

ACTIVE Governance™

ACTIVE Access Governor™ User's Guide

Software Version 7.1

© 2006 LogicalApps

All rights reserved. Printed in USA.

Restricted Rights Legend

This software and associated documentation contain proprietary information of LogicalApps. It is provided under a license agreement containing restrictions on use and disclosure and it is also protected by copyright law. Reverse engineering of this software is prohibited.

The information contained in this document is subject to change without notice. LogicalApps does not warrant that this document is error free. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of LogicalApps.

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.

ACTIVE Governance, ACTIVE Access Governor, ACTIVE Data Governor, ACTIVE Policy Governor, AppsRules, AppsAccess, and AppsFlow are trademarks of LogicalApps. All trademarks and registered trademarks are the property of their respective owners.

Document Version AG003-710I

8/24/07

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

Contents

Introducing ACTIVE Access Governor	1
Segregation of Duties	1
Access Monitoring	3
Starting ACTIVE Access Governor	3
Rights to Features	4
Navigational Conventions.....	5
Library Navigator	5
Breadcrumbs	5
Lists of Values.....	6
Sorting and Selecting Items in Lists.....	6
Defining Segregation-of-Duties Rules	9
Filtering the Display of SOD Rules.....	10
Creating SOD Rules Manually	10
Starting the Rule	11
Filtering Entities	12
Finishing the Rule.....	12

Linking the SOD Rule to AppsForm Rules.....	13
Viewing, Editing, and Copying SOD Rules	14
Working with Entity Groups	14
Creating Groups.....	14
Viewing Groups	16
Editing Groups.....	16
Copying Groups.....	17
Creating Global Subscribers.....	18
Operating Units.....	18
Submenus	19
Data Groups	20
Users	20
Uploading SOD Rules from a Spreadsheet	21
Generating and Reviewing Conflicts	23
Generating User Conflicts.....	24
Viewing User Conflicts	24
Updating Status for User Conflicts	25
Mass Updating User Conflicts	27
Resolving Conflicts.....	29
Manual Conflict Resolution.....	29
Simulation and Remediation	30
Creating Simulation Rules.....	31
Generating and Viewing Simulation Results.....	33
Remediation.....	34
Automated Conflict Resolution.....	35
Activating Responsibilities.....	35
Responding to Notifications	37
Background Programs	39
Generate User Conflicts	41
Archive User Conflicts.....	41
Extract SOD Conflict Rules.....	41
Load SOD Conflict Rules.....	41
Reset User Conflicts	42

LAA Populate WF Roles Table	42
LAA Populate User Access Data Table.....	42
LA Export/Import Groups and Rules	43
Access Monitoring	47
Preparing Tables for Auditing.....	48
Selecting Audit Tables and Columns.....	48
Setting Up Translations	50
Saving Your Work.....	51
Creating Database IDs	51
Displaying a List of Access Requests	52
Creating a New Request.....	52
Starting the Request	52
Requesting Database-Table Access	54
Requesting Responsibility Access	54
Completing the Request	54
Viewing Requests	55
Reports	57
Segregation of Duties Folder.....	58
User Conflicts Report.....	58
Conflict Summary Report	59
Responsibilities with Conflicts Report.....	59
Responsibility Menu Report	60
Function Where Used Report	60
User Conflicts Trend Analysis Report	61
Conflict Rule Listing Report.....	61
Reviewer Performance Report	62
Conflicts by Responsibility or Application Report.....	62
Simulation Remediation History Report.....	62
Global Subscribers Report.....	63
User Conflicts Master CSV Report.....	63
Oracle EBS Security Folder.....	64
Oracle EBS User Details Report.....	64
Oracle EBS Function Details Report.....	65

Oracle EBS Responsibility Details Report.....66

Access Monitoring Folder67

Access Monitoring User Activity Report67

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.

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

Segregation of Duties

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

groups that should not be assigned simultaneously to individuals. Users may create rules one at a time, or upload a set of rules supplied by 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 runs a “background program” called Generate User Conflicts; it evaluates Oracle Applications users, noting those whose work assignments violate rules. ACTIVE Access Governor then lists the conflicts generated by each rule in a panel called User Conflicts. It treats these conflicts in either of two ways:

- A user may have been assigned responsibilities or functions before a rule was created to define them as conflicting. If so, the User 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.

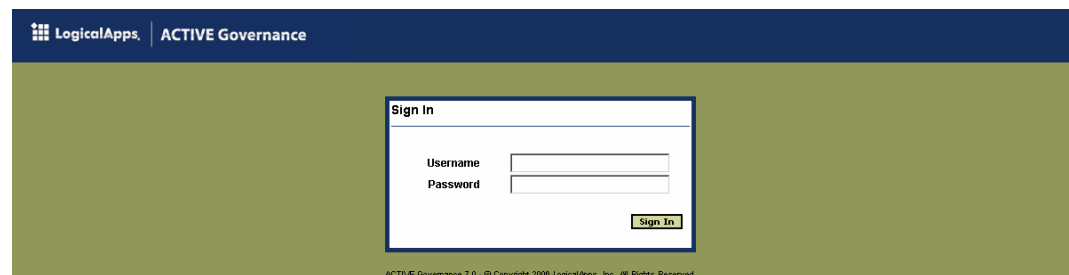
Access Monitoring

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

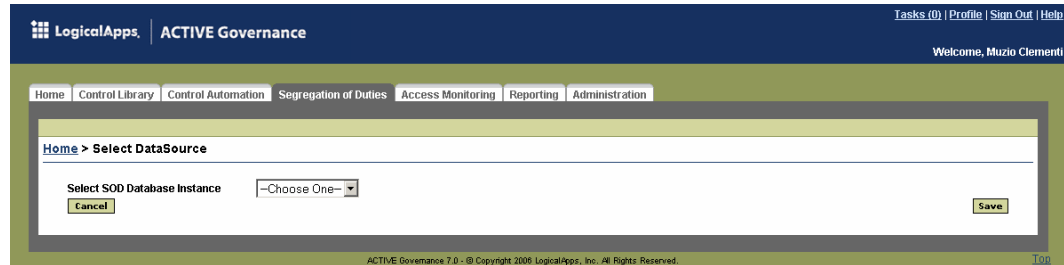
Starting ACTIVE Access Governor

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

- 1 Open Internet Explorer.
- 2 In the Address field, type the URL for your instance of the ACTIVE Governance Platform, and press the Enter key. (Using standard Windows procedures, you can, of course, save the URL as a favorite or create a desktop shortcut to the URL.)
- 3 A Sign In dialog box appears. Type your user name and password in the appropriate fields, and click on the Sign In button.



- 4 The ACTIVE Governance Platform opens. In it, click on either of two tabs: Segregation of Duties to make use of the SOD features, or Access Monitoring to make access requests.
- 5 No matter which tab you select, a Select Datasource panel prompts you to choose among instances of databases that store Oracle Applications data, and to which access controls may be applied. Select a database instance in the list box and click on the Save button.



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

Rights to Features

Each user is assigned a “primary application role” when his user account is created in the ACTIVE Governance Platform. At any role, you can use Access Monitoring. Among the features available from the Segregation of Duties tab, any role enables you to review conflicts generated by SOD rules, either viewing the status of a conflict or updating status if the conflict is generated by a rule that designates you as an approver. Your rights to other features on the Segregation of Duties tab depends on your role:

- If your role is SOD Super User, you have full rights. You can view, create, and edit SOD rules; view, create, and edit entity groups; view, create, and edit global subscribers (data groups, submenus, functions, operating units, or users who are exempt from SOD rules); create, edit, and view rules that simulate changes intended to resolve conflicts; run simulation and view results; and run remediation (put simulated conflict resolutions to actual use).
- If you are an Author, Manager, or Rule Builder, you have create rights. These are the same as full rights, except that you cannot run remediation.
- If you are a User, you have more limited create rights. You can view, create, or edit SOD rules. 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. You have no access to global subscribers.

- If you are an Auditor, Executive, or System Administrator, you have view rights. You can open a list of SOD rules, but do not have access to configuration details for individual rules, and can neither create nor edit them. Additionally, you have the same view rights as a User to entity groups and simulation features. Like a User, you have no access to global subscribers.

Navigational Conventions

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

Library Navigator

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

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



Breadcrumbs

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

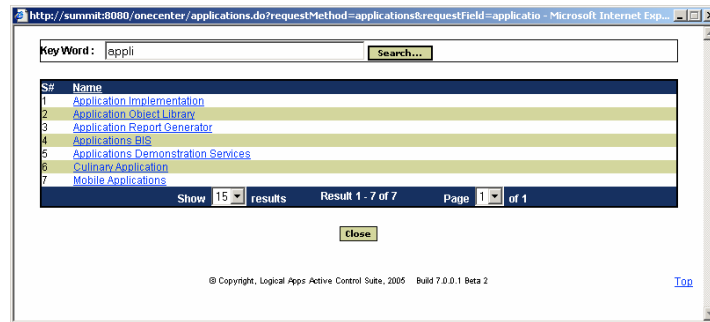


Lists of Values

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



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



- 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 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

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.

