ACTIVE Governance™

ACTIVE Access Governor User's Guide

Software Version 7.0

LogicalApps®

Restricted Rights Legend

LogicalApps Provides on-site support as well as remote phone and web support to ensure quick and effective product implementation. To request support, to suggest product enhancements, or to comment on LogicalApps software or documentation, send email to support@logicalapps.com, or contact us at the address or phone number given below.

Document Version AG003-700A

4/10/06

LogicalApps
15420 Laguna Canyon, Suite 150
Irvine, CA 92618
949.453.9101

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 three modules that provide the capability to automate the enforcement of controls. One of these modules is ACTIVE Access Governor, which detects segregation-of-duties conflicts within an organization, either preventing them from occurring or uncovering 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.

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 LogicalApps and adapt them as needed.

Each rule applies one of three "control types" — Prevent, Allow 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, provided that other rules, written in LogicalApps AppsForm, mitigate the conflict by modifying Oracle Applications forms.
- An Approval Required rule designates a reviewer 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.

Once segregation-of-duties rules are defined, an ACTIVE Access Governor user "generates conflicts" — evaluates Oracle Applications users to note those who are in violation of rules. ACTIVE Access Governor then lists the conflicts generated by each rule in a form 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 Conflict form 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 Approval Required rule. Only a Pending status can be updated: a reviewer may approve or reject the conflict, either by itself (in an Action History form) or along with others (in a Mass Update form).

  Statuses recorded in these forms, 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 at least one AppsForm rule has been associated with the segregation-of-duties rule (but applies end dates if not).

  If the control type is Approval Required, the responsibility assignment does not take effect immediately, and ACTIVE Access Governor posts a notification of

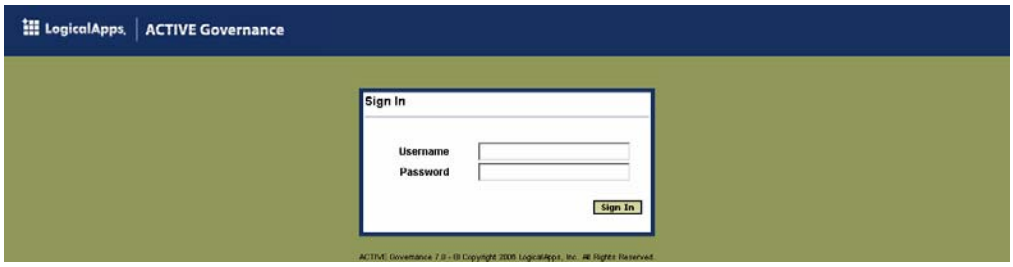
the conflict to the designated reviewer's Oracle Applications home site. Similarly, when a new user is created, his assignments are analyzed for conflicts, and notifications are transmitted to designated reviewers.

The reviewer's 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 form.

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 the Segregation of Duties tab.
5. 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. A panel, labeled SOD Rules, opens. The name of the database instance you selected in step 5 is displayed near the upper right corner. 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 role when his user account is created in the ACTIVE Governance Platform. Your rights to features available from the Segregation of Duties tab depend on the role you have been assigned:

- If your user role is SOD Super User, you have full rights. You can view, create, and edit SOD rules; view conflicts generated by rules and assign status to them; view, create, and edit entity groups; create, edit, and view rules that simulate changes intended to resolve conflicts; run simulation and view results; and run remediation (put simulated conflict resolutions to actual use).
- If your user role is Author, Manager, or Rule Builder, you have create rights. These are the same as full rights, except that you cannot run remediation.
- If your user role is Auditor, Executive, System Administrator, or User, you have view rights. You can open a list of SOD rules, although you do not have access to configuration details for individual rules. You can view conflicts generated by individual rules (and their status), but not update status. You can view a list of entity groups and configuration details for individual groups, but you cannot create or edit groups. You can view simulation rules and results, but you cannot create or update the rules, or run simulation or remediation.

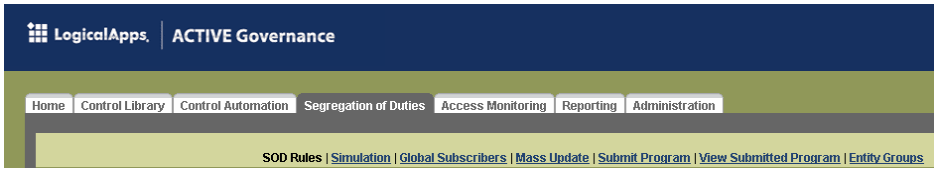
Navigational Conventions

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 (see page 7).

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 screens that support those tasks. The illustration shows a full set of Library Navigator links; however, you would see only those links that are appropriate to your user role.



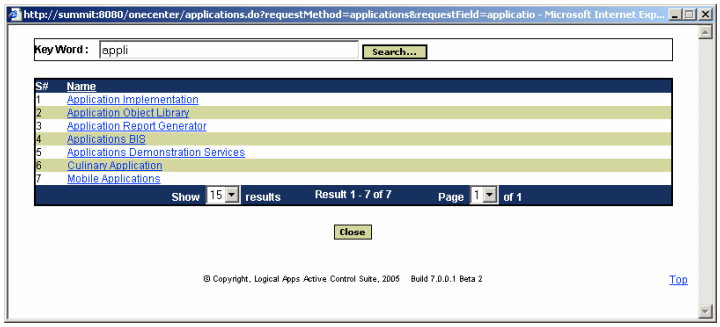
Breadcrumbs

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 trail of breadcrumbs begins with the word *Home*.) To return to any of the earlier screens, 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 filtered list of values that may be entered in the field:



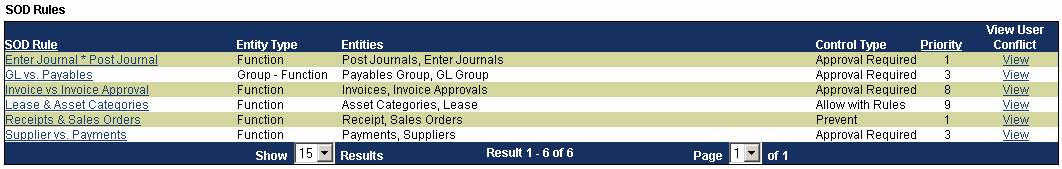
1. In the Key Word field, type a string of text that matches text a value you want to select. Or, leave the Key Word field blank.
2. Click on the Search button. ACTIVE Access Governor returns values, the selection of which depends on your entry in the Key Word field:
   - If your Key Word entry includes 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 *Application 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 Rules

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

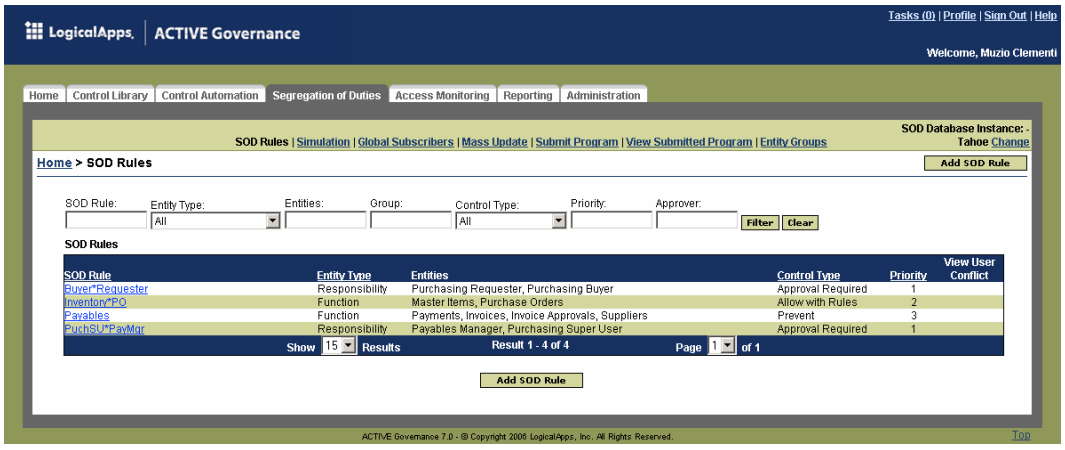
Each of these lists implements the following conventions:

- 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.

Chapter 2

Defining Segregation-of-Duties Rules

When you click on the Segregation of Duties tab, ACTIVE Access Governor opens a panel that lists summary descriptions of existing segregation-of-duties rules — for each, its 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

In the SOD Rules panel, you can limit the display 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 elements:
   - 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 a function or responsibility to find rules in which that entity is set in conflict with another. Type a text fragment to display rules involving entities whose names contain the fragment. Or, leave the field blank to search for rules involving any functions or responsibilities.
   - Group: Use this field only if you selected Group–Function or Group–Responsibility in the Entity Type field. Type the name of a group to find rules in which that group is named as a base or conflicting entity. Type a text fragment to display rules involving groups whose names contain the fragment. Or, leave the field blank to search for rules involving any functions or responsibilities.
   - Control Type: Select one of the control types (Prevent, Allow with Rules, or Approval Required) to search for rules of that type. Or select All to search for rules of all types.
   - Priority: Type a priority number to search for rules at that priority, or leave the field blank to search for rules at any priority.
   - Approver: Type the full name of a workflow role to find rules for which that role is the designated conflict approver. Type a text fragment to find rules for which the names of the designated conflict approvers contain that fragment. Or leave the box blank to see rules for which anyone is a designated approver.
2. When you finish specifying filtering criteria, click on the Filter button.

