Oracle® Application Access Controls Governor

User Guide

Release 8.5

Part No. E25640-01

October 2009

ORACLE

Oracle Application Access Controls Governor User Guide

Part No. E25640-01

Primary Author: David Christie

Contents

4 Reporting

1

Introduction

Application Access Controls Governor (AACG) regulates access to duties assigned in business-management applications. By default it controls access to Oracle E-Business Suite and PeopleSoft Enterprise, and it may be configured to work with other business-management applications as well. It implements "access policies," which identify duties that are considered to conflict with one another because, in combination, they would enable individual users to complete transactions that may expose a company to risk.

AACG runs in a Governance, Risk and Compliance Controls (GRCC) platform. So does a second application, Transaction Controls Governor (TCG). The GRCC platform offers administrative and other functionality shared by AACG and TCG. Administrative features include tools to connect GRCC to Oracle, PeopleSoft, and other business-management-application data sources (instances), and to refresh "snapshots" of data gathered from those applications; to create GRCC users and user roles; and to set GRCC parameters, connect with your email server (for the purpose of sending notifications to GRCC users), and integrate GRCC with other applications. Moreover, the GRCC platform can display information in any of eleven languages.

These shared administrative and language capabilities are documented in detail in a distinct *Governance, Risk and Compliance Controls User Guide*. The *Application Access Controls Governor User Guide* focuses on the creation of AACG access policies, and analysis of the conflicts they generate.

Access Policies

An access policy defines conflicts among a selection of "access points" to an organization's systems. In broad terms, an access point is an object in a business-management application which, when made available to a user, enables him to do something. Access points may be gathered into "entitlements," and AACG policies may use entitlements in place of, or in addition to, access points.

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

An access policy may contain any number of access points, but it also directs the AACG "engine" to evaluate them in distinct combinations. (For example, a policy may contain four access points, but consider them to be distinct pairs, in each of

which one access point conflicts with another.) Each distinct combination of conflicting access points is considered to be a "subpolicy."

Moreover, AACG recognizes "paths" to conflicting access points. Each path consists of a "privilege" (an access point actually included in an access policy, such as an Oracle function), a "role" (the level of object that's actually assigned to a user, such as an Oracle responsibility), and objects that lead from one to the other (such as the menus and submenus that lead from a responsibility to a function).

Each access policy conforms to one of three "policy types" — Prevent, Monitor, or Approval Required. These determine the actions to be taken when a business-management-application user is assigned duties that a policy defines as conflicting:

- A Prevent policy should deny access to conflicting access points. All paths to such a conflict are assigned a Prevent status, and this status cannot be changed.
- A Monitor policy permits access to conflicting access points. Paths to conflicts generated by a Monitor policy are initially set to a Monitor status, indicating that the access should be re-examined periodically. Analysts can update the status to Approved (the user retains access granted by that path, and it need not be re-examined) or Rejected (the user must not have the access granted by that path). Typically, the ultimate choice for a policy of this type is Approved or Rejected.
- An Approval Required policy allows a user to work at conflicting access points only upon approval by a reviewer designated by the policy. Paths to conflicts generated by an Approval Required policy are initially set to a Pending status, and analysts may reset the status to Approved or Rejected.

In addition, each access policy must name at least one "participant," and may also specify "conditions" and "dimensions":

- Participants are AACG users who are assigned to access policies, either as individuals or as members of participant groups. One participant (either an individual or a group) is charged with resolving conflicts generated by the policy; others observe the decisions made by those who are entitled to act.
- Conditions specify users or other objects, such as companies in PeopleSoft or operating units in Oracle EBS, that are exempt from the policy. Or, they specify circumstances under which the policy is enforced.
- A dimension is, in effect, a category of values. One can define dimensions, then define values for them, and then assign dimension values to access policies or to entitlements. One can then sort displays of entitlements, policies, and the conflicts they generate by dimension value. (For example, one might create a Region dimension, and then create values for it, such as North, South, East, and West. Individual policies or entitlements that apply to a particular region would then be given its dimension value.)

Conflict Analysis

Once policies are defined, an AACG user runs a Find Conflicts program, which may be applied to selected policies or to all policies. It evaluates business-management-application users, noting those whose work assignments violate policies, and displays the results.

When the assignment of duties to one user violates one access policy, this is considered to be one conflict, no matter how many subpolicies the assignment may violate, or how many paths it may involve. Even so, a user may have any number of paths to one (or another) of the conflicting access points in a given policy or subpolicy, and so AACG reports results at the path level. Policy participants can assign status to individual paths leading to conflicts. Thus, participants may be able to resolve a user's conflict by shutting off access to one path, or a few, while permitting access to many others.

Several AACG conflict-analysis tools identify conflicts, and enable users to assign status to their paths, but do not resolve them in the business-management system. Analysts who use these tools would undertake "cleanup" — implement the statuses assigned in AACG by making adjustments in the business-management application. In Oracle, for example, an administrator might end-date the assignment of a responsibility to a user, or exclude a function from a responsibility in which it conflicts with another function.

These AACG tools include the following:

- A Heat Map enables analysts to select parameters that divide conflicts into increasingly narrowly focused sets. Through its use, analysts can evaluate trends in the generation of conflicts and prioritize their resolution.
- A Definition page (in which one creates access policies) can display the conflicts generated by individual policies.
- A Conflict Analysis page displays a "subpolicy-level" view of conflicts generated by all policies. That is, it sorts by specific combinations of access points within a policy that have produced conflict paths.
- A Work Queue enables users to assign status to conflict paths, although this status assignment is purely documentary. Conflicts need to be cleaned up in the business-management system.
- A Simulation feature enables AACG users to forecast the effects of cleanup in the business-management application.

Moreover, when a user is assigned duties after an AACG policy has been created to define them as conflicting, AACG can automatically enforce that policy — a feature known as "User Provisioning." AACG disallows roles if their assignment to a user violates a Prevent policy, or allows them if the assignment triggers a Monitor policy. When an assignment violates an Approval Required policy, AACG notifies approvers via email, and presents the assignment for review in a User Provisioning Requests page.

Starting Application Access Controls Governor

To start Application Access Controls Governor:

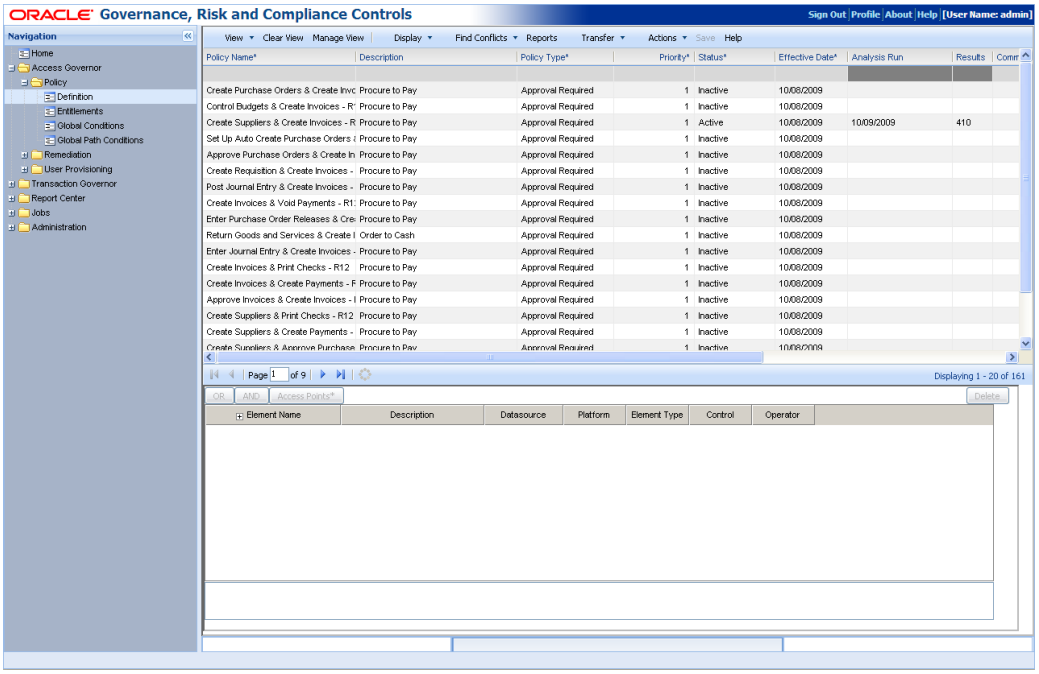
1. Open a web browser.
2. In the Address field, type the URL for your instance of Governance, Risk and Compliance Controls, and press the Enter key.

3. A Login dialog box appears. Type your user name and password in the appropriate fields, optionally, select a language in which to work in the Language Preference list box, and click on the Login button.

   You can leave the Language Preference field blank. If so, GRCC selects (in order of preference) the language specified in your user profile, the language of your web browser, or US English.

Using the Navigation Panel

The left column of the GRCC GUI is a Navigation panel. To its right, a larger frame initially displays a Home page, but then presents items you select in the Navigation panel. The illustration below shows the page in which users define access policies.



Of the top-level nodes in the Navigation panel, Access Governor and Report Center present links to features that are the focus of this *User Guide*.

See the *Transaction Controls Governor User Guide* for information on features available from the Transaction Governor node, or the *Governance, Risk and Compliance Controls User Guide* for information on features available from the other nodes.

The Access Governor node offers links to pages in which users can define AACG access policies and dimensions, gather access points into entitlements, and create "global conditions" and "global path conditions" (which focus the effect of access policies). They can also find and display conflicts, use the Heat Map, simulate the effects of actions intended to resolve conflicts, assign status in the Work Queue, and view reports. Moreover, they can employ User Provisioning to approve or reject assignments of duties that violate Approval Required access policies, and create participant groups.

The Report Center node offers links to reports about the configuration of access policies, the generation of conflicts, the simulation of conflict resolutions, and AACG User Provisioning.

When you select a high-level link, it opens a list of subordinate links. Some of these display a box containing a symbol that toggles between a plus sign and a minus sign. These entries provide a path to lower-level entries, but do not themselves open pages in which you can work. Click on a plus sign to reveal lower-level entries; click on a minus sign to hide the lower-level entries from view. When you reach an entry with no plus or minus sign, click on the entry to open pages in the frame to the right.

To expand the Navigation panel, position the mouse cursor over its right border, hold down the left mouse button, and drag the border to the right. Having done so, you can drag the border to the left, causing the panel to contract up to its original size. To close the Navigation panel entirely (and so expand the frame in which you will be working), click on the button with the << symbol, located at the top right of the Navigation panel. The button then changes to display a >> symbol; click on it to reopen the Navigation panel.

Creating Views

In lists — such as the upper grid in each of the pages in which AACG policies and entitlements are defined, or the Conflict Analysis page — you can limit the display of entries to those that satisfy filtering criteria, and you can sort the entries. You can also remove columns from display, or restore them; rearrange the order in which columns appear; and resize them. You can then save your selections as a "view," and then either select your view for display or cause it to be displayed by default.

Filtering Data

To filter the values displayed in a list:

1. Determine where to enter filtering criteria. In some lists, you do so in text boxes that appear directly below column headings. Some lists omit these text boxes; in these, you enter filtering criteria in the first row of the list.
2. In any combination of columns in the view row or text boxes, enter (or select) values appropriate to the columns.

3. Click on the View button in the tool bar above the list. The list then contains only entries that match the values you've entered.

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

Sorting Data

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

Removing and Restoring Columns

To remove columns from display, or to restore them:

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

Rearranging Columns

To rearrange the order in which columns appear:

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

Resizing Columns

To alter the width of columns in lists:

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

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

Saving or Deleting a View

In most cases, there is a Manage View button. If so, you can save the view you define. To do so:

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

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

Displaying a View

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

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

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

2

Creating Access Policies

An access policy may define conflicts among any number of access points or entitlements. A single policy may mix differing access-point types — for example, it may include both Oracle functions and responsibilities. It may include access points from more than one business-management system, for example defining equivalent conflicts in Oracle E-Business Suite and PeopleSoft Enterprise. It may include both access points and entitlements.

It does so by joining access points or entitlements, or groups of them, into AND or OR relationships with one another.

- When items are joined by an AND "operator," all must be true for a conflict to exist. For example, if an access policy joins functions "f1" and "f2" with an AND operator, a conflict occurs only if a responsibility assignment grants a user access to both f1 and f2.
- When items are joined by an OR operator, only one need be true for a conflict to exist. For example, if an access policy joins f1 and f2 with an OR operator, a conflict occurs if a responsibility assignment grants a user access to f1 or f2 or both.

Some Policy Examples

The simplest access policy might select two access points — say, two PeopleSoft page definitions — and join them with an AND operator. Users assigned both those definitions would be in conflict, but a user assigned only one or the other would not.

However, access policies may be more complex. For example, suppose that two functions (f1 and f2) represent duties that should not be assigned to an individual user in the Oracle E-Business Suite, and two page definitions (pd1 and pd2) would grant access to similar duties in PeopleSoft. Suppose further that an organization implements both Oracle EBS and PeopleSoft. An access policy may then say that a conflict exists when a user has either pair of access points: (f1 and f2) or (pd1 and pd2).

Application Access Controls Governor represents such relationships in a hierarchical structure: "parent" objects exercise authority over "child" objects. For example, the access policy involving the Oracle functions and PeopleSoft page definitions would look like the one shown at the top of the next page.

```
OR
  AND
    f1
    f2
  AND
    pd1
    pd2
```

An operator applies to its immediate children — objects beneath, and indented one level to the right, of it. Moreover an operator may be both a parent of objects below it and a child of an operator above it. Thus, in the example above, each AND operator applies to the access points beneath it — in one case the two functions and in the other the two page definitions. The OR operator applies to the two AND relationships. So if a user has either both functions or both page definitions, a conflict occurs. However, if he has one Oracle function but not the other, and one PeopleSoft page definition but not the other, there is no conflict.

In AACG, an access point is specific to the instance in which it runs. So when there is more than one instance of a business-management system, an access policy may repeat a conflict definition for each instance, and the result would look quite like the previous example. Suppose, for instance, that functions f1 and f2 are in conflict, but an organization has two Oracle instances ("ora1" and "ora2"). The access policy defining the conflict in both instances might look like this:

```
OR
  AND
    f1 on ora1
    f2 on ora1
  AND
    f1 on ora2
    f2 on ora2
```

If a user has both functions in either instance (or both instances), a conflict occurs. However, if he has one function but not the other in each instance (say, f1 in ora1 and f2 in ora2), there is no conflict.

Some other common constructions follow. First, an access policy might list a selection of access points, all of which a user must have for a conflict to occur:

```
AND
  AccPt1
  AccPt2
  AccPt3
  AccPtx
```

If these were entitlements rather than access points, a user would need to have at least one access point contained in each entitlement for a conflict to occur.

Second, an access policy might define a conflict between any point in one set of access points, and all points in a second set: (AccPt1 or AccPt2) and (AccPt3 and AccPt4). When configured in AACG, the policy would look like this:

```
AND
  OR
    AccPt1
    AccPt2
  AND
    AccPt3
    AccPt4
```

In this case, the purpose of the higher-level AND is to join (AccPt1 or AccPt2) in an AND relationship with (AccPt3 and AccPt4). This defines three conflicts — access points 1, 3, and 4; access points 2, 3, and 4; and access points 1, 2, 3, and 4.

Next, an access policy might define a conflict between one access point (or entitlement) and any of two (or more) others: AccPt1 and (AccPt2 or AccPt3 or AccPt*x*). When configured in AACG, the policy would look like this:

```
AND
  AND
    AccPt1
  OR
    AccPt2
    AccPt3
    AccPtx
```

In this case, the OR operator indicates that the user must have access point 2, 3, or *x*, or any combination of them. The higher-level AND operator indicates that the user must also have the item — access point 1 — contained within the lower-level AND operator. Thus access points 1 and any combination of the remainder — for example 1 and 2, 1 and 3, or 1 and 2 and 3 — would result in a conflict. The lower-level AND is something of a special case; it exists only because something must exist at the second level of the hierarchical structure to correspond to the OR operator.

An access policy may define a conflict between two items, either of which is one of any number of items: (AccPt1 or AccPt2 or AccPt*x*) and (AccPt3 or AccPt4 or AccPt*y*).When configured in AACG, the policy would look like this:

```
AND
  OR
    AccPt1
    AccPt2
    AccPtx
  OR
    AccPt3
    AccPt4
    AccPty
```

In this case, however, you could create two entitlements, one consisting of AccPt1, AccPt2, and AccPt*x*, and the other of AccPt3, AccPt4, and AccPt*y*. You would then create an access policy that joins the two entitlements in an AND relationship.

