Oracle® Application Access Controls Governor

User Guide

Release 8.6.3

Part No. E24372-03

January 2012

ORACLE

Oracle Application Access Controls Governor User Guide

Part No. E24372-03

Primary Author: David Christie

Contents

Preface

This Preface introduces the guides and other information sources available to help you more effectively use Oracle Fusion Applications.

Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Publishing other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

The Oracle Fusion Applications information is provided as a solution pack that you can upload to your own deployment of Oracle Enterprise Repository. You can document and govern integration interface assets provided by Oracle with other assets in your environment in a common repository.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww@oracle.com. You can use the Send Feedback to Oracle link in the footer of Oracle Fusion Applications Help.

1

Introduction

Oracle Application Access Controls Governor (AACG) enforces segregation of duties in Oracle E-Business Suite, PeopleSoft, and (if a "connector" is installed) Oracle Fusion.

AACG runs in an Enterprise Governance, Risk and Compliance Controls (EGRCC) platform. So does a second application, Enterprise Transaction Controls Governor (ETCG). The EGRCC platform offers administrative and other functionality shared by AACG and ETCG. Administrative tools connect EGRCC to Oracle, PeopleSoft, and other application datasources, and refresh snapshots of data gathered from those applications; create EGRCC users and user roles; and set EGRCC parameters, connect with your email server (for the purpose of sending notifications to EGRCC users), and integrate EGRCC with other applications. Moreover, the EGRCC platform can display information in any of twelve languages.

These shared administrative and language capabilities are documented in detail in a distinct *Enterprise Governance, Risk and Compliance Controls User Guide*. Features specific to ETCG are documented in an *Enterprise Transaction Controls Governor User Guide*. This *Application Access Controls Governor User Guide* focuses on the SOD features of AACG.

AACG Models and Controls

AACG implements "models" and "controls," which define conflicts among duties that can be assigned in a company's applications and identify users who have conflicting access to those duties. An AACG model returns "temporary" results — a snapshot of risk that is replaced each time the model is evaluated. A control returns "permanent" results — records of violations that remain available to be resolved no matter how often the control is run.

A user creates a model, and may then convert the model into a control; users cannot create controls directly. Thus a model and the control into which it is converted are structurally alike (the principal difference between them being the temporary or permanent nature of the results each generates). Although the creation of a model is a preliminary step in the creation of a control, models may be created to run on their own, so that users such as auditors can assess the risk inherent in a system at a given moment.

An AACG model or control defines conflicts among "access points" in a company's systems. An access point is an object in a business-management application which, when made available to a user, enables him to view or manipulate application data. Access points may be gathered into sets called "entitlements," and a model or control may define conflicts among individual access points, those included in entitlements, or both.

Access points are considered to conflict when, in combination, they would enable individual users to complete transactions that may expose a company to risk. For example, distinct functions in Oracle EBS enable users to initiate a purchase order and to approve payment on that purchase order. In general, individual users should not be able to do both, so a model or control may be created to define the functions as conflicting.

A model, or a control into which the model is converted, consists of "filters." Each selects business-management-application users who have been assigned a specified access point (or who have been assigned any of the access points in a specified entitlement). Within a model, any number of filters may be defined. For a conflict to exist, a user must be selected by a specified combination of those filters; that is, the user must be assigned the access points named in that combination of filters.

Each filter cites a "business object," an "attribute" of that object, and a value for that attribute; these supply access data for analysis. Every AACG model uses an Access Point business object, an Access Entitlement business object, or both. The Access Point business object includes a Name attribute, for which values include the access points available in an application. The Access Entitlement business object also includes a Name attribute, for which values include entitlements configured by AACG users.

In addition, filters may be created to serve as "conditions." These select users or other objects (such as companies in PeopleSoft or operating units in Oracle EBS) that are exempt from the control, or they define circumstances under which the control is enforced. Additional business objects supply values for use in creating conditions.

Records of control violations are known as "incidents." So that incidents may be resolved, each control must name one or more "participants" — EGRCC users who are associated with controls either as individuals or as members of participant groups. At least one participant (either individual or group) is assigned to address incidents generated by the control; other participants observe the decisions made by those who are entitled to act.

Moreover, each AACG control is assigned one of three "enforcement types" — Prevent, Monitor, or Approval Required. The enforcement types determine what actions a participant may take when the control identifies incidents. Distinctions among these types are explained in "Incident Analysis" (page 1-3).

Controls may also employ "tags," each of which is, in effect, a category of values. One can define tags, then define values for them, and then assign tag values to controls. One can then sort displays of controls and the incidents they generate by tag value. (For instance, one might create a Region tag, and then create values for it, such as North, South, East, and West. Individual controls that apply to a particular region would then be given its tag value.)

Incident Analysis

Once controls are defined, EGRCC users may run all or a selection of them, generating incidents. Each AACG incident traces the path through which a user of a business-management application, assigned access points that a control defines as conflicting, can reach one of those access points.

Each incident identifies a "privilege" (an access point actually included in a control) and a "role" (the level of object actually assigned to a user). Depending on how a control is configured, these may be a single object — for example, an Oracle EBS responsibility, if the control sets one responsibility in conflict with another. More commonly, however, they are distinct objects — for example, the role might be an Oracle EBS responsibility, and the privilege might be a function available within that responsibility. In such a case, the incident would identify not only the role and the privilege, but also the objects that lead from one to the other — in the Oracle EBS example, menus and submenus that lead from a responsibility to a function.

AACG can either discover conflicts that existed before controls were written to protect against them ("detective" analysis), or intervene when a user is assigned duties after controls have been written to define them as conflicting ("preventive" analysis). Incidents identified through detective analysis are displayed in a Manage Incidents page. There, users may generate a list of incidents, or a list of controls in which each control links to a list of the incidents it has generated.

Each of these incidents defaults to an Assigned status. This means that the control participant is assigned to address the incidents generated by a control. The participant might:

- Look at the incidents generated by a control, decide that nothing need be done to resolve them, and change status to Accepted.
- Look at the incidents generated by a control, decide that something must be done in the business-management application to resolve them, and change status to Remediate. For an AACG incident, a remedial action might be to rescind a user's role assignment; or, it might involve excluding a privilege from the role through which a user has access to it.
- In this second case, ensure that appropriate action has been taken in the business-management application, and update status from Remediate to Resolved.

Status in the Manage Incidents page does not indicate what a participant has done in the business-management application to resolve incidents, but shows instead that he has or has not done something.

For AACG detective analysis, the enforcement type assigned to the control — Prevent, Monitor, or Approval Required — serves as a guideline for what the participant may do (or recommend doing) in the business-management application. However, he can actually do whatever he determines to be necessary. For example, he may discontinue the access represented by one incident generated by a Prevent control, allow the access represented by another, and so eliminate the conflict while allowing some access. Moreover, a Simulation feature enables AACG users to forecast the impact of incident resolution on the business-management application.

When users are assigned duties after controls have been created to define them as conflicting, AACG may implement preventive analysis. In this case, a control's enforcement type directly determines what happens:

- For a Prevent control, roles are denied to users if they lead to access points the control defines as conflicting. No incidents are generated, and there is nothing for the control participant to do.
- For a Monitor control, roles are granted to users even if they lead to access points the control defines as conflicting. The next time the control is analyzed, the incidents resulting from the role assignments appear in the Manage Incidents page, and their status is Assigned. The control participant may then update status; if so, the detective-analysis rules apply.
- For an Approval Required control, roles assigned to users are suspended until control participants can review the assignments. If the control finds conflicts in Oracle Fusion, the review process is handled by Oracle Identity Management, not EGRCC. If the control finds conflicts in E-Business Suite or PeopleSoft, EGRCC handles the review process: Users, the roles assigned to them, and incidents generated by the control appear in a Manage Access Approvals page. There, a participant may approve or reject each role assigned to each user.

  Regardless of where the conflict exists, when a role is approved and the control is subsequently analyzed, the related incidents appear in the Manage Incidents page, with the status set to Authorized. When a role is rejected, no records of related incidents appear in the Manage Incidents page. In either case, the control participant need do nothing further.

In addition to the Assigned, Accepted, Remediate, Resolved, and Authorized statuses, EGRCC may automatically assign two other statuses to incidents. A Control Inactive status means that an incident is no longer of concern because the control that generated it has been inactivated. A Closed status indicates that because an incident has been resolved in the business-management application, a subsequent evaluation of controls finds that the incident need no longer be addressed.

Reporting

EGRCC users can run reports concerning AACG processing, ETCG processing, and administration. Those that apply to AACG include summary and detail reports about access controls and about the incidents they identify, as well as the approval or rejection of role assignments that are subject to AACG preventive analysis.

All these reports can be run (or be scheduled to run) from EGRCC Reports Management pages. The control and incident reports can also be run "contextually," from the EGRCC pages in which controls are managed and incidents are resolved. Some of these reports may produce either output formatted to be printed or read on-screen, or text files suitable for export to another program, such as a spreadsheet, for further analysis. Others, known as "extract" reports, produce only the latter.

Oracle also provides "report templates," which enable users not only to generate reports about activity in EGRCC, but also to modify the layouts of those reports. Although the templates display information about the use of EGRCC, they run separately, using functionality provided by an instance of Oracle Business Intelligence Publisher (BIP).

Starting Enterprise Governance, Risk and Compliance Controls

To start the Enterprise Governance, Risk and Compliance Controls platform:

1. Open a web browser.
2. In the Address field, type the URL for your instance of EGRCC, and press the Enter key.
3. A Login dialog box appears. Type your user name and password in the appropriate fields.

Navigating in EGRCC

A Tasks panel, located along the left of the EGRCC GUI, presents up to five lists of tasks you can complete in EGRCC. Click on a task from one of these lists, and a workspace to the right of the Tasks panel displays pages in which you can complete the task you've selected. Task lists include the following:

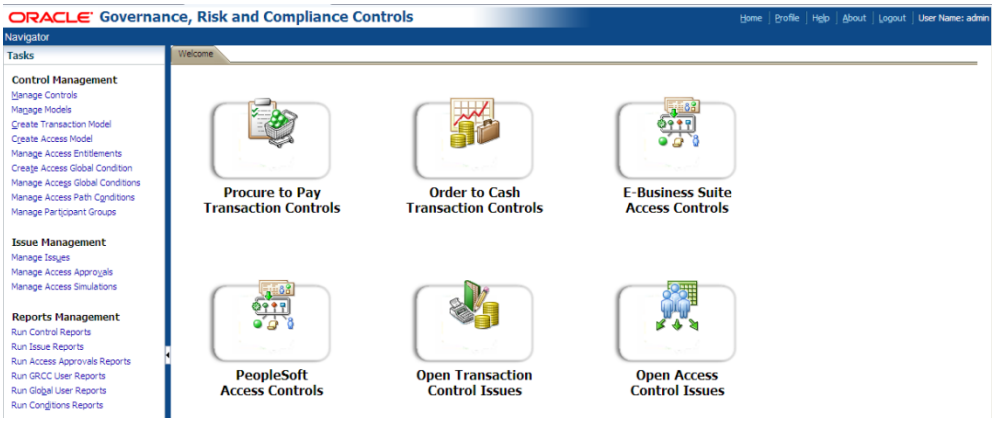
- Control Management tasks open pages in which users can define and manage models, controls, and the objects they use — tags, entitlements, conditions, and participant groups. Here, users can also view the temporary results generated by models.
- Incident Management tasks open pages in which users named as participants to controls can review incidents generated by their controls, and approve or reject roles assigned in E-Business Suite or PeopleSoft, but suspended by AACG preventive processing. Users can also create simulations, which evaluate the effect of proposed resolutions to AACG incidents in business-management applications.
- Reports Management tasks enable users to generate, schedule, or review EGRCC reports.
- Jobs and Scheduling tasks display records of individual requests to synchronize data, evaluate models or controls, export results, generate reports, or complete other background jobs. It also displays schedules on which those jobs are configured to run. A user with proper permissions can modify job schedules.
- Administration Management tasks open pages in which users can define roles, create users and assign roles to them, configure connectivity to business-management-application instances, use data synchronization to transfer data from those instances to EGRCC, upload business objects and patterns, purge

incidents from the system, configure notifications, set EGRCC properties, and integrate EGRCC with other applications.

The tasks available to you are limited by the permissions defined for the EGRCC roles granted to you. If, for example, your role denies you access to administrative features, the entire Administration Management list of tasks would not appear in your tasks panel. Or, if your role focuses on the analysis of access risk, your Control Management list might include tasks relating to the creation of access models, but exclude those relating to transaction models.

Moreover, all the tasks available to you do not appear at once. Initially, the workspace displays a Home page; when it is active, the Tasks panel presents lists of Control Management, Incident Management, and Reports Management tasks (assuming you have rights to these tasks). When any other page is active, the Tasks panel displays only the list of tasks from which that page is opened.

In the illustration below, the workspace displays the EGRCC home page:



To display missing lists of tasks, click on the Navigator (a link above the Tasks panel, in the dark blue band that runs along the top of the application). A pop-up window opens; in it, click on the name for the list of tasks you want the Tasks panel to display. (To restore the Home page, click on the Home link at the upper right of the application.)

You can close the Tasks panel, and so expand the workspace: Click on the button with a left-pointing triangle located at the middle of the border between the Tasks panel and the workspace. The button then changes so that the triangle points to the right; click on it to reopen the Tasks panel.

Synchronizing Data

Models and controls evaluate access granted in datasources (instances of business-management applications). It's assumed that a set of datasources is configured for your GRCC instance. (See the *Governance, Risk and Compliance Controls User Guide*.)

For models and controls to recognize changes made in their datasources, you must synchronize data — run a process that captures changes made since the last time a model or control was run. To complete this process:

1. Select Manage Application Data under Administration Management in the Tasks list.

2. In the Manage Application Data page, select the Datasources tab.
3. Select the row for the datasource with which you want to synchronize data.
4. Do either of the following:
    - Click on Actions > Synchronize Access. Alternatively, click on the Synchronize button in the tool bar, then on a Run Now option, and then on an Access option. This causes data used by AACG to be synchronized once, immediately.
    - Click on Actions > Schedule Synchronize. Alternatively, click on the Synchronize button in the tool bar, then on a Schedule option. A Schedule Parameter dialog opens; in it, you may create a schedule on which any number of synchronization operations run automatically. Select the Access check box to synchronize data used by AACG, and enter values that set the name of the schedule, its start date and time, the regularity with which the synchronization should occur, and an end date (if any). Then click on the Schedule button.

Each data synchronization job is incremental. Rather than reload all ERP data, the synchronization job updates data existing from the last job, editing existing records or adding new records as needed.

Creating Views

In lists — such as the list of controls in the Manage Controls page or a list of incidents in the Manage Incidents page — you can limit the display of entries to those that satisfy filtering criteria, and you can sort the entries. You can also remove columns from display, or restore them; rearrange the order in which columns appear; and resize them. You can then save your selections as a "view," and then either select your view for display or cause it to be displayed by default.

Filtering Data

To filter the values displayed in a list:

1. Determine where to enter filtering criteria. In some lists, you do so in text boxes that appear directly above column headings. Some lists omit these text boxes; in these, you enter filtering criteria in the first row of the list.
2. In any combination of columns in the view row or text boxes, enter (or select) values appropriate to the columns.
3. Click on the View button in the tool bar above the list. The list then contains only entries that match the values you've entered.

For columns that accept values, the percent sign (%) serves as a wild-card character. If it is placed after a string of text or numbers, the view returns all values that begin with the string. If it is placed before a string, the view returns all values that end with the string. If it is placed both before and after a string, the view returns all values in which the string appears at any position. If you omit the wild-card character, the view returns only a value that matches the string exactly.

Sorting Data

To set a sort order for items in a list, click in the heading for one of its columns. Entries in that column are then arranged in alphanumeric order (and entries in other columns are, of course, rearranged so that rows remain intact). Click in the column heading a second time to arrange entries in reverse alphanumeric order.

This sorting method is available in all lists. In some lists, however, a Manage Saved Views feature provides an alternative (and more flexible) sorting method. See "Saving or Deleting a View" (page 1-9).

Removing and Restoring Columns

To remove columns from display, or to restore them:

1. Right click in the header row of the list from which you wish to remove columns, or to which you wish to restore them.
2. In some cases, a menu appears. If so, position the mouse cursor over its Columns option, and a list of available columns appears. In other cases, the parent menu does not appear, and the list of available columns opens directly.
3. To remove a column from view, click on its check box so that its check mark disappears. To restore a column to view, click on its check box so that its check mark reappears.
4. Left click anywhere outside of the menu and list of columns to close them.

This method of exposing or hiding columns is available in all lists. In some lists, however, a Manage Saved Views feature provides an alternative method. See "Saving or Deleting a View" (page 1-9).

Rearranging Columns

To rearrange the order in which columns appear:

1. Position the mouse cursor over a column you want to move, and hold down the left mouse button.
2. A "shadow" instance of the column heading appears. Continue to hold down the left mouse button, and drag that instance to the right or left.
3. Blue arrows appear — one above and one below the header row — to show where the column will be inserted. When they appear at the position you want, release the left mouse button.

This column-ordering method is available in all lists. In some lists, however, a Manage Saved Views feature provides an alternative sorting method. See "Saving or Deleting a View" (page 1-9).

Resizing Columns

To alter the width of columns in lists:

1. In the row that displays column titles, position the mouse cursor over the faint bar that separates one column from another.

2. The cursor changes to look like a pair of parallel vertical lines, each with an arrow extending horizontally from it. When that happens, hold down the left mouse button and drag the column border to the left or right.

Saving or Deleting a View

In some cases, a list displays a Manage View button. If so, then to save a view:

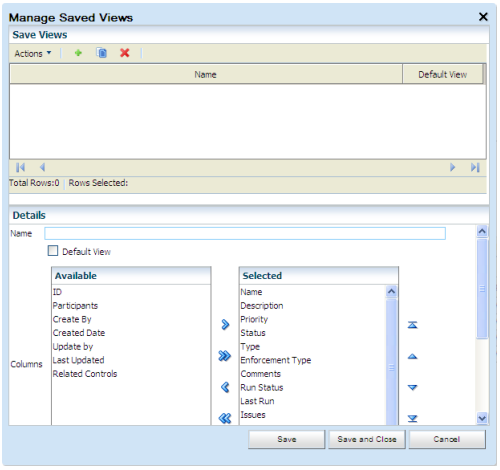
1. Define the view: In a list, set filtering criteria and sort order for data entries, and select, arrange, and resize columns as you wish.
2. Click on the Manage View button. A Manage View dialog opens.
3. Enter values and click on the Save button
   - Create a new name in the "Type new view name" field. The new view criteria are then saved under the new name.
   - Use the "Select view name to override" list box to select an existing view. Its name is retained, but the new criteria replace earlier values. If you choose a value in the "Select view name to override" list box, the "Type a new view name" field becomes inactive, and you cannot enter a value in it.
   - If you want this view to appear each time you open the page in which you are working, select the Set as Default check box. There can be only one default view, so when you select this check box for a view, it overrides any prior selections involving other views.

You can also delete a saved view. To do so, open the Manage View dialog, select the view in the "Select view name to override" field, and click on the Delete button.

In other cases, a list displays a Manage Saved Views button. If so, you can use alternative means to select or order columns for display, to sort rows, and to save a view:

1. In the list itself, set filtering criteria and sort order for data entries, and select, arrange, and resize columns as you wish.
2. Click on the Manage Saved Views button. A Manage Saved Views dialog opens.

   The upper pane — "Save Views" — lists already-configured views. The lower pane — "Details" — shows some of the selections you've already made for your view. For example, if you excluded columns from a list, those columns appear in an Available box; those you have not excluded appear in a Selected box.



3. Optionally, make additional view selections:
    - Expose or hide columns: Click on column titles in the Selected box or Available box, and click on buttons to move them from one box to the other. Those in the Selected box are displayed, and those in the Available box are hidden. The > and >> buttons move column titles to the Selected box, one at a time or all at once; the < and < < buttons move column titles to the Available box, one at a time or all at once
    - Change the order in which columns appear: In the Selected box, click on a column title, and then on an upward pointing triangle to move it up in the Selected box, or a downward pointing triangle to move it down in the Selected box. (A triangle pointing to a horizontal line moves a column title to the very top or bottom of the list.) The uppermost column appears all the way to the left in its list; the second appears second to the left; and so on, until the bottommost appears all the way to the right in its list.
    - Select sort options: In the Sort Options fields, select up to three columns, and select ascending or descending order for each. Entries in the first column are rearranged in the order you specify, with entries in other columns rearranged so that rows remain intact. Where the first column contains duplicate entries, the sort order for the second column takes effect; where the second column contains duplicate entries, the sort order for the third column takes effect.
4. In the Name field of the Details area, type a name for the view.
5. If you want this view to appear each time you open the page in which you are working, select the Default View check box. There can be only one default view, so when you select this check box for a view, it overrides any prior selections involving other views.
6. Click on the Save button (or Save and Close button) to save the view. When you do, a row for the view appears in the Save Views list. In that list, the Default View column contains one check mark in the row for the one view selected as default; all other cells in the column are blank.

To delete a view, click on its row in the Save Views list, and then click on Actions > Delete, or on the red × button. The view disappears from the list. You can copy a view: select its row, and then click on Actions > Duplicate, or on the Duplicate button (which looks like one page overlapping another).