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:

LogicalApps | ACTIVE Governance

Tasks (0) | Profile | Sign Out | Help

Welcome, Muzio Clementi

Home | Control Library | Control Automation | Segregation of Duties | Access Monitoring | Reporting | Administration

SOD Rules | Simulation | Global Subscribers | Mass Update | Submit Program | View Submitted Program | Entity Groups

SOD Database Instance: Yahoo China

Home > SOD Rules

Add SOD Rule

SOD Rule: Entity Type: Entities: Group: Control Type: Priority: Approver:

Filter Clear

SOD Rule	Entity Type	Entities	Control Type	Priority	View User Conflict
Buyer/Requester	Responsibility	Purchasing Requester, Purchasing Buyer	Approval Required	1	View
Inventory/PQ	Function	Master Items, Purchase Orders	Allow with Rules	2	View
Payables	Function	Payments, Invoices, Invoice Approvals, Suppliers	Prevent	3	View
PurchSUPPayMgt	Responsibility	Payables Manager, Purchasing Super User	Approval Required	1	View

Show 15 Results Result 1 - 4 of 4 Page 1 of 1

Add SOD 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

As you create SOD rules, you may consider limiting their number (or at least the number that are active), so that the number of conflicts they generate is not overwhelming. A typical strategy is to start with a set of rules that define what you determine to be the most important conflicts, then clean up those conflicts before moving on to another set of rules.

To create a segregation-of-duties rule, click on the Add Rule button in the SOD Rules panel. An Add SOD Rules panel opens:

The screenshot shows the 'Add SOD Rules' panel in the LogicalApps ACTIVE Governance interface. The panel is titled 'Home > SOD Rules > Add SOD Rules'. It contains several input fields and buttons:

- SOD Rule ***: A text input field.
- Entity Type**: A dropdown menu with 'Function' selected.
- Application ***: A text input field.
- Available Entities**: A list box with 'Filter' and 'Clear' buttons.
- Selected Entities ***: A list box with a '>' button to move items from Available Entities.
- Control Type**: A dropdown menu with 'Approval Required' selected.
- Priority ***: A text input field.
- Start ***: A date/time picker showing '27-Jan-2006 08:19 PM'.
- Reason ***: A text input field.
- Approver ***: A text input field.
- End**: A date/time picker.
- Same Operating Unit**: A checked checkbox.
- Same Set of Books**: A checked checkbox.
- Required**: A red asterisk indicating required fields.
- Cancel** and **Save** buttons at the bottom.

Starting the Rule

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

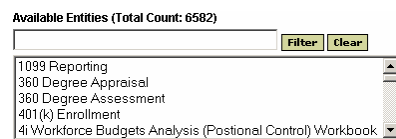
- 1 Type a name for the rule in the SOD Rule field.
- 2 Make a selection in the Entity Type list box. To define a conflict between individual items, choose Responsibility or Function. To define a conflict between entity groups, choose Group–Responsibility or Group–Function.
- 3 Choose the first of the 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. 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.

Filtering Entities

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 next to the label for the Available Entities field.



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

- 1 In the text box to the left of the Filter button, type the first few letters of the name of the item you want to select. (For example, type *Pur* for the Purchases function.)
- 2 Click on the Filter button; the Available Entities field displays only those items whose names begin with the letters you typed.

You can click on the Clear button to discard filtering criteria and redisplay the original selection of entities.

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.
- 2 In the Priority field, type a number, from 1 to 10, that reflects the importance of this rule in relation to others. (Your company should determine whether it considers 1 or 10 the highest priority, and then enforce consistent usage.) You can use the priority value to filter the rules displayed in the SOD Rules panel.
- 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, you must run a background program, called LAA Populate WF Roles Table, each time new roles are added in Oracle Applications. See “Background Programs” (page 39).

- 4 The Start field is set to the date and time at which you create the rule, and the End 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 SOD 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 Rules button near the bottom center:

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

- 3 Click on the Add Row button 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 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 Rules Manually.” 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 string of up to 4,000 characters.

Creating Groups

To create an entity group:

- 1 Click on Entity Groups in the Library Navigator. An Entity Groups panel then displays entries for all existing groups. (It’s illustrated on page 16.)

- 2 At the upper right or bottom center of this panel, click on an Add Entity Group button. An Add Entity Group panel appears:

The screenshot shows the 'Add Entity Group' panel within the LogicalApps ACTIVE Governance application. The panel has a header with the application name and user information. Below the header is a navigation bar with tabs for Home, Control Library, Control Automation, Segregation of Duties, Access Monitoring, Reporting, and Administration. The main content area is titled 'SOD Rules > Simulation > Global Subscribers > Mass Update > Submit Program > View Submitted Program > Entity Groups'. The 'Add Entity Group' panel contains the following fields and controls:

- Group Name ***: A text input field.
- Group Description**: A text input field.
- Start**: A date and time picker showing '07-Jun-2006 09:04 AM'.
- End**: A date and time picker.
- Entity Type**: A dropdown menu with 'Function' selected.
- Application ***: A text input field.
- Available Entities**: A list box with a 'Filter' button.
- Selected Entities ***: A list box with '>' and '<' buttons between the two list boxes.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom.

- 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 field is set to the date and time at which you create the group, and the End 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 then 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.

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 12).

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, then click on the < button to return it to the Available Entities field.
- 8** When you finish selecting responsibilities or functions, click on the Save button. Once the group is saved, only its name, description, and end date can be changed.

Viewing Groups

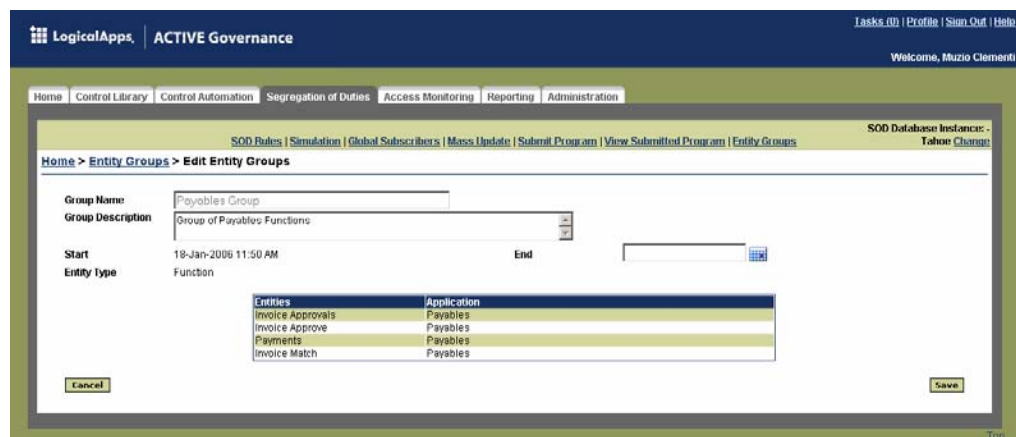
After you save a group you have created, the Entity Groups panel reappears, adding a listing for the new group to its display. The listing for each group displays its name, the entity type of its members, its description, and its start and end dates.



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

Editing Groups

To edit a group, click on 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:

LogicalApps | ACTIVE Governance

Tasks (0) | Profile | Sign Out | Help

Welcome, Muzio Clementi

Home | Control Library | Control Automation | Segregation of Duties | Access Monitoring | Reporting | Administration

SOD Rules | Simulation | Global Subscribers | Mass Update | Submit Program | View Submitted Program | Entity Groups

SOD Database Instance: - Tahoe Change

Home > Entity Groups > View Entity Group

Group Name: Payables Group
 Group Description: Group of Payables Functions
 Start: 18-Jan-2006 11:50 AM
 End:
 Entity Type: Function

Entities	Application
Invoice Approvals	Payables
Invoice Approve	Payables
Payments	Payables
Invoice Match	Payables

Cancel Copy Entity Group

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. 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).

LogicalApps | ACTIVE Governance

Tasks (0) | Profile | Sign Out | Help

Welcome, Muzio Clementi

Home | Control Library | Control Automation | Segregation of Duties | Access Monitoring | Reporting | Administration

SOD Rules | Simulation | Global Subscribers | Mass Update | Submit Program | View Submitted Program | Entity Groups

SOD Database Instance: - Tahoe Change

Home > Entity Groups > View Entity Group > Copy Entity Group

Group Name:
 Group Description:
 Start: 07-Jun-2006 09:51 AM
 End:
 Entity Type: Function
 Application:

Available Entities: Filter

Selected Entities:

Cancel Save

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

Creating Global Subscribers

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

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

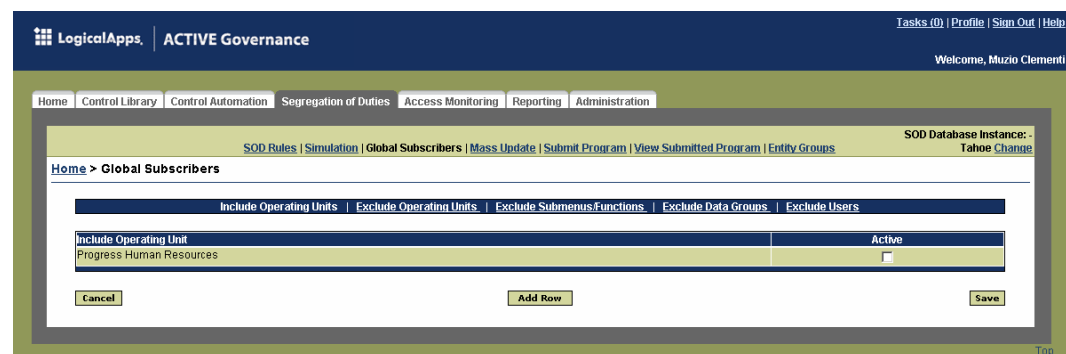
Or, you may use global subscribers to make the cleanup process more manageable (*cleanup* being the term for the resolution of conflicts that exist because responsibilities or functions were assigned to users before SOD rules were written to define them as conflicting). The number of conflicts found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

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

Operating Units

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

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



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



- 3 In each row you create, select an operating unit. It is permissible for entries to exist in both the Include and Exclude panels, but entries should be active (see the next step) in only one panel at a time.
- 4 Select or clear the Active check boxes at the right of the entries:
- If Active check boxes are selected in the Include panel, the corresponding operating units are eligible for rule processing and all others are excluded.
 - If Active check boxes are selected in the Exclude panel, the corresponding operating units are excluded from rule processing, and all others are included.

