# ACTIVE Governance

## ACTIVE Access Governor User's Guide

Software Version 7.2

ORACLE®

ACTIVE Access Governor User's Guide

Part No. AG003-7221A

# Contents

# Chapter 1

# Introducing ACTIVE Access Governor

ACTIVE Governance both documents and enforces business controls, enabling users to demonstrate regulatory compliance and to promote operational efficiency. An ACTIVE Governance Platform fulfills the documentary purpose, maintaining a "control library" in which users describe and catalog controls as well as other items that establish the business context in which controls exist. The Platform also provides for the review of control-library items, and for reporting on their status.

Moreover, the Platform serves as a foundation for modules that provide the capability to automate the enforcement of controls. One of these modules is ACTIVE Access Governor, which uncovers segregation-of-duties conflicts within an organization, either preventing them from occurring or detecting them so that they can be properly managed. Designed for use with Oracle Applications, ACTIVE Access Governor identifies conflicts at both the responsibility and function levels.

ACTIVE Access Governor also allows "access monitoring" — it grants users temporary access to duties they do not ordinarily fulfill, and then guards against potential conflicts by auditing all actions performed by such users.

## Segregation of Duties

Users of ACTIVE Access Governor create "segregation-of-duties rules," each of which may specify two or more responsibilities or functions that should not be assigned simultaneously to an individual person. Or, users may gather responsibilities or functions into "entity groups," and then define rules identifying two or more

groups that should not be assigned simultaneously to individuals. Users may create rules one at a time, or upload a set of rules supplied by Oracle and adapt them as needed.

Each rule applies one of four "control types" — Prevent, Allow with Rules, Approve with Rules, or Approval Required. These determine the action to be taken when an Oracle Applications user is assigned duties that violate a rule:

- A Prevent rule denies access to conflicting responsibilities or functions. When a user is assigned responsibilities that trigger a Prevent rule, ACTIVE Access Governor sets their end dates to match their start dates, thus ensuring there is no period during which the user has access to conflicting elements.
- An Allow with Rules SOD rule permits access to conflicting responsibilities or functions if one or more additional rules, written in Oracle Form Rules, mitigate the conflict by modifying Oracle Applications forms. This control type (like the Prevent type) requires no approval, and does not send approval requests to reviewers.
- An Approve with Rules SOD rule also permits access to conflicting responsibilities or functions on condition that one or more Form Rules mitigate the conflict by modifying Oracle Applications forms. In this case, however, the rule designates a reviewer — either an "owner" or an approval group. ACTIVE Access Governor sends an approval request to the reviewer, and access to the conflicting entities is granted only if the reviewer approves.
- An Approval Required rule designates an approval group or an owner who can either accept a conflict (that is, allow an Oracle Applications user to work at responsibilities or functions that are known to be in conflict) or reject it. In this case, no Form Rule is attached to the SOD rule, and for access to be granted to conflicting responsibilities or functions, no condition need be met other than that the reviewer approve the conflict.

Once segregation-of-duties rules are defined, an ACTIVE Access Governor user runs a "background program" called Generate User Conflicts; it evaluates Oracle Applications users, noting those whose work assignments violate rules. ACTIVE Access Governor then lists the conflicts generated by each rule in a panel called User Conflicts. It treats these conflicts in either of two ways:

- A user may have been assigned responsibilities or functions before a rule was created to define them as conflicting. If so, the User Conflicts panel displays appropriate status for the conflict: "Prevent" or "Allow with Rules" if the conflict was generated by a segregation-of-duties rule of either type, or "Pending" if it was generated by an Approve with Rules or Approval Required rule. Only the Pending status can be updated: a reviewer may approve or reject the conflict, either by itself (in an Action History panel) or along with others (in a Mass Update panel).

  Statuses recorded in these panels, however, do not take effect; instead, they are logged to ACTIVE Access Governor reports. Administrators would then use information from the reports to undertake "cleanup" — to make adjustments in

Oracle Applications such as end-dating responsibilities assigned to users affected by conflicts, or excluding a function from a responsibility in which it conflicts with another function.

To aid with cleanup, ACTIVE Access Governor enables users to simulate the effects of remedial actions — changes to the assignment of functions or menus to responsibilities — and carry out those actions if the simulation shows that they reduce conflicts.

- A user may be assigned responsibilities or functions after a rule is created to define them as conflicting. In this case, ACTIVE Access Governor automatically applies end dates if the control type is Prevent. If it is Allow with Rules, ACTIVE Access Governor automatically removes end dates.

  If the control type is Approve with Rules or Approval Required, the responsibility assignment does not take effect immediately, and ACTIVE Access Governor posts notification of the conflict to the designated reviewers. Similarly, when a new user is created, his assignments are analyzed for conflicts, and notifications are transmitted to designated reviewers.

  The reviewers' response to this notification updates responsibility end dates for the affected user: For an approval, the end dates are removed, permitting indefinite access to the conflicting elements. For a rejection, the end dates are made to match the start dates, preventing any access. Moreover, the user's status is updated in the ACTIVE Access Governor User Conflicts panel.

## Access Monitoring

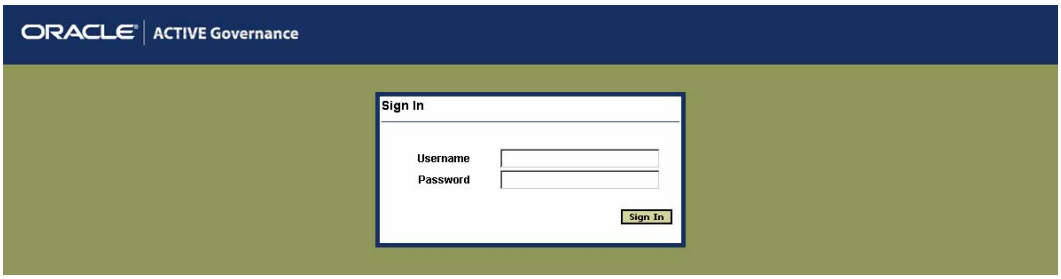
It is occasionally necessary to assign users temporary access to duties they do not ordinarily perform. The Access Monitoring feature of ACTIVE Access Governor implements a formal process of requesting extraordinary access to Oracle responsibilities or database tables, and requires requests to be approved by designated reviewers. Once approval is granted, Access Monitoring audits all actions taken by users at their temporary duties, and presents the audit data in a report.

## Starting ACTIVE Access Governor

ACTIVE Access Governor is a web-based application designed to run in Microsoft Internet Explorer. (It may run in other browsers as well, but only Internet Explorer is supported.) To start ACTIVE Access Governor:

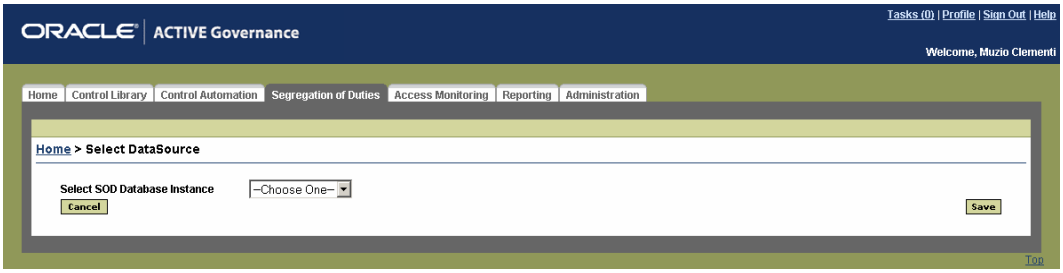
1. Open Internet Explorer.
2. In the Address field, type the URL for your instance of the ACTIVE Governance Platform, and press the Enter key. (Using standard Windows procedures, you can, of course, save the URL as a favorite or create a desktop shortcut to the URL.)

3 A Sign In dialog box appears. Type your user name and password in the appropriate fields, and click on the Sign In button.




4 The ACTIVE Governance Platform opens. In it, click on either of two tabs: Segregation of Duties to make use of the SOD features, or Access Monitoring to make access requests.

5 No matter which tab you select, a Select Datasource panel prompts you to choose among instances of databases that store Oracle Applications data, and to which access controls may be applied. Select a database instance in the list box and click on the Save button.




6 Depending on the tab you select, an Access Monitoring or SOD Rules panel opens. The database instance you selected applies to both; its name is displayed near the upper right corner of both. From within either, you can select another database instance: click on a Change link near the upper right corner of the panel to reopen the Select Datasource panel.

# Rights to Features

Each user is assigned a "primary application role" when his user account is created in the ACTIVE Governance Platform. Access Monitoring is unavailable to a role called SOD Approver, and another role called Auditor has only view rights to Access Monitoring; all other roles can both view and create requests for temporary access, for themselves or others. Among the features available from the Segregation of Duties tab:

- An SOD Super User, Rule Builder, Author, or Manager can view, create, and edit SOD rules and entity groups; run the background program that generates conflicts, and other background programs as well; and view, but not approve or reject, conflicts generated by SOD rules. These roles can view, create, and edit "global subscribers" (data groups, submenus, functions, operating units, or users who are exempt from SOD rules); create, edit, and view rules that simulate changes intended

to resolve conflicts; run simulations and view results; and run remediation (put simulated conflict resolutions to actual use).

- An SOD Approver can approve or reject conflicts generated by Approve with Rules or Approval Required SOD rules that name him as an owner or designate an approval group of which he is a member; he can judge such conflicts individually in the Action History panel or collectively in the Mass Update panel. He can also view SOD rules and entity groups, but cannot create or edit them. The SOD Approver has no access to background programs, global subscribers, simulation, or remediation.
- An Executive, Auditor, or System Administrator can view SOD rules, entity groups, global subscribers, and simulation rules, but cannot create or edit them; can view conflicts generated by SOD rules, but cannot approve or reject them; can run simulation, but not background programs or remediation.
- A User can view, create, and edit SOD rules. In all other respects, she has the same rights as an Executive, Auditor, or System Administrator.

The remainder of this manual is written without regard to the constraints imposed by primary application roles. As you read, keep in mind that you will be able to use only ACTIVE Access Governor features consistent with the role you have been assigned.

# Navigational Conventions

As you work with ACTIVE Access Governor, you'll make repeated use of the following features.

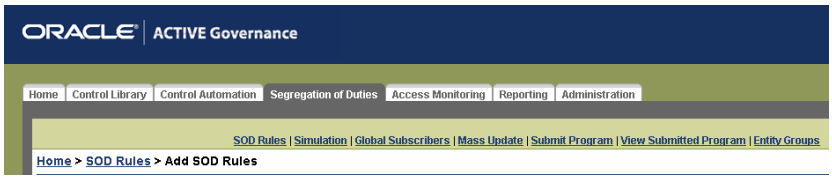
## Library Navigator

When you click on the Segregation of Duties tab, ACTIVE Access Governor opens a panel that displays a list of existing segregation-of-duties rules. From that panel, rules may be viewed, edited, or created.

However, you also have access to an assortment of related tasks, such as generating conflicts, approving (or rejecting) conflicts en masse, creating entity groups, uploading "seeded" rules, and others. A "Library Navigator" — a string of links near the top of the Segregation of Duties Rules panel (beginning with the phrase *SOD Rules* in the figure below) — provides access to these related tasks. Click on any of the links to open panels that support those tasks. The illustration shows a full set of Library Navigator links; however, you would see only the links appropriate to your role.

## Breadcrumbs

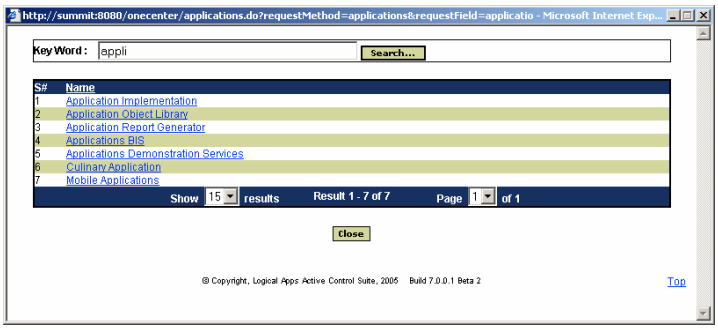
Once you have selected a link in the Library Navigator and begun to select options within the panel it opens, ACTIVE Access Governor leaves a trail of "breadcrumbs" — a string of links to each of the screens you have navigated to reach the screen you are using, culminating in the title of the current screen. (In the figure below, the bread-crumb trail begins with the word *Home*.) To return to an earlier screen, click on its link.




## Lists of Values

In some cases, a field may offer a set of values from which you can select. In these cases, the field displays an icon that looks like an ellipsis:

When you click on the icon, ACTIVE Access Governor opens a window in which you can produce a filterable list of values that may be entered in the field:




To use this feature:

1. In the Key Word field, type a string of text that matches text a value you want to select. Or, leave the Key Word field blank.
2. Click on the Search button. ACTIVE Access Governor returns values, the selection of which depends on your entry in the Key Word field:
   - If your Key Word entry includes text but excludes wild-card characters, ACTIVE Access Governor returns all values that begin with the text string. For example, if the search string is *appli*, return values might include *Appli-cation Implementation*.
   - If your Key Word entry includes a percent sign (%) as a wild-card character followed by text, ACTIVE Access Governor returns values with the text string at any position. For example, *%appli* would return *Culinary Application* as well as *Application Implementation*.
   - If you leave the Key Word field blank, ACTIVE Access Governor returns all possible values.

**3** Among the returned values, click on the one you want; ACTIVE Access Governor closes the search window and inserts the selected value in the LOV field.

## Sorting and Selecting Items in Lists

Several panels in ACTIVE Access Governor present lists of items — for example, of segregation-of-duties rules, conflicts generated by a rule, or function or responsibility groups:

| SOD Rule | Entity Type | Entities | Control Type | Priority | View User Conflict |
|---|---|---|---|---|---|
| Enter Journal * Post Journal | Function | Post Journals, Enter Journals | Approval Required | 1 | View |
| GL vs. Payables | Group - Function | Payables Group, GL Group | Approval Required | 3 | View |
| Invoice vs Invoice Approval | Function | Invoices, Invoice Approvals | Approval Required | 8 | View |
| Lease & Asset Categories | Function | Asset Categories, Lease | Allow with Rules | 9 | View |
| Receipts & Sales Orders | Function | Receipt, Sales Orders | Prevent | 1 | View |
| Supplier vs. Payments | Function | Payments, Suppliers | Approval Required | 3 | View |

Show 15 Results Result 1 - 6 of 6 Page 1 of 1

Each of these lists implements the following conventions:

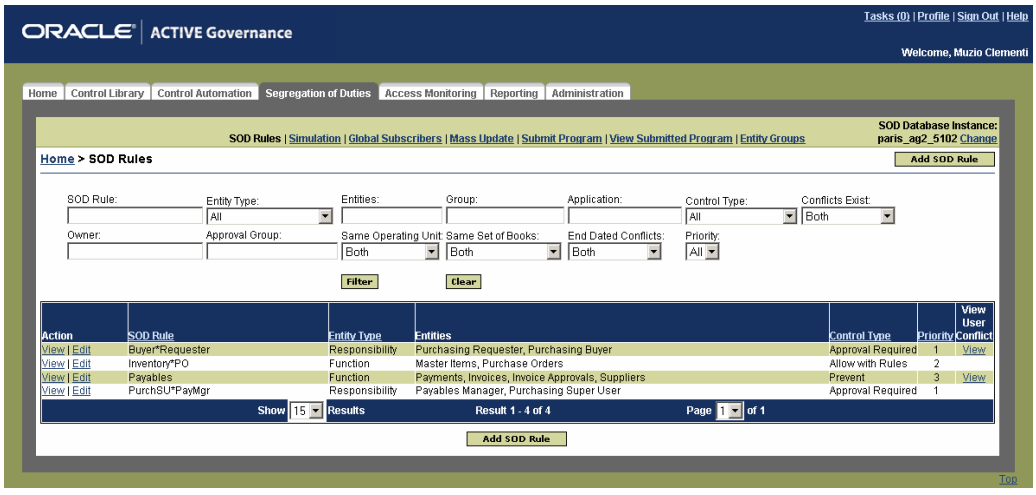
- In the header row, some column headings are underlined. Each of these is a sort column. When you click on one of these headings, the contents of its column are arranged in alphanumeric order; the values in other columns are arranged appropriately so that records remain intact.
- In the footer row, you can select a number in the Show Results list box to determine how many rows the list displays at once. The list entries are divided into pages, each of which consists of the number of rows you've chosen to display. To move to another page than the one currently displayed, click on its number in the Page list box. Or, click on the Next Page or Previous Page link, each of which is present only if there is a next or previous page to go to.

  In some cases, for performance reasons, two items are omitted from the footer — the Page list box and the Result field, which shows the number of items available for review in the current page and the numbers assigned to those items. In these cases, the list includes a Display Record Count check box; select it to make the omitted elements appear, or clear it to hide them once again.

# Chapter 2

# Defining Segregation-of-Duties Rules

When you click on the Segregation of Duties tab, ACTIVE Access Governor opens a panel titled SOD Rules, which lists summary descriptions of existing segregation-of-duties rules. For each rule, this panel displays the name, the type of entity it sets in conflict (responsibility, function, or group of either), the actual items it defines as being in conflict, its control type, its priority (with respect to other rules), and whether any Oracle users possess work assignments that violate the rule.




From this panel, you can view details of, add, or edit rules. Or, you can select Library Navigator links to upload "seeded" rules from an Excel spreadsheet, create entity groups for use in rules, or create global subscribers — data groups, submenus, functions, operating units, or users who are exempt from rules.

# Filtering the Display of SOD Rules

Using fields positioned above the list of SOD rules, you can limit the display of rules to those that satisfy filtering criteria. The following filters are always available:

- SOD Rule: Type a full SOD-rule name to display the single rule bearing that name. Type a fragment to display all rules whose names contain the fragment. Or, leave the field blank to display rules of any name.
- Entity Type: Select Function, Responsibility, Group—Function, or Group—Responsibility to find rules defining conflicts in the entity you select. Or select All to see rules for all types.
- Entities: Use this field only if you selected Function or Responsibility in the Entity Type field. Type the name of an entity to display rules in which that entity is set in conflict with another, a text fragment to display rules involving entities whose names contain the fragment, or no value to search for rules involving any entities.
- Group: Use this field only if you chose Group—Function or Group—Responsibility as Entity Type. If so, type a group name to find rules with that group as a base or conflicting entity, a text fragment to display rules involving groups whose names contain the fragment, or no value to search for rules involving any groups.
- Application: Type the name of an Oracle application to find rules in which conflicts involve responsibilities or functions belonging to that application. Type a text fragment to find rules involving all applications whose names include the fragment. Or, leave the field blank to see rules in which conflicts involve any application.
- Control Type: Select one of the control types (Prevent, Allow with Rules, Approve with Rules, or Approval Required) to search for rules of that type. Or select All to search for rules of all types.
- Conflicts Exist: Select Yes to find rules for which conflicts exist, No to find rules for which no conflicts exist, or Both to search for both types of rule.
- Owner: Type the full name of a workflow role to find rules for which that role is the owner, a text fragment to find rules for which the names of the owners contain that fragment, or no value see rules for which anyone is an owner.
- Approval Group: Type the name of an approval group to find rules for which the group is designated to judge conflicts. Type a text fragment to find rules that designate approval groups whose names contain that fragment. Or leave the box blank to see rules for which any (or no) approval group is designated.
- End Dated Conflicts: Select Yes to find rules configured to have end dates, No to find rules without end dates, or Both to search for both types of rule.
- Priority: Select a priority number to search for rules at that priority, or select All to search for rules at any priority.
- Same Operating Unit: Select Yes to find rules with a Same Operating Unit check box selected, so that each rule detects conflicts within individual operating units. Select No to find rules for which the check box is cleared, and so rules apply both within and across operating units. Or, select Both to find both types of rule.

The following filter is available only if you are currently connected to a data source that runs Oracle Applications Release 11. (See "Starting ACTIVE Access Governor" on page 3 for information on connecting to data sources.)

- Same Set of Books: Select Yes to find rules with a Same Set of Books check box selected, so that each rule detects conflicts within individual sets of books. Select No to find rules for which the check box is cleared, and so rules apply both within and across sets of books. Or, select Both to find both types of rule.

The following filters are available only if you are currently connected to a data source that runs Oracle Applications Release 12 (and exist only if you have installed ACTIVE Governance version 7.2.2):

- Same Ledgers: Select Yes to find rules with a Same Ledgers check box selected, so that conflicts are generated only if conflicting entities enable a user to access data in an individual ledger. Select No to find rules for which the Same Ledgers check box is cleared, and so conflicts are generated across ledgers. Or select Both find both types of rule.
- Same Access Sets: Select Yes to find rules with a Same Access check box selected, so that conflicts are generated only if conflicting entities enable a user to access data in ledgers belonging to a single data access set. Select No to find rules for which the check box is cleared, and so conflicts can be generated across data access sets. Or select Both to find both types of rule.
- Ignore Read Only: Select Yes to find rules with an Ignore Read Only check box selected, so that conflicts are generated only if conflicting entities would grant write access to ledger data. Select No to find rules for which the check box is cleared, and conflicts can be created if ledger access is read-only or write. Or select Both to find both types of rule.

Specify filtering criteria by entering complementary values in any combination of these fields. Then do either of the following:

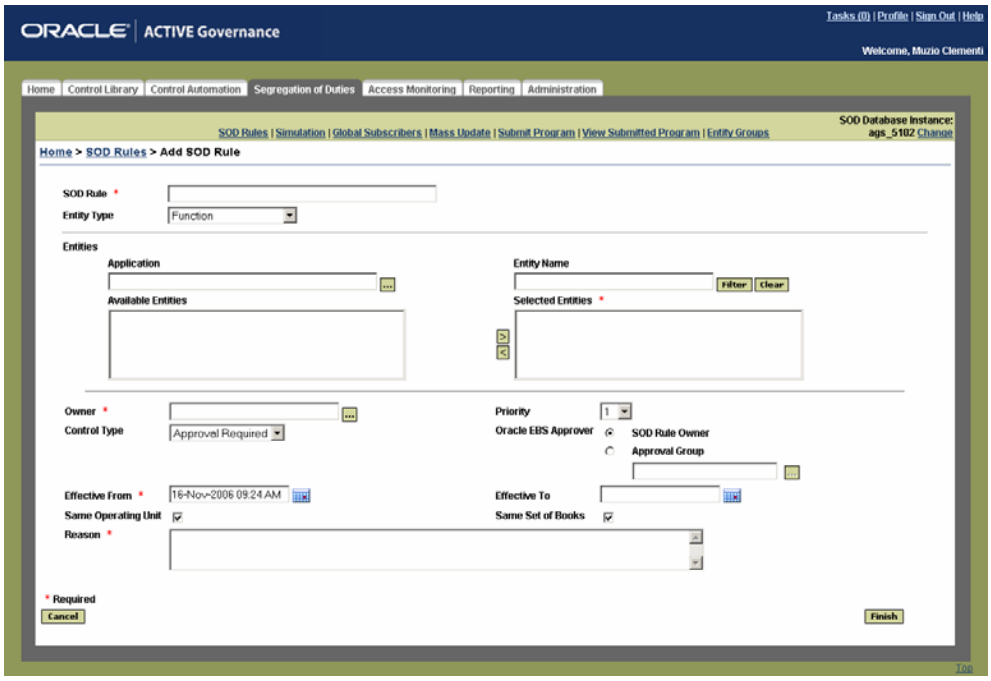
- To display only SOD rules that satisfy filtering criteria, click on the Filter button.
- To discard filtering criteria and redisplay all SOD rules, click on the Clear button.

# Creating SOD Rules Manually

As you create SOD rules, consider limiting the number that are active, so they do not generate an overwhelming volume of conflicts. A typical strategy is to run a set of rules that define conflicts you determine to be most important, then clean up those conflicts before running another set of rules. (A rule is inactive if the date on which you generate conflicts falls outside of effective dates specified for the rule. To reactivate inactive rules, you can edit their effective dates and regenerate conflicts.)

If you select the Allow with Rules or Approve with Rules control type for an SOD rule, you must associate it with at least one rule created in Form Rules, an "embedded agent" that runs in Oracle Applications. Before creating such an SOD rule, ensure that you have configured the form rules you want to associate with it.

To create an SOD rule, click on either of two Add SOD Rule buttons, near the bottom center or upper right of the SOD Rules panel. An Add SOD Rule panel opens:




## Starting the Rule

Begin to create an SOD rule by naming it and selecting the items it sets in conflict:

1. Type a name for the rule in the SOD Rule field.
2. Make a selection in the Entity Type list box. To define a conflict between individual items, choose Responsibility or Function. To define a conflict between entity groups, choose Group–Responsibility or Group–Function.
3. Populate the Available Entities field with a selection of items that may be included in a conflict definition.

   If you chose Group–Responsibility or Group–Function in the Entity Type list box, the Available Entities field instantly displays a list of entity groups configured for your system. If you chose Responsibility or Function in the Entity Type list box, you must generate a list of entities in the Available Entities field. To do so, select an application in the Application field, enter a filtering value in the Entity Name field, or both, and then click on the Filter button.

