Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.5.6000

Part No. E57664-01

November 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E57664-01

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." These uncover segregation of duties (SOD) conflicts and transaction risk within business applications. AACG and EETCG belong to a set of applications 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.

Access Visualization

AACG offers a visualization feature, which has been upgraded. The following replaces the description of the visualization feature in the current version (for release 8.6.5.1000) of the *Application Access Controls Governor User Guide*.

You can create an image that displays results returned by an access model or incidents generated by access controls. The image traces paths by which people are granted access points the model or controls define as conflicting. (An access point is an object in a business application — such as a role, menu, or function — that enables users to view or manipulate data.)

Each image consists of nodes that form rows. Nodes in the highest row represent users; those at the next level represent roles or responsibilities; those at lower levels represent subordinate access points extending down to those, such as functions, that

directly enable a user to work with data. Arrows connect nodes from one row to the next to define user-to-function access paths.

To create a visualization, select one or more records from the Results window generated by a model, or one or more incidents in the Manage Results page. (Hold down the Shift or Ctrl key to select a continuous or discontinuous set of records.) Then click Actions > Visualize, or click the Visualize button.

Collapse or Expand Nodes

You can simplify a visualization by hiding higher-level nodes, or you can collapse nodes or expand them. To collapse a node is to hide any nodes that descend from it. To expand a node is to restore its hidden descending nodes.

- Select a node, right-click, and then select a Collapse or Expand option.
- Make a selection in the Choose the Simplification Level list box. You can elect to display all nodes, to hide nodes representing users, or to hide nodes representing users and the roles assigned directly to them.

Enlarge or Reduce the Image

You can enlarge or reduce a visualization. If the image is large enough, each node displays the name of the item it represents. If the image is smaller, symbols replace the names. In an Oracle EBS path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function. If the image is smaller still, the nodes are unlabeled.

Use tools located at the upper right of a visualization:

- Plus: Zoom in (enlarge the image). You can also use the mouse wheel to zoom in.
- Minus: Zoom out (reduce the image). You can also use the mouse wheel to zoom out.
- Circle: Click to activate a magnifying glass. When this feature is active, hover over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area beneath the magnifying glass. Click the circle button again to deactivate the magnifying glass.
- Square: Click to center the image and size it so that it is as large as it can be and still fit entirely in its display window. (Nodes that you have collapsed remain collapsed.)

Manipulate the Image

Use these techniques to enhance your view of a visualization, or of nodes or paths within it:

- If nodes are labeled with symbols or are unlabeled, hover over any node to display the name of the user or access point it represents.
- Click the background of the visualization, then drag the entire image in any direction.

- Click any node to highlight it, higher-level nodes that connect to it, and the arrows connecting the nodes. This action highlights nodes from all paths involving the node you select.
- Select a model or control in the Highlight Model/Control list box to highlight the paths that apply to that model or control.
- Select a pair of access points in the Highlight Conflicting Access Points list box to highlight paths that involve those access points. (This list box is active only if you have selected a model or control in the Highlight Model/Control list box.)

Resolved Issues

Issues resolved by version 8.6.5.6000 include the following:

- 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 were purged in GRC, and the DA schema was subsequently refreshed, the purged incidents continued to appear in GRCI reports.
- Issue 19382757: A role was created to combine view-only rights to access controls with the ability to perform control analysis. A user assigned the role could not perform control analysis.
- Issue 19461143: GRC failed to start if worklist, notification, or watchlist data was bad. (A worklist is both a record of a task that is assigned to the user who has logged on to GRC, and a link to the page on which the task can be completed. A notification is a record of a task in which the user has an interest, but on which he need not act. A watchlist is a summary of worklist entries.)
- Issue 19462642: The packaging of a file installed with GRC, jython-2.5.1.jar, has changed. The installation process has changed to reflect the new packaging. The *Installation Guide* for GRC 8.6.5.6000 contains appropriately updated instructions.
- Issue 19481993: A global condition consists of one or more filters that select records to be excluded from analysis by all access models or controls evaluated on a given datasource. A role was created to grant view-only access to global conditions. A user assigned the role had write access.
- Issue 19482462: A Manage Jobs page monitors the completion of requests to run background tasks such as synchronizing data, evaluating models or controls, or importing or exporting data. The Manage Jobs page did not correctly report the status of jobs that failed.
- Issue 19517264:In the Manage Controls page, a search produced a maximum of 25 controls, even when a greater number of controls satisfied search parameters.
- Issue 19519570: In AACG, an entitlement is a configured set of access points. (An AACG model or control defines conflicts among access points, and may use entitlements to do so.) In the Manage Access Entitlements page, an attempt to scroll through a list of access points belonging to one entitlement could result in the display of access points belonging to another entitlement.