You may choose to create a "sensitive access" policy — one that sets an access point in conflict with itself, because that access point provides so much authority that any user should require approval before being granted access to it. An example might be the Purchasing Super User responsibility in Oracle EBS. To create such a policy, you select the access point only once, and make it subject to either the AND or OR operator. For example, the following sets responsibility "r1" in conflict with itself:

```
OR
  r1
```

If there are several such access points, you have several options. You can create a distinct policy for each. You can include all in a single policy, subject to a single OR operator. Or you can include all in an entitlement, and create a policy in which the entitlement is set in conflict with itself:

```
OR
  ent1
```

You can create more complex structures, but it is incumbent on you to make sure your access policies make logical sense. For example, the following structure could generate a conflict if a user were assigned a single access point — AccPt1 or AccPt2 — but the presence of AccPt3 and AccPt4 in the policy suggests that this is probably not its author's intention. One possible correction would be to replace the higher-level OR with AND.

```
OR
  OR
    AccPt1
    AccPt2
  AND
    AccPt3
    AccPt4
```

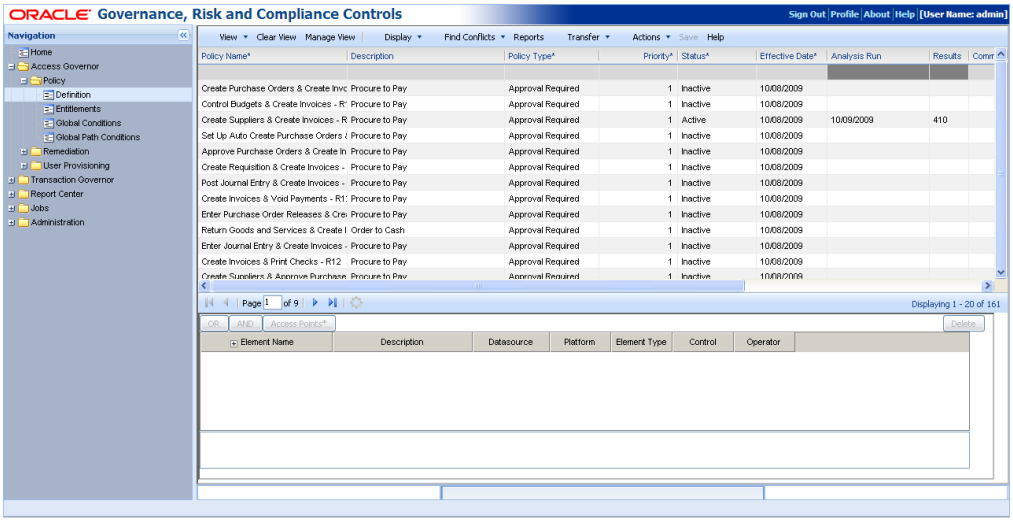
Or, an access policy could define the relationship (AccPt1 and AccPt2) and (AccPt3 and AccPt4), which would look like the structure on the left, below. But this is needlessly complex, because the simpler AccPt1 and AccPt2 and AccPt3 and AccPt4 (on the right, below) would be evaluated in the same way.

```
AND                          AND
  AND                          AccPt1
    AccPt1                     AccPt2
    AccPt2                     AccPt3
  AND                          AccPt4
    AccPt3
    AccPt4
```

For one additional example, see page 2-24.

Opening the Definition Page

To create or edit access policies, select Access Governor in the Navigation panel. Click on the plus sign next to the Policy node, which reveals lower-level nodes. Of them, click on Definition. This opens a Definition page, which is in two parts: A grid occupies the upper half of the page and lists existing policies. A "Policy Details" area occupies the lower half; it provides tools for adding access points or entitlements to a policy selected in the upper grid, and for defining the relationships among them.



Adding an Access Policy

To create a new access policy, begin by naming it, selecting its policy type, and setting a few other values:

1. Click on the Actions button in the tool bar near the top of the Definition page. This activates an Actions menu; in it select Add. A new row appears in the grid, second from the top (immediately beneath the view row).
2. Insert the following values in the new row. To do so, double-click in each field, or press the Tab key to move from an active field to the next field.
   - Policy Name: Type a name for the new policy.
   - Description: Briefly explain the business risk addressed by this policy.
   - Policy Type: From a list box, select the policy type you want to assign to the policy. (For type definitions, see page 1-2.)
   - Priority: Enter a value that expresses the importance of this policy in relation to others. The value must be a number. (Your company should establish a set of priority values and enforce consistent usage.)
   - Status: From a list box, select a status. "Active" permits the policy to be enforced, providing that its effective date, set in the next field, has arrived. "Inactive" prevents the policy from being enforced, regardless of its effective date.
   - Effective Date: Select a date on which AACG can begin to enforce the policy. (For enforcement to occur, the status must also be set to Active.) Accept the default value (the current date) or double-click in the Effective Date column, and then click on the grid-like icon it presents. A pop-up calendar appears. In it, click on the left- or right-pointing symbol surrounding the month and year to display an earlier or later month. Or, click on the downward-pointing symbol to produce a list of months in the current year, and click on the one you want. Then, in the calendar, click on the date you want. Alternatively, click on the Today button to select the current date.
   - Comments: Optionally, record additional statements about any aspect of a policy. If you have used the migration utility to convert version-7.*x* "SOD rules" into version-8.5 access policies (see page 2-22), each SOD rule was assigned a "control type" (equivalent to a version-8.5 policy type). Two control types associated SOD rules with "form rules," which alter the properties of Oracle EBS forms in ways that mitigate conflicts. If you have migrated an SOD rule of either control type, AACG displays the name of the associated form rule in the Comments field.
   - Dimensions: If you have configured dimensions, additional columns appear, one for each dimension. To assign dimension values to the policy you are creating, double-click in the cell for a given dimension. The cell becomes a list box; in it, select one or more values. (To create dimensions or to use an alternative method of assigning their values to policies, see "Creating Dimensions and Assigning Dimension Values" on page 2-19.)

An Analysis Run column displays the date on which the Find Conflicts program was run most recently against each policy, and a Results column displays the number of conflicts found in that run. The values are set automatically by AACG.

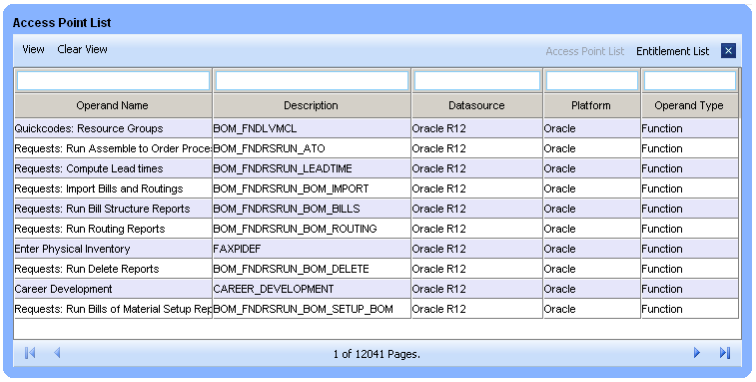
Adding Access Points or Entitlements to a Policy

Once you have created a policy by completing a row in the upper grid, you are ready to add access points or entitlements to it in the lower portion of the Definition page. Typically, as you do so, you work from low level to high — first selecting all the access points you intend to use, then defining the first level of relationships among them, then setting the next-higher level of relationships, and so on until you have reached the highest level.

For example, suppose two Oracle functions conflict, two equivalent PeopleSoft page definitions conflict, and a user's duties violate a policy if she has both functions or both page definitions. You would first select all four access points and insert them in the lower portion of Definition page. Next you would select the two functions and join them in an AND relationship, and then do the same for the two page definitions. You would complete the policy by selecting the two AND operators and joining them in an OR relationship. The result would be a policy that looks like the example at the top of page 2-2.

To add access points or entitlements to a policy:

1. If you are editing an existing policy, double-click on its row in the upper grid. (If you are creating a new policy, its row is necessarily selected already.) Also ensure that the Policy Details option is selected in the Display list box (located in the tool bar near the top of the Definition page). This is the default.
2. Click on the Access Points button in the bottom portion of the Definition page. A pop-up window, titled Access Point List, appears:



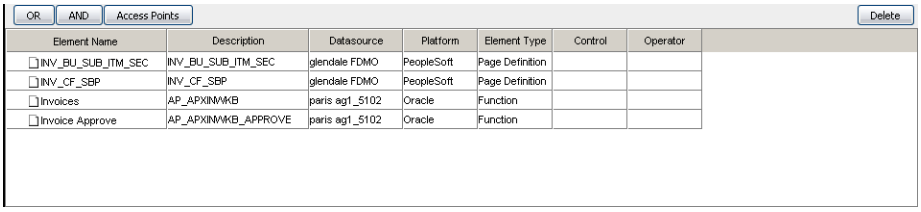
3. Generate a list of objects from which you can select as you build your policy. By default, the window displays access points. Click on the Entitlement List button to enable it to display entitlements instead (if some have been configured; see page 2-15). Click on the Access Point List button to reset the window to display access points.

   Use filtering tools to search for the items you want to select. Enter complementary values in any combination of the following five fields. In each, you can use the percent sign (%) as a wild-card character (as described in "Filtering Data" on page 1-5) to search for a selection of values that contain a text string.

   - Operand Name: Type a text string to search for matching display names of access points or entitlements.
   - Description: Type a text string to search for matching internal names of access points, or descriptions configured for entitlements.

- Datasource: If you are searching for access points, enter a data source name for a business-management-application instance whose access points you want to use. An access point is specific to the instance in which it runs. If, for example, an organization runs two Oracle EBS instances, each function, responsibility, or other access point would be available for selection twice, once for each instance. Use this filter to select access points from the instance you want. If you are searching for entitlements, this field does not apply.
- Platform: If you are searching for access points, enter a business-management-application type — such as Oracle or PeopleSoft — whose access points you want to use. (These values are set during data-source configuration; see the *Governance, Risk and Compliance Controls User Guide*.) If you are searching for entitlements, this field does not apply.
- Operand Type: Select a type of operand for which you wish to search. If you have set the window to display entitlements, then the only valid value is Entitlement. If you have set the window to display access points, valid values include Function, Responsibility, Menus, Grant, and Concurrent Programs (in an Oracle context); Permission List, Panel Group Component, and Page Definition (in a PeopleSoft context); and Role (in either context).

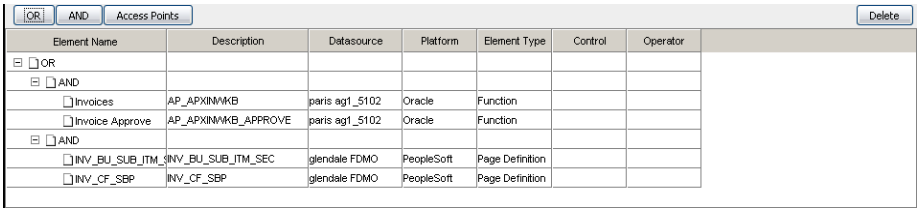
4. Once you have entered filtering values, click on the View button. The Access Point List window then displays access points or entitlements that match your filtering criteria.
5. Select those you want to use in an access policy, and drag them into the Policy Details area of the Definition page.
   - To select a single item, click on it.
   - To select a continuous set of items, click on the first one, hold down the Shift key, and click on the last one.
   - To select a discontinuous set of items, hold down the Ctrl key as you click on the items.
6. If you need to select additional access points that were excluded by your original filtering criteria, click on the Clear View button in the Access Point List window, enter new filtering criteria, and drag additional items into the Policy Details area of the Definition page. When you finish selecting items, close the Access Point List window by clicking on the × symbol in its upper right corner.
7. The Policy Details area now lists the access points or entitlements you selected, as in the following illustration. (Notice that the Control column is not used. The Operator column displays results only after you have selected operators that apply to the access points or entitlements, and have closed and reopened the access policy. Other columns display values as described in step 3, with "Element Name" corresponding to "Operand Name" and "Element Type" corresponding to "Operand Type.")



8. Select objects you want to join in an AND or OR relationship. (As described in step 5, use the Ctrl or Shift key to select multiple objects.) Then click on the AND or OR button to create the relationship. Continue doing so until you have created all the relationships, at all levels, that you want.

   Each operator you add has a ± toggle icon. Click on the minus sign to hide objects that descend from the operator, or on the plus sign to expose them to view.

   For example, three actions modified the screen shown in step 7 to the one below: The two functions were selected and the AND button was clicked. Then the two page definitions were selected and the AND button was clicked again. This added two AND operators; they too were selected and the OR button was clicked.



9. When you are done configuring the access policy, click on the Save button (in the tool bar near the top of the Definition page). A message indicates that the policy has been saved; click on its OK button to clear it.

Viewing Entitlement Details

If an access policy includes entitlements, you can view the details of those entitlements (either as you create the policy or afterwards):

1. In the Policy Details area, expose the row displaying information about the entitlement whose details you want to see. (Click on the + icon for the AND or OR operator that contains it.) Then click on the name of the entitlement.
2. An Entitlement View window opens. It's a replica of the page in which one creates or edits entitlements, except that it's read-only and displays information only about the entitlement you've selected.
   - In the upper portion of the window, review the name, description, status, and effective date of the entitlement, as well as the dimension values assigned to it.
   - Click on the entry in the upper portion of the window and, in the lower portion, review the access points assigned to the entitlement
3. Click on the Close button to close the Entitlement View window.

Designating Policy Participants

As you create an access policy, you may assign it any number of participants. Each participant may be an individual AACG user or a group of users. (To create participant groups, use the Participant Groups option under User Provisioning in the Navigation panel; see page 3-26.) For each policy, one participant (individual or group) must be designated as "first to act," and that participant is charged with resolving conflicts generated by the policy:

- The first-to-act participant approves or rejects the assignment of duties to business-management-application users when such an assignment appears in the User Provisioning Requests page. This happens when the access policy is of the Approval Required type, and duties that violate the policy are assigned after the policy is activated (after its effective date has arrived).

  If the first-to-act participant is an individual, she has sole responsibility for approving or rejecting User Provisioning requests generated by her policy. If the first-to-act participant is a group, any member may approve or reject a User Provisioning request, but the first to do so acts for all; others cannot act after the first member has.

- The first-to-act participant also "owns" paths to conflicts for which access points were assigned to users before a policy was written to define them as conflicting. These paths are displayed in remediation tools other than the User Provisioning Requests page, such as the Conflict Analysis page and the Work Queue.

  If the first-to-act participant is an individual user, these paths are assigned to her by default. If the first-to-act participant is a group, the default reviewer is an individual identified as the "primary" member of the group. In the Work Queue, paths may be reassigned to other users.

Other participants assigned to a policy are AACG users (once again, individuals or participant groups) with some interest in the conflicts generated by the policy, but no default responsibility for resolving them.

To designate participants:

1. Click on the row for a policy in the upper grid of the Definition page.
2. Click on the Display list box in the tool bar and, in its list, select Participants. A "Participants" area then occupies the lower half of the Definition page. For a new policy, it lists the admin user (the default user for every AACG implementation) as the default first-to-act participant; you can, however, change this first-to-act designation (see step 4).
3. Click on the Add button in the Participants area. A Participant List window appears, displaying entries for all AACG users and participant groups. Select any number of them:

   - To select a single participant, click on its ID.
   - To select a continuous set of participants, click on the first one, hold down the Shift key, and click on the last one.
   - To select a discontinuous set of participants, hold down the Ctrl key as you click on their IDs.

   Then click on the OK button in the Participant List window.
4. The Participant List window disappears, and a row for each participant you've selected appears in the Participants area. Review their settings, and alter them as you wish:

   - Participant and Type: These fields identify the participant (displaying either an AACG user name or a participant group name) and its type (either *User* or *Group*). You cannot change these values.

- Effective Date: Select the date on which the user or group can begin to serve as a participant. Either accept the default value — the current date — or click the Effective Date field, and, in the pop-up calendar it presents, click on the left- or right-pointing symbol surrounding the month and year to display an earlier or later month. Then, in the calendar, click on the date you want.
- First to Act: Select the radio button in the row for the participant who is to serve as first-to-act participant. You must select one, and you cannot select more than one; each time you make a new selection, the earlier selection is cleared. If your site implements User Provisioning, ensure that the participant you select — the user if an individual, or all members if you select a participant group — has been assigned an AACG role for which the User Provisioning Requests property has been selected.
- Notify: Select the check box to cause AACG to notify the participant when the policy generates conflicts, or clear the check box to forgo notifications. (When you select the check box for a participant group, all its members receive notifications.)

  For AACG to generate email notifications, however, an administrator must connect GRCC with your email server, then schedule the notifications. Each participant receives notifications at the address provided for him in the Email Address 1 field of the User Administration page. For more on configuring connections to the email server, scheduling notifications, or configuring user accounts, see the *Governance, Risk and Compliance Controls User Guide*.
- Active: Select the check box to activate the participant's status, or clear the check box to render it inactive.

5. When you finish, click on the Save button.

Editing an Access Policy

You can alter any aspect of existing access policies — for each, the values set in the fields of the upper grid, the selection of access points or entitlements, its participants, or its conditions (see page 2-12).

You can reset the status or policy type of any number of existing policies at once:

1. In the upper grid, select the rows for the policies whose status you want to change. Do either of the following:
   - Within a single grid page, select a continuous set of policies by clicking on the first one, holding down the Shift key, and clicking on the last one. Or, to select a discontinuous set of policies, hold down the Ctrl key as you click on the policies.
   - Create a view (see page 1-5) to edit all the policies included in the view. This enables you to select policies that appear on more than one page in the grid.

   If you do not select a set of policies (by one means or the other), a mass update of status or policy type will apply to all policies.

2. Click on the Actions button in the tool bar near the top of the Definition page. This activates an Actions menu; in it, select Mass Edit.

3. A Mass Edit popup window opens. In its list boxes, select the status or policy type (or both) you want to assign to the policies you chose in step 1. Then click on its Save button.

4. A Records Successfully Updated message appears. Click on its OK button, and the Definition page refreshes with the statuses or policy types updated.

Otherwise, you edit existing access policies individually: Double-click on the row for a policy in the upper grid and then follow the processes described in "Adding an Access Policy" and "Adding Access Points or Entitlements to a Policy." Here are some concepts to keep in mind as you work with access points or entitlements:

- When you drag access points (or entitlements) from the Access Point List window into the Policy Details area of the Definition page, you can insert them beneath an existing operator. To do so, position the mouse cursor (as you drag the access points) over the operator; when it turns pink, release the mouse button.

  If you drag an access point to the space outside the rows that define the relationships among existing operators and access points (or entitlements), they are inserted at the highest point in the hierarchy of your access policy (not yet subject to any operator).

- Once an access point exists in the Policy Details area, you can drag it to another position within the hierarchy of your access policy — for example, beneath an existing operator or to the highest point in the hierarchy (not yet subject to any operator). However, when you do so, you actually drag a copy of the access point; the original access point continues to exist as well, at its original position in the hierarchy of your access policy.

- You can also drag an operator to another position within the hierarchy of your access policy. When you do so, you also drag everything that descends from the operator. (As you do so, make sure to position the mouse cursor over the word AND or OR, and not over the icon to its left.) Once again, you actually drag a copy of the operator (and its descendents); the original continues to exist as well.