Displaying a View

To cause a list to display entries selected by a saved view:

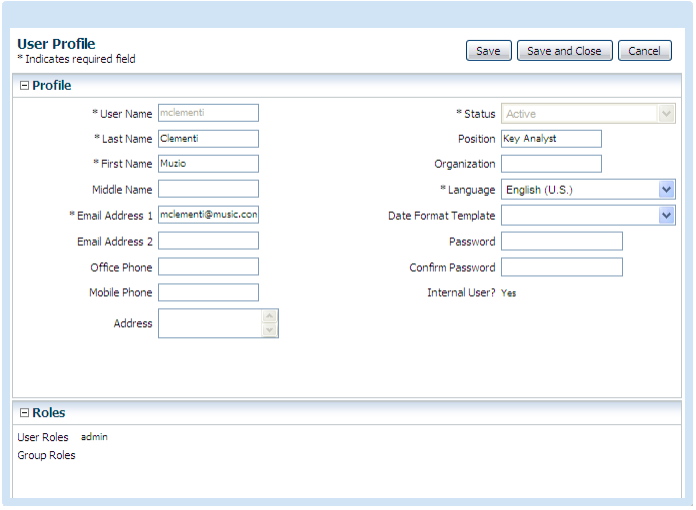
1. Click on the downward-pointing triangle at the right of the View button.
2. A list of saved views appears. Click on the one you want to use.

Finally, to override a selected view (whether saved or defined ad hoc), click on the Clear View button. This causes all entries to disappear from the list; to restore content, either select (or define) another view, or click on the View button to display all possible entries.

Creating a User Profile

From any page in EGRCC, the user who is currently logged on can open a User Profile, review information pertaining to his own user account, and change some of it.

To open the User Profile, click on the Profile link near the upper-right corner of EGRCC (in the dark blue band that runs along the top of the application). A User Profile dialog appears:



In read-only fields, the User Profile displays the username, status, and roles assigned to the user. It also shows whether the user is an "internal user" (created directly in EGRCC or in an external source). These values cannot be changed.

The User Profile dialog includes write-enabled fields for the following information: first, last, and middle names; physical address; email and second email addresses; office and mobile phones; position and organization; and password. The password field is blank for security purposes, but all the others display current values.

To make changes to these fields, type new entries in them. (If you are changing your password, type the new one not only in the Password field, but also in the Confirm Password field.)

The two remaining fields enable you to set a language in which you wish to work:

- In the Language field, select the language. You can choose among languages configured for use in the Manage Application Configurations page.

  EGRCC displays information in the language you choose here. (If you make no selection here, EGRCC uses, in order of preference, a language selected for you when your user account was created, the language selected for your web browser, or US English.)

- In the Date Format Template field, select a date format appropriate for the language in which you wish to work. If you make no selection, EGRCC displays dates in its default format: *mm/dd/yyyy*.

When you finish setting user-profile options, save them: Click on the Save button or the Save and Close button. The former leaves profile values on display for further editing, and the latter closes the User Profile window. Alternatively, click on Cancel to close the window without saving new profile values.

2

Creating and Managing Models

An access model specifies access points (duties) in business-management applications that conflict with one another — that would enable individual users to complete risky transactions. An access model may incorporate conditions (limitations on the model's scope), and users may create global conditions that apply to all models that run in a given business-application instance, or all controls into which those models are converted.

An access model consists of filters, which may serve either of two purposes:

- A filter may specify an access point or an entitlement (a set of access points); if so, it identifies users who have been assigned the specified access point, or any access point in the specified entitlement. A conflict exists when a user is selected by a combination of these filters. Combinations are determined by the way you arrange filters in the model.

  In Oracle E-Business Suite, access points include roles, responsibilities, menus, functions, grants, and concurrent programs. In PeopleSoft, they include roles, permission lists, panel group components, menus, and page definitions.

- A filter may define a condition, which sets limits on the conflicts a model may identify. Typically, a condition specifies users or other items (such as companies in PeopleSoft or operating units in Oracle EBS) that are excluded from analysis by the model, or it specifies a type of item (operating unit, for example) and requires that the model return results only when access points conflict within individual instances of that item type.

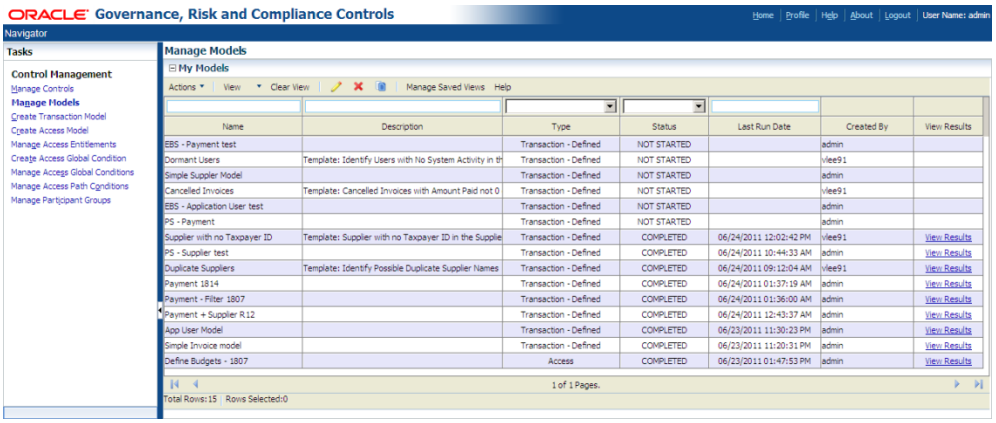
A global condition also uses filters, which are exactly like those that define model-specific conditions in access models.

EGRCC provides pages for creating access models and global conditions, and for managing them once they are created. It also provides capability to create entitlements and another type of condition — a "path condition."

Managing Models

A Manage Models page provides information about transaction and access models created or imported by the user who is currently logged on to EGRCC — for your purposes, you. Although it does not provide immediate access to models created by

other users, you can share models — you can export your models so that other users can import them, or you can import models exported by others.



In the Manage Models page, a "My Models" pane displays a list of existing models, with summary information about them — for each model, its name and description, type and status, the username of the person who created it, and the date when it was last evaluated. All this information is supplied by EGRCC, from data recorded when a model is created, edited, or run; you cannot update these records directly.

The Manage Models page lists both access and transaction models, and the value for model type reflects this. An Access type model specifies conflicts among access points in a company's systems. Transaction—Defined and Transaction—Pattern models are created in Enterprise Transaction Controls Governor.

Model status indicates whether the model has been evaluated and has produced results — records of transactions or access it has found to be risky. Values include Not Started, Started, Completed, and Canceled. In addition, an Error status links to the EGRCC Jobs page, which can provide information about processing errors.

From the Manage Models page, you can also open pages from which models are created or edited, copy or delete models, run models, and review their results. To open the Manage Models page, select Manage Models under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)

Creating, Editing, Copying, or Deleting Models

To create an access model, click on Actions > Create Access Model in the Manage Model page. Or select Create Access Model under Control Management in the Tasks panel. A Create Access Model page opens (see "Creating an Access Model," page 2-4).

To edit an access model, click in the My Models pane on the row for the access model you want to edit. Then click on Actions > Edit. This opens an Edit Access Model page— a replica of a model-creation page, except that it is populated by values for the model you want to edit.

Rather than create a model from scratch, you can copy an existing model, then modify the copy. To do so, select (click on) the model you want to copy. Then select Actions > Duplicate. A new row appears in the My Models pane, identical to the listing for the copied model except that the model name ends in a number in parentheses. (The value of the number depends on how often you copy the original.) Once the copy exists, you can select Actions > Edit to modify the model as you please.

To delete a model, click in the My Models pane on the row for the model you want to delete. Then click on Actions > Delete, and respond to a pop-up message that asks you to confirm the deletion.

Model-Data Synchronization

The Actions menu of the Manage Model page includes a Synchronize option, but this option applies *only* to transaction models. To synchronize data used by access models, do not use this option. Instead, follow the procedure described in "Synchronizing Data" on page 1-6.

Exporting and Importing Models and Templates

You can export models from a source instance to a file, then import them from the file to a destination instance. However, several rules apply:

- A version of "seeded content" (models created by Oracle for use with AACG) is released with each GA release of GRC. (A GA release is defined as one available on Oracle eDelivery.) That version of seeded content can be imported into the GA release or any patch to that release.
- Content exported from an instance of a GA release can be imported into any patch for that release (but not from one patch to another, or one GA release to another).
- Content exported from a GRC instance at any particular version can be imported into another instance at the same version.

You can export models either as models or as templates. A template is a broadly defined model that can serve as the basis for models you create. (Templates may also be provided, in import files, by Oracle.) To export models:

1. In the My Models pane, select models to export. To select one, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold the Ctrl key as you click on models.
2. Click on Actions > Export to export models as models. Click on Actions > Export as Template to export models as templates.
3. An Export Statistics pop-up window appears. Click on its Download button.
4. A pop-up window offers you options to open or save the export file. Click on its Save button and, in a Save As dialog, navigate to a folder in which you want to save the file. The file is saved in .xml format; depending on your choice in step 2, its name begins with the word *Models* or *Templates*, followed by a number.

If you import models, they are available only to you. If you import templates, they are available to all users. To import models or templates:

1. In the My Models pane, click on Actions > Import to import models, or on Actions > Import as Template to import templates.
2. An Import File pop-up window opens. Click on its Browse button.
3. A Choose File dialog opens. In it, navigate to, and select, the file you want to import. If you chose the Import option in step 1, select an .xml file whose name begins with the word *Models*. If you chose the Import as Template option in step 1, select an .xml file whose name begins with the word *Templates*. The

path and name of the file then populate the field next to the Browse button in the Import File window.

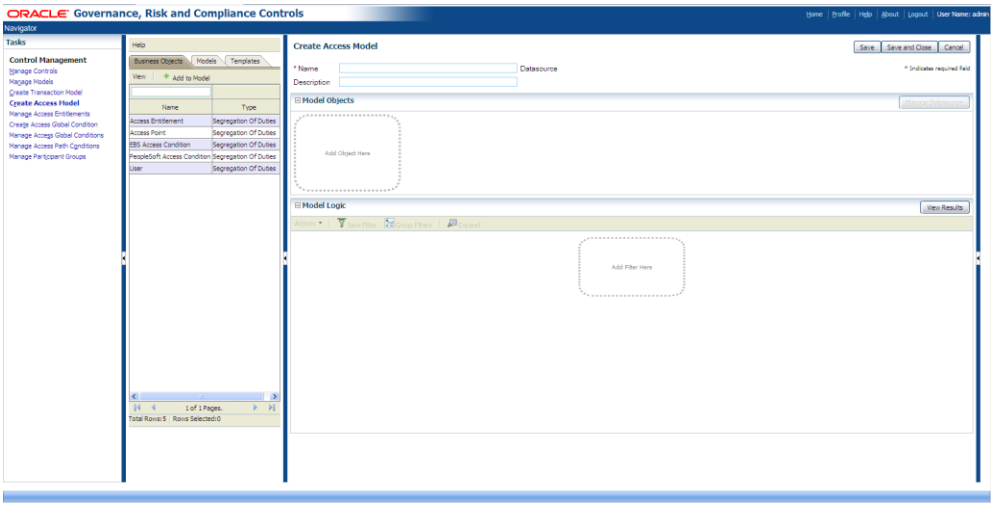
4. Click on the OK button in the Import File window.
5. A Select Items to Import window lists the models or templates contained in the import file. Select those you wish to import, bearing in mind that you can import only those models or templates that use business objects to which your EGRCC roles grant you access. To select one item, click on it. To select a continuous set, click on the first item, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on items.
6. If you are importing models, click the Next button. An Import Datasource Mapping window opens, displaying one row for each datasource specified in the models you've chosen to import. For each, in a Mapped Datasources list box, select a datasource appropriate for the instance in which you are importing the models. (The list box displays datasources configured in the EGRCC Manage Application Data page, to which your EGRCC roles provide you access.)

   If you are importing templates, this step does not apply.
7. Click on the Import button. A pop-up message reports the number of models or templates imported and the status of the import operation. Click on its × button to close it.

Creating an Access Model

To create an access model:

1. Open the Create Access Model page: Click on Actions > Create Access Model in the Manage Model page (see page 2-2). Or, select Create Access Model under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)



2. Name and describe the model (page 2-5).
3. Select business objects (page 2-5) and datasources (page 2-6). These supply the access data the model will evaluate.

4. Create filters. As you create them, arrange their vertical and horizontal alignment to one another, to set the order in which they are to be evaluated (pages 2-7 through 2-12).
5. Save the model (page 2-12).

Naming the Model

Near the top of the Create Access Model page, locate the Name field. Click in it, and type a name for your model. Then click in the Description field immediately below the Name field, and enter a brief explanation of the purpose for the model.

Alongside the Name field, a Datasource field displays the datasources subject to the model you create. Initially, the field may be blank. You can add datasources to the model, or delete datasources (including the default datasource), but you do so elsewhere. EGRCC updates the Datasource field, and you cannot do so directly.

Selecting Business Objects

A business object corresponds to one or more database tables (existing in one or more datasources) that hold information pertinent to user access.

- Add the Access Point business object to your model if you intend to create a filter that specifies an access point (and returns users who have been assigned that access point).
- Add the Access Entitlement business object to your model if you intend to create a filter that specifies an entitlement (and returns users who have been assigned any access point included in that entitlement).
- Select among the remaining three business objects — EBS Access Condition, PeopleSoft Access Condition, and Fusion Access Condition — if you intend to create a condition filter (which defines exemptions from analysis by a model).

To add business objects to a model:

1. In a grid at the left of the Create Access Model page, select (click on) the Business Objects tab, and then on an object in the grid. (Although it's unlabeled, this grid is known as "the Library.")
2. Do either of the following:
    - In the Library, click on the Add to Model button. The selected business object appears in the pane labeled "Model Objects."
    - Use your mouse to drag the business object to the area labeled "Add Object Here" in the Model Objects pane.
3. Repeat this process if you wish to add more objects to the model.

Within the Model Objects pane, each object appears as a window that lists the attributes belonging to the object. In this window, you can view, but not actually select, the attributes. You can, however, do the following:

- Remove a business object from the model: click on its × button.
- Move a business object to the left or right of other objects: Click on the downward-pointing, green triangle. Two options appear; click on either Move Left or Move Right.

- Create custom attributes. (You can do so, however, only after having selected at least one datasource for the business object with which you're working.)

  1. Click on the green + icon. An Add Custom Attribute dialog opens.
  2. In an Attribute Name field, create a name for the new attribute.
  3. In a Base Attribute field, select one of the existing attributes.
  4. In a Modifier field, select a mathematical operator: + (addition), – (subtraction), * (multiplication), or / (division).
  5. In a Value field, enter a value the Modifier will apply to the Base Attribute.
  6. Click on the OK button.

  You can use the custom attribute in filters. Custom attributes appear at the top of the list of attributes displayed by the business object, and each has an edit icon (which looks like a pencil). You can click on a custom attribute to open another dialog box in which you may either edit or delete the custom attribute.

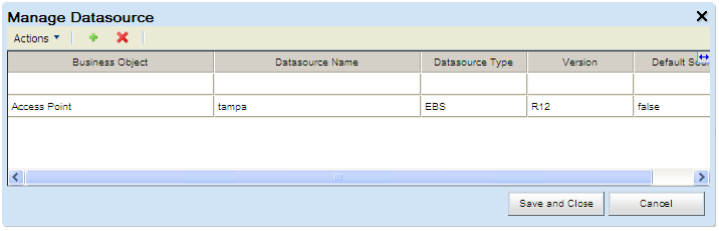
Selecting Datasources

Before a business object can supply access points, entitlements, or other data to a model, it must be associated with at least one datasource. As the model is evaluated, a filter citing that business object will analyze data from the associated datasource.

- Associate the Access Entitlements business object with a datasource called *Grcc* — the EGRCC instance in which you are working, and have configured entitlements for use in models. (The Grcc datasource exists automatically.)
- Associate any of the other four business objects — Access Point, EBS Access Condition, PeopleSoft Access Condition, and Fusion Access Condition — with datasources for instances of business-management applications in which a model is to be run. (These datasources are configured in the EGRCC Manage Data Administration page.)

To associate a business object with a datasource, complete these steps:

1. When you add a business object to the Model Objects pane, a Manage Datasource button becomes active there. Click on it. A Manage Datasource window opens.



2. To add a datasource, create a new row: click on Actions > Create New, or on the green + sign. (You can have multiple rows for each business object.) To change a selection already made for an object, work in its existing row.
3. If you're adding a datasource, click in the Business Object field of a new row and select the business object for which you want to add a source. If you're modifying an existing datasource, locate the row in which the Business Object field displays the name of the object whose source you want to change.

4. Click in the Datasource Name field. From its list of datasources, click on the datasource you want to associate with the business object. Other fields are populated automatically.
5. Click on the Save and Close button. If you've added datasources, their names appear in the Datasource field (alongside the Name field near the top of the Create Access Model page.)

You can also delete the association of a datasource with a business object. While the Manage Datasources window is open, select (click on) the row for the association you want to delete. Click on Actions > Delete or on the red × icon.

Arranging Filters

Each filter you create appears as a dialog box in a Model Logic pane. To define a filter, make selections in the fields displayed by its dialog box. As you add access point or entitlement filters, position each vertically or horizontally with respect to others:

- A vertical arrangement indicates an AND relationship: Filters at one level are evaluated before those at the level below it, the topmost first and the bottommost last. Presuming that processing at any vertical level returns records, processing continues on those records at the next level. For the model to return any results, every vertical level must evaluate to true.

  For example, a model contains two filters, one above the other. The upper filter identifies users assigned one access point, and the lower identifies users assigned a second access point. A conflict exists for each user identified by both filters.

- A horizontal arrangement indicates an OR relationship: If any one filter within a horizontal set returns results, processing moves to the next vertical level.

  For example, two filters alongside one another may be positioned above a third filter. Each filter specifies its own access point. A conflict would exist for each user assigned either of the first two access points, and the third access point.

Condition filters — no matter whether they are placed vertically or horizontally to other filters, or before or after them — always have an OR relationship to one another, and an AND relationship to access point and entitlement filters.

To add filters to a model, click on the New Filter button (or a New Filter option in the Actions menu). As you do, keep these concepts in mind:

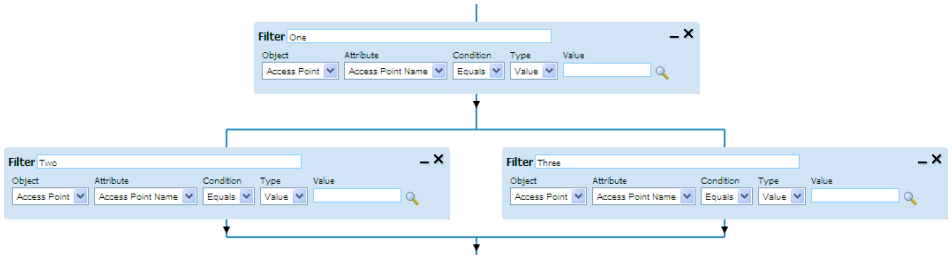
- When you add a filter, it appears by default immediately beneath the lowest filter in your model hierarchy. If, for example, a model contains four vertical levels and you click on the New Filter button, a filter appears at the fifth vertical level.
- Once two or more filters exist in your model, you can select them: hold down the Ctrl key and click in the Filter field of the filters you want to select. When you select a filter, the interior of its dialog box turns a dark shade. (An unselected filter is light blue.) You can select one or multiple filters, but in the latter case, those you select must be adjacent to one another.
- Having selected filters, you can add a new filter specifically in relation to those you've selected. If, for example, your model includes two filters in an AND relationship (stacked vertically), you select the higher one, and you click on the

New Filter button, the new filter appears immediately beneath that higher one; the filter that had been second in the model hierarchy moves to the third level.

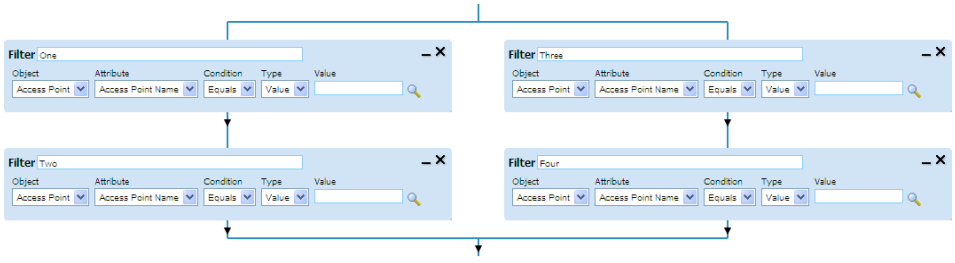
- You can drag and drop existing filters to new positions within the model:
  - To create an OR (horizontal) relationship, click on one filter and drag it to the left or right edge of another.
  - To create or rearrange an AND (vertical) relationship, click on one filter and drag it to the upper edge of another, to place it above. Or drag it to the lower edge of another, to place it below.
  - Alternatively, to move a filter into an AND relationship with other filters, click on it and drag it to an arrowhead at any point in the model hierarchy.

Using these techniques, create structures as complex as you like. For example, an OR statement may contain any number of filters.

Or, a filter may have an AND or OR relationship with blocks of other filters. For example, suppose filters One, Two, and Three are in an AND relationship — stacked vertically. You could drag Two to the left of Three, creating a horizontal pairing between them; One would remain centered above them. If each filter named an access point, the model would identify users assigned access point One and either access point Two or Three.



You could then drag One on top of Two, creating an AND relationship (vertical pairing) between the two of them, with Three in an OR (horizontal) relationship to both. You could then select Three and add a fourth filter, which would appear immediately beneath Three. If each filter named an access point, the model would identify users assigned either access points One and Two, or access points Three and Four.