To discard filtering criteria and redisplay all SOD rules, click on the Clear button.

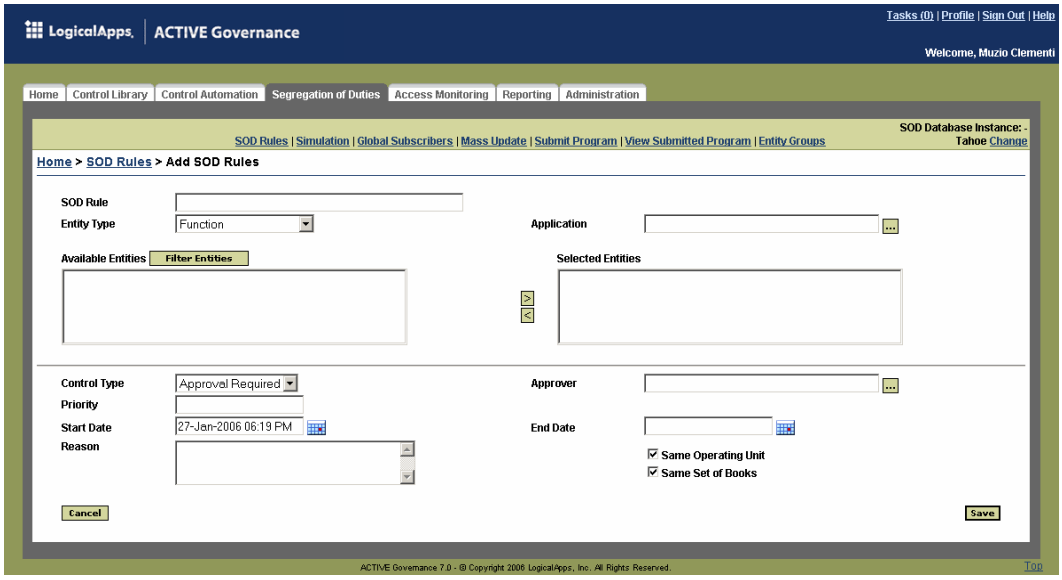
Creating SOD Rules Manually

To create a segregation-of-duties rule, click on the Add Rule button in the SOD Rules panel. An Add SOD Rules panel opens (as shown at the top of the next page).

Starting the Rule

Begin to create the 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 Choose the first of the items you want to include in a conflict definition.

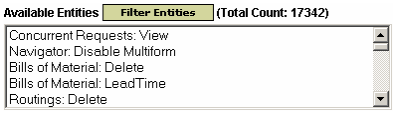
- If you chose Responsibility in the Entity Type list box, select an application in the Application list of values. The Available Entities field then displays the responsibilities that belong to the application you chose. Click on the one you want, and then on the > button to move it to the Selected Entities field.
- If you chose Function in the Entity Type list box, use the Application field to select either an application or the value *No Associated Application*. The Available Entities field displays functions belonging either to the application you chose or to no application. Click on the function you want, and then on the > button to move it to the Selected Entities field.
- If you chose Group–Responsibility or Group–Function in the Entity Type list box, the Available Entities field displays a list of entity groups configured for your system (see page 12). Click on the one you want, and then on the > button to move it to the Selected Entities field. In this case, the Application list of values does not accept input.

If you wish to rescind a selection, click on an entry in the Selected Entities field, and then click on the < button to return it to the Available Entities field.

4 Choose any number of conflicting items; for each, use the process described in step 3.

- The conflicting items you select must be of the same type as the original item.
- If you are selecting an individual responsibility or function, you need to select its application only if the new item belongs to a different application than the preceding one; otherwise the appropriate application is already selected.

When you select an entity type, and so load items into the Available Entities field, ACTIVE Access Governor presents a count of the items. It appears above the Available Entities field, next to a Filter Entries button.



If the count exceeds 1,000, you should filter the items in the Available Entities field; otherwise, performance may suffer. To filter the items:

1. Click on the Filter Entities button. An Explorer User Prompt dialog appears.
2. In the text box on the dialog, type the first few letters of the name of the item you want to select. (For example, type *Pur* for the Purchases function.) Click on the OK button.
3. The dialog closes, and the Available Entities field displays only those items whose names begin with the letters you typed.

Finishing the Rule

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

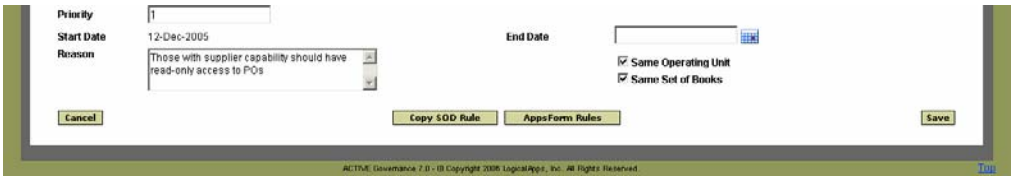
1. In the Control Type list box, select the control type you want to apply to the rule — Prevent, Allow with Rules, or Approval Required. (See page 2 for definitions of these control types.)
2. In the Priority field, type a number from 1 to 10. This sets the priority by which conflicts generated by the SOD rule are listed in reports, with respect to conflicts generated by other rules. (The value *1* sets the highest priority.)
3. In the Approver list of values, select the workflow role that is to set the status of individual conflicts generated by the SOD rule. Although status can be set only for conflicts generated by Approval Required rules, you must select an approver for every rule, regardless of control type.

   For the Approver LOV to offer an up-to-date selection of workflow roles, run a background program, called LAA Populate WF Roles Table, each time new roles are added in Oracle Applications. See "Running Background Programs" (page 41).
4. The Start Date field is set to the date and time at which you create the rule, and the end date field is blank. Retain these values to have the rule take effect immediately and remain in effect indefinitely. Or select a new start or end value: Edit the date and time manually in either field (use the format *DD-Mon-YYYY Hr:Mn:Sc*). Or click on the icon next to a field and select a date in the pop-up calendar that appears.
5. In the Reason box, type an explanation of the business risk addressed by this rule.
6. Select the Same Operating Unit check box to have the rule apply only within individual operating units. Select the Same Set of Books check box to have the rule apply only within individual sets of books. Clear the appropriate check box to have the rule apply across operating units or sets of books.
7. Save the rule: Click on the Save button at the bottom right. The SOD Rules panel reappears, with a listing for the new rule.

Linking the SOD Rule to AppsForm Rules

If you assigned the Prevent or Approval Required control type to a segregation-of-duties rule, you have finished creating it (and so can skip this section). If you selected the Allow with Rules control type, you must link this SOD rule with one or more AppsForm rules:

1. In the SOD Rules panel, click on the name of the rule. An Edit SOD Rules panel opens, displaying the values you configured for the rule. The panel also displays an AppsForm Rule button near the bottom center:



2. Click on the AppsForm Rule button. An AppsForm Rules panel appears:

3. Click on the Add Row link and complete fields in the row you create:
   - In the AppsForm Rule list box, select a rule that addresses the conflict. Obviously, an appropriate AppsForm rule would have to have been created prior to the configuration of this SOD rule.
   - In the Comments box, type a comment explaining why the AppsForm rule is being attached to the SOD rule.
   - The Creation Date field displays by default the date on which you establish a link between the AppsForm rule and SOD rule. You cannot change it.
4. Optionally, repeat step 3 any number of times to associate any number of additional AppsForm rules with the SOD rule.
5. Click on the Save button. Click on the SOD Rules link in the "breadcrumbs" trail to return to the SOD Rules panel.

Viewing, Editing, and Copying SOD Rules

You can review the configuration details for any existing rule, edit some of those details, or copy the rule as a starting point for creating a new rule. Simply click on the name of the rule in the SOD Rules panel to open the Edit SOD Rules panel.

You can edit only the following elements of a rule: the priority, reason, approver, end date (if it has not already passed), and the settings of the Same Operating Unit and Same Set of Books check boxes. If the control type is Allow with Rules, you can add AppsForm rules to the SOD rule; you cannot delete those already assigned (although you can inactivate them in AppsForm).

If you click on a Copy SOD Rule button (at the bottom center of the Edit panel), a Copy SOD Rules panel opens. It's functionally identical to the Add SOD Rules panel, except that it takes the following values from the rule you copied: entity type, selected entities, control type, priority, approver, start and end dates, and the same operating unit/set of books settings.

To create a new rule, supply a new name in the SOD Rule field and edit the remaining fields as you wish. Use the procedure described in "Creating SOD Rule Manually" (page 8). You can add to or remove the responsibilities, functions, or groups you inherited from the rule you copied, but you cannot change the entity type.

