Oracle® Governance, Risk, and Compliance Controls Suite

Transaction Controls Governor User Guide

Release 7.2.3

June 2008

ORACLE

Oracle Transaction Controls Governor User Guide

Primary Author: David Christie

Contents

1

Introduction

Oracle Governance, Risk, and Compliance Controls Suite documents and enforces business controls, enabling users to demonstrate regulatory compliance and to promote operational efficiency. It provides a "control library" in which users describe and catalog controls as well as other items that establish the business context in which controls exist.

Control Monitors and Workflows

The Governance, Risk, and Compliance Controls Suite includes modules that automate the enforcement of controls. One of these is Transaction Controls Governor, which enables users to create "control monitors," "workflow routings," and "workflow definitions":

- A control monitor employs one or more statements, written in structured query language (SQL), that define actions subject to control. It establishes a sequence in which the statements are evaluated and the records they return are designated as "suspect tasks." Each monitor, once configured, is attached to a control definition written in Governance, Risk, and Compliance Controls Suite.

  Transaction Controls Governor enables you to create control monitors one at a time or to import "prepackaged" control monitors.

- A workflow routing selects sets of users, user groups, or both, and establishes a sequence in which they receive requests to review suspect tasks. The routing can designate users or groups with authority to "pass" a suspect or declare it an "exception," and others who are notified of decisions made about the suspect.

- A workflow definition associates a workflow routing with any number of controls. Suspects generated by control monitors attached to those controls become subject to review by the users and groups specified in the workflow routing.

Access Monitoring

It is occasionally necessary to assign users temporary access to duties they do not perform ordinarily. The Access Monitoring feature implements a process for requesting extraordinary access to Oracle responsibilities or database tables, and requires

requests to be approved by designated reviewers. Like control-monitor suspects, Access Monitoring requests are routed to reviewers by workflow routings and workflow definitions. Once approval is granted, Access Monitoring audits all actions taken by users at their temporary duties, and presents the audit data in a report.

Starting Transaction Controls Governor

Transaction Controls Governor is a web-based application designed to run in the Microsoft Internet Explorer web browser. To start Transaction Controls Governor:

1. Open your web browser.
2. In the Address field, type the URL for your instance of the Governance, Risk, and Compliance Controls Suite, and press the Enter key.
3. A Sign In dialog box appears. Type your user name and password, and click on the Sign In button.

4. The Governance, Risk, and Compliance Controls Suite opens.
   - To create control monitors or workflows, click on the Control Automation tab.
   - To create Access Monitoring requests, click on the Access Monitoring tab. A Select Datasource panel prompts you to choose among instances of databases that store Oracle E-Business Suite data, and to which access requests may be applied. Select a database instance in the list box and click on the Select button.

     An Access Monitoring panel opens. The database instance you selected is displayed near the upper center. You can select another database instance: click on a Change link near the upper center of the panel to reopen the Select Datasource panel.

Access to Features

Each user is assigned a “primary application role” when his user account is created in the Governance, Risk, and Compliance Controls Suite. Your access to features in Transaction Controls Governor depends on the role you have been assigned:

- An Author, SOD Super User, Manager, or Rule Builder has full access, and so can view, create, or alter control monitors, workflow routings, or workflow definitions.

- An Auditor, Executive, System Administrator, or User can view these items, but cannot create or modify them (and an SOD Approver has no access).
- An Author, Manager, Rule Builder, SOD Super User, Executive, User, or System Administrator can create Access Monitoring requests. An Auditor can view, but not create, requests, and an SOD Approver has no access.

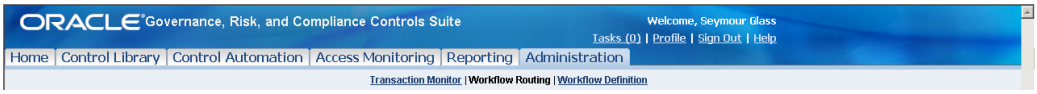
This manual is written in the assumption that you have full access rights. Be aware that, depending on your role, you may only have only view rights, or no rights, to the options described in this manual.