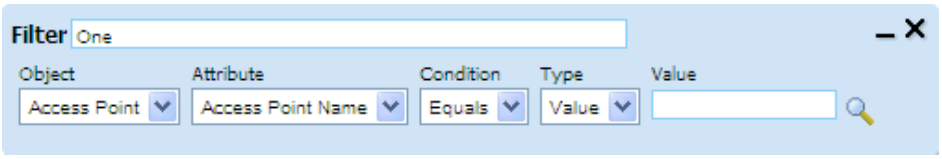


- You can incorporate filters into groups: select those you want to include and click on the Group Filters button (or on Actions > Group Filters). Once you have placed filters in a group, you cannot remove them from the group.

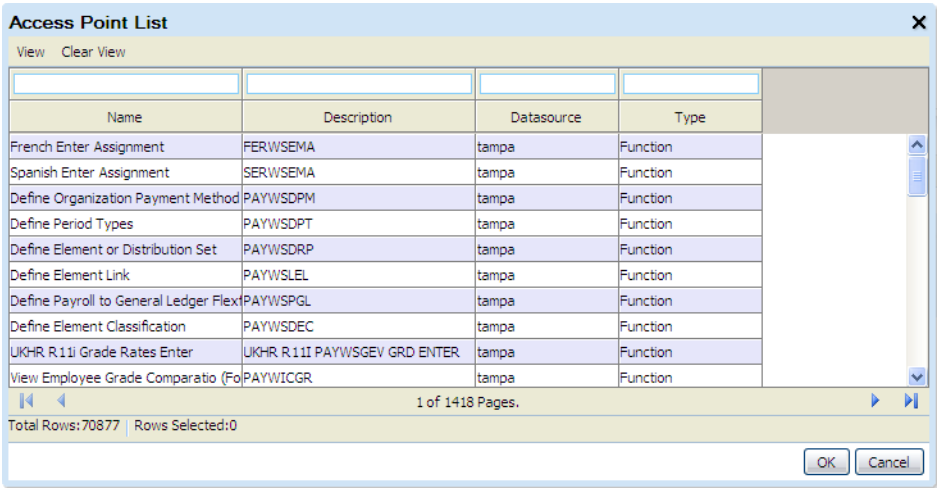
Creating an Access Point or Entitlement Filter

To create an access point filter (one that specifies an access point, and returns users who have been assigned that access point) or an entitlement filter (one that specifies an entitlement, and returns users who have been assigned any access point included in that entitlement):

1. Click on the New Filter button, or on Actions > New Filter. A dialog box appears in the Model Logic pane.



2. Enter a name for the filter in the Filter field.
3. An Object field lists the business objects you've added to the model in the Model Objects pane. Select (click on) Access Point for an access point filter, or Access Entitlement for an entitlement filter.
4. Accept default values in several fields, each of which displays a single value. These include an Attribute field (its value is set to Access Point Name for an access point filter, or Access Entitlement Name for an entitlement filter), a Condition field (Equals in either case), and a Type field (Value in either case).
5. To the right of a Value field, click on an icon that looks like a magnifying glass. A pop-up window opens, in which you will ultimately select an access point (for an access point filter) or an entitlement (for an entitlement filter). The filter will return users who have been assigned the access point you select, or any access point in the entitlement you select.



6. Use filtering tools to search for the access point or entitlement you want to select. Enter complementary values in any combination of the following four fields. In each, you can use the percent sign (%) as a wild-card character to search for a selection of values that contain a text string.
   - Name: Type a text string to search for matching display names of access points or entitlements.

- Description: Type a text string to search for matching internal names of access points, or descriptions configured for entitlements.
- Datasource: Enter a datasource name for a business-application instance whose access points you want to use. For each entitlement, the field displays datasources — potentially multiple — for access points included within the entitlement.
- Type: If you are searching among access points, select a type. Valid values include Function, Responsibility, Role, Menu, Grant, and Concurrent Program in an Oracle EBS context; Permission List, Panel Group Component, Role, and Page Definition in a PeopleSoft context; and Role, Privilege, and Permission in a Fusion context. If you are searching among entitlements, the only valid value is Entitlement.

7. Click on the View button. The Access Point List window then displays access points or entitlements that match your filtering criteria.
8. Click on the access point or entitlement you want to select, and then on the OK button. The pop-up window closes, and your selection populates the Value field of the filter.

Creating a Condition Filter

To create a filter that defines a condition:

1. Click on the New Filter button, or on Actions > New Filter. A dialog box (shown near the top of page 2-9) appears in the Model Logic pane.
2. Enter a name for the filter in the Filter field.
3. An Object field lists the business objects you've added to the model in the Model Objects pane. Select (click on) one from which you want to choose an attribute for use in this filter — EBS Access Condition, PeopleSoft Access Condition, or Fusion Access Condition.
4. In the Attribute field, select an attribute on which you want to base a condition.
   - To create a condition that excludes an item (for example, a set of books) from analysis by the model, select its type as an attribute — for example, Set of Books in the EBS Access Condition business object.
   - To create a condition that requires the model to find conflicts for access points assigned only within instances of an item type, select one of the "Within Same" attributes — for example, the Within Same Set of Books attribute in the EBS Access Condition business object.
5. A Condition field presents a list of operators that may be applied to the attribute you selected, usually to force a comparison between each attribute value and a third (yet-to-be specified) term in the filter. Select one. The following operators are available for attributes that are not dates, although you will see only those appropriate for the attribute you've selected:
   - Equals and Does not equal: The filter returns results if the value of the attribute matches or does not match a specified value. If you selected a "Within Same" attribute in step 4, Equals is the only operator available to you.

- Contains and Does not contain: The filter returns results if the value of the attribute is a text string that includes, or excludes, a specified text string.

In addition to Equals and Does not equal, the following operators are available for date attributes:

- Mathematical operators: The filter returns results if the value of the attribute is less than, less than or equal to, greater than, or greater than or equal to a specified date.
- Between: The filter returns results if the value of the attribute falls between two other specified dates.
- Is blank and Is not blank: The filter returns records for which the attribute column either contains no date, or contains any date.

6. Define the third term of the filter. You have several options, which depend on selections you made in steps 4 and 5.

First, if you selected a "Within Same" attribute in step 4, a Type field defaults to Value. In a Value field, select Yes to find conflicts for access points assigned within, but not across, instances of the item you specified in step 4.

Second, if you selected a date attribute in step 4, the Type field enables you to select a Value option or, for some operators, either Fixed Value or Relative Value. If you select Value or Fixed Value, click on an icon that looks like a calculator, and a pop-up window displays a calendar. In it, select a date; the window closes, and the date appears in a Value field. If you select Relative Value in the Type field, use Value and Units fields to specify a number of days, weeks, or months from the attribute date.

Third, if you selected an attribute in step 4 that is neither a date nor one of the "Within Same" attributes, you may select Value in the Type field. If you do:

a Click on an icon that looks like a magnifying glass. An Attribute Values List pop-up window opens. It lists values that correspond to the attribute you selected in step 4 — for example, sets of books if you selected the Set of Books attribute from the EBS Access Condition business object.

b Use filtering tools to search for a value you want to select — for example, a specific set of books if you want to exclude it from analysis by the model. Enter complementary values in any combination of the following three fields. In each, you can use the percent sign (%) as a wild-card character to search for a selection of values that contain a text string.

- Name: Type a text string to search for matching internal names.
- Display Name: Type a text string to search for matching display names.
- Datasource: Enter a datasource name for a business-management-application instance whose data you want to use.

c Once you have entered filtering values, click on the View button. The Attribute Values List window then displays values that match your filtering criteria.

d Click on the value you want to select, and then on the OK button. The Attribute Values List window closes, and your selection populates the Value field of the filter.

Fourth, if you selected an attribute other than a "Within Same" attribute in step 4, you may select Object in the Type field. If so, new Object and Attribute fields appear. In them, select a business object and an attribute within it, whose values are compared with those of the attribute in the first term of this filter.

7. If appropriate, click on the + toggle next to an Advanced Options label, then select the Exclude advanced option. This removes records defined by the filter from analysis; in effect the filter returns all records that do not meet its specifications.

   For example, if you selected the Set of Books option from the EBS Access Condition business object in step 4, Equals in step 5, and the name of a specific set of books in step 6, selecting Exclude here would remove that set of books from analysis by the model. (Creating the same filter but clearing the Exclude check box would eliminate all sets of books other than the specified one from analysis.)

   There may be more than one way to configure a given condition. For example, to exclude a set of books called "SOB1," you might create a filter in which the Set of Books attribute from the EBS Access Condition business object equals SOB1, and then select the Exclude advanced option. But this would effectively be the same as choosing the Set of Books attribute from the EBS Access Condition object, Does not equal, and SOB1, and clearing the Exclude advanced option.

Notes on the **EBS Access Condition business object**: Attributes of this business object that point to EBS security profiles can detect only profiles configured at the responsibility level. Also, beginning with release 8.6.3.5000, attributes are added or modified to enable users to create conditions for multi-org access control (MOAC) profiles in EBS R12. Among them, "Operating Unit" and "Within Same Operating Unit" are existing attributes that are extended to consider operating units within a MOAC security profile. However, this extension applies only to operating units selected as "Include" on the Organization Security tab of the Global Security Profile.

Saving the Model

To save the model, click on the Save button or the Save and Close button. Both buttons are located near the upper right corner of the Create Access Model page. The Save option saves the model, but leaves its values on display for potential further editing, or for the generation of results. The Save and Close option saves the model but empties the Create Access Model page so that it is ready for the creation of a new model. Alternatively, you can click the Cancel button and respond to a confirmation prompt to restore the blank Create Access Model page without saving the model.

Managing and Creating Global Conditions

A global condition sets limits on the conflicts identified by all access models or controls evaluated on a given datasource. Like a condition written for a specific model, a global condition typically specifies users or other items (such as companies in PeopleSoft or operating units in Oracle EBS) that are excluded from analysis by a model or control, or it specifies a type of item (operating unit, for example) and

requires the model or control to return results only when access points conflict within individual instances of that item type.

A Manage Access Global Conditions page lists these global conditions, displaying summary information about them. For each condition, it presents the name and description, status (Active or Inactive), and the datasource to which it applies. To open this page, select Manage Access Global Conditions under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.) The values it displays are updated by EGRCC, from information recorded when a condition is created or edited; you cannot update them directly.

Creating Global Conditions

The process of creating a global condition is essentially like creating an access model that contains only condition filters. As you create filters for a global condition, however, EGRCC places them horizontally to one another, indicating an OR relationship — the condition produces results if any combination of its filters evaluates to true. You cannot arrange condition filters to create AND relationships. Moreover, each global condition applies to a single datasource. To create a global condition:

1. Click on Actions > Create New in the Manage Access Global Conditions page. Alternatively, click on Create Access Global Condition under Control Management in the Tasks panel. Either action opens a Create Access Global Condition page.
2. Near the top of the Create Access Global Condition page, locate the Name field. Click in it, and type a name for your global condition. Then click in the Description field immediately below the Name field, and enter a brief explanation of its purpose. Finally, in the Status field, select a status for the condition — typically Active. (You cannot delete a global condition; you can only inactivate it.)
3. Select the EBS Access Condition, PeopleSoft Access Condition, or Fusion Access Condition business object, depending on whether you want the global condition to apply to an Oracle EBS, PeopleSoft, or Fusion instance.

   The procedure for doing so is the same as for models (see "Selecting Business Objects" on page 2-5), except that (here and in following steps) labels in the Create Access Global Condition page apply to conditions. (Here, for example, an Add to Condition button replaces the Add to Model button, and a Condition Objects pane replaces the Model Objects pane.)
4. Select a datasource to which the condition will apply. The procedure for doing so is the same as for models (see "Selecting Datasources" on page 2-6), except that you can select only one datasource for the global condition.
5. Create one or more filters. The procedure for doing so is the same as the one for creating condition filters for an access model (see "Creating a Condition Filter" on page 2-10).
6. Save the global condition: Click on the Save button or the Save and Close button. Both buttons are located near the upper right corner of the Create Access Global Condition page. The Save option saves the condition, but leaves its values on display for potential further editing. The Save and Close option saves the condition but empties the Create Access Global Condition page so that it is ready for

the creation of a new condition. Alternatively, you can click the Cancel button and respond to a confirmation prompt to restore the blank Create Access Global Condition page without saving the model.

Editing or Copying Global Conditions

To edit a global condition, click in the Manage Global Access Conditions page on the row for the condition you want to edit. Then click on Actions > Edit. This opens an Edit Access Global Condition page — a replica of a condition-creation page, except that it is populated by values for the condition you want to edit. Modify values as described in "Creating Global Conditions" (page 2-13).

Rather than create a condition from scratch, you can copy an existing condition, then modify the copy. To do so, click in the Manage Global Access Conditions page on the row for the condition you want to copy. Then select Actions > Duplicate. A new row appears in the Manage Global Access Conditions page; it's identical to the listing for the copied condition except that the condition name ends in a number in parentheses. (The value of the number depends on how often you copy the original.) Once the copy exists, you can select Actions > Edit to modify the condition as you please.

Exporting and Importing Global Conditions

You can export global conditions from a source instance to a file, then import them from the file to a destination instance. However, global conditions are subject to the same import rules as those that apply to models (see page 2-3).

To export global conditions from a source instance to a file:

1. In the Manage Global Access Conditions page, select conditions to export. To select one, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold the Ctrl key as you click on conditions.
2. Click on Actions > Export.
3. An Export Statistics pop-up window appears. Click on its Download button.
4. A pop-up window offers you options to open or save the export file. Typically, click on its Save button and, in a Save As dialog, use standard techniques to navigate to a folder in which you want to save the file. The file is saved in .xml format.

To import global conditions from a source file to a destination instance.

1. In the Manage Global Access Conditions page, click on Actions > Import.
2. An Import File pop-up window opens. Click on its Browse button.
3. A Choose File dialog opens. In it, use standard techniques to navigate to, and select, the file you want to import. The path and name of the file then populate the field next to the Browse button in the Import File window.
4. Click on the OK button in the Import File window.
5. A Select Items to Import window lists the conditions contained in the import file. Select those you wish to import: To select one item, click on it. To select a

continuous set, click on the first item, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on items.

6. Click on the Next button. An Import Datasource Mapping window opens, displaying one row for each datasource specified in the conditions you've chosen to import. For each, in a Mapped Datasources list box, select a datasource appropriate for the environment into which you are importing the conditions. (The list box displays datasources configured in the EGRCC Manage Application Data page.
7. Click on the Import button. A pop-up message reports the number of models or templates imported and the status of the import operation. Click on its × button to close it.
8. Confirm the import: The conditions you have imported should be listed in the Global Access Condition pane of the Manage Access Global Conditions page.

Creating Models or Global Conditions from Templates

Rather than create a model from scratch, you may use an existing model or a template as a starting point, editing it to create a new model. A template is a "starter" model uploaded to EGRCC through the import feature of the Manage Model page (see page 2-3). Although a model is available only to the user who has created or imported it, a template is generally available. For you to use a template, however, your EGRCC role must give you access to all the business objects selected for it.

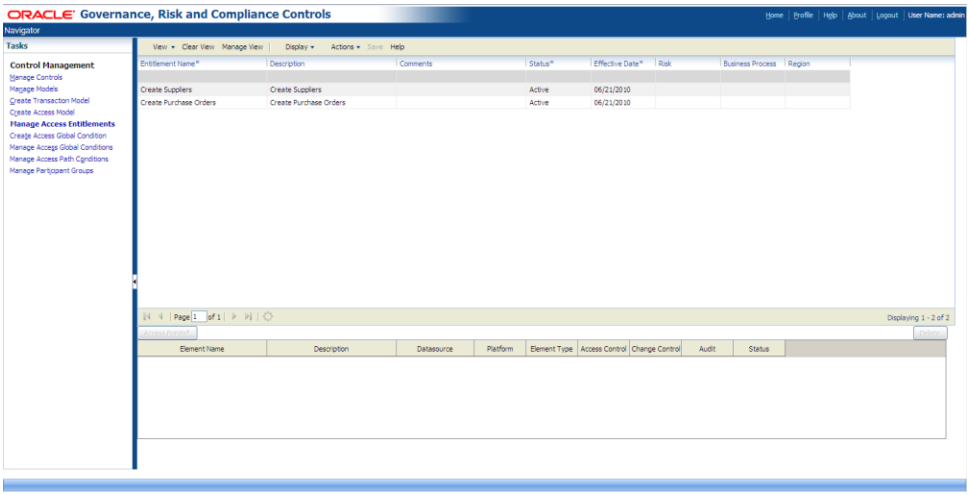
1. Open the Create Access Model page (see page 2-4).
2. In the Library pane at the left of the page, click on the Models tab or Templates tab, depending on the type of object you want to use in creating a new model.
3. The Library displays instances of the object you've selected. (As you create or import models, they populate a grid available in the Models tab. The Templates grid is populated when you import templates.) Click on the model or template you want to use.
4. Click on the Open button. The model or template values populate the Name, Model Objects, Model Logic, and Result Display panes. Using procedures described in "Creating an Access Model" (page 2-4), rename the model, and then edit, add to, or delete from the source model or template values. Save the new model.

Similarly, rather than create a global condition from scratch, you may use an existing global condition as a starting point, editing it to create a new global condition.

1. Open the Create Access Global Condition page (see page 2-13).
2. In the Library pane at the left of the page, click on the Conditions tab.
3. The Library displays previously configured global conditions. Click on the one you want to use.
4. Click on the Open button. The condition values populate the Name, Condition Objects, and Condition Logic panes. Using procedures described in "Creating Global Conditions" (page 2-13), rename the condition, and then edit, add to, or delete from the condition values. Save the new condition.

Managing and Creating Entitlements

You can collect access points into entitlements. You can then create access models that define conflicts by using entitlements in place of, or in addition to, access points. Each access-model filter that specifies an entitlement returns users who have been assigned any access point included in the entitlement. To work with entitlements, select Manage Access Entitlements under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)



Creating an Entitlement

To create an entitlement:

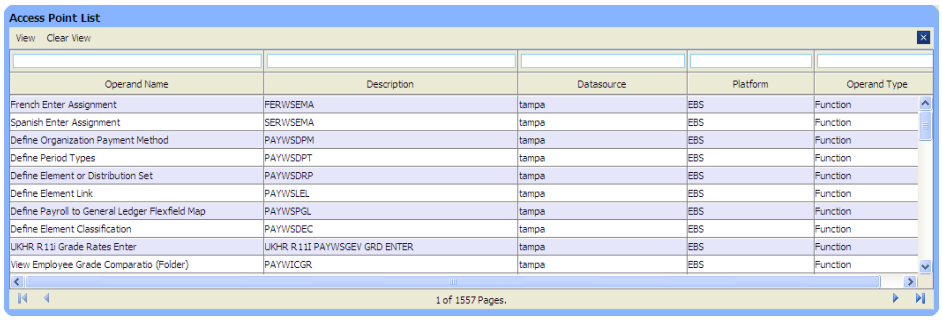
1. In the Manage Access Entitlements page, click on Actions > Add. A new row appears in the grid, second from the top.
2. Insert the following values in the new row. To do so, double-click in each field, or press the Tab key to move from an active field to the next field.
   - Entitlement Name: Type a name for the new entitlement.
   - Description: Explain briefly the organizing principle or business purpose of the entitlement.
   - Comments: Record additional statements about any aspect of the entitlement, for example whether a given access point is covered by a compensating control.
   - Status: Select Active or Inactive. (An Inactive entitlement cannot be selected for use in an access model or control.)
   - Effective Date: Select a date on which AACG can begin to use the entitlement. (Its status must also be set to Active.) Either accept the default value — the current date — or double-click in the Effective Date column, and then click on the grid-like icon it presents. A pop-up calendar appears. In it, click on the left- or right-pointing symbol surrounding the month and year to display an earlier or later month. Or, click on the downward-pointing symbol to produce a list of months in the current year, and click on the one you want. Then, in the calendar, click on the date you want. Alternatively, click on the Today button to select the current date.

- Tags: If you have configured tags (see page 2-19), additional columns appear in the grid, one for each tag. To assign tag values to the entitlement you are creating, activate the field for a given tag and, in it, select one or more values.

Adding Access Points to an Entitlement

To add access points to an entitlement:

1. In the upper grid, select the row for the entitlement to which you want to add access points. (If you are creating a new entitlement, the row is necessarily already selected. If you are editing an existing entitlement, double-click on the row.)
2. Ensure that Display > Entitlement Details is selected. This is the default.
3. Click on the Access Points button in the bottom portion of the Manage Access Entitlements page. A pop-up window, titled Access Point List, appears.



4. Generate a list of access points from which you can select as you build your entitlement. Use filtering tools to search for the access points you want to select. You can use the percent sign as a wild-card character, and you can enter complementary filtering values in any combination of the following fields:
   - Operand Name: Type a text string to search for matching display names of access points.
   - Description: Type a text string to search for matching internal names of access points.
   - Datasource: Enter a datasource name for a business-application instance whose access points you want to use. An access point is specific to the instance in which it runs. If, for example, an organization runs two Oracle EBS instances, each function, responsibility, or other access point would be available for selection twice, once for each instance. Use this filter to ensure your entitlement contains access points selected from the instance you want.
   - Platform: Enter a business-management-application type — such as Oracle or PeopleSoft — whose access points you want to use. (These values are set during data-source configuration.)
   - Operand Type: Select a type of access point for which you wish to search. Valid values include Function, Responsibility, Menus, and Concurrent Programs (in an Oracle context); Permission List, Panel Group Component, and Page Definition (in a PeopleSoft context); and Role (in either context).
5. Once you have entered filtering values, click on the View button. The search window then displays access points that match your filtering criteria.