Do not select Active check boxes simultaneously in both panels.

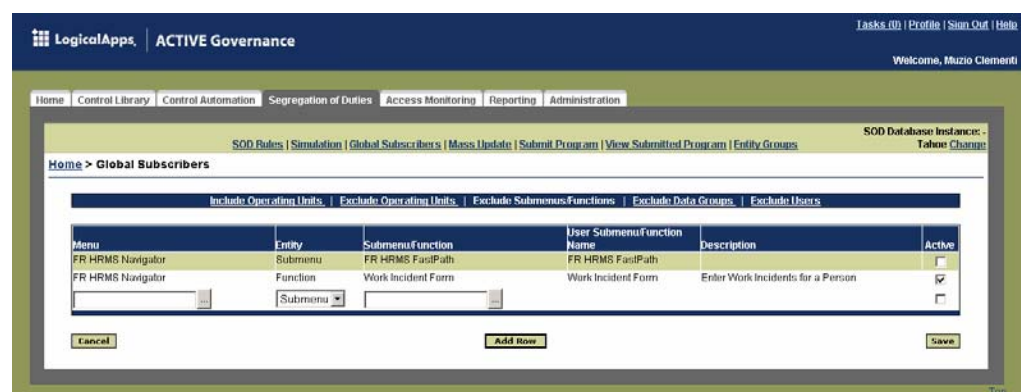
- 5 Click on the Save button.

Submenus

A submenu under one menu may provide query-only access to functions, even 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 when a user has write access, but falsely for query-only access.

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

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



- 2 Make selections in the Menu, Entity, and Submenu/Function fields. ACTIVE Access Governor supplies corresponding values in the Name and Description fields. This exclusion feature recognizes only direct parent-child relationships:
- To exclude a function, select Function in the Entity list box. Select the function and its immediate parent submenu in the Submenu/Function and Menu fields.

- To exclude a submenu, select Submenu in the Entity list box. Then specify the submenu and its immediate parent menu in the Submenu/Function and Menu fields. To exclude a submenu is to exclude all functions on that submenu.
- 3 Select the Active check box to exempt the query-only instance of the function or functions from SOD rules, while leaving write-enabled instances subject to rules. Or, clear the check box to deactivate the exemption.
 - 4 Click on the Save button.

Data Groups

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

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

- 2 In the Data Group list of values, select the group that is to receive the exclusion.
If a description was written when the group was created, it appears by default in the Description field. If no description was written, the field remains blank. The Description field does not accept direct input.
- 3 The Active check box is selected by default. Leave it selected for the exclusion to take effect. Clear it (click on it so that no check mark appears) to reserve an exclusion for the group, but not have it take effect at present.
- 4 Click on the Save button.

Users

You can exclude individual users from SOD rule processing:

- 1 In the Global Subscribers panel, click on the Exclude Users link. Then click on its Add Row button.
- 2 In the User list of values, select the ID of the user who is to receive the exclusion.
If a description of the user was written when the user ID was created, it appears by default in the Description field. If no description was written when the user

ID was created, the field remains blank. The Description field does not accept direct input.

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

4 Click on the Save button.

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

Uploading SOD Rules from a Spreadsheet

Rather than create SOD rules one at a time, you can select rules in a Microsoft Excel spreadsheet, edit them to contain values appropriate for your site, and upload them at once. 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 controls.
Requisition Summary*Purchase Orders	Function	Oracle Purchasing	Requisition Summ	Oracle Purchasing	Purchase Orders	Approval Required	SYSADMIN	Buyers should not process their own process controls.
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 controls.
Requisitions*Releases	Function	Oracle Purchasing	Requisitions	Oracle Purchasing	Releases	Prevent	SYSADMIN	Buyers should not process their own process controls.
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 controls.
Requisition Summary*Releases	Function	Oracle Purchasing	Requisition Summ	Oracle Purchasing	Releases	Prevent	SYSADMIN	Buyers should not process their own process controls.
Requisitions*AutoCreate Documents	Function	Oracle Purchasing	Requisitions	Oracle Purchasing	AutoCreate Documents	Prevent	SYSADMIN	Buyers should not process their own process controls.
Requisition Summary*AutoCreate Document	Function	Oracle Purchasing	Requisition Summ	Oracle Purchasing	AutoCreate Documents	Allow with Rules	SYSADMIN	Buyers should not process their own process controls.
PO Summary: Create New PO*Receipts	Function	Oracle Purchasing	PO Summary: Cre	Oracle Purchasing	Receipts	Allow with Rules	SYSADMIN	Receiving personnel should never h
Releases*Receipts	Function	Oracle Purchasing	Releases	Oracle Purchasing	Receipts	Allow with Rules	SYSADMIN	Receiving personnel should never h
AutoCreate Documents*Receipts	Function	Oracle Purchasing	AutoCreate Docu	Oracle Purchasing	Receipts	Allow with Rules	SYSADMIN	Receiving personnel should never h

- 2** In the upper left corner of the Access Load Values sheet, provide the ODBC driver name, connect string, Apps user name, and Apps password.
- 3** Click on the Update Data button. The spreadsheet is populated with up to 65,536 rows of SOD rule data. (Owing to Excel limitations, this is the maximum number.)
- 4** Review the rules and select those you want to upload: In the Load column, select *Y* for rules you want or *N* for those you don't want.
- 5** Edit values in the following columns as appropriate for the rules you are uploading: Control Type, Approver, Reason, Same Operating Unit, and Same Set of Books. (Note that if the Same Operating Unit or Same Set of Books value is null, the upload operation will fail.) You cannot change the values in other columns.

In particular, SYSADMIN is the default conflict approver for all SOD rules. For each rule, change this value to an appropriate approver.
- 6** On the Tools menu, click Create CSV for 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 “Background Programs” (page 39).

Generating and Reviewing Conflicts

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

For conflicts generated by Prevent or Allow with Rules SOD rules, the status is set to Prevent or Allow with Rules, respectively, and stays that way. For 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 the Action History or Mass Update form 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

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

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

To generate user conflicts, run the Generate User Conflicts background program. For the procedure, see “Background Programs” (page 39).

Viewing User Conflicts

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

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

The screenshot shows the 'User Conflicts' panel in the LogicalApps ACTIVE Governance interface. The panel is titled 'Home > SOD Rules > User Conflicts'. It displays details for a specific SOD rule and a table of conflicts.

SOD Rule Details:

SOD Rule	Buyer*Requester
Entity	Purchasing Requester, Purchasing Buyer
Entity Type	Responsibility
Run Date	Jan 30, 2006

Filtering Fields:

User Name:	Responsibility:	Conflicting Responsibility:	Status:	Filter	Clear
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="All"/>		

Conflicts Table:

User Name	Responsibility	Conflicting Responsibility	Status
USCARLOTTI	Purchasing Buyer	Purchasing Requester	Pending
ACORRELLI	Purchasing Buyer	Purchasing Requester	Pending

At the bottom of the table, it says 'Show 15 results' and 'Page 1 of 1'.

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 a full responsibility name to see conflicts in which your selection is the “base” responsibility, or type a text fragment to display conflicts generated by rules for which the base responsibility name includes the fragment. A base responsibility is the first of two that are in conflict, or the one containing the first of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the first responsibility.
- **Conflicting Responsibility:** Type the full name of a responsibility to see conflicts in which your selection is the “conflicting” responsibility, or type a text fragment to display conflicts generated by rules for which the conflicting responsibility name includes the fragment. A conflicting responsibility is the second of two that are in conflict, or the one containing the second of two functions that are in conflict. For a rule that includes more than two responsibilities or functions, the search identifies pairs of responsibilities for which conflicts exist, and returns those for which this is the second responsibility.
- **Status:** Select a status — Approved, Pending, or Rejected — to see conflicts at the selected status, or select All to see conflicts at all statuses. This filter pertains only to conflicts generated by 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.

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 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. The Action History panel opens:

The screenshot shows the LogicalApps ACTIVE Governance web interface. The top navigation bar includes links for Home, Control Library, Control Automation, Segregation of Duties, Access Monitoring, Reporting, and Administration. The main content area displays the 'Action History' panel for a specific Segregation of Duties Rule. The panel includes a table with columns for Action by, Action Type, Start, End, and Comments. The table shows a single row with the following data:

Action by	Action Type	Start	End	Comments
MCLEMENTI	Approved	15-Dec-2005 00:00:00		Access approved per Policy HR124.

Below the table are buttons for 'Cancel', 'Add Row', and 'Save'. The 'Add Row' button is highlighted, indicating it is the next step in the process.

- 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.