- You can delete unwanted access points and operators. To do so, click on the object you no longer want, and then click on the Delete button located at the upper right of the Policy Details area. Be aware, however, that if you delete an object, you also delete everything that descends from it.

- You cannot drag a copy of an access point to a position that is subservient to another access point (because you would then not be able to do anything with it).

  Moreover, after you drag copies of access points to the top of the hierarchy, you must then place them beneath an operator (which must have proper logical relationships to other operators). Otherwise, you cannot save the policy; when you attempt to do so, Application Access Controls Governor displays a message stating that you have created an invalid rule expression.

When you finish making changes to the access policy, click on the Save button to save your changes.

Copying an Access Policy

You can copy an access policy as a template for the creation of a new policy. In the upper grid of the Definition page, click on the row for the policy you want to copy. Then click on the Actions button in the tool bar near the top of the Definition page. This activates an Actions menu; in it select Copy.

The new policy is named "Copy(*n*) of *Name*," in which *n* is a number (1 for the first copy, 2 for the second, and so on) and *Name* is the name of the original policy. The copy is Inactive, but is otherwise identical to the original. After you make the copy:

- Use the procedures described in "Editing an Access Policy" to modify its selection of access points or entitlements as desired.
- Give the copy a new name that reflects the alterations you've made to its access points or entitlements.
- When you are ready to use the policy, change its status to Active.
- When you finish making changes to the copied access policy, click on the Save button to save your changes.

Defining Conditions

You can create three types of condition that affect the generation of conflicts:

- As you create or edit an access policy, you can create conditions for it. These can specify users or other objects, such as companies in PeopleSoft or operating units in Oracle EBS, that are exempt from the policy. Or they can specify circumstances under which the policy is enforced — for example, only when a user's access to conflicting access points would be granted within a single set of books.
- You can create global conditions. These are essentially the same as the conditions that are configured to apply to an individual policy, except that a global condition applies to all policies as they are enforced on a given instance of a business-management application.
- You can create global path conditions. Each excludes one access point from another, such as an Oracle function from a menu or a responsibility. A path including those points would be excluded from conflict generation. For example, an access policy might set functions f1 and f2 in conflict. If a global path condition excludes f1 from responsibility r1, and a user has access to both functions, then no conflict would occur if the user's access to f1 comes from r1.

Setting Conditions and Global Conditions

To create conditions for a policy:

1. With the Definition page open (see page 2-4), click on the row for a policy in the upper grid of the page.
2. Click on the Display list box in the tool bar and, in its list, select Condition. The lower area of the Definition page then displays one row for each instance of a business-management application the policy will affect. A Registered Instances column displays the name of each instance, together with a plus sign.
3. Click on a plus sign to reveal rows in which you can enter condition values.

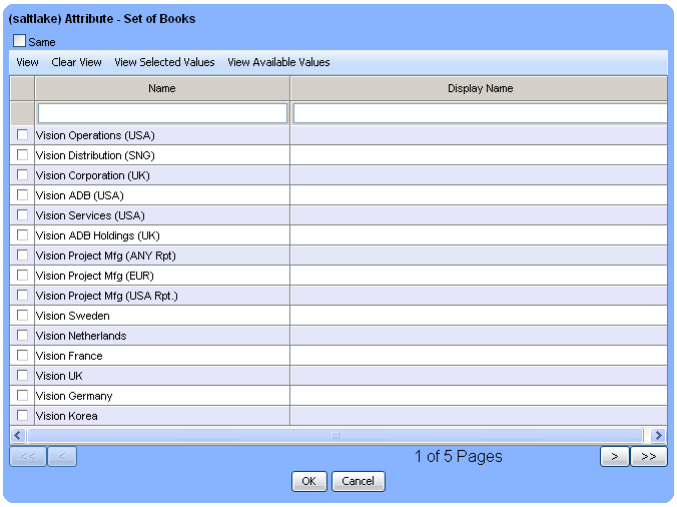
To set global conditions:

1. Locate the Global Conditions entry in the Navigation panel — the third entry under Policy in the Access Policies section.
2. Click on its plus sign to reveal a list of data sources, each of which corresponds to one of the instances for which you've run the data-synchronization process.
3. Click on one of those data sources. A Global Conditions page opens, displaying a row for the data source you've selected.
4. Click on the plus sign in its Registered Instances column to reveal rows in which you can enter condition values.

In either case, you have opened a conditions grid, which looks like this:

Registered Instances	Conditions Exists?	Types	Values	Same	Comments
Oracle R12	No				
		Users			
		Data Group		No	
		MO: Operating Unit		No	
		Set of Books		No	
		Prompt			
		Submenu Grant Flag			
		AK Region Code		No	
		Query Only			
		Function Grant Flag			
		Responsibility Query Only			
		Responsibility			
		Menu			
		Function			
		Role			
		Responsibility End Date			
		User End Date			
		User Responsibility End Date			

A Conditions Exist column, which is updated by AACG, indicates whether any conditions have already been set. (Its valid values are *Yes* and *No*.) Each of the entries in the Types column is a condition you can set; to set one, you click on the corresponding cell in the Value column. This opens a pop-up window:



Typically, you click on check boxes that correspond to entities you want to exempt from evaluation by an access policy.

You can search for items to select: enter text strings in the Name or (if available) Display Name fields to search for matching entries, and click on the View button. As usual, you can use the percent sign (%) as a wild-card character. Click on the Clear View button to discard search criteria and display all possible entries. (Once

you have saved a selection of items, click on View Selected Values to see only those items, or View Available Values to see all other items.)

For some conditions, you can select a Same check box. If you do, the word *Yes* appears in the Same column of the conditions grid; if not, the word *No* appears. When the check box is not offered for a condition, its cell in the Same column remains blank.

- If you select the Same check box, a policy generates conflicts when a user is given rights to conflicting access points only within individual instances of the items for which you are configuring a condition. For example, if you select Same as you create a condition for operating units, a conflict would occur if a user is assigned conflicting access points within an operating unit, but not if he is granted one of those access points in one operating unit, and another access point in a second operating unit.
- If you clear the Same check box, the policy generates conflicts within or across such items. For example, a conflict occurs if a user is assigned one of two conflicting access points in one operating unit, and the second in another operating unit.

Note that the Same option applies only to conditions on business attributes assigned at the access-point level, not to those assigned at the user level. In the latter case, the condition would always be met, and therefore have no benefit.

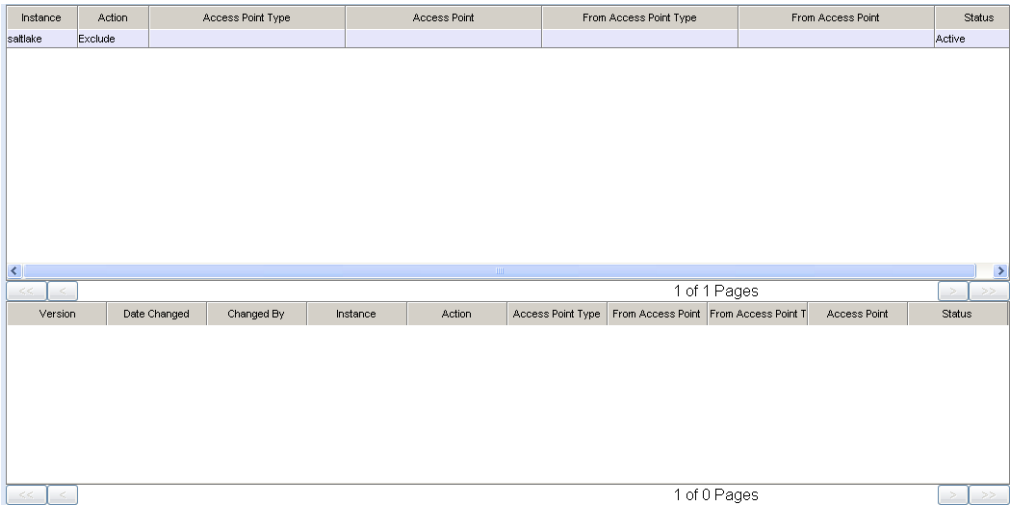
Optionally, click in the appropriate cell of the Comments column, and briefly describe the purpose of the condition.

When you finish selecting values for a condition, click on the OK button in the pop-up window.

Setting Global Path Conditions

To create a global path condition:

1. Locate the Global Path Conditions entry in the Navigation panel — the fourth entry under Policy in the Access Policies section.
2. Click on its plus sign to reveal a list of data sources, each of which corresponds to one of the instances for which you've run the data synchronization process.
3. Click on one of those data sources. A Global Path Conditions page opens:



4. Click on Action in the tool bar and then Add in the Action list. A new row appears in the top section of the page. Its Instance field is set automatically to the data source you selected in step 2, and the Action field to Exclude. These cannot be changed.
5. Double-click on each of the remaining fields. In each, a pop-up window presents a list; in it, select an appropriate value:
   - In the Access Point Type field, choose the type of access point you want to exclude from another.
   - In the Access Point field, select the specific access point to be excluded.
   - In the From Access Point Type field, select the type of access point from which you want to exclude the one you've already selected.
   - In the From Access Point field, select the specific access point from which the first is to be excluded.
   - In the Status field, accept the default value, Active, to use the condition or select Inactive to hold in reserve.
6. Click on Action in the tool bar and then Save in the Action list.

To edit a global path condition

1. Select its row in the upper portion of the page.
2. Select Edit from the Action list.
3. Select new values as described in step 5, above.
4. Save the condition.

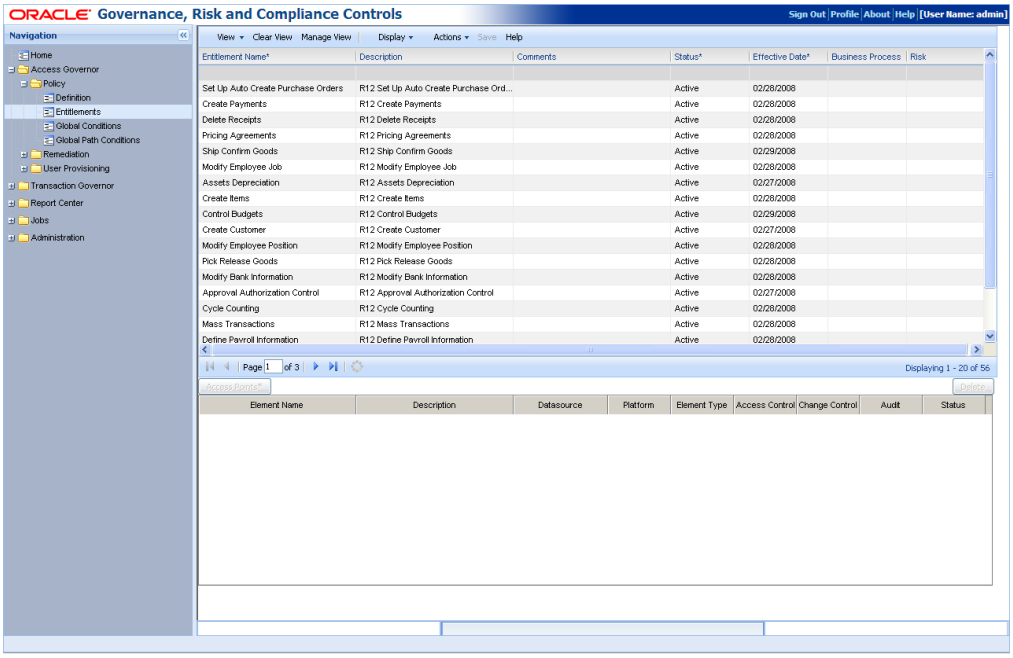
Subsequently, when you select the condition in the upper portion of the page, change history appears in the lower portion — one row displaying the settings for each version up to, but not including, the current version.

Creating an Entitlement

You can, as noted earlier, collect access points into "entitlements." You can then create access policies that define conflicts by using entitlements in place of, or in addition to, access points. In such a policy, the entitlement would be one component in a subpolicy (AND or OR statement), and each of its access points would be considered to conflict with every access point in other entitlements named in the subpolicy, as well as with access points included in the subpolicy independently of entitlements.

The process of creating an entitlement is similar to that of creating an access policy, except that it can contain only access points, and it simply lists them. Members of an entitlement necessarily have OR relationships with one another, so there is no need to define relationships among them.

1. Locate and click on the Entitlements entry in the Navigation panel. This opens an Entitlements page (shown at the top of the next page). A grid occupies the upper half of the page and lists existing entitlements. An "Entitlement Details" view occupies the lower half; it provides tools for adding access points to an entitlement.



2. Click on the Actions button in the tool bar near the top of the Entitlements page. This activates an Actions menu; in it select Add. A new row appears in the grid, second from the top (immediately beneath the view row).
3. Insert the following values in the new row. To do so, double-click in each field, or press the Tab key to move from an active field to the next field.
    - Entitlement Name: Type a name for the new entitlement.
    - Description: Explain briefly the organizing principle or business purpose of the entitlement.
    - Comments: Record statements about any aspect of the entitlement, for example whether a given access point is covered by a compensating control.
    - Status: From a list box, select a status. An Inactive entitlement cannot be selected for use in an access policy. An Active entitlement can (even if its effective date, set in the next field, is in the future, in which case the policy will use the entitlement beginning on that date).
    - Effective Date: Select a date on which AACG can begin to use the entitlement. (Its status must also be set to Active.) Either accept the default value — the current date — or double-click in the Effective Date column, and then click on the grid-like icon it presents. A pop-up calendar appears. In it, click on the left- or right-pointing symbol surrounding the month and year to display an earlier or later month. Or, click on the downward-pointing symbol to produce a list of months in the current year, and click on the one you want. Then, in the calendar, click on the date you want. Alternatively, click on the Today button to select the current date.
    - Dimensions: If you have configured dimensions, additional columns appear in the Entitlements-page grid, one for each dimension. To assign dimension values to the entitlement you are creating, double-click in the cell for a given dimension. The cell becomes a list box; in it, select one or more values. (To

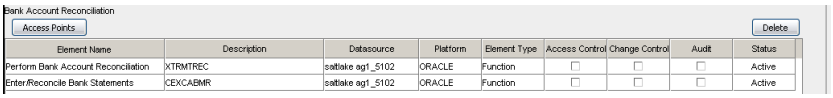
create dimensions or use an alternative method of assigning their values to policies, see “Creating Dimensions and Assigning Dimension Values” on page 2-19.)

Adding Access Points to an Entitlement

Once you have created an entitlement by completing a row in the upper grid, you are ready to add access points to it.

1. If you are editing an existing entitlement, select (double-click on) its row in the upper grid. (If you are creating a new entitlement, its row is selected already.) Also ensure that the Entitlement Details option is selected in the Display list box (located in the tool bar near the top of the Entitlements page). This is the default.
2. Click on the Access Points button in the bottom portion of the Entitlements page. This opens an Access Point List window like the one used for access policies (see step 2 on page 2-6), except that because you can add only access points to an entitlement, it has no Entitlement List or Access Point List button.
3. Generate a list of access points from which you can select as you build your entitlement. Use filtering tools to search for the access points you want to select. You can use the percent sign as a wild-card character, and you can enter complementary filtering values in any combination of the following fields:
   - Operand Name: Type a text string to search for matching display names of access points
   - Description: Type a text string to search for matching internal names of access points
   - Datasource: Enter a data source name for a business-management-application instance whose access points you want to use. An access point is specific to the instance in which it runs. If, for example, an organization runs two Oracle EBS instances, each function, responsibility, or other access point would be available for selection twice, once for each instance. Use this filter to ensure your entitlement contains access points selected from the instance you want.
   - Platform: Enter a type — such a Oracle or PeopleSoft — for the application whose access points you want to use.
   - Operand Type: Select a type of operand for which you wish to search. valid values include Function, Menus, Responsibility, and Concurrent Programs (in an Oracle context); Permission List, Panel Group Component, and Page Definition (in a PeopleSoft context); and Role (in either context).
4. Once you have entered filtering values, click on the View button. The search window then displays access points that match your filtering criteria.
5. Select access points you want to add to the entitlement, and drag them into the Entitlement Details area of the Entitlements page.
   - To select a single access point, click on it.
   - To select a continuous set of access points, click on the first one, hold down the Shift key, and click on the last one.
   - To select a discontinuous set of access points, hold down the Ctrl key as you click on the access points.

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



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

   The Access Control, Change Control, and Audit check boxes are reserved for future development, and have no meaning. Other columns display values as described in step 3, with "Element Name" corresponding to "Operand Name" and "Element Type" corresponding to "Operand Type.")

8. When you are done configuring the entitlement, click on the Save button (in the tool bar near the top of the Entitlements page). A message indicates that the entitlement has been saved; click on its OK button to clear it.

Editing an Entitlement

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

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

Use caution. If you edit an entitlement after it has been selected for use in an access policy, you necessarily alter the meaning of that policy, potentially to the point at which it no longer defines meaningful conflicts.

When you finish making changes to the entitlement, click on the Save button to save your changes. If you are editing an entitlement that is used by access policies, a warning message appears, identifying the polices that use it:

- If you want to proceed with your edit, click on the Save button in the warning message.
- If you determine that saving your edit would distort an access policy, click on the Cancel button in the warning message. (In that case, the entitlement reappears in its original form when you refresh your screen, for instance by selecting another entitlement and then reselecting the one you had been working on.)

Copying an Entitlement

You can copy an entitlement as a template for the creation of a new entitlement. In the upper grid of the Entitlements page, click on the row for the entitlement you want to copy. Then click on the Actions button in the tool bar near the top of the Entitlements page. This activates an Actions menu; in it select Copy.