6. Select access points to add to the entitlement, and drag them into the Entitlement Details area of the Manage Access Entitlements page. To select a single access point, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on access points.

7. If you need to select additional access points that were excluded by your original filtering criteria, click on the Clear View button in the search window, enter new filtering criteria, and drag additional items into the Entitlement Details area of the Manage Access Entitlements page. When you finish selecting access points, close the search window by clicking on the × symbol in its upper right corner. The Entitlement Details area now lists the access points you selected.

8. For each access point, confirm that the status column reads "Active." (This should be the default.) If you wish to inactivate any access point, double-click in its cell in the Status column; this activates a list box, in it, select Inactive. Typically, however, you want the access points you've selected to be active, and so would leave the Status settings as they are.

   The Change Control and Audit check boxes are reserved for future development, and have no meaning. The Access Control check box is selected because the access point is available for use in access controls. Other columns display values as described in step 4, with "Element Name" corresponding to "Operand Name" and "Element Type" corresponding to "Operand Type."

9. When you are done, click Actions > Save button . A message indicates that the entitlement has been saved; click on its OK button to clear it.

Editing an Entitlement

You can edit an existing entitlement, essentially by selecting its row in the upper grid of the Manage Access Entitlements page and following the processes described in "Creating an Entitlement" (page 2-16) and "Adding Access Points to an Entitlement" (page 2-17). You can alter any aspect of the entitlement — not only the values set in the fields of the upper grid, but also the selection of access points. Add access points as you would to a new entitlement. To remove an access point, you have two options:

- Inactivate it: Click on its cell in the Status column in the bottom portion of the Entitlements page. In the list, select the Inactive value.
- Delete it: In the bottom portion of the Entitlements page, click on the row for the access point, and then click on the Delete button

Use caution — if you edit an entitlement after it has been selected for use in a model or control, you necessarily alter the meaning of that model or control, potentially to the point at which it no longer defines meaningful conflicts.

When you finish making changes to the entitlement, click on Actions > Save to save your changes. If you are editing an entitlement that is used by access models or controls, a warning message appears, identifying the objects that use it:

- If you want to proceed with your edit, click on the Save button in the warning message.

- If you determine that saving your edit would improperly distort a model or control, click on the Cancel button in the warning message. (In that case, the entitlement reappears in its original form when you refresh your screen.)

Copying an Entitlement

You can copy an entitlement as a template for the creation of a new entitlement:

1. In the upper grid of the Manage Access Entitlements page, click on the row for the entitlement you want to copy.
2. Click on Actions > Copy.

The new entitlement is named "Copy(*n*) of *Name*," in which *n* is a number (1 for the first copy, 2 for the second, and so on) and *Name* is the name of the original entitlement. The copy is identical to the original, but inactive. (That is, the status field for the entitlement as a whole, located in the upper grid, is set to Inactive. The status for each member of the copied entitlement is set in the same way as it was in the original.)

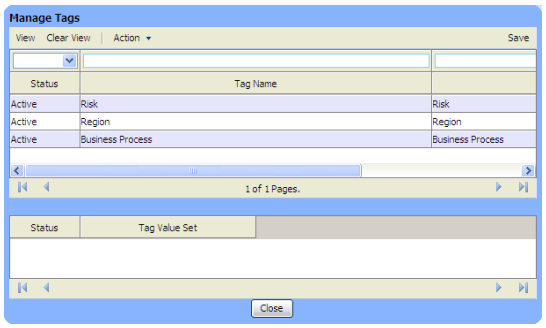
After you make the copy:

- Use the procedures described in "Editing an Entitlement" (page 2-18) to modify its selection of access points as desired.
- Give the copy a new name that reflects the alterations you've made to it.
- When you are ready to use the entitlement, change its status to Active.
- Click the Save button to save your changes.

Creating Tags

You can assign tag values to entitlements as a means of categorizing them, and as a device for filtering their display. (Typically, you would coordinate these tag values with those you assign to controls.) To create tags:

1. In the Manage Access Entitlements page, click on Actions > Manage Tags.
2. A Manage Tags pop-up window opens. In its tool bar, click on Action > Add Tag. A blank row appears in its upper grid.



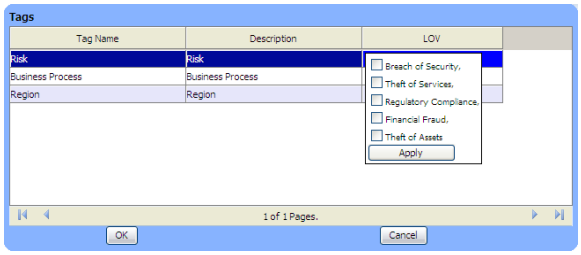
3. Click in the Status field. This activates a list box; in it, select Active or Inactive.
4. Click in each of the Tag Name and Description columns, and enter a name and description for the tag.
5. Select Action > Add Tag Value. A blank row appears in the lower area of the Manage Tags window.

6. Click in the Tag Value Set column of that row and enter a value for the tag.
7. Click in the Status column of that row and select Active or Inactive.
8. Repeat steps 5–7 any number of times to create as many values as you wish for the tag.
9. Click on the Save button (an then click on the Close button to close the Manage Tags window). A column for the tag you have created appears in the Manage Access Entitlements page when you navigate away from, and back to, it.

Assigning Tag Values to Entitlements

You can assign tag values to entitlements as you create or edit them. (See step 2 in "Creating an Entitlement" on page 2-16). Otherwise:

1. In the Manage Access Entitlements page, select any number of rows to assign a set of tag values to the entitlements identified by those rows. (Click on a row to select it. To select a continuous set of rows, click on the first one, hold down the Shift key, and click on the last one. To select a discontinuous set of rows, hold down the Ctrl key as you click on the rows.)
2. Click on Actions > Assign Tag. The Tags pop-up window opens.



3. Locate the row for the tag whose values you want to assign. Click in its LOV column. A set of check boxes appears, one for each value configured for the tag.
4. Click in the check boxes for the values you want to assign (you can select more than one), and then on the Apply button. The list of check boxes disappears, and your selections appear in the LOV column.
5. Click on the OK button; the Tags window closes. The Entitlement page refreshes, and the values you selected appear in the column for the tag, in the rows for the entitlements you selected in step 1.

Viewing Change History

To review a history of changes made to entitlements:

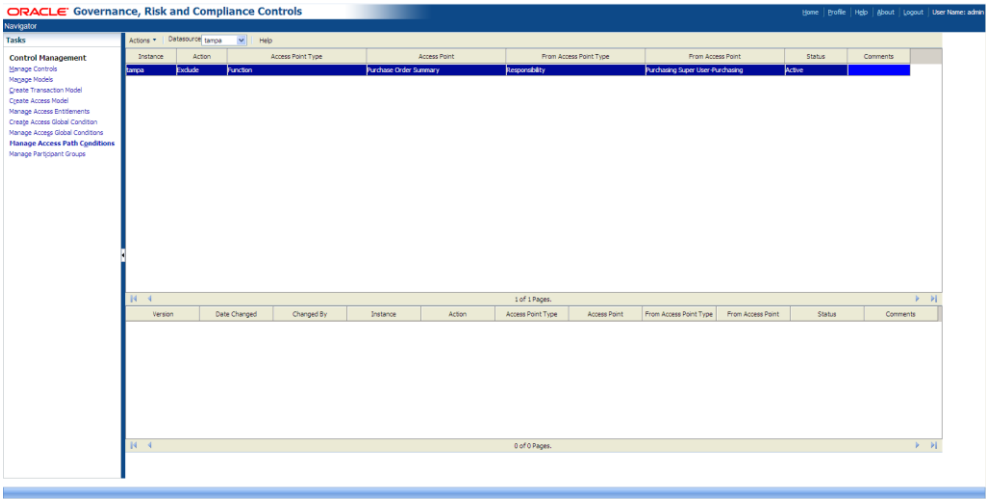
1. In the Manage Access Entitlements page, select (click on) an entitlement whose change history you want to view.
2. Click on Display > Change History. The lower area of the Entitlements page displays one row for each version of the entitlement, up to (but not including) the current version.
3. Double-click on a row for any version to open a pop-up window that displays its access points.

Using Path Conditions

A path condition excludes one access point from another, such as an Oracle function from a menu or a responsibility. A path including those points would be excluded from incident generation. For example, an access control might set functions f1 and f2 in conflict. If a path condition excludes f1 from responsibility r1, and a user has access to both functions, then no incident would be generated if the user's access to f1 comes from r1.

To create a path condition:

1. Select Manage Access Path Conditions under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)



2. In the Datasource list box at the upper left of the Manage Access Path Conditions page, click on the datasource for which you want to configure path conditions.
3. Click on Actions > Add. A new row appears in the top section of the page. Its Instance field is set automatically to the datasource you selected in step 1, and the Action field to Exclude. These cannot be changed.
4. Double-click on each of the remaining fields. In each, a pop-up window presents a list; in it, select an appropriate value:
   - In the Access Point Type field, choose the type of access point you want to exclude from another.
   - In the Access Point field, select the specific access point to be excluded.
   - In the From Access Point Type field, select the type of access point from which you want to exclude the one you've already selected.
   - In the From Access Point field, select the specific access point from which the first is to be excluded.
   - In the Status field, accept the default value, Active, to use the condition, or select Inactive to hold it in reserve.
   - In the Comments field, optionally enter a brief description of the purpose of the condition.
5. Click on Actions > Save.

6. Repeat these steps to create as many additional conditions as you wish.

To edit a path condition, select its row in the upper portion of the Manage Access Path Conditions page, and then select Actions > Edit. Select new values and then select Actions > Save.

To view the history of changes to path conditions, click on the row for a condition in the upper portion of the page. Change history appears in the lower portion — one row displaying the settings for each version of the condition up to, but not including, the current version.

Viewing or Exporting Model Results

Once a model has been saved, you can view its results from the Manage Models page, the Create Access Model page, or the Edit Access Model page. You can view results from the most recent run of the model (if it has been run before), or run the model and view a new set of results.

Before running a model, consider synchronizing data from the datasource against which the model will run; this would ensure that access data is up to date. See "Synchronizing Data" on page 1-6.

No matter which page you use to display model results, a Results pop-up window presents a grid. Each row in the grid documents a path through which a user of a business application, assigned access points that a model defines as conflicting, can reach one of those access points. The row also displays related information, such as the user's identity and the datasource on which the conflict exists.

To display results from either the Create or Edit Access Model page, click on a View Results button, located in the title bar of the Model Logic pane.

From the Manage Models page, do either of the following:

- The My Models pane of the Manage Models page includes a column labeled "View Results." In it, the entry for each model contains a prompt (which also reads "View Results") if the model has been run. (If not, the View Results cell is blank.) Click on the prompt (if one appears) for the model whose results you want to view.
- In the My Models pane, click on the row for the model whose results you want to view. Then, in the menu bar, select Actions > View Results.

Then, in any of the pages, respond to prompts:

- If the model has not been evaluated previously, a dialog box prompts you to choose between Run and Run in Background options. If you select Run, the page remains open, and displays run status at its foot. If you select Run in Background, the model runs, but you may navigate to another EGRCC page and work there. (A Cancel option also exists.)
- If the model has been evaluated previously, a dialog box prompts you to decide whether to overwrite existing results. Select No to display the existing results. Select Yes to generate and display a new set of results. In this case, the dialog box prompting you to run the model directly or in the background appears; make a selection there. When you generate a new run, the earlier set of results is lost.

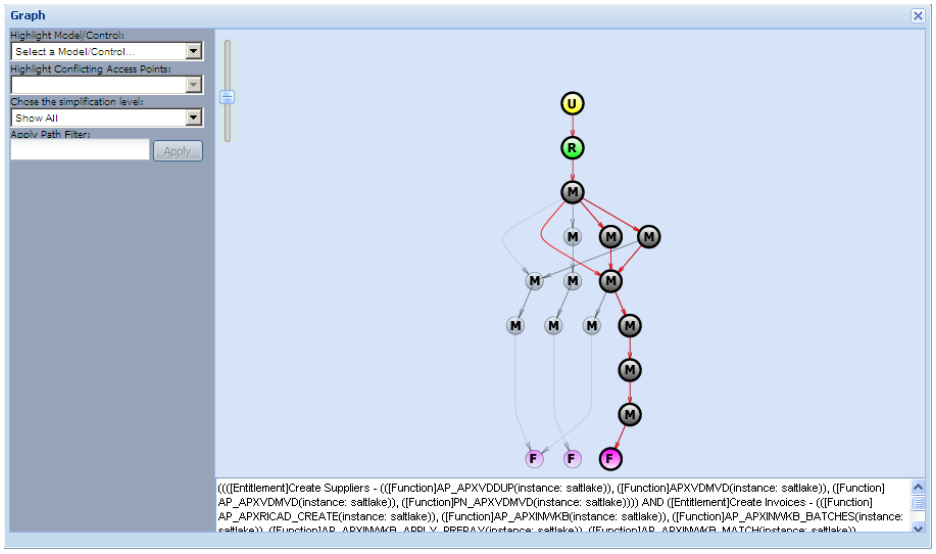
You can export model results to an Excel spreadsheet. To do so:

1. In the results window, click on Actions > Export to Excel.
2. A pop-up window offers you options to open or save the export file. Typically, click on its Save button and, in a Save As dialog, navigate to a folder in which you want to save the file.

Visualizing Access Results

As you view the results of an access model, you can generate a graphic depiction of paths from any number of users to any number of access points involved in conflicts.

1. In the Results window, select any number of paths. To select one, click on it; to select a continuous set of paths, click on the first one, hold down the Shift key, and click on the last one; or to select a discontinuous set of paths, hold down the Ctrl key as you click on the paths.
2. In the Results window, click on Actions > Visualize. A Graph window opens, depicting the paths you've selected.

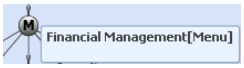


3. Review information presented by the image:
   - The top-level node in a Visualization image is initially a user whose duty assignments have violated the access model. Depending on the paths you've selected in step 1, there may be more than one user.
   - The bottom-level nodes in a Visualization image represent the lowest-level objects affected by the model — those that actually enable a user to do something. For example, if a model sets one Oracle responsibility in conflict with another, the graph shows not only the responsibilities, but also the menus to which they lead and the functions to which those menus lead.
   - All nodes represent objects that lead from a user to a privilege (functionality that enables the user to do something), and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.

- You can expand or contract the size of the image: Click on the square with a horizontal line at the upper left of the frame containing the diagram, and slide it up to enlarge the diagram (and so expose fewer of its objects to view), or down to reduce the diagram (and so expose more of its objects to view).

4. Manipulate information presented by the image:

   - If you move your cursor over any of the objects in a path, the image displays the name of that specific object.

   - If you click on any object in a path, the arrows leading to that object are highlighted in red, distinguishing those paths from others that do not lead to the object you've selected.

   - Because the Results window focuses on a single model, a Highlight Model/Control list box displays only an entry for the model whose results you are reviewing. If, in step 1, you selected paths involving more than one pair of access points, you can select one of those pairs to highlight its paths in red. To do so, first use the Highlight Model/Control list box to select the model. Then click on the downward-pointing icon in the Highlight Conflicting Access Points list box, and select the pair of access points you want. (If, in step 1, you selected paths involving only one pair of access points, only that pair is displayed in the Highlight Conflicting Access Points list box.)

   - You can narrow the focus of the Visualization image by eliminating its first hierarchical level (users whose assignments have generated conflicts), or the first and second hierarchical levels (users and the roles assigned to them). To do so, click on the downward-pointing icon in the list box labeled Chose a simplification level, and select the Hide User option or the Hide User & Role/Permission List option.

5. Select a path that serves as a filter for paths listed in the Results window: Click on any node in the graph. The path to that node appears in the Apply Path Filter field. Click on the Apply button. The Visualization graph closes, and the Results window displays only paths defined by the filter you've selected.

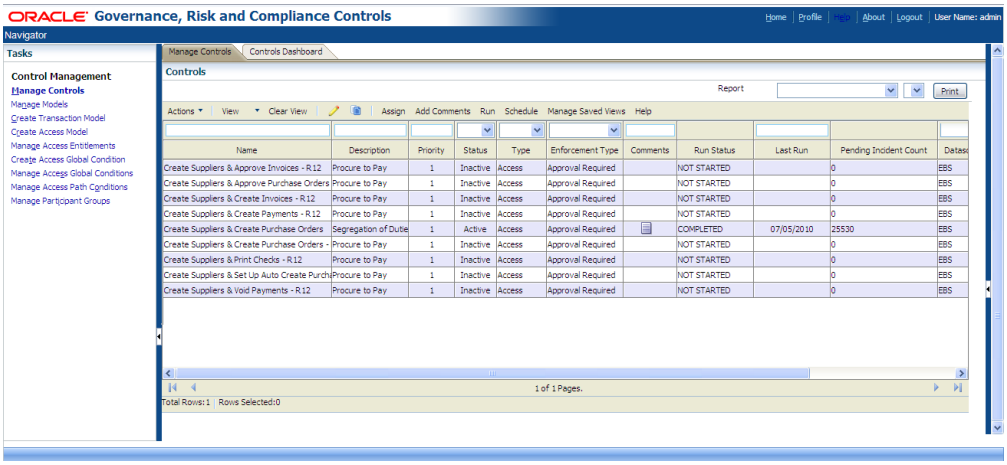
To close the Visualization window without first selecting a filtering path, click on the × symbol in its upper right corner.

3

Creating and Managing Controls

An access control defines risk and generates incidents — records of access-point assignments that exceed the defined risk. To create the control, a user selects an access model; the control adopts its risk definition (filtering logic). The user adds information needed for the control to be run and its incidents to be resolved: a data-source to which the control is applied, participants who resolve its incidents, a priority, and more. The user also selects an enforcement type — Prevent, Monitor, or Approval Required — that determines what a participant may do about the control's incidents.

A Manage Controls home page presents a list of controls (access and transaction), and enables you to edit them or to convert models into new controls. You can also import and export controls, run reports about them, and view their change history.



From the Manage Controls home page, you can navigate to other pages, in which you can view a "controls dashboard," or view and edit detailed records of individual controls. Manage Controls pages also offer tools for maintaining "tags," each of which is a set of values. Users may assign any tag value to a control to characterize it and its incidents. EGRCC comes with two default tags — Business Process and Risk — and users may create others.

Viewing Controls

The Manage Controls home page presents a list of controls you are entitled to view — those that specify datasources and business objects to which your EGRCC role

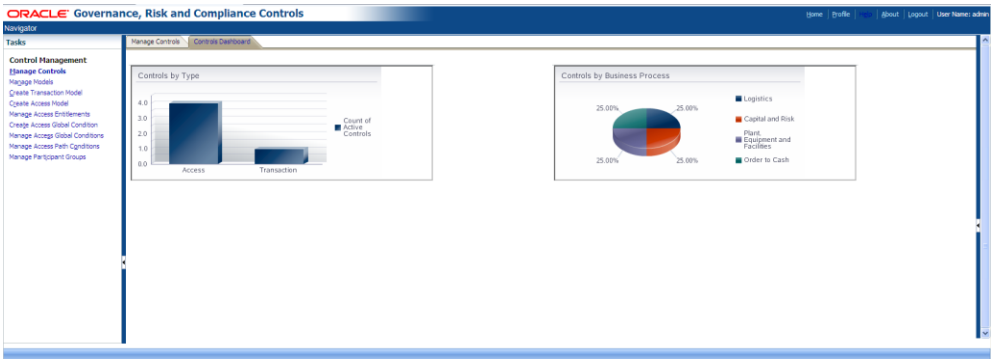
gives you access. To open it, select Manage Controls under Control Management in the Tasks panel. (See “Navigating in EGRCC,” page 1-5.)

For each access control, the page displays these values by default: name and description, priority, status (Active or Inactive), type (Access or Transaction), enforcement type, the datasource on which the control runs and its type (Oracle EBS, PeopleSoft, or Fusion), the date and status of the most recent run, the number of incidents it has generated, its tag values, and whether comments have been appended to it.

Other values are hidden by default, but you can display them, or hide any of those already on display. (See “Removing and Restoring Columns,” page 1-8.) For each control, hidden values include the participants assigned to it, the users who created and most recently updated it, the dates on which they did so, and controls that are considered to be related to it.

Reviewing Summary Graphs

Two graphs display summary information about active controls. To view them, click on the Controls Dashboard tab.



A bar graph sorts active controls by type: one bar represents access controls, and the other transaction controls. The height of each is proportional to its number of active controls. Hold the cursor over a bar, and a pop-up message displays its control type and number of controls.