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:

- 1 Click on the Add Row button. (This button appears only if you are a designated approver for the conflict). The Action By field defaults to your user name. The Start field defaults to the date on which you are taking action, and cannot be changed; the End field is blank and does not accept input.
- 2 In the Action Type field of the row you created, select Approved, Rejected, or Pending:
 - Approving a user conflict means that you know it exists 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, and must take steps to resolve the conflict (see “Resolving Conflicts” on page 29).
 - Pending is the default status, indicating that a decision is yet to be made.
- 3 In the Comments field, type a brief explanation for your approval decision.
- 4 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:

LogicalApps | ACTIVE Governance Tasks (0) | Profile | Sign Out | Help
Welcome, Muzio Clementi

Home | Control Library | Control Automation | Segregation of Duties | Access Monitoring | Reporting | Administration

SOD Database Instance: Tahoe Change

Home > Mass Update

User Name: SOD Rule: Responsibility: Conflicting Responsibility:

<input type="checkbox"/>	User Name	SOD Rule	Responsibility	Conflicting Responsibility
<input type="checkbox"/>	JPALMER	AT1	System Administrator, Progress S&L	Asset Manager, Progress S&L
<input type="checkbox"/>	JPALMER	AT1	Super User, Progress S&L	Asset Manager, Progress S&L
<input type="checkbox"/>	JPALMER	AT1	System Administrator, Progress S&L	Super User, Progress S&L
<input type="checkbox"/>	JPALMER	AT1	Super User, Progress S&L	Super User, Progress S&L
<input type="checkbox"/>	PSTOCKMAN	AT1	System Administrator, Vision University	Assets, Vision University
<input type="checkbox"/>	SWEDEN	AT1	System Administration Vision Sweden	Assets Vision Sweden
<input type="checkbox"/>	OPERATIONS	AT1	System Administrator	Assets, Vision Operations (USA)
<input type="checkbox"/>	BRUNO	AT1	System Administration Vision France	Assets Vision France
<input type="checkbox"/>	TREASURER	AT1	Implementation Financials	Implementation Financials
<input type="checkbox"/>	SPAIN	AT1	System Administration Vision Spain	Assets Vision Spain
<input type="checkbox"/>	DTRIPPE	AT1	System Administrator, Vision University	Assets, Vision University
<input type="checkbox"/>	CHORTON	AT1	System Administrator	Assets, Vision Operations (USA)
<input type="checkbox"/>	BIRGIT	AT1	System Administration Vision Germany	Assets Vision Germany
<input type="checkbox"/>	BIRGIT	AT1	System Administration Vision Germany	Financial Management Vision Germany
<input type="checkbox"/>	EBUSINESS MANUFACTURING	AT1	Applications Administration	Applications Administration

Show 15 Results

☐ Display record count

Comments

- 2 Set filtering criteria that determine what conflicts you will see (although no matter what criteria you select, you have access only to conflicts generated by SOD rules for which you are a designated approver). Then click on the Filter button. If you set no criteria, the panel 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** If you want to assign status to all the filtered conflicts at once, skip ahead to step 4. If you want to assign status to a subset of the filtered conflicts, select those whose status you want to update. The Mass Update form presents conflicts in a grid divided into “pages,” and if you are selecting individual conflicts, you can select them from only one page at a time.

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

- Select check boxes alongside individual conflicts you intend to approve or reject.
 - Select a check box in the header row of the grid (to the left of the User Name heading) if you want to approve or reject all conflicts in the currently displayed page of the grid.
- 4** In the Comments field, type an explanation for your decision to update status. The comment is required, and it applies to all of the conflicts whose status you are updating.
 - 5** If (in step 3) you selected a set of conflicts, click on either the Approve or Reject button. If not, click on the Approve All or Reject All button to approve or reject all the conflicts that match your filtering criteria (that is, all the conflicts in all the pages of the grid). In either case, ACTIVE Access Governor assigns the status you select and the comment you wrote to each newly statused conflict. It removes these conflicts from the list, and leaves the Mass Update form in place.
 - 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.

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, or when they are regenerated after SOD rules have changed, you are likely to find users who had been granted access to responsibilities or functions before rules defined them as conflicting. ACTIVE

Access Governor uncovers these conflicts but does not resolve them. Instead, you can eliminate these conflicts manually, a process known as “cleanup.”

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

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

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

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

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

See Oracle documentation for procedures on excluding functions or menus from responsibilities, or removing functions from menus. To facilitate mapping functions to menus, a Function Where Used Report (see page 60) displays the menu paths to functions involved in function-based conflicts.

Simulation and Remediation

To aid in cleanup, ACTIVE Access Governor enables you to write simulation 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, ACTIVE Access Governor can perform “remediation” — modify function, menu, and responsibility configurations in Oracle Applications to implement the simulated conditions.



Note

If changes have been made manually in Oracle Applications since the most recent user-conflict snapshot was created in Access Governor, simulation results may *appear* to be inaccurate. Such changes include the creation of users, the modification of responsibility assignments for existing users, or alterations in the exclusion of functions from responsibilities, the assignment of functions to menus, or the assignment of submenus to other menus or responsibilities.

When such changes are made, they are likely to resolve existing conflicts in your system or to create new conflicts, thus rendering the most recent user-conflict snapshot obsolete. Because the simulation process involves the generation of a new snapshot, the process no longer addresses the conflicts in the snapshot that had been most recent, but is now obsolete. Hence the *apparent* inaccuracy; simulation addresses a set of actual conflicts that is in fact more accurate than the set displayed in the User Conflicts panel.

To prevent this discrepancy, you should run the Generate User Conflicts background program immediately before evaluating a set of simulation rules.

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 Function 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 may 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 Criteria panel opens, displaying an entry for each existing simulation rule:

The screenshot shows the 'Simulation Criteria' panel in the LogicalApps ACTIVE Governance interface. The panel has a header with 'LogicalApps | ACTIVE Governance' and a user welcome message 'Welcome, Muzio Clementi'. Below the header is a navigation bar with tabs: Home, Control Library, Control Automation, Segregation of Duties, Access Monitoring, Reporting, and Administration. The main content area shows a table with the following data:

Enabled	Action	Entity Type	Entity	Entity Type From (Remove) / Into (Insert)	Entity
N	Exclude	Function	Invoice Approvals	Responsibility	Payables Super User

Below the table, there are controls for 'Show' (set to 15), 'Results', 'Page 1 of 1', and 'Page 1 of 1'. At the bottom of the panel are buttons: Cancel, Update Simulation Criteria, Simulate, Remediate, and View Results.

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

The screenshot shows the 'Edit Simulation Criterion Value' panel in the LogicalApps ACTIVE Governance system. The panel has a breadcrumb trail: Home > List Simulation Criteria > Edit Simulation Criterion Value. It features a table with the following columns: Enable, Action, Entity Type, Entity, Entity Type From (Remove) / Info (Insert), Entity, and Delete. The first row is pre-filled with 'Exclude' in the Action field, 'Function' in the Entity Type field, 'Invoice Approvals' in the Entity field, 'Responsibility' in the Entity Type From field, and 'Payables Super User' in the Entity field. The 'Add Row' button is located at the bottom center of the table.

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

For example, to create the rule that simulates the exclusion discussed in step 1, select Exclude in the Action field, Function in the Entity Type field, and 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 enabled simulation rules at one time. Create as many rules as you need to define a set of simulation criteria, and select the Enable check box for each of them. Clear the Enable check box for any rule that does not fit your simulation criteria. (To select a check box is to click on it so that a check mark appears, and to clear it is to click on it again so that the mark disappears.) You can select the Enable check box in the header row to enable all existing simulation rules.

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

- 6 Click on the Save button. The Simulation Criteria panel returns, displaying all rules you have not deleted. (For each, the Enabled field reads *Y* if the rule is enabled or *N* if it is not.)

Generating and Viewing Simulation Results

To run the simulation rules you have configured, click on the Simulate button in the Simulation Criteria panel. 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 Criteria panel.

Then click on the View Results button. A Simulation Results panel shows the following:

- Summary information: Near the top, 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.

You can change this initial focus: 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.

The screenshot displays the 'Simulation Results' page in the LogicalApps ACTIVE Governance interface. At the top, there are navigation tabs: Home, Control Library, Control Automation, Segregation of Duties, Access Monitoring, Reporting, and Administration. Below these, a breadcrumb trail reads: Home > Simulation Criteria > Simulation Results. The main content area shows summary statistics: Total User Conflicts: 95818, Simulation Results: Removed (95799) | Created (0) | Net Change (-95799). Below this, there are links for User Conflicts (95799), Users (238), and Responsibilities (393). A filter section allows users to search by User Name, SOD Rule, Responsibility, Conflicting Responsibility, and Control Type. A table lists individual conflicts with columns for User Name, +/-, SOD Rule, Responsibilities, Conflicting Responsibilities, and Control Type. The table shows five rows of conflicts for user ZSTUDENTL, all related to rule 703. At the bottom, there is a pagination bar showing 'Result 1 - 5 of 95799' and 'Page 1 of 19160'.

User Name	+/-	SOD Rule	Responsibilities	Conflicting Responsibilities	Control Type
ZSTUDENTL	-	copy of rule is 703	General Ledger Super User (Process Operations)	General Ledger Super User (Process Operations)	Approval Required
ZSTUDENTL	-	copy of rule is 703	General Ledger Super User Payables Super User (Process Operations)	General Ledger Super User Payables Super User (Process Operations)	Approval Required
ZSTUDENTL	-	copy of rule is 703	General Ledger Super User Purchasing Super User (Process Operations)	General Ledger Super User Purchasing Super User (Process Operations)	Approval Required
ZSTUDENTL	-	copy of rule is 703	General Ledger Super User Inventory Super User (Process Operations)	General Ledger Super User Inventory Super User (Process Operations)	Approval Required
ZSTUDENTL	-	copy of rule is 703	General Ledger Super User Receivables Super User (Process Operations)	General Ledger Super User Receivables Super User (Process Operations)	Approval Required

Whether you are focused on conflict, user, or responsibility, you can filter the results. Enter complementary values in any combination of the following fields, and then press the Filter button:

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

When you are finished viewing results, click on the Cancel button, or on the Simulation Criteria link in the breadcrumbs trail, to return to the Simulation Criteria panel.