Navigational Conventions

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

Library Navigator

When you click on the Control Automation tab, Transaction Controls Governor opens a panel that displays existing control monitors, enabling you to view them, edit them, or create new monitors. However, you also have access to related tasks — the configuration of workflow routings and workflow definitions. A "Library Navigator" — a horizontal string of links near the top of the Control Automation panel (beginning with the phrase *Transaction Monitor* in the figure below) — provides access to these related tasks. Click on any of the links to open screens that support those tasks.

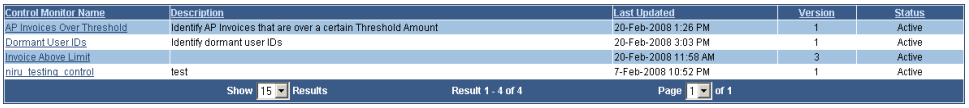


Breadcrumbs

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

Sorting and Selecting Items in Lists

Several panels in Transaction Controls Governor present lists of items — control monitors, workflow routings, or workflow definitions.



Each of these lists implements the following conventions:

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

2

Monitors and Workflows in Principle

A control monitor is one of several elements that may enforce a control defined in the Governance, Risk, and Compliance Controls Suite. When used, a control monitor is attached directly to the control it enforces.

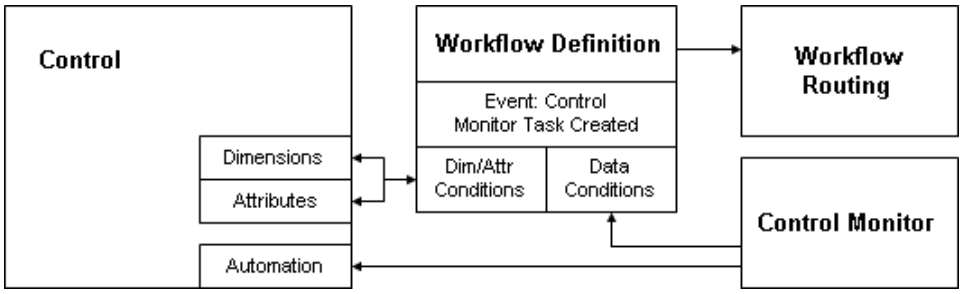
A workflow routing may be linked directly to one or more control monitors, and so its members would review suspects generated by those monitors.

Alternatively, a workflow routing may be associated indirectly with controls (and so with suspects generated by monitors attached to those controls), or with Access Monitoring requests. In such a case, a workflow definition serves as the intermediary, by specifying events, conditions, and a priority:

- An event is the circumstance that triggers the distribution of messages to users or groups named in the workflow routing. Although there are many events, only one — "Control Monitor Task Created" — triggers the review of suspects generated by control monitors. Two others — "DB User ID Requested" and "E-Business User ID Requested" — apply to Access Monitoring requests. (All others apply to controls and related objects created in the GRC Controls Suite platform.)
- Dimension/attribute conditions enumerate a set of dimension and attribute values. Each control is configured to have dimensions (segments of your business environment in which a control is used) and attributes (values that may describe the qualities or nature of a control). So dimension/attribute conditions select the controls to which the workflow routing applies — those configured with a corresponding set of dimension and attribute values.
- Data conditions filter the suspects returned by a control monitor. Each specifies a value that may be held in a column of a suspect record, so that only suspects with the specified values are selected.
- Data source conditions identify database instances in which user-access requests are to be implemented.
- The priority determines which workflow routing is used when more than one might otherwise apply to a suspect. (See "Combining Priorities and Conditions in Workflow Definitions," below.)

A Simple Workflow Example

The following figure illustrates how a control, control monitor, workflow routing, and workflow definition may work together to distribute suspect tasks for review:



In this example:

- The control monitor generates suspect tasks. It's attached to the control as an "automation."
- The control specifies a set of dimensions and attributes.
- The workflow definition specifies a matching set of dimension/attribute conditions. It also has the Control Monitor Task Created event. So it can forward suspect tasks generated by the control monitor to the workflow routing.
- The workflow definition also specifies data conditions. Thus, of all suspect tasks generated by the control monitor, only those with data values matching the data conditions are forwarded to the workflow routing.

Combining Priorities and Conditions in Workflow Definitions

Only one workflow routes a suspect for review when it is returned by a control monitor attached to a control, but any number of workflows may contend to be that one. That's because any workflow definition may apply if it specifies the Control Monitor Task Created event, and if a control and suspect satisfy every one of its conditions.