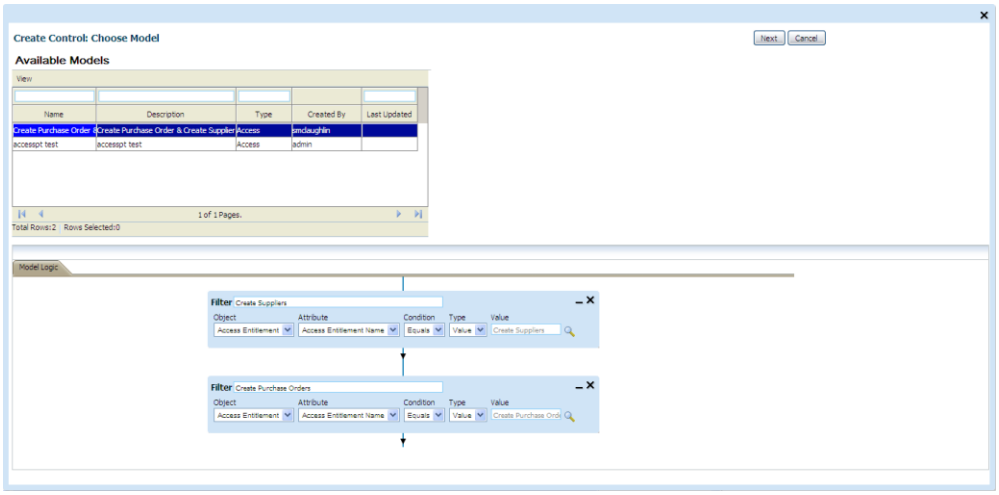
A pie graph depicts counts of active controls assigned each of the values for the Business Process tag. Each “pie slice” represents one of the values, its area proportional to the number of controls assigned that value. Hold the cursor over a pie slice, and a pop-up message displays the name of its Business Process tag value and the number of controls assigned that value.

To return to the Manage Controls home page, click on the Manage Controls tab.

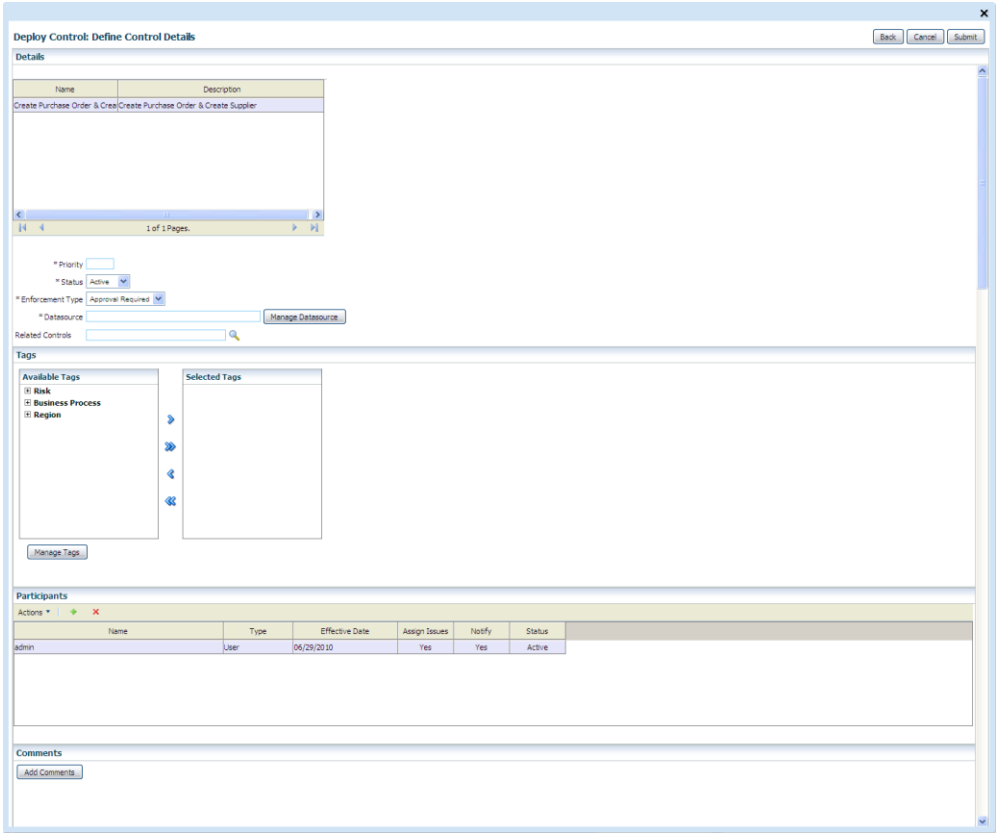
Creating Access Controls

Because every control is based on a model, ensure that at least one access model exists before you attempt to create an access control. You may convert any number of access models into controls at once. If you create more than one, their processing logic, names, and descriptions remain distinct, but other values are the same for all the controls you create at once.

1. In the Manage Controls home page, click on Actions > Create Access Control.
2. A Create Control: Choose Model window opens. In an Available Models grid, select models you want to convert into controls: To select one, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on models. A Model logic pane displays the filters that define each model you select; the last model you select is the one whose filters remain on view.



3. Click on the Next button. A Deploy Control: Define Control Details window replaces the Choose Model window.



4. Set the following values, as described below: name, description, priority, status, enforcement type, datasource, related controls, tags, participants, and comments.

   You may click on a Back button, to return to the Choose Model window and revise your model selection. If so, when you return to the Define Control Details window, any values you have selected remain in force.

5. When you are satisfied with all the selections you have made, click on the Submit button in the Define Control Details window.

Naming and Describing Controls

In the Define Control Details window, a Details grid displays a row for each model you selected. Each row contains the name and description of its model. You can accept these as the names and descriptions of the controls you are creating, or click in each Name and Description field to create new values.

Setting Priority, Status, and Enforcement Type

In the Priority field, enter a value that expresses the importance of the controls you are creating in relation to others. The value must be a number. (Your company should establish a set of priority values and enforce consistent usage.)

In the Status list box, select Active (the default) to use the controls you create, or Inactive to hold them in reserve.

In the Enforcement Type list box, select Prevent, Monitor, or Approval Required. See “Incident Analysis” (page 1-3) for definitions of these enforcement types.

Selecting Datasources

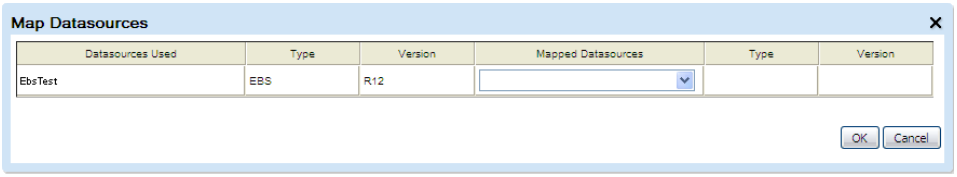
The models upon which you are basing the controls you create are already associated with datasources. You may retain those associations, or select new datasources for the controls you are creating.

Suppose, for example, you have distinct test and production systems, each of which consists of an Oracle EBS instance. You’ve set up both EBS instances as datasources to EGRCC, called EbsTest and EbsProd.

Suppose further that you created a model to run in the test system; it cites business objects associated with the EbsTest datasource. You want to convert the model into a control that runs in the production system. To do so, you would replace the EbsTest datasource with EbsProd.

To select datasources for a control:

1. Click on the Manage Datasource button. A Map Datasources window opens. It displays one row for each datasource specified in the models upon which you are basing your controls.



2. In the Mapped Datasources list box of each row, select a datasource appropriate for the environment in which the controls are to be applied.

   In each row, a Datasources Used field displays the datasource associated with a source model. You may select this or another datasource in the Mapped Datasources field to apply to controls you are creating.

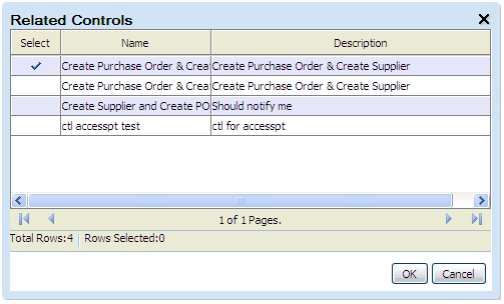
   As you create a model that includes entitlements, you associate the Access Entitlement business object with a Grcc datasource. However, if you are converting an entitlement model into a control, you do *not* select the Grcc datasource here. Instead, select datasources that contain access points included in the entitlements.

3. Click on the OK button. The Map Datasources window closes, and your selections appear in the Datasource field of the Define Control Details window.

Selecting Related Controls

Controls may be related to one another for any reason your company determines to be meaningful. To select controls related to those you are creating:

1. Click on a magnifying-glass icon next to the Related Controls field.
2. A Related Controls window opens, listing the controls that already exist on your EGRCC instance. Select any number of them: To select each, click in the Select field in its row. A check mark appears in each row you've selected.



3. Click the OK button. The Related Controls window closes, and your selections appear in the Related Controls field of the Define Control Details window.

Selecting Tags

Select tag values, which will apply not only to the controls you are creating, but also to incidents they generate:

1. Available Tags and Selected Tags boxes list tags configured for your instance of EGRCC. In either box, click on the ± toggle next to any tag to reveal its values.
2. Add tag values to, or remove them from, the controls:

   To add tag values, click on a value in the Available Tags box, and then click on the > button. The value moves to a Selected Tags box. Repeat this process for all tag values you want to assign to the incident. Alternatively, click on the >> button to move all tags and tag values to the Selected Tags box.

   To remove tag values, select them individually in the Selected Tags box and click on the < button to return them to the Available Tags box. Or, click on the << button to return all tags and tag values to the Available Tags box.

Optionally, use the Manage Tags button to edit tags themselves and their values. (See "Managing Tags," page 3-10.) If you do, the changes you make are available to all incidents and controls.

Selecting Participants

To add participants to the controls:

1. In the Participants grid, click on Actions > Add (or click on the green plus sign). A new row appears in the grid.
2. Click in the Name field of the row. A list of EGRCC users and participant groups appears; select one. The next field, Type, indicates whether the participant you've added is a group or a user; you cannot edit this value.
3. An Effective Date field displays a date on which the participant is added to the controls you are creating. The default is the date on which you are creating the controls; to accept it, do nothing in this field. Otherwise, click in the field and a calendar pop-up window appears. Click right- or left-pointing triangles to move forward or back through months; in a given month, click on the date you want.
4. Click in the Assign Incidents field and select Yes to make the participant responsible for resolving incidents generated by the controls, or No to make the participant an observer with no default responsibility for resolving incidents.
5. Click in the Notify field and select Yes to have EGRCC send email notifications to the participant when the controls generate incidents, or No to forgo notifications. (A connection to your email server must be set up in the EGRCC Manage Application Configurations page.) Notifications are consolidated; each participant receives a single message for all incidents generated by a run of a control.
6. Typically, ensure that Active is selected in the Status field (or, choose Inactive to create participants without actually using them).
7. Repeat these steps for each participant you want to add.

To delete a participant, click on its row and select Actions > Delete (or click on the red × symbol).

Writing Comments

To add a comment to the controls:

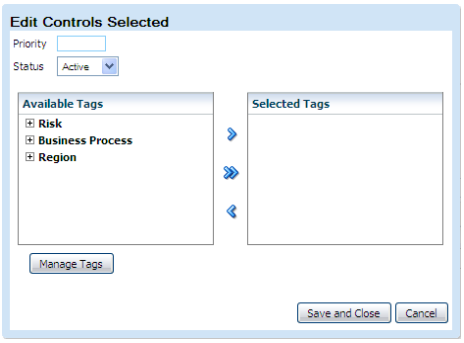
1. Click on the Add Comments button. A Comments dialog opens.
2. In the Comments dialog, type the comment you want to add to the controls.
3. Click on the Save button. The comment appears in the Comments pane of the Define Control Details window, together with the date, time, and your name.

Mass-Editing Controls

You can modify the priority, status, tag values, or participants, or add comments, to any number of existing controls at once. To perform any of these operations, first select the controls you want to modify from the list of controls on the Manage Controls home page. To select one control, click on it. To select a continuous set of controls, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on controls.

To modify priority, status, or tags:

1. Click on Actions > Mass Edit. An Edit Controls dialog opens.



2. Set new values in any combination of the Priority or Status (page 3-4) or Tags (page 3-5) areas of this dialog. (The controls retain their original values for any of these areas you leave unedited.)
3. Click on the Save and Close button.

To modify the assignment of participants to the selected controls:

1. In the Manage Controls home page, click on Actions > Assign, or on the Assign button. An Assign dialog opens.
2. Do either, or both, of the following:
   - Add participants — move them from the Available Participants box to the Selected Participants box. In Available Participants, click the ± toggle next to a Users entry or a Groups entry to reveal users or participant groups that are not yet assigned to the selected controls. Click on one, and then on the > button. Repeat for each participant you want to add. Or, click the >> button to move all users and groups to the Selected Participants box.

     (Participants are added with the Assign Incidents and Notify values set to Yes, and with Status set to Active. You can edit these values for each control individually.)
   - Remove participants — move them from the Selected Participants box to the Available Participants box. In Selected Participants, click the ± toggle next to a Users entry or a Groups entry to reveal users or participant groups that are assigned to the selected controls. Click on one, and then on the < button. Repeat for each participant you want to remove. Or, click the << button to move all users and groups to the Available Participants box.
3. Click on the Save and Close button.

To add a comment to the selected controls:

1. In the Manage Controls home page, click on Actions > Add Comments, or click on the Add Comments button. A Comments dialog opens.
2. In the Comments dialog, type the comment you want to add to the selected controls.
3. Click on the Save button.

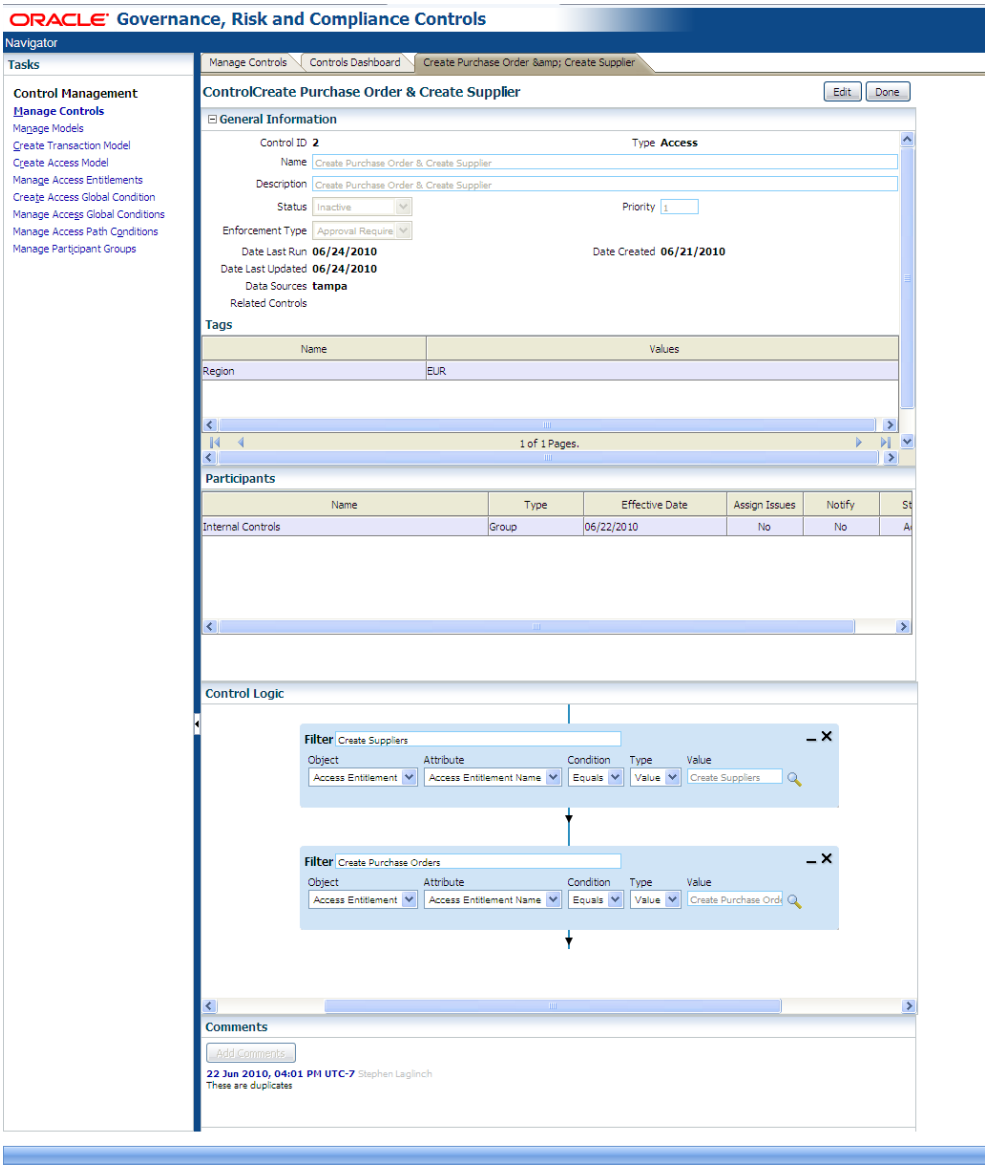
When a comment has been written, an icon appears in the comments field for each of its controls. To read a comment, click on the icon. A pop-up window displays comments written for the control.

Opening and Editing Controls Individually

To open pages that display detailed accounts of individual controls:

1. Select any number of controls in the list on the Manage Controls home page. To select one, click on its row. To select a continuous set of controls, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on controls.
2. Select Actions > Open.

One page opens for each control you've selected. A tab appears at the top of each page, labeled with the appropriate control name. To view a control detail page, click on its tab. To return to the Manage Controls home page, click on its tab.



Initially, each page presents a read-only display of control details:

- A General Information pane displays the name and description of the control; its ID and type (Access or Transaction); its status, priority, and (if it is an access control) enforcement type; dates on which it was created, last run, and last updated; the datasources to which it applies; its related controls; and tag values assigned to it.
- A Participants pane lists the EGRCC users or participant groups selected as participants to the control.
- A Control Logic pane displays the filters that define the processing logic of the control, arranged in the AND/OR order in which they are analyzed.
- A Comments pane displays all comments written about the control. Each comment appears with the date and time on which it was written, and the name of the user who wrote it.

To edit controls, open their detail pages, and then click on the Edit button in each page. Or, select controls in the list on the Manage Controls home page, and select Actions > Edit. In either case, a write-enabled version of the detail page opens for each control. In each page, you can update the name, description, status, or priority for a control by entering new values in the appropriate fields. You can modify related controls (page 3-5), tag values (page 3-5), or participants (page 3-6), or write comments (page 3-6), as you would if you were creating a new control. When you finish modifying a control, click on the Save button in its edit page.

To close either the detail page or the edit page for a control, click on its Done button.

Running Controls

You can cause EGRCC to analyze, and return incidents for, any selection of controls. To begin, choose the controls you want to analyze from the list on the Manage Controls home page: To select one, click on its row. To select a continuous set of controls, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on controls.

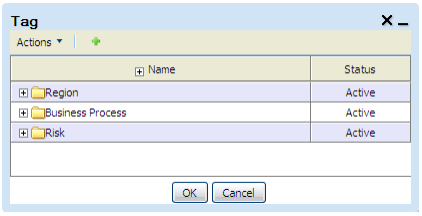
Then, do either of the following:

- Evaluate the selected controls once, immediately. Before doing so, consider synchronizing data from the datasources against which the controls will run; this would ensure that access data is up to date. See “Synchronizing Data” on page 1-6. To evaluate the controls, select Actions > Run, or click on the Run button. EGRCC displays status of the run at the base of the Manage Controls home page.
- Create a schedule on which the selected controls run regularly. To do so, select Actions > Schedule, or click on the Schedule button. A Schedule Parameter dialog opens; in it, enter values that set a name for the schedule, the date and time at which it starts, the regularity with which the controls are evaluated, the date and time (if any) on which the schedule expires, and whether data should be synchronized immediately before each control evaluation. Then click on the Schedule button.

Managing Tags

To create and edit tags and tag values used for classifying controls and the incidents they generate:

1. In the Manage Controls home page, select Actions > Manage Tags. Or click on the Manage Tags button that is available as you create or edit a control (or incident). In either case, a Tag dialog opens, listing all currently configured tags.



2. To create a new tag, click on Actions > Add Tag (or on a green plus sign); an Add Tag window opens. To edit an existing tag, select its row and click on Actions > Edit Tag; an Edit Tag window opens.
3. If you are creating a new tag, type a name for it in the unlabeled field beneath the title bar of the Add Tag window. If you are editing an existing tag, you may edit its name in the equivalent field of the Edit Tag window. In either case, typically ensure that Active is selected in the list box next to this field (or, choose Inactive if you want to hold the tag in reserve).
4. Create or modify any number of tag values:
   - To create a tag value, select Actions > Add Tag Value (or on a green plus sign). A new row appears. In its Name field, type a name for the value; in its Status field, typically ensure that Active is selected (or, choose Inactive if you prefer).
   - To modify a tag value, click in an existing row, and then edit the values it contains.
5. When you are finished, save the tag and its values: Click on the OK button in the Add Tag or Edit Tag window, and then on the OK button in the Tag window.

Importing and Exporting Controls

You can export controls from a source instance to a file, then import them from the file to a destination instance. However, controls are subject to the same import rules as those that apply to models (see page 2-3).

To export controls from a source instance to a file:

1. From the list on the Manage Controls home page, select controls to export. To select one, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold the Ctrl key as you click on controls.
2. Click on Actions > Export Controls.
3. An Export Statistics pop-up window appears. Click on its Download button.

4. A pop-up window offers you options to open or save the export file. Typically, click on its Save button and, in a Save As dialog, use standard techniques to navigate to a folder in which you want to save the file. The file is saved in .xml format; its name begins with the word *Controls*.