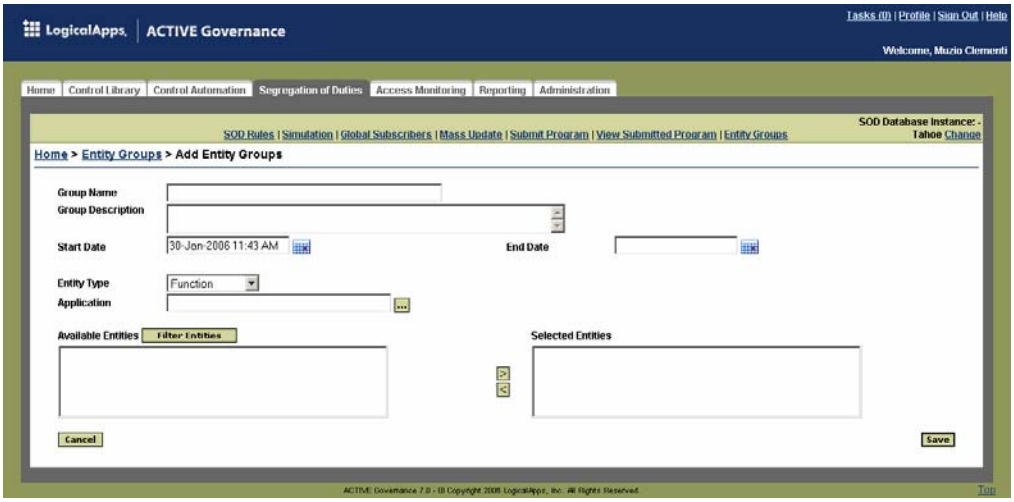
Working with Entity Groups

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 text 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.
2. Click on the Add Entity Groups button near the bottom center of this panel. An Add Entity Groups panel appears (as shown at the top of the next page).
3. Type a unique name for the group in the Group Name field.
4. In the Group Description field, type a brief explanation of the group. (For example, explain the organizing principle by which functions or responsibilities are included in the group.)
5. The Start Date field is set to the date and time at which you create the group, and the end date field is blank. Retain these values to have the group take effect immediately and remain in effect indefinitely. Or select a new start or end value: In either field, you can edit date and time manually. Or, to set a date, 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 the items you want to include in the group. It may contain functions or responsibilities, but not a mixture of the two.

- If you chose Responsibility in the Entity Type list box, select an application in the Application list of values. The Available Entities field then displays the responsibilities that belong to the application you chose. Click on the one you want, and then on the > button to move it to the Selected Entities field. A group can contain responsibilities belonging to any number of applications. To gain access to a responsibility not currently displayed in the Available Entities field, select its application in the Application list box.
- If you chose Function in the Entity Type list box, use the Application field to select either an application or the value *No Associated Application*. The Available Entities field displays functions belonging either to the application you chose or to no application. Click on the function you want, and then on the > button to move it to the Selected Entities field. A group can contain functions belonging to any number of applications, or some that belong to applications and others that don't. To gain access to a function not currently displayed in the Available Entities field, select its application or the *No Associated Application* value in the Application list box.

If you wish to rescind a selection, click on an entry in the Selected Entities field, and then click on the < button to return it to the Available Entities field. Moreover, the Available Entities field works here as it does in the Add SOD Rules panel — it displays a count of the items it contains. When the count exceeds 1,000, you should filter the items (see page 10).

8 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

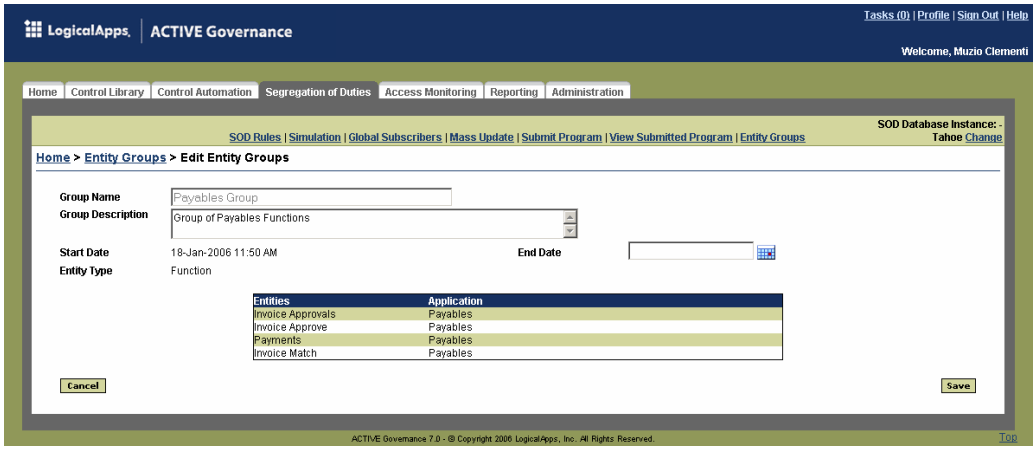
After you save a group you have created, the Entity Groups panel reappears, adding a listing for the new group to its display. The listing for each group displays its name,

the entity type of its members, its description, and its start and end dates. Listings are alphabetized by group name.

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

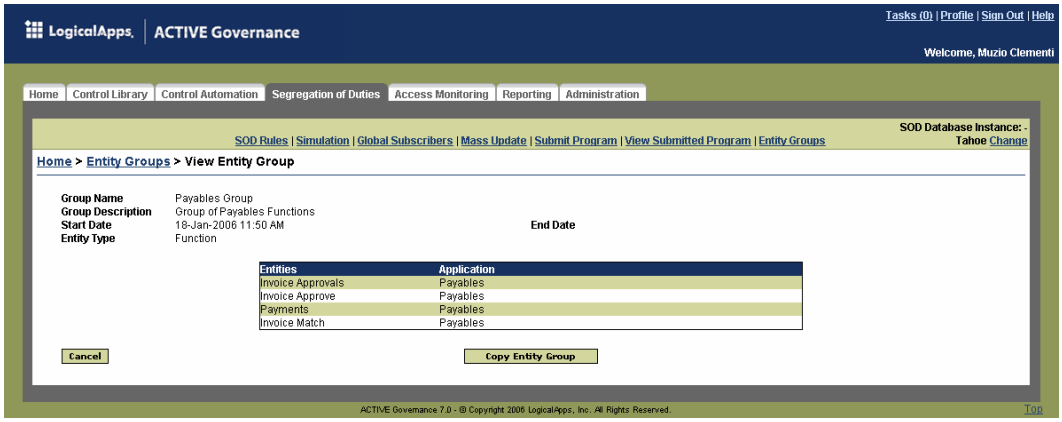
To edit a group, click on its name in the Entity Groups panel. An edit panel opens:



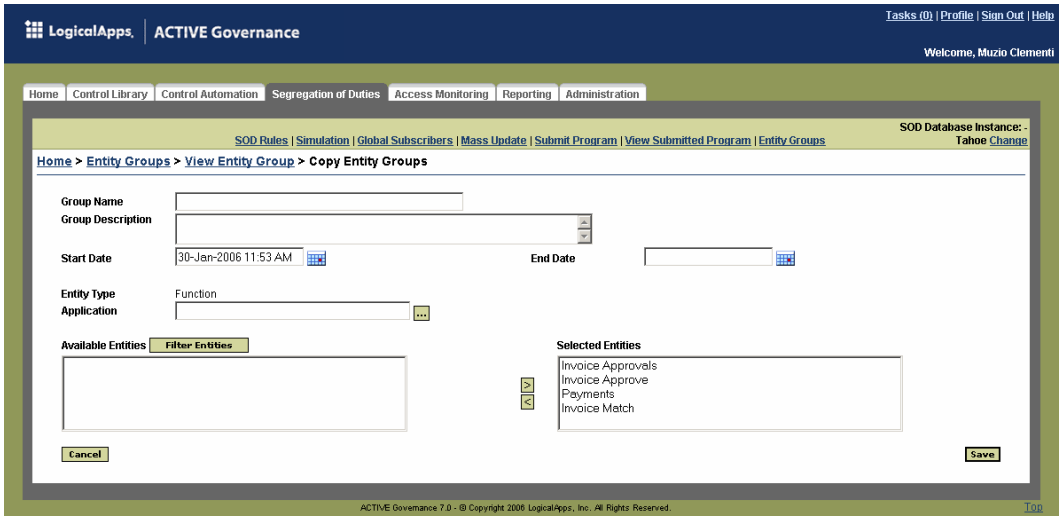
Although you can view all the elements that make up the group, you can edit only the group name, description, and end date. (For each, click in the appropriate field and enter a new value). The group name can be edited only if the group has not yet been used in a rule; once the group has been, the group 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 its View link in the SOD Groups panel. A view panel opens; it's very 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 Groups panel opens; it's functionally identical to the Add Entity Groups panel. However, its Selected Entities field contains the responsibilities or functions selected for 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" on page 12. You can remove responsibilities or functions you inherited from the group you copied, or you can add to them. However, you cannot change the entity type

Creating Global Subscribers

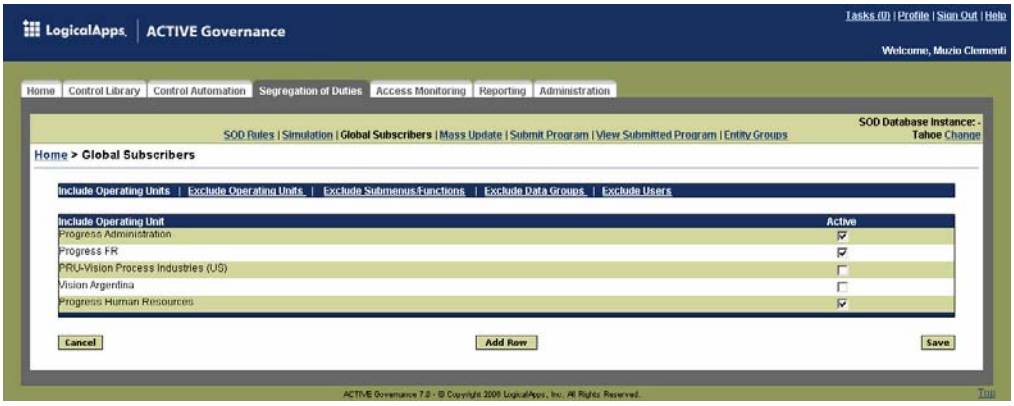
You can specify submenus, functions, data groups, operating units, and users who are exempt from SOD rules. Such exclusions can ensure that query-only access to Oracle Applications features does not trigger rules, even when standard access to the same features would. Or they may avoid the generation of conflicts that need not be tracked.