   - When you select an application name in the Application field (or, for functions, the value *No Associated Application*), the Available Entities field lists only items that belong to the application you select (or to no application). Otherwise, the field lists items without regard to application.
   - When you enter a text string in the Entity Name field, the Available Entities field lists items whose names begin with that text string. (The percent sign serves as a wild-card character.) Although this capability is typically used for filtering responsibilities or functions, it can also filter responsibility or function groups.

When you load items into the Available Entities field, ACTIVE Access Governor presents a count of the items, which appears next to the label for the Available Entities field. If the count exceeds 1,000, you should filter the items in the Available Entities field; otherwise, performance may suffer.

4 Choose items you want to include in the conflict definition. In the Available Entities field, highlight one or more items. Then click on the > button to move them to the Selected Entities field. (To rescind a selection, highlight one or more entries in the Selected Entities field, and then click on the < button to return them to the Available Entities field.)

In either field, you can select one or more items at a time. To select a single item, click on it. To select a continuous set of items, click on the first one, hold down the Shift key, and click on the last one. To select a discontinuous set, hold down the Ctrl key as you click on items.

5 If you are selecting individual responsibilities or functions, repeat steps 3 and 4 any number of times to select among entities that earlier application or name filters have excluded. Within a given rule, you can select entities belonging to any combination of applications, but all the entities must be of one type.

If you click on the Clear button, you remove the contents of the Application, Entity Name, and Available Entities fields. As you configure new application or name filters, or if you click on the Clear button, the contents of the Selected Entities field remain.

## Finishing the Rule

To complete the SOD rule, select a control type, owner, and other remaining values:

1 In the Owner list of values, select the Oracle workflow role that assumes principal authority for this rule. As a practical matter, the owner approves or rejects individual conflicts generated by the SOD rule, if the rule is of the Approval Required or Approve with Rules control type, and if no approval group is designated (see step 4).

For the Owner LOV to offer an up-to-date selection of workflow roles, you must run a background program, called Populate WF Roles Table, each time new roles are added in Oracle Applications. See "Background Programs" (page 49).

2 In the Priority field, select a number, from 1 to 10, that reflects the importance of this rule in relation to others. (Your company should determine whether it considers 1 or 10 the highest priority, and then enforce consistent usage.) You can use the priority value to filter the rules displayed in the SOD Rules panel, as well as the results returned by some SOD reports.

3 In the Control Type list box, select the control type you want to apply to the rule — Prevent, Allow with Rules, Approve with Rules, or Approval Required. (See page 2 for definitions of control types.)

4 If you select the Approve with Rules or Approval Required control type, use a set of fields, labeled Oracle EBS Approver, to determine who approves or rejects conflicts generated by the rule. (If you select the Prevent or Allow with rules con-

trol type, these fields disappear, because conflicts generated by rules with those control types are not subject to approval.)

- To have the rule owner (selected in step 1) review conflicts, click on the SOD Rule Owner radio button.
- To designate an approval group to review conflicts, click on the Approval Group radio button, and then select a group in the LOV immediately beneath the Approval Group radio button. (Approval groups are created in Flow Rules, an "embedded agent" that runs within Oracle Applications. See its user's guide for more information.)

**Note**
Both SOD rule owners and members of approval groups are Oracle workflow roles. When an ACTIVE Governance user is created, he is associated with an "OracleApps User" — a workflow role. He is also assigned one of nine primary application roles, of which only SOD Approver has rights to update the status of conflicts. It is possible for the author of an Approve with Rules or Approval Required SOD rule to select an owner, or an approval group with members, whose primary application roles deny them the right to approve or reject conflicts. If so, status for those conflicts cannot be assigned. As you write SOD rules, take care to select owners, or approval groups with members, that correspond to ACTIVE Governance users at the SOD Approver role.

**5** Set effective dates. The rule becomes active if the Generate User Conflicts program is run on a date that falls between dates you enter in the Effective From and Effective To fields. Do one of the following:

- The Effective From field defaults to the date and time you create the rule; the Effective To field is blank. Retain these values to have the rule take effect the next time Generate User Conflicts is run and remain in effect indefinitely.
- Set new values. Edit the date and time manually in either field (use the format *DD-M0n-YYYY HH:MM AM/PM*), or click on the icon next to a field and select a date in the pop-up calendar that appears.

**6** A set of check boxes is positioned beneath the effective-date fields. The assortment depends upon your ACTIVE Governance version (the last three boxes are available only if you have installed version 7.2.2) and upon the version of Oracle Applications that runs on the data source to which you are currently connected:

- Same Operating Unit: Select the check box to have the rule generate a conflict only if a user's responsibility assignments would grant access to base and conflicting entities within an individual operating unit; clear it to have the rule apply across operating units as well. This check box appears regardless of Oracle Applications version.
- Same Set of Books: Select the check box to have the rule apply only if a user would have access to base and conflicting entities within an individual set of books; clear it to have the rule apply across sets of books as well. This check box appears if you are connected to an Oracle Applications 11 instance.

- Same Ledgers: Select the check box to have the rule generate a conflict only if the conflicting entities would enable a user to access data in an individual ledger (because the ledger is included in data access sets assigned to responsibilities involved in the conflict). Clear the check box to have the rule generate conflicts across ledgers. This check box appears if you are connected to an Oracle Applications 12 instance.
- Same Access Sets: Select the check box to have the rule generate a conflict only if the conflicting entities would enable a user to access data in ledgers belonging to a single data access set (because that access set is assigned to responsibilities involved in the conflict). Clear the check box to have the rule generate conflicts across data access sets. This check box appears if you are connected to an Oracle Applications 12 instance.
- Ignore Read Only: Select the check box to have the rule generate a conflict if the conflicting entities would grant write access to ledger data, but not when either entity would grant read-only access (because data access sets are configured to grant read-only access). Clear the check box to have the rule generate conflicts regardless of whether ledger-data access is read-only or write. This check box appears if you are connected to an Oracle Applications 12 instance.

As you set the Same Access Sets and Same Ledgers check boxes, consider how they interact. Typically, if you select one, you would not select the other.

For example, suppose an SOD rule defines a conflict between two functions, which are available through distinct responsibilities. Each responsibility is associated with its own data access set, and both data access sets contain a particular ledger. Now suppose a user is assigned the two responsibilities:

- If Same Ledgers is selected but Same Access Sets is not, a conflict would be generated, because the user would be able to perform the conflicting functions in the ledger that belongs to both data access sets.
- If Same Access Sets is selected, no conflict would be generated even if Same Ledgers were also selected, because each function would provide access to the commonly held ledger through a distinct data access set. In this case the Same Access Sets selection would effectively "override" the Same Ledgers setting. (Although a responsibility can have only one data access set, an access set can be associated with more than one responsibility. So a conflict is generated if Same Access Sets is selected, the two functions are accessed through distinct responsibilities, but a single data access set is linked to both responsibilities.)

However, suppose that the two functions are available through a single responsibility. A responsibility can have only one data access set, so in this case a potential conflict would necessarily involve only one data access set, and so the settings of both the Same Access Sets and Same Ledgers check boxes would be irrelevant.

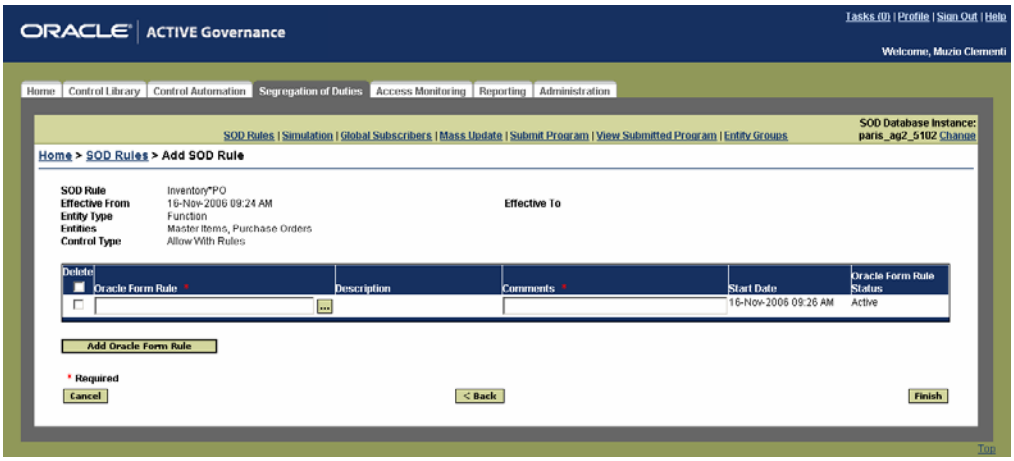
**7** In the Reason field, explain the business risk addressed by this SOD rule.

**8** If you selected the Prevent or Approval Required control type, click on the Finish button. The SOD Rules panel reappears, with a listing for the new rule. If you selected the Allow with Rules or Approve with Rules control type, see the next section, "Linking the SOD Rule to Form Rules."

## Linking the SOD Rule to Form Rules

If you assigned the Allow with Rules or Approve with Rules control type to an SOD rule, you must associate it with one or more rules written in Form Rules. (If you chose Prevent or Approval Required, this section does not apply.)

1 With the selection of the Allow with Rules or Approve with Rules control type, the Finish button in the Add SOD Rule panel changes to read "Next." After completing fields in the initial panel, click on the Next button; a second Add SOD Rule panel opens:




2 Click the Add Oracle Form Rule button and complete fields in the row you create:

- In the Oracle Form Rule LOV, select a form rule that addresses the conflict. (You can select only active form rules.)
- The Description field displays the description configured for the form rule you've selected. This value is read-only.
- In the Comments field, explain briefly why you are attaching the form rule to the SOD rule.
- The Start Date field displays the date on which you establish a link between the form rule and SOD rule. You cannot change it.
- The Oracle Form Rules Status field accepts no input and displays the status of the form rule associated with the SOD rule. Initially, this is Active, but the rule may later be inactivated in the Form Rules application, and this field displays current status when the SOD rule is reopened for viewing or editing.

3 Optionally, repeat step 2 any number of times to select additional form rules.

4 To delete form rules from the grid, select the Delete check box for each of the form rules you no longer want. Ensure the Delete check box is cleared for each form rule you want to retain. To mark all form rules for deletion, or to ensure that all rules are retained, select or clear the Delete check box in the header row.

5 Click on the Finish button. The SOD Rules panel reappears, with a listing for the new rule.

## Viewing, Copying, and Editing SOD Rules

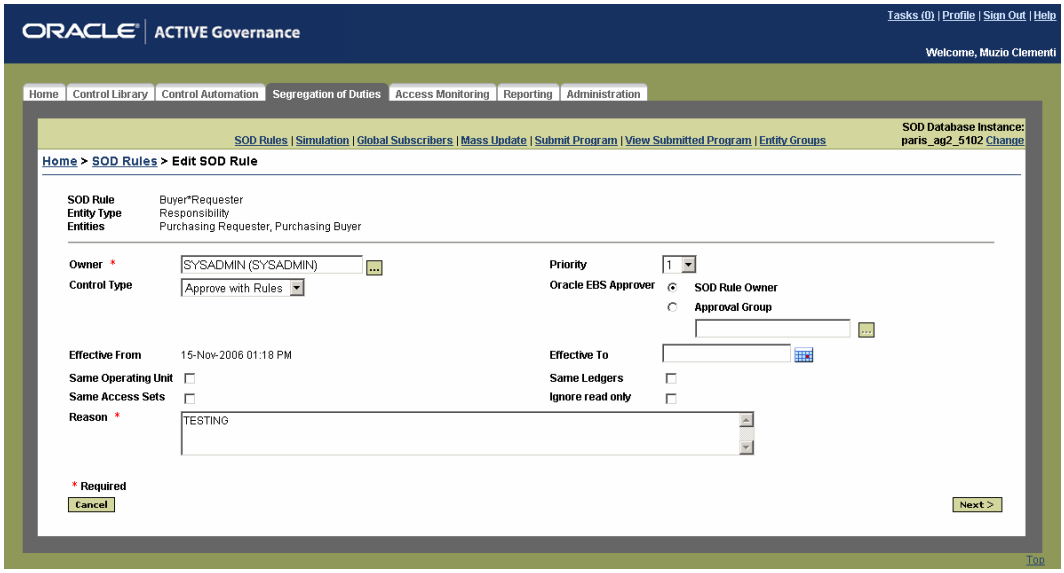
You can review the configuration details for an existing rule, edit some details, or copy the rule as a template for the creation of a new rule. Open one of three panels; each is similar to the Add SOD Rule panel, but displays the values already set for a rule you select; procedures for modifying these values, where modifications are permitted, are the same as those described for the Add SOD Rule panel (see "Creating SOD Rules Manually," beginning on page 11).

To view the settings for a rule, open the SOD Rules panel and, in the Action column, click on the View link for the rule you want to see. A read-only View SOD Rule panel opens. If the rule's control type is Allow with Rules or Approve with Rules, the panel also displays a ± icon labeled *Oracle Form Rules*. Click on the + icon to display information about form rules associated with the SOD rule, or click on the – icon to hide the information. To return to the SOD Rules panel, click on the Cancel button.

To make a copy, choose the rule that is to serve as the original, open its View SOD Rule panel, and click on the Copy SOD Rule button. A Copy SOD Rule panel opens:

- The copy takes these values from the original: entity type, selected entities, control type, priority, owner, approval group, reason, and settings for the Same Operating Unit and other check boxes (the boxes vary depending on the version of Oracle Applications to which you are connected). The Effective From field is set to the date and time you make the copy, and the Effective To field is blank.
- You must supply a name for the new rule in the SOD Rule field.
- You cannot change the entity type, but you can add to or remove responsibilities, functions, or groups inherited from the copied rule, or edit other values.
- If the control type is Allow with Rules or Approve with Rules, the new version does not inherit form rules from the original, so you must click on the Next button to add at least one form rule to the new version of the SOD rule.

To edit a rule, open the SOD Rules panel and, in the Action column, click on the Edit link for the rule you want to alter. This opens an Edit SOD Rule panel.



In this panel:

- You can modify the owner, priority, approval group, effective-to date, reason, and settings for the Same Operating Unit and other check boxes (as before, the boxes you see depend on the version of Oracle Applications to which you are connected). If the rule has generated no conflicts, you can also change the control type; if the rule has generated conflicts, the control type cannot be edited.
- Fields that display other values are read-only.
- If the control type is Allow with Rules or Approve with Rules, you can click on the Next button to add form rules to the SOD rule, or delete those already selected.

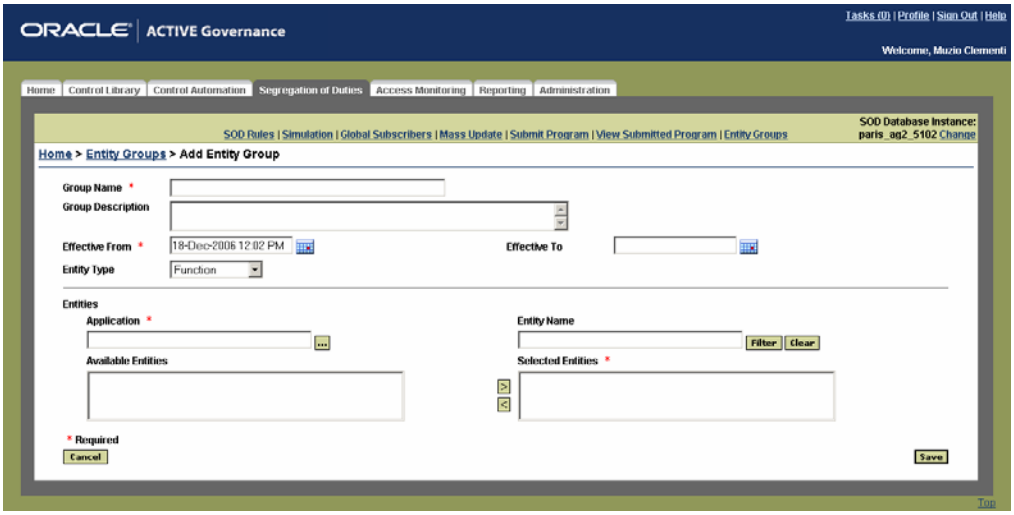
# Working with Entity Groups

You can collect responsibilities or functions into "entity groups." Then, using the Group–Responsibility or Group–Function entity type as you define SOD rules, you can identify two or more groups that should not be assigned simultaneously to individual Oracle Applications users. In such a rule, each item (responsibility or function) in a group is considered to conflict with every item in other groups named in the rule, but not with items in its own group. A group may contain a single item, or a number of items whose names constitute a comma-delimited string of up to 4,000 characters.

## Creating Groups

To create an entity group:

1. Click on Entity Groups in the Library Navigator. An Entity Groups panel then displays entries for all existing groups. (It's illustrated on page 20.)
2. Click on the Add Entity Group button near the bottom center of this panel. An Add Entity Group panel appears:




3. Type a unique name for the group in the Group Name field Do not use a comma in the name.

4. In the Group Description field, type a brief explanation of the group. (For example, state the reason functions or responsibilities are included in the group.)
5. By default, the Effective From field is set to the date and time at which you create the group, and the Effective To field is blank. Do one of the following:
   - Retain these values to have the group take effect immediately and remain in effect indefinitely.
   - Select a new start or end value manually: Edit the date and time in either field (use the format *DD-Mon-YYYY HH:MM AM/PM*).
   - Click on the icon next to a field and select a date in the pop-up calendar that appears.
6. In the Entity Type list box, select Function or Responsibility.
7. Choose an item to include in the group.

   First, generate a list of entities in the Available Entities field: Select an application in the Application field, enter a filtering value in the Entity Name field, or both, and then click on the Filter button.

   - When you select an application name in the Application field (or, for functions, the value *No Associated Application*), the Available Entities field lists only items that belong to the application you select (or to no application). Otherwise, the field lists items without regard to application.
   - When you enter a text string in the Entity Name field, the Available Entities field lists items whose names begin with that text string. (You can use the percent sign as a wild-card character.)

     When you load items into the Available Entities field, ACTIVE Access Governor presents a count of the items. It appears next to the label for the Available Entities field. If the count is greater than 1,000, you should filter the items in the Available Entities field more narrowly; otherwise, performance may suffer.
   - If you click on the Clear button, you remove the contents of the Application, Entity Name, and Available Entities fields. The contents of the Selected Entities field remain.

   From the list of selections you've generated in the Available Entities field, choose one (click on it), and click on the > button to move it to the Selected Entities field.
8. Choose additional items to include in the group. It may contain functions or responsibilities, but not a mixture of the two. The entities in a group may belong to any selection of applications.

   If you wish to rescind a selection, click on its entry in the Selected Entities field, and then click on the < button to return it to the Available Entities field.
9. When you finish selecting responsibilities or functions, click on the Save button. Once a group is saved, only its name, description, and end date can be changed.

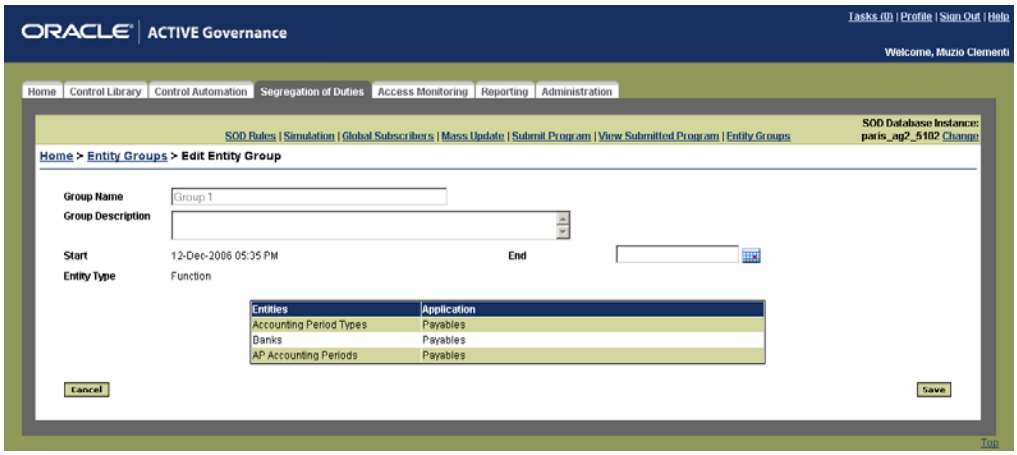
## Viewing Groups

After you save a group you have created, the Entity Groups panel reappears, adding a listing for the new group to its display. The listing for each group displays its name, the entity type of its members, its description, and its start and end dates.


From this panel, you can view the configuration details for a group, including the responsibilities or functions that belong to it, by clicking on either of two links in its listing. One of the links enables you to edit some of those configuration details; the other enables you to copy the group as a starting point for creating a new group.

## Editing Groups

To edit a group, click on the Edit link in the Action column of its entry in the Entity Groups panel. An Edit Entity Group panel opens:

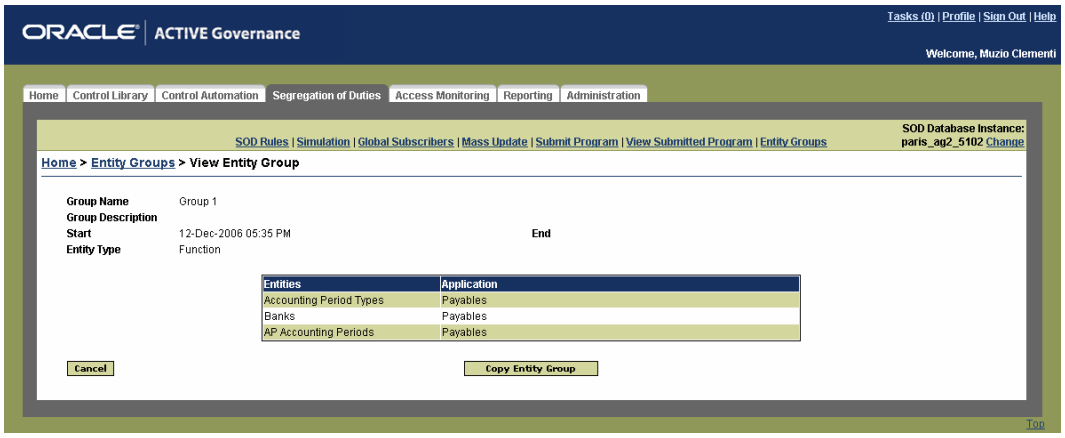



Although you can view all the elements that make up the group, you can edit only the group name, description, and end date. (For each, click in the appropriate field and enter a new value). The group name can be edited only if the group has not been used in a rule; once the group has been, the group name field becomes read-only. You cannot add responsibilities or functions to, or remove them from, the group.

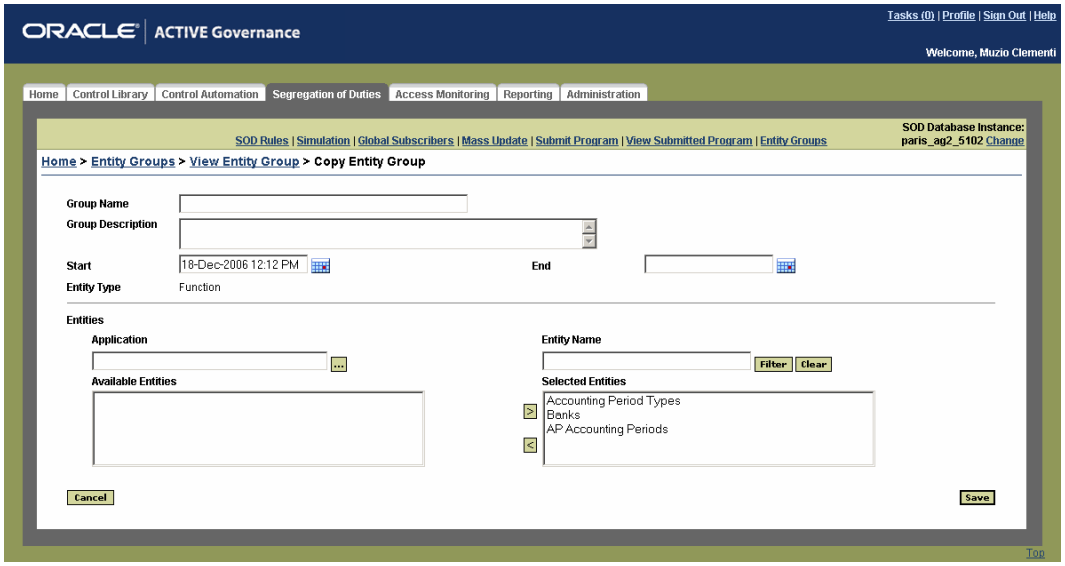
## Copying Groups

To view a read-only display of the configuration details of an entity group, or to copy the group, click on the View link in the Action column of its entry in the Entity

Groups panel. A View Entity Group panel opens; it's similar to the Edit panel, except that all of its fields are read-only and it includes a Copy button near its bottom center:




When you click on the Copy Entity Group button, a Copy Entity Group panel opens. It's similar to the Add Entity Group panel, except that its Selected Entities field contains responsibilities or functions inherited from the group you copied, and its Entity Type field is set appropriately to Responsibility or Function.