Remediation

If you are satisfied with the results, Access Governor can implement “remediation” — actually make the simulated changes. To do this, an SOD Super User clicks on the Remediate button in the Simulation Criteria panel. (For other users, this button does not appear.) This launches a 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 Users form open, a system administrator selects a user and, in the grid accessible from the Responsibilities tab, assigns responsibilities. Both the start and end dates for these responsibilities are set by default to the current date, and cannot be modified directly. The administrator saves the new assignments.
- 2 The administrator clicks on Actions in the menu bar, then on Activate Responsibilities in the Actions menu. An Activate Responsibilities form opens; it presents a copy of the responsibilities listed in the Users form, but allows the administrator to change the end dates.

The screenshot shows the Oracle Applications Users form and the Activate Responsibilities dialog box. The Users form has tabs for Direct Responsibilities, Indirect Responsibilities, and Securing Attributes. The Activate Responsibilities dialog box is open, showing a table of responsibilities for user ALAN.

Responsibility	Application	Security Group	From	To
Purchasing Super User	Purchasing	Standard	03-JUN-2005	03-JUN-2005
Payables Manager	Payables	Standard	03-JUN-2005	03-JUN-2005

Buttons: Cancel, Initiate Conflict Analysis

**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 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 Rules 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.

Responsibility	Conflicting Responsibility	Conflict Rule Name	Control Type	Status
Purchasing Super User	Payables Manager	Conflict Rule 1	Approval R	Approval Flow will b
Payables Manager	Purchasing Super User	Conflict Rule 1	Approval R	Approval Flow will b
Purchasing Super User	Purchasing Super User	Purch/Rec Function	Approval R	Approval Flow will b

- 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:

From	Subject	Sent
SYSADMIN	User ALAN has conflicting Responsibilities as per conflict Conflict Rule 1	11-May-2005

- 2 Click on the notification to open it:

ORACLE
E-Business Suite Home

[Return to Portal](#) [Logout](#) [Preferences](#) [Help](#)

User ALAN has conflicting Responsibilities as per conflict Conflict Rule 1

From: SYSADMIN
To: SAdams
Sent: 11-May-2005 19:33:00
Notification ID: 406598

Conflict Name: Conflict Rule 1
User: ALAN
Responsibility: Purchasing Super User
Conflicting Resp: Payables Manager
Notification History

Seq	Performer	Start Date	End Date	Action	Comment
1	SYSADMIN	11-MAY-2005 19:32:59	11-MAY-2005 19:32:59	Submitted	

Response

COMMENT

[Return to Worklist](#)

☐ Display next notification after my response

[Return to Portal](#) [Logout](#) [Preferences](#) [Help](#)

Copyright 2003 Oracle Corporation. All rights reserved.

[Privacy Statement](#)

- 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. 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 were 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.

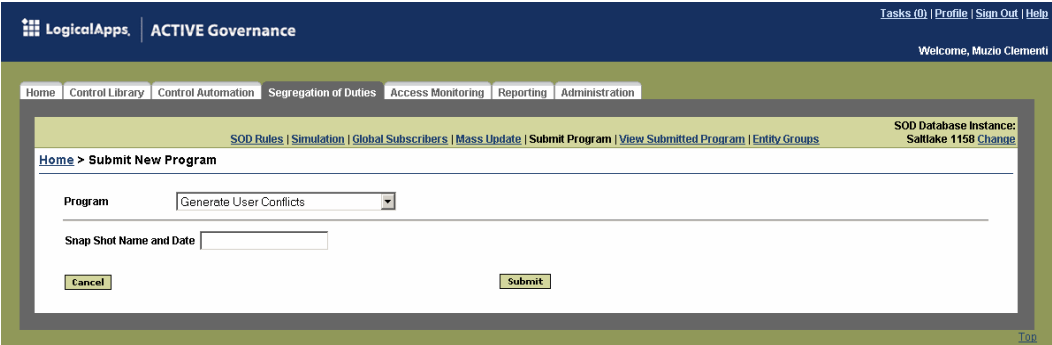
5 Click on the Return to Portal link.

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

Background Programs

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

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



The screenshot displays the ACTIVE Governance Platform interface. At the top, the header includes the LogicalApps logo and the text 'ACTIVE Governance'. On the right side of the header, there are links for 'Tasks (0)', 'Profile', 'Sign Out', and 'Help', along with a welcome message 'Welcome, Muzio Clementi'. Below the header is a navigation bar with tabs: 'Home', 'Control Library', 'Control Automation', 'Segregation of Duties' (which is selected), 'Access Monitoring', 'Reporting', and 'Administration'. Under the 'Segregation of Duties' tab, there is a sub-navigation bar with links: 'SOD Rules', 'Simulation', 'Global Subscribers', 'Mass Update', 'Submit Program' (which is selected), 'View Submitted Program', and 'Entity Groups'. The main content area shows the 'Submit New Program' panel. It features a 'Program' dropdown menu with 'Generate User Conflicts' selected. Below this is a 'Snap Shot Name and Date' text input field. At the bottom of the panel are two buttons: 'Cancel' and 'Submit'. In the top right corner of the panel, there is a status bar that reads 'SOD Database Instance: Saltlake 1158' with a 'Change' link next to it.

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

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

The screenshot shows the 'View Submitted Program' panel in the ACTIVE Governance interface. The panel has a header with 'LogicalApps | ACTIVE Governance' and a welcome message 'Welcome, Muzio Clementi'. Below the header is a navigation bar with links: Home, Control Library, Control Automation, Segregation of Duties, Access Monitoring, Reporting, and Administration. The main content area has a sub-header 'SOD Rules | Simulation | Global Subscribers | Mass Update | Submit Program | View Submitted Program | Entity Groups'. The 'View Submitted Program' link is active. Below the sub-header is a search bar with fields for Scheduled, Program ID, Program Name, Phase, and Requester. The Program ID field is filled with '1473962'. There are 'Filter' and 'Clear' buttons. Below the search bar is a table with columns: Scheduled, Program ID, Program Name, Phase, Status, View Log, and Parameters. The table contains one row with the following data: Scheduled: 08-Jun-2006 04:15 PM, Program ID: 1473962, Program Name: LA AppsAccess Generate User Conflicts, Phase: Pending, Status: Scheduled, View Log: (link), Parameters: (link). Below the table is a 'Show 15 Results' button and a 'Page 1 of 1' indicator. There is also a 'Cancel' button at the bottom left.

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

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

- **Scheduled:** Enter a date to see programs that ran on that date. Type the date, in the format *DD-MMM-YYYY*. Alternatively, click on the icon next to the field, and a pop-up calendar appears. In it, click on the < or > symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want.
- **Program ID:** Enter the ID number of program run you want to view. This number is assigned automatically when the program is run (and is the value ACTIVE Access Governor uses, when you submit a program, to display only an entry for that program).
- **Program Name:** Enter a program name (or a fragment of the name) to see entries for occasions when that program was run.
- **Phase:** Select the “phase” of a program run — Completed, Running, or Pending — to see entries for programs that have finished running, are still running, or have yet to run. Or select All to see entries for programs in any phase.
- **Requester:** Select a username to see entries for programs run by that user.

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

Generate User Conflicts

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

Archive User Conflicts

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

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

You can view archived conflicts in reports that are available in the Segregation of Duties folder of the Report Center (see page 58): User Conflicts, Conflict Summary, Responsibilities with Conflicts, Responsibility Menu, User Conflicts Trend Analysis, and Conflicts by Responsibility or Application. In each report, use the Snapshot Run Date parameter to select a snapshot containing archived conflicts you want to see.

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

Extract SOD Conflict Rules

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

The CSV file is located in the directory that corresponds to the \$APPLCSF/\$APPLOUT environment variables on the Oracle ERP server. The file name is o*ProgramID*.out, in which the *ProgramID* placeholder stands for the ID number generated as you run the

Extract SOD Conflict Rules program. This number is displayed in the Program ID field of the View Submitted Program panel.

Load SOD Conflict Rules

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

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

Reset User Conflicts

The Reset User Conflicts program rescinds the provisional assignment of conflicting responsibilities to a user if no approver has passed judgment on the assignment. Until an approver acts, the user has no access to the responsibilities and the assignment cannot be changed. If the judgment never occurs (if, for example, the approver leaves the company), the Reset User Conflicts request can be run; the user's responsibilities return to their original state, and the assignment can be made again (with the rule that generated the conflict rewritten to designate another approver). The program takes a single parameter: In the User Name list box of the Submit New Program panel, select the name of the user whose conflicts you want to reset.

LAA Populate WF Roles Table

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

LAA Populate User Access Data Table

The LAA Populate User Access Data Table program updates a database table that contains information about users' responsibility, menu, and function assignments. The table provides this information to the Oracle EBS Security reports when they

are run, and so whenever the reports are run, the LAA Populate User Access Data Table program should be run first. The program takes no parameters.