Items designated for exclusion (or, in one case, inclusion) are called global subscribers. To select them, 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 link. 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.

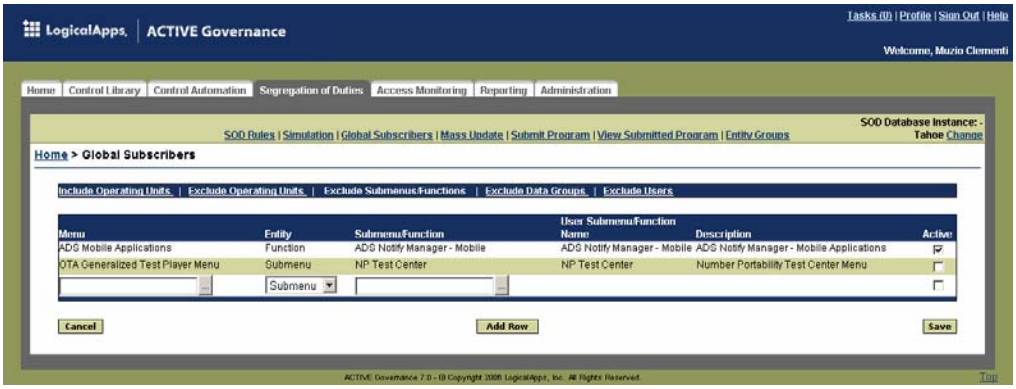
5 Click on the Save button.

Submenus

A submenu under one menu may provide query-only access to functions, even though 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 if 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 link:



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 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.
- To exclude a function, select Function in the Entity list box. Select the function and its parent submenu in the Submenu/Function and Menu fields.

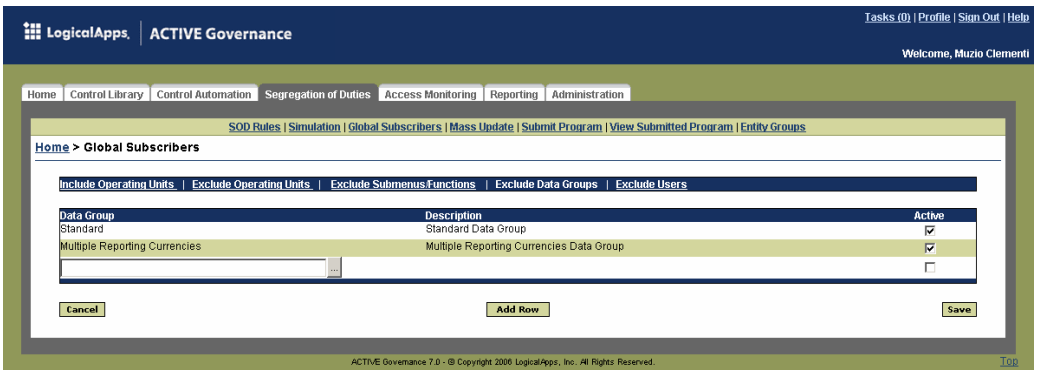
3 Select the Active check box to exempt the query-only instance of the function or functions from SOD rules, while leaving write-enabled instances subject to rules. Or, clear the check box to deactivate the exemption.

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 link:



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.

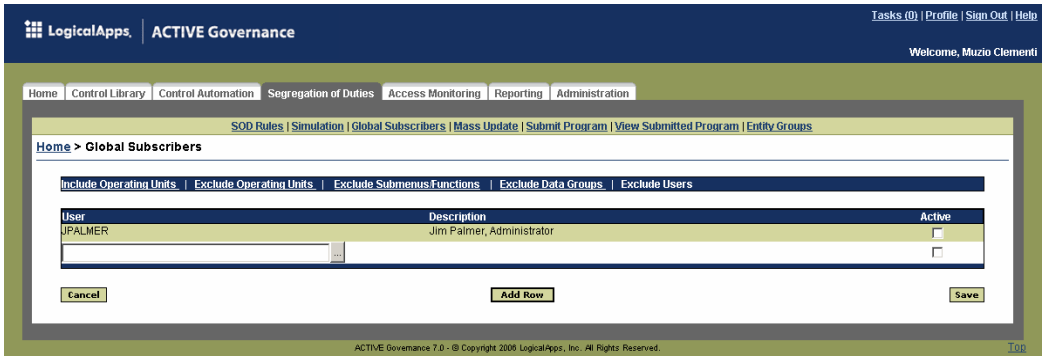
3 The Active check box is selected by default. Leave it selected for the exclusion to take effect. Clear it (click on it so that no check mark appears) to reserve an exclusion for the group, but not have it take effect at present.

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 link:



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.

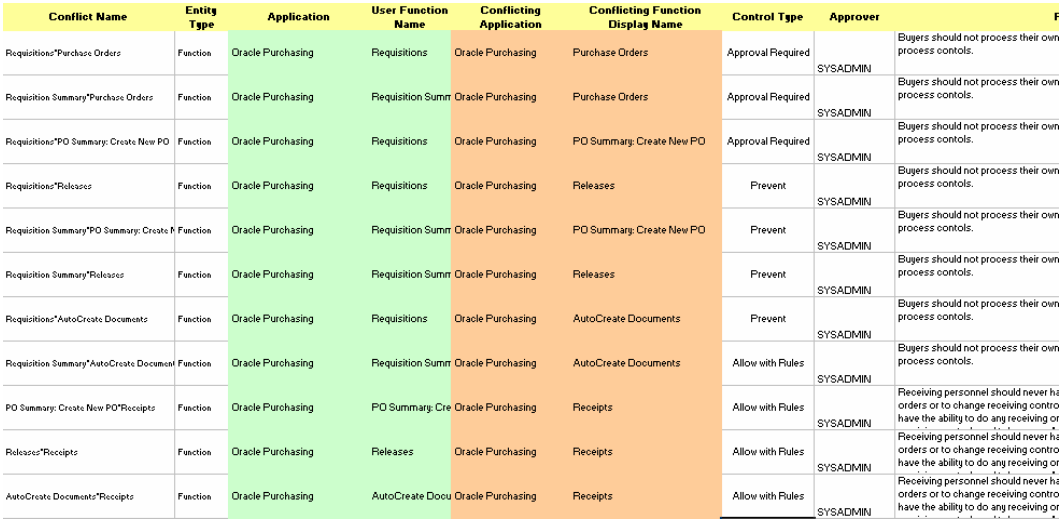
Uploading SOD Rules from a Spreadsheet

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 then upload them all 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 possible.)

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 AppsAccess. 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 AppsAccess 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 "Running Background Programs" on page 41.

Chapter 3

Generating and Reviewing Conflicts

Once SOD rules are defined and saved, the next step is to generate conflicts — to have ACTIVE Access Governor search users' work assignments for violations of the rules. In a User Conflicts form, you can then view a list of conflicts generated by each rule, 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 Approval Required conflicts, status begins at Pending; the approver designated in the rule can update the status to Approved or Rejected, either one conflict 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 of the Action History or Mass Update forms does nothing more than add 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 created 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 is created 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

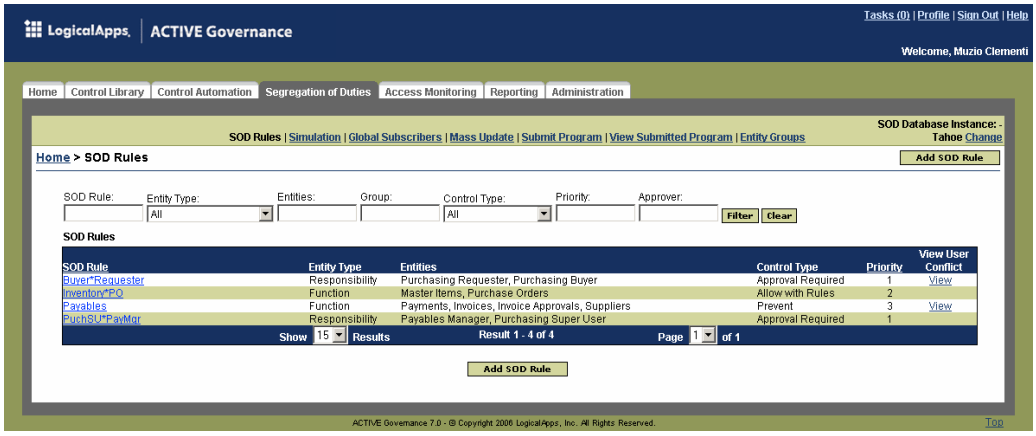
When you generate user conflicts, ACTIVE Access Governor evaluates all SOD rules that have been saved and produces a "snapshot" — a set of conflicts existing at the current moment, as distinct from other sets of conflicts generated at past moments. With each new snapshot, ACTIVE Access Governor saves the previous snapshot to an archive table.