To import controls from a source file to a destination instance:

1. In the Manage Controls home page, click on Actions > Import Controls.
2. An Import File pop-up window opens. Click on its Browse button.
3. A Choose File dialog opens. In it, use standard techniques to navigate to, and select, the file you want to import. Select an .xml file whose name begins with the word *Controls*.
4. Click on the OK button in the Import File window.
5. A Select Items to Import window lists the controls contained in the import file. Select those you wish to import: To select one control, click on it. To select a continuous set, click on the first control, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on controls.
6. Click on the Next button. An Import Datasource Mapping window opens, displaying one row for each datasource specified in the controls you've chosen to import. For each, in a Mapped Datasources list box, select a datasource appropriate for the environment into which you are importing the controls (The list box displays datasources configured in the EGRCC Manage Application Data page.)
7. Click on the Import button. A pop-up message reports the number of imported controls and the status of the import operation. Click on its × button to close it.

Viewing Change History

To view a history of changes made to controls:

- Click on a control in the list on the Manage Controls home page. Or, open the detail page for a control (see page 3-7).
- Click on a left-pointing triangle located at the midway down the right border of the Manage Controls home page, or a control detail page. A change-control pane opens at the right of the screen.

A Change History grid displays one row for each version of the control you've selected up to, but not including, the current one. The information includes a revision number and the date on which that revision was created.

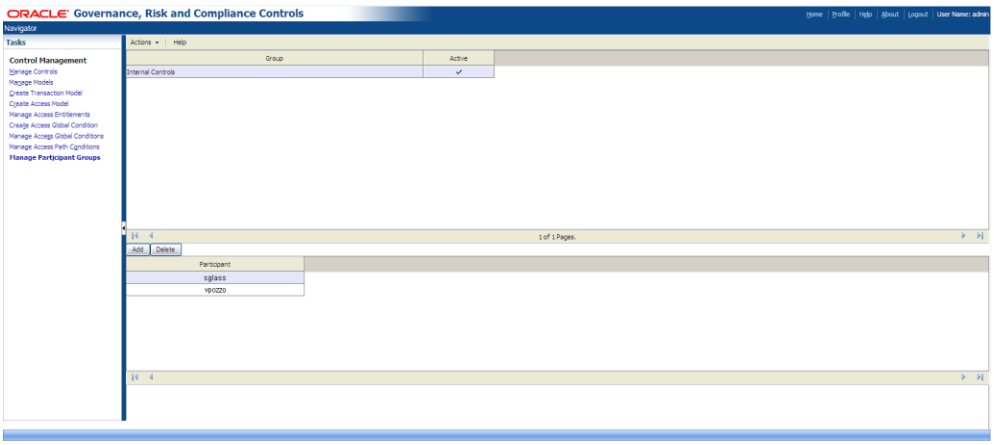
When you open the change-control pane, the triangle on which you clicked changes to point to the right. To close the pane, click on the right-pointing triangle.

Creating Participant Groups

At least one participant is associated with each control, to review its incidents or, if AACG preventive analysis has caused the control to suspend role assignments in

Oracle EBS or PeopleSoft, to approve or reject those assignments. A participant may be an EGRCC user or a group. Any member of a group may review a given incident or role assignment, but the first user to do so acts for all; there is no need for a second member to act after the first has made a judgment. To create a participant group:

1. Open the Manage Participant Groups page: select Manage Participant Groups under Control Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)



2. In the upper half of the Manage Participant Groups page, click on Actions > Add. A new row appears.
3. Click on the Group field in the new row, and type a name for the group.
4. Ensure that the Active check box is selected to make the group available for use (or clear the check box to withhold the group from use).
5. In the lower half of the Manage Participant Groups page, click on the Add button. A new row appears.
6. Click on that row. A list appears; from it, select an EGRCC user. Ensure that the user's role assignments grant necessary permissions: Rights to business objects and datasources cited in the controls to which the group will be assigned, as well as update rights to the Manage Incidents page (for the review of access incidents identified through detective analysis), the Manage Access Approvals page (for the review of roles suspended through AACG preventive analysis), or both.
7. Repeat steps 5 and 6 for each additional user you want to include in the group.
8. When you finish adding members, click on Actions > Save in the upper half of the Manage Participant Groups page. A Records Saved pop-up window appears; click on its OK button to clear it.

To modify an existing group, click on its row in the upper half of the Manage Participant Groups page. Add members (follow the procedure described above) or delete members — select a member's row in the lower half of the page, then click the Delete button. When you finish editing, save the group.

4

Resolving Incidents

The evaluation of access controls produces either "detective" or "preventive" results. Detective analysis uncovers control violations that existed before a given access control is created. Preventive analysis (see chapter 5) permits, prevents, or suspends the assignment of roles to users after access controls have been written to define conflicts within those assignments.

Detective processing generates "incidents." An access incident traces the path through which a user of a business-management application, assigned access points that a control defines as conflicting, can reach one of those access points. (The analysis of transaction controls also produces incidents, although transaction incidents are defined differently from access incidents.)

A Manage Incidents home page presents incidents (both access and transaction) belonging to the person who is currently logged on to EGRCC — for your purposes, you. Incidents may belong to you because you are a participant to the controls that generated them, or because other participants have assigned them to you. From the Manage Incidents home page, you can navigate to other pages, which show an "incidents dashboard" or detailed records of individual incidents.

The actual resolution of incidents occurs outside of EGRCC. For example, you may determine that a user's access to a role should be rescinded if it violates an access control; that action would be completed in the business-management application to which it applies. The EGRCC Manage Incidents pages enable you to review incident details, and to set the status of incidents to reflect whether anything should be, or has been, done about them. Moreover, a Simulation feature enables you to preview how resolutions to access incidents would affect a business-management application.

Initially, incidents appear in the Manage Incidents home page at an Assigned status, which means that you (potentially along with others) have been designated to address them. You can update an Assigned incident to any of the following statuses:

- Accepted, which means you have determined that nothing need be done to resolve the incident.
- Remediate, which means you have decided that some action must be taken in the business-management application to resolve the incident.
- Resolved, which means you have confirmed that the remedial action has been carried out in the business-management application.

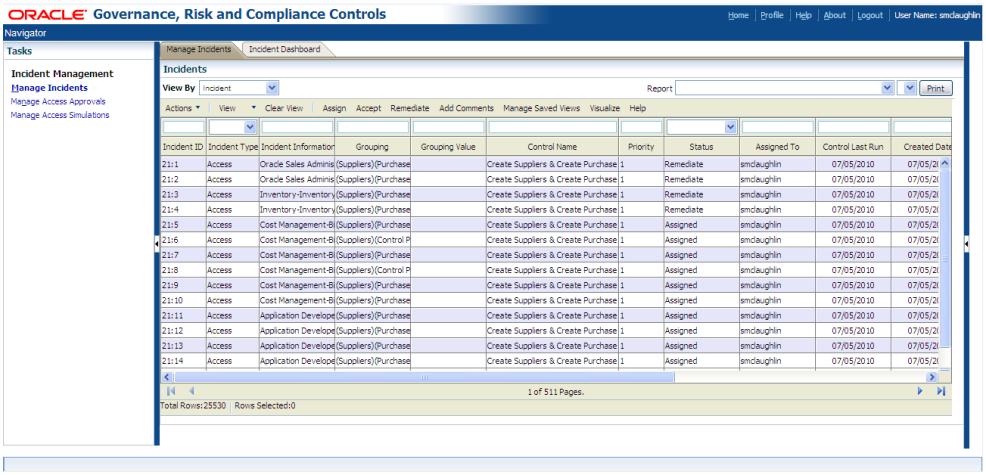
EGRCC may set other statuses:

- Authorized is given to incidents that result from preventive analysis: If a control violation causes the assignment of a role to a user to be suspended, a participant then approves the assignment, and the control is subsequently run, incidents related to the assignment receive Authorized status.
- Control Inactive means that an incident is no longer of concern because the control that generated it has been inactivated.
- Closed indicates that because an incident has been resolved in the business-management application, a subsequent evaluation of controls finds that the incident need no longer be addressed.

An incident is considered to be pending if it is at the Assigned or Remediate status. By default, the Manage Incidents home page shows only pending incidents.

Managing Incidents

To review, edit, or assign status to incidents, open the Manage Incidents home page: select Manage Incidents under Incident Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.)



You can set the Manage Incidents page to display either a list of controls that have generated incidents, or a list of incidents generated by those controls. In the control list, each control links to a list of the incidents only it has generated. From any list of incidents, you can open pages that provide details of individual incidents.

- For a list of controls, select Control Summary in the View By list box.

  For each active control, the Manage Incidents page displays the name, type (access or transaction), priority, the dates on which the control was most recently updated and evaluated, tag values (user-defined classifications), control participants (users or groups of users selected when the control was created to resolve the incidents it generates), the datasource to which the control applies, and comments appended to it by participants. The listing for each control also shows the number of pending incidents it has generated.

- For a general list of incidents, select Incident in the View By list box. For a list of incidents generated by a specific control, double-click on its pending-incidents value in the Control Summary list.

In either case, the Manage Incidents page displays the following values for each pending incident: An ID value generated by EGRCC; the name of the control that generated it; its status; its type (access or transaction); its priority; the datasource in which it exists; dates on which it was created, most recently updated, and closed, and on which its control was last run; the participants to whom it is assigned and who most recently updated its status; and comments configured for it.

Each access incident provides an Incident Information value — the path through which a user can reach one of the access points a control defines as conflicting.

Each access incident also contains Grouping and Grouping Value fields. The Grouping field identifies pairs of access points. Every pair includes the access point identified in the Incident Information field (at the path specified in that field). Each pair also includes an access point assigned to the user that the control defines as conflicting with the Incident Information access point. There may be any number of pairs. For access incidents, the Grouping Value field is blank.

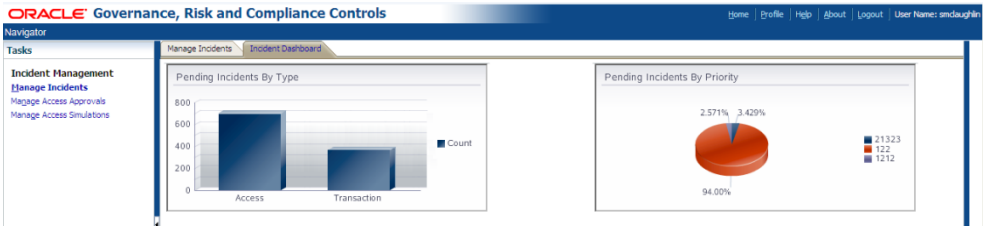
When you generate a list of incidents belonging to a selected access control, AACG returns hidden columns: Default Security, First Name, and Last Name. For an Oracle EBS datasource, Default Security displays the root menu for the responsibility associated with each incident, or the permission set granted to the role associated with each incident; for a PeopleSoft datasource, it displays the primary permission list assigned to the ERP user associated with each incident. The First Name and Last Name columns identify the ERP user associated with each incident. See “Removing and Restoring Columns” (page 1-8) for information on exposing hidden columns.

By default, the Manage Incidents page shows only pending incidents. You can, however, create views to display lists of incidents at any status: In the list box above the Status column, select the status for which you want to generate a list of incidents. Then click on the View button. To restore the list of pending incidents, click on the Clear View button, and then on the View button.

A list of controls or incidents may have more entries than can be displayed at once. If so, the list is divided into pages. (Click on a right-pointing triangle to advance from one page to the next, or a left-pointing triangle to move back one page at a time. Click on an icon that looks like a triangle pointing rightward at a vertical line to move to the last page, or a triangle pointing leftward at a vertical line to move to the first page.) To open incidents, set status, assign participants to incidents, or add comments, you select one or more controls or incidents, but you can select from only one page at a time. If you wish to select multiple controls or incidents, you can define a view (see page 1-6) so that those you want to select appear in one page.

Reviewing Summary Graphs

Two graphs display summary information about pending incidents. To view them, click on the Incident Dashboard tab in the Manage Incidents page.



A bar graph depicts counts of pending incidents sorted by the type of control that generated them. One bar represents access incidents, and the other transaction incidents. The height of each is proportional to the number of incidents generated by controls of the type it represents. Hold the cursor over a bar, and a pop-up message displays its control type and number of incidents.

A pie graph depicts counts of pending incidents sorted by severity. Each "pie slice" represents a priority assigned to controls that have generated incidents. The area of each slice is proportional to the number of incidents generated at its priority. Hold the cursor over a pie slice, and a pop-up message displays the priority value and the number of incidents at that priority.

To return to the Manage Incidents home page, click on the Manage Incidents tab.

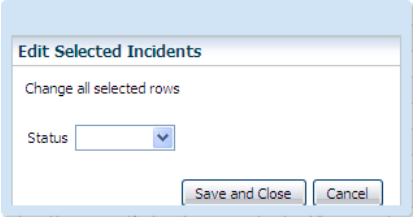
Mass-Editing Status, Participants, or Comments

You can set status for any number of incidents, assign participants to them, or write comments for them, all at once. To do so, first choose the incidents with which you want to work:

1. Generate a list of controls (to set values for all incidents generated by a selection of those controls) or a list of incidents. (See "Managing Incidents" on page 4-2.)
2. In that list, select any number of controls or incidents. To select one item, click on it. To select a continuous set of items, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on items.

To set status for the selected incidents, do either of the following:

- Click on Actions > Edit Status. An Edit Selected Incidents dialog box opens. In its Status list box, select the status you want to set. Then click on the Save and Close button.

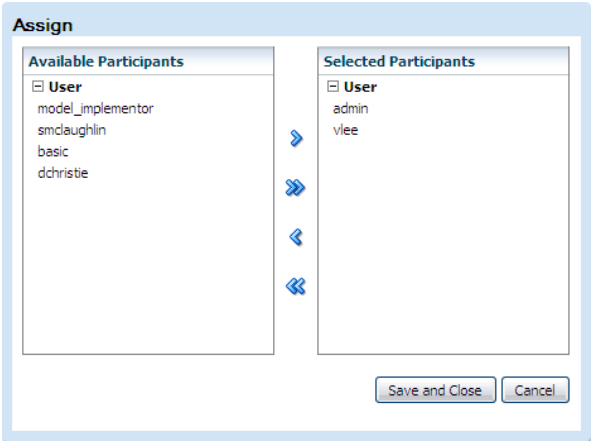


- If you are in a list of incidents, click on the Accept button or the Remediate button to set either of those statuses. (These buttons are unavailable in the Control Summary list.)

Because the Manage Incidents page displays pending incidents by default, an incident disappears from its list if you select a status other than Assigned or Remediate. The row for a control remains in the Control Summary list, but its pending-incidents entry is updated to count only those of its incidents that remain pending (and may therefore read 0). In an incidents list, you may create a view to see incidents that are no longer pending.

To assign participants to the selected incidents:

1. Click on Actions > Assign, or click on the Assign button. An Assign dialog opens.



2. Do either, or both, of the following:

   - Add participants — move them from the Available Participants box to the Selected Participants box. In Available Participants, click the ± toggle next to a Users entry or a Groups entry to reveal users or participant groups that are not yet assigned to the selected incidents. Click on one, and then on the > button. Repeat for each participant you want to add. Or, click the >> button to move all users and groups to the Selected Participants box.

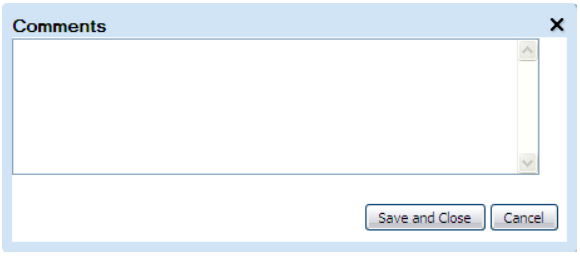
     (Participants are added with the Assign Incidents and Notify values set to Yes, and with Status set to Active.)

   - Remove participants — move them from the Selected Participants box to the Available Participants box. In Selected Participants, click the ± toggle next to a Users entry or a Groups entry to reveal users or participant groups that are assigned to the selected incidents. Click on one, and then on the < button. Repeat for each participant you want to remove. Or, click the << button to move all users and groups to the Available Participants box.

3. Click on the Save and Close button.

To add a comment to the selected incidents:

1. Click on Actions > Add Comments, or click on the Add Comments button. A Comments dialog opens.



2. In the Comments dialog, type the comment you want to add to the selected incidents.

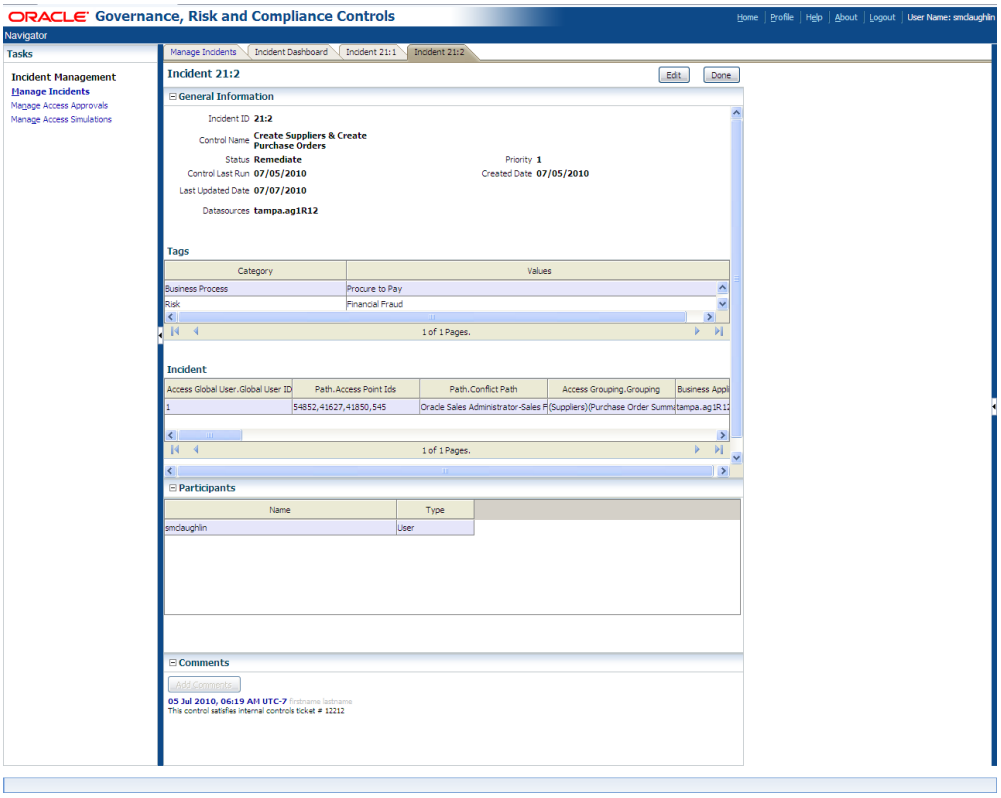
3. Click on the Save button.

Opening Incidents Individually

To open pages that display detailed accounts of individual incidents:

1. Generate a list of incidents. (See “Managing Incidents” on page 4-2.)
2. In that list, select any number of incidents. To select one, click on its row. To select a continuous set of incidents, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on incidents.
3. Select Actions > Open.

One page opens for each incident you’ve selected. A tab appears at the top of each page, labeled with the appropriate incident ID number. To view an incident page, click on its tab. To return to the Manage Incidents page, click on its tab.



Initially, each page presents a read-only display of incident details:

- A General Information pane displays the incident ID, the name and priority of the control that generated the incident, the current incident status, dates on which the control was last run and on which the incident was created and last updated, and datasources on which the incident exists. The General Information pane also includes:
  - A tags grid, which lists tag values, if any, that apply to the incident. These may have been selected for the control that generated the incident, or assigned directly to the incident.
  - An Incident grid, which defines the incident in question. For an access incident, the grid displays the path to an access point that conflicts with another

access point, and related information. One column in the grid contains a full expression of this path; others display individual access points within the path, and their type. The related information includes the user who has been assigned the access point that is the focus of this incident, and a grouping value (an access point that conflicts with the one that is the focus of this incident).

- A Participants pane lists the EGRCC users or participant groups who are participants to the incident. They may have been named as participants to the control that generated the incident, or they may subsequently have been assigned to the incident itself.
- A Comments pane displays all comments written about the incident. Each comment appears with the date and time on which it was written, and the name of the user who wrote it.

Editing Incidents

To edit an incident, open its detail page, and then click on the Edit button. This opens a write-enabled version of the incident detail page. In it, you can:

- Set status: The status field becomes an active list box. From this list, select the status you want to assign (see page 4-1).
- Modify the selection of tag values assigned to the incident:

  1. Available Tags and Selected Tags boxes list tags configured for your instance of EGRCC. In either box, click on the ± toggle next to any tag to reveal its values.
  2. Add tag values to, or remove them from, the incident:

     To add tag values, click on a value in the Available Tags box, and then click on the > button. The value moves to a Selected Tags box. Repeat this process for all tag values you want to assign to the incident. Alternatively, click on the >> button to move all tags and tag values to the Selected Tags box.

     To remove tag values, select them individually in the Selected Tags box and click on the < button to return them to the Available Tags box. Or, click on the << button to return all tags and tag values to the Available Tags box.

  You can also manage tags themselves and their values (see “Managing Tags“ on page 3-10).
- Add or delete participants:

  1. In the Participants grid, click on Actions > Add (or click on the green plus sign). A new row appears in the grid.
  2. Click in the Name field of the row. A list of existing participants and groups appears; select one. A Type field is populated by EGRCC.