For example, a control with an attached monitor may be assigned values for two dimensions and one attribute — d1, d2, and a1. A workflow definition with d1, d2, and a1 as dimension/attribute conditions (for the moment, assume it has no data conditions) might apply to suspect records returned for the control. But so might definitions that set any combination of the three as conditions — such as d1 and d2, or d1 and a1, or d2 alone — or that set no conditions at all.

To resolve contention among workflow definitions, you assign each a priority. The value *1* indicates highest priority, and precedence declines as number values increase. When several workflow definitions might apply to a suspect, the highest-priority definition among them is the one to be used.

(Although a workflow configured for the review of Access Monitoring requests must also set a priority and may include data-source conditions, it is typically not so complex as other workflows, and contention issues typically do not arise.)

Assume that a control monitor has generated a set of suspect tasks. Moreover, several workflow definitions are configured to have the Control Monitor Task Created

event; any of them may apply to each of the suspect tasks. The GRC Controls Suite engine selects one suspect and determines whether it meets all the conditions specified for the highest-ranking of these workflow definitions. Does the suspect-task record contain all values specified by data conditions? The control monitor is attached to a control; does the control have all the dimensions and attributes specified as dimension/attribute conditions for the workflow definition?

If the answer to these questions is yes, the workflow definition applies, and the suspect task is sent for review to users or groups named in a workflow routing mapped to the definition. If the answer is no, the engine compares the suspect record with the second-highest-priority definition that has the Control Monitor Task Created event. If the record satisfies all conditions set by the definition, the mapped workflow is used; if not, the engine moves to the next-highest-priority workflow definition. It continues until it finds a match.

Then the engine moves to the next suspect-task record and repeats the process, continuing until all suspect-task records have been matched to workflow routings.

Therefore priority is the first factor in determining which among competing workflow definitions (and so routings) is used; precision of the match between workflow-definition conditions and the dimension, attribute, and data values contained in a suspect record comes second. In the example of the control with dimensions d1 and d2 and attribute a1, a definition that sets these values as conditions might be considered to be more closely matched than one that sets only a data condition. Even so, if that second definition has the higher priority, it would be used whenever the data condition evaluates to true.

You can use this to your advantage. You might want suspects who meet the d1-d2-a1 definition generally to be reviewed by the members of an “everyday” workflow routing. You might also identify some emergency circumstance that requires review by another set of approvers, and so create a higher-priority workflow definition that includes only a data condition to define the emergency. The emergency workflow would be used for appropriate suspects, but other suspects would fall through to the everyday workflow.

There is a danger, however, of configuring a workflow definition with a highly specific set of conditions, and have it never be used because a more general definition has a higher priority. (Any suspect that would qualify for the d1-d2-a1 definition would, for example, be captured first by a higher-priority definition that specifies any one of these as its only condition.)

As a result, it is generally advisable that as the conditions configured for a workflow definition become more specific, the definition should receive a higher priority. Moreover, a definition with no conditions and the lowest priority serves as a “catch-all,” implementing a workflow routing for any control whose dimension and attribute assignments do not match up with the conditions of any higher-priority workflow definitions. A “Default Workflow” serves this purpose. It routes requests to a user selected during installation, and its definition has priority number 1000, has no dimension or data conditions, and calls all possible events.

If priority is the first factor in resolving contention among workflow definitions, however, precision still matters. You may, for example, design a control that requires review of invoices valued higher than a certain amount. The control may have, let’s say, a Region dimension with two values — East and West. Suspects for

each region are to be reviewed by approvers from that region, so you intend to map two workflow routings to the control. But a single table contains invoice records for both regions; fortunately, it contains a column (called, let's say, REGN) that stores the region for each record, and this column is included among the values returned with each suspect.

To direct suspects to appropriate reviewers, each workflow definition would set a dimension/attribute condition (Region equals either East or West) as well as a data condition (REGN equals either East or West). As the GRC Controls Suite engine evaluates an individual suspect record (let's say one for the eastern region) it would necessarily consider the higher-priority definition first. If that were the Eastern definition, it would (appropriately) evaluate to true without the other definition being considered. Or, if the Western definition had the higher priority, the engine would evaluate it first, get a false result, and move on to the Eastern definition and a true result. So priority, while implemented, would become irrelevant.