To create a new group, complete the remaining fields; use the procedure described in "Creating Groups" (page 18). You can add to, or remove, responsibilities or functions you inherited from the group you copied, but you cannot change the entity type.

# Creating Global Subscribers

You can specify users who are exempt from SOD rules as they detect conflicts that exist at the moment the Generate User Conflicts background program is run. You can also exempt submenus, functions, data groups, and operating units from SOD rules as they both detect existing conflicts and continue to uncover conflicts as responsibilities are assigned after the Generate User conflicts program is run. Items designated for exclusion (or, in one case, inclusion) are called global subscribers.

You may configure global subscribers to ensure that query-only access to Oracle Applications features does not trigger rules, even when standard access would.

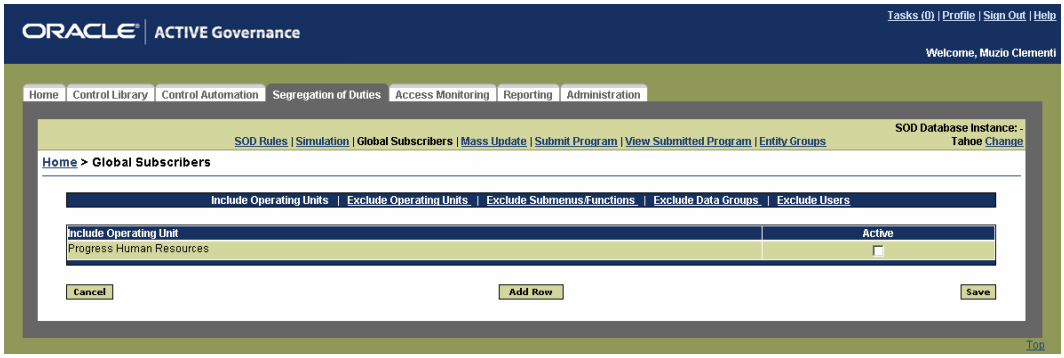
Or, you may use global subscribers to make the cleanup process more manageable (*cleanup* being the term for the resolution of conflicts that exist because responsibilities or functions were assigned to users before SOD rules were written to define them as conflicting). The number of conflicts found by Access Governor is typically large, so you can create global subscribers to generate fewer conflicts. For example, you can exempt users who may account for disproportionately large numbers of conflicts (such as those with super user responsibilities), or you can apply rules only to operating units in most immediate need of cleanup. After generating and resolving one set of conflicts, you can deactivate some or all of the global subscribers to generate and clean up a new set of conflicts, continuing until all pre-existing conflicts are resolved.

To create global subscribers, click on the Global Subscribers link in the Library Navigator. Then, in a Global Subscribers panel, click on the link for a subscriber type.

## Operating Units

You can select operating units either to be included in, or excluded from, SOD rule processing. These selections apply to operating units assigned to users, responsibilities, applications, or sites through use of the MO: Operating Unit profile option in the system administrator responsibility. The option may be set simultaneously at any or all of these levels, and the active setting is the one at the most narrowly focused level (first user, then responsibility, then application, then site).

**1** In the Global Subscribers panel, click on the Include Operating Units link or the Exclude Operating Units link:




**2** Click on the Add Row button. A new row appears, displaying a list box:


**3** In each row you create, select an operating unit. It is permissible for entries to exist in both the Include and Exclude panels, but entries should be active (see the next step) in only one panel at a time.

4 Select or clear the Active check boxes at the right of the entries:

- If Active check boxes are selected in the Include panel, the corresponding operating units are eligible for rule processing and all others are excluded.
- If Active check boxes are selected in the Exclude panel, the corresponding operating units are excluded from rule processing, and all others are included.

Do not select Active check boxes simultaneously in both panels.

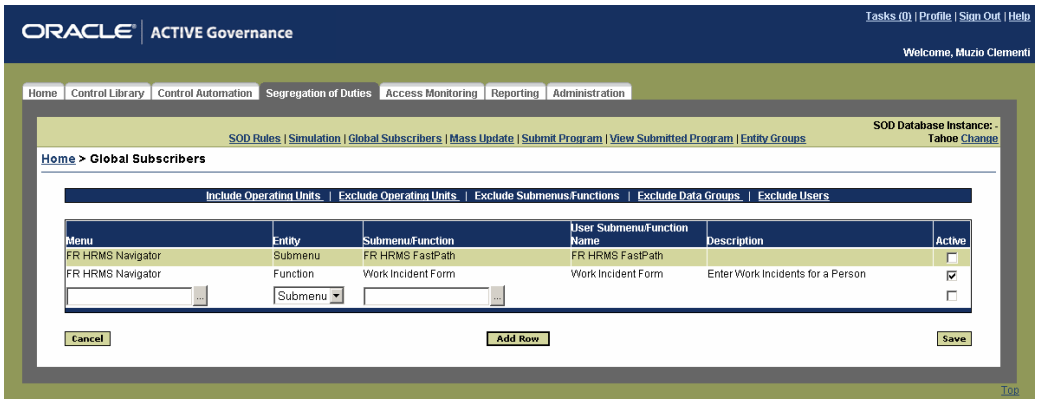
5 Click on the Save button.

## Submenus

A submenu under one menu may provide query-only access to functions, even as the same submenu under another menu provides write access to the same functions. A rule that includes such a function would trigger conflicts for all instances of the function — rightly when a user has write access, but falsely for query-only access.

To exclude the query-only functions from rule processing, create submenu subscribers:

1 In the Global Subscribers panel, click on the Exclude Submenus/Functions link. Then click on its Add Row button:




2 Make selections in the Menu, Entity, and Submenu/Function fields. ACTIVE Access Governor supplies corresponding values in the Name and Description fields. This exclusion feature recognizes only direct parent-child relationships:

- To exclude a function, select Function in the Entity list box. Select the function and its immediate parent submenu in the Submenu/Function and Menu fields.
- To exclude a submenu, select Submenu in the Entity list box. Then specify the submenu and its immediate parent menu in the Submenu/Function and Menu fields. To exclude a submenu is to exclude all functions on that submenu.

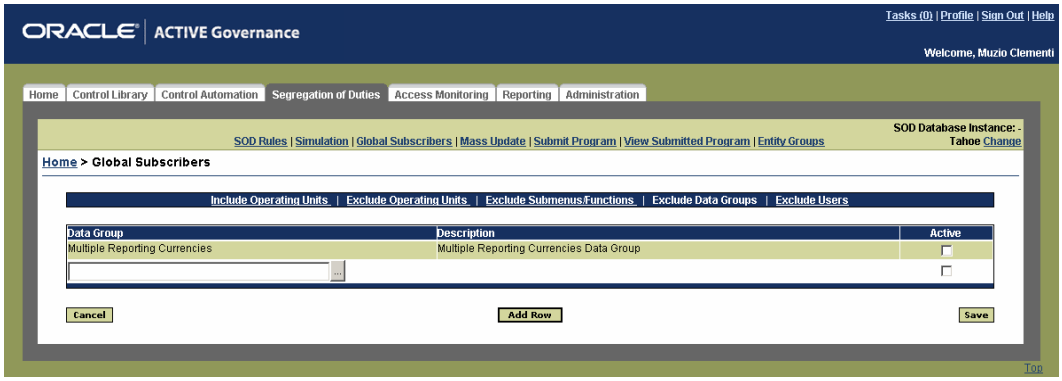
3 Select the Active check box to exempt the query-only instance of the function or functions from SOD rules, while leaving write-enabled instances subject to rules. Or, clear the check box to deactivate the exemption.

4 Click on the Save button.

## Data Groups

ACTIVE Access Governor includes the capability to evaluate SOD rules against data groups. To eliminate false conflicts that can occur when custom responsibilities are assigned to query-only data groups, you can exempt data groups from rule processing:

1 In the Global Subscribers panel, click on the Exclude Data Groups link. Then click on its Add Row button:




2 In the Data Group list of values, select the group that is to receive the exclusion.

If a description was written when the group was created, it appears by default in the Description field. If no description was written, the field remains blank. The Description field does not accept direct input.

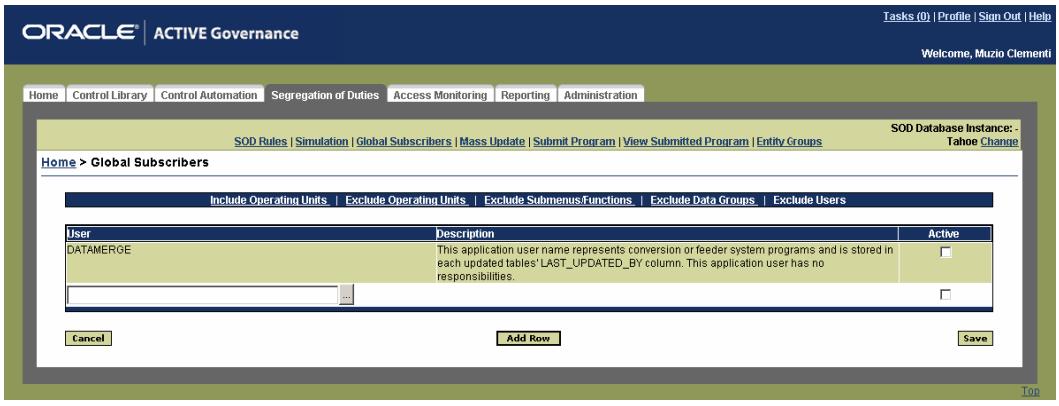
3 The Active check box is selected by default. Leave it selected for the exclusion to take effect. Clear it (click on it so that no check mark appears) to reserve an exclusion for the group, but not have it take effect at present.

4 Click on the Save button.

## Users

You can exclude individual users from SOD rule processing:

1 In the Global Subscribers panel, click on the Exclude Users link. Then click on its Add Row button.



2 In the User list of values, select the ID of the user who is to receive the exclusion.

If a description of the user was written when the user ID was created, it appears by default in the Description field. If no description was written when the user ID was created, the field remains blank. The Description field does not accept direct input.

3 The Active check box is selected by default. Leave it selected for the user exclusion to take effect. Clear it (click on it so that no check mark appears) if you want to reserve a user exclusion for the user, but not have it take effect at present.

4 Click on the Save button.

When you are finished creating global subscribers, click on the SOD Rules link in the "breadcrumbs" trail to return to the SOD Rules panel.

# Uploading SOD Rules from a Spreadsheet

Rather than create SOD rules one at a time, you can select rules in a Microsoft Excel spreadsheet, edit them to contain values appropriate for your site, and upload them at once. Before you start, be sure you have created approval groups if you intend to designate them as conflict approvers for the rules you upload. You also need to know the name of the ODBC driver that enables you to connect to your Oracle system.

To prepare the spreadsheet for uploading:

1 Open the LA_SOD spreadsheet.

| Conflict Name | Entity Type | Application | User Function Name | Conflicting Application | Conflicting Function Display Name | Control Type | Approver | F |
|---|---|---|---|---|---|---|---|---|
| Requisitions*Purchase Orders | Function | Oracle Purchasing | Requisitions | Oracle Purchasing | Purchase Orders | Approval Required | SYSADMIN | Buyers should not process their own process contols. |
| Requisition Summary*Purchase Orders | Function | Oracle Purchasing | Requisition Summ | Oracle Purchasing | Purchase Orders | Approval Required | SYSADMIN | Buyers should not process their own process contols. |
| Requisitions*PO Summary: Create New PO | Function | Oracle Purchasing | Requisitions | Oracle Purchasing | PO Summary: Create New PO | Approval Required | SYSADMIN | Buyers should not process their own process contols. |
| Requisitions*Releases | Function | Oracle Purchasing | Requisitions | Oracle Purchasing | Releases | Prevent | SYSADMIN | Buyers should not process their own process contols. |
| Requisition Summary*PO Summary: Create N | Function | Oracle Purchasing | Requisition Summ | Oracle Purchasing | PO Summary: Create New PO | Prevent | SYSADMIN | Buyers should not process their own process contols. |
| Requisition Summary*Releases | Function | Oracle Purchasing | Requisition Summ | Oracle Purchasing | Releases | Prevent | SYSADMIN | Buyers should not process their own process contols. |
| Requisitions*AutoCreate Documents | Function | Oracle Purchasing | Requisitions | Oracle Purchasing | AutoCreate Documents | Prevent | SYSADMIN | Buyers should not process their own process contols. |
| Requisition Summary*AutoCreate Document | Function | Oracle Purchasing | Requisition Summ | Oracle Purchasing | AutoCreate Documents | Allow with Rules | SYSADMIN | Buyers should not process their own process contols. |
| PO Summary: Create New PO*Receipts | Function | Oracle Purchasing | PO Summary: Cre | Oracle Purchasing | Receipts | Allow with Rules | SYSADMIN | Receiving personnel should never ha orders or to change receiving contro have the ability to do any receiving or |
| Releases*Receipts | Function | Oracle Purchasing | Releases | Oracle Purchasing | Receipts | Allow with Rules | SYSADMIN | Receiving personnel should never ha orders or to change receiving contro have the ability to do any receiving or |
| AutoCreate Documents*Receipts | Function | Oracle Purchasing | AutoCreate Docu | Oracle Purchasing | Receipts | Allow with Rules | SYSADMIN | Receiving personnel should never ha orders or to change receiving contro have the ability to do any receiving or |

2 In the upper left corner of the Access Load Values sheet, provide the ODBC driver name, connect string, Apps user name, and Apps password.

3 Click on the Update Data button. The spreadsheet is populated with up to 65,536 rows of SOD rule data. (Owing to Excel limitations, this is the maximum number.)

4 Review the rules and select those you want to upload: In the Load column, select *Y* for rules you want or *N* for those you don't want.

5 Edit values in the following columns as appropriate for the rules you are uploading: Control Type, Approver, Reason, Same Operating Unit, and Same Set of Books. (Note that if the Same Operating Unit or Same Set of Books value is null, the upload operation will fail.) You cannot change the values in other columns.

   In particular, SYSADMIN is the default conflict approver for all SOD rules. For each rule, change this value to an appropriate approver.

6 On the Tools menu, click Create CSV for Access Governor. In response to prompts, enter a file name (of 30 or fewer characters) and location (which, in conformance with UNIX conventions, must end in a slash). Click OK to save the file.

**Note**
The Create CSV for Access Governor option appears in the Excel Tools menu only if the macro security level for Excel is set to low. To effect this setting, click on Tools in the Excel menu bar, then on Options in the Tools menu. In the Options window, click on the Security tab. In the Security panel, click on the Macro Security button. A Security window opens; in its Security Level panel, click on the Low radio button. Then close the Security and Options windows — click on the OK button in each.

To deploy the CSV file you've prepared, log on to the database server as an admin user and upload the file to the UTL directory. Then run the Load SOD Conflict Rules background program; for the procedure, see "Background Programs" (page 49).

# Chapter 3

# Generating and Reviewing Conflicts

Once SOD rules are defined, the next step is to generate conflicts — to search users' work assignments for rule violations. You can then select a rule and display its conflicts in a User Conflicts form, together with the user affected by each conflict, and its status.

For conflicts generated by Prevent or Allow with Rules SOD rules, the status is set to Prevent or Allow with Rules, respectively, and stays that way. For Approve with Rules or Approval Required conflicts, status begins at Pending, but may be updated to Approved or Rejected. Only users designated by an SOD rule can update status for the conflicts it generates: a member of an approval group, if one has been selected for the rule, or if not, the owner of the rule. Approvers may set the status of conflicts one at a time in an Action History form or any number at once in a Mass Update form.

However, the assignment of status in either form simply adds information to reports. It neither grants, denies, nor prevents access to conflicting responsibilities or functions. The actual enforcement of SOD rules is carried out in either of two ways (which are described briefly as follows, but discussed in detail in Chapter 4):

- Some users will have been given access to functions or responsibilities before a rule was in force to define them as conflicting. For these conflicts, administrators use information from ACTIVE Access Governor reports to implement status decisions manually in Oracle Applications.
- Other users may provisionally be assigned responsibilities or functions after a rule was in force to define them as conflicting. For these conflicts, ACTIVE

Access Governor adds functionality to the Oracle Users form so that SOD rules are applied automatically as responsibilities are assigned to users.

# Generating User Conflicts

A Generate User Conflicts background program evaluates all active SOD rules (all that are not end-dated) and produces a "snapshot" — a set of conflicts detected by the active rules at the moment the program is run. It also saves the prior snapshot to an archive table.

The SOD rules that contribute to the snapshot continue to identify conflicts as, subsequently, new Oracle users are added or changes are made to existing users' responsibility assignments. If SOD rules are added or edited, the changes do not take effect until a new snapshot is taken, so the Generate User Conflicts program should be run whenever SOD rules change.

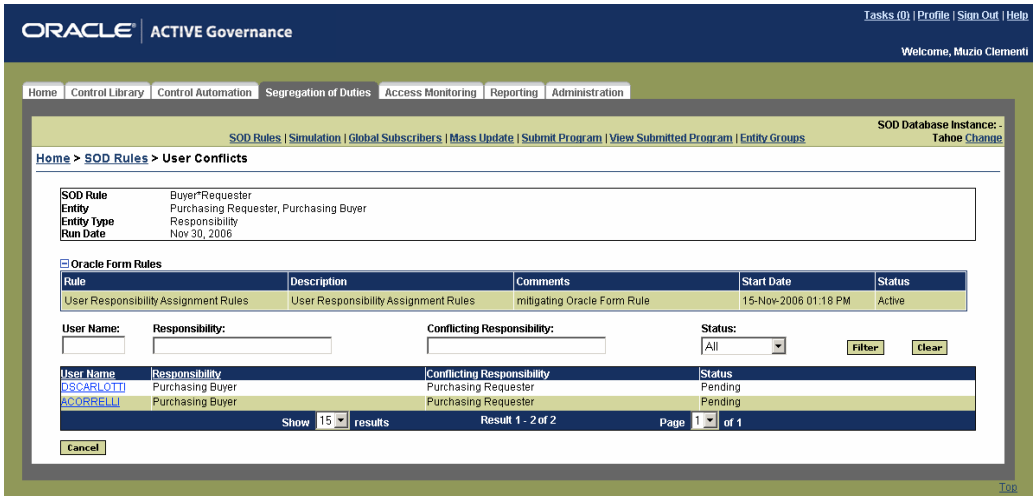
Alterations in the assignment of functions to responsibilities in Oracle also have the potential to resolve existing conflicts or create new conflicts. When they occur, however, you can run either Generate User Conflicts or an Analyze Responsibility Conflicts program. The former enables Access Governor to recognize the new function-responsibility configuration as it enforces rules for pre-existing and new responsibility assignments, and the latter for new assignments only.

For instructions on running either program, see "Background Programs" (page 49).

# Viewing User Conflicts

In the list of rules displayed by the SOD Rules panel, a View link appears in the View User Conflict column for each rule that has generated conflicts in the most recent snapshot. The View User Conflict column is located all the way to the right of the SOD Rules panel (as shown in the illustration on page 9).

To review the conflicts for a rule, click on its View link. A User Conflicts panel opens:



Initially, this panel displays information about the rule that has generated conflicts, as well as a set of filtering fields, but no conflicts. If the rule is of the Allow with Rules or Approve with Rules control type, the panel also displays a +/– icon labeled *Oracle Form Rules*. Click on the + icon to display information about form rules associated with the SOD rule (as shown in the illustration above), or click on the – icon to hide the information.

The panel lists conflicts only after you use the filtering mechanism to determine what conflicts you want to see. To see all conflicts for the rule, make no selections in the filtering fields, and then click on the Filter button. To limit the display of conflicts, enter complementary values in any combination of the filtering fields, and then press the Filter button:

- User Name: Type the full username of a user to see conflicts associated with that user, or type a text fragment to see conflicts associated with users whose names contain the fragment.
- Responsibility: Type a full responsibility name to see conflicts in which your selection is the "base" responsibility, or type a text fragment to display conflicts generated by rules for which the base responsibility name includes the fragment. A base responsibility is the first of two that are in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.
- Conflicting Responsibility: Type the full name of a responsibility to see conflicts in which your selection is the "conflicting" responsibility, or type a text fragment to display conflicts generated by rules for which the conflicting responsibility name includes the fragment. A conflicting responsibility is the second of two that are in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.
- Status: Select a status — Approved, Pending, or Rejected — to see conflicts at the selected status, or select All to see conflicts at all statuses. This filter pertains only to conflicts generated by rules whose control type is Approve with Rules or Approval Required. Set this filter to All if you are reviewing conflicts generated by a rule whose control type is Allow with Rules or Prevent.

When you click on the Filter button, the panel displays a list of conflicts appropriate to your filter criteria. Each entry in the list includes:

- The User Name that identifies the user whose work assignments are in conflict.
- The base and conflicting responsibilities (as defined above in the discussion of filtering criteria) involved in the conflict.
- The conflict status, which depends on the control type assigned to the SOD rule:
  - If the control type is Approve with Rules or Approval Required, each conflict status begins at Pending, but can be updated to Approved or Rejected. (If you used status as a filtering criterion, of course, the entire list consists only of conflicts at the status you selected.)

– If the control type is Allow with Rules, each user's status is Allow with Rules. This status cannot be updated.

– If the control type is Prevent, each user's status is Prevent. This status cannot be updated.

# Updating Status for User Conflicts

If a conflict is generated by an Approve with Rules or Approval Required SOD rule, its status is Pending, Approved, or Rejected. Any of these statuses can be updated from one to another, and status can be reset any number of times.

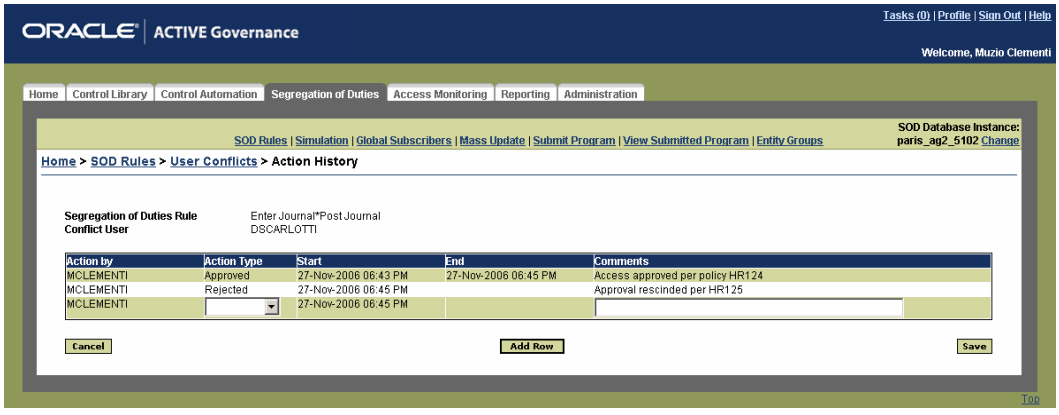
For each of these conflicts, the User Name in its entry on the User Conflicts panel is a link to an Action History panel, in which any Access Governor user may view status details — the current and past statuses, the dates on which they were effective, and comments that apply to them.

An approver (as designated in the rule that generated the conflict) can also use the Action History panel to update the status, under certain conditions: As has been noted, the Generate User Conflicts program activates all SOD Rules that have not been end-dated at the moment it is run, and this set of rules remains active until the Generate User Conflicts program is run again. If responsibilities have been assigned to a user, and subsequently rules are activated that uncover conflicts in the assignment, the status of those conflicts can be updated in the Action History panel. If, however, the assignment of responsibilities to a user triggers SOD rules that are already active, notifications are issued in Oracle Applications to approvers designated by those rules; the conflicts are recorded in the Action History panel, but their status cannot initially be updated there. Instead, the approvers' responses to the notifications update the Action History status. After all approvers have responded to the notifications, approvers can reset status directly in the Action History panel.

Neither the Allow with Rules nor the Prevent status can be updated. For conflicts at either status, you cannot navigate to the Action History panel.

To view or update status history for an Approval Required or Approve with Rules conflict:

**1** In the User Conflicts panel, click on the User Name for the conflict whose status you want to review or update. The Action History panel opens:



2. Review the details of earlier status assignments. Each row on the panel represents an occasion on which status was assigned, and the most recent row (the last in the list) displays the status that is in force.
3. If you are not an approver for the rule, this review is all you can do in the Action History panel; click on the Cancel button to return to the User Conflicts panel.

   You are an approver for the rule if you are a member of its approval group, or its owner if no approval group has been designated, *and* if your primary application role is SOD Approver. Even in this case, if approval notifications related to this conflict are outstanding in Oracle Applications, you'll see this message: "Approval request pending, hence no action can be taken." In this case, once again, click on the Cancel button to return to the User Conflicts panel.

   However, if you are a designated approver for the rule and no approval notifications are outstanding in Oracle Applications, you can also update status for the conflict. To do so, click on the Add Row button, which appears only if you are a designated approver for the conflict.
4. In the Action Type field of the row you created, select Approved, Rejected, or Pending:
   - Approving a user conflict means that you know it exists but decide to allow the user access to conflicting responsibilities or functions.
   - Rejecting a user conflict means that you decline to allow the user access.
   - Pending is the default status, indicating that a decision is yet to be made.
5. In the Comments field, type a brief explanation for your approval decision.
6. Click on the Save button.