Thus rules may be added or edited, but the existing snapshot reflects the way rules were configured the last time conflicts were generated, and will continue to do so until the Generate User Conflicts process is run again. So you should generate user conflicts whenever SOD rules change.

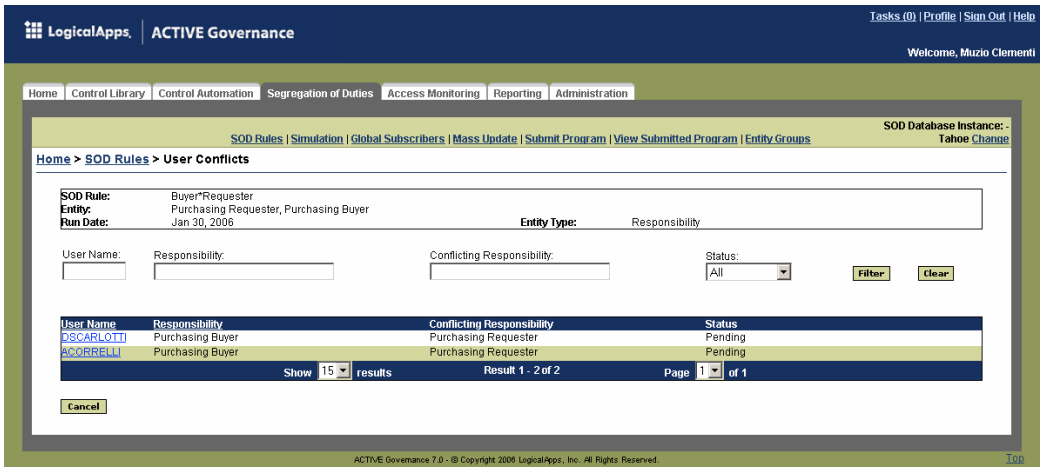
To generate user conflicts, run the Generate User Conflicts background program. For the procedure, see "Running Background Programs" on page 41.

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:



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. 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 the full name of a responsibility 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 a rule whose control type is Approval Required. It has no effect with 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 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.

If you click on the Clear button, the list of conflicts disappears, along with any criteria specified in the filtering fields, and you can select new filtering values.

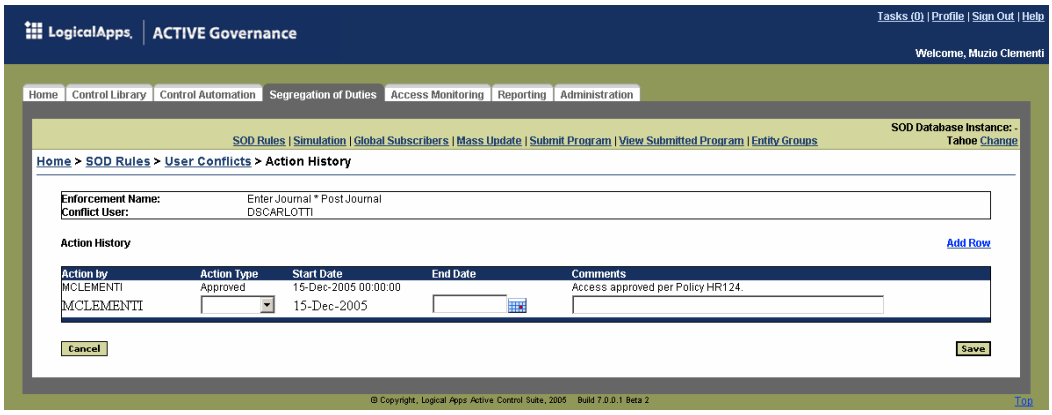
Updating Status for User Conflicts

If a conflict is generated by an Approval Required SOD rule, its status is Pending, Approved, or Rejected; any of these statuses can be updated from one to another. For each of these conflicts, the User Name in its entry on the User Conflicts panel is a link to an Action History panel. An approver (as designated in the rule that generated the conflict) can use the Action History panel to update the status of the conflict. Other users can open this panel to view, but not update, status details.

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 for an Approval Required 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) specifies the status that is in force.

3 If you are not a designated 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.

If you are a designated approver for the rule, you can also update status for the conflict. To do so, click on the Add Row link. (This link appears only if you are a designated approver for the conflict).

4 In the Action Type list of the row you created, select Approved, Rejected, or Pending. Approving a user conflict means that you know it exists and decide to allow it for the user. Rejecting a user conflict means that you decline to allow the user access to conflicting responsibilities or functions. Pending is the default status, indicating that a decision is yet to be made.

5 Specify dates during which this status is to remain in effect.

- Start Date defaults to the date on which you are taking action, and cannot be changed.
- End Date is blank by default. Insert a date on which you want the status to expire, or leave the box blank to allow the status to remain in effect indefinitely. To insert a date, click on the icon next to the End Date field, and then click on a date in the popup calendar that appears.

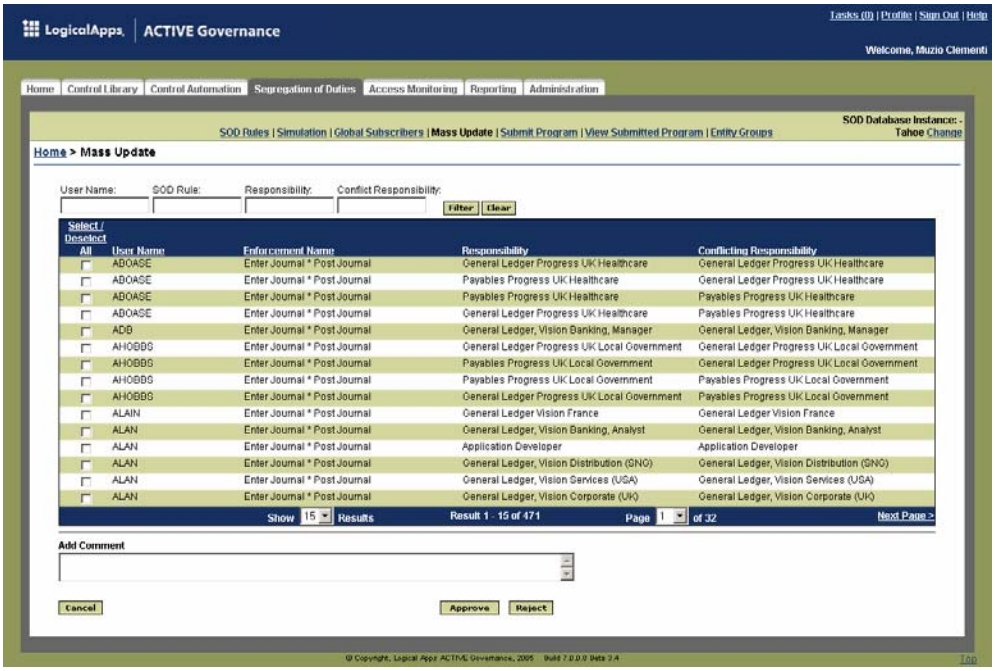
6 In the Comments field, type a brief explanation for your approval decision.

7 Click on the Save button.

Mass Updating User Conflicts

You can select sets of Approval Required conflicts and approve or reject them all at once, rather than one at a time. To do so, you would work in a Mass Update form:

1 Click on the Mass Update link in the Library Navigator. The following Mass Update form opens, initially displaying only a set of filtering fields.



2 As in the User Conflicts panel, 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), and then click on the Filter button. If you set no criteria, the panel will display 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 that apply to that user. Type a fragment to display conflicts applying to 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.
- 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 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.

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 Select the conflicts whose status you want to update. For each, select the check box in the leftmost column of the grid. Or, click on the heading for that column — Select/Deselect All — to select all the conflicts or, if all are already selected, to clear all the selections.

4 In the Add Comment field, type an explanation for your decision to update status as you have. The comment is required, and it applies to all of the conflicts whose status you are updating.

5 Click on either the Approve or Reject button. ACTIVE Access Governor assigns the status you selected and the comment you wrote to each conflict you selected. It then removes the newly statused conflicts from the list, and leaves the Mass Update form in place.

6 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.

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.
- Adding a user affected by an Allow-with-Rules conflict as a subscriber to the AppsForm rule associated with the SOD rule. For instructions on adding subscribers to AppsForm rules, see the *AppsForm User's Guide*.

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

Manual Conflict Resolution

The first time conflicts are generated, and afterwards whenever SOD rules change, you are likely to find users who have 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.
- An Approval Required conflict 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, ACTIVE Access Governor provides a Where Used Report, which displays the menu paths to functions involved in function-based conflicts. (See page 38.)

Simulation and Remediation

To aid in cleanup, ACTIVE Access Governor enables you to write simulation rules. Each 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. As it evaluates these rules, ACTIVE Access Governor determines how conflict generation would differ if the simulated conditions were in force.

It does so by creating two snapshots: The first is a set of conflicts that are generated with functions, menus, and responsibilities as they are actually configured. The second is a set that would be generated under the simulated conditions. 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 the former outnumber the latter, you can have ACTIVE Access Governor perform "remediation" — modify function, menu, and responsibility configurations in Oracle Applications to implement the simulated conditions.