In a case like this one, it is theoretically possible not to use data conditions, but instead to add a WHERE condition to the SQL statement run by the control monitor that produces suspects, so that it would return values only for the East or only for the West. This, however, is not recommended. First, it's less efficient (rather than one control for both regions, it would require two controls, one for each region).

Perhaps more important, the SQL queries included in control monitors are commonly very complex, and the attempt to edit one (particularly by a person who did not write it originally) risks distorting its logic. So that data conditions can be written, SQL queries should include all return columns they might use.

When a workflow routes Access Monitoring requests for review, the interaction between conditions and priorities is simpler. Only a "data source condition" — one that selects a business-management-application instance in which access requests may be made — applies to such workflows. So the highest-priority workflow for a given instance (and given event — database access or responsibility access) is always the one that routes requests for approval.

Combining Events and Conditions in Workflow Definitions

You may combine any number of events within a single, multipurpose workflow definition. However, each event can be paired only with conditions that do not filter out all of the items the event is intended to select. For example:

- Access requests are not associated with dimensions or attributes and do not return data values, so an access-request event would never generate results if it were paired with a dimension/attribute condition or a data condition.
- Control-library elements are associated with dimensions and attributes, but do not return data values. So a "Created" or "Updated" event for a control-library element may be paired with dimension/attribute conditions, but would never generate results if associated with a data condition.

Therefore, as you create a workflow definition, you select events before conditions, and you cannot set conditions that do not agree with the events you've chosen. Specifically:

- If you select only the Control Monitor Task Created event, you can create dimension/attribute conditions and data conditions.

- If you combine the Control Monitor Task Created event with any of those that trigger the review of control-library elements as they are created or updated, you can create dimension/attribute conditions, but not data conditions.
- If you combine the Control Monitor Task Created event with either of those that apply to the review of access requests as they are generated in the Access Monitoring feature, you cannot configure any conditions.
- If you select the DB User ID Requested or E-Business User ID Requested event (or both) but no others, you can create data source conditions.

Moreover, when you edit a workflow definition, you cannot add or remove events if the definition includes any condition.

SQL Queries in Control Monitors

You are assumed to know how to write a SQL query. (If not, please consult a SQL reference.) However, writing a query for use in a control monitor involves a few special considerations.

When a control monitor runs a SQL query, the return values are incorporated into messages displayed at the Task Inbox of the GRC Controls Suite. Therefore each SQL query must return values for columns with the following aliases:

- suspectName: Although not displayed at the Task Inbox, this value is required in the SQL query. It can be any label that applies to values returned by the query.
- suspectDesc: This column provides an encapsulation of the issue involved in each record retuned by the SQL query, for display in a Task Description field. It may incorporate text and return values, for a maximum length of 255 characters.
- suspectInfo: This column provides a more thorough account of the issue involved in each record returned by the SQL query, for display in a Suspect Details panel. It may incorporate text and return values, for a length of up to 4,000 characters.
- uniqueSuspectIdentifier: This alias identifies a column (or combination of columns) that contains a unique value for each record. This value is used to eliminate duplicate suspects generated in multiple runs of a control monitor. (Note, however, that a control monitor may be attached to more than one control; if so, duplicate suspects can be generated, one for each control.)

As noted earlier, a query should also include any columns that might return data useful for a data condition in a workflow definition.

Moreover, a SQL query may include parameters, which serve as placeholders either for information displayed in the suspectDesc or suspectInfo messages, or for values in the WHERE clause that filter the results returned by the SQL query. At run time, a user may either supply a value in place of the parameter, or accept a default value. To use a parameter, you would first create it in Transaction Controls Governor; you would then site the ID configured for it, preceded by an ampersand (&), in the SQL query. There are three types of parameter:

- A character parameter represents a string of text. When the query is evaluated, the parameter is replaced by actual text (either a default or a value provided by

the user who runs the control monitor), and that text must be placed in single quotation marks. To make this happen, you can either type these marks around the parameter ID (and its ampersand) as you create the query, or instruct Transaction Controls Governor to supply them automatically when you create the parameter.