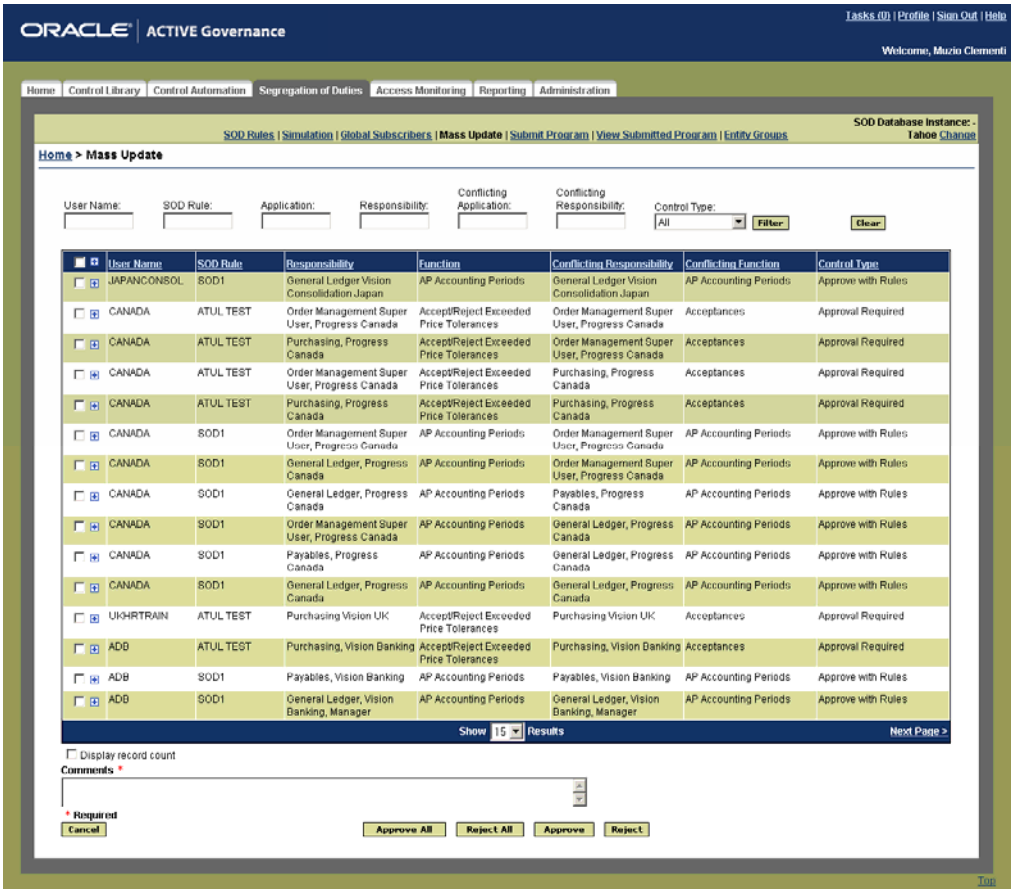
As you save a status, ACTIVE Access Governor automatically sets effective dates for status assignments:

- The Start field for a new status (displayed in the row in which you have been working) is set to the current date and time. The status becomes active at that moment.
- The End field for the new status remains blank (meaning that the status remains in effect indefinitely). The End field for the prior status (displayed in the row above the one in which you have been working) is set to the current date and time (indicating that it expires at the moment the new status takes effect).

# Mass Updating User Conflicts

A Mass Update panel lists Approve with Rules or Approval Required conflicts that are at the Pending status, enabling you to select a set of them and approve or reject the entire set at once, rather than one at a time:

1. Click on the Mass Update link in the Library Navigator. The Mass Update form opens (it's shown at the top of the next page), and initially it displays only a set of filtering fields.




**2** Set filtering criteria that determine what conflicts you will see (although no matter what criteria you select, you have access only to conflicts generated by SOD rules for which you are a designated approver). Then click on the Filter button. If you set no criteria, the panel displays all conflicts you are designated to approve. Or, you can filter on these values:

- User Name: Type the full username assigned to a user to display conflicts involving that user. Type a fragment to display conflicts involving all users whose usernames contain the fragment.
- SOD Rule: Type the full name of a rule to display the conflicts generated by that rule. Type a fragment to display conflicts generated by rules whose names contain the fragment.
- Application: Type the full name of an Oracle application to find conflicts in which your selection is the "base" application — the one that owns the first of two responsibilities or functions that a rule sets in conflict. Or type a text fragment to find conflicts in which the first conflicting entity belongs to any application whose name includes the fragment. For a rule that sets more than two entities in conflict, the search identifies pairs of conflicting entities, and returns conflicts in which the first entity belongs to the application you choose.
- Responsibility: Type the full name of a responsibility to see conflicts in which your selection is the base responsibility, or type a text fragment to display con-

flicts generated by rules for which the base responsibility name includes the fragment. A base responsibility is the first of two that are in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.

- Conflicting Application: Type the full name of an Oracle application to find conflicts in which your selection is the "conflicting" application — the one that owns the second of two responsibilities or functions that a rule sets in conflict. Or type a text fragment to find conflicts in which the second conflicting entity belongs to any application whose name includes the fragment. For a rule that sets more than two entities in conflict, the search identifies pairs of conflicting entities, and returns conflicts in which the second entity belongs to the application you choose.
- Conflicting Responsibility: Type the full name of a responsibility to see conflicts in which your selection is the conflicting responsibility, or type a text fragment to display conflicts generated by rules for which the conflicting responsibility name includes the fragment. A conflicting responsibility is the second of two that are in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.
- Control Type: Select Approve with Rules or Approval Required to see only conflicts generated by rules of the control type you choose, or select All to see conflicts generated by rules of both types. (Because you cannot update status for Prevent or Allow with Rules SOD rules, these control types are not available for selection.)

If you click on the Clear button, you discard both filtering criteria and the currently displayed list of conflicts, and can select new filtering criteria to generate a new list.

**3** A grid appears, in which each row displays information about a conflict. Each row contains a +/– icon. Optionally, click on the + icon for an Approve with Rules conflict to display information about the form rule intended to mitigate the conflict — that is, the form rule associated with the SOD rule that generated the conflict. (The display is identical to the Oracle Form Rules area of the User Conflicts panel, as shown in the illustration on page 28.) Click on the – icon to hide the display. For an Approval Required rule, this feature simply displays a message stating that no form rule is attached to the SOD rule.

**4** If you want to assign status to all the filtered conflicts at once, skip ahead to step 5. If you want to assign status to a subset of the filtered conflicts, select those whose status you want to update. The Mass Update form presents conflicts in a grid divided into "pages," and if you are selecting individual conflicts, you can select them from only one page at a time.

Choose the page that displays conflicts you want to update. You can click on Next Page and Previous Page links in the footer row of the grid. Or you can select a page number in a field of the footer row that shows the number of pages in the grid and the number assigned to the current page. For performance reasons, this field is hidden by default, but you can select a Display Record Count check box to make it appear. (When you do, another field in the footer shows the number of conflicts available for review and the numbers assigned to the conflicts in the current page.)

Once you have chosen a page, do either of the following:

- Select check boxes alongside individual conflicts you intend to approve or reject.
- Select a check box in the header row of the grid (to the left of the User Name heading) if you want to approve or reject all conflicts in the currently displayed page of the grid.

**Note**
A rule may designate an approval group of which you are a member, even though your primary application role is other than SOD Approver. Typically, this is because you have only notification rights in the approval group. In this case, you can review conflicts in the Mass Update panel, but it does not display the check boxes with which you can select conflicts for approval or rejection, and you cannot actually approve or reject conflicts.

5. In the Comments field, type an explanation for your decision to update status. The comment is required, and it applies to all of the conflicts whose status you are updating.
6. If (in step 4) you selected a set of conflicts, click on either the Approve or Reject button. If not, click on the Approve All or Reject All button to approve or reject all the conflicts that match your filtering criteria (that is, all the conflicts in all the pages of the grid). In either case, ACTIVE Access Governor assigns the status you select and the comment you wrote to each newly statused conflict. It removes these conflicts from the list, and leaves the Mass Update form in place.
7. Optionally, make another selection of conflicts and assign status to them. (You can, for example, approve a first selection of conflicts and then reject a second selection of conflicts.) When you finish with the Mass Update form, click on the Cancel button or on the SOD Rules link in the Library Navigator to return to the SOD Rules panel.

After you have used the Mass Update panel to assign status to a set of conflicts, you can use the Action History panel if you wish to reassign status to individual conflicts in the set. However, a conflict will not reappear in the Mass Update panel unless it is reassigned Pending status.

# Chapter 4

# Resolving Conflicts

Although a conflict is defined, and may be approved or rejected, in ACTIVE Access Governor, it is not resolved until actions are taken outside of ACTIVE Access Governor. These actions may include:

- Adjusting the end dates for responsibilities assigned to a user affected by a conflict. For an approved conflict, end dates may be set in the future (or removed) so that access to a responsibility is extended. For a rejected conflict, end dates are set to the present moment so that access to a responsibility is cut off.
- Excluding one or more conflicting functions from a responsibility or from menus, or removing a submenu containing conflicting functions from menus.
- Ensuring that subscribers are configured correctly for each form rule associated with an SOD rule whose control type is Allow with Rules or Approve with Rules. A subscriber is a user (or other entity) to which a form rule (or rule element) applies. If no subscribers have been configured for a form rule, it applies universally, and so subscriber configuration is not an issue if the form rule is associated with an SOD rule. However, if a user's work assignments violate an Allow with Rules or Approve with Rules SOD rule, and that rule is associated with a form rule that has one or more subscribers, the user must be added as a subscriber to the form rule. For instructions on adding subscribers to form rules, see the *Form Rules User's Guide*.

The process for effecting these resolutions depends on whether a user has been assigned duties before or after a rule is put in force to define them as conflicting.

# Manual Conflict Resolution

The first time conflicts are generated, or when they are regenerated after SOD rules have changed, you are likely to find users who had been granted access to responsibilities or functions before rules defined them as conflicting. ACTIVE Access Governor uncovers these conflicts but does not resolve them. Instead, you can eliminate these conflicts manually, a process known as "cleanup."

To uncover these conflicts, you would generate user conflicts and then review them, either in the User Conflicts panel or in the User Conflicts Report. The course of action for each conflict depends on its control type:

- For an Allow with Rules conflict, the user's access to conflicting entities should be permitted to continue.
- For a Prevent conflict, the user's access to one or both conflicting entities would have to be terminated.
- For an Approve with Rules or Approval Required conflict, the user's access to conflicting entities could be approved or rejected. In either case, the reviewer should, for auditing purposes, assign status to the conflict in the Action History panel or the Mass Update panel.

To allow or approve a conflict, you need do nothing in Oracle Applications.

To prevent or reject a conflict, you have four options. The first resolves a function- or responsibility-based conflict. The remaining three are appropriate for function-based conflicts — particularly those involving two functions within a single responsibility:

- In the Oracle Applications Users form, set the end date for at least one responsibility involved in the conflict to the current date.
- Exclude one of two conflicting functions from the responsibility through which the user has access to that function.
- Remove the function from menus through which the user has access to it, or remove a submenu containing a conflicting function from the user's menus.
- Exclude those menus from the responsibility that provides the user with access to the function.

See Oracle documentation for procedures on excluding functions or menus from responsibilities, or removing functions from menus. To facilitate mapping functions to menus, a Function Where Used Report (see page 71) displays the menu paths to functions involved in function-based conflicts.

# Simulation and Remediation

To aid in cleanup, ACTIVE Access Governor enables you to write simulation scenarios. Each scenario comprises a set of rules that instruct Access Governor to determine how conflict generation would change if the Oracle Applications configuration were altered. Each rule names a function or menu that might be excluded from a responsibility, or a function or submenu that might be removed from, or inserted in, a menu.

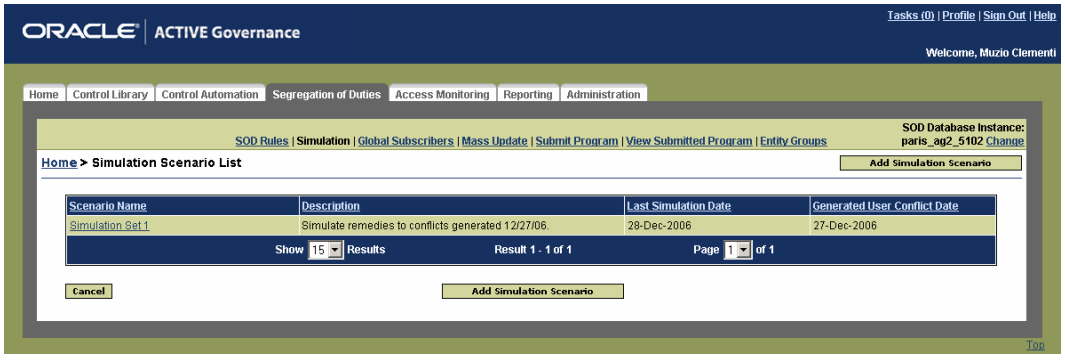
The simulation feature uses two snapshots. A "base" snapshot contains conflicts generated with functions, menus, and responsibilities as they are actually configured. The second snapshot contains conflicts that would be generated under conditions defined by a simulation scenario. ACTIVE Access Governor compares the two and presents results — a list of conflicts that would no longer exist, as well as those that would be newly generated.

If SOD rules have changed since the last time the Generate User Conflicts program was run, you must generate a new base snapshot as part of the simulation process. If SOD rules have not changed, you can choose whether to generate a new snapshot as the base snapshot, or to use the most recent one:

- Choose to generate a new snapshot if certain changes have been made manually in Oracle Applications since the most recent snapshot was created in Access Governor. The Oracle changes include the creation of users; the modification of responsibility assignments for existing users; or alterations in the exclusion of functions from responsibilities, the assignment of functions to menus, or the assignment of submenus to other menus or responsibilities. Such changes are likely to resolve existing conflicts in your system or to create new conflicts, thus rendering the most recent snapshot obsolete. A new snapshot not only makes the simulation results as accurate as they can be, but also updates the information displayed in the User Conflicts, Action History, and Mass Update panels, so that all parts of the system are in sync.
- Select the most recent snapshot if such changes have not been made since that snapshot was created in Access Governor. In that case, no disparities have been introduced between that snapshot and the actual state of your user conflicts, and the simulation process runs more rapidly because a new set of actual conflicts need not be generated.

If simulation shows that resolved conflicts outnumber those that are newly generated, Access Governor can perform "remediation" — modify function, menu, and responsibility configurations in Oracle Applications to implement the simulated conditions.

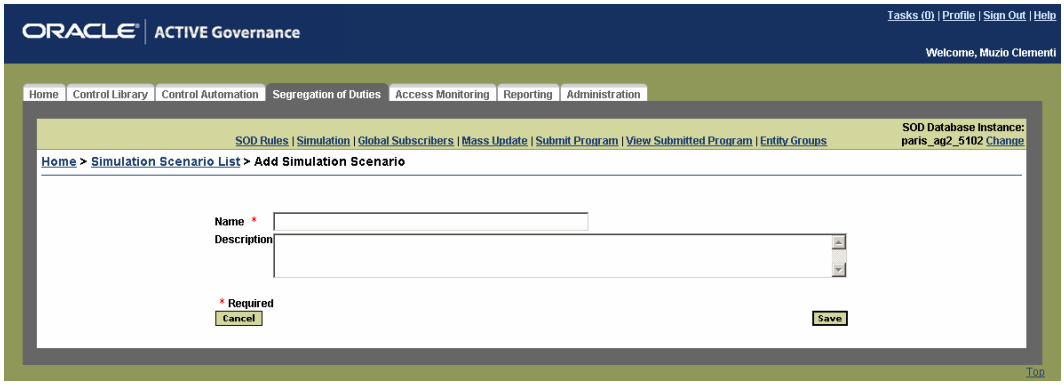
To complete any task related to simulation or remediation, begin by clicking on the Simulation link in the Library Navigator. A panel titled Simulation Scenario List appears, displaying the name and description of each existing scenario, together with the date on which it was most recently run and the date of the base snapshot associated with that most-recent running:



## Creating Scenarios

A scenario is a "container" that holds any number of individual simulation rules. You need to create the scenario before you create any of the rules it holds. To do so:

1. Click on an Add Simulation Scenario button; one appears at the bottom center, and another near the upper right, of the Simulation Scenario List panel. An Add Simulation Scenario panel appears:




2. In the Name field, type a name for the scenario.
3. Optionally, in the Description field, type a brief explanation of the scenario. (For example, explain the organizing principle by which rules are included in the scenario.)
4. Click on the Save button. The Simulation Scenario List panel is restored, displaying an entry for the scenario you have created.

## Creating Simulation Rules

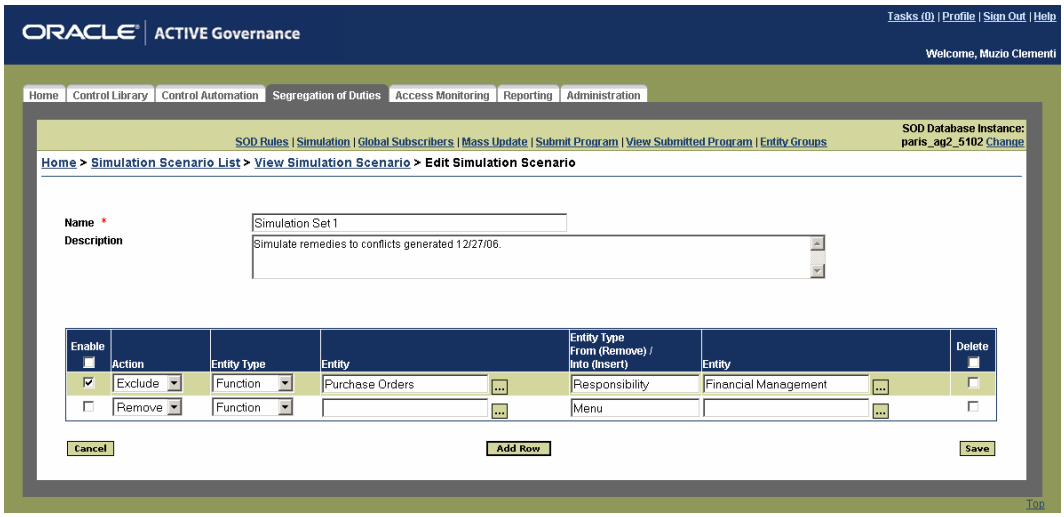
To create or edit simulation rules:

1. Begin by identifying modifications you want to simulate in the relationships among functions, menus, and responsibilities. Do so by reviewing conflicts in the User Conflicts panel and, if necessary, by using the Function Where Used Report to uncover the relationships among functions, submenus, and menus.

   For example, an SOD rule may set two functions — Purchase Orders and Receipts — in conflict. The User Conflicts panel may show conflicts for several users who have access to both functions through a single responsibility — Financial Management. Rather than end-date the responsibility for each user, you may want to determine what would happen if you were to exclude one of the functions — say, Purchase Orders — from the Financial Management responsibility.
2. Open the scenario in which want to create simulation rules: In the Simulation Scenario List panel, the name of each scenario is a hyperlink. Click on the name of the one you want.
3. A View Simulation Scenario panel opens. If no rules have yet been defined, it displays the name of the scenario, its description, and a date on which it was most recently changed, together with a button labeled Edit. If rules have been defined,

the panel also displays a read-only entry for each rule as well as some additional buttons (which will be discussed later). In either case, click on the Edit button to create new rules or edit existing rules.

**4** An Edit Simulation Scenario panel opens, displaying a write-enabled entry for each existing rule. To edit an existing rule, work directly in its entry. To create a new rule, click on the Add Row button:




**5** In the appropriate row, enter or modify values for a simulation rule. (As you do, note that a given menu may be a parent to submenus as well as a submenu to higher-level menus. So when you choose a menu or submenu, you choose from the same list of values.)

- In the Action field, choose what you want the rule to do: Select Exclude to simulate excluding a function or menu from a responsibility, Remove to simulate removing a function or submenu from a menu, or Insert to simulate inserting a function or submenu into a menu.
- In the Entity Type field, choose the type of item you want to exclude, remove, or insert: Function or Menu if you selected Exclude in the Action field, Function or Submenu if you selected Remove or Insert in the Action field.
- The first Entity field displays values appropriate to your Entity Type selection. In it, pick the specific function, submenu, or menu to be acted upon.
- In the Entity Type From/To field, accept the default value. This field displays the one value made necessary by your earlier selections: Responsibility if you chose Exclude in the Action field, or Menu if you selected Remove or Insert.
- The second Entity field displays values appropriate to the Entity Type From/To selection. In it, pick the specific menu or responsibility from which the first entity is to be excluded or removed, or into which it is to be inserted.

For example, to create the rule that simulates the exclusion discussed in step 1, select Exclude in the Action field, Function in the Entity Type field, and Purchase Orders in the first Entity field. The Entity Type From/To field would default to Responsibility; select Financial Management in the second Entity field.

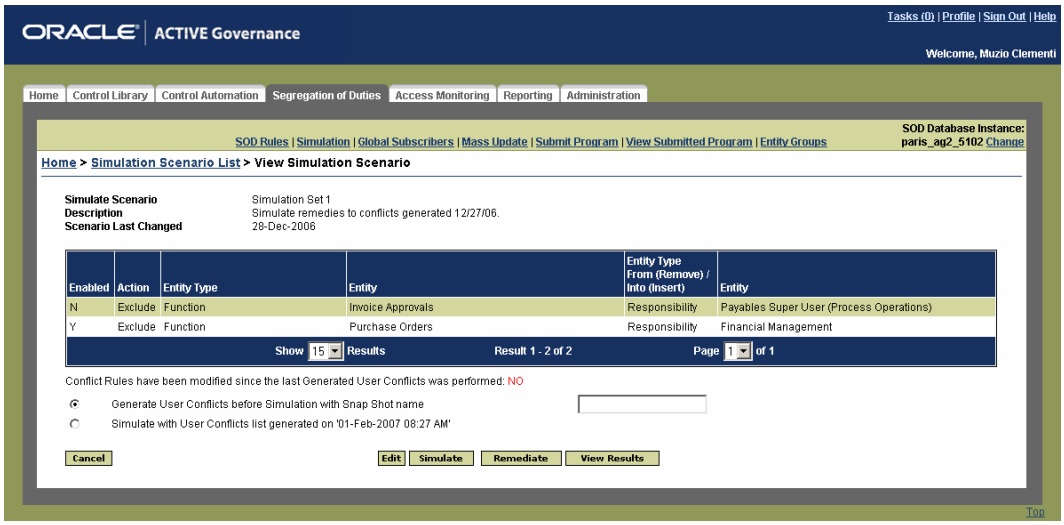
6 Repeat steps 4 and 5 to edit or create any additional rules you want the scenario to contain.

7 To be evaluated, simulation rules must be enabled. Select the Enable check box for each rule you want to include in a given simulation run. Clear the Enable check box for any rule you do not want to include. (To select a check box is to click on it so that a check mark appears, and to clear it is to click on it again so that the mark disappears.) You can select the Enable check box in the header row to enable all existing simulation rules.

You have the option of deleting rules you do not want to run. For each, select the Delete check box. (You can select the Delete check box in the header row to mark all rules for deletion.) However, this is not necessary; to avoid using a rule in a simulation run, you need only ensure that its Enable check box is cleared.

8 Optionally, modify the name or description of the scenario; use the Name and Description fields.

9 Click on the Save button. If you've marked any of the rules for deletion, dialog boxes prompt you to confirm the deletion. Then the View Simulation Scenario panel returns, displaying read-only entries for the rules you have not deleted. (For each, the Enabled field reads *Y* if the rule is enabled or *N* if it is not.)




## Generating and Viewing Simulation Results

To evaluate a simulation scenario:

1 Select the scenario that contains simulation rules you want to run (if it is not selected already). In the Simulation Scenario List panel, click on the name of the scenario you want; this opens its View Simulation Scenario panel (as shown above).

2 Review entries in the Enabled column to ensure that the only those rules you want to evaluate are enabled. If this is not the case, modify the enabled status of the rules in the scenario as needed. (See the previous section, "Creating Simulation Rules," paying particular attention to its step 7.)

3 Choose the snapshot of actual conflicts you want to compare with the snapshot of simulated conflicts.

- You must generate a new snapshot if SOD rules have changed since the Generate User Conflicts program was last run (and a message, beneath the grid that lists simulation rules, informs you whether this is the case). Even if not, generate a new snapshot if your Oracle configuration has changed since conflicts were last generated (as discussed on page 37). Select the "Generate User Conflicts before Simulation with snapshot name" option (which is the only option if SOD rules have changed) and in the field to its right, supply a name for the new snapshot.
- Use the most recent snapshot if no changes have been made to SOD rules or your Oracle configuration. Select the radio button labeled "Simulate with User Conflicts list generated on *Date*" (in which the placeholder value is replaced by the date and time of your most recent snapshot). This option appears only if no SOD-rule changes have been made since conflicts were last generated.