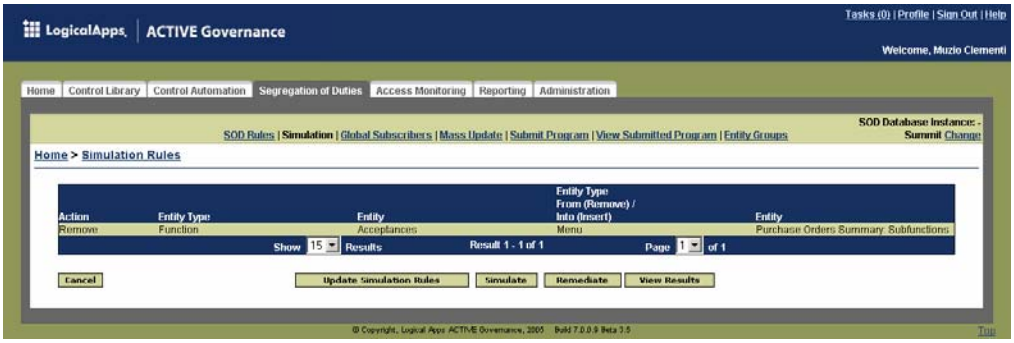
Creating Simulation Rules

To create and evaluate simulation rules:

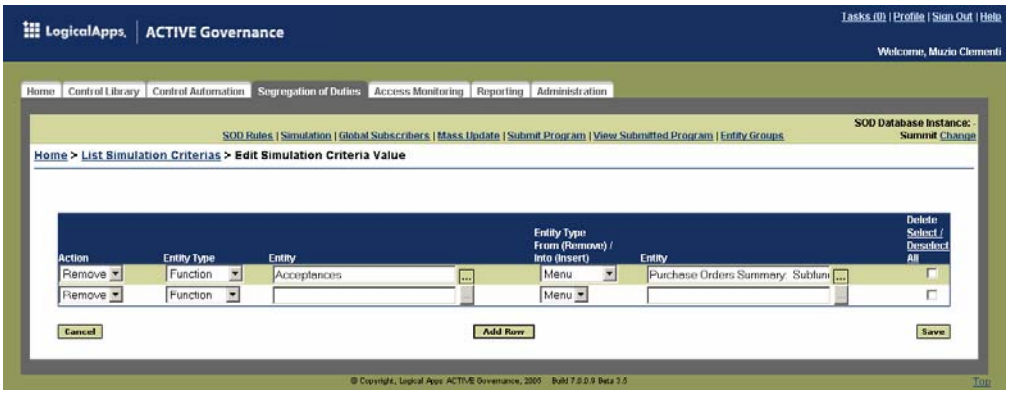
1. Identify modifications you want to simulate in the relationships among functions, menus, and responsibilities. Do so by reviewing conflicts in the User Conflicts panel and, if necessary, by using the Where Used Report to determine the relationships among functions, submenus, and menus.

   For example, a rule may set two functions — Invoice and Invoice Approvals — in conflict. The User Conflicts panel may show conflicts for several users who have access to both functions through a single responsibility — Payables Super User. Rather than end-date the responsibility for each user, you might want to determine what would happen if you were to exclude one of the functions — say, Invoice Approvals — from the Payables Super User responsibility.

2. Click on the Simulation link in the Library Navigator. A Simulation Rules panel opens, displaying an entry for each existing simulation rule:



3. Click on the Update Simulation Rules button to open an Edit Simulation Criteria Value panel. In that panel, click on the Add Row button:



4. In the row you've created, enter values for a simulation rule. (As you do, note that a given menu may be a parent to submenus and a submenu to higher-level menus. So when you choose a menu or submenu for use in a rule, 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 sim-

ulate 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 Invoice Approvals in the first Entity field. The Entity Type From/To field would default to Responsibility; select Payables Super User in the second Entity field.

5 ACTIVE Access Governor evaluates all existing simulation rules at once, so ensure that all rules serve to define the conditions you want to simulate. Create as many rules as you may need; for each, click on the Add Row button and supply values in the row you create. Delete any rules that would distort your simulation conditions; for each, select the deletion check box at the right end of its row.

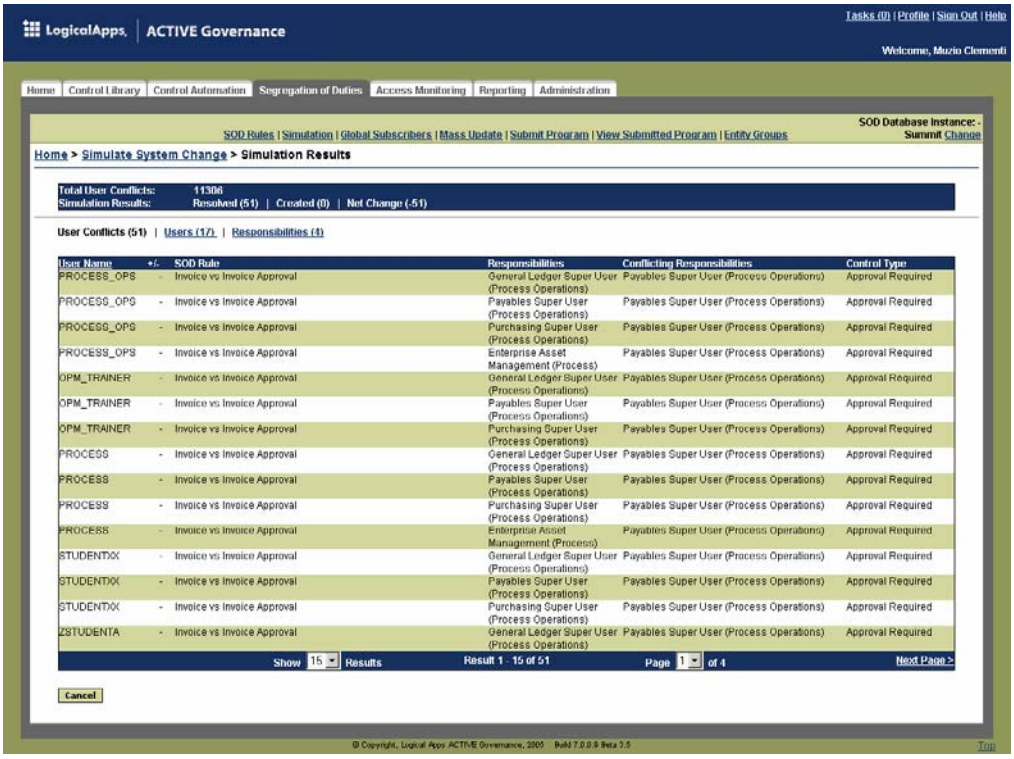
6 Click on the Save button. The Simulation Rules panel returns, displaying all rules you have not deleted.

7 Click on the Simulate button. ACTIVE Access Governor runs a background program to perform the simulation, and it presents a View Submitted Program panel to track the status of the program. Click the Refresh button on your web browser and, in the row for your request, check status in the Phase column. When the process is complete, click on the Simulation link in the Library Navigator to return to the Simulation Rules panel.

8 Click on the View Results button. A Simulation Results panel (shown at the top of the next page) provides the following:

- Summary information: The blue band near the top of the panel shows the number of existing conflicts, the numbers that would be resolved and created by the simulation, and the net change.
- Individual results: Initially, the panel lists an entry for each conflict that would be resolved or newly created. A minus sign in a column labeled +/– designates a resolved conflict, and a plus sign designates a newly generated conflict.

  Click on the Users link to show results for each user whose conflicts would change, or the Responsibilities link to show results for each responsibility for which conflicts would change. Click on the User Conflicts link to return to the display of results by conflict.



9 Click on the Cancel button, or on the Simulate System Changes link in the bread-crumbs trail, to return to the Simulation Rules panel.

Remediation

If you are satisfied with the results, you can initiate "remediation" — actually make the changes you have simulated. To do this, click on the Remediate button in the Simulation Rules panel. This launches another background program; the View Submitted Program panel displays its status. Moreover, remediation deletes the existing simulation rules, as they no longer reflect the function, submenu, and menu configuration.

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.