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

After you make the copy:

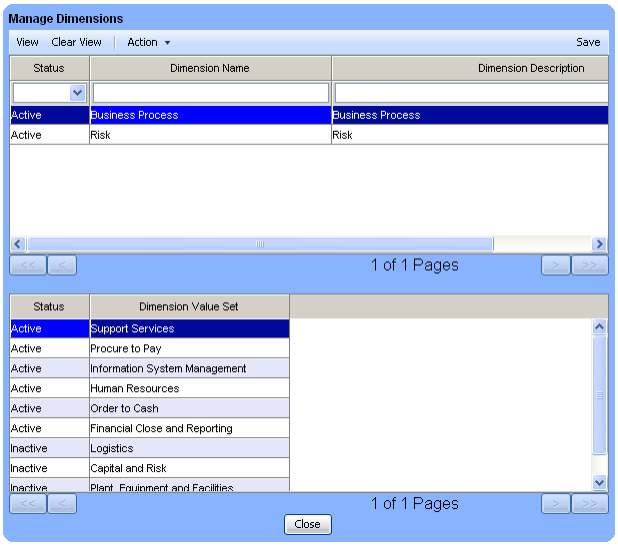
- Use the procedures described in "Editing an Entitlement" to modify its selection of access points as desired.
- Give the copy a new name that reflects the alterations you've made to it.
- When you are ready to use the entitlement, change its status to Active.
- Click the Save button to save your changes.

Creating Dimensions and Assigning Dimension Values

A dimension is a category of values; its values may be assigned to access policies (and so to conflicts generated by those policies) or entitlements (and so to conflicts generated by policies that include those entitlements). They serve to flag related items, and to distinguish them from unrelated items. They may therefore be used as sort criteria in AACG pages that display policies, entitlements, or conflicts.

To create dimensions and their values.

1. Open either the Definition page or the Entitlements page.
2. Click on the Action button in the tool bar and, in its menu select Manage Dimensions. The following pop-up window opens:



3. Click on the Action button in the tool bar, and, in its menu, Add Dimension. A blank row appears in the upper grid of the Manage Dimensions window.
4. Click in the Status field. This activates a list box; in it, select a status:
   - "Active" causes a column to be added for the dimension to each of the Definition, Entitlements, and Conflict Analysis pages (and so permits values to be assigned to policies or entitlements).
   - "Inactive" removes the dimension's column from these pages.
5. Click in each of the Dimension Name and Dimension Description columns, and enter a name and description for the dimension.
6. In the Action list box, select Add Dimension Value. A blank row appears in the lower area of the Manage Dimensions window.
7. Click in the Dimension Value Set column of that row and enter a value for the dimension.
8. Click in the Status column of that row and select Active or Inactive.
9. Repeat steps 6–8 any number of times to create as many values as you wish for the dimension.
10. When you finish creating values, select Save in the Action list box.
11. Close the Manage Dimensions window (click on the Close button). A column for the dimension you have created appears in the Definition or Entitlements page when you navigate away from, and back to, it.

Once you have created a dimension, you can edit its status, name, description, or values.

1. Open the Manage Dimensions window and double-click on the dimension you want to edit.

   (To search for a dimension, enter values in any combination of the Status, Dimension Name, and Dimension Descriptions fields; you can use the percent sign as a wild-card character. Then click on the View button; click the Clear View button to restore the full list of dimensions.)
2. Set status or add values as you would for a new dimension; click on name or description fields and alter their contents as you wish.
3. When you are done, select Save in the Action list box.

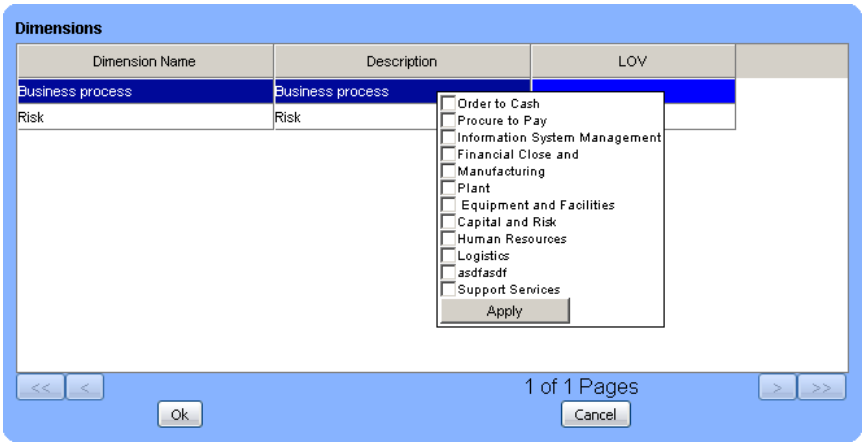
Inactivating and then reactivating a dimension, or changing its name, does not alter any prior assignments of dimension values to policies or entitlements.

As you create policies (page 2-5) or entitlements (page 2-15), you can assign dimension values to them. As an alternative, you can complete the following steps:

1. Open the Definition page to assign values to policies, or the Entitlements page to assign values to entitlements.
2. In the upper grid of the page, select any number of rows to assign a set of dimension values to the policies or entitlements identified by those rows. (Click on a row to select it. To select a continuous set of rows, click on the first one, hold down the Shift key, and click on the last one. To select a discontinuous set of rows, hold down the Ctrl key as you click on the rows.)

3. Click on the Actions button in the tool bar near the top of the page. This activates an Actions menu; in it select Assign Dimensions. The Dimensions pop-up window opens.

4. Locate the row for the dimension whose values you want to assign. Double-click in its LOV column. A set of check boxes, one for each value configured for the dimension, appears:



5. Click in the check boxes for the values you want to assign (you can select more than one), and then on the Apply button. The list of check boxes disappears, and your selections appear in the LOV column.

6. Click on the OK button; the Dimensions window closes. The Definition or Entitlements page refreshes, and the values you selected appear in the column for the dimension, in the row for the policy or entitlement you selected in step 2.

Viewing Change History

As you make changes to access policies or entitlements, you can view records of their earlier versions, and so track their change history. To do so:

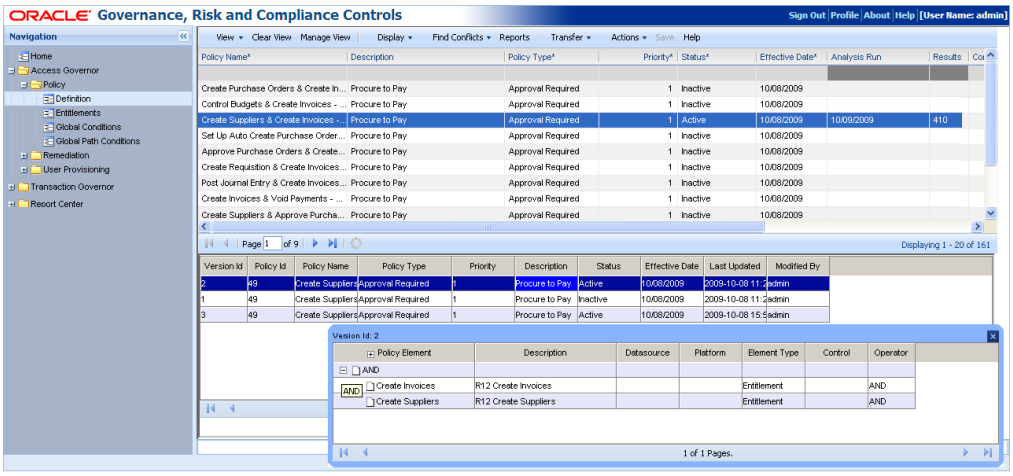
1. Open the Definition page and, in its upper grid, select an access policy whose change history you want to view. Or, open the Entitlements page and, in its upper grid, select an entitlement whose change history you want to view.

2. Click on Display in the tool bar, and then on Change History in the Display list box.

   The lower area of the Definition or Entitlements page displays change-history data: one row for each version of the item up to (but not including) the current version. Each row contains:

   - The values set in the upper grid for its version of the item.
   - A policy ID or entitlement ID (an internal number generated by AACG).
   - A version ID (one in a sequence of numbers, the value *1* being the earliest version, and so on working forward)
   - The date on which changes were saved and so this version was created.
   - The ID of the person who made the changes.

For example, the following figure shows an access policy that is currently in its third version, with its history grid displaying rows for the two earlier versions.



3. Double-click on a row for any version to open a pop-up window that displays its members and, in the case of an access policy, the relationships among them. For example, the preceding illustration shows the access points selected for version 2 of an access policy. You can simultaneously open these windows for any number of versions. To close them, click on the × symbol in the upper right corner of each.

Exporting, Importing, and Migrating Policies

You can import access policies from another version-8.*x* instance of AACG. To import a set of policies to a destination instance, you must first export them from a source instance to a file. An alternative is to use a migration utility to transform version-7.*x* "SOD rules" into version-8.5 access policies.

The export, import, and migration utilities capture not only access policies (or SOD rules), but also entitlements (or "entity groups," their version-7.*x* equivalent) used by those policies or rules.

To export access policies from a source instance to a file:

1. Open the Definition page (see page 2-4).
2. Optionally, in the upper grid of the Definition page, select one or more policies you want to export. To select one policy, click on it. To select a continuous set of policies, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on policies. If you make no selection, all policies will be exported.
3. Click on the Transfer button in the tool bar near the top of the Definition page. This produces a list of options; in it, click on Export.
4. An Export Policies pop-up window reports the number of policies to be exported. Click on its Download button:
5. A File Download pop-up window offers you options to open or save the export file. Typically, click on its Save button and, in a Save As dialog, use standard Windows techniques to navigate to a folder in which you want to save the file.

To import access policies from a file to a destination instance:

1. Open the Definition page.
2. Click on the Transfer button in the tool bar near the top of the Definition page, and then click on the Import option in the list that it produces. An Import Policies pop-up window opens.
3. Click on its Browse button, and a Choose File dialog opens. In it, use standard Windows techniques to navigate to, and select, the file you want to import. The path and name of the file then populate the field next to the Browse button in the Import File window.
4. With the file selected, click on the OK button.
5. A Select Items to Import window lists the policies contained in the import file. Select those you wish to import: To select one item, click on it. To select a continuous set, click on the first item, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on items.
6. Click on the Next button. An Import Data Source Mapping window opens, displaying one row for each data source specified in the policies you've chosen to import. For each, in a Mapped Data Sources list box, select a data source appropriate for the environment into which you are importing the policy. (The list box displays data sources configured in the GRCC Data Administration page.)

   For example, in a test environment, a policy may set f1 in conflict with f2 in each of two test data sources (ora1test and ora2test). You may wish to import these to a production environment, in which there are equivalent production data sources (ora1prod and ora2prod). The Import Data Source Mapping window would include a row for each of ora1test and ora2test, and in the Mapped Data Sources list box, you would supply the appropriate production-instance values — ora1prod and ora2prod, respectively.
7. Click on the Import button. A pop-up message reports the number of models imported and the status of the import operation. Click on its × button to close it.

Before migrating policies, you must configure both the source and destination instances as data sources. (See the *Governance, Risk and Compliance Controls User Guide*.)

1. Open the Definition page.
2. Ensure that no individual policy is selected. If one or more are, click on the filtering row to clear them.
3. Click on the Transfer button in the tool bar near the top of the Definition page, and then click on the Migrate option in the list that it produces. A Migrate Policies pop-up window opens.
4. In the field on the left, click on the version of AACG from which you want to migrate policies. This populates the field on the right with instances of that version that you have configured as data sources. Click on the instance whose policies you want to migrate. Then click on the Migrate button.
5. A pop-up message reports the number of policies migrated and the status of the migration operation. Click on its OK button to clear it.
6. Navigate away from, and then back to, the Definition page to refresh it.

As you review the policies you've migrated, bear these concepts in mind:

- Version 7.*x* of AACG offers four "control types" — Prevent, Allow with Rules, Approve with Rules, and Approval Required. In version 8.2.1 there are three equivalent policy types (as described on page 1-2). As the migration utility converts SOD rules into access policies, it maps control types to version-8.2.1 types as follows:

7.*x* Control Types	**8.2.1 Policy Types**
Prevent	Prevent
Allow with Rules	Monitor
Approve with Rules	Approval Required
Approval Required	Approval Required

- A version-7.*x* SOD rule with the Allow with Rules or Approve with Rules control type is associated with a "form rule," created in an "embedded agent," that alters the properties of an Oracle form in a way that mitigates the conflict. The form rule continues to exist, and the migration utility identifies the form rule in the Comments column of the version-8.2.1 Definition page.
- A version-7.*x* SOD rule could hold any number of entities — either functions, responsibilities, or groups of either — and a conflict would be generated if a user were granted any two of these entities. It was not necessary for a user to have all of the entities named in an SOD rule for a conflict to be generated. Thus the equivalent 8.2,1 access policy should employ an OR operator that is a parent to pairs of entities, each joined by an AND operator. Suppose, for example, that a version-7.*x* SOD rule contained three functions:

  ```
  f1, f2, f3
  ```

  The equivalent version-8.2.1 access policy would *not* be the following, which would require a user to be assigned all three functions before it would generate a conflict:

  ```
  AND
    f1
    f2
    f3
  ```

  Rather, the equivalent access policy should look like the following, which generates a conflict when a user has any two of the functions:

  ```
  OR
    AND
      f1
      f2
    AND
      f1
      f3
    AND
      f2
      f3
  ```

3

Finding and Resolving Conflicts

Once access policies are defined, the next step is to find conflicts — to search users' work assignments for policy violations. You can then use any of several tools to examine the conflicts you've found:

- The Definition page can display conflict results generated by a selected access policy. It sorts by user, listing the paths each has to the access points that the policy defines as conflicting.
- The Conflict Analysis page presents results for conflicts generated by all policies, or a selection of them. Although, like the Definition page, it displays lists of conflict paths, it sorts them differently — first by policy, then subpolicy, then role, then user.
- The Work Queue enables users to assign conflict paths to reviewers, and for the reviewers to assign status to those paths.
- Simulation enables analysts to preview the effects of cleanup in the business-management application — that is, what would happen if the statuses assigned to conflict paths were actually implemented.
- The Heat Map enables analysts to evaluate trends in the generation of conflicts.
- The User Provisioning Request page enables "first-to-act" policy participants to approve or reject the assignment of duties to users of business-management applications, when those assignments violate Approval Required policies. A User Provisioning Administration page displays a history of requests.

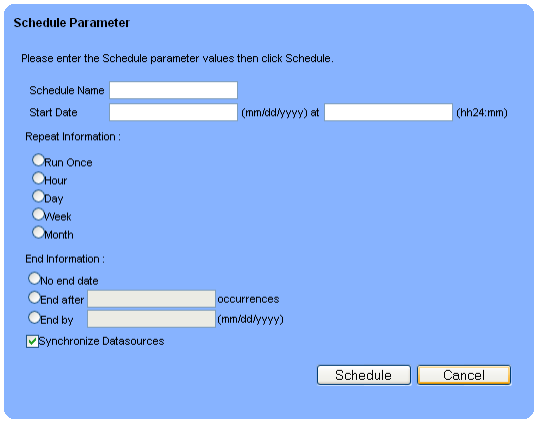
Finding Conflicts

To evaluate access policies, run a Find Conflicts program from the Definition page or the Conflict Analysis page. In the Definition page, you can either run Find Conflicts or schedule it to run in the future, and you can evaluate all policies or a selection of them. In the Conflicts Analysis page, you must evaluate all policies, and the scheduling option is unavailable.

Whenever you run the Find Conflicts program, consider whether to synchronize data first, so that business-management-system data is current and conflict generation is up to date. (For information on data synchronization, see the *Governance, Risk and Compliance Controls User Guide*.)

To find conflicts from the Definition page:

1. Open the Definition page: Select Access Governor in the Navigation panel. Click on the plus sign next to the Policy node, which reveals four lower-level nodes. Of those four, click on Definition.
2. Optionally, in the upper grid of the Definition page, select one or more policies you want to evaluate. To select one policy, click on it. To select a continuous set of policies, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on policies. If you make no selection, all policies will be evaluated.
3. Click on the Find Conflicts button, located in the tool bar near the top of the Definition page. A two-item list appears; in it, click on Run Now or Schedule.
   - If you select Run Now, the Find Conflicts program runs once, immediately.
   - If you select Schedule, the following dialog opens. Enter values that set a name for the schedule, the date and time at which it should start, the regularity with which the Find Conflicts program should run, the date and time (if any) on which the schedule should expire, and whether data should be synchronized before each running of Find Conflicts. Then click on the Schedule button.



To find conflicts from the Conflict Analysis page:

1. Open the Conflict Analysis page: In the Access Governor section of the Navigation panel, click on the plus sign next to the Remediation node. Four subsidiary nodes appear. Click on the first, Conflict Analysis.
2. Click on the Find Conflicts button in the tool bar of the Conflict Analysis page.

In either case, a progress bar indicates that the Find Conflicts process is running, and then announces its completion.

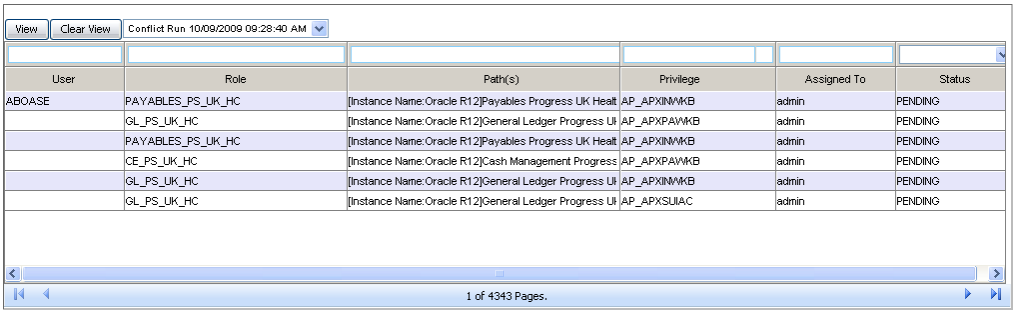
Reviewing Conflicts in the Definition Page

To view conflicts from the Definition page:

1. Open the Definition page (see above).
2. Select an access policy whose conflicts you wish to see: click on its row in the upper grid of the Definition page.