  To delete a participant, click on its row and select Actions > Delete (or click on the red × symbol).
- Add a comment:

  1. Click on the Add Comments button. A Comments dialog opens.

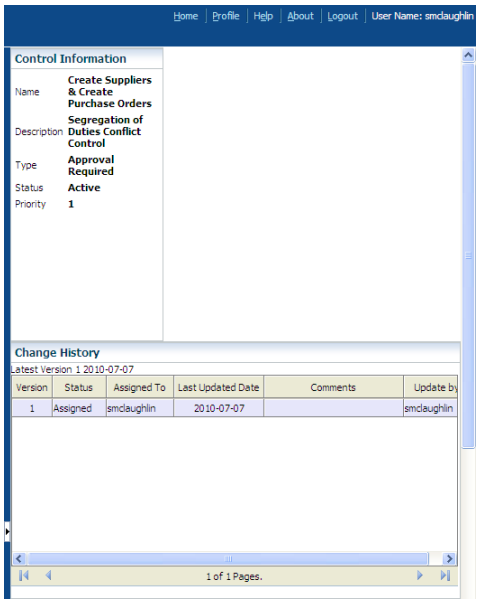
2. In Comments dialog, type the comment you want to add to the selected incidents.
3. Click on the Save button.

- Save the edits: When you finish editing the incident, click on the Save button near the top of the incident page. To close the page, click on the Done button (in either the read-only or edit version of the page). If you've made changes, but select Done before selecting Save, you lose all changes you've made.

Viewing Change History

In the Manage Incidents pages, you can view a history of changes made to incidents or to the controls that generated them. To do so:

- Generate a list of controls or a list of incidents (See "Managing Incidents" on page 4-2); in the list, click on the row for a control or an incident. Or, open the details page for an incident (see "Opening Incidents Individually" on page 4-6).
- Click on a left-pointing triangle located at the midway down the right border of the Manage Incidents home page, or an incident-detail page. A change-control pane opens at the right of the screen.



A Control Information segment of the change-control pane displays information either about a control you've selected, or about the control that generated an incident you've selected. The information includes name, description, type (the enforcement type for an access control), status, and priority. Beneath this, a Change History grid displays one row for each version of the control or incident you've selected up to, but not including, the current one. The information includes a version number (sequentially assigned by EGRCC), status, the date on which that version was updated and the person who updated it, and the comment (if any) written for that version. For an incident, the grid also shows the person to whom the incident was assigned at that version.

When you open the change-control pane, the triangle on which you clicked changes to point to the right. To close the pane, click on the right-pointing triangle.

Visualizing Access Incidents

You can generate a graphic depiction of incidents generated by access controls — paths from any number of users to any number of access points involved in conflicts. Select Incident in the View By field of the Manage Incidents page; select any number of access incidents, using the Shift or Ctrl key to select a continuous or discontinuous set; then either click the Visualize button or select Actions > Visualize. A Graph window opens; use it as you would to visualize the results of access models (see "Visualizing Access Results" on page 2-23).

Using Access Simulation

Simulation enables you to preview how a business-management application would be affected if its configuration were changed so that higher-level access points no longer granted access to lower-level access points, and incidents involving those lower-level access points were therefore resolved. It is a purely visual feature.

A Simulation model enables you to select an access point involved in incidents and display its hierarchy — a diagram showing how the access point connects to all other access points that relate to it as "parents" and "children." In the diagram, you select parent-child pairs of access points and then "remove" each child from its parent. As you do, the simulation feature builds a remediation plan, essentially listing, as steps, the child access points and the parents from which they would be removed. Once you are satisfied with your plan, you run the simulation and review statistics that show how the removal of the child access points from their parents would impact your incidents, roles, controls, and users. You can print the remediation plan, or save it to your computer.

To create and run a simulation:

1. Name and describe the simulation.
2. Select an access point that's involved in one or more incidents, and create a graphic model of its hierarchy.
3. Develop remediation steps. In the graphic model, select an access point whose removal might resolve an incident and select its immediate parent. Then select a "Remove" option. Repeat this process as often as you like to create additional remediation steps.

   For example, in an Oracle context, a user might have access to functions f1 and f2, and a control may define them as conflicting. You might select f1 and the responsibility through which the user has access to it (assuming there's a direct link between the two).
4. Run the simulation and view its results.
5. Print a copy of the remediation plan you've created, or save a copy to your computer.

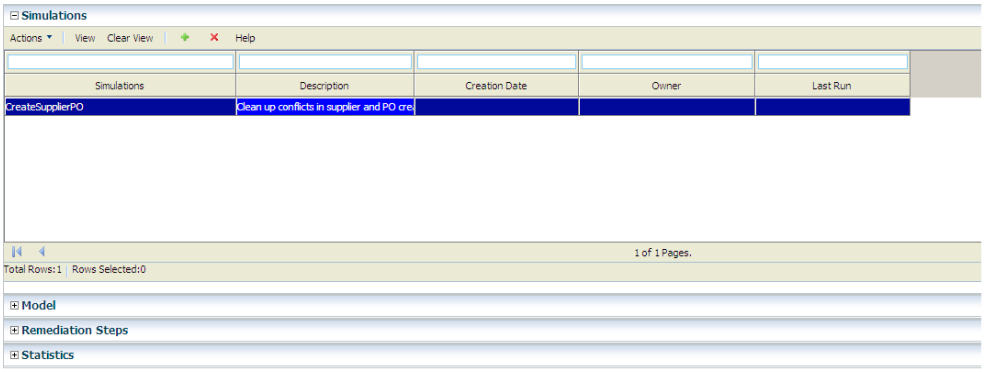
Simulation "scenarios" created in AACG versions earlier than 8.5 are incompatible with version 8.6.3. If you wish to reuse simulation plans you created in versions earlier than 8.5, you need to re-create them in version 8.6.3.

Creating and Naming a Simulation

To create a simulation:

1. Open the Manage Access Simulations page: select Manage Access Simulations under Incident Management in the Tasks panel. (See “Navigating in EGRCC,” page 1-5.)
2. In the Simulations pane, click on Actions > Create New. A new row appears in the Simulations grid.
3. Click in the Simulations field, and type a name for the simulation you are creating.
4. Click in the Description field (or, from the Simulations field, press the Tab key). Then type a brief description of your goal in creating the simulation.

The remaining three fields in the row will be completed by EGRCC when the simulation is saved; you cannot edit them directly. Creation Date shows the date on which the simulation was created; Owner shows the username of the person who created the simulation; and Last Run shows the date on which the simulation was most recently evaluated (the field is blank if the simulation has never been evaluated).



Creating a Simulation Model

A simulation model applies to incidents generated by one or more user-selected controls. Even so, you would typically want to run synchronization and access analysis on the selected controls before creating a simulation model, to ensure that incidents generated by the controls are up to date.

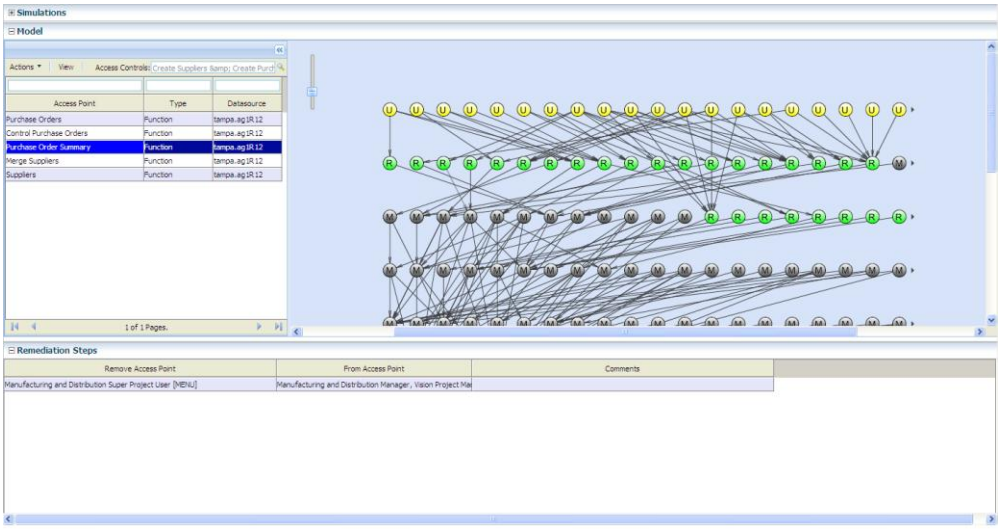
1. In the Models pane, select controls in the Access Controls field.

   Click on the icon that looks like a magnifying glass, to the right of the Access Controls field. A Select Access Controls window opens. Optionally, filter on Name or Status, and click the View button, to search for the control you want to select. From the list that’s generated, select one or more controls, using the Shift or Ctrl key to select a continuous or discontinuous set. Then click on the OK button.

2. The grid below the Access Controls field lists access points named in incidents that were generated by the selected controls and that have Accepted, Assigned, or Remediate status. Select an access point around which you wish to build a model.

More access points may exist than can be displayed at once, and so the Model grid is divided into pages. Click on the icon that looks like a right-pointing triangle to move forward one page, or the right-pointing triangle with a vertical bar to move to the last page. Click on the left-pointing triangle to move back one page, or the left-pointing triangle with a vertical bar to move to the first page.

3. In the Actions menu available from the Models pane, select the Apply option. The space to the right of the Models pane then displays a diagram that shows the selected access point as a central focus, from which radiate all the access points that have any relationship to it. The model diagram shows only those relationships that existed when the data synchronization process was last run.



The simulation model appears as a collection of nodes; arrows show how each node connects to others. As you interpret this diagram, keep the following in mind:

- All nodes represent objects that lead from a user to an access point that enables the user to do something, and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.
- If you move your cursor over any of the nodes, the image displays the name of the access point that the node represents.
- If you click on an arrow linking one node to another, the arrow appears in red, to distinguish it from other connections.
- If you double click on any node, the model redraws itself with the selected node as the central focus.
- You can expand or contract the size of the image: Click on the square with a horizontal line at the upper left of the frame containing the diagram, and slide it up its "track" to enlarge the diagram (and so expose fewer access points to view), or down to reduce the diagram (and so expose more access points to view).
- Once you create a simulation model, you can clear it (thus making way to replace it with a model based on some other access point). To do so, select the Clear Model value from the Actions menu available in the Model pane.

Having selected an access point involved in incidents, and created a model around it, you may narrow the model to focus on particular users or roles:

1. Within the model diagram, users and roles are each represented by a single node (labeled *U* or *R*). Click on one of them.
2. In the Actions menu of the Model pane, select Show Users or Show Roles.
3. A pop-up window opens, in which a column lists users with incidents involving the access point upon which the model is based, or roles that provide access to that access point (depending on your selection in step 2). Select (click on) one. If you've selected a user, a second column lists roles through which the user has access; if you've selected a role, a second column lists users granted access through the chosen role. Make a selection in the second column, so that ultimately you've selected a user-role combination.
4. Click on the > button to move to move your selection to the field all the way to the right.
5. Repeat steps 3 and 4 for each user-role combination you want in your model. If you reconsider, you can select items in the field at the right, the click on the < button to remove them from the field.
6. In the end, each entry in the field at the right displays either a user and a role assigned to her, or a role and a user assigned to it. Click on the OK button, and the simulation-model diagram redraws itself to display only access-point connections appropriate to the selected users and roles.

Developing Remediation Steps

From the graphic model you've created, generate steps to remediate incidents:

1. In the simulation model diagram, locate a child access point that you want to exclude from the parent so that the exclusion resolves incidents. Then do any of the following:
   - Single-click on that child and its parent, or on the link between them, and then select Remove from the Actions menu of the Model pane.
   - Double-click on the link between that child and its parent.
   - Hold down the Ctrl key and single-click on the link between the child and parent access points.

   A record of the exclusion you created appears in a row in the Remediation Steps pane. In the model diagram, the nodes you selected, and those that descend from them, are grayed out.
2. In the Remediation Steps pane, optionally click in the Comments field of the row you've added, and enter a comment about the step.
3. Repeat steps 1 and 2 any number of times to create additional remediation steps.

Should you change your mind about any remediation step you create, you can use any of several methods to rescind it: In the Model pane, once again select its pair of access points, and then select Revert from the Actions menu; double-click on the link between the access points; or hold down the Ctrl key as you single-click on the link. Or, in the Remediation Steps pane, double-click on the step.

Having generated remediation steps from one graphic model, you can select another access point in the Model pane, develop another model, and create additional reme-

diation steps from it. The steps you create from the original model remain in the simulation. (Any filters you applied to the original model, however, are not saved.)

When you finish creating remediation steps, save the model. Select Save from the Actions menu in the Simulations pane.

Running the Simulation and Viewing Results

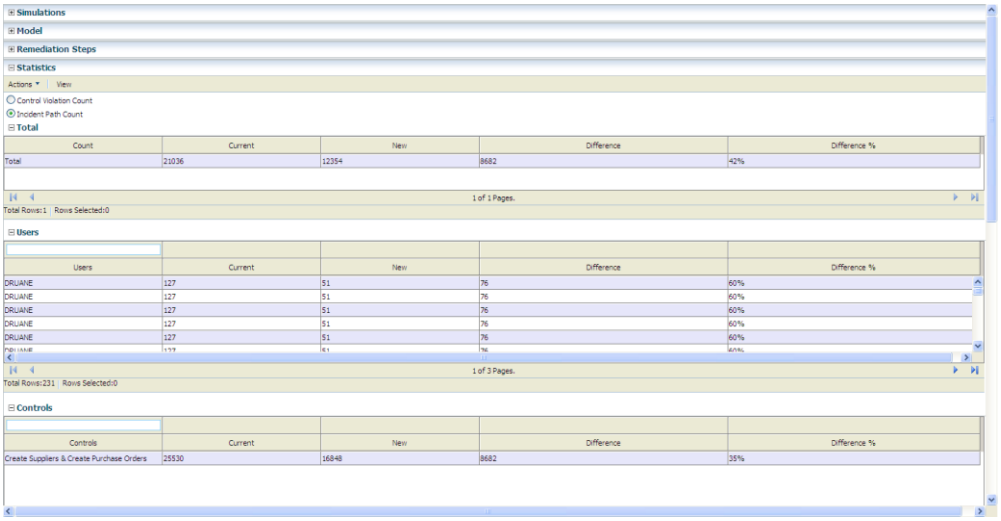
To run a simulation:

1. Select the simulation you want to run: Click on its row in the Simulations pane.
2. Select Run Statistics from the Actions menu of the Simulations pane. A progress bar at the bottom of the EGRCC window tells you when the simulation job is complete.

When the Simulation run ends, select either the Control Violation Count or Incident Path Count radio button in the Statistics pane:

- A control violation is the assignment of duties to one user violating one access control, no matter how many access points may be included in the control and therefore how many ways the user's access may violate the control.
- An incident path is a route by which a user gains access to one of the access points involved in a control violation. If a control defines a conflict between two functions, for example, one path might show how a user's responsibility assignment leads to a menu which leads to one of the functions named by the control.

Almost every control includes at least two access points. (The exception is a specialized "sensitive access" control that may set a single access point in conflict with itself.) Thus there are almost always a minimum of two paths per control violation (one to each of the minimum two access points), and usually very many more. Thus you can expect counts by control violation to be smaller — usually much smaller — than counts by incident path.



Depending on your choice, the Statistics pane displays either numbers of control violations or numbers of incident paths affected by your remediation plan:

- A Total grid displays the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually

executed, and the difference between the two stated both as an absolute value and a percentage.

- A Users grid lists the users who would be affected by remediation and, for each, states the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Controls grid lists the controls that would be affected by remediation and, for each, states the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Remaining Incident Paths grid shows all incident paths remaining — those unaffected by the Simulation. It has User and Control columns for easy filtering and sorting.
- A User and Role Impact grid lists users and roles that would be affected by the simulation. For each, a Type field tells whether the entry is a user or a role, and a User and Roles Impacted field identifies the user or role. The removal of a lower-level access point from a higher-level one may not only resolve an incident. Some users may have legitimate access from the higher-level point to the lower-level one, and implementation of the remediation plan would shut off that legitimate access. This grid lists both types of users (and the roles through which they have access) — those with resolved control violations, and those with lost legitimate access.

Printing or Saving a Remediation Plan

For reference — for example, for use when you actually implement a remediation plan in a business-management application — you can print a remediation plan or save it to your computer. To do so, run the simulation and then select Actions > View Remediation plan in the Statistics pane. You are then prompted either to save, or to open and print, a copy of the plan in .PDF format.

5

Managing Access Approvals

AACG preventive enforcement applies access controls to each user as he is assigned responsibilities in Oracle E-Business Suite, or roles in Oracle Fusion or PeopleSoft. Results depend on what (if any) controls are violated:

- If an assignment generates no conflict, or if it violates a Monitor control, it is allowed. When access is granted even though it has violated a Monitor control, and the control is subsequently run in the EGRCC Manage Controls page, incidents resulting from that grant appear in the EGRCC Manage Incidents page, with status set to Assigned.
- If an assignment violates a Prevent control, it is rejected, and no incidents are generated.
- If an assignment violates an Approval Required control, it is suspended until it can be reviewed:

  If the control finds conflicts in E-Business Suite or PeopleSoft, EGRCC notifies control participants, who use an EGRCC Manage Access Approvals page to approve or reject responsibilities or roles involved in the conflicts.

  If the control finds conflicts in Oracle Fusion, the review process is handled by Oracle Identity Management; although records of these conflicts appear in the EGRCC Manage Access Approvals page, it's recommended that control participants do nothing with them. (When conflicts are resolved in Oracle Identity Management, their records are removed automatically from the Manage Access Approvals page. For more information on the interaction of Oracle Identity Management and AACG, see the *Oracle Fusion Applications Security Guide*.)

  In either case, when an approval decision is made and the control is subsequently run in the Manage Controls page, incidents related to approved responsibilities or roles appear in the Manage Incidents page, with status set to Authorized.

When multiple control violations occur, EGRCC takes the most restrictive possible action. The "pecking order" is Prevent, Approval Required, Monitor, no conflict. For example, when a role assignment violates a Prevent control and an Approval Required control, access is denied and no notification is sent to control participants.

When EGRCC sends notifications of Approval Required control violations, it sends them to addresses recorded for participants in the Email Address 1 field of the EGRCC Manage Users page. Depending on how notifications are configured in the EGRCC

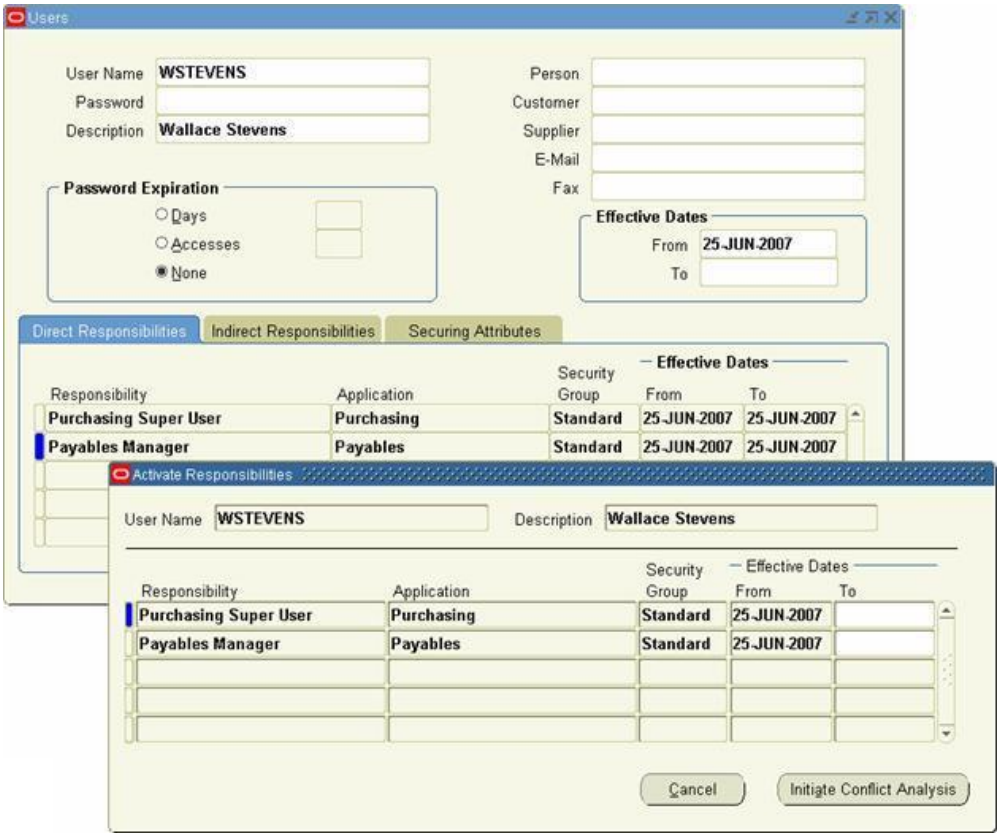
Manage Application Configurations page, notification of the enforcement outcome may be sent to the user who has been prospectively assigned new duties (see the *Enterprise Governance, Risk and Compliance Controls User Guide*). If so, it's sent to the email address associated with the user in the business application.

A Manage Access Approvals History page in EGRCC displays a history of assignments that violate access controls of any type.

Assigning Responsibilities in Oracle EBS

In Oracle EBS, the access approvals process begins in the Oracle Users form, as a new user is created or an existing user receives new responsibility assignments:

1. With the Users form open, a system administrator selects a user. He may assign responsibilities in the Direct Responsibilities grid, or review those inherited from newly assigned roles in the Indirect Responsibilities tab. In either case, both the start and end dates for these responsibilities are set by default to the current date, and cannot be modified directly. The administrator saves the new assignments.
2. The administrator clicks on Actions in the menu bar, then on Activate Responsibilities in the Actions menu. An Activate Responsibilities form opens. It presents a copy of the responsibilities listed in the Users form, but allows the administrator to change the end dates.