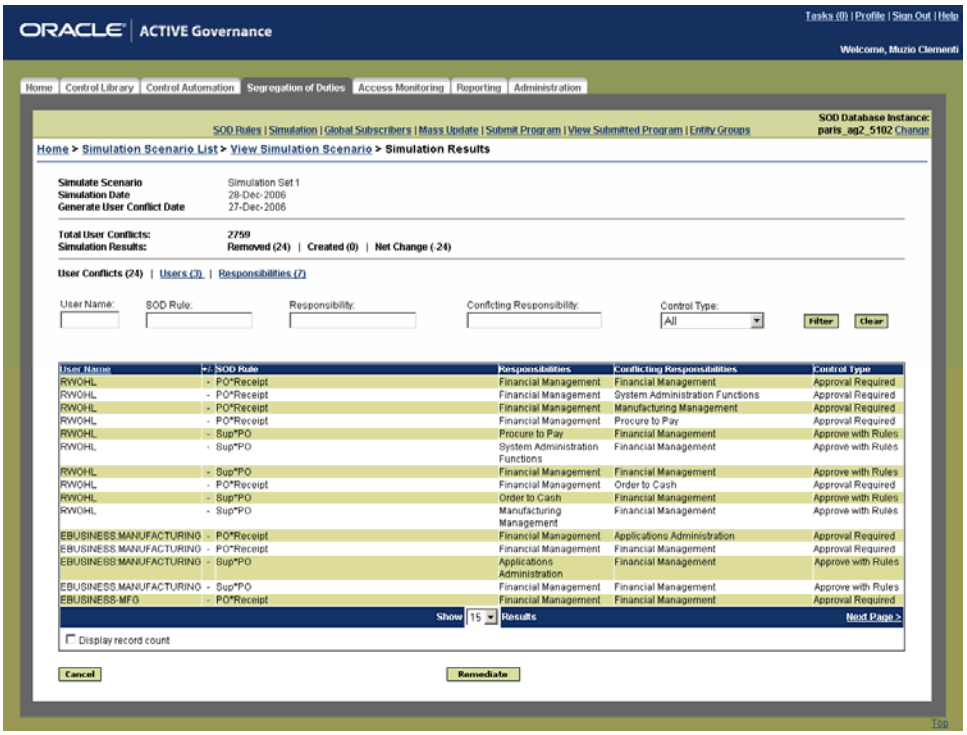
4 Click on the Simulate button. Access Governor runs a background program to perform the simulation, and the View Submitted Program panel displays the status of the program. The simulation is finished when, in the row for your request, the Phase field reads "Completed" and the Status field reads "Normal."

To view the results of the simulation run:

1 Click on the Simulation link in the Library Navigator.

2 The Simulation Scenario List panel reopens; in it, reselect the scenario for which you have run simulation.

3 The View Simulation Scenario panel reopens; in it, click on the View Results button. A Simulation Results panel appears:



Initially, the panel displays only summary information and a set of filtering fields. The summary information includes not only the name of the scenario, the date on which the simulation results were produced, and the date of the base snapshot used in the simulation, but also the number of existing user conflicts, the numbers that would be resolved and created by the simulation, and the net change.

You can generate lists of individual conflicts that would be resolved or newly created (the default), of individual users whose conflicts would change, or of individual responsibilities for which conflicts would change. To change from one list to another, click on any of the User Conflicts, Users, or Responsibilities links that appear immediately beneath the summary results.

The filtering fields apply only to the User Conflicts list. If you choose to display simulated changes by user or by responsibility, the filtering fields disappear and the Simulation Results panel displays entries for all users or all responsibilities for which conflicts would change. In this case, each entry shows an affected item (user or responsibility), the number of actual conflicts applying to that item, the number that would apply if simulated changes were made, and the net change.

If you choose to display simulated changes by conflict, select filtering criteria that determine what conflicts you will see, and then click on the Filter button. If you set no criteria, the panel displays all conflicts that would change. Or, you can filter on these values:

- User Name: Type the full username assigned to a user to display simulated changes that apply to that user. Type a fragment to display changes applying to all users whose usernames contain the fragment.
- SOD Rule: Type the full name of a rule to display simulated changes involving that rule. Type a fragment to display changes involving rules whose names contain the fragment.
- Responsibility: Type the full name of a responsibility to see simulated changes for which your selection is the "base" responsibility, or type a text fragment to view changes for which the base responsibility name includes the fragment. A base responsibility is the first of two that are in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.
- Conflicting Responsibility: Type the full name of a responsibility to see simulated changes for which your selection is the "conflicting" responsibility, or type a text fragment to display changes for which the conflicting responsibility name includes the fragment. A conflicting responsibility is the second of two that are in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.
- Control Type: Select one of the control types — Prevent, Allow with Rules, Approve with Rules, or Approval Required — to see simulated changes to conflicts of that type, or select All to see all changes, regardless of control type.

If you choose to display simulated changes by conflict, each entry in the list displays:

- The name of the user affected by a conflict.
- A minus sign (in a column labeled +/–) to indicate a resolved conflict, or a plus sign to indicate a newly generated conflict.
- The name of the SOD rule that generated the conflict.
- The responsibility and conflicting responsibility involved in the conflict (as defined above in the description of filtering criteria).
- The control type of the SOD rule that generated the conflict.

When you are finished viewing results, click on the Cancel button to return to the View Simulation Scenario panel (or use a breadcrumbs link or the Library Navigator to move elsewhere).

## Remediation

If you are satisfied with the results of a simulation scenario, Access Governor can implement "remediation" — actually make the simulated changes. A Remediate button is available to SOD Super Users, Rule Builders, Authors, and Managers; it appears both in the View Simulation Scenario and Simulation Results panels. (For other users, this button does not appear.) When you click the Remediate button, Access Governor prompts for confirmation that remediation should be run. Click an OK button in the prompt dialog, and Access Governor launches a background program; the View Submitted Program panel displays its status.

Within Oracle Applications, functions or submenus are inserted, removed, or excluded as dictated by the simulation rules. An inserted item appears in its menu with the label *(AGS)*, to indicate that the insertion occurred through the agency of ACTIVE Governance simulation. Other changes are noted (if at all) according to standard Oracle Applications functionality. For example, a function excluded from a responsibility is listed in the Exclusions grid of the Responsibility form.

Within Access Governor, the View Simulation Scenario panel for the scenario used in the remediation continues to list the simulation rules, for auditing purposes. The Simulation Results panel continues to list the conflicts (or the users or responsibilities to which they apply) that existed before the remediation. If you run simulation again, however, the Simulation Results panel is updated to reflect the results of the remediation.

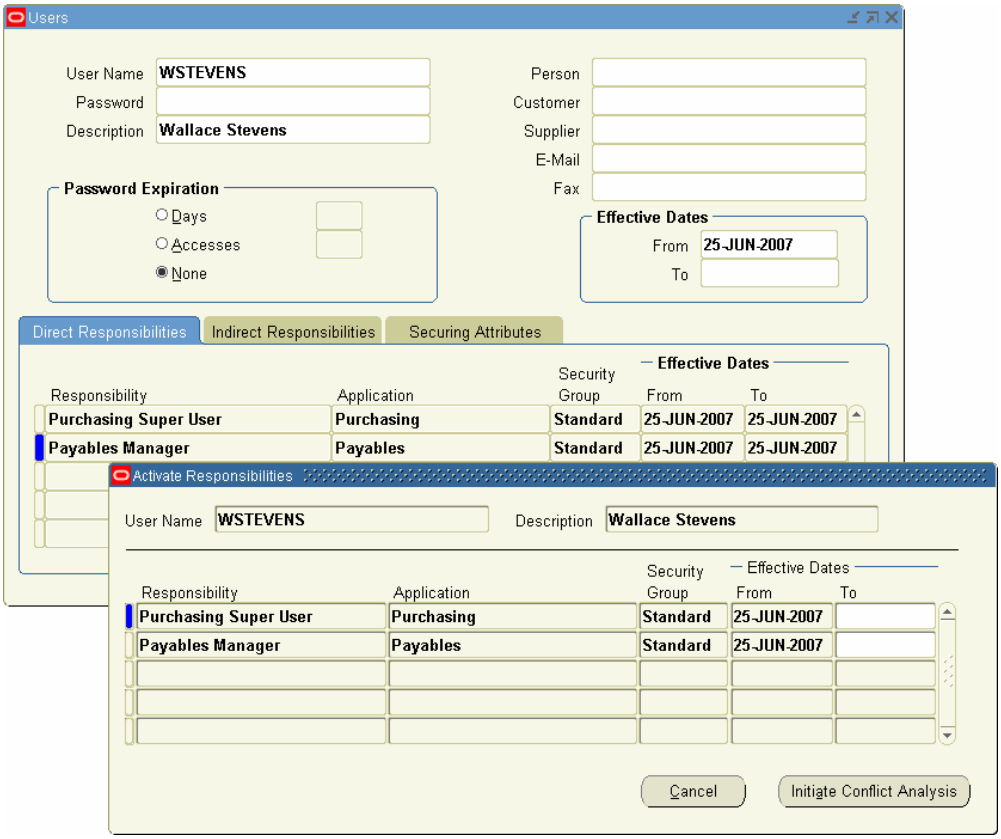
# Automated Conflict Resolution

When a user is assigned new responsibilities, ACTIVE Access Governor evaluates the assignment for violations of SOD rules that were in force the last time the Generate User Conflicts program was run. Access Governor presents an option to "submit" or cancel the assignment, and upon submission, it enforce rules that have been violated: depending on control type, it automatically grants or denies access, or sends on-line notifications to approvers.

## Activating Responsibilities

The process begins in the Oracle Applications Users form, as a new user is created or an existing user receives new responsibility assignments. (See Oracle documentation for information on the Users form, creating users, and assigning responsibilities.)

1. With the Users form open, a system administrator selects a user and, in the grid accessible from the Responsibilities tab, assigns responsibilities. 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.

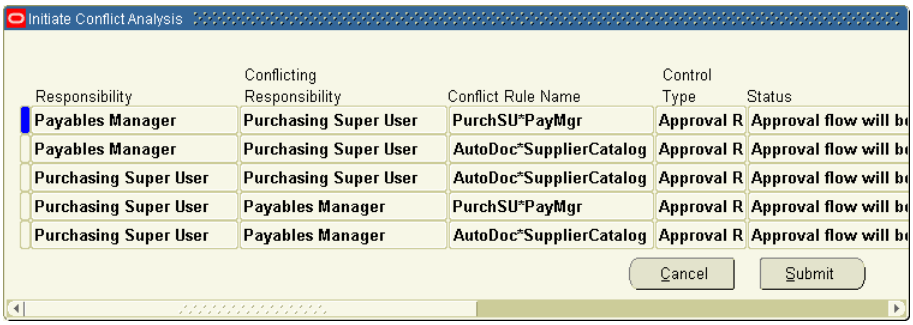



**Note**
If the Activate Responsibilities option is inactive, use a Mass Associate feature, available in Form Rules or Flow Rules, to associate a function called Activate Responsibilities with the responsibility or the menu from which you gain access to the Users form. For information on the Mass Associate feature, see the user's guide for Form Rules or Flow Rules.

3. 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** An Initiate Conflict Analysis form provides data about responsibilities for which the administrator changed end dates, noting those for which no conflict exists and listing all conflicts in which the responsibilities are involved. For each conflict, a Status field displays a message:

- For a Prevent conflict, end dates will not be removed.
- For an Allow with Rules conflict, end dates will be removed, providing the SOD rule is associated with a form rule.
- For an Approval Required or Approve with Rules conflict, an approval flow will be launched.




**5** The administrator may, at this point, take either of two actions:

- Click on the Cancel button to avoid assigning conflicting responsibilities. The Activate Responsibilities form would reappear; the administrator would click on its Cancel button, and then on the No button in a prompt to save changes. He can then reselect the Assign Responsibilities option in the Actions menu and try granting access to a different selection of responsibilities.
- Click on the Submit button to accept the selection of responsibilities, even if it contains conflicts. ACTIVE Access Governor then grants access to responsibilities with no conflicts or with Allow with Rules conflicts. For responsibilities with Prevent conflicts, it denies access.

  In these cases, "granting access" means setting end dates in the Users form to match those selected in the Activate Responsibilities form — or removing them if they have been removed in that form. "Denying access" means setting end dates in the Users form to the current date.

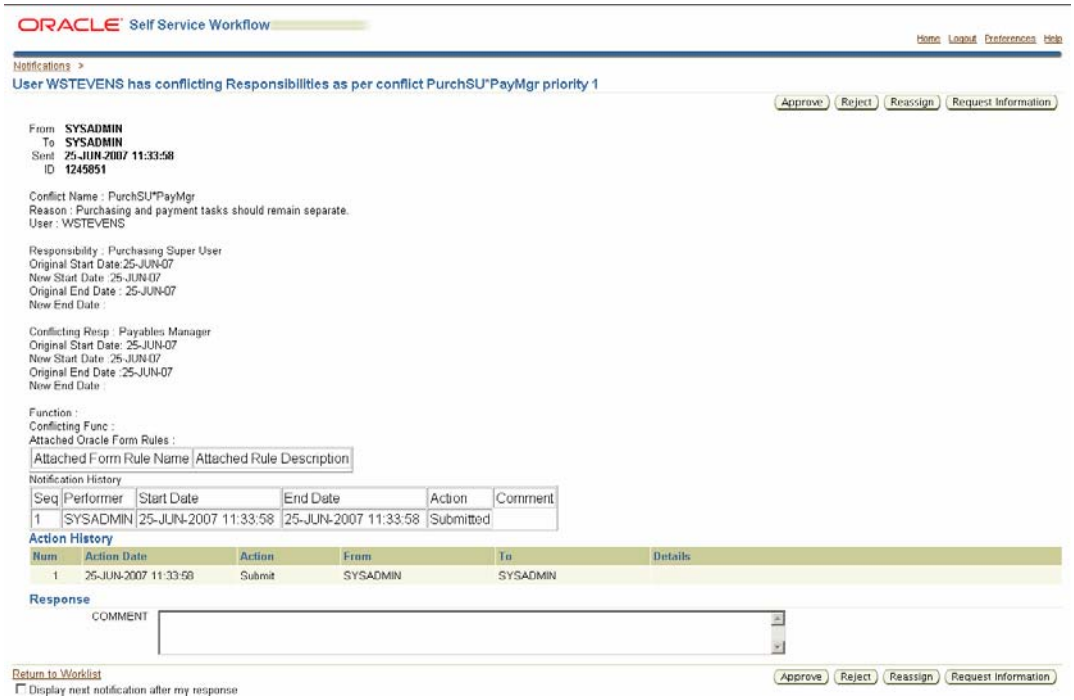
  For responsibilities involved in Approval Required or Approve with Rules conflicts, Access Governor sends notifications to approvers. The end dates in the Users form remain temporarily set at the current date. Whether that value is made permanent or reset depends upon the approvers' responses to the notifications.

  However, Access Governor takes the most restrictive possible action when multiple conflicts occur. For example, when a responsibility assignment violates both a Prevent rule and an Approval Required rule, access is denied and no notification is sent to approvers. The "pecking order" is Prevent, Approve with Rules, Approval Required, Allow with Rules, no conflict.

## Responding to Notifications

For an Approval Required or Approve with Rules conflict, an approval workflow notifies the approver defined by the SOD rule. To respond to a notification:

1. In the Oracle E-Business Suite, select Notifications in the Workflow responsibility. A Worklist opens; in it, locate an approval notification to which you want to respond. Click on the notification to open it:




2. Review information about the conflict. This includes the name of the affected user; the responsibilities and, if appropriate, functions involved; and the associated form rule for an Approve with Rules conflict. Optionally, use the Comment field to type an explanation of the decision you are about to make.
3. Click one of the following buttons:
   - Approve: The user is given access to the responsibilities. When they were provisionally assigned, their end dates were removed or set to a future date in the Activate Responsibilities form. Approval of this notification resets the end dates in the Users form to match the setting in the Activate Responsibilities form. (This takes effect, however, only when the Oracle Workflow background process has run.)
   - Reject: The user is denied access to the responsibilities. End dates in the Users form are set permanently to the dates that were current when the responsibilities where provisionally assigned.
   - Reassign: You reassign the conflict to another reviewer. The originally assigned end dates remain, but an approval by the other reviewer will update them.
   - Request Information: Compose a message to the originator of the notification, requesting additional information.

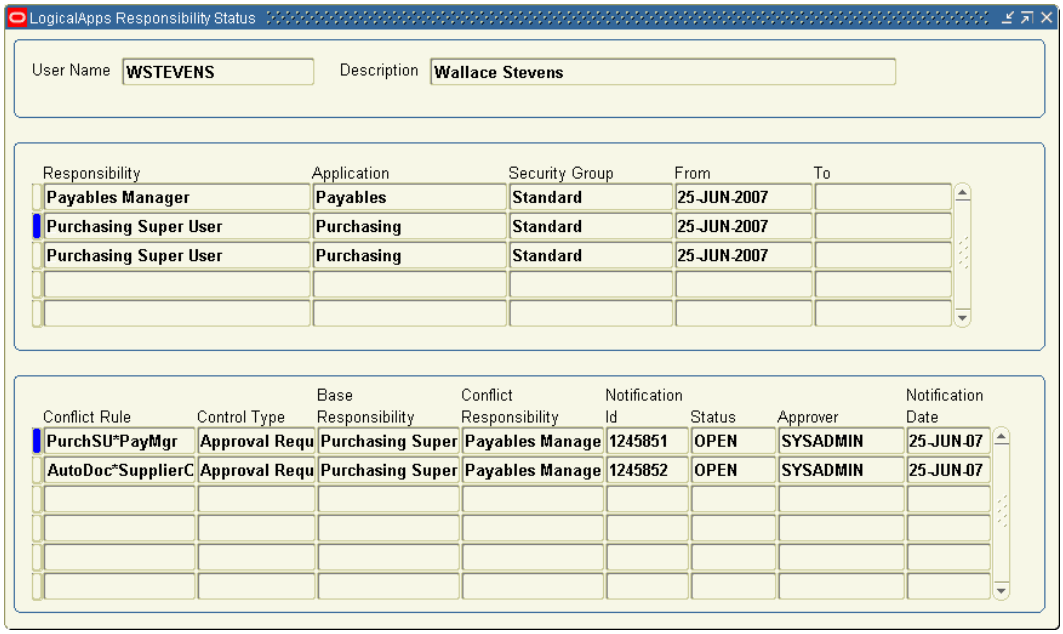
   An approval or rejection updates the User Conflicts panel in Access Governor.

## Viewing the Status of Notifications

Although authorization notifications are distributed immediately upon the submission of new responsibility assignments, approvers may not respond to them promptly. You can check on the status of notifications for which approval decisions have not yet been made:

1. Open the Oracle Users form and select a user whose responsibility assignments have generated outstanding notifications.
2. Click on Actions in the menu bar, and then on Responsibility Status in the Actions menu. A Responsibility Status form appears. Fields at the top of the form display the name and description of the user you selected in step 1.

   The upper grid displays one row for each newly assigned responsibility (matched to a conflicting responsibility) that has generated approval notifications; each row identifies the responsibility, the application to which it belongs and the security group to which it is linked, and the dates of its proposed assignment to the user.




3. Select a row in the top grid, and each row in the bottom grid displays information about a notification associated with your selection — the SOD rule that generated a notification and its control type (necessarily Approval Required or Approve with Rules, as the other two types do not generate notifications); the base and conflicting responsibilities; and the ID of the notification, its status, the user charged with making an approval decision, and the date on which it was sent.

In the illustration shown above, for example, the Responsibility Status form reports on notifications (and conflicts) generated by two rules. One sets the Payables Manager and Purchasing Super User responsibilities in conflict. The other sets two functions — AutoCreate Documents and Supplier Item Catalog — in conflict. Both functions are available from Purchasing Super User, and AutoCreate Documents is also available from Payables Manager.

The user WSTEVENS has been assigned both these responsibilities, and so three notifications have resulted: one for the conflict between the two responsibilities, one for the conflict between the two functions as they are available from Purchasing Super User, and one for the conflict between AutoCreate Documents on Payables Manager and Supplier Item Catalog on Purchasing Super User.

The Responsibility Status form groups information according to pairs of responsibilities involved in conflicts, so it may appear to display duplicate information. The second and third rows of the upper grid in the illustration shown above, for example, are identical. That's because each row identifies the same responsibility (Purchasing Super User) as its focus, but for each the second responsibility involved in its conflicts differs from the other. The upper grid does not show them, but in this example one is Payables Manager and the other is Purchasing Super User.

Thus, when the second row is selected in the upper grid, the lower grid displays the two notifications for which Payables Manager is the second responsibility — for the responsibility conflict and the conflict in which one function is available from each responsibility. If the third row were selected, the remaining notification would appear, for the conflict in which both functions are accessible from Purchasing Super User.

Moreover, the upper grid provides a row for each newly assigned responsibility that has generated notifications, so for conflicts that involve two responsibilities, the upper grid contains two rows corresponding to their notifications. In the illustration shown above, the second row is selected in the upper grid; it identifies Purchasing Super User as its focus, and, as already noted, the lower grid displays the two notifications involving both the Purchasing Super User and Payables Manager responsibilities. The first row in the upper grid identifies Payables Manager as its focus; if it were selected, the lower grid would display the same two notifications.

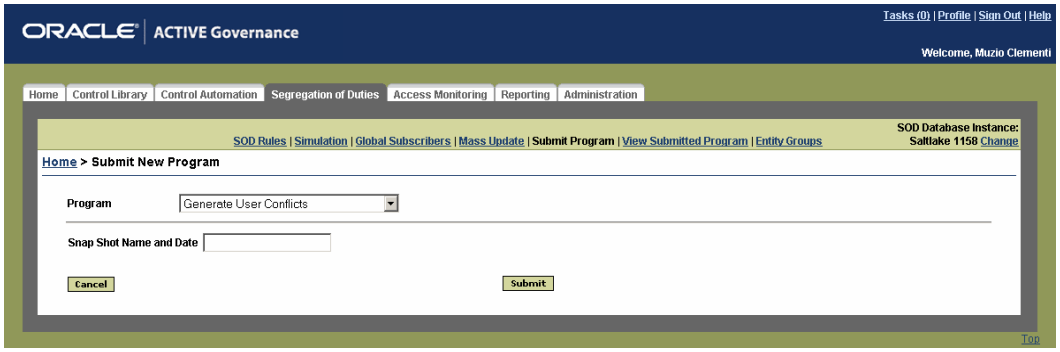
When approvers respond to notifications, the corresponding entries disappear from the Responsibility Status form. When all notifications are resolved for a given user, the form displays no data. Because the form is meant only to provide information, it is read-only.

# Chapter 5

# Background Programs

In ACTIVE Access Governor, background programs generate user conflicts, archive data, prepare export files or load import files, reset values, and update workflow roles (so that they can be selected as conflict approvers). To run a background program, complete these steps:

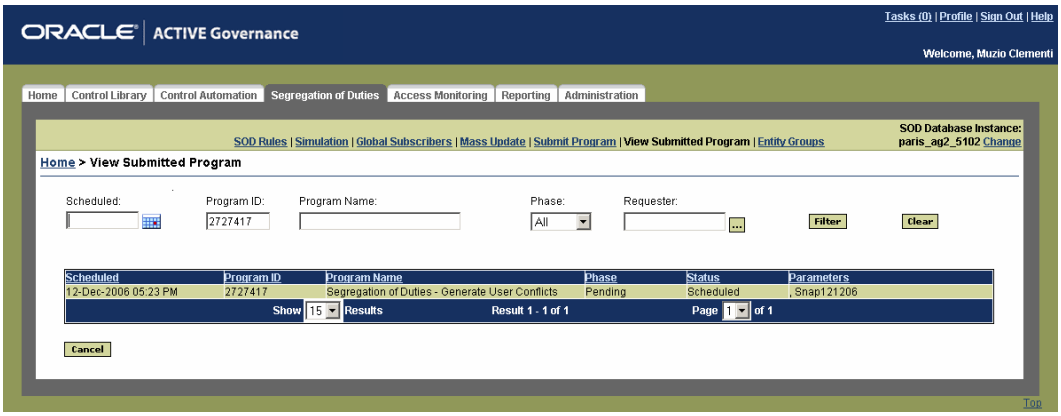
1. With the Segregation of Duties tab selected in the ACTIVE Governance Platform, select Submit Program in the Library Navigator. The following panel appears:




2. In the Program list box, select the background program you want. (The programs are identified and described below.)

3. If the program accepts parameters, select values for them in the lower section of the panel. Some programs do not accept parameters, and among those that do, each takes its own set, so the fields in this section of the panel vary according to the program you selected. (Parameters are documented in the descriptions of the programs that appear below.)

4 Click on the Submit button. The program is "submitted," and the ACTIVE Access Governor display shifts to a View Submitted Program panel. Results are filtered so that the panel displays only an entry for the program you submitted:




5 Click on the Refresh button of your web browser to update the Phase and Status fields. The program you submitted has finished running without errors when, in its row, the Phase field reads "Completed" and the Status field reads "Normal."