3. Click on Display in the tool bar, and then on Conflicts in the Display list box. The lower portion of the Definition page then displays the most recent set of conflicts generated by the access policy you selected in step 2.

Here, for example, is the first page of the display of conflict paths for a policy called Payables, in which a Payments function (AP_APXPAWKB) conflicts with either an Invoice Approvals function (AP_APXSUIAC) or an Invoices function (AP_APXINWKB).



For each user affected by the policy, the Definition page presents paths to access points that violate the policy:

- Each path begins with an object listed in a Role column; it's the level of object that's actually assigned to a user, such as an Oracle responsibility.
- Each path ends with an object listed in a Privilege column. This is an access point that's actually included in an access policy (either directly or because it is a member of an entitlement that is included in an access policy). It might, for example, be an Oracle function.
- In between is a Paths column, which identifies the role, privilege, and all the objects that lead from one to the other. These intermediate objects might be, for example, a series of menus and submenus that lead from a responsibility to a function. (Each Paths entry also shows the instance in which its access point exists.)

As you review conflict paths in the Definition page, be aware of these concepts:

- Each row is not a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
- All the paths for a single user constitute a single conflict. Those paths may extend over several pages (click on the > or < button to move forward or back one page at a time, or the >> or << button to move to the last or first page). On each page, the user is identified only once, in the User column. Rows with blank User cells belong to the user identified in a row above them.

  In the illustration, for example, all the rows apply to the user ABOASE, and they include paths to all three access points included in the Payables policy, and so both subconflicts defined by it. (The paths for this conflict continue on pages 2 and 3 of the display, although this is not visible in the illustration.)
- Each entry in the User ID column is a "global user" — a unique ID, assigned by AACG to a business-application user, that corresponds to any number of potentially varying IDs identifying that user in any number of business-management applications.
- Each row displays the ID of the user assigned to review its path, the status of the path, and comments created when a reviewer or a status was assigned to the

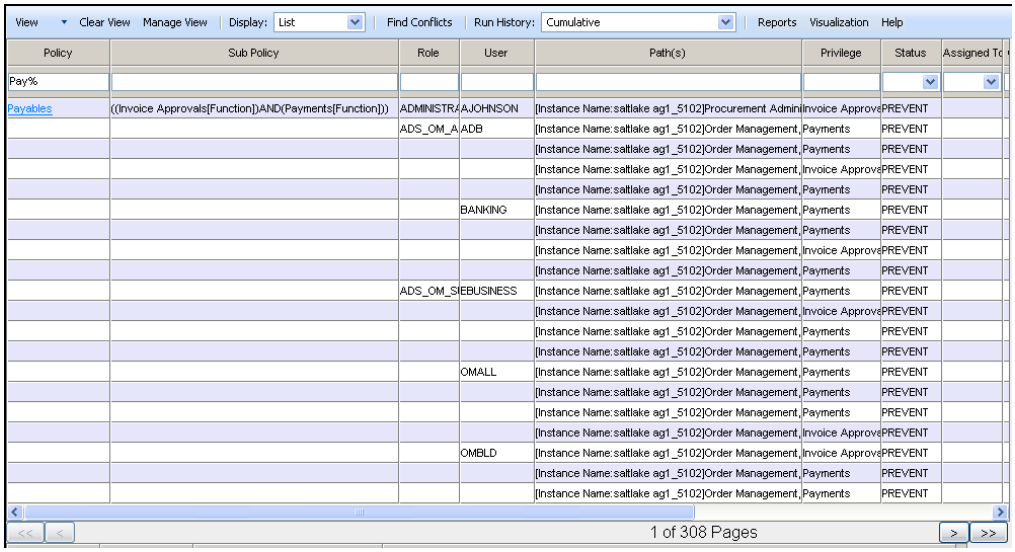
path. Like other values, however, these are read-only. The reviewer is initially the first-to-act participant configured for the policy (or, if that participant is a group, its "primary" member). The reviewer may be reassigned in the Work Queue; status and comment are assigned to a path in the Work Queue or the User Provisioning Requests page.

- You can use any of the column values to filter the display of paths (see "Filtering Data" on page 1-5). If you do, however, you will see only those paths that conform to your filter criteria, and so may no longer have a complete picture of a conflict. If, for example, you were to filter on the value PAYABLES_PS_UK_HC in the Role column of the illustration above, you would eliminate the rows containing other roles (such as GL_PS_UK_HC and CE_PS_UK_HC).
- The Conflicts grid displays a list box whose entries identify individual runs of the Find Conflicts program. To view results for a run other than the one on display, click on the downward-pointing triangle in that list box, and then click on the run whose conflicts you want to see.

Reviewing Conflicts in the Conflict Analysis Page

To view conflicts in the Conflict Analysis page, simply open that page. (In the Access Governance section of the Navigation panel, click on the plus sign next to the Remediation node. Four subsidiary nodes appear. Click on the first, Conflict Analysis.) It displays a "cumulative" view of conflicts generated by all runs of the Find Conflicts program.

Here, for example, are the paths it would display for the Payables policy discussed in "Reviewing Conflicts in the Definition Page" (page 3-2).



As you review conflict paths in the Conflict Analysis page, be aware of these concepts:

- The Conflict Analysis page provides a "subpolicy-level" view. That is, its default sort order groups conflict paths not merely by policy, but also by specific combinations of access points within a policy that produced a conflict. The page sorts paths further by role (the object actually assigned to a user, such as an Oracle

responsibility) and the user assigned the role. These elements are identified, respectively, in the Policy, Sub Policy, Role, and User columns. (Here, as in the conflict display of the Definition page, the User column presents global users.)

For example, the Payables policy defines two potential conflicts — Payments versus Invoices and Payments versus Invoice Approvals. However, the Conflict Analysis page first lists the paths that apply to one of those conflicts (Payments versus Invoice Approvals, as shown in the illustration above), and on a subsequent page the paths that apply to the other. Within each grouping, paths are sorted further by role and user.

- The path itself consists of a role, a privilege (an access point actually included in an access policy, such as an Oracle function), and the objects that lead from one to the other (such as menus and submenus that lead from a responsibility to a function). The Privilege column identifies the privilege, and the Paths column displays the intermediary objects.
- Each row is not a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
- Paths in a given group (for example, those belonging to the Payments versus Invoice Approvals subpolicy) may extend over several pages of the Conflict Analysis display. Within each column, rows with blank cells belong to the entity identified in a row above them.
- Additional columns display values selected for the policy that generated a given conflict path. These include the policy type, priority, dimension values (if any), the datasource, and entitlements used by the policy.
- Each row displays the ID of the user assigned to review its path, the status of the path, and comments created when a reviewer or a status was assigned to the path. Like other values, however, these are read-only. The reviewer is initially the first-to-act participant configured for the policy that generated the conflict path (or, if that participant is a group, its "primary" member). The reviewer may be reassigned in the Work Queue; status and comment are assigned to a path in the Work Queue or the User Provisioning Requests page.
- When a conflict is approved through User Provisioning, entries for its conflict paths appear in the Conflict Analysis page. For these entries, the Approved By column identifies the individual user who approved the conflict (which may differ from the value in the Assigned To column if the first-to-act participant is a group). The Approved column displays the date on which the approval occurred. For all paths, a Type column displays the value *ANALYSIS* if status for the conflict path was set in the Work Queue, or *AUTHORIZED* if status was set through User Provisioning.
- You can move from the Conflict Analysis page to the Work Queue, and back. In the Display list box at the top of the listing of conflict paths, select Work Queue to move there or List to return to the Conflict Analysis page.
- In the Run History list box, you can choose a run of the Find Conflict program to display conflicts generated in that run, select Provisioning Requests to view only conflict data generated by the User Provisioning feature, or select Cumulative to display conflicts generated in all runs.
- You can use any of the column values to filter the display of paths (see "Filtering Data" on page 1-5). Doing so may alter the perspective of the Conflict

Analysis page. For example, if you were to filter on a specific user, the page would display only the paths for that user, grouped by policy (and subpolicy), so that you would in effect have a conflict-level view.

- From Conflict Analysis, you can view a history of the changes made to each path. (These changes are made in the Work Queue.) Select (click on) a path, and a panel beneath the listing of conflict paths presents one row for each version of the path up to (but not including) the current version. Each row shows (as appropriate) the reviewer assigned to a path, or the status and comment assigned to a path by its reviewer. (If no changes have been in the Work Queue, of course, this history panel remains blank. You cannot enter or alter data directly in this panel.)

Viewing Policy Details

From the Conflict Analysis page or the Work Queue, you can view the details of access policies that have generated conflict paths:

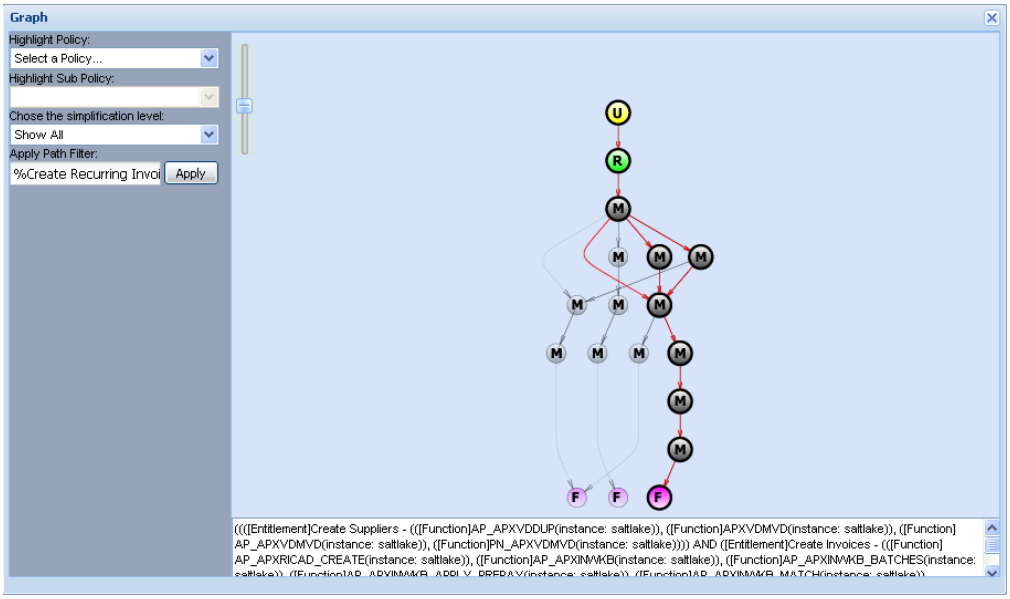
1. In the Policy column, double-click on the name of the policy that has generated a given conflict path. (If the Policy column is blank for the path in question, then the appropriate policy is the nearest one identified in a row above the path.)
2. A Policy View window opens. It's a replica of the page which one creates or edits policies, except that it's read-only and displays information only about the policy you've selected.
   - In the upper portion of the window, review the name, description, type, priority, status, and effective date of the policy, the dimension values assigned to it, and summary results for its most recent conflict-analysis run.
   - Click on the entry in the upper portion of the window. In the lower portion, review the access points or entitlements assigned to the policy.
   - In the Display menu, select other information to display in the lower portion of the Policy View window — conflicts generated by the policy, conditions and participants configured for it, and its change history. Having selected any of these options, click on Policy Details to restore the display of access points or entitlements assigned to the policy.
3. Click on the Close button to close the Policy View window.

Visualization

From the Conflict Analysis page or the Work Queue, you can generate a graphic depiction of paths from any number of users to any number of access points involved in conflicts. Having done so, you may select any path — to any access point within a full path, from a user to a privilege named in an access policy — and use that path to filter the rows displayed in the Conflict Analysis page or Work Queue.

1. Select any number of conflict paths. You can select only paths displayed in an individual page of the Conflict Analysis page or Work Queue, so you may first create a view that filters entries. Then, to select path, click on it; to select a continuous set of paths, click on the first one, hold down the Shift key, and click on the last one; or to select a discontinuous set of paths, hold down the Ctrl key as you click on the paths.

2. In the tool bar, click on Visualization. A Graph window opens, depicting the paths you've selected.

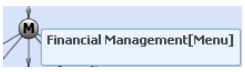


3. Review information presented by the image:

   - The top-level node in a Visualization image is initially a user whose duty assignments have violated access policies. Depending on the paths you've selected in step 1, there may be more than one user.
   - The bottom-level nodes in a Visualization image represent the lowest-level objects affected by policies — those that actually enable a user to do something. For example, if a policy is defined to set one Oracle responsibility in conflict with another, the graph shows not only the responsibilities, but also the menus to which they lead and the functions to which those menus lead.
   - All nodes represent objects that lead from a user to an object that enable the user to do something, and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.
   - You can expand or contract the size of the image: Click on square with a horizontal line at the upper left of the frame containing the diagram, and slide it up to enlarge the diagram (and so expose fewer of its objects to view), or down to reduce the diagram (and so expose more of its objects to view).

4. Manipulate information presented by the image:

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

   - If you click on any object in a path, the arrows leading to that object are highlighted in red, distinguishing those paths from others that do not lead to the object you've selected. (In the illustration above, the function farthest to the right has been selected. As a result, paths leading to it are highlighted.)
   - If, in step 1, you selected paths involving more than one policy, you can select one of them to highlight its paths in red. To do so, click on the down-

ward-pointing icon in the Highlight Policy list box, and select the policy you want. (If, in step 1, you selected paths involving only one policy, only that policy is displayed in the Highlight Policy list box.)

- If, in step 1, you selected paths involving more than one subpolicy, you can select one of them to highlight its paths in red. To do so, first use the Highlight Policy list box to select a policy (even if you have selected paths involving only one policy). Then, click on the downward-pointing icon in the Highlight Sub Policy list box, and select the subpolicy you want. (If, in step 1, you selected paths involving only one subpolicy, only that subpolicy is displayed in the Highlight Sub Policy list box.)
- You can narrow the focus of the Visualization image by eliminating its first hierarchical level (users whose assignments have generated conflicts), or the first and second hierarchical levels (users and the roles assigned to them). To do so, click on the downward-pointing icon in the list box labeled *Chose a simplification level*, and select the Hide User option or the Hide User & Role/Permission List option.

5. To select a path that serves as a filter for paths listed in the Conflict Analysis page or Work Queue, click on any node (at any level in the conflict-path hierarchy displayed in the graph). The path to that node appears in the Apply Path Filter field. With that path displayed, click on the Apply button. The Visualization graph closes, and the Conflict Analysis page or Work Queue displays only paths defined by the filter you've selected.

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

Simulation

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

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

To create and run a simulation:

1. Name and describe it.
2. Select an access point that's involved in one or more conflicts, and create a graphic model of its hierarchy.

3. Develop remediation steps. In the graphic model, select an access point whose removal might resolve a conflict, and select its immediate parent. (Either click on the two access points, or click on the link between them.) For example, in an Oracle context, a user might have access to functions f1 and f2, and a policy may define them as conflicting. You might select f1 and the responsibility through which the user has access to it (assuming there's a direct link between the two). Then select a "Remove" option.

   Repeat this process as often as you like to create addition remediation steps.

4. Run the simulation and view its results.

5. Print a copy of the remediation plan you've created, or save a copy to your computer.

In version 8.5, the Simulation functionality is significantly redesigned. As a result, simulation "scenarios" created in earlier 8.*x* versions of AACG are incompatible with version 8.5. If you wish to reuse simulation plans you created in earlier versions, you need to re-create them in version 8.5.

Creating and Naming a Simulation

To create a simulation:

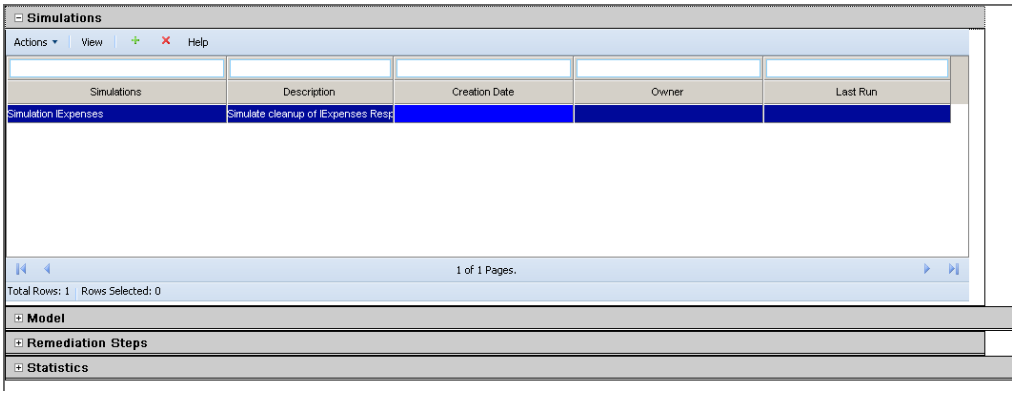
1. Open the Simulations page. In the Access Governance section of the Navigation panel, click on the plus sign next to the Remediation node. Four subsidiary nodes appear. Click on the second, Simulation.

2. In the Simulations pane, select Create New from the Actions menu. A new row appears in the Simulations grid.

3. Click in the Simulations field of the new row, and type name for the simulation you are creating.

4. Click in the Description field (or, from the Simulations field, press the Tab key). Then type a brief description of your goal in creating the simulation.