- A numeric parameter represents a number.
- A dimension parameter represents a dimension value, as configured in the GRC Controls Suite. Within a query, you must place the ID for a dimension parameter (and its ampersand) in single quotation marks.

  For example, assume that a dimension called *CorpDivision* has been configured, and one of its values is *Manufacturing*. You might create a parameter based on this dimension, and you might set the Manufacturing value as the parameter default; assume that the configured ID for this parameter is *CD*. If a SQL statement includes the clause where *InventoryOrg = '&CD'*, the statement would return those records for which a table column called InventoryOrg contained a particular value — *Manufacturing* if the default value were accepted at run time, or another value configured for the CorpDivision dimension if that value were selected at run time.

Finally, a control-monitor SQL statement may contain a constant, called last_run_date, which stores the last date upon which the query has been evaluated; if so, it may check a date stored within records, and return those with a defined relationship to the last_run_date. For instance, if a query were based on a table in which a record_date column contained the date on which each record was generated, then the clause *WHERE record_date > last_run_date* would return values generated since the last time the parameter was run.

The following sample query is directed at a table (ap_invoices_all) that stores invoice data; it returns a record for each invoice with a value greater than a threshold amount. That threshold is represented by a numeric parameter (ThresholdParm), so that a user can set an appropriate amount as he runs the control monitor. Moreover, the query returns values from two table columns, invoice_num and invoice_amount:

```
select 'Invoice amount too great' suspectName,
 'Invoice '||invoice_num||' may exceed acceptable value' suspectDesc,
 'The invoice '||invoice_num||' is valued at '||invoice_amount||
  ', but the value threshold has been set at '||&ThresholdParm||
  '. Please review.' suspectInfo,
 invoice_num uniqueSuspectIdentifier
from ap_invoices_all
where invoice_amount > &ThresholdParm
```

Imagine that a user sets the threshold at $5000; one invoice in the ap_invoices_all table has a greater invoice_amount value ($5001); and the identifying number for that invoice (its invoice_num value) is 98765:

- The suspectName return value is “Invoice amount too great” (as it would be for any other record returned by this query, as it’s configured to be static text).
- The suspectDesc return value is “Invoice 98765 may exceed acceptable value,” because the text configured for suspectDesc is concatenated with the value of invoice_num.
- The suspectInfo return value is “The invoice 98765 is valued at 5001, but the value threshold has been set at 5000. Please review,” because the text config-

ured for suspectInfo is concatenated with the values of invoice_num, invoice_amount, and the ThresholdParm parameter.

- The uniqueSuspectIdentifier value is the invoice number, 98765. This ensures that a suspect returned for the same invoice in a second running of the control monitor would be deleted because it's redundant; the suspect record from the first running of the control monitor already exists.

Statuses and Versions

For either a control monitor or a workflow routing, there may be any number of versions, and each version exists at one or more of four statuses: Editing, Active, Pending Inactivation, and Inactive.

- A control monitor or workflow routing at the Editing status is in development. Editing is the default status for a newly created version of a monitor or workflow, and only a version at the Editing status can be modified.
- An Active control monitor or workflow routing is actually used; it identifies suspects or distributes review requests. Only one version of a control monitor or workflow routing can be Active at a time.
- When a control monitor or workflow routing is promoted from Editing to Active, the version that had been Active should be made inactive. At that moment, however, any number of review requests or suspect tasks may have been initiated but not completed under the terms of the earlier Active version. If so, status for that earlier version is set automatically to Pending Inactivation; it remains at that status until all of its outstanding issues are resolved.
- An Inactive control monitor or workflow routing is no longer used. A version may reach this status either from Active (when a subsequent version is promoted from Editing and replaces it as Active) or from Pending Inactivation (upon resolution of issues that were outstanding when it was replaced as the Active version). You can assign Inactive status to a version manually. Or, when you promote a version to Active status, the version (if any) that had previously been active is inactivated.