Automated Conflict Resolution

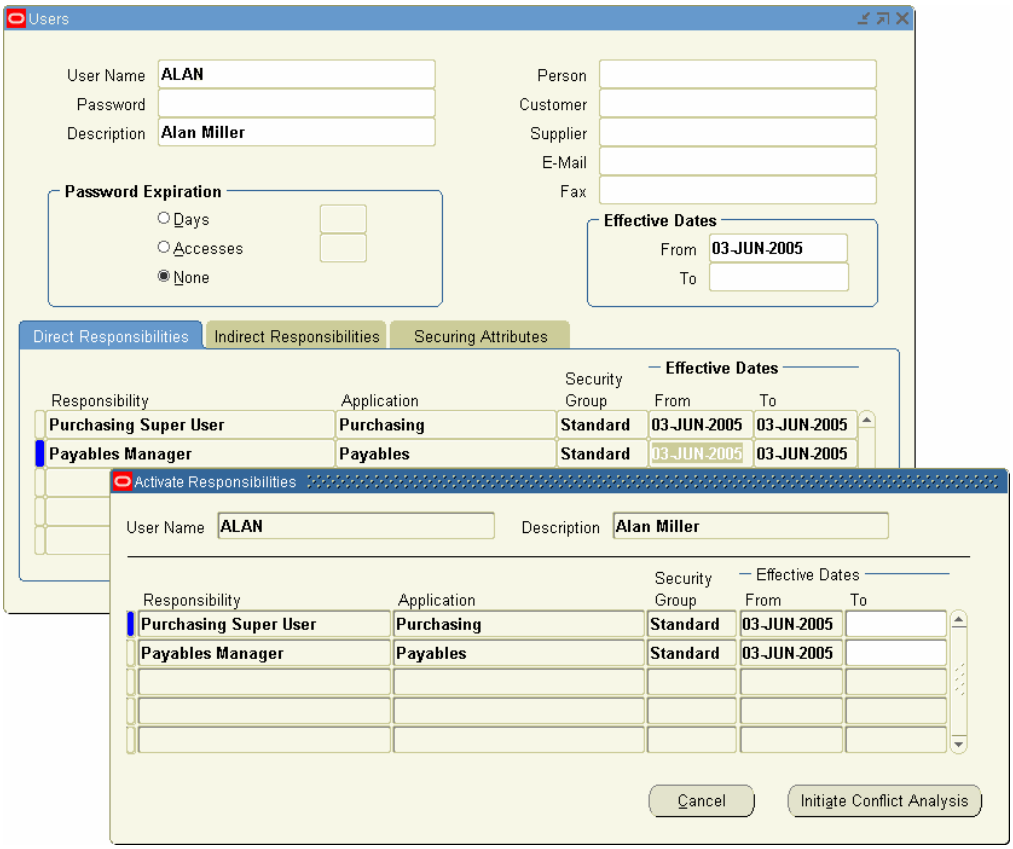
When a user is assigned new responsibilities, ACTIVE Access Governor evaluates the assignment for violations of existing SOD rules and presents an option to "submit" or cancel it. Upon submission, ACTIVE Access Governor enforces rules that have been violated: depending on control type, it automatically 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 User 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.

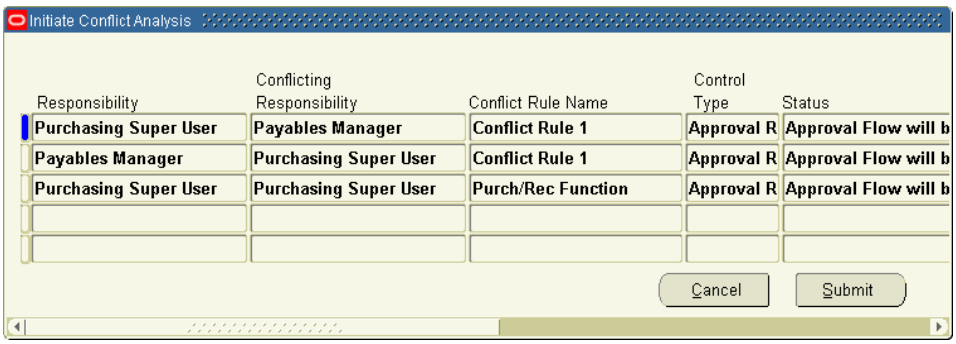


Note
If the Activate Responsibilities option is inactive, use a Mass Associate feature, available in AppsForm or AppsFlow, to associate a function called AppsAccess Activate Responsibilities with either the responsibility or the menu from which you gain access to the Users form. For information on the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

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 Rule conflict, end dates will be removed, providing the SOD rule is associated with an AppsForm rule.
- For an Approval Required 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. For responsibilities with Allow with Rules conflicts, it grants access if the SOD rule is associated with an AppsForm rule, but denies access if not. 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 Activate Responsibilities. "Denying access" means setting end dates in the Users form to the current date.

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

Responding to Notifications

For an Approval Required conflict, the approval workflow forwards a notification to the approver defined in the SOD rule. To respond to such a request:

1 Go to the Oracle E-Business Suite Home site and find the approval notification:

2 Click on the notification to open it:

3 Review information about the assignment of responsibilities that either are in conflict with one another or contain conflicting functions. Optionally, type a comment explaining the decision you are about to make.

4 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 (see step 3 on page 32). 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.

5 Click on the Return to Portal link.

The decision you make automatically updates the User Conflicts panel in ACTIVE Access Governor.

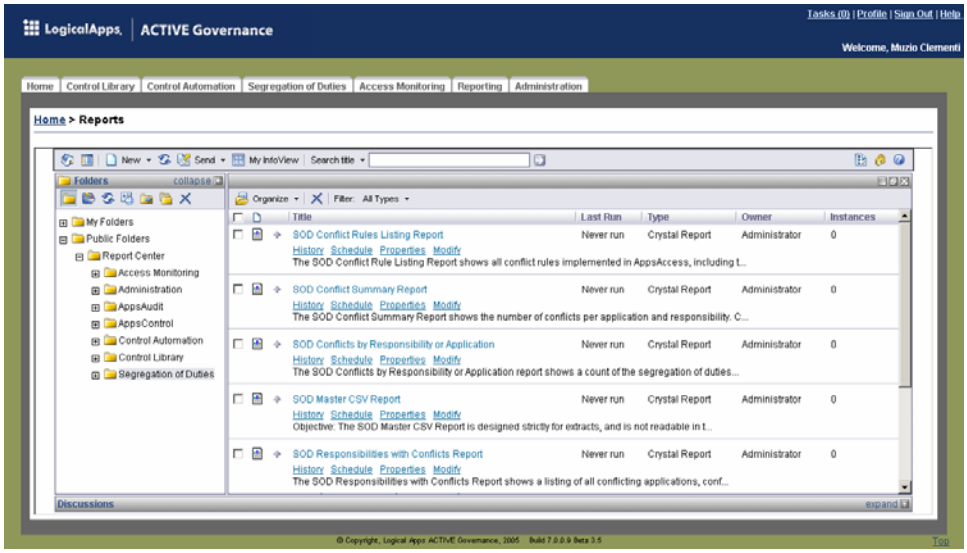
Chapter 5

Reports and Background Programs

ACTIVE Access Governor reports present SOD analysis results as well as configuration data. ACTIVE Access Governor also runs "background programs" that generate conflicts, archive data, load import files, and reset values.

Running Reports

To run reports, open ACTIVE Governance and click on the Reports tab to display the Reports panel:



A Folders area to the left of the Reports panel presents a hierarchical display of available reports and the folders that contain them. In it, click on Public Folders, then Report Center, and then either on Access Monitoring or Segregation of Duties. Then, in the larger panel on the right, click on the link for the report you want.

Note that in addition to parameters listed in the following report descriptions, reports commonly accept the following two parameters:

- Source Data: Select the instance that contains the data about which you want to generate reports.
- Include Graph: ACTIVE Access Governor reports can display data not only textually, but also graphically. Select *Y* to include graphs in a report or *N* to exclude graphs.

User Conflicts Report

The User Conflicts Report presents information on the resolution of conflicts for individual users. It collects data generated when conflicts are resolved in the User Conflict Actions form (or the Mass Update form). A system administrator would use information from the report to implement conflict-resolution decisions. As you generate the report, you can select the following parameters:

- Snapshot Run Date: Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.
- Application Name: Select one or more applications to view conflicts associated with those applications. Or select All to view conflicts associated with all applications.
- Conflict Rule 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.
- Control Type: Select a control type — Approval Required, Allowed with Rules, or Prevent — to view only information on the resolution of conflicts generated by that type of SOD rule. Or accept the default value, All, to see information on the resolution of conflicts generated by all types of rule.
- 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 all three statuses.
- User Name: Select a user Name to view only information on the resolution of conflicts concerning that user. Or select All to see information on the resolution of conflicts concerning all users.

Conflict Summary Report

The Conflict Summary Report lists responsibilities within each application, then shows the number of approved, rejected, prevent, and pending conflicts, and the total of those four counts, at each responsibility.

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, you can select these parameters:

- Snapshot Run Date: Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.
- 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.

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. As you generate the report, you can select the following parameters:

- Application Name: 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.
- Control Type: Select a control type — Approval Required, Allowed with Rules, or Prevent — to view only conflicts of that type. Or accept the default value, All, to view conflicts of all types.
- Intra Responsibility Conflict: Select *Y* (for yes) to view information on conflicts between functions within a responsibility, or *N* (for no) to view information on conflicts between entities across responsibilities. Or leave this parameter blank to view information on conflicts of both types.

- Snapshot Run Date: Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.

Responsibility Menu Report

The Responsibility Menu report gives a count of user conflicts for a given function within a responsibility. The report also shows the mappings of responsibility to menu and function, which is helpful in conflict cleanup. As you generate the report, you can select the following parameters:

- Application: Select one or more applications to view counts of conflicts associated with those applications. Or, select All to view counts of conflicts associated with all applications.
- Responsibility: Select one or more responsibilities to view only counts of conflicts for those responsibilities. Or select All to view counts for all responsibilities.
- Function: Select one or more functions to view only counts of conflicts for those functions. Or select All to view counts for all functions.
- Conflict Name: Select one or more SOD rules to view only counts of those rules. Or select All to view counts for all rules.
- Intra Responsibility Conflict: Select *Y* (for yes) to view counts of conflicts between functions within a responsibility, *N* (for no) for conflicts between entities across responsibilities, or Both for conflicts of both types.
- Report Output: Select Print or Export to determine the format of the report.

Where Used Report

The Where Used Report displays the menu paths to functions involved in function-based conflicts. The information is useful if the resolution of a conflict requires removing one of the conflicting functions from the menus available to a responsibility. As you generate the report, you can select the following parameters:

- Rule Name: Select one or more SOD rules to trace the menu paths of functions named in those rules.
- Function: Select a "base" function 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 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.
- User: Select one or more users whose conflicts you wish to resolve. The prompt displays users affected by the conflict you defined in the Function and Conflicting Function prompts.