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



Creating a Simulation Model

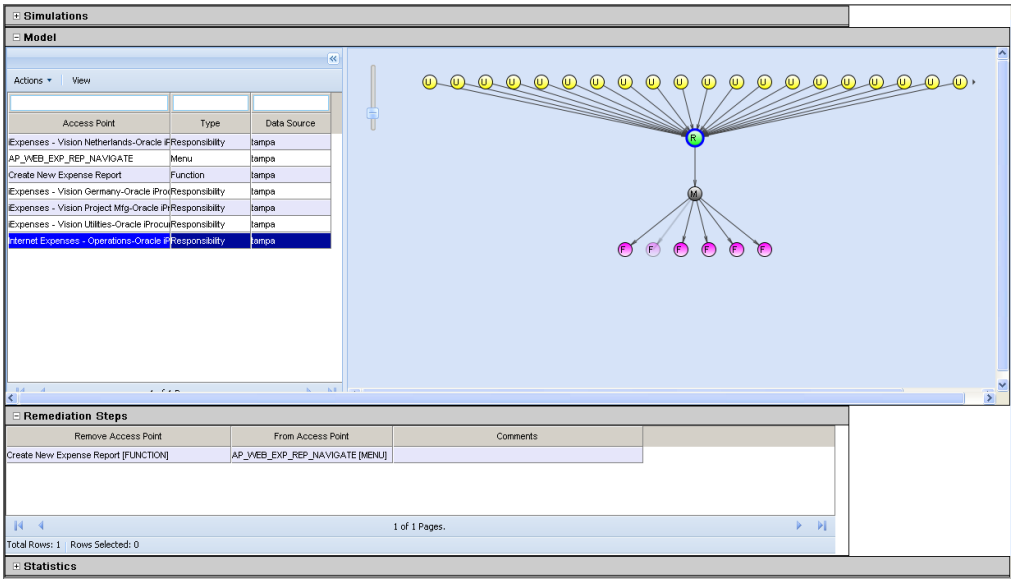
To create the graphic model used in a simulation:

1. In the grid to the left of the Model pane, select an access point around which you wish to build a model. The grid lists only access points that were involved in conflicts in the most recent AACG conflict-analysis run.

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

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

Because the model bases its results on the most recent synchronization and conflict-analysis runs, you would typically want to run synchronization and conflict analysis before creating a simulation model.



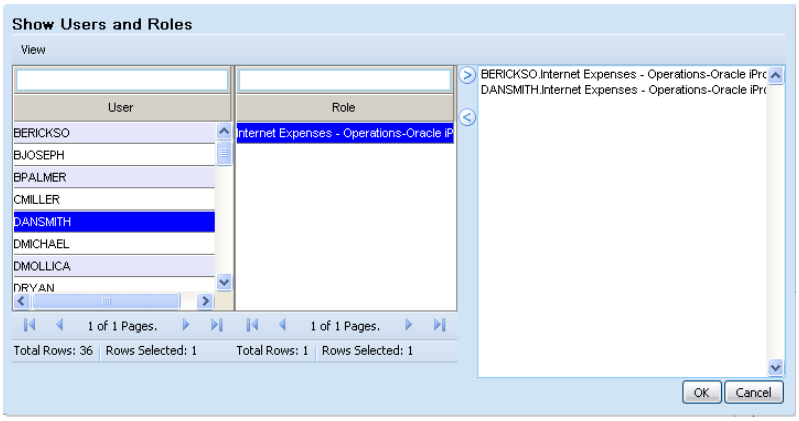
The simulation model appears as a collection of nodes, with arrows showing how each node connects to others. As you interpret this diagram, keep the following in mind:

- All nodes represent objects that lead from a user to an access point that enables the user to do something, and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.
- If you move your cursor over any of the nodes, the image displays the name of the access point that the node represents.

- If you click on any node, the arrows leading from that object are highlighted in red, distinguishing those paths from others that do not lead from the object you've selected. (In addition, if you hold your mouse cursor over an arrow linking one node to another, the arrow appears in blue, helping to distinguish it from other connections.)
- You can expand or contract the size of the image: Click on the square with a horizontal line at the upper left of the frame containing the diagram, and slide it up to enlarge the diagram (and so expose fewer of its access points to view), or down to reduce the diagram (and so expose more of its access points to view).
- Once you create a simulation model, you can clear it (thus making way to replace it with a model based on some other access point). To do so, select the Clear Model value from the Actions menu available in the Model pane.

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

1. Within the model diagram, users and roles are each represented by a single node (labeled *U* or *R*). Click on one of them.
2. In the Actions menu of the Model pane, select Show Users or Show Roles.
3. A pop-up window opens, in which a column lists users with conflicts involving the access point upon which the model is based, or roles that provide access to that access point (depending on your selection in step 2). Select (click on) one. If you've selected a user, a second column lists roles through which the user has access; if you've selected a role, a second column lists users granted access through the chosen role. Make a selection in the second column, so that ultimately you've selected a user-role combination.
4. Click on a > button to move your selection to the field all the way to the right.



5. Repeat steps 3 and 4 for each user-role combination you want in your model. If you reconsider, you can select items in the field at the right, the click on the < button to remove them from the field.
6. In the end, each entry in the field at the right displays either a user and a role assigned to her, or a role and a user assigned to it. Click on the OK button, and the simulation-model diagram redraws itself to display only access-point connections appropriate to the selected users and roles.

Developing Remediation Steps

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

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

   A record of the exclusion you created appears in a row in the Remediation Steps pane (as shown in the illustration on page 3-10). In the model diagram, the nodes you selected, and those that descend from them, are grayed out.
2. In the Remediation Steps pane, optionally click in the Comments field of the row you've added, and enter a comment about the step.
3. Repeat steps 1 and 2 any number of times to create additional remediation steps.

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

Having generated remediation steps from one graphic model, you can select another access point in the Model pane, develop another model, and create additional remediation steps from it. The steps you created from the original model remain in the simulation. (Any filters you applied to the original model, however, are not saved.)

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

Running the Simulation and Viewing Results

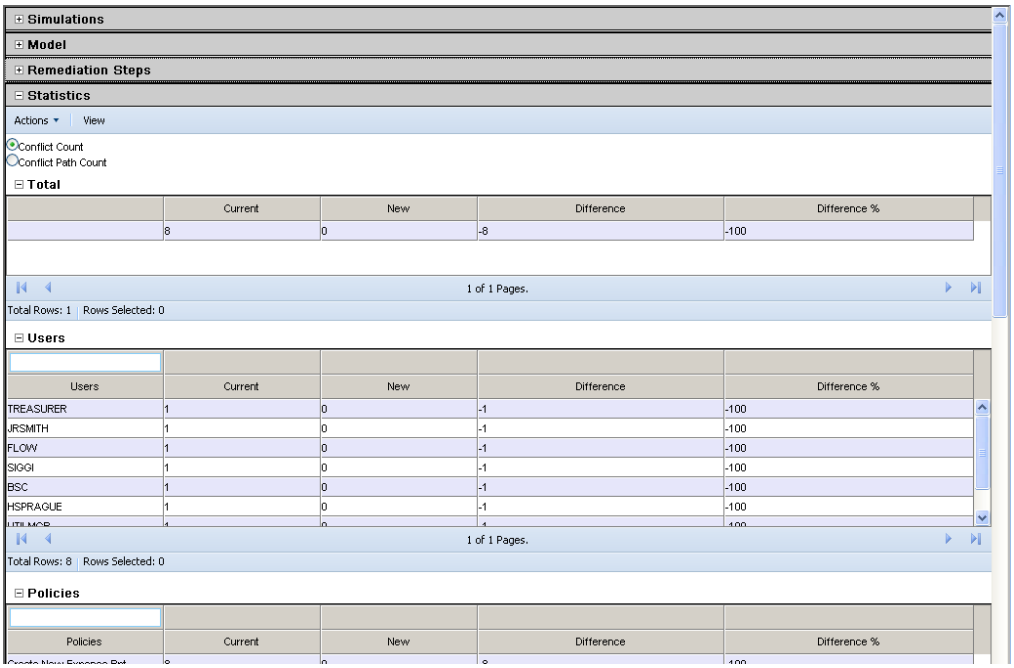
To run a simulation:

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

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

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

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



Depending on your choice, the Statistics pane displays either numbers of conflicts or numbers of conflict paths affected by your remediation plan:

- A Total grid displays the number of conflicts (or conflict paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Users grid lists the users who would be affected by remediation and, for each, states the number of conflicts (or conflict paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Policies grid lists the policies that would be affected by remediation and, for each, states the number of conflicts (or conflict paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Roles grid lists roles that would be affected by remediation. In this context, a "role" is an access point that is actually assigned to a user — in Oracle EBS, a responsibility or a role, and in PeopleSoft, a role. For each, the grid states the number of conflict paths that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage. (The Roles grid does not display results by conflict — that is, it does not appear if you selected the Conflict Count radio button.)
- A Conflict Paths grid shows all conflict paths that would be affected by the Simulation. It has User and Policy columns for easy filtering and sorting.

- A User and Role Impact lists users and roles that would be affected by the simulation. For each, a Type field tells whether the entry is a user or a role, and a User and Roles Impacted identifies the user or role. The removal of a lower-level access point from a higher-level one may not only resolve a conflict. Some users may have legitimate, unconflicted access from the higher-level point to the lower-level one, and implementation of the remediation plan would shut off that legitimate access. This grid lists both types of users (and the roles through which they have access) — those with resolved conflicts, and those with lost legitimate access.

Printing or Saving a Remediation Plan

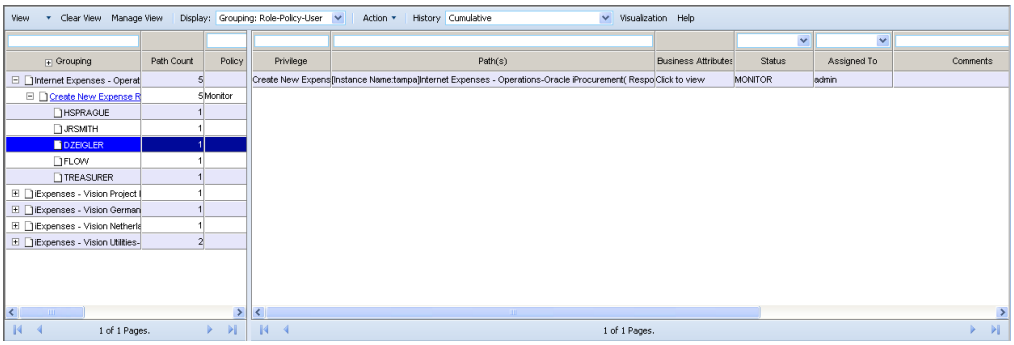
For reference — for example, for use when you actually implement a remediation plan in a business-management application — you can print a remediation plan or save it to your computer. To do so, run the simulation and then select the View Remediation plan option in the Statistics pane. You are then prompted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

Assigning Status in the Work Queue

From the Work Queue, you can select a "View" page, which lists all conflict paths, and either assign them to others or claim them for yourself. You can then open a "My Queue" page, which lists the conflict paths that you have claimed or that have been assigned to you by others, and select statuses for them.

Typically, a single user would be assigned (or would claim) all the paths to a given conflict, so that the entire conflict can be addressed in a coherent way. However, for enhanced flexibility, reviewers are assigned to individual conflict paths, so multiple reviewers can address facets of an individual conflict.

To open the Work Queue, click on its link in the Navigation panel — the third entry under Remediation in the Access Governor section:



First, select the conflict data that the Work Queue presents to you:

- Click on the downward-pointing triangle next to the View button. A list appears. In it, select View to display conflict paths that you can then assign to reviewers or claim for yourself. Click on My Queue to display paths for which you are the reviewer; you can then assign status to them. If you have defined views (page 1-5), these also appear in the View-button list. However the View and My Queue entries always appear, even if you have not defined any views.

- In the Display list box, select a hierarchy for the display of information: Role–Policy–User, Policy–Role–User, or User–Role–Policy. (See below for more on this.)

  In the Display list box, you may instead select List, which opens the Conflict Analysis page. Or you may select Conflict Path History, which opens a pane that provides information about resolved conflicts. (See "Conflict Path History" on page 3-18 for more on that topic.)
- In the History list box, choose a run of the Find Conflict program to display conflicts generated in that run, select Provisioning Requests to view only conflict data generated by the User Provisioning feature, or select Cumulative to display conflicts generated in all runs.

In both the View and the My Queue pages, objects in the left column form a list that reflects the hierarchy you select in the Display list box:

- An initial list displays the highest-level objects in your hierarchy for which conflicts exist — for example roles, if you chose Role–Policy–User. "Role" means an object that is directly assigned to a user, such as a responsibility in Oracle EBS. "User" is the global user (as defined on page 3-3).
- If you expand one of these objects, you see a subordinate list of second-level objects for which conflicts exist — for example access policies that affect the role you've expanded. (You can double-click on a policy to view its details; see page 3-6.)
- If you expand one of these second-tier objects, you see a subordinate list of third-level objects for which conflicts exist — for example, users affected by an access policy you've expanded.
- Finally, if you select a third-tier object, the right side of the page displays paths to conflicts for the specific instance of the object to which you have "drilled down."

To expand one of these objects, click on its plus-sign icon (or, to contract it, click on its minus sign). To select the object, click on it.

The left portion of each of the View and My Queue pages also has columns displaying the following values:

- For any type of object, the number of conflict paths generated for the object.
- For a role, the datasource name for the business-management application in which that role exists.
- For an access policy, the policy type (Prevent, Monitor, or Approval Required), priority, and dimension values configured for the policy.

The right portion of each page includes the columns that define conflict paths. You can select any number of paths and engage the Visualization feature (see page 3-6). Except as noted, all columns are read-only:

- Privilege displays an access point actually included in an access policy (directly or because it is a member of an entitlement that is included in an access policy).
- Path presents all the objects that lead from a role to the privilege. These might be, for example, a series of menus and submenus that lead from a responsibility to a function.
- The Business Attributes column displays parameters that are configured within the business-management application for the objects in a path — for example, the Oracle EBS set of books to which a responsibility, menus, and a function

belong. Each entry in this column reads, "Click to view"; click on one of these entries to open a pop-up window that displays its values.

- Status displays the current status of the path:
  - Prevent indicates that a user must not have the access afforded by a path. It is assigned by default to paths generated by policies of the Prevent type.
  - Monitor indicates that a user is permitted the access afforded by a path, but that access should be re-examined periodically. It is assigned by default to conflict paths generated by policies of the Monitor type.
  - Pending indicates that no decision has yet been made, and is assigned by default to conflict paths generated by policies of the Approval Required type.
  - Approved indicates that a user may have free access to a path.
  - Rejected indicates that a user must not be allowed access to a path.

  You can use this field to reset the default status of any path at the Monitor, Pending, Approved, or Rejected status, and each can be changed to any of the other three. However, you can do so only from the My Queue page. The Prevent status can be assigned only by AACG, and only to conflict paths generated by a Prevent policy; this status cannot be changed.
- The Comments column displays an explanation for an assignment of a path to a reviewer or a reviewer's status decision. You can set this field from the View or My Queue page.
- The Entitlement column displays the name of the entitlement (if any) that was used by the policy that generated this conflict path, and contains the privilege included in this conflict path.
- Assigned To identifies the user who is expected to select a status for the path. This reviewer is initially the first-to-act participant configured for the policy that generated the conflict path (or, if that participant is a group, its "primary" member). You can reset this value (either assigning the path to another user or claiming it for yourself), from either the View or My Queue page.
- Approved By identifies the user who approved the conflict if that approval occurred in the User Provisioning Requests page. (This user may differ from the one identified in the Assigned To column if the first-to-act participant is a group. In that case, the Assigned To field displays the "primary" member of the group, but the Approved By may be any member of the group.)
- Approved displays the date of the approval, if that approval occurred in the User Provisioning Requests page.
- Type displays the value *ANALYSIS* if status for the conflict path is to be set in the Work Queue, or *AUTHORIZED* if status has been set through User Provisioning.

You can double-click on the row for a path to display a history of changes made to the reviewer assignment or status of that path.

Assigning Paths to Yourself or to Others

To assign a path to another user or claim it for yourself:

1. Select the View page (see page 3-14).

2. Use the Display list box to select the hierarchy with which you want to work. For example, if you know that you want to assign someone to review conflicts generated for a particular user, you might select User-Role-Policy.
3. In the left portion of the page, drill down (page 3-15) to a particular set of conflict paths, which appears in the right pane. Select (click on) one or more of the paths (using the Ctrl or Shift key as you click to select multiple paths).
4. Click on the Action button in the tool bar at the top of the page.
5. A list appears. In it select Claim to assign the path to yourself. Or, select Assign to assign it to someone else. In the latter case, an Assign to User pop-up window appears. Select a user in its list box, optionally add a comment, and click on its OK button. In either case, the username of the user assigned to review the path appears in the appropriate cell of the Assigned To column. The assignment is saved automatically.

As you assign status to paths, you may choose to reassign any number of your paths to other users. See the next section, "Assigning Status to Paths."

Assigning Status to Paths

To set the status for a path you have been assigned.

1. Select the My Queue page (see page 3-14).
2. Use the Display list box to select the hierarchy with which you want to work. For example, if you know that you want to set status for conflicts generated by a particular policy, you might select Policy-Role-User.
3. In the left portion of the pane, drill down (page 3-15) to a particular set of conflict paths, which appears in the right pane.
4. In one of the paths that appear in the right portion of the page, do one of the following:
   - Click on the Status column. A list box appears; in it, select the status you want to assign to the path. (See page 3-16 for a description of status options.)
   - Click on the Assigned To column. A list box appears; in it, select a user to whom you wish to reassign the conflict path.
5. In that same path, single-click in the Comments field and type a brief explanation of your approval or reassignment decision.
6. Repeat steps 4 and 5 for other paths on display.
7. When you have finished assigning statuses to paths, click on Action in the tool bar, and then Save in the Action list. (Alternatively, you can click on Cancel in the Action list to void your status decisions and start over again.)

As an alternative, you can set status for any number of paths at once:

1. Perform steps 1–3 in the previous status-assignment procedure.
2. Select a set of paths. Hold the Ctrl key as you click on a discontinuous set, or click on a path, press the Shift key, and click on another path to select a continuous set.

3. Click on Action in the tool bar, and then Mass Edit in the Action list.
4. A Mass Edit pop-up window appears. In its list box, select the status you want to assign.
5. Click on the Save button in the Mass Edit pop-up window. The window closes, and the new status assignments are saved.