3

Configuring Monitors and Workflows

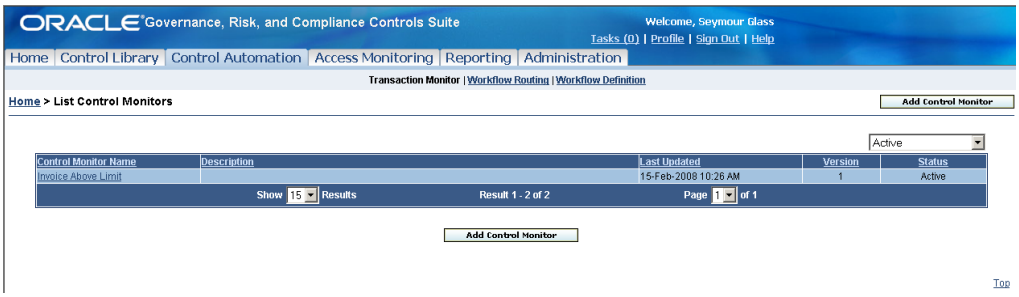
To work with a control monitor or a workflow routing, you first create the item (in effect, give it a name and describe it). Then you edit it, either to configure its first version (set the values that initially define it) or to configure later versions (modify existing values). You follow virtually identical processes for creating each of these items and for selecting versions of them for editing, although of course the values you supply as you edit each (and the procedures for supplying them) are very different.

Each version of each workflow routing is associated with a workflow definition, which is edited (and actually used) while its routing version is at the Active status; it may be viewed, but not changed, when its routing version is at either inactive status. Rather than create workflow definitions, you select them for editing or viewing from automatically generated lists of the workflow routings to which they apply.

This manual, by convention, directs you to select the Control Automation tab in the Governance, Risk, and Compliance Controls Suite to configure control monitors, workflow routings, or workflow definitions. For control monitors, this is required; for workflow routings or definitions, you can instead select the Administration tab, from which identical workflow features are available.

Displaying a List of Control Monitors or Workflow Routings

To view, create, or modify a control monitor or workflow routing, ensure that the Control Automation tab is selected. Then select either the Transaction Monitor link (the default) or the Workflow Routing link in the Library Navigator. A List panel shows active control monitors or workflow routings (according to your selection in the Library Navigator), and presents information about them — name, description, date last modified, version number, and status:

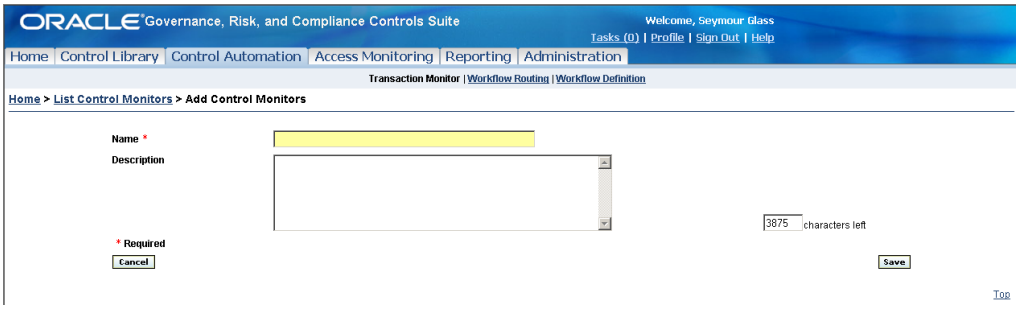


To view entries for monitors or workflow routings at a specific status, use the Status list box (it's unlabeled, but is located above the list of control monitors or workflow routings, along the right side). You can select All or any of the individual statuses — Active, Editing, Pending Inactivation, or Inactive.

Adding a Control Monitor or Workflow Routing

To create a new control monitor or workflow routing:

1. The List panel displays two buttons — one at the top right, and another at the bottom center — labeled either Add Control Monitor or Add Workflow Routing (depending on your selection in the Library Navigator). Click on a button to open a panel called Add Control Monitors or Add Workflow Routings.



2. In the Name field, type a name for the control monitor or workflow routing.
3. In the Description field, explain how the monitor or routing is to be used. (Note that a second field keeps a tally of the number of characters you may use.)
4. Click on the Save button.

The act of saving the monitor or routing automatically opens a panel that lists its existing versions — in this case, a single version at the Editing status. From this panel (which is shown on page 3-3), you can open the monitor or routing for editing.

Viewing or Editing a Control Monitor or Workflow Routing