User Conflicts Trend Analysis

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 results in total and by application. 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.)

Conflict Rule Listing Report

The Conflict Rule Listing Report lists SOD rules and, for each rule, displays the values that define it. As you run the report, you can select the following parameters:

- Conflict Rule 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.
- Application Name: Select one or more applications to view rules involving those applications, or select All to view rules involving all applications.
- Control Type: Select a control type — Approval Required, Allowed with Rules, or Prevent — to view only information on rules involving that type. Or accept All to see information on rules involving all types.
- Conflicts Exist: Select *Y* (for yes) to list rules for which conflicts exist or *N* (for no) to list rules for which conflicts do not exist. Or select Both to list both types of rule.
- End Dated Conflicts: Select *Y* (for yes) to list rules for which conflicts are end-dated or *N* (for no) to list rules for which conflicts are not end-dated. Or select Both to list both types of rule.
- Same OU: Select *Y* (for yes) to list rules that apply within operating units or *N* (for no) to list rules that apply across operating units. Or select Both to list both types of rule.
- Same SOB: Select *Y* (for yes) to list rules that apply within sets of books or *N* (for no) to list rules that apply across sets of books. Or select Both to list both types of rule.

Reviewer Performance Report

The Reviewer Performance Report shows — in total and at each status — the number of conflicts handled by individual reviewers and the average number of days per judgment. As you generate 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.
- Approved By: Select one or more reviewers to view results for those reviewers, or select All to view results for all reviewers.
- Start and End Dates: Select a range of dates the report should cover.

Master CSV Report

The Master CSV Report produces a CSV (text) file that contains data generated by ACTIVE Access Governor. The file can then be exported to a spreadsheet for further analysis. As you generate the report, you can select the following parameters:

- Application: Specify one or more applications to select SOD rules associated with them. Or select All to select rules associated with all applications.
- Responsibility: Specify one or more responsibilities to select rules associated with those responsibilities. Or select All to select rules associated with all responsibilities.
- Conflict: Specify one or more conflicts to select rules associated with those conflicts. Or select All to select rules associated with all conflicts.
- User: Specify one or more user names or descriptions to select rules that affect those users. Or select All to select rules that affect all users.
- Reviewer: Specify one or more reviewers to select rules subject to those reviewers. Or select All to select rules subject to all reviewers.
- Entity Type: Specify Function or Responsibility to select rules based on one entity or the other, or Both for both types of conflict.
- Control Type: Specify Approval Required, Allow with Rules, or Prevent select rules based on the control type you select, or All to select all control types.
- Conflict Status: Specify a status — Approved, Rejected, Pending, or Prevent — to select conflicts only at that status, or select All to view conflicts at all three statuses.
- Same OU: Select *Y* (for yes) to list rules that apply within operating units or *N* (for no) to list rules that apply across operating units. Or select Both to list both types of rule.
- Same SOB: Select *Y* (for yes) to list rules that apply within sets of books or *N* (for no) to list rules that apply across sets of books. Or select Both to list both types of rule.

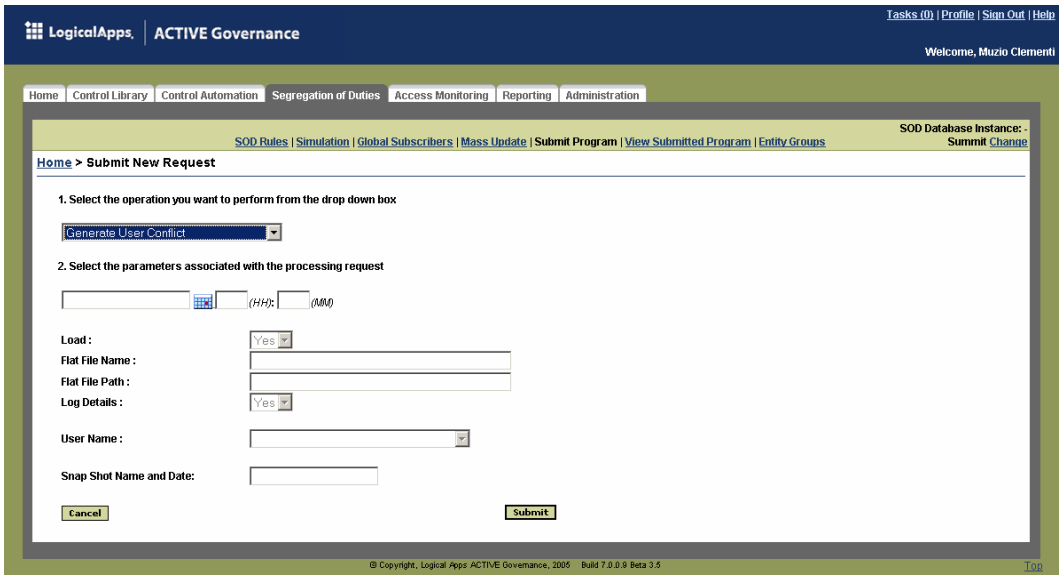
Running Background Programs

You can run background programs to complete six tasks:

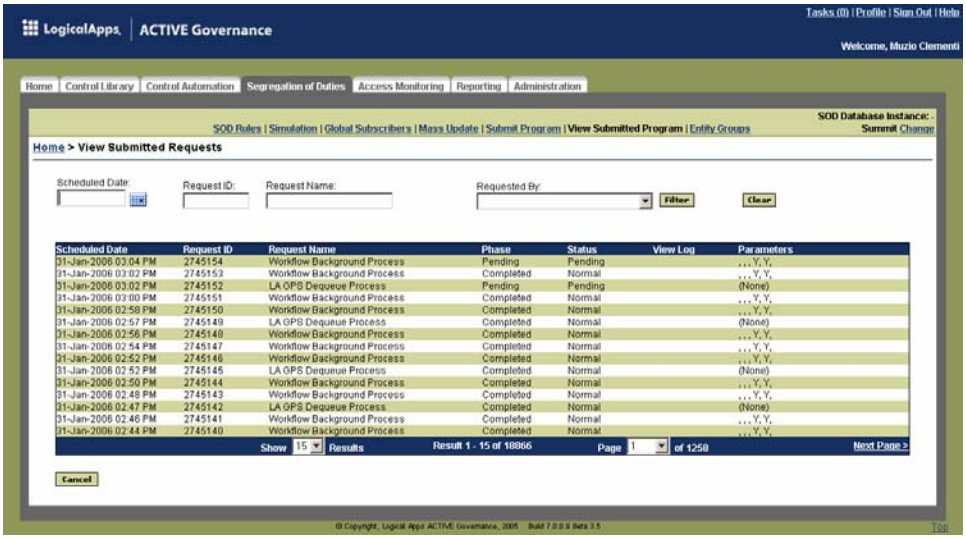
- Generate User Conflicts determines whether assignments of responsibilities to users violate SOD rules. It generates a "snapshot" — a record of the conflicts that exist at the moment you run the conflict-generation program.
- Extract SOD Conflict Rules generates a CSV file containing a record of each SOD rule that is not end-dated. The file is used for uploading rules to another instance.
- 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 LogicalApps.
- Archive User Conflicts selects records of conflicts older than a specified date and stores them in a history table.
- Reset User Conflicts 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).
- LAA Populate WF Roles Table 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 Approver 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.

To run a background program:

1 With the Segregation of Duties tab selected in the ACTIVE Governance Platform, select Submit Program in the Library Navigator:



2. In the Select Operation list box (beneath the descriptive text labeled as step 1), select the request you want.
3. In the "step 2" area of the panel, select parameters for the request you chose. You can enter values only in fields appropriate to the request you chose.
   - Generate User Conflicts: In the Snap Shot field, type a unique name for the generation of conflicts you are about to create. (This parameter is optional.)
   - Extract SOD Conflict Rules: Do not enter any parameters.
   - Load SOD Conflict Rules: Set the following four parameters.
     – Load: Select *Yes* to upload SOD rules from a spreadsheet, or *No* to validate the rules without uploading 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 upload file. (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.
   - Archive User Conflicts: Use the date and time fields to select the date before which all conflict data should be archived. Click on the icon next to the first field to display a popup calendar, and select a date from it; type two-digit numbers to define a time of day in the *HH* (hours), *MM* (minutes), and *SS* (seconds) fields.
   - Reset User Conflicts: Select in the User Name list box the name of the user whose conflicts you want to reset.
   - LAA Populate WF Roles Table: Do not enter any parameters.
4. Click on the Submit button. A background program is "submitted," and the ACTIVE Access Governor display shifts to a View Submitted Program panel, which displays the status of programs that have been run or are running:



5. Optionally, filter the entries in the list: Enter values in any combination of the fields that form a horizontal row above the list of submitted programs. Then click on the Filter button, and the panel displays only entries that match your filtering criteria. You can filter on the date a program is scheduled to run (click on the icon next to the Scheduled Date field, and then on a date in a pop-up calendar), the ID number or name of the program, its "phase" (completed, running, or pending), or the username of the user who submitted the program.

   To restore the full list of submitted programs, click on the Clear button.

6. As needed, click on the Refresh button of your web browser to update the Phase and Status fields. The program you submitted has finished running when, in its row, the Phase field reads "Completed" and the Status field reads "Normal."