Conflict Path History

AACG no longer detects a conflict once actions have been taken to resolve it in a business-management application (such as Oracle EBS or PeopleSoft). The Conflict Path History page displays records of such resolved conflicts. Each row represents a path to a conflict that had been detected in a run of the AACG Find Conflicts program, but was not detected in a subsequent run. Each record comprises these values:

- Original Run ID: An identifier (assigned by AACG) for the Find Conflicts run in which a path was first determined to belong to a conflict.
- Run ID: An identifier for the last run of the Find Conflicts program in which that conflict path continued to be detected.
- Remediation Run ID: An identifier for the first run of the Find Conflicts program in which that path was no longer detected.
- Remediation Date: The date of the Find Conflicts run identified by the remediation run ID. That is, the date on which the Find Conflicts program no longer detected the conflict it had found in an earlier run.
- Updated Date: The last date on which the conflict path was updated in AACG, through the assignment of the path to a reviewer, the assignment of a status to the path, or the creation of a comment about the path.
- Assigned To: The AACG user (if any) who was assigned to select a status for the conflict path.
- Comments: The comments (if any) created for the conflict path in AACG.

To open the Conflict Path History page, select Conflict Path History in the Display list box of the Work Queue. To quit the Conflict Path History page, select any other value in the Display list box. While the Conflict Path History page is open, other menu options (View, Action, and History) are unavailable.

Using the Heat Map

A Heat Map enables analysts to prioritize the resolution of conflicts by determining where the greatest numbers are being generated. It sorts conflicts according to user-selected parameters, and displays the results graphically. The analyst selects two parameters to produce an initial sort. She then chooses one set of the conflicts returned by that sorting and applies an additional parameter to it, to focus results more narrowly. She may repeat this process, producing still more finely focused results.

For example, the initial parameters may be priority and conflict status, and these would produce a grid in which cells display the number of conflicts existing at each combination of status and priority. An analyst may then select one cell in that grid

— in this example, the conflicts existing a particular status (say, Pending) and a particular priority (say, 2). She would then apply another parameter to that set of conflicts. If that parameter were, for example, policy, the result might be a bar graph showing the number of second-priority, pending conflicts generated by each access policy. She might then apply another parameter — say, user — to the conflicts generated by one of those policies, but at this final sort have the Heat Map open the Work Queue, which would display only the second-priority, pending conflicts at the selected policy, sorted by user. The ultimate purpose of the Heat Map is to produce an instance of the Work Queue that displays only the conflicts to which the analyst has "drilled down," so that they may be assigned or reviewed.

As you use the Heat Map, you may sort conflicts according to these parameters:

- Policy. Each set of conflicts returned in response to this parameter is generated by a particular access policy.
- User. Each set of conflicts returned in response to this parameter applies to a particular user's work assignments. The Heat Map displays global users (as defined on page 3-3). Note that Policy and User are not a good parameter pair to select. Because a conflict is defined as a user violating a policy (no matter how many subpolicies or conflict paths are involved), this would always produce a display in which every cell or bar is set to the value *1*, and so there would be no distinction among sets of conflicts.
- Entitlement. Each set of conflicts returned in response to this parameter is generated by an access policy that uses a particular entitlement.
- Role: Each set of conflicts returned in response to this parameter applies to users assigned a particular role (the level of object assigned directly to a user, such as an Oracle responsibility).
- Priority. Each set of conflicts returned in response to this parameter is generated by an access policy assigned a particular priority (see step 2 in "Adding an Access Policy" on page 2-5.)
- Conflict Status. Each set of conflicts returned in response to this parameter exists at a particular status.

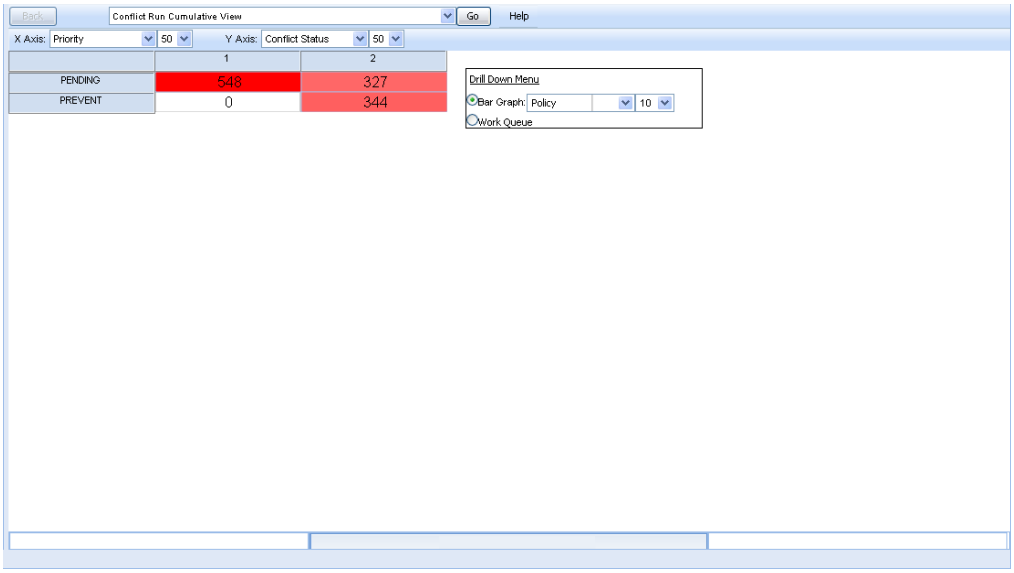
  Status is assigned at the conflict-path level, so the following logic determines the status of an entire conflict: All paths to a conflict generated by a Prevent access policy exist at the Prevent status, and cannot be changed, so the conflict itself is also at the Prevent status. For conflicts generated by Monitor or Approval Required policies, statuses are ranked: Approved, then Monitor, then Pending, then Rejected. The conflict as a whole takes the highest-level status assigned to any of its paths.

  For example, if an Approval Required conflict has three paths, the status of all three, and of the conflict as a whole, is initially Pending. If an analyst rejects one path and leaves the other two pending, the conflict status is still Pending. If he approves a second path, the conflict status becomes Approved (even though the first path was rejected and the third remains pending). The conflict status would be Rejected only if all three paths were rejected.
- Dimension. The Heat Map creates a parameter for each dimension configured for your AACG instance. Each set of conflicts returned in response to one of these parameters would correspond to one of the values configured for the dimension.

To use the Heat Map:

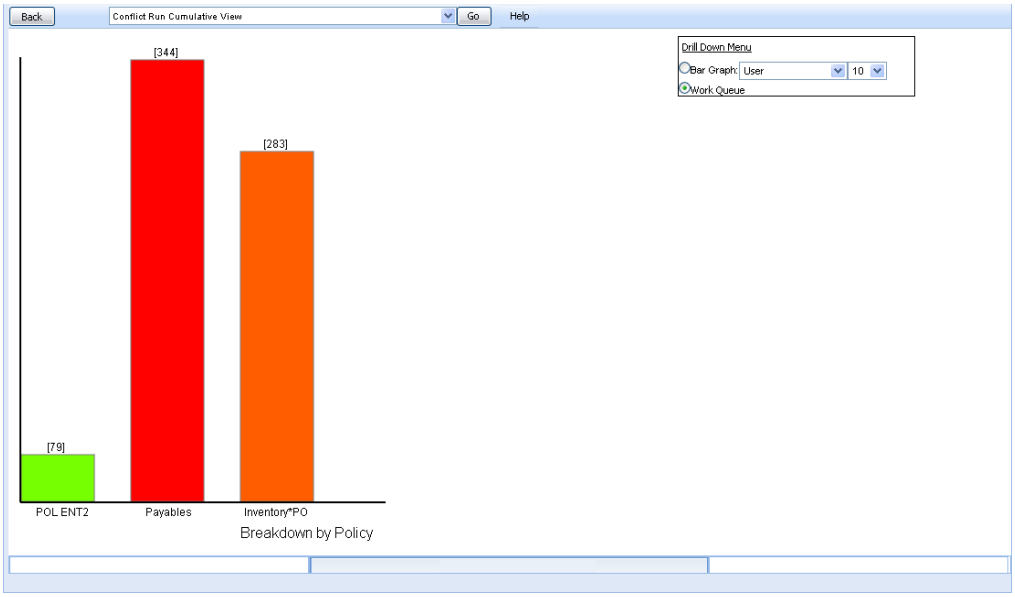
1. Open the Heat Map: Click on Access Governor > Remediation > SOD Heatmap, in the Navigation panel.
2. Accept default values for the initial sort, or select new values. By default, the Heat Map returns cumulative results (a view of conflicts generated by all runs of the Find Conflicts program) sorted by Policy versus Conflict Status, displayed in a grid with a maximum of 50 rows and 50 columns. To choose new values, do any of the following:
   - Select an individual Find Conflicts run from the list box at the top of the Heat Map.
   - Select new sort parameters in the X-Axis and Y-Axis list boxes. (X-Axis parameter values are displayed horizontally as the headings of columns. Y-Axis parameter values are displayed vertically as the headings of rows.)
   - Select new maximum numbers of entries along the X axis and Y axis in the list boxes next to the parameter-selection list boxes.

   When you have finished making selections, click on the Go button. No matter whether you accept defaults or select new values, the Heat Map displays a grid like the following one. Each cell corresponds to one pair of values for the parameters you've selected and displays the number of conflicts that satisfy those values (for example, 548 conflicts at the Pending status with a Priority of 1). The greater the number of conflicts, the more brightly red the cell is colored.



3. In the Drill Down Menu box, select another parameter. (You can select only parameters you have not already selected in an earlier sort.) Also select the maximum number of sets of conflicts you want to see for that parameter. Finally, select either the Bar Graph or Work Queue radio button. Typically, you would select Work Queue only if you are making your final parameter selection.
4. Click on a cell in the grid that corresponds to a set of conflicts you want to examine more closely. If you selected Bar Graph in the Drill Down Menu box, the result is a display like the one below. Each bar represents one of the values for the parameter you selected in step 3, and displays the number of conflicts that satisfy

that value (for example, 344 conflicts generated by a policy called Payables, all, of course, at the priority and status defined by the cell on which you clicked). Again, the greater the number of conflicts, the more brightly the bar is colored.



5. From a bar graph, you may refine results further: Select another parameter (and maximum number of sets of conflicts) in the Drill Down Menu, then click a bar that corresponds to a set of conflicts you want to examine. Do this as often as you wish until you exhaust all parameters. For your final selection, choose Work Queue in the Drill Down Menu. This opens an instance of the Work Queue that displays only the conflicts to which you have drilled down. Use this instance of the Work Queue as described in "Assigning Status in the Work Queue" (page 3-14).

User Provisioning

User Provisioning implements "preventive" enforcement, applying access policies to each user as he is assigned responsibilities in the User form of Oracle E-Business Suite, or roles in the User Profile page of PeopleSoft Enterprise. Results depend on what (if any) policies are violated:

- If there is no conflict, or if an assignment violates a Monitor policy, the assignment is allowed. In the Oracle Users form, an end date in the future (or no end date) may be configured for responsibilities assigned to the user. In PeopleSoft, roles remain added to the user's list in the Roles tab of the User Profile page.
- If an assignment violates a Prevent policy, it is rejected. In Oracle, the newly added responsibility is end-dated. In PeopleSoft, the newly added role is deleted from the user's list of roles.
- If an assignment violates an Approval Required policy, it is suspended. Notifications are sent to policy participants, who use a User Provisioning Request page in AACG to approve or reject individual responsibilities or roles involved in the conflict. End dates are removed from approved responsibilities, but kept for those that are rejected; approved roles are restored to a PeopleSoft user's list, and rejected roles are not.

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

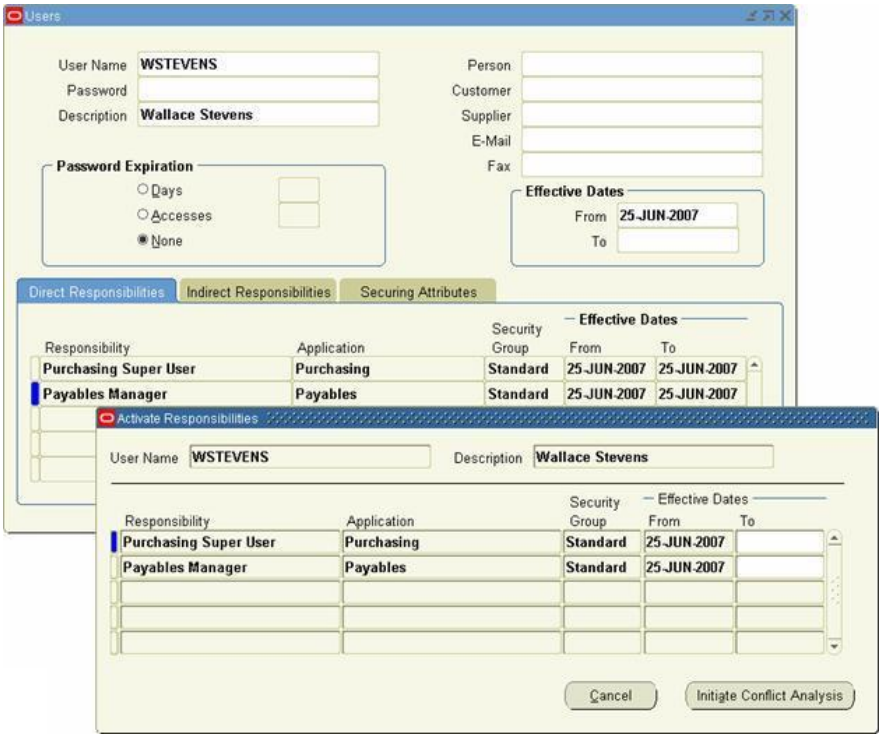
For an Approval Required conflict, participants in the policy that generated the conflict receive notification at the email address provided for each participant in the Email Address 1 column of the GRCC User Administration page. Notifications are consolidated: each participant receives one message for all conflicts awaiting her review. For any conflict, notification of the enforcement outcome is sent to the user who has been prospectively assigned new duties, at the email address associated with the user in the business-management application.

A User Provisioning Administration page in AACG displays a history of assignments that violate access policies of any type.

Assigning Responsibilities in Oracle EBS

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

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



3. In the Activate Responsibilities form, the administrator removes end dates (or alters them to a future date) for a selection of responsibilities, and so provisionally grants access to them. He then clicks the Initiate Conflict Analysis button.

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

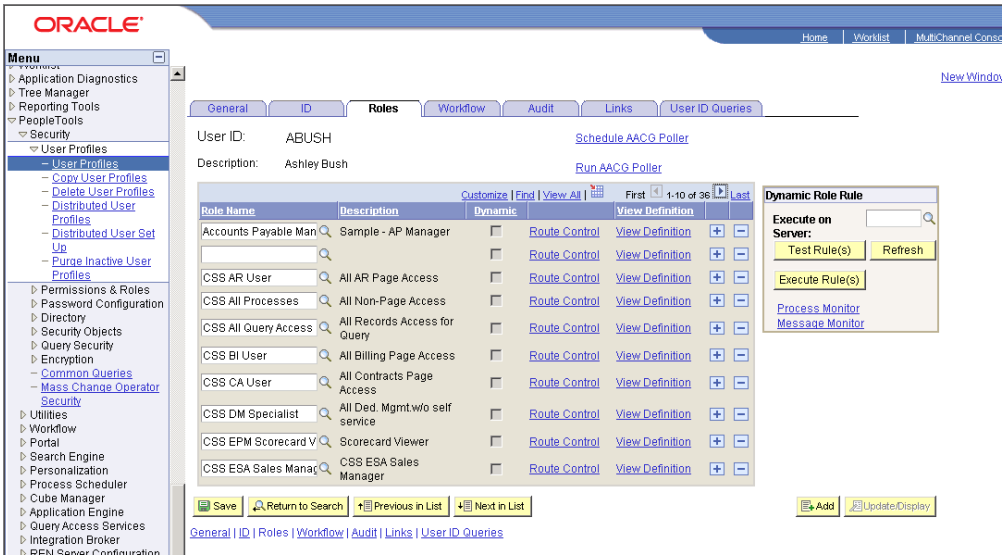
   Within Oracle EBS, a concurrent request called AACG User Provisioning Poll handles approvals and rejections; it runs periodically, but may be run manually (it takes no parameters). An AACG web service initiates conflict analysis in the AACG engine. At this point, policy participants may review any type of conflict in the AACG User Provisioning Administration page, or Approval Required conflicts in the AACG User Provisioning Requests page (see "Responding to Notifications," page 3-24).

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

Assigning Roles in PeopleSoft

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

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



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

The Roles pane of the User Profiles page returns, but newly added roles have been removed if they are involved in conflicts. At this point, policy participants may review any type of conflict in the AACG User Provisioning Administration page, or Approval Required conflicts in the AACG User Provisioning Requests page (see "Responding to Notifications," page 3-24).

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

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

Although the Run AACG Poller link is activated from a specific user's instance of the Roles pane, it updates role assignments for all users whose role assignments have been resolved in AACG. The Schedule AACG Poller link causes the poller to run regularly at an interval specified in a pea.properties file (which is configured during installation; see the *Governance, Risk and Complicance Controls Installation Guide* for version 8.5.) When you select this link, a message states "Successfully started the poller"; click its OK button to clear it. Once selected, the link becomes inactive.