LA Export/Import Groups and Rules

The LA Export/Import Groups and Rules program works with pairs of files, one containing entity groups and the other containing SOD rules that specify groups as their conflicting entities. The program exports groups and rules from one ACTIVE Access governor instance to the files, and then imports the groups and rules from the files to a second instance. It takes the following parameters:

- **Group File Name:** Enter the name of a CSV file to which you are exporting, or from which you are importing, groups.
- **Rules File Name:** Enter the name of a CSV file to which you are exporting, or from which you are importing, rules.
- **Location:** Enter the directory path to the files to which you are exporting, or from which you are importing, groups and rules.
- **Mode:** Select *Export* or *Import* to specify the operation the program is to perform.
- **Debug:** Select *Yes* to add LogicalApps content to the default Oracle log file, or *No* to withhold that content. Typically, select *Yes* only to troubleshoot a problem with an export or import operation.
- **Default Reviewer:** Select a user whose ID can be inserted as approver into rules as they are imported into an ACTIVE Access Governor instance. For a given rule, the original approver is retained during an import operation if that approver exists on the import instance, but this default reviewer is inserted into the rule if the original approver does not exist on the import instance. Be sure to specify a default reviewer whose ID exists on the instance into which you intend to import rules.

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

In the group file, there is one record for each function or responsibility in each group, and records alternate among groups: The first entity in the first group is followed by the first entity in the second group, and so on until the first entity in every group is recorded. Next comes the second entity in the first group, the second entity in the second group, and so on. A record in the group file comprises the following fields:

- **Group Name.**
- **Group Description.**
- **Entity Type:** The value *1* represents function and *2* represents responsibility.

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

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

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

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

- Rule Name.
- Reason.
- Entity Type for the first of the two conflicting entities. The value *1* represents function and *2* represents responsibility.
- The application with which that first entity is associated (or, for a function, the value *No Associated Application*).
- The name of the first conflicting entity.
- For a function only, the internal Oracle name for the first conflicting function.
- Entity Type for the second of the two conflicting entities. The value *1* represents function and *2* represents responsibility.
- The application with which that second entity is associated (or, for a function, the value *No Associated Application*).
- The name of the second conflicting entity.
- For a function only, the internal Oracle name for the second conflicting function.
- Control Type: The value *1* represents Approval Required, *2* represents Prevent, and *3* represents Allow with Rules.
- Approver.
- The Effective To date for the rule, in the format *DD-Mon-YY*.
- Same OU: The value *Y* indicates that the rule applies only within individual operating units, and the value *N* indicates that the rule applies across operating units.
- Same SOB: The value *Y* indicates that the rule applies only within individual sets of books, and the value *N* indicates that the rule applies across sets of books.

- This field is always blank. (It's reserved for approval groups, a feature scheduled to be introduced in version 7.2. In this file, it's represented by a semicolon.)
- Priority.
- The value *Group*. This field is populated only for a rule that sets entity groups in conflict.
- The name of the entity group that contains the first conflicting function or responsibility. This field is populated only for a rule that sets entity groups in conflict.
- The name of the entity group that contains the second conflicting function or responsibility. This field is populated only for a rule that sets entity groups in conflict.
- A final three fields are always blank (and so are always represented by three semicolons).

For example, the following record would define a conflict between two functions — Suppliers (in the Payables application) and Receivables Activities (in the Receivables application). Each belongs to an entity group, and the conflict is one among several defined by a Prevent SOD rule — called Vend*Receive — that sets the two groups in conflict. The approver is a user whose ID is WSTEVENs. The rule priority is 3:

```
Vend*Receive;Vendor-selection functions should be separate from
receiving functions;1;Payables;Suppliers;AP_APXVDMVD;1;Receivables;
Receivables Activities;AR_ARXSUMRT;2;WSTEVENs;31-Dec-07;Y;Y;;3;
Group;Payables Functions Group;Receivables Functions Group;;;;
```

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

Access Monitoring

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

Because such access may introduce segregation-of-duties conflicts, requests must be approved; they are routed by ACTIVE Governance workflows to approvers, who receive and respond to them at the Task Inbox of the ACTIVE Governance Platform. A user is prevented from creating a request if workflows are configured so that he is an approver for the request.

Upon approval of a request, the user who receives temporary access also receives an email message informing him of the rights he has been newly assigned, the dates on which the assignment begins and ends, and his temporary logon ID. If access has been granted to an Oracle responsibility, the message also includes a logon password (which is generated by ACTIVE Access Governor); if access has been granted to database tables, the message directs the user to consult his database administrator for a logon password. The requester also receives a confirming email message. Once granted, access is continually audited, and an Access Monitoring User Activity Report presents the audit results (see page 67).

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

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

Preparing Tables for Auditing

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

Selecting Audit Tables and Columns

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

In it, select a table.

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

If a table is not yet audit-enabled:

- 1 In a blank row of the Tables block, select an application in the Application Name list of values (LOV).
- 2 The Table Name LOV can now display only tables that support the application you’ve chosen. Select one of them. Not only does the Table Name field display

your selection, but the Table Description field also displays the description configured for it.

The screenshot shows the 'Access Monitoring Content' window. The 'Tables' section lists four tables under the 'Payables' application: 'AP_BANK_ACCOUNTS_ALL' (Detailed bank account information), 'AP_BANK_ACCOUNT_USES_ALL' (Information about bank account use), 'AP_DISTRIBUTION_SETS_ALL' (Invoice Distribution Set definitions), and 'AP_DISTRIBUTION_SET_LINES_ALL' (Individual Distribution Set line definitions). The 'Columns' section lists columns for the selected table, including 'BANK_ACCOUNT_ID', 'BANK_ACCOUNT_ID', 'ACCOUNT_HOLDER_NAME', 'ACCOUNT_HOLDER_NAME_ALT', 'ACCOUNT_TYPE', 'AGENCY_LOCATION_CODE', 'BANK_ACCOUNT_NAME', and 'BANK_ACCOUNT_NAME'. Each column has a 'Primary Key' checkbox, a 'Translation Type' dropdown, a 'Lookup Table' dropdown, and a 'Lookup Column' dropdown. The 'BANK_ACCOUNT_ID' columns are marked as primary keys and use 'Table Lookup' with 'AP' as the lookup table and 'APXVDMVD' as the lookup column. The other columns use 'Table Lookup' with 'CM' as the lookup table and 'APXSUMBA' as the lookup column. The 'BANK_ACCOUNT_NAME' columns use 'No Lookup'.

- 3 Optionally, use the scroll bar located beneath the Table Description field to scroll to the right and enter values in additional fields:
 - Form Name: Enter the internal name for the form supported by the table you selected. (For example, *APXVDMVD* is the internal name for the Enter Vendors form.)
 - User Form Name: This field automatically displays the external name for the form whose internal name you selected. You cannot enter a value directly in this field.
 - Block Name: Enter the internal name for the block that both exists on the form you selected and is supported by the table you selected.

Next, choose the columns you want to audit.

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

The screenshot shows the 'Columns for Audit' window. It has a 'Select From Available Columns' dialog box. The 'Available Columns' list includes: ACTION, ACTIVITY_DATE, AP_ACCOUNTING_EVENTS, AP_AE_HEADERS, AP_AE_LINES, AP_BATCHES, AP_CHECKS, AP_CHRG_ALLOCATIONS, AP_ENCUMBRANCE_LINES, AP_HOLDS, AP_INVOICES, AP_INVOICE_DISTRIBUTIONS, AP_INVOICE_PAYMENTS, AP_INVOICE_PREPAYS, AP_MATCHED_RECT_ADJ, AP_MC_CHECKS, AP_MC_INVOICES, and AP_MC_INVOICE_DISTS. There are four buttons between the 'Available Columns' and 'Selected Columns' lists: a right arrow, a right arrow with a plus sign, a left arrow with a minus sign, and a left arrow. The 'Selected Columns' list is currently empty. A 'Done' button is at the bottom right.

- 2 Select the columns individually or collectively:
 - In the Available Columns box, click on the name of a column you want to audit. Then click on the right-pointing single-arrow button to move it to the Selected Columns box. Repeat for each column you want.
 - Alternatively, click on the right-pointing double-arrow button to move all columns to the Selected Columns box.
 - If you reconsider, you can click on a column name in the Selected Columns box, then click on the left-pointing single-arrow button to move it back to the Available Columns box. Or, click on the left-pointing double-arrow button to move all columns back to the Available Columns box.
- 3 When you are satisfied with your selection, click on the Done button. For each column you selected, a row appears in the Columns block of the Access Monitoring Content form. The Column Name field shows the internal name, and the User Column Name field shows the external name, for the column. If the column is a primary key, the Primary Key check box is selected.

Setting Up Translations

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

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

The screenshot shows the 'Access Monitoring Content' window. It contains two main sections: 'Tables' and 'Columns'.

Tables Section:

Application Name	Table Name	Table Description
General Ledger	GL_JE_BATCHES	Journal entry batches

There is an 'Import Columns' button on the right.

Columns Section:

Column Name	User Column Name	Primary Key	Translation Type	Lookup Table	Lookup Column
JE_BATCH_ID	JE_BATCH_ID	<input checked="" type="checkbox"/>	No Lookup		
CREATED_BY	CREATED_BY	<input type="checkbox"/>	Table Lookup	FND_USER	USER_NAME
		<input type="checkbox"/>			
		<input type="checkbox"/>			
		<input type="checkbox"/>			
		<input type="checkbox"/>			
		<input type="checkbox"/>			

Translation Configuration Section:

Type	Audit Table Column	Translation Table Column
Column	CREATED_BY	USER_ID

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

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

To set up this linkage:

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

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

Saving Your Work

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

Creating Database IDs

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

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

Displaying a List of Access Requests

When you start Access Monitoring, a Request Access List panel displays summary descriptions of all requests that have ever been made. Each entry includes the name and temporary ID of the user for whom access was requested, as well as the type of access — “E-Business User” is a request for access to an Oracle responsibility, and “DB User” is a request for access to database tables. It presents number values for a task ID and for user tasks — the former is the ID of the workflow that distributed the request for approval, and the latter is both the ID of a step in that workflow and the ID of the request in the approver’s Task Inbox. The panel further presents the date on which the request was made, as well as the dates on which the user’s access is proposed to start and end. Finally, it displays the status of the request — Pending, Approved, or Rejected.