- Issue 19525608: An access model or control may contain conditions — filters that select records to be excluded from analysis. In such a filter, or in a global condition, a Within Same Ledger / Set of Books attribute should limit conflicts (as defined by models or controls) to those that occur (depending on configuration) only within or only across individual ledgers or sets of books. If the attribute was set to "No" and an Exclude check box was unchecked, the condition excluded conflicts that it should not have.
- Issue 19564129: If an access model or control uses entitlements to define conflicts, the display of its results includes a column containing entitlement names. Each row states the name of an entitlement that included a conflicting access point. An attempt to filter this column — to list access paths associated with particular entitlements — failed to return valid records.
- Issue 19631666: Access model results were incorrect under the following circumstances:
  - An entitlement included a set of function access points.
  - The model used the entitlement to define conflicts, but included a condition that each conflict must occur within an individual set of books.
  - In a global condition, the Submenu Grant Flag attribute or the Menu Function Grant Flag attribute was set to "No," and the Exclude check box was selected.

  Without the global condition, the model returned correct results. With the global condition, the number of incidents increased and included results not in the set of books specified by the model.
- Issue 19655999: Business applications subject to models and controls may have user-account information that varies from one application to the next. GRC maps each person's business-application IDs to a single global-user ID. The information GRC uses to identify each person uniquely is configurable: e-mail address; e-mail address and user name; or e-mail address, user name, given name, and surname. After a change in global-user setup, controls did not generate incidents that existed before the change.
- Issue 19713845: AACG analysis may be "preventive," meaning that access controls are evaluated at the moment a person is assigned new access. Depending on how a control is configured, it may suspend access pending approval.

  AACG users review suspended assignments in a Manage Access Approvals page. It presents business-application users and the roles provisionally assigned to them. A Preview option should show incidents for each assignment the AACG reviewer approves. If the assignment of two responsibilities resulted in a conflict, and the reviewer rejected one responsibility but approved the other, the Preview option showed a conflict even though it should not have.
- Issue 19768529: When the assignment of a role in Oracle E-Business Suite was subject to AACG preventive analysis, and the assignment was approved in the Manage Access Approvals page, its end date should have been removed in EBS, but was not.
- Issue 19932529: A business object is a set of related data fields from an ERP application. Each GRC model or control may cite one or more business objects to provide data for analysis. A user-defined object (UDO) is a set of data returned

by a continuous control that is used as if it were a business object. Only a transaction model or control can use a UDO.

A control that creates a UDO specifies its results as "Dataset," whereas a control that produces records of transaction risk specifies its results as "Incident." After an upgrade to release 8.6.5.5039, a refresh of the DA schema included Dataset results, but should have included only Incident results.

Known Issues

The following issues are known to exist in version 8.6.5.6000 of GRC, and will be addressed in a future release:

- Issues 19909902 and 19452051: The existence of global conditions causes access requests to be automatically approved even though they involve conflicts uncovered by AACG preventive analysis. The interim workaround is to review control analysis daily for new incidents.
- Issue 19904776: It should be possible to upgrade GRC to a given patch from the previous patch or from the first release in series (for example, upgrade to version 8.6.5.5000 from 8.6.5.4000 or from 8.6.5.1000). Currently, you can upgrade only from the previous patch.
- Issue 19359278: You should be able to use an access visualization to filter conflict records — those displayed in the Results grid (if you are visualizing model results) or in the Manage Results page (if you are visualizing incidents generated by controls). To do so, you would select a set of paths within a visualization, then click an Apply Path Filter field. This filtering feature does not work correctly.

Documentation

Documentation written expressly for release 8.6.5.6000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E57665-01). Otherwise, documents written for GRC release 8.6.5.1000 (as well as *Release Notes* for 8.6.5.2000 through 8.6.5.5000) apply also to release 8.6.5.6000. 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 8.6.5.6000 only as an upgrade from version 8.6.5.5000. Be sure to back up your 8.6.5.5000 transaction ETL repository and GRC schema before you upgrade to 8.6.5.6000.

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 updates GRC with data for records that are new or have been changed 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 through all the 8.6.5 releases to 8.6.5.6000). 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 8.6.5.6000, 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: `ee25e2391157cfd614e699a6f0cdd08b`
- grc.war: `07849f5465a23cd64b3eb8e6e634efba`

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