3. In the Activate Responsibilities form, the administrator removes end dates (or alters them to a future date) for a selection of responsibilities, and so

provisionally grants access to them. He then clicks the Initiate Conflict Analysis button.

4. A message, reading “Started Conflict Analysis Successfully,” appears. The administrator clicks its OK button to clear it.

   Within Oracle EBS, a concurrent request called AACG User Provisioning Poll handles approvals and rejections; it runs periodically, but may be run manually (it takes no parameters). An AACG web service initiates conflict analysis in the access engine. At this point, control participants may review Approval Required conflicts in the Manage Access Approvals page, or any type of conflict in the Manage Access Approvals History page.

5. If responsibility assignments had violated Monitor controls, or if they had violated Approval Required controls and the resulting conflicts were approved in the Manage Access Approvals page, end dates are removed in the Oracle EBS Users form (or modified to match the setting in the Activate Responsibilities form). The administrator can edit these end dates. If Approval Required assignments were rejected, or assignments had violated Prevent controls, the responsibilities remain end-dated.

Assigning Roles in PeopleSoft

In PeopleSoft, the access approvals process begins in the User Profiles page, as a new user is created or an existing user receives new role assignments:

1. With the User Profiles page open, an administrator creates a user or selects an existing one, then selects the Roles tab. She activates a new row, and selects a role in it; she may repeat this to add any number of roles.

2. The administrator clicks the Save button. A message appears, instructing the administrator to submit a request for review in EGRCC. The instructor clicks the OK button on this message.

   The Roles pane of the User Profiles page returns, but newly added roles have been removed if they are involved in conflicts. At this point, control participants

may review Approval Required conflicts in the Manage Access Approvals page, or any type of conflict in the Manage Access Approvals History page.

3. The administrator clicks on the Run AACG Poller link in the Roles pane of the PeopleSoft User Profiles page. A message states that the Poller has run successfully, and the administrator clicks an OK button to clear it.

   She then refreshes the page (navigates away from, and back to, the user account). Roles are restored to the display (and accessible to the user) if they had violated Monitor controls, or if they had violated Approval Required controls and the resulting conflicts were approved in the Manage Access Approvals page. Roles remain deleted if Approval Required conflicts were rejected, or if role assignments had violated Prevent controls.

Although the Run AACG Poller link is activated from a specific user's instance of the Roles pane, it updates role assignments for all users whose role assignments have been resolved in EGRCC. The Schedule AACG Poller link causes the poller to run regularly at an interval specified in a pea.properties file (which is configured during installation; see the *Governance, Risk and Compliance Installation Guide* for version 8.6.3). When you select this link, a message states "Successfully started the poller"; click its OK button to clear it. Once selected, the link becomes inactive.

Responding to Notifications

When a response is required — that is, when an Approval Required control has been violated in an Oracle EBS or PeopleSoft instance — the approver can respond in the Manage Access Approvals page. The approver is a participant designated to have "Assign Incidents" rights in the control that generated the conflict. Any such participant (individual or group member) may approve or reject the role assignment, but the first one to do so acts for all; other participants cannot act after the first participant has.

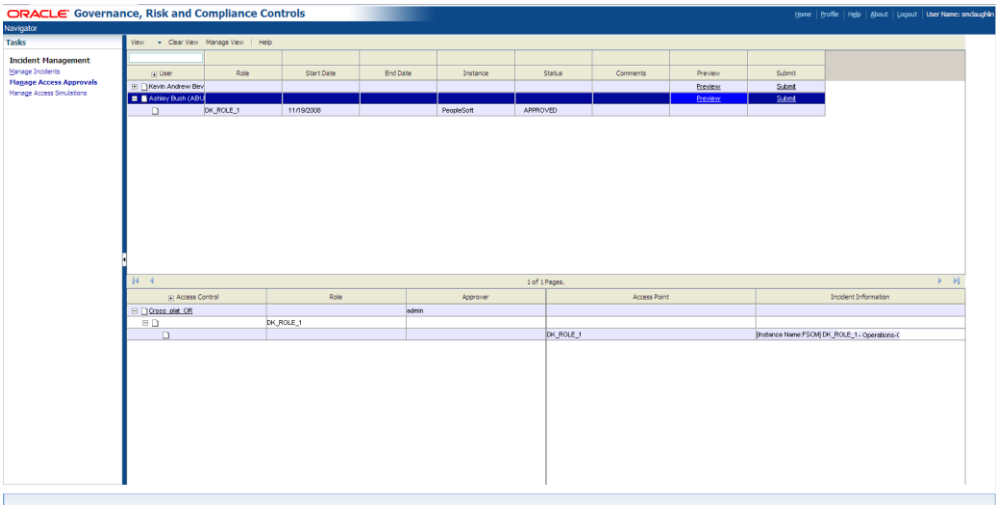
It is possible (even likely) for a control violation to involve more than one role, and for the assignment of duties to a user to violate more than one control. In such cases, EGRCC evaluates all controls, automatically approves access to roles that may be granted without conflict, and displays records of only those roles that would conflict with those already granted.

For example, suppose (in an Oracle EBS context) responsibility r1 contains function f1, r2 contains f2, and r3 contains f3. Suppose further that an Approval Required access control sets f1, f2, and f3 in conflict with one another, and that a user is assigned r1, r2, and r3. The user would be granted access to r1 (if its function, f1, happens to be the first one cited in the access control), but not to r2 or r3. A record for the user would appear in the Manage Access Approvals page; it would contain two subordinate records, one each for r2 and r3, with the status of each set to Pending. The participant would then approve or reject each of r2 and r3, and "submit" the decisions.

To approve or reject a user's role assignments:

1. Select Manage Access Approvals in the Incident Management list of the Tasks panel. (See "Navigating in EGRCC," page 1-5.)

2. The Manage Access Approvals page opens. Its top portion displays rows containing the user names of users whose assignments have violated controls for which you are a participant. Locate the user whose assignment you wish to review, and click on the + symbol next to his name.



3. One or more subordinate rows appear. Each shows a role provisionally assigned to the user, its start and end dates, the EBS or PeopleSoft instance on which the role is assigned, and the assignment status (set initially to Pending). In the Status field of each row, select Approve or Reject. Optionally, type a comment about your decision in the Comments field.

4. If you set the status for any role to Approve, click on the Preview prompt (in the Preview column of the parent row that identifies the user). The lower half of the page then displays records of paths to the access points included in the conflict. Each identifies the violated control, the objects that define the conflict path (the assigned role, the access point included in the control, and path leading from one to the other), and the approver. (If you set the conflict status to Reject, the Preview feature does not apply, and an attempt to run it produces a warning.)

   After reviewing conflict paths, you may determine that you should reject the conflict. If so, change the status in the upper half of the Request page to Reject.

5. When you have set status for all provisionally assigned roles to Approve or Reject, click on the Submit prompt (in the Submit column of the parent row that identifies the user, in the upper half of the page). The user's record then disappears from the page.

Viewing Access Approvals History

The Manage Access Approvals History page displays records of all users whose responsibility assignments violated access controls of any type. When a user's assignments violate Prevent or Monitor controls, the status of those assignments is set, respectively, to Reject or Approve. When a user's assignments violate Approval Required controls, their status is set initially to Pending. Once the conflict is resolved in the Manage Access Approvals page, the user's records disappear from there, and her responsibility-assignment statuses are reset in the History page to the values (Approve or Reject) selected in the Approvals page.

Users with view permission to the Manage Access Approvals History page can review approval history. Users with update permission to this page can both review history and reject role assignments at the Pending status; other statuses cannot be updated. The assumption is that such users would reject Pending roles only under extraordinary circumstances (for example, the participant for a control has resigned from the company); update rights to the Manage Access Approvals History page should be granted sparingly. (View and update rights are, of course, determined by roles assigned to EGRCC users.)

To open the Manage Access Approvals History page, select Manage Access Approvals under Administration Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.) Use the History page essentially in the same way as you would use the upper half of the Approvals page:

- The page displays rows containing the user names of users whose responsibility or role assignments have violated access controls. Locate the user whose request you wish to review, and click on the + symbol next to his name
- One or more subordinate rows appear, each showing a role assigned to the user, the start and end dates configured for it, the Oracle EBS or PeopleSoft instance on which the role was assigned, the status selected for the assignment, and any comments entered by the user who approved or rejected it.
- If you have view rights, all you can do is review these entries. If you have update rights, then for any row set to the Pending status, you can select a Reject link in the Reject column, and then select a Submit link in the Submit column. The responsibility or role assignment is then end-dated in the Oracle EBS Users form or deleted from the Roles tab on the PeopleSoft User Profiles page.

6

Reporting

Enterprise Governance, Risk and Compliance Controls produces summary and detail reports about access and transaction controls and about the incidents they identify, about the approval or rejection of role assignments that are subject to AACG preventive analysis, about conditions configured for access models and controls, about EGRCC users and roles, and about global users.

All these reports may be run, or scheduled to run at regular intervals, from pages available under Reports Management in the Tasks panel. (See "Navigating in EGRCC," page 1-5.) The control and incident reports may also be run "contextually" — from the EGRCC pages in which controls are managed and incidents are resolved.

This chapter discusses reports that apply specifically to AACG or commonly to AACG and ETCG. For discussion of other ETCG reports, see the *Enterprise Transaction Controls Governor User Guide*. For discussion of a report about users and roles, see the *Enterprise Governance, Risk, and Compliance Controls User Guide*.

Choosing Among Reports

The following reports apply to Application Access Controls Governor:

- A Control Detail Extract Report provides information about controls configured in EGRCC. For each control, the data includes name, description and comments, type (Access or Transaction), priority, the users who created and most recently updated the control, the dates on which they did so, and status (Active or Inactive), as well as the number of pending incidents it has generated. The report also lists tag values assigned to the control, its participants, and related controls. Finally, it displays the processing logic of the control and, for an access control, any conditions defined for it and entitlements that belong to it.
- The Incident Summary Extract Report lists incidents generated by access and transaction controls. For each incident, the report provides the name of the control that generated it; its status; its type (access or transaction); its priority; the datasource in which it exists; values of tags associated with it; dates on which it was created and most recently updated, and on which its control was last run; the users to whom it is assigned and who most recently updated its status; and comments configured for it. The report also provides an "Incident Information" value: For an access incident, this is the path through which a

user, assigned conflicting access points, can reach one of those access points. For a transaction incident, this is the value of the first attribute among those selected (during configuration of the control that generated the incident) to characterize the suspect transaction.

- The Incident by Control Summary Extract Report lists access and transaction controls that have generated pending incidents — those at the Assigned or Remediate status. For each control, the report shows the control name, type (access or transaction), and priority; the datasource to which it applies; values of tags associated with it; dates on which it was most recently run and most recently updated; participants assigned to it; comments configured for it; and the number of pending incidents it has generated.
- The Access Incident Details Extract Report lists incidents generated by access controls, providing for each not only the information that would be included in the Incident Summary Extract Report, but also additional details. These include the ID and name of the user whose work assignments have violated a control; the status, enforcement type, and full definition of that control; the pair of access points, among any number specified in the control, that define a conflict addressed by this incident; the full path through which the user can reach one of those conflicting access points; within that path, the access point directly assigned to the user ("role") and the one that provides actual functionality ("conflicting access point"); the entitlement (if any) that is named in the control and includes the conflicting access point specified in the incident path; and comments.
- The Access Point Report lists paths to access points involved in conflicts. Each path expresses the hierarchical relationship between a "parent" object that can be assigned to a user (such as an Oracle EBS responsibility), a "child" access point that is included in a control and involved in a conflict (such as an Oracle EBS function), and the objects that lead from one to the other (for example, menus and submenus that lead from a responsibility to a function). For a given access point, each record in the report is not a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
- The Access Violations by User Report lists the ten users with the greatest number of conflicts, as well as the number of conflicts for each. It names the controls violated by each user's work assignments (and, for each control, provides the enforcement type, priority, status, effective date, description, and comments). For each control, the report also identifies individual pairs of access points that have been assigned to the user, and that the control defines as conflicting.
- The Access Violations Within a Single Role Report lists roles for which access controls generate "intra-role" conflicts. These are conflicts between privileges granted within a given role, so that the role cannot be assigned to any user without a conflict occurring. (In this context, "role" means an Oracle EBS role or responsibility, or a PeopleSoft role.) For each such role, the report also lists the controls that define its intra-role conflicts.
- The Intra-Role Violations by Control Report lists access controls that generate intra-role conflicts for which incidents exist at the Assigned, Remediate, Authorized, or Accepted status. For each control, it also lists the roles for which the conflicts are generated. (Once again, "intra-role conflicts" are those involving privileges granted by a single role, and "role" means an Oracle role or respon-

sibility, or a PeopleSoft role.) In effect, this report reverses the sort order of the Access Violations Within a Single Role Report.

- The Users with Access Violations by Control Report lists access controls that have generated incidents at the Assigned, Remediate, Authorized, or Accepted status. For each control, it lists users whose work assignments have violated the control. For each user, the report supplies both the global user ID and the user's full name.
- The Access Approvals report displays records of role assignments in business-management applications which, because they violated Approval Required controls, were suspended until a control participant could review them. The report sorts records of role assignments into those that were accepted, rejected, or remain pending. Each record in the report specifies the user for whom access has been requested, the roles requested for that user, the business-management-application instance on which they were requested, the date on which the access request was made, and the dates on which access would begin and end.
- The Conditions report provides information about the three sorts of condition that may be set in AACG:

  A global condition applies to all access controls as they are enforced on a given datasource (instance of a business-management application), specifying users or other objects that are exempt from controls. The report identifies datasources and, for each, lists configured conditions. For each condition, it lists types of object (such as company in PeopleSoft, operating unit in Oracle EBS, or business unit in Fusion) and excluded instances of each type. Moreover, if a "Same" value is set to Yes, controls are enforced only if a user's access to conflicting access points would be granted within a single instance of an object type (for example, a single set of books).

  A global path condition excludes one access point from another, such as an Oracle function from a menu or a responsibility. A path including those points would be excluded from access incident generation. For each configured condition, the report identifies both the excluded access point and its parent, as well as their types and the status of the condition (Active or Inactive).

  A control-specific condition is like a global condition, except that it applies only to one control. The report lists the controls for which conditions have been configured.
- Finally, the Global Users Report provides information about global users — IDs created by EGRCC. Each identifies one person, and each correlates to any number of potentially varying IDs that person may have in business-management applications subject to access controls. Each record in the report contains the global user ID, a corresponding user ID in a business-management-application instance, the name of that instance and its type (Oracle or PeopleSoft), and the user's status on that instance. Each record also provides an "identifying value" — information that identifies the user uniquely. This may be email address; email address and user ID; or email address, user ID, given name, and surname. (Typically, the selection of values is configured during EGRCC installation.) For a given global user ID, the report may contain any number of records, one for each instance of a business-management application on which a user has an account.

Running Contextual Reports

You can generate the Control Detail Extract Report from the Manage Controls home page, or reports about incidents from the Manage Incidents home page:

1. Open the page that provides access to the report you want to run: select Manage Controls under Control Management, or Manage Incidents under Incident Management, in the Tasks panel.

   If you've opened the Manage Incidents page, generate a list of controls if you want to run the Intra-Role Violations by Control, Users with Access Violations by Control, or Incident by Control Summary Extract report; generate a list of incidents if you want to run any of the remaining incident reports. (See "Managing Incidents" on page 4-2).

2. Select controls or incidents upon which you want to focus the report. You can do this by clicking on any number of controls or incidents (use the Shift or Ctrl key to select a continuous or discontinuous set). If you do not select individual items, the report includes information about all controls or incidents in the list.

   Or, you can filter the list of controls or incidents to include only those you want. (See "Filtering Data" on page 1-7.) For example, you can generate a list of controls at a particular priority, or a list of incidents at a particular status. (If you do not filter incidents for status, the report contains pending incidents — those at the Assigned and Remediate statuses.)

   Some incident reports are specific to access or transaction incidents (or controls), and others are general. EGRCC automatically filters by type as needed: An access-specific report includes information only about access controls or incidents, a transaction-specific report includes information only about transaction controls or incidents, and a general report includes information about both.

3. In the Report list box, click on the report you want to run.

4. In the list box immediately to the right of the Report list box, click on the format in which you want to produce the report. For some reports, you can select only the value *csv*; this produces a file designed for export to another application, such as a spreadsheet, for further manipulation. For other reports, you may choose *csv* or *pdf*; the latter produces a formatted report that can be viewed in Adobe Acrobat.

5. Click on the Print button.

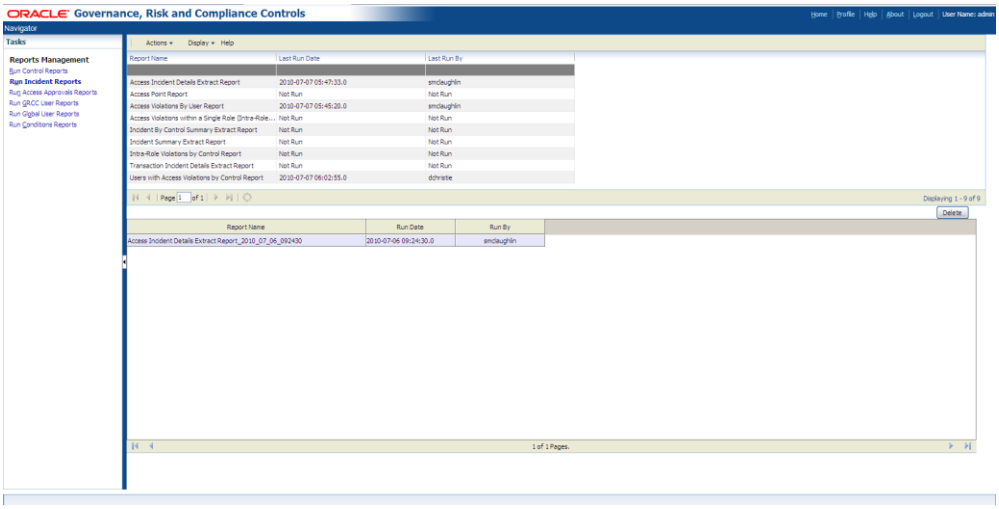
6. A File Download dialog appears. In it, choose whether to save or open the report. If you choose to save the report, another dialog opens; in it, navigate to a directory in which you want to save the report.

Using Reports Management

From Reports Management pages, you can run ad hoc reports or schedule them to be run at intervals over a period that you define. Reports Management saves the scheduled reports it generates, enabling you to view them at any time. As you run reports from Reports Management, you can select parameter values, thus focusing the results on records that match those values.

1. In the Reports Management list of the Tasks panel, select an option for the report you want to run: Run Control Reports for the Control Detail Extract Report, Run Incident Reports for any of the incident reports, or the appropriate option for each of the Access Approvals, Global User, or Conditions reports.

2. A Reports Management page opens; its upper portion lists reports you can run. Click on the row for the report you want.



3. Click on Actions > Run Now or Actions > Schedule.

4. A pop-up window appears; in it, select parameter values. In general, parameters correspond to the selections you make as you create or otherwise work with the object on which you are reporting. As you set parameters, you would select among the same values.

   For example, if you created a view (see page 1-6) in the Manage Controls page, you can select that view to have the Control Detail Extract Report display information about controls that belong to the view. For another example, you can select a control name to have the report apply only to that control. Each of the control- and incident-parameter windows also lists tags you have created; you can select one or more values for each tag to report on only the controls or incidents assigned those values. You can also select the format in which the report should be generated — *pdf* (Adobe Acrobat file) or *csv* (a text file for export to another application, such as a spreadsheet).

   If you select a datasource as a parameter, it filters for controls that involve access points associated with the selected datasource.

   Because the Incident by Control Summary Extract, Users with Access Violations by Control, and Intra-Role Violations by Control reports are status-specific (see their descriptions in “Choosing Among Reports”), they do not offer a status parameter. For other incident reports, a status parameter enables you to generate results about incidents at any status.

   If you are scheduling a report to be run, you must select a view as a parameter (and may select other parameters as well).

5. If you selected Run Now in step 3, the parameter window displays a Generate Report button; click on it to generate the report.

If you selected Schedule in step 3, this button is replaced by a Schedule Information button. Click on this button to produce a Schedule Parameter pop-up window, and to schedule the report to run. Enter values that set a name for the schedule, the date and time at which it should start, the regularity with which the report should run, and the date and time (if any) on which the schedule should expire. Then click on the Schedule button.

Reviewing Scheduled Reports

If you have scheduled a report to run, the bottom portion of the Reports Management page displays a row for each generation of the report. (Note that the Last Run Date and Last Run By columns in the top portion of the screen are populated by EGRCC, but only for scheduled runs of reports, not for ad hoc runs.)

To view a report generated on a schedule:

1. In the top portion of the Reports Management page, click on the title of the report you want to see.
2. Click on Display > Report History.
3. In the bottom portion of the Reports Management page, double-click on the instance of the report you want to see.

To view the schedule on which the report was generated:

1. In the top portion of the Reports Management page, click on the title of the report you want to see.
2. Click on Display > Scheduled Reports.
3. In the bottom portion of the Reports Management page, review summary information about the schedule, including its most recent and next scheduled run times.
4. Double-click on the row containing the summary information to reopen the Schedule Parameter pop-up window. Here, you can re-enter schedule values and select a Reschedule button, or turn off the scheduling by selecting an Unschedule button.