Name	Task ID	Request	Request Type	Request for User ID	Status	User Tasks	Start	End
Thia, Anand	131	07-Jun-2006 03:13 PM	E-Business User	LAAG28	Approved	128	07-Jun-2006 03:13 PM	09-Jun-2006 03:14 PM
Wasser, Newberry	119	07-Jun-2006 11:00 AM	E-Business User	LAAG4	Approved	116	07-Jun-2006 11:00 AM	30-Jun-2006 11:00 AM
Tress, Andy	3	06-Jun-2006 06:39 PM	E-Business User	LAAG2	Approved	3	06-Jun-2006 06:39 PM	09-Jun-2006 06:49 PM
lastname_user2	2	06-Jun-2006 04:44 PM	DB User	LAAGDB1	Approved	2	06-Jun-2006 04:44 PM	07-Jun-2006 04:45 PM
lehdnran, sushama	1	06-Jun-2006 04:23 PM	E-Business User	LAAG1	Approved	1	06-Jun-2006 04:23 PM	07-Jun-2006 04:24 PM

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

Creating a New Request

To create a new access request, click on either of two buttons labeled Add Request. One button is located at the top right, and the other at the bottom center, of the List panel. A Request Access panel appears (as shown at the top of the next page).

Starting the Request

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

- 1 Your request applies automatically to the database instance to which you are logged on, and the System field displays the name of the instance. You cannot change this field value directly. If you want to request access to another database instance, use the Change link (at the upper right of the panel) to log on to that instance.
- 2 In the First Name and Last Name fields, enter the given name and surname of the user for whom you are requesting access.

- 3 In the Email field, enter the email address of the user for whom you are requesting access. This is the address at which the user is notified of his new access rights, logon ID, and password. (Your own confirming email message goes to the address configured for you in the Add User panel of the ACTIVE Governance Platform.)
- 4 The Support Ticket # field is for use if you are requesting access in response to a notification from an issue-tracking system. If so, enter the number assigned to the issue in the tracking system. (Any format is acceptable.) If not, leave the field blank.
- 5 The Start field is set to the date and time at which you create the access request, and the End field is blank. If you want the user to receive access immediately upon approval of the request, retain the default Start value; otherwise, specify a later date and time. Since the access you are requesting is necessarily temporary, you must select an End date and time.

You can insert a date and time manually in either field (use the format *DD-Mon-YYYY Hr:Mn:Sc*). Alternatively, you can click on the icon next to either field, and a pop-up calendar appears. In it, click on the < or > symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want. The pop-up window closes, and the date you selected appears in the field, together with the time of day at the moment you select the date. You can edit the time.

- 6 If you want to request access to database tables, click on the Database Access radio button. If you want to request access to an Oracle responsibility, click on the Oracle E-Business Suite radio button.

Requesting Database-Table Access

If you selected the Database Access radio button as you started the request, the LAAG User field displays logon IDs your DBA has created for database access; the Available Tables, Selected Tables, and Table Grant fields are active; and the Responsibility field is inactive. Complete the following steps:

- 1** Select one of the available database user IDs in the LAAG User field.
- 2** Select tables by moving them from the Available Tables field to the Selected Tables field:
 - Highlight tables you intend to select. Click on a table to highlight it. Or, to highlight a continuous group of tables, click on the first one, hold down the Shift key, and click on the last one. To highlight a discontinuous group, hold the Ctrl key as you click on tables.
 - Click on the > button to move highlighted tables from the Available field to the Selected field. Or, click on the >> button to send all values in the Available field (regardless of whether you've highlighted them first) to the Selected field.
 - If you reconsider, click on the < button to return highlighted values from the Selected field to the Available field. Or, click on the << button to return all values in the Selected field to the Available field.
- 3** Select the access privileges you want to request for the user. Highlight (click on) a table in the Selected Tables field. Then select any combination of the three privileges — Insert, Update, and Delete — listed in the Table Grant field. (As before, you can use the Shift or Ctrl key, together with the mouse, to select more than one.) Repeat this process for each table you've placed in the Selected Tables field. (ACTIVE Governance remembers the rights you choose for each table even as you highlight others to set their rights; you don't need to save each selection of rights individually.)

Requesting Responsibility Access

If you selected the Oracle E-Business Suite radio button as you started the request, the LAAG User field displays logon IDs provided by LogicalApps for responsibility access; the Responsibility field becomes active; and the Available Tables, Selected Tables, and Table Grant fields become inactive. Complete the following steps:

- 1** Select one of the available responsibility user IDs in the LAAG User field.
- 2** Select the responsibility you want to assign to the user in the Responsibility list of values. (You can select only one responsibility per request.)

Completing the Request

When you have defined the database or responsibility access you want to request for the user, complete these final steps:

- 1** In the Reason field, tell why the user should be given the access you requested.

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

Viewing Requests

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

- 1 Specify filtering criteria by entering complementary values in any combination of the fields that run horizontally above the list of requests:
 - Name: Enter the first or last name of a user for whom access has been requested to see entries pertaining to that user, or enter a text fragment to see entries that apply to all users whose names contain the fragment.
 - Task ID: Enter a full task ID to see the request corresponding to that ID. (This is the identifier for the workflow that distributed the request for approval. It corresponds to the Task ID column, and not to the User Tasks column, in the grid that lists requests.)
 - Request: Enter a date to see all requests created on that date.
 - Request Type: Select the value *E-Business* to see requests for responsibility access, *DB User* to see requests for database-table access, or *All* to see all requests. (Do not select the value *Execute SQL*.)
 - User ID: Enter one of the temporary responsibility or database-table logon IDs to see requests assigning that ID to a user. (Responsibility-access request IDs use the format *LAAGx*, where *x* is a number; database-table-access requests start with *LAAG*, but otherwise follow a format specified at your site.)
 - Status: Select a status to see requests at that status, or *All* to see requests at all statuses. Options include *Approved* (requests that have been approved), *Rejected* (requests that have been rejected), *Pending* (requests for which no approval decision has yet been made), and *Failed* (requests that have been approved, but for which some processing error has occurred).
 - Start: Enter a date to see all requests for which this is the proposed start date.
 - End: Enter a date to see all requests for which this is the proposed end date.

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

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

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

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

LogicalApps | ACTIVE Governance Tasks (0) | Profile | Sign Out | Help
 Welcome, Muzio Clementi

Home | Control Library | Control Automation | Segregation of Duties | **Access Monitoring** | Reporting | Administration

Database Instance: Squaw [Change](#)

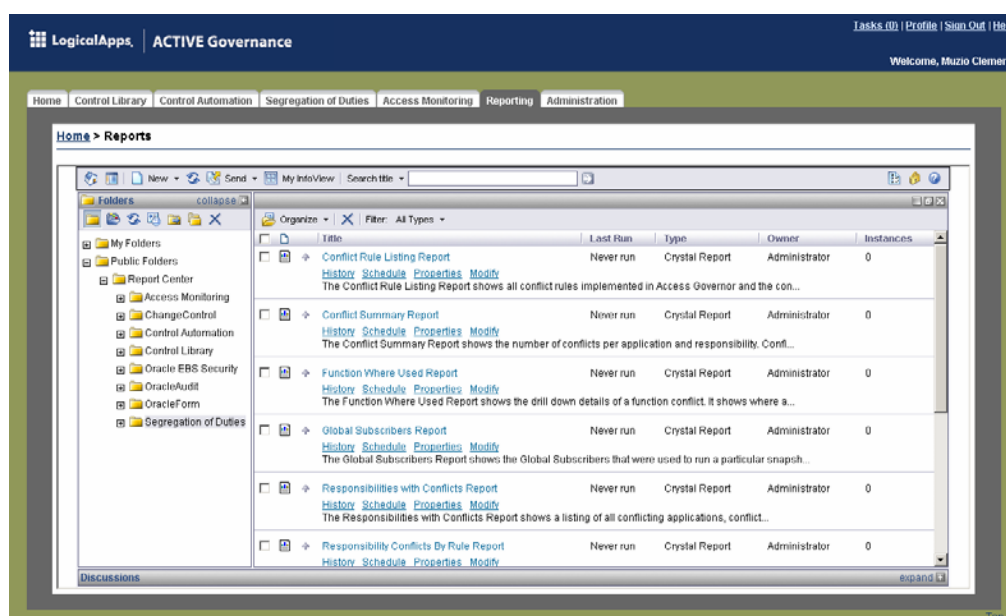
[Home](#) > [Request Access List](#) > **View Request Access**

System	SQUAW	Support Ticket #	
First Name	Wallace	Start	16-Jun-2006 03:41 PM
Last Name	Stevens	End	20-Jun-2006 03:41 PM
Email	asdfasdf@asdfasdf.com	Status	Approved
LAAG User	LAAG8		
Access Type	E-Business User		
Reason	Fill in for vacationing employee		

Top

Reports

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



A Folders area to the left of the Reports panel presents a hierarchical display of available reports and the folders that contain them. In it, click on Public Folders, and

then Report Center. The panel presents a selection of folders, three of which pertain to ACTIVE Access Governor: Segregation of Duties, Access Monitoring, and Oracle EBS Security. Click on one of them and, in the larger panel on the right, click on the link for the report you want. The panel then displays fields in which you can enter values for report parameters; do so, then click on the OK button to run the report.