You can open the View Submitted Program panel directly, by clicking on the View Submitted Program link in the Library Navigator. If you were to do so, the panel would initially display no results at all. Regardless of whether you open the panel directly or by submitting a program, you can set filtering criteria to select the program runs for which the panel displays entries. Then click on the Filter button. If you set no criteria, the panel displays an entry for every occasion on which programs have been run. Or, you can filter on these values:

- Scheduled: Enter a date to see programs that ran on that date. Type the date, in the format *DD-Mon-YYYY*. (Although the field displays a time of day as well as a date, the time value has no effect on filtering.) Alternatively, click on the icon next to the field, and a pop-up calendar appears. In it, click on the < or > symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want.
- Program ID: Enter the ID number of program run you want to view. This number is assigned automatically when the program is run (and is the value ACTIVE Access Governor uses, when you submit a program, to display only an entry for that program).
- Program Name: Enter a program name (or a fragment of the name) to see entries for occasions when that program was run.
- Phase: Select the "phase" of a program run — Completed, Running, or Pending — to see entries for programs that have finished running, are still running, or have yet to run. Or select All to see entries for programs in any phase.
- Requester: Select a username to see entries for programs run by that user.

To discard filtering criteria (and have the pane display no results), click on the Clear button.

## Generate User Conflicts

The Generate User Conflicts program determines whether assignments of responsibilities to users violate SOD rules. It generates a "snapshot" — a record of the conflicts that exist at the moment you run the program. The rules in effect for the most recent snapshot continue to identify conflicts as changes are made to existing users' responsibility assignments or new users are added. The Generate User Conflicts program takes a single parameter, which is optional: In the Snap Shot Name and Date field of the Submit New Program panel, type a unique name for the generation of conflicts you are about to create. (This is purely a text field, so you can enter a name, a date, or both, and the date can be in any format you like.)

## Analyze Responsibility Conflicts

The Analyze Responsibility Conflicts program enables Access Governor to recognize functions as existing in the responsibilities that are assigned to users, a necessary first step in evaluating function-based SOD rules.

This is also the first of several steps executed by the Generate User Conflicts program, so if you've run that program, you don't need to run this one. However if, after running Generate User conflicts, you modify the assignments of functions to responsibilities, you have the option of rerunning Generate User Conflicts or of running Analyze Responsibility Conflicts. If you rerun Generate User Conflicts, Access Governor will recognize your new function-responsibility configuration as it analyzes SOD rules for users as they already exist, and for new assignments (new users or existing users assigned new responsibilities). If you run Analyze Responsibility Conflicts, Access Governor will recognize your new function-responsibility configuration only as it enforces rules for new assignments; the compensating advantage is that the Analyze Responsibility Conflicts program takes less time to run that the Generate User Conflicts program.

The Analyze Responsibility Conflicts program takes no parameters.

## Archive User Conflicts

The Archive User Conflicts program selects records of conflicts older than a specified date and stores them in a history table (the name of which is LAA_USER_CONFLICT_ENTITIES_H).

The Archive User Conflicts program runs automatically whenever the Generate User Conflicts program is run. As a result, only the current snapshot is available for viewing in the User Conflicts panel; all earlier snapshots are archived.

You can view archived conflicts in reports that are available in the Segregation of Duties folder of the Report Center: User Conflicts, Conflict Summary, Responsibilities with Conflicts, Responsibility Menu, User Conflicts Trend Analysis, and Conflicts by Responsibility or Application. In each report, use the Snapshot Run Date parameter to select a snapshot containing archived conflicts you want to see.

Because the Archive User Conflicts program runs automatically, there is typically no need to run it manually, even though it is available to be run. If you choose to run it, supply a single parameter: In the Archive field of the Submit New Program panel, enter a date and time. Conflict data generated before then is archived. You can type the date and time, in the format *DD-Mon-YYYY HH:MM AM/PM*. Alternatively, click on a grid-like icon next to the field, and a pop-up calendar appears. In it, click on the < or >symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want. The pop-up window closes, and the date you selected appears in the field, along with the current time. You can edit the time.

## Extract SOD Conflict Rules

The Extract SOD Conflict Rules program generates a CSV file containing a record of each SOD rule that is not end-dated. The file is used for uploading rules to another instance. It takes no parameters.

The CSV file is located in the directory that corresponds to the $APPLCSF/$APPLOUT environment variables on the Oracle ERP server. The file name is o*ProgramID*.out, in which the *ProgramID* placeholder stands for the ID number generated as you run the Extract SOD Conflict Rules program. This number is displayed in the Program ID field of the View Submitted Program panel.

## Load SOD Conflict Rules

Load SOD Conflict Rules uploads rule definitions from a CSV file. That file is generated either by the Extract SOD Conflict Rules request or from a spreadsheet provided by Oracle. The program takes the following parameters:

- Load: Select Yes to upload SOD rules from a CSV file, or No to validate the rules without loading them.
- Flat File Name: Enter the name (up to 30 characters) of the CSV file from which you are uploading rules.
- Flat File Path: Enter the directory path to the file from which you are uploading rules. (In conformance with UNIX conventions, the path must end in a slash).
- Log Details: Select Yes to create a detailed log or No to create a more cursory log. Typically, select Yes only to troubleshoot a problem with an upload operation.

## Reset User Conflicts

The Reset User Conflicts program rescinds the provisional assignment of conflicting responsibilities to a user if no approver has passed judgment on the assignment. Until an approver acts, the user has no access to the responsibilities and the assignment cannot be changed. If the judgment never occurs (if, for example, the approver leaves

the company), the Reset User Conflicts request can be run; the user's responsibilities return to their original state, and the assignment can be made again (with the rule that generated the conflict rewritten to designate another approver). The program takes a single parameter: In the User Name list box of the Submit New Program panel, select the name of the user whose conflicts you want to reset.

## Populate WF Roles Table

The Populate WF Roles Table program filters workflow roles, as they are defined in Oracle Applications, to select those appropriate to serve as SOD-rule approvers, and places the filtered selection of roles in a table that supplies values to the Owner LOV on the Add SOD Rule panel. Run the program when ACTIVE Access Governor is installed, and whenever workflow roles are altered in Oracle Applications. The program takes no parameters.

## Populate User Access Data Table

The Populate User Access Data Table program updates a database table that contains information about users' responsibility, menu, and function assignments. The table provides this information to the SOD Remediation Impact Report and the Oracle EBS Security reports when they are run, and so whenever the reports are run, the Populate User Access Data Table program should be run first. If you use version 7.2.1 or 7.2.0 of Access Governor, the program takes no parameters.

If you use version 7.2.2, the program takes a single parameter, Only Active Responsibilities. Select Yes to have the program return data pertaining only to users' active responsibilities (and exclude users who have been assigned no active responsibilities). Select No to have the program return data for users assigned any responsibilities, whether active or inactive.

## Export/Import Groups and Rules

The Export/Import Groups and Rules program works with pairs of files, one containing entity groups and the other containing SOD rules. Use it to export groups and rules from an ACTIVE Access Governor instance to the files. Then, in a distinct operation on a second instance, use it to import the groups and rules from the files. It takes the following parameters:

- Group File Name: Enter the name of a CSV file to which you are exporting, or from which you are importing, groups.
- Rules File Name: Enter the name of a CSV file to which you are exporting, or from which you are importing, rules.
- Location: Enter the directory path to the files to which you are exporting, or from which you are importing, groups and rules.

- Mode: Select Export or Import to specify the operation the program is to perform.
- Debug: Select Yes to add content to the default Oracle log file, or No to withhold that content. Typically, select Yes only to troubleshoot a problem with an export or import operation.
- Default Reviewer: Select a user whose ID can be inserted as owner into rules as they are imported into an ACTIVE Access Governor instance. For a given rule, the original owner is retained during an import operation if that owner exists on the import instance, but this default reviewer is inserted into the rule if the original owner does not exist on the import instance. Be sure to specify a default reviewer that exists on the instance into which you intend to import rules.
- Default Approval Group: Select an approval group whose ID can be inserted into rules as they are imported into an ACTIVE Access Governor instance. For any rule that specifies an approval group, the original group is retained during an import operation if that group exists on the import instance, but this default group is inserted into the rule if the original group does not exist on the import instance. (If the original rule does not specify an approval group, this default group is not inserted into the rule on the import instance.) Be sure to specify a default approval group that exists on the instance into which you intend to import rules.

Although you do not need to, you can edit files (or write them from scratch) before importing them in the destination instance. To do so, use any text editor. Each file has a *.csv* extension. Each consists of a set of records; each record is a text string divided into fields; each field ends in a semicolon. A field can be blank (if the information it would contain is inappropriate for a given record), and if so it consists only of the delimiting semicolon.

In the group file, there is one record for each function or responsibility in each group, and records alternate among groups: The first entity in the first group is followed by the first entity in the second group, and so on until the first entity in every group is recorded. Next comes the second entity in the first group, the second entity in the second group, and so on. One group may, of course, have a smaller number of members than others; in that case, when the last record in the small group is recorded, the rotation continues without that group.

For example, suppose that Group1 contains five functions, Group2 contains two responsibilities, and Group3 contains three functions. The group file would order their records as follows:

```
Group1 Function1
Group2 Responsibility1
Group3 Function1
Group1 Function2
Group2 Responsibility2
Group3 Function2
Group1 Function3
Group3 Function3
Group1 Function4
Group1 Function5
```

A record in the group file comprises the following fields:

- Group Name.
- Group Description.
- Entity Type: The value *1* represents function and *2* represents responsibility.
- The application with which a function or responsibility is associated (or, for a function, the value *No Associated Application*).
- The name of the entity (function or responsibility) that is to be included in the group.
- For a function only, the internal Oracle name for the function.
- The Effective To date of the group, in the format *DD-Mon-YY*.

For example, the following record would add a function called Asset Calendars to a group called Assets Group:

```
Assets Group;This group contains functions within the Assets
application;1;Assets;Asset Calendars;FAXSUCAL;31-Dec-07;
```

In the rules file, there is one record for each pair of conflicting entities defined by each SOD rule, and all records for a given rule are grouped one after another. A record in the rule file comprises the following fields:

- Rule Name.
- Reason.
- Entity Type for the first of the two conflicting entities. The value *1* represents function and *2* represents responsibility.
- The application with which that first entity is associated (or, for a function, the value *No Associated Application*).
- The name of the first conflicting entity.
- For a function only, the internal Oracle name for the first conflicting function.
- Entity Type for the second of the two conflicting entities. The value *1* represents function and *2* represents responsibility.
- The application with which that second entity is associated (or, for a function, the value *No Associated Application*).
- The name of the second conflicting entity.
- For a function only, the internal Oracle name for the second conflicting function.
- Control Type: The value *1* represents Approval Required, *2* represents Prevent, *3* represents Allow with Rules, and *5* represents Approve with Rules. (The value *4* is not used.)
- Owner.
- The Effective To date for the rule, in the format *DD-Mon-YY*.

- Same OU: The value *Y* indicates that the rule applies only within individual operating units, and the value *N* indicates that the rule applies across operating units.
- Same SOB: The value *Y* indicates that the rule applies only within individual sets of books, and the value *N* indicates that the rule applies across sets of books.
- The name of the approval group (if any).
- Priority.
- The value *Group*. This field is populated only for a rule that sets entity groups in conflict.
- The name of the entity group that contains the first conflicting function or responsibility. This field is populated only for a rule that sets entity groups in conflict.
- The name of the entity group that contains the second conflicting function or responsibility. This field is populated only for a rule that sets entity groups in conflict.
- A final three fields are always blank (and so are always represented by three semicolons).

For example, the following record would define a conflict between two functions — Suppliers (in the Payables application) and Receivables Activities (in the Receivables application). Each belongs to an entity group, and the conflict is one among several defined by an Approve with Rules SOD rule — called Vend*Receive — that sets the two groups in conflict. The rule owner is a user whose ID is WSTEVENS, and there is no approval group. The rule priority is 3:

```
Vend*Receive;Vendor-selection functions should be separate from
receiving functions;1;Payables;Suppliers;AP_APXVDMVD;1;Receivables;
Receivables Activities;AR_ARXSUMRT;5;WSTEVENS;31-Dec-07;Y;Y;;3;
Group;Payables Functions Group;Receivables Functions Group;;;;
```

If you choose to edit these files, it is incumbent upon you to ensure that the content of the files is coordinated. If a rule sets groups in conflict, you must make certain that the groups are defined in the group file, and that a record exists in the rules file for each possible pair of conflicts — each item in one group must conflict with every item in every other group named in the rule. Where a piece of information is duplicated from one record to another (for example, a rule name, or the internal name of an Oracle function), you must ensure that it spelled exactly alike in every record of both files. Moreover, recall that a group can contain functions or responsibilities, but not both.

# Chapter 6

# Access Monitoring

Access Monitoring enables ACTIVE Governance users to request temporary access to database tables or to Oracle responsibilities. A user may request access for himself or for others, and the person for whom rights are requested need not have an existing user account either in Oracle Applications or in ACTIVE Governance. Each request specifies not only a person and the objects that may be assigned to him, but also dates on which the assignment is to begin and end, a temporary logon ID that is to provide access specifically to the requested objects, and a reason why access is sought.

Requests must be approved; they are routed by ACTIVE Governance workflows to approvers, who receive and respond to them at the Task Inbox of the ACTIVE Governance Platform. A user is prevented from creating a request if workflows are configured so that he is an approver for the request.

Upon approval of a request, the user who receives temporary access also receives an email message informing him of the rights he has been newly assigned, the dates on which the assignment begins and ends, and his temporary logon ID. If access has been granted to an Oracle responsibility, the message also includes a logon password (which is generated by ACTIVE Access Governor); if access has been granted to database tables, the message directs the user to consult his database administrator for a logon password. The requester also receives a confirming email message. Once granted, access is continually audited, and an Access Monitoring User Activity Report presents the audit results (see page 84).

Before any requests can be made, however, some setup steps must be completed:

- Database tables must be audit-enabled, regardless of whether they are to be accessed directly or through a responsibility. A set of tables is typically audit-enabled during system installation. Moreover within Oracle, through the use of an "embedded agent," a user can open an Access Monitoring Content form to view tables (and columns) that are already audit-enabled, and add to them.
- Database user IDs must be created. Access Monitoring maintains a set of 30 IDs for responsibility-access requests; as each user's access expires, his ID can be reused. However, a distinct set of IDs applies to database-table access, and a database administrator must create these database user IDs.
- ACTIVE Governance workflows must be configured to route access requests to approvers. For instructions on configuring them, see "Creating Workflows" in the *ACTIVE Governance Platform User's Guide*. As you review this information, note that the E-Business User ID Requested event pertains to the review of responsibility access requests, the DB User ID Requested event applies to the review of database access requests, and the Request SQL Created event is not used.

# Preparing Tables for Auditing

When a user requests access, he is able to select only among tables that are enabled for auditing, or responsibilities supported by audit-enabled tables. Even within audit-enabled tables, access can be granted only to specified columns (although for each, translation values — corresponding columns in a lookup table — may be specified).

## Selecting Audit Tables and Columns

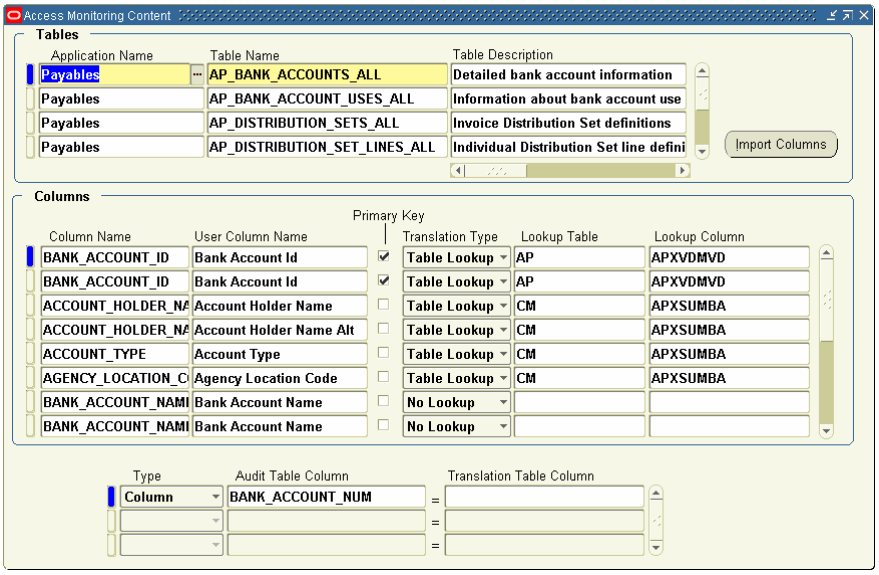
To add to the selection of tables, columns, and translations available for access requests, open your instance of Oracle Applications and select the GRC Controls responsibility. From the available applications, select Access Monitor Content. An Access Monitoring Content form appears (as shown at the top of the next page).

In it, select a table.

If you know that a table is already audit-enabled (and you want to edit or add to the audit columns selected for it), use the Oracle query feature to load its record in the Tables block. Doing so also loads entries in the Columns block for all columns in the table that have already been selected for auditing. You can query on an application instead to load records for all the audit-enabled tables associated with it, and click in one of the rows to select a particular table.

If a table is not yet audit-enabled:

1. In a blank row of the Tables block, select an application in the Application Name list of values (LOV).
2. The Table Name LOV can now display only tables that support the application you've chosen. Select one of them. Not only does the Table Name field display your selection, but the Table Description field also displays the description configured for it.

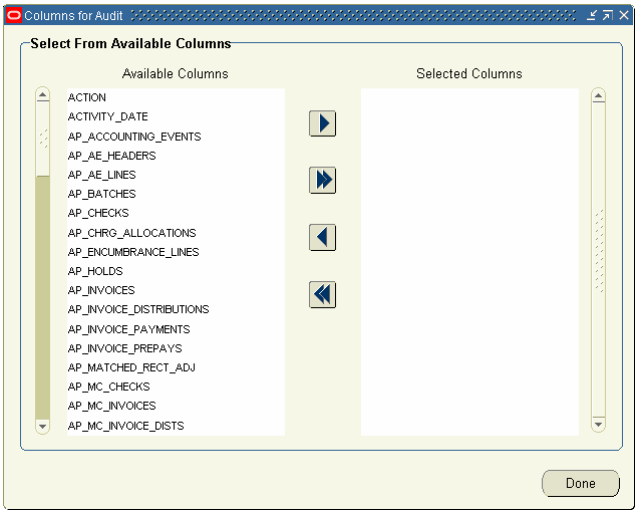



**3** Optionally, use the scroll bar located beneath the Table Description field to scroll to the right and enter values in additional fields:

- Form Name: Enter the internal name for the form supported by the table you selected. (For example, *APXVDMVD* is the internal name for the Enter Vendors form.)
- User Form Name: This field automatically displays the external name for the form whose internal name you selected. You cannot enter a value directly in this field.
- Block Name: Enter the internal name for the block that both exists on the form you selected and is supported by the table you selected.

Next, choose the columns you want to audit.

**1** Click on the Import Columns button, and a Columns for Audit form appears:



2 Select the columns individually or collectively:

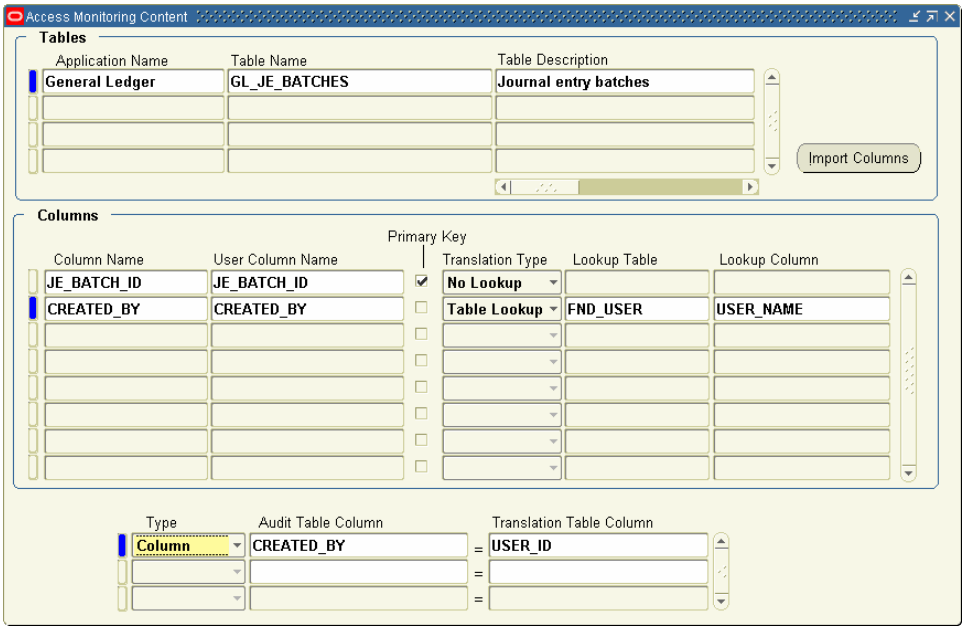
- In the Available Columns box, click on the name of a column you want to audit. Then click on the right-pointing single-arrow button to move it to the Selected Columns box. Repeat for each column you want.
- Alternatively, click on the right-pointing double-arrow button to move all columns to the Selected Columns box.
- If you reconsider, you can click on a column name in the Selected Columns box, then click on the left-pointing single-arrow button to move it back to the Available Columns box. Or, click on the left-pointing double-arrow button to move all columns back to the Available Columns box.

3 When you are satisfied with your selection, click on the Done button. For each column you selected, a row appears in the Columns block of the Access Monitoring Content form. The Column Name field shows the internal name, and the User Column Name field shows the external name, for the column. If the column is a primary key, the Primary Key check box is selected.

## Setting Up Translations

You can link audited columns to translations — meaningful values that correspond to the values held in audited tables. For example, a person's actual name might be the translation value when an audited table column holds a numeric ID for the person.

If you want the Access Monitoring User Activity Report to display actual values from an audited column, select No Lookup in its Translation Type LOV in the Access Monitoring Content form. (In the example illustrated below, this setting has been configured for a JE_BATCH_ID column.)



If, however, you want the report to display a translation value for an audited column, join it to a corresponding column in a lookup table. Typically, you would specify a linkage among three columns:

- The first is the column that contains an audited value. In the example illustrated above, this is CREATED_BY in the GL_JE_BATCHES table.
- The second is a lookup-table column that contains an identifying value — the same value as in the audited table. In the example illustrated above, this is USER_ID in the FND_USR table.
- The last is a column in the lookup table that contains the translation value. In the example illustrated above, this is USER_NAME in the FND_USR table.

To set up this linkage:

1. In the Translation Type LOV, select Table Lookup.
2. In the Lookup Table field, select the name of the lookup table you want.
3. In the Lookup Column field, select the name of the lookup-table column that contains translation values for the audited column.
4. Move to the lower grid and, in the Type LOV, select the value *Column*.
5. In the Audit Table Column field, select once again the column from the audited table that contains the audited value.
6. In the Translation Table Column field, select the lookup-table column that contains the identifying value.

In the lower grid, you can complete as many rows as you like to create a translation value as complex as you like. The rows have an AND relationship — all must be true for a value to be returned.

### Saving Your Work

Once you've finished selecting columns and defining translation values, save the new configuration: click on File in the menu bar, then on Save in the File menu. Or, click on the Save icon, located first on the left in the toolbar.

## Creating Database IDs

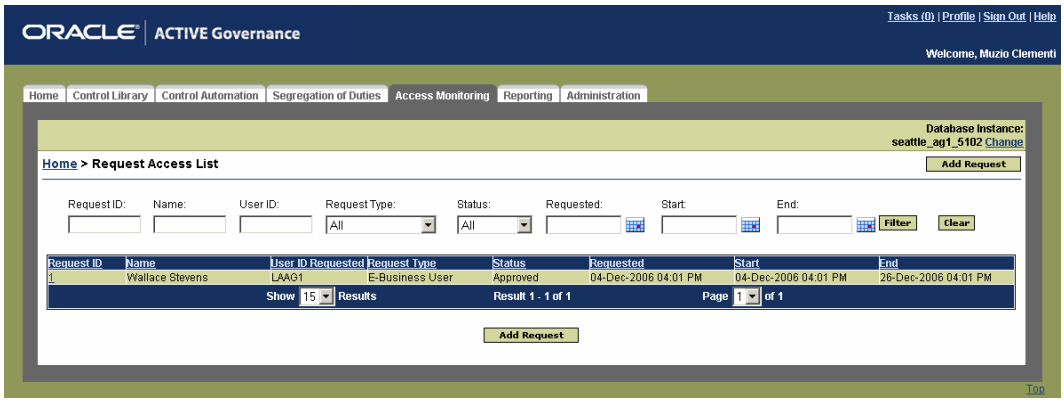
Before direct access to database tables can be requested, database administrators must create database IDs to be assigned to users who receive access. Each of these user IDs must begin with the letters *LAAG*. Although they may otherwise follow any format, the recommended format is *LAAGDBx*, where *x* is a unique number.

After the IDs are created, a concurrent request, called Access Monitor — DB Users Synchronization Process, must be run in the GRC Controls responsibility of Oracle Applications; this enables Access Monitoring to recognize the IDs and display them so that they are available for selection. The request takes no parameters.

**Note**
Three other concurrent requests apply to Access Monitoring. One, called Access Monitor — Content Load, is intended for use by Professional Services. The other two, called Access Monitor — Cleanup Process and Access Monitor — Create User, are used in the background by Access Monitoring. None of these three concurrent requests should be run by end-users.