Responding to Notifications

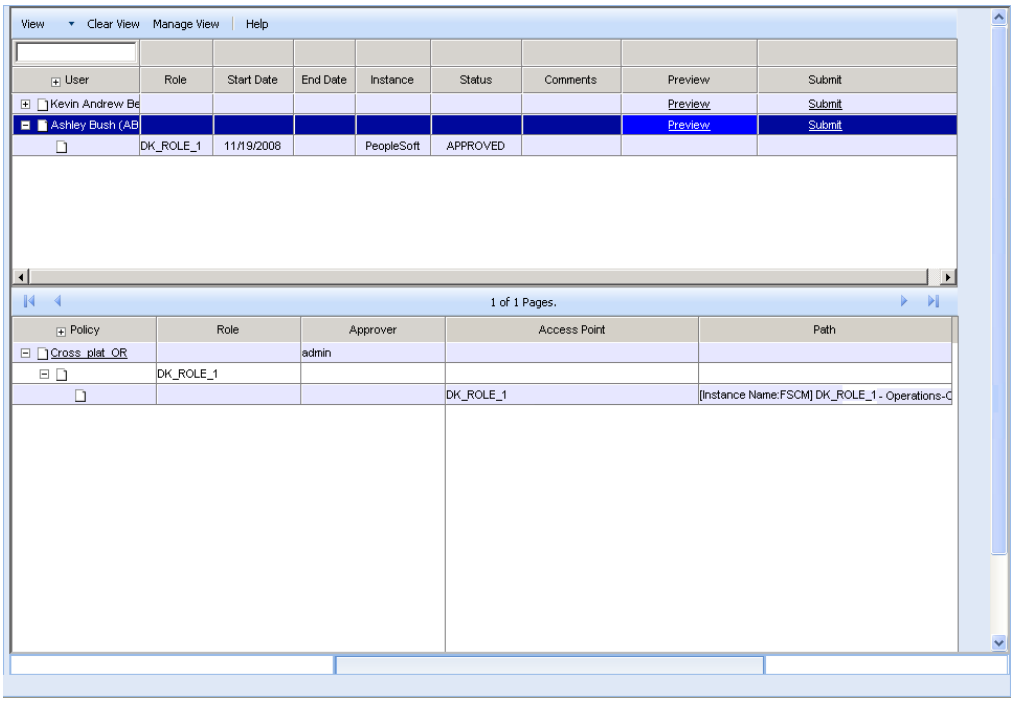
When a response is required — that is, when an Approval Required policy has been violated — the approver can respond in the User Provisioning Requests page. The approver is the first-to-act participant designated in the policy that generated the conflict. If this participant is an individual, he has exclusive authority to approve or reject User Provisioning requests generated by his policy. If the participant is a group, any member may approve or reject the User Provisioning request, but the first one to do so acts for all; other members cannot act after the first member has.

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

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

To approve or reject a request:

1. Locate and click on the Requests entry in the Navigation panel. It's the first entry in the User Provisioning section.
2. The Requests page opens. Its top portion displays rows containing the IDs of users whose assignments have violated policies for which you are the first-to-act participant. Locate the user whose assignment you wish to review, and click on the + symbol next to his name.



3. One or more subordinate rows appear. Each shows a role provisionally assigned to the user, its start and end dates, the EBS or PeopleSoft instance on which the role is assigned, and the assignment status (set initially to Pending). In the Status field of each row, select Approved or Rejected. Optionally, type a comment about your decision in the Comments field.
4. If you set the status for any role to Approved, click on the Preview prompt (in the Preview column of the parent row that identifies the user). The lower half of the page then displays records of paths to the access points included in the conflict. Each identifies the violated policy, the objects that define the conflict path (the assigned role, the access point included in the policy, and path leading from one to the other), and the approver. (If you set the conflict status to Rejected, the Preview feature does not apply, and an attempt to run it produces a warning.)

   After reviewing conflict paths, you may determine that you should reject the conflict. If so, change the status in the upper half of the Request page to Rejected.
5. When you have set status for all provisionally assigned roles to Approved or Rejected, click on the Submit prompt (in the Submit column of the parent row that identifies the user, in the upper half of the page). The user's record then disappears from the Requests page.

Creating Participant Groups

A participant group is a set of AACG users who review conflicts generated by access policies to which the group is assigned. For each policy, one participant (individual or group) is designated as "first to act":

- This participant approves or rejects User Provisioning requests generated by the policy. If the participant is a group, any member may approve or reject a request, but the first to do so acts for all members.
- The first-to-act participant is also the default "Assigned to" user when conflict paths generated by the policy appear in conflict-analysis tools other than the User Provisioning Requests page (such as the Conflict Analysis page and the Work Queue). If the participant is a group, this default user is an individual identified as the "primary" member of the group.

Participants (individual or group) who are not first to act may receive email notifications that their policies have generated conflicts, but do not resolve User Provisioning requests or (by default) set status for conflict paths in the Work Queue.

To configure a participant group:

1. Locate and click on the Participant Groups entry in the Navigation panel. It's the second entry in the User Provisioning section.
2. The Participant Groups page opens. In its upper half, click on the Add button, and a new row appears.
3. Click on the Group field in the new row, and type a name for the group.
4. Ensure that the Active check box is selected to make the group available for use (or clear the check box to withhold it from use).
5. In the lower half of the Participant Groups page, click on the Add button. A new row appears.
6. Click on that row. A list appears; from it, select an AACG user who has been assigned an AACG role with access to the User Provisioning Requests page.
7. Repeat steps 5–6 for each additional user you want to include in the group.
8. Select the Primary radio button in the row for the AACG user who is to serve as primary group member. You must select one, and you cannot select more than one; each time you make a new selection, the earlier selection is cleared.
9. When you finish adding members, click on the Save button in the upper half of the Participant Groups page. A Records Saved pop-up window appears; click on its OK button to clear it.

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

User Provisioning History

The User Provisioning Administration page displays records of all users whose responsibility assignments violated access policies of any type. When a user's assignments violate Prevent or Monitor policies, the status of those assignments is set, respectively, to Rejected or Approved. When a user's assignments violate

Approval Required policies, their status is set initially to Pending. Once the conflict is resolved in the Requests page, the user's records disappear from there, and her responsibility-assignment statuses are reset in the Administration page to the values (Approved or Rejected) selected in the Request page.

Users with view permission to the User Provisioning Administration page can review approval history. Users with update permission to this page can both review history and reject User Provisioning requests at the Pending status; other statuses cannot be updated. The assumption is that such users would reject Pending roles only under extraordinary circumstances (for example, the first-to-act participant for a policy has resigned from the company), and that update rights to the User Provisioning Administration page would be granted sparingly. (View and update rights are, of course, determined by roles assigned to AACG users.)

To open the User Provisioning Administration page, click on Administration in the Navigation panel, and then on the User Provisioning Administration entry in the Administration list.

Use the User Provisioning Administration page essentially in the same way as you would use the upper half of the Requests page:

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

4

Reporting

From each of several pages, or from a Report Center, you can run reports that document your use of Application Access Controls Governor.

Choose a Policy Report

The Access Policy Detail Report provides the following information about each in a selection of access policies: the name, description, policy type, priority, effective date, and status, as well as the number of conflicts it has most recently generated. It also lists the access points or entitlements that belong to the policy and their AND/OR relationships to one another, the policy participants, and any conditions defined for it.

Choose a Conflict Report

Several reports provide information about conflicts generated by access policies:

- The Access Violations Within a Single Role Report lists roles for which access policies generate "intra-role" conflicts. These are conflicts between privileges granted within a given role, so that the role cannot be assigned to a user without a conflict occurring. (In this context, "role" means an Oracle role or responsibility, or a PeopleSoft role.) For each such role, the report also lists the access policies that define its intra-role conflicts.
- The Intra-Role Violations by Policy Report lists access policies that generate intra-role conflicts. For each policy, it also lists the roles for which the conflicts are generated. (Once again, "intra-role conflicts" are those involving privileges granted by a single role, and "role" means an Oracle role or responsibility, or a PeopleSoft role.) In effect, this report reverses the sort order of the Access Violations Within a Single Role Report.
- The Access Violations by User Report lists the ten users with the greatest number of conflicts, as well as the number of conflicts for each. It then provides details of the conflicts for each user. Details include policies violated by each user's work assignments (including the type, priority, status, effective date, description, and comments configured for each policy), and the subpolicies (pairs of access points included within the policy) that have been violated.

- The Users with Access Violations by Policy Report lists access policies that have generated conflicts. For each policy, it lists users whose work assignments have violated the policy. For each user, the report supplies both the global user ID and the user's full name.
- The Access Point Report lists paths to access points involved in conflicts. Each path expresses the hierarchical relationship between a "parent" object that can be assigned to a user (such as an Oracle responsibility), a "child" access point that is included in an access policy and involved in a conflict (such as an Oracle function), and the objects that lead from one to the other (for example, menus and submenus that lead from a responsibility to a function). For a given access point, each record in the report is not a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
- The Access Conflicts Extract Report produces a file that contains records of conflict paths. Each record contains information corresponding to values displayed in the Conflict Analysis page. The report displays data in Microsoft Excel, in which you can perform further analysis. As you run the report, you must select the Excel output format.

Choose a User Provisioning Report

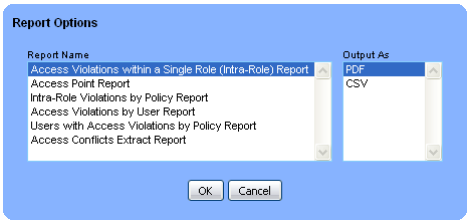
The Access User Provisioning Report displays records of provisioning requests sorted by status (approved, pending, or rejected). A request occurs when a user is provisionally assigned duties after an Approval Required access policy has been created to define them as conflicting. The request is resolved at the User Provisioning Requests page by the first-to-act participant designated for the policy that generated the conflict. Each record in the report specifies the user for whom access has been requested, the roles requested for that user, the business-management-application instance on which they were requested, the date on which the access request was made, and the dates on which access would begin and end. To run or schedule the report, click on Report Center in the Navigation panel, then on User Provisioning Reports in the Report Center list, and then on Access User Provisioning Report.

Running Reports

To run reports from a page:

1. Open the page — Definition or Conflict Analysis — that provides access to the report you want to run (The Access User Provisioning Report can be run only from the Report Center — see page 4-3).
2. Optionally, create a view (see page 1-5) to generate a report that displays information only about items included in the view. (If you do not create a view, the report displays information about all possible items).
    - In the Definition page, you can create views to select policies included in the Access Policy Detail Report.
    - In the Conflict Analysis page, you can create views to select conflict paths included in reports (for example, those involving particular users, or specified roles or privileges).

3. In the tool bar at the top of a page, click on the Reports button. This opens a Report Options pop-up window:

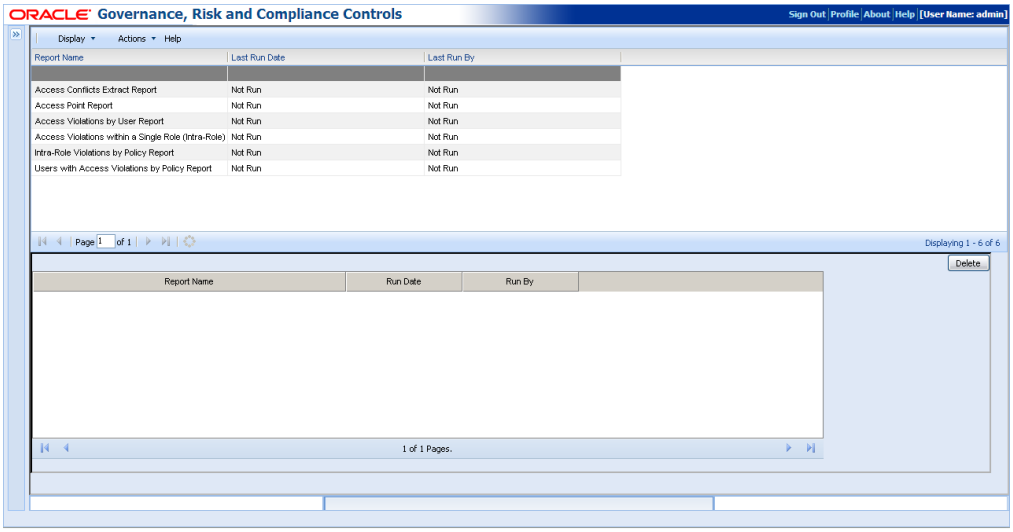


4. In the Report Name field, click on the report you want to run. In the Output As field, click on the format in which you would like to generate the report. You can make only one selection at a time in each field. In the Output As field:
   - CSV generates a text file that you can use to import report data to another application, such as a spreadsheet program.
   - PDF generates the report as an Adobe Acrobat file.
5. Click on the OK button. A File Download window prompts you to open or to save the report. If you select Open, the report opens directly; if you select Save, a Save As dialog enables you to use standard Windows techniques to navigate to a folder in which you want to save the report and give it a meaningful name.

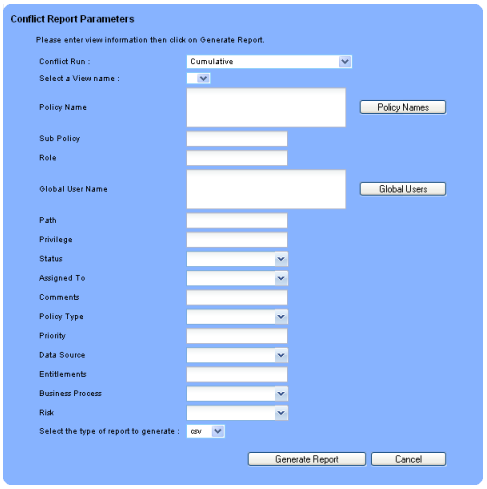
Using the Report Center

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

1. Open the Report Center. In the Navigation panel, click on the Report Center link and then on Policy Reports, Conflict Reports, or User Provisioning Reports.
2. A page like the following one opens. In it, click on the row for the report you want to run (or to schedule).



3. With the report selected, click on Actions in the tool bar. In the two-item list that appears, click on either Run Now or Schedule.
4. A pop-up window appears; in it, select parameter values.

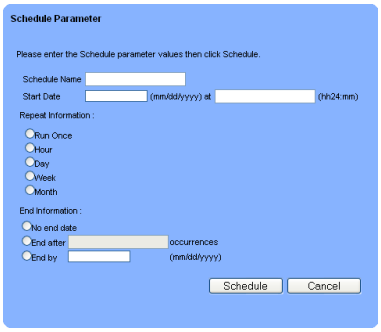


In general, parameters correspond to the selections you make as you create or otherwise work with the object on which you are reporting. As you set parameters, you would select among the same values.

For example, if you configured a view in the Definition window, you can select that view to have the Access Policy Detail report display information about policies that belong to the view. Or you can select a policy name to have the report apply only to that policy. Each of the Policy and Conflict parameter windows also list dimensions you have created; you can select one or more values for each dimension to report on only the policies or conflicts assigned those values. You can also select the format in which the report should be generated — PDF (Adobe Acrobat file) or Excel (for viewing in an Excel spreadsheet).

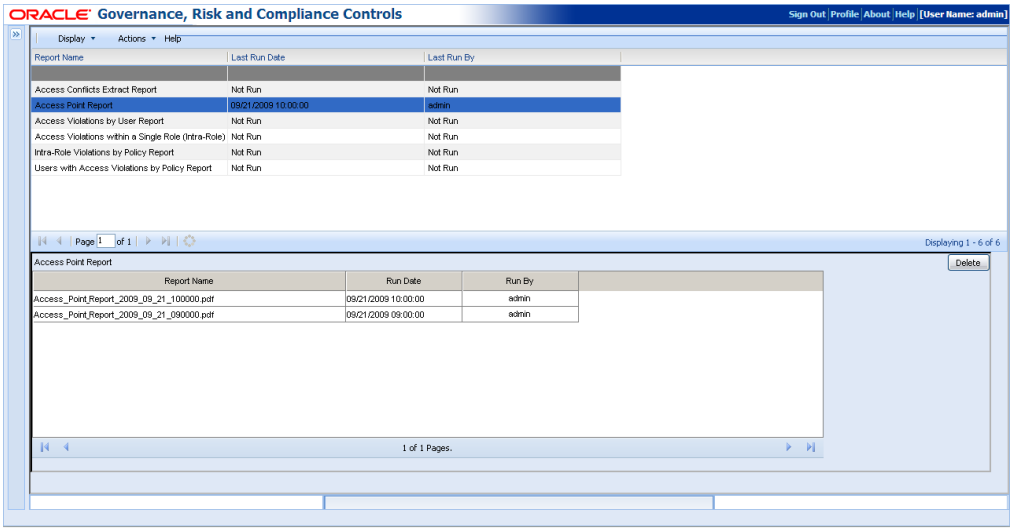
If you are scheduling a report to be run, you must select a view as a parameter (and may select other parameters as well).

5. If you selected Run Now in step 3, the parameter window displays a Generate Report button; click on it to generate the report. If you selected Schedule in step 3, this button is replaced by a Schedule Information button. Click on this button to produce the following Schedule Parameter pop-up window, and to schedule the report to run:



Enter values that set a name for the schedule, the date and time at which it starts, the regularity with which the report runs, and the date and time (if any) on which the schedule expires. Then click on the Schedule button.

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



To view a report generated on a schedule:

1. In the top portion of the Report Center, click on the title of the report you want to see.
2. Click on Display in the tool bar in the top portion of the Report Center, and then on Report History in the list that appears.
3. In the bottom portion of the Report Center, double-click on the instance of the report you want to see.

To view the schedule on which the report was generated:

1. In the top portion of the Report Center, click on the title of the report whose schedule you want to see.
2. Click on Display in the tool bar in the top portion of the Report Center, and then on Scheduled Reports in the list that appears.
3. In the bottom portion of the Report Center, a row displays summary information about the schedule, including its most recent and next scheduled run times.
4. Double-click on the row to reopen the Schedule Parameter pop-up window. Here, you can re-enter schedule values and select a ReSchedule button, or turn off the scheduling by selecting an UnSchedule button.

Report Templates

In addition to the reports accessible through the Report Center, Oracle offers report templates, from which you can develop custom AACG reports. These run in Oracle Business Intelligence Publisher, or BIP, and are separate from the Report Center reports. For more information on report templates, see the *GRCC Reporting Framework: BIP for GRCC Admin/Implementation Guide*.)