Segregation of Duties Folder

The Segregation of Duties folder contains the following reports. In addition to parameters listed in the report descriptions, reports commonly accept the following two parameters:

- **AppsRules 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, select values for the following parameters:

- **Application:** Select one or more applications to view conflicts associated with those applications. Or select *All* to view conflicts associated with all applications.
- **Conflict:** Select one or more SOD rules to view information on the resolution of conflicts generated by those rules. Or select *All* to see information on the resolution of conflicts generated by all rules.
- **User 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.
- **Control Type:** Select a control type — Approval Required, Allow 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.
- **Snapshot Run Date:** Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.

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

Conflict Summary Report

The Conflict Summary Report lists responsibilities within each application, then shows the number of Allow with Rules, Prevent, Approved, Rejected, and Pending conflicts, and the total of those five counts, at each responsibility.

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

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

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

- **Application:** Select one or more applications to view summary values for conflicts associated with those applications. Or, select *All* to view summary values for conflicts associated with all applications.
- **Snapshot Run Date:** Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.

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, select values for the following parameters:

- **Application:** Select one or more applications to view responsibilities that have conflicts associated with those applications. Or select *All* to view responsibilities that have conflicts associated with all applications.
- **Responsibility:** Select a responsibility to view only conflicts for that responsibility. Or select *All* to view conflicts for all responsibilities.
- **Function:** Select one or more functions to view only conflicts involving those functions. Or select *All* to view conflicts involving all functions.
- **Snapshot Run Date:** Select a snapshot date to view summary values for conflicts generated in that snapshot. This parameter is required.

- **Control Type:** Select a control type — Approval Required, Allow 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 *Yes* to view information on conflicts between functions within a responsibility, or *No* to view information on conflicts between entities across responsibilities.

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

Function Where Used Report

The Function 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, select values for the following parameters:

- **Function Type Conflicts:** 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.
- **Users:** 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 Report

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

- **Applications:** 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:

- **Application:** Select one or more applications to view rules involving those applications, or select All to view rules involving all applications.
- **Conflict:** Select one or more rules to view information about those rules. Or select All to see information about all rules.
- **Entity Type:** Select Function or Responsibility to view rules that find conflicts in one entity or the other, or Both to see both types of rule.
- **Control Type:** Select a control type — Approval Required, Allow with Rules, or Prevent — to view only information on rules involving that type. Or accept All to see information on rules involving all types.
- **Same OU:** Select 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.

- **Active 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.

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, select values for the following parameters:

- **Application:** Select one or more applications to view results for those applications, or select *All* to view results for all applications.
- **Approved By:** Select one or more 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.

Conflicts by Responsibility or Application Report

The Conflicts by Responsibility or Application Report devotes a section to each responsibility or application (depending on how one chooses to focus the report). For each responsibility or application, it lists the SOD rules that have generated conflicts; for each rule, it displays the number of conflicts generated within the responsibility or application, as well as the entity, application, conflicting entity, and conflicting application specified in the rule. (The entity is the first of two functions or responsibilities that the rule defines as conflicting; the application is the application to which that entity belongs; the conflicting entity is the second of two functions or responsibilities that the rule defines as conflicting; and the conflicting application is the application to which the conflicting entity belongs.) As you generate the report, select a value for the *View By* parameter: *Application* or *Responsibility* to have the report group conflicts by one or the other.

Simulation Remediation History Report

The Simulation Remediation History Report displays simulation rules that have been used to remediate user conflicts. For a remediation operation, the report shows the name of the user who submitted the rules, the date and time on which the operation took place, and the rules. For each rule, it shows the action, entity type, entity type from, and entity elements of the rule. As you generate the report, select values for the following parameters:

- **Simulation Date:** Select the date on which the remediation operation took place.
- **Action:** Select any combination of simulation/remediation actions that may be configured: *Exclude*, *Remove*, or *Insert* to have the report show only rules configured to perform those actions.
- **User:** Select the name of the user who performed a remediation operation.

Global Subscribers Report

The Global Subscribers Report displays settings for all global subscribers that have been configured. It displays headings for all possible subscriber types, even if no subscribers have been configured for a given type. As you generate the report you must select a Snapshot Run Date parameter: select the date of a user-conflict snapshot to view subscribers configured at the moment that snapshot was generated.

User Conflicts Master CSV Report

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

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

- Application: Specify one or more applications to select SOD rules 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.

Oracle EBS Security Folder

The Oracle EBS Security Folder contains the following reports.



Note

To ensure that the Oracle EBS Security reports present current information, run the LAA Populate User Access Data Table background program before running any of the reports. (See page 42.)

Oracle EBS User Details Report

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

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

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

- **User:** Select one or more users about whom you want information. For each, type the user's Oracle username in the Enter a Value field, and then click on the > button.

You can instead accept the default selection, All. Be aware, however, that the report provides copious information about each user, and so the All selection may impact performance. To nullify the default selection, click on All in the Selected Values field and then click on the Remove button.

- **Grant:** Choose *Y* (for yes) to have the report list only submenus and functions for which the Grant check box is selected in the Oracle Applications Menus form. Or select *N* (for no) to list submenus and functions for which the grant flag is cleared.
- **View Only:** Select *Y* to have the report list functions to which a user has read-only access (or, more technically, the query-only parameter is set to *Yes* in the Oracle Applications Form Functions form). Or Select *N* to have the report list functions that enable a user both to view and modify data (functions for which the query-only parameter is not set).
- **Prompt:** Choose Not Null to have the report list submenus and functions a given user is able to select, because higher-level menus present prompts for them.

(More technically, the report would provide information about a submenu or function if, in the Oracle Applications Menus form, a row adds it to a menu accessible from one of the user's responsibilities, and the row includes a value in the Prompt field.)

Choose Null to have the report list submenus or functions for which higher-level menus do not display prompts, and which a user therefore cannot select. (In this case, in the Menus-form row that adds a submenu or function to a menu, no value is entered in the Prompt field.)

Or choose Both to have the report list submenus or functions regardless of whether higher-level menus present prompts for them.

- **Active Users:** Choose whether the report should present information about active users, inactive users, or both. A user is considered to be active if his Effective To date, as configured in the Oracle Applications Users form, has not passed. He is inactive if the date has passed.

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

- **Active Responsibilities:** Choose whether the report should present, for each user, information about active responsibilities (and the menus and functions available from them), inactive responsibilities, or both. A responsibility is considered to be active for a given user if two dates have not yet passed: the Effective To date configured for the responsibility on the Oracle Applications Responsibilities form, and the Effective To date for the assignment of that responsibility to the user on the Oracle Applications Users form. A responsibility is inactive if either of those dates has passed.
- **AppsRules Source Data:** Select the database instance that contains the data about which you want to generate a report.

Oracle EBS Function Details Report

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

- The responsibilities from which the function is accessible, together with the start and end dates for each responsibility.
- The users whose responsibility assignments give them access to the function. The report also shows each user's start and end dates.
- The root menu associated with each responsibility. The report shows both user name (the one displayed to an Oracle Applications user) and internal name for each menu.

- The menus available for selection under those roots. The report shows the user and internal names for each menu, as well as its prompt (the label that identifies it for selection on other menus). The report also indicates whether its grant-flag value is set to *Y* (for yes) or *N* (for no).

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

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

The remaining parameters — Grant, View Only, Prompt, Active Users, Active Responsibilities, and AppsRules Source Data — take the same values (and filter report results in the same way) as they do for the Oracle EBS User Details Report.

Oracle EBS Responsibility Details Report

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

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

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

- **Responsibility Name:** Choose one or more responsibilities, or the value *All*.
- **Active Responsibilities:** Choose whether the report should present information about active responsibilities, inactive responsibilities, or both. A responsibility is considered to be active if the Effective To date configured for the responsibility on the Oracle Applications Responsibilities form has not passed.

The remaining parameters — Grant, View Only, Prompt, Active Users, and AppsRules Source Data — take the same values (and filter report results in the same way) as they do for the Oracle EBS User Details Report.

Access Monitoring Folder

The Access Monitoring folder contains a single report.

Access Monitoring User Activity Report

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

- **AppsRules Source Data:** Select the instance that contains the data about which you want to generate reports. (Supply this value twice, first to generate a list of the remaining parameters and second, within that list, to generate the report itself.)
- **User Type:** Select the value *Database User* to view results for users granted direct access to database tables, *Ebiz User* to view results for users granted access to Oracle responsibilities, or both.
- **User — Access Time:** Select the users whose transactions you want to review. For each, the parameter field lists the user’s name and the dates and times on which her access begins and ends (so that you can distinguish among multiple access sessions granted to a given user).
- **Action Type:** Select any combination of three transaction types to review: INSERT, UPDATE, or DELETE.
- **Transaction Date Range:** Define a period in which transactions must have occurred to be included in the report. You may enter dates and times in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the start date and select the No Lower Value check box to start with the earliest existing transaction, or omit the end date and select the No Upper Value check box to finish with the latest existing transaction.

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

You can click on the calendar icons to select dates. If you do, each date you select is automatically accompanied by the time 00:00:00. You can then edit this time. Or, for an end value, you may target all of a day’s transactions by selecting the next day’s date and retaining the 00:00:00 time value.