# Displaying a List of Access Requests

When you start Access Monitoring, a Request Access List panel displays summary descriptions of all requests that have ever been made. Each entry includes and ID number assigned to the request, the name and temporary ID of the user for whom access was requested, and the type of access — "E-Business User" is a request for access to an Oracle responsibility, and "DB User" is a request for access to database tables. The panel further presents the date on which the request was made, as well as the dates on which the user's access is proposed to start and end. Finally, it displays the status of the request — Pending, Approved, or Rejected.




From this panel, you can create a new request or view the details of an existing request.

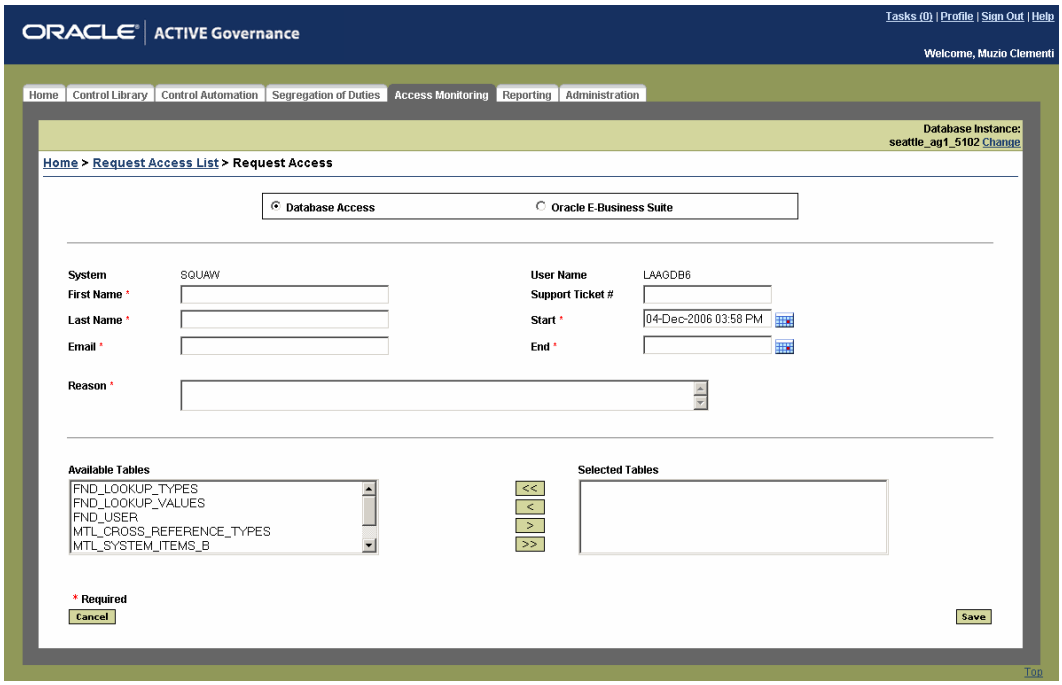
# Creating a New Request

To create a new access request, click on either of two Add Request buttons in the List panel. A Request Access panel appears. If you have installed version 7.2.1 or later, the panel looks like the one shown at the top of the next page. For the initial 7.2.0 release, the panel contains the same features, positioned slightly differently.

## Starting the Request

Begin to create the request by identifying the user, dates, and database instance for which access rights are requested, and the type of request you want to make:

**1** If you want to request access to database tables, click on the Database Access radio button. To request access to Oracle responsibilities, click on the Oracle E-Business Suite radio button.




2. Your request applies to the database instance to which you are logged on, and the System field displays the name of the instance. You cannot change this field value directly. If you want to request access to another database instance, use the Change link (at the upper right of the panel) to log on to that instance.

3. In the First Name and Last Name fields, enter the given name and surname of the user for whom you are requesting access.

4. In the Email field, enter the email address of the user for whom you are requesting access. This is the address at which the user is notified of his new access rights, logon ID, and password. (Your own confirming email message goes to the address configured for you in the Add User panel of the ACTIVE Governance Platform.)

5. The Support Ticket # field is for use if you are requesting access in response to a notification from an issue-tracking system. If so, enter the number assigned to the issue in the tracking system. (Any format is acceptable.) If not, leave the field blank.

6. The Start field displays the date and time at which you create the request, and the End field is blank. If you want the user to receive access immediately upon approval of the request, retain the default Start value; otherwise specify a later date and time. The access you are requesting is necessarily temporary, so you must supply an End date and time. The default Start value is read from the Oracle Applications server to which you are requesting access, and values you enter should be appropriate to that server.

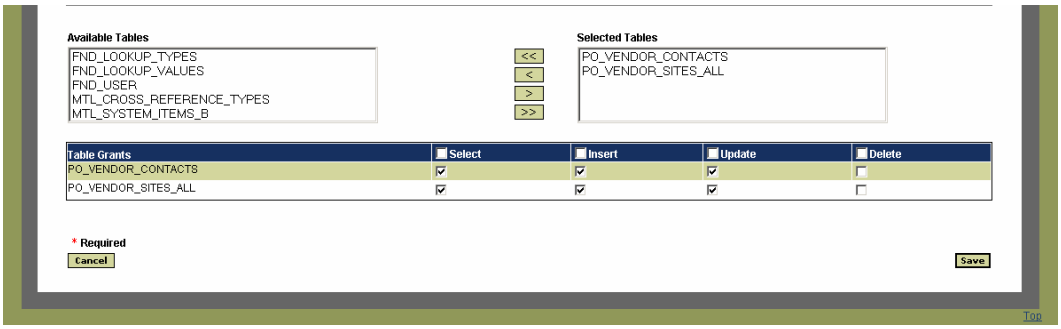
   You can insert a date and time manually in either field (use the format *DD-Mon-YYYY HH:MM AM/PM*). Alternatively, you can click on the icon next to either field, and a pop-up calendar appears. In it, click on the < or > symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want. The pop-up window closes, and the date

you selected appears in the field, together with the time of day at the moment you select the date. You can edit the time.

**7** In the Reason field, type an explanation for the user's being given the access you've requested.

## Completing a Request for Database-Table Access

If you selected the Database Access radio button as you started the request, the User Name field displays an unused logon ID, selected from those your DBA has created for database access; you cannot change it. In the bottom portion of the panel, the Available Tables and Selected Tables fields are active, with the Available Tables field listing those tables that have been audit-enabled.




Complete the following steps:

**1** Select tables by moving them from the Available Tables field to the Selected Tables field:

- Highlight tables you intend to select. Click on a table to highlight it. Or, to highlight a continuous group of tables, click on the first one, hold down the Shift key, and click on the last one. To highlight a discontinuous group, hold the Ctrl key as you click on tables.
- Click on the > button to move highlighted tables from the Available field to the Selected field. Or, click on the >> button to send all values in the Available field (regardless of whether you've highlighted them first) to the Selected field.
- If you reconsider, click on the < button to return highlighted values from the Selected field to the Available field. Or, click on the << button to return all values in the Selected field to the Available field.

**2** When you select a table, a Table Grants grid appears; it generates a row for each table you select. For each table, select the check boxes corresponding to the privileges you want to assign — Select, Insert, Update, and Delete. Or choose any of these privileges for all tables by selecting its check box in the header row of the grid.

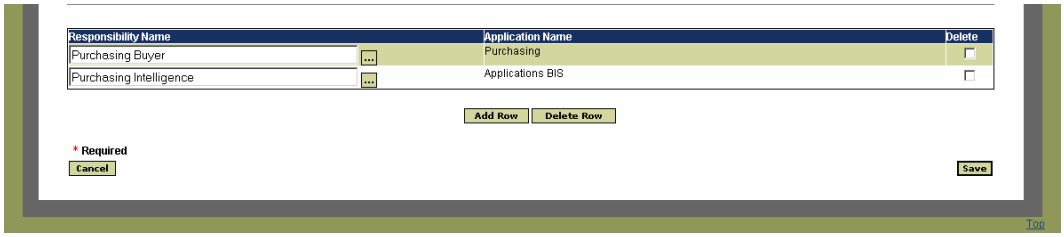
**3** Click on the Save button. A pop-up window prompts to submit the request. Click on the OK button. ACTIVE Governance submits the request and restores the Request Access List panel, with a new entry for the request you've made.

## Completing a Request for Responsibility Access

If you selected the Oracle E-Business Suite radio button as you started the request, the User Name field displays an unused logon ID, selected from those provided by Oracle for responsibility access; you cannot change it.

If you are using the initial version 7.2.0 release, a Responsibility list of values becomes active (and fields pertaining to database tables become inactive). In this field, select the responsibility you want to assign to the user; you can select only one.

If you have installed version 7.2.1, a Responsibility grid appears at the bottom of the panel, initially displaying only a header row (and the fields pertaining to database tables disappear).




In this grid, you can request access to any number of responsibilities. Complete the following steps:

1. For each responsibility you want to select, click on the Add Row button.
2. In each row that you add, the Responsibility Name field is a list of values. In each, select a responsibility. In each row, Access Monitoring automatically populates the Application Name field with the application to which the selected responsibility belongs; you cannot change this value.
3. If you have selected responsibilities you do not want to request for the user, or you have created more rows that you need, select the Delete check box in the rows you no longer want, and then click on the Delete Row button.

No matter whether you are using the 7.2.0 or 7.2.1 release, click on the Save button when you are satisfied with your selection. A pop-up window prompts you to submit the request; click on its OK button. ACTIVE Governance submits the request and restores the Request Access List panel, with a new entry for your request.

# Viewing Requests

From the Request Access List panel, you can select an existing request to view the values selected for it as it was configured and its current status. However, ACTIVE Governance does not delete requests from the List panel. To manage long lists of requests, you can limit the contents of the List panel to entries that satisfy filtering criteria:

1. Specify filtering criteria by entering complementary values in any combination of the fields that run horizontally above the list of requests:
   - Request ID: Enter a number to see the request for which that number is the request ID assigned by Access Monitoring.

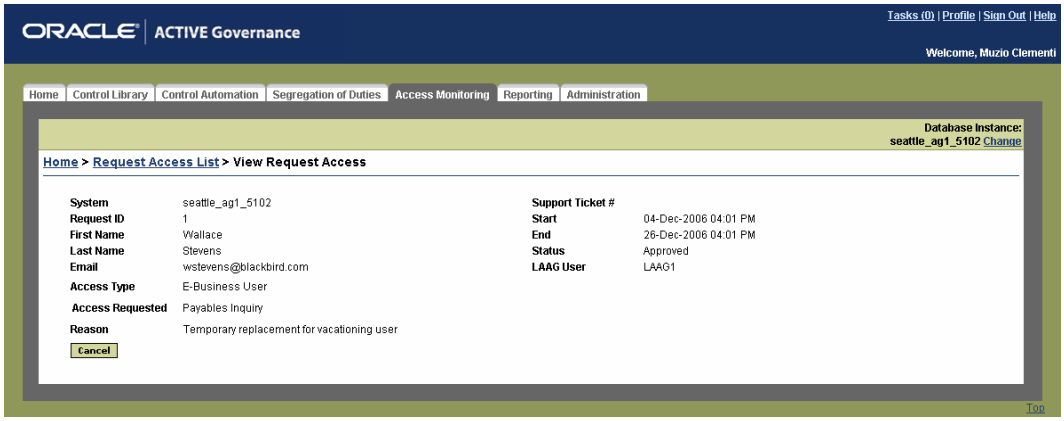
- Name: Enter the first or last name of a user for whom access has been requested to see entries pertaining to that user, or enter a text fragment to see entries that apply to all users whose names contain the fragment.
- User ID: Enter one of the temporary responsibility or database-table logon IDs to see requests assigning that ID to a user. (Responsibility-access user IDs use the format *LAAGx*, where *x* is a number; database-table-access user IDs start with *LAAG*, but otherwise follow a format specified at your site.)
- Request Type: Select the value *E-Business User* to see requests for responsibility access, *DB User* to see requests for database-table access, or *All* to see all requests. (Do not select the value *Execute SQL*.)
- Status: Select a status to see requests at that status, or *All* to see requests at all statuses. Options include *Approved* (requests that have been approved), *Rejected* (requests that have been rejected), *Pending* (requests for which no approval decision has yet been made), and *Failed* (requests that have been approved, but for which some processing error has occurred).
- Requested: Enter a date to see all requests created on that date.
- Start: Enter a date to see all requests for which this is the proposed start date.
- End: Enter a date to see all requests for which this is the proposed end date.

The three date filter fields display time of day as well as date, but the time is not significant. When you execute the filter, the panel displays all requests created on the selected date, or for which the date is the start or end date. As before, you can enter a date manually or select it from a pop-up window.

**2** When you finish specifying filtering criteria, click on the Filter button.

To discard filtering criteria and redisplay all access requests, click on the Clear button.

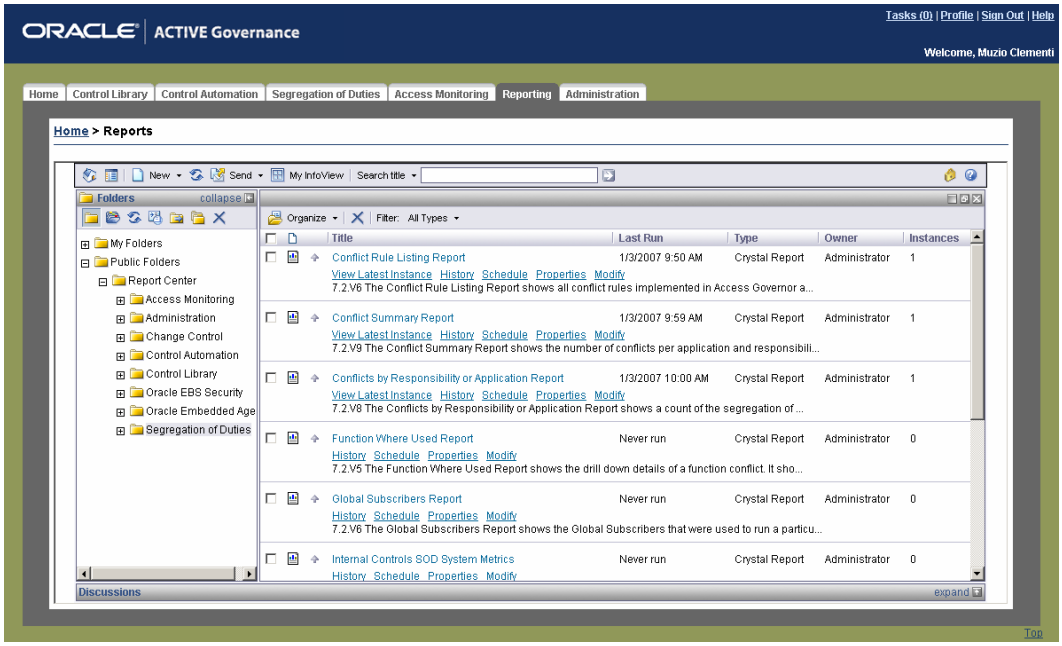
Having filtered the list, select a request by clicking on the name of the user for whom access is requested. The following View Request Access panel opens. This panel is read-only; you cannot change any of the values for a request after it's been submitted. After reviewing details, click on the Request Access List link in the breadcrumbs trail, or on the Cancel button, to return to the Request Access List panel.



# Chapter 7

# Reports

In ACTIVE Access Governor, reports present information about SOD analysis, rule configuration, and user access to responsibilities, menus, and functions. To run reports, open ACTIVE Governance and click on the Reporting tab to display the Reports panel:



A Folders area to the left of the Reports panel presents a hierarchical display of folders containing reports. In it, click on Public Folders, and then Report Center. The panel then presents a selection of folders, three of which pertain to ACTIVE Access Governor: Segregation of Duties, Access Monitoring, and Oracle EBS Security.

To open a report, locate the folder that contains it under the Report Center heading in the Folders panel. Click on the folder, and the larger panel on the right presents links to the reports contained in the folder. Click on the link for the report you want. The larger panel then displays fields in which you can enter values for report parameters; do so, then click on the OK button to run the report. (The reports contained in each folder, and the parameters that apply to each report, are listed below.)

## Exporting a Report

When you generate a report, it appears in the larger panel on the right of the Reports browser. For ease of viewing, however, you may want to export it to another format, such as Adobe Acrobat. To do so:

1. Click on the Export icon in the Reports browser. (It looks like two juxtaposed rectangles, representing a disc and a sheet of paper. It appears only when a report has been generated, and is located at the upper left corner of the larger panel in the Reports browser.)
2. An Export Report dialog appears. In it, select a destination program in the File Format field (for example, Adobe Acrobat). Then click on the OK button.
3. A dialog presents you with options appropriate to the program to which you've elected to export the file — for example, save or open in Adobe Acrobat. If you select the open option, the report opens in a new window. If you select the save option, you can specify a file path and name to which to save it.

## Other Report Features

ACTIVE Governance reports are presented through use of a "third-party" component, which offers features in addition to the presentation or exporting of reports. For documentation of these features, open the Help file available from the Reports browser. You can do this by clicking on a Help icon, which looks like a question mark enclosed in a circle, and is located at the very right of the tool bar, just above the upper right corner of the larger panel in the Reports browser.

## The Data Source Parameter

One report parameter — called Oracle ERP Agent Source Data — is used by every report in all three folders. For it, select the Access Governor instance about which you want to generate reports. For a given instance, the parameter prompt lists two data sources, one of which holds Oracle Applications data and the other of which holds data generated by the embedded agent that supports Access Governor. Choose the latter. If your site follows Oracle naming conventions, its name contains the

value *XXLAAPPS*. If not, consult your database administrator to distinguish the two data sources. Typically, you supply this value twice for a given report, first to generate a list of the remaining parameters and then, within that list, to generate the report itself.

# Segregation of Duties Folder

The Segregation of Duties folder contains the following reports.

## Conflict Rule Listing Report

The Conflict Rule Listing Report lists SOD rules and, for each rule, displays the values that define it. For a rule that sets more than two entities in conflict, the report includes a discrete entry for each pair of conflicting entities. If you choose to include a graph, it displays bars representing the ten applications for which the most SOD rules have been written, with the size of each bar corresponding to the number of rules for its application. As you run the report, you can select the following parameters:

- Application: Select one or more applications to view rules involving those applications, or select All to view rules involving all applications.
- Conflict Name: Select one or more rules to view information about those rules. Or select All to see information about all rules.
- Entity Type: Select Function or Responsibility to view rules that find conflicts in one entity or the other, or Both to see both types of rule.
- Control Type: Select a control type — Approval Required, Approve with Rules, Allow with Rules, or Prevent — to view only information on rules involving that type. Or accept All to see information on rules involving all types.
- Same OU: Select Yes to list rules that apply within operating units or No to list rules that apply across operating units. Or select Both to list both types of rule.
- Same SOB: Select Yes to list rules that apply within sets of books or No to list rules that apply across sets of books. Or select Both to list both types of rule. This parameter applies only if you are reporting on a data source that runs Oracle Applications Release 11.5.3–11.5.10.
- Active Conflicts: Select Yes to list rules for which conflicts are not end-dated or No to list rules for which conflicts are end-dated. Or select Both to list both types of rule.
- Include Graph: Select Yes to include the graph in the report or No to exclude the graph.
- Same Access Sets: Select Yes to list rules that generate conflicts if the conflicting entities would enable a user to access data in ledgers belonging to individual data access sets, or No to list rules that generate conflicts across data access sets. Or select Both to list both types of rule. This parameter applies only if you are reporting on a data source that runs Oracle Applications Release 12.

## Conflict Summary Report

The Conflict Summary Report lists responsibilities within each application, then shows the number of Allow with Rules, Prevent, Approved, Rejected, and Pending conflicts, and the total of those five counts, at each responsibility. (In the report, Allow with Rules conflicts are labeled *AWR*; conflicts generated by Approve with Rules or Approval Required SOD rules are apportioned among the Approved, Rejected, and Pending conflicts.) If you choose to include a graph, it displays bars representing the ten applications containing the most conflicts, with the size of each bar corresponding to the number of conflicts for its application.

There are two ways in which a responsibility may be considered to be associated with an application: the first is a direct association, with a given responsibility linked to only one application. The second way is through the following linkage: an application is associated with a function, which is associated with a menu, which is granted to a responsibility. To ensure a correct count of both function-based and responsibility-based conflicts for each application, the report bases its calculations on the second association. As a result, the report may show responsibilities within an application that are not directly linked to the application.

Moreover, a given conflict is counted in each of the applications (base and conflicting) it affects. A rule, for example, may define a conflict between two functions, each associated with a distinct application. If the rule were to generate 10 conflicts, the report would show 10 conflicts in each of the applications, for a total of 20.

As you generate the report, select values for these parameters:

- Application: Select one or more applications to view summary values for conflicts associated with those applications. Or, select All to view summary values for conflicts associated with all applications.
- Set of Books: Select one or more sets of books to view only responsibilities belonging to those sets of books, and only the conflicts that apply to them.
- Operating Unit: Select one or more operating units to view only responsibilities belonging to those operating units, and only the conflicts that apply to them.
- Snapshot: Select a snapshot date to view summary values for conflicts generated in that snapshot.
- Include Graph: Select Yes to include the graph in the report or No to exclude the graph.

## Conflicts by Responsibility or Application Report

The Conflicts by Responsibility or Application Report devotes a section to each responsibility or application (depending on how one chooses to focus the report). For each, it lists the SOD rules that have generated conflicts; for each rule, it displays the number of conflicts generated within the responsibility or application, as well as the entity, application, conflicting entity, conflicting application, and priority specified in the rule. (The entity is the first of two functions or responsibilities that the rule de-

fines as conflicting; the application is the application to which that entity belongs; the conflicting entity is the second of two functions or responsibilities that the rule defines as conflicting; and the conflicting application is the application to which the conflicting entity belongs.)

You may choose to include a graph. If so, it takes the form of a pie chart in which each wedge represents the number of conflicts (as a percentage of the whole) in each of the ten responsibilities or applications containing the most conflicts.

As you generate the report, select values for the following parameters:

- View By: Select *Application* or *Responsibility* to have the report group conflicts by one or the other.
- Snapshot: Select a snapshot date to view values for conflicts generated in that snapshot.
- Priority: Select one or more priority numbers to view only conflicts generated by rules assigned the priorities you select.
- Include Graph: Select Yes to include the graph in the report or No to exclude the graph.

## Function Where Used Report

The Function Where Used Report identifies menus and responsibilities that provide access to specific instances of functions. In the case of menus, the report names a parent menu and lists the submenus of that parent from which a function is available. The intention is for you to trace the paths of functions involved in function-based conflicts in order to resolve them: with this information you can create a global subscriber for a function, exclude it from a responsibility, remove it from a menu, or exclude such a menu from a responsibility. Be aware, however, that the report can generate information about instances of functions that are not involved in conflicts — those, for example, that are already excluded from responsibilities or for which global subscribers are already created. Use report parameters to focus the report on instances of functions actually involved in conflicts. As you generate the report, select values for the following parameters:

- Conflict Name: Select one or more SOD rules to trace the menu paths of functions named in those rules. (The selection field lists only function-based SOD rules.)
- Responsibility: Select one or more responsibilities to focus the report on functions available from those responsibilities.
- Function: Select a "base" function (the first of two that a rule sets in conflict) whose menu path you want to know. For a rule that includes more than two functions, the report identifies pairs of functions for which conflicts exist, and lists the first of each pair in this prompt.
- Conflicting Function: Select a "conflicting" function (the second of two that a rule sets in conflict) whose menu path you want to know. For a rule that includes more than two functions, the report identifies pairs of functions for which conflicts exist, and lists the second of each pair in this prompt.

## Global Subscribers Report

The Global Subscribers Report displays settings for all global subscribers that have been `configured`. It displays headings for all possible subscriber types, even if no subscribers have been configured for a given type. It presents a distinct set of headings for each snapshot, providing data about subscribers configured at the moment each snapshot was generated.

## Internal Controls SOD System Metrics Report

The Internal Controls SOD System Metrics report provides information that may be useful in the evaluation of SOD rules: a list and count of operating units, a list and count of sets of books (including, for each, its name, short name, and ID), a list of users assigned more than a specified number of responsibilities (together with the number for each), and a list of users who have not logged on for a specified number of days (together with the number for each). Finally, there is a summary, which provides counts of operating units, sets of books, active and total users, active and total responsibilities, and active and total SOD rules. As you run the report, select values for the following parameters:

- Responsibilities Greater Than: Enter a number to have the report list users assigned more than that number of responsibilities.
- Logon Days Greater Than: Enter a number to have the report list users who have not logged on for more than that number of days.

