Oracle EBS. When a custom connector was in use, the wrong popup window appeared.
- Issue 19001840: Each GRC management or overview page includes a grid that displays summary information about items on which the page focuses. In each grid, a "seeded search" displays the most expansive list of items appropriate for a given user, and the user can create and save custom searches — filtered lists of items. Initially, the seeded search is selected as the default. An error resulted from an attempt to deselect the seeded search so that a saved custom search could be selected as default. A "Set as Default" check box can no longer be deselected for the seeded search. However, if a user selects this check box for a custom search, the setting is ignored for the seeded search.
- Issue 18975925: In the Manage Models page, a custom search set as default for transaction models remained in force when a user opened the page to display access models.
- Issue 18907896: An attempt to run access synchronization generated errors.
- Issue 18632339: In the Manage Results page, an attempt to search for incidents created on a particular date (or dates) failed.
- Issue 18449502: In the Manage Results page, as well as in pages for updating job and duty roles, last-update fields displayed the wrong date.
- Issue 17581106: All AACG pages required excessive time to fetch data.

Known Issues

The following issues are known to exist in version 8.6.5.4000 of GRC, and will be addressed in a future release:

- Issue 19227734: AACG may implement preventive analysis — apply access controls as business-application users are assigned new duties. Depending on the enforcement type specified in a control, it may suspend the assignment of duties to a user pending approval. Suspended assignments are approved or rejected in a Manage Access Approvals page. This page does not observe data-security definitions built into GRC roles; GRC users are able to see duty assignments to which their data rights should not give them access.
- Issue 19154005: Distinct database schemas support GRC and GRCI. The Data Analytics (DA) schema, which supports GRCI, is refreshed regularly by the GRC schema. When CCM incidents are purged in GRC, and the DA schema is subsequently refreshed, the purged incidents continue to appear in GRCI reports.
- Issue 19129954: If a user is assigned a job role that grants read-only access to transaction models, an error occurs when the user attempts to select Continuous Control Management in the GRC Navigator.
- Issue 19072602: When preventive analysis is in force, AACG rejects the assignment of duties that violate a control whose enforcement type is Prevent. If multiple users are assigned Oracle E-Business Suite responsibilities within a

brief time, and any assignment violates a Prevent control, then all are rejected. A workaround is to reassign responsibilities to users for whom the assignment should not violate Prevent controls, but this action has inconsistent results when performed for multiple users.

Documentation

Documentation written expressly for release 8.6.5.4000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E55702-01). Otherwise, documents written for GRC release 8.6.5.1000 (as well as *Release Notes* for 8.6.5.2000 and 8.6.5.3000) apply also to release 8.6.5.4000. Documents include user guides for GRC itself as well as AAGC, ETCG, EGRCM, and GRCI; and implementation guides for GRC security, AACG, ETCG, and EGRCM. These documents are available on Oracle Technology Network at http://www.oracle.com/technetwork.

Installation

You can install GRC 8.6.5.4000 only as an upgrade from version 8.6.5.3000. Be sure to back up your 8.6.5.3000 transaction ETL repository and GRC schema before you upgrade to 8.6.5.4000.

If you use CCM, after you upgrade you must complete the following procedures in the order indicated:

- Perform access synchronization on all datasources used for AACG analysis. (Ordinary synchronization is incremental, collecting data only for records that are new or have been updated since the previous synchronization job.)
- Perform a graph rebuild on all datasources used for ETCG analysis. (A graph rebuild is a comprehensive form of synchronization. Available only to ETCG, it discards existing data and imports all records for all business objects used in all existing ETCG models and controls.)
- Run all controls that compile data for user-defined objects (controls for which the result type is "Dataset").
- Run all models and all controls that generate incidents (controls for which the result type is "Incidents").

Note: You may be upgrading through several releases (for example, from version 8.6.4.7000 to 8.6.5.1000 to 8.6.5.2000 to 8.6.5.3000 to 8.6.5.4000). If so, synchronize access data, rebuild the graph for transaction data, and run controls and models only once, after the final upgrade is complete.

As you install GRC 8.6.5.4000, you will use a file called grc.ear (if you run GRC with WebLogic) or grc.war (if you run GRC with Tomcat Application Server). You will be directed to validate the file by generating a checksum value, and comparing it with a value published in these *Release Notes*.

Your checksum value should match one of the following:

- grc.ear: `0e0777d3f2fa62a51ea6d73e4db2eaff`
- grc.war: `863ba8779bb14a584b63c14d93b3f5ed`

For more information, see the *Enterprise Governance, Risk and Compliance Installation Guide*.