## Responsibilities with Conflicts Report

The Responsibilities with Conflicts Report lists responsibilities for which conflicts exist, and identifies the components of each conflict as well as the SOD rule that defines it. If you choose to include a graph, it displays bars representing the ten responsibilities containing the most conflicts, with the size of each bar corresponding to the number of conflicts. As you generate the report, select values for the following parameters:

- Application: Select one or more applications to view responsibilities that have conflicts associated with those applications. Or select All to view responsibilities that have conflicts associated with all applications.
- Responsibility: Select a responsibility to view only conflicts for that responsibility. Or select All to view conflicts for all responsibilities.
- Function: Select one or more functions to view only conflicts involving those functions. Or select All to view conflicts involving all functions.
- Conflict Name: Select one or more SOD rule names to view only conflicts generated by those rules. Or select All to view conflicts generated by all rules.
- Control Type: Select a control type — Approval Required, Approve with Rules, Allow with Rules, or Prevent — to view only conflicts of that type. Or accept the default value, All, to view conflicts of all types.

- Set of Books: Select one or more sets of books to view only conflicts for which the base entity (the function or responsibility named first in the conflict) is contained in those sets of books. Or select All to view conflicts for which the base entity may exist in any set of books.
- Operating Unit: Select one or more operating units to view only conflicts for which the base entity is contained in those operating units. Or select All to view conflicts for which the base entity may exist in any operating unit.
- Conflict Set of Books: Select one or more sets of books to view only conflicts for which the conflicting entity (the function or responsibility named second in the conflict) is contained in those sets of books. Or select All to view conflicts for which the conflicting entity may exist in any set of books.
- Conflict Operating Unit: Select one or more sets of books to view only conflicts for which the conflicting entity is contained in those operating units. Or select All to view conflicts for which the conflicting entity may exist in any operating unit.
- Priority: Select one or more priority numbers to view only conflicts generated by rules assigned the priorities you select.
- Snapshot: Select a snapshot date to view summary values for conflicts generated in that snapshot.
- Intra Responsibility Conflict Only: Select Yes to view information on conflicts between functions within a responsibility, or No to view information on conflicts between entities across responsibilities.
- Include Graph: Select Yes to include the graph in the report or No to exclude the graph.
- Include User Details: Select the value *Include User Details* to have each entry identify the user affected by a conflict, or the value *Not Include User Details* to have each entry exclude this information.

## Responsibility Conflicts by Rule Report

The Responsibility Conflicts by Rule Report lists conflicts that exist within a designated snapshot, displaying the name of the rule that generated the conflict, the user to whom it applies, and two responsibilities that the rule defines as conflicting (if it is responsibility-based) or that provide access to conflicting functions (if the rule is function-based). An individual rule may generate conflicts for more than one user, and it may find conflicts for an individual user among more than one pair of assigned responsibilities, so the report typically includes many entries for a given rule and, within the rule, many entries for a given user. The conflicts are ordered alphabetically by rule name, within a rule alphabetically by user name, and for a user alphabetically by base responsibility. As you generate the report, select values for the following parameters:

- Conflict Name: Select one or more SOD rules about which you want the report to present results.

- Snapshot: Select the snapshot (the generation of user conflicts) about which you want the report to present results.
- User: Enter one or more user names to view information on conflicts concerning those users. Or select All to see information on conflicts concerning all users.
- Approval Status: Select a status — Allow with Rules, Prevent, Approved, Pending, or Rejected — to view conflicts at that status. Or select All to view conflicts at all statuses.

## Responsibility Menu Report

The Responsibility Menu Report devotes a section to each pair of conflicting entities (functions or responsibilities), as defined by SOD rules. Each section is divided into rows, and each row displays a combination of responsibilities, menus (both internal and display names are given), sets of books, and operating units from which the conflicting entities are available to users. Each section concludes with a count of the conflicts that exist for the two entities. As you generate the report, select values for the following parameters:

- Application: Select one or more applications to view conflicts associated with those applications. Or, select All to view conflicts associated with all applications.
- Responsibility: Select one or more responsibilities to view only conflicts for those responsibilities. Or select All to view conflicts for all responsibilities.
- Function: Select one or more functions to view only conflicts for those functions. Or select All to view conflicts for all functions.
- Conflict Name: Select one or more SOD rules to view only conflicts generated by those rules. Or select All to view conflicts for all rules.
- Resp Set of Books: Select one or more sets of books to view only conflicts for which the base responsibility belongs to those sets of books. (The base responsibility is the first of two that a rule sets in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the filter identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.)
- Resp Operating Unit: Select one or more operating units to view only conflicts for which the base responsibility belongs to those operating units.
- Conflict Resp Operating Unit: Select one or more operating units to view only conflicts for which the conflicting responsibility belongs to those operating units.
- Conflict Resp Set of Books: Select one or more sets of books to view only conflicts for which the conflicting responsibility belongs to those sets of books. (The conflicting responsibility is the second of two that a rule sets in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the filter identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.)

- Snapshot: Select a snapshot date to view values for conflicts generated in that snapshot.
- Intra Responsibility Conflicts Only: Select Yes to view conflicts between functions within a responsibility, or No for conflicts between entities across responsibilities.
- Report Output: Select Print or Export to determine the format of the report.

## Simulation History Report

The Simulation History Report displays configuration details of the rules involved in simulation runs. It groups rules by run, and for each run specifies the simulation scenario to which the rules belong, the date and time of the run, and the user who ran the simulation. For each rule the details include the action being simulated (exclusion, removal, or insertion); the type of entity being acted upon (function, submenu, or menu); the name of that entity; the type of entity from which it is to be excluded or removed, or in which it is to be inserted (menu or responsibility); the name of that entity; and whether the rule is enabled.

As you generate the report, select values for the following parameters:

- Simulation Date/Time: Select the date on which the simulation rules were run.
- Action Name: Select any combination of simulation actions that may be configured — Exclude, Remove, or Insert — to have the report show only rules configured to perform those actions.
- User Name: Select the name of the user who performed a simulation operation.
- Active Simulation: Select Enabled or Disabled to have the report include only active or inactive rules (those for which the Enabled check box was selected or cleared, respectively, when they were configured), or select Include Both to have the report display rules in both states.

## SOD Approver Performance Report

The SOD Approver Performance Report shows how each approver has disposed of conflicts. The section of the report devoted to a given approver shows the numbers of conflicts he has approved, rejected, and pended, for each application and in total. It also shows average numbers of days per judgment — at each status within each application, as a total for each status, as a total for each application, and for all judgments.

The report can include four graphs. Two are pie charts, one showing judgments at each status, and the other average days per judgment, both as a percentage of total judgments. The other two are bar graphs, one showing the numbers of judgments, and the other the average days per judgment, for each application. (Each of these graphs shows results for all reviewers rather than individual reviewers.)

As you generate the report, select values for the following parameters:

- Application: Select one or more applications to view results for those applications, or select All to view results for all applications.
- Approved By: Select one or more approvers to view results for those approvers, or select All to view results for all approvers.
- Date Range: Define a period the report should cover. You may enter dates in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the start date and select the No Lower Value check box to start with the earliest existing judgment, or omit the end date and select the No Upper Value check box to finish with the latest existing judgment.

  If you do enter actual dates, select an Include This Value check box (for either or both dates) to include the value you specify in the period, or clear the check box to exclude the value (thus selecting transactions that begin after but not on the start date, or end before but not on the end date). You can type dates manually (use the format *YYYY-MM-DD*) or click on the calendar icons to select dates.
- Include Graph: Select Yes to include graphs in the report or No to exclude graphs.

## SOD Remediation Impact Report

The SOD Remediation Impact Report lists responsibilities and users who would be affected if a simulation scenario were used in a remediation operation. It compiles distinct lists of responsibilities and users. The latter includes those involved in conflicts and those with legitimate access to functions and responsibilities, and matches each user to the responsibility through which he would be affected. To ensure that the report presents current information, run the Populate User Access Data Table background program before running the report.

As you run the report, use its Simulation Scenario Name parameter to select the scenario for which you want to see results. This parameter offers for selection only those scenarios that contain at least one enabled rule.

## User Conflicts Report

The User Conflicts Report presents information on the resolution of conflicts for individual users. For each SOD rule that has generated conflicts, it displays the rule name, the type of entity (function or responsibility) the rule sets in conflict, the names of the base and conflicting entities as well as applications with which they are associated, the control type of the rule, and the number of conflicts the rule has generated. For each rule, the report then lists individual conflicts. For each, it displays the name of the affected user; information about the base and conflicting responsibilities, including the name of each, the start and end dates of its assignment to the user, and the set of books and operating unit through which the user has access to it; and finally the status of the conflict (as recorded in the Action History

panel), its reviewer, the date upon which action was taken (status was set in the Action History or Mass Update panel), and the comments recorded at that time.

The report can include two bar charts. In one, each bar represents one of the ten applications with the most conflicts, and in the other each bar represents one of the ten SOD rules that have generated the most conflicts. In each, the size of a bar corresponds to the number of conflicts.

As you generate the report, select values for the following parameters:

- Application: Select one or more applications to view conflicts associated with those applications. Or select All to view conflicts associated with all applications.
- Conflict Name: Select one or more SOD rules to view information on the resolution of conflicts generated by those rules. Or select All to see information on the resolution of conflicts generated by all rules.
- User: Enter one or more user names to view only information on the resolution of conflicts concerning those users. Or select All to see information on the resolution of conflicts concerning all users.
- Resp Set of Books: Select one or more sets of books to view only conflicts for which the base responsibility belongs to those sets of books. (The base responsibility is the first of two that a rule sets in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the filter identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.)
- Resp Operating Unit: Select one or more operating units to view only conflicts for which the base responsibility belongs to those operating units.
- Conflict Resp Set of Books: Select one or more sets of books to view only conflicts for which the conflicting responsibility belongs to those sets of books. (The conflicting responsibility is the second of two that a rule sets in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the filter identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.)
- Conflict Resp Operating Unit: Select one or more operating units to view only conflicts for which the conflicting responsibility belongs to those operating units.
- Snapshot: Select a snapshot date to view conflicts generated in that snapshot.
- Control Type: Select a control type — Approval Required, Approve with Rules, Allow with Rules, or Prevent — to view only conflicts of that type. Or accept the default value, All, to see conflicts of all types.
- Entity Type: Select Function or Responsibility to view conflicts in one entity or the other, or Both to see both types of conflict.
- Approval Status: Select a status — Approved, Pending, or Rejected — to view conflicts only at that status, or select All to view conflicts at every status (including Prevent or Allow with Rules).

- Show Action Comments: Select Yes to have the report contain comments recorded in the Action History panel or the Mass Update panel as status was set for the conflicts. Or select No to have the report exclude these comments.
- Include Graph: Select Yes to include graphs in the report or No to exclude graphs.

## User Conflicts Master CSV Report

The User Conflicts Master CSV Report produces a CSV (text) file that contains records of SOD rules and conflicts they have generated. Unlike other reports, this one is not meant to be viewed in the browser available from the Reports tab. Instead, it is intended simply to produce the CSV file for export to a spreadsheet for further analysis. Once the report is generated, click on the Export icon in the Reports browser. (It looks like two juxtaposed rectangles, representing a disc and a sheet of paper, and is located at the upper left corner of the main Reports panel.) Then, in an Export Report dialog, select a destination program (for example, Excel) and click on the OK button.

As you generate the report, select values for the following parameters:

- Application: Specify one or more applications to select SOD rules and conflicts associated with them. Or select All to select rules associated with all applications.
- Responsibility: Specify one or more responsibilities to select rules and conflicts associated with those responsibilities. Or select All to select rules associated with all responsibilities.
- Conflict Name: Specify one or SOD rules to see them and the conflicts they have generated. Or select All to select all rules.
- User Name: Specify one or more user names to select rules and conflicts that affect those users. Or select All to select rules that affect all users.
- Owner: Specify one or more owners to select rules and conflicts subject to those owners. Or select All to select rules subject to all owners.
- Set of Books: Select one or more sets of books to view only conflicts for which the base entity (the function or responsibility named first in the conflict) is contained in those sets of books. Or select All to view conflicts for which the base entity may exist in any set of books.
- Operating Unit: Select one or more operating units to view only conflicts for which the base entity is contained in those operating units. Or select All to view conflicts for which the base entity may exist in any operating unit.
- Conflict Set of Books: Select one or more sets of books to view only conflicts for which the conflicting entity (the function or responsibility named second in the conflict) is contained in those sets of books. Or select All to view conflicts for which the conflicting entity may exist in any set of books.
- Conflict Operating Unit: Select one or more sets of books to view only conflicts for which the conflicting entity (the function or responsibility named second in

the conflict) is contained in those sets of books. Or select All to view conflicts for which the conflicting entity may exist in any set of books.

- Entity Type: Specify Function or Responsibility to select rules and conflicts based on one entity or the other, or Both for both types of conflict.
- Control Type: Specify Approval Required, Approve with Rules, Allow with Rules, or Prevent select rules and conflicts based on the control type you select, or All to select all control types.
- Conflict Status: Specify a status — Approved, Rejected, Pending, Allow with Rules, or Prevent — to select conflicts at that status, or select All to view conflicts at all three statuses.
- Same OU: Select Yes to list rules and conflicts that apply within operating units or No to list those that apply across operating units. Or select Both to list both types of rule.
- Same SOB: Select Yes to list rules and conflicts that apply within sets of books or No to list those that apply across sets of books. Or select Both to list both types of rule. This parameter applies only if you are reporting on a data source that runs Oracle Applications Release 11.5.3–11.5.10.
- Same Access Sets: Select Yes to list rules that generate conflicts if the conflicting entities would enable a user to access data in ledgers belonging to individual data access sets, or No to list rules that generate conflicts across data access sets. Or select Both to list both types of rule. This parameter applies only if you are reporting on a data source that runs Oracle Applications Release 12.

## User Conflicts Trend Analysis Report

The User Conflicts Trend Analysis Report depicts graphically the number of outstanding user conflicts over time. The word *outstanding* indicates those that have not yet been resolved, with new conflicts added in and those that have been resolved subtracted out. The time intervals are snapshot dates — the occasions at which user conflicts are generated. The report presents two graphs, one showing the results in total and the other by application, as well as a table that shows the number of conflicts in each snapshot, again by application and in total. As you run the report, you can select the following parameters:

- Application: Select one or more applications to view results for those applications, or select All to view results for all applications.
- Snapshot Run Date: Select snapshot dates to define the range of time the report should cover. Select not only the first and last dates in the range, but also all those in between. (Note that it is possible to select only a single date, but you should not do so, as this defeats the purpose of the report.)

# Oracle EBS Security Folder

The Oracle EBS Security Folder contains the following three reports. To ensure that the Oracle EBS Security reports present current information, run the Populate User Access Data Table background program before running any of the reports.

## Oracle EBS User Details Report

The Oracle EBS User Details Report lists the following information about each user you specify:

- The responsibilities assigned to the user, and for each responsibility, its set of books and operating unit, its start and end dates, and the start and end dates for the user's access to it.
- The root menu associated with each responsibility, with both user name (the one displayed to an Oracle Applications user) and internal name for each menu.
- The menus available for selection under those roots. The report shows the user and internal names for each menu, as well as its prompt (the label that identifies it for selection on other menus). The report also indicates whether its grant-flag value is set to *Y* (for yes) or *N* (for no) and whether it is excluded.
- The functions to which these menus give the user access. For each function, the report shows its user and internal names, its prompt, its view rights (*Y*, for yes, indicates the user has view-only access, and *N*, for no, indicates the user has write access as well as view access), its grant-flag value, and whether its menu is excluded.

As you run the report, you can select values for the following parameters:

- User: Select one or more users about whom you want information. For each, type the user's Oracle username in the Enter a Value field, and then click on the > button. You can instead select *All*. Be aware, however, that the report provides copious information about each user, and so this selection may impact performance.
- Set of Books: Select one or more sets of books to have the report display responsibilities (and the menus and functions available from them) that belong to the sets of books you select. Or choose *All* to have the report display results without regard to sets of books.
- Operating Unit: Select one or more operating units to have the report display responsibilities (and the menus and functions available from them) that belong to the operating units you select. Or choose *All* to have the report display results without regard to operating units.
- Active Users: Choose whether the report should present information about active users, inactive users, or both. A user is considered to be active if his Effective To date, as configured in the Oracle Applications Users form, has not passed. He is inactive if the date has passed.

Ensure that the value you select here complements the value you select for the User parameter. For example, it would be appropriate to select *All* for the User parameter and the value *Include Only Active Users* here; the report would display information about all users whose Effective To dates had not passed. If the User parameter selection were a specific user whose Effective To date has passed, however, it would be inappropriate to select *Include Only Active Users* here; in this case the report would show no results.

- Grant: Choose *Y* (for yes) to have the report list only submenus and functions for which the Grant check box is selected in the Oracle Applications Menus form. Or select *N* (for no) to list submenus and functions for which the grant flag is cleared.
- View Only: Select *Y* to have the report list functions to which a user has read-only access (or, more technically, the query-only parameter is set to *Yes* in the Oracle Applications Form Functions form). Or Select *N* to have the report list functions that enable a user both to view and modify data (functions for which the query-only parameter is not set).
- Prompt: Choose *Not Null* to have the report list submenus and functions a given user is able to select, because higher-level menus present prompts for them. (More technically, the report would provide information about a submenu or function if, in the Oracle Applications Menus form, a row adds it to a menu accessible from one of the user's responsibilities, and the row includes a value in the Prompt field.) Choose *Null* to have the report list submenus or functions for which higher-level menus do not display prompts, and which a user therefore cannot select. (In this case, in the Menus-form row that adds a submenu or function to a menu, no value is entered in the Prompt field.) Or choose *Both* to have the report list submenus or functions regardless of whether higher-level menus present prompts for them.
- Responsibilities: Choose whether the report should present information about active responsibilities (and the menus and functions available from them), inactive responsibilities, or both. A responsibility is active if its Effective To date, configured on the Oracle applications Responsibilities form, has not yet passed.
- Active Responsibility Assignments: Choose whether the report should present, for each user, information about active responsibility assignments, inactive assignments, or both. A responsibility assignment is active if its Effective To date, configured for the user on the Oracle Applications Users form, has not yet passed.
- Show Menu/Function Exclusions: Choose the *Do not show...* value to prevent the report from displaying menus and functions that are excluded from responsibilities. Choose the *Only show...* value to have the report display only those excluded menus and functions. Or choose the *Show all* to have the report show both included and excluded menus and functions.

## Oracle EBS Function Details Report

The Oracle EBS Function Details Report lists the following information about each function you specify:

- The responsibilities from which the function is accessible, and for each responsibility, its set of books and operating unit, and its start and end dates.
- The users whose responsibility assignments give them access to the function. The report also shows each user's start and end dates.
- The root menu associated with each responsibility. The report shows both user name (the one displayed to an Oracle Applications user) and internal name for each menu.
- The menus available for selection under those roots. The report shows the user and internal names for each menu, as well as its prompt (the label that identifies it for selection on other menus). The report also indicates whether its grant-flag value is set to *Y* (for yes) or *N* (for no), and whether it is excluded.

As you run the report, use two parameters to select functions about which the report displays information:

- Application Name: Choose one or more applications, or the value *No Associated Applications*. When you do, a list of functions associated either with applications you've chosen, or with no application, appears in an Available Values field for the User Form Function parameter.
- User Form Function: Select one or more functions about which you want the report to present information.

The remaining parameters — Set of Books, Operating Unit, Active Users, Grant, View Only, Prompt, Responsibilities, Active Responsibility Assignments, and Show Menu/Function Exclusions — take the same values (and filter report results in the same way) as they do for the Oracle EBS User Details Report.

## Oracle EBS Responsibility Details Report

The Oracle EBS Responsibility Details Report lists the following information about each responsibility you specify:

- The root menu associated with the responsibility, with both user name (the one displayed to an Oracle Applications user) and internal name for the menu.
- The users who are assigned the responsibility. The report also shows each user's start and end dates.
- The menus available for selection under the root. The report shows the user and internal names for each menu, as well as its prompt (the label that identifies it for selection on other menus). The report also indicates whether its grant-flag value is set to *Y* (for yes) or *N* (for no) and whether it is excluded.
- The functions to which these menus give users access. For each function, the report shows its user and internal names, its prompt, its view rights (*Y*, for yes,

indicates the user has view-only access, and *N*, for no, indicates the user has write access as well as view access), its grant-flag value, and whether its menu is excluded.

As you run the report, use the Responsibility Name parameter to choose one or more responsibilities about which the report displays information; or select the value *All*.

The remaining parameters — Set of Books, Operating Unit, Active Users, Grant, View Only, Prompt, Responsibilities, Active Responsibility Assignments, and Show Menu/Function Exclusions — take the same values (and filter report results in the same way) as they do for the Oracle EBS User Details Report.

# Access Monitoring Folder

The Access Monitoring folder contains the following reports. Note that two of these reports — Access Monitor Request and Access Requests Awaiting Approval — exist on your system only if you have installed ACTIVE Governance version 7.2.2.

## Access Monitor Request Report

The Access Monitor Request Report lists requests for database or responsibility access generated through use of the Access Monitoring feature. For each user for whom access is requested, it may present two sections, one for each type of request (responsibility or database). Each section then lists an entry for each item that is requested — for example, a single request for two database tables would generate two entries, one for each table. Each entry displays the name of the requested responsibility or database table; the Access Monitoring ID assigned to the user; the request ID; the status, approver, and support ticket of the request; and dates when the request is made, when access would start, and when access would end.

- System: Select one or more Oracle Applications instances to have the report list requests made on those instances.
- Access Type: Select E-Biz User to have the report list requests for access to responsibilities, Database User to have the report list requests for access to database tables, or both.
- Access Requested: Select any number of responsibilities or database tables to have the report list requests for access to those items. This parameter lists only items for which access requests have been made, and depending on you selection in the Access Type parameter, may list only responsibilities, only database tables, or both.
- User: Select one or more users to have the report list requests to grant those users access. This parameter lists Access Monitoring user IDs.
- Approver: Select any number of users to see requests for which those users are designated to be approvers by ACTIVE Governance workflows.
- Status: Select statuses — Approved, Rejected, Failed, or Pending — to see requests at those statuses, or select All to see requests at all statuses.

- Request Date: Define a period the report should cover. You may enter dates in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the Start date and select the No Lower Value check box to start with the earliest existing request, or omit the End date and select the No Upper Value check box to finish with the latest existing request.

  If you do enter actual dates, select an Include This Value check box (for either or both dates) to include the value you specify in the period, or clear the check box to exclude the value (thus selecting requests generated after but not on the Start date, or before but not on the End date). You can type dates manually (use the format *YYYY-MM-DD*) or click on the calendar icons to select dates.

## Access Monitoring User Activity Report

The Access Monitoring User Activity Report lists transactions completed by users as they implement rights granted to them through the Access Monitoring feature. In this context, a "transaction" is a change to a value in a database table, made via direct access to that table or to a responsibility supported by the table. For each user, the report presents the user's name, her temporary Access Monitoring logon ID, the database instance in which she is working, the start and end dates of her temporary access, the responsibility or database tables to which she has been granted access, and her transactions. For each transaction, the report presents its date and time, the action taken (select, insert, delete, or update), the name of the table and its primary key column, the column in which the change has been made, and the old and new values. As you generate the report, select values for the following parameters:

- User Type: Select the value *Database User* to view results for users granted direct access to database tables, *Ebiz User* to view results for users granted access to Oracle responsibilities, or both.
- User Name: Select the users whose transactions you want to review.
- Action Type: Select any combination of three transaction types to review: INSERT, UPDATE, or DELETE.
- Transaction Date Range: Define a period in which transactions must have occurred to be included in the report. You may enter dates and times in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the start date and select the No Lower Value check box to start with the earliest existing transaction, or omit the end date and select the No Upper Value check box to finish with the latest existing transaction.

  If you do enter actual dates and times, select an Include This Value check box (for either or both dates) to include the value you specify in the period, or clear the check box to exclude the value (thus selecting transactions that begin after but not at the start time on the start date, or end before but not at the end time on the end date).

  You can click on the calendar icons to select dates. If you do, each date you select is automatically is accompanied by the time 00:00:00. You can then edit

this time. Or, for an end value, you may target all of a day's transactions by selecting the next day's date and retaining the 00:00:00 time value.

## Access Requests Awaiting Approval Report

The Access Requests Awaiting Approval Report lists pending conflicts generated after "preventive" SOD analysis, if disabled, has been re-enabled. Preventive SOD analysis is the automatic distribution of approval messages within Oracle when SOD rules are triggered by the creation of new users or the assignment of new responsibilities to existing users. It's implemented by a rule in the Form Rules application, but that form rule can be disabled. This report lists conflicts generated after preventive analysis is re-enabled, for which the SOD rule owners (or approval groups) have received approval messages in Oracle, but for which no approval decision has yet been made. As you generate the report, select values for the following parameters:

- Rule Name: Select one or more rules to have the report list conflicts generated by those rules.
- User Name: Select one or more users to have the report list conflicts involving those users.
- Approver: Select one or more users to have the report list conflicts for which your selections are the SOD-rule-designated approvers.
- Access Requests: Define a period the report should cover. You may enter dates in the Access Requested From and Access Requests To fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the From date and select the No Lower Value check box to start with the earliest existing conflict, or omit the To date and select the No Upper Value check box to finish with the latest existing conflict.

  If you do enter actual dates, select an Include This Value check box (for either or both dates) to include the value you specify in the period, or clear the check box to exclude the value (thus selecting conflicts generated after but not on the From date, or before but not on the To date). You can type dates manually (use the format *YYYY-MM-DD*) or click on the calendar icons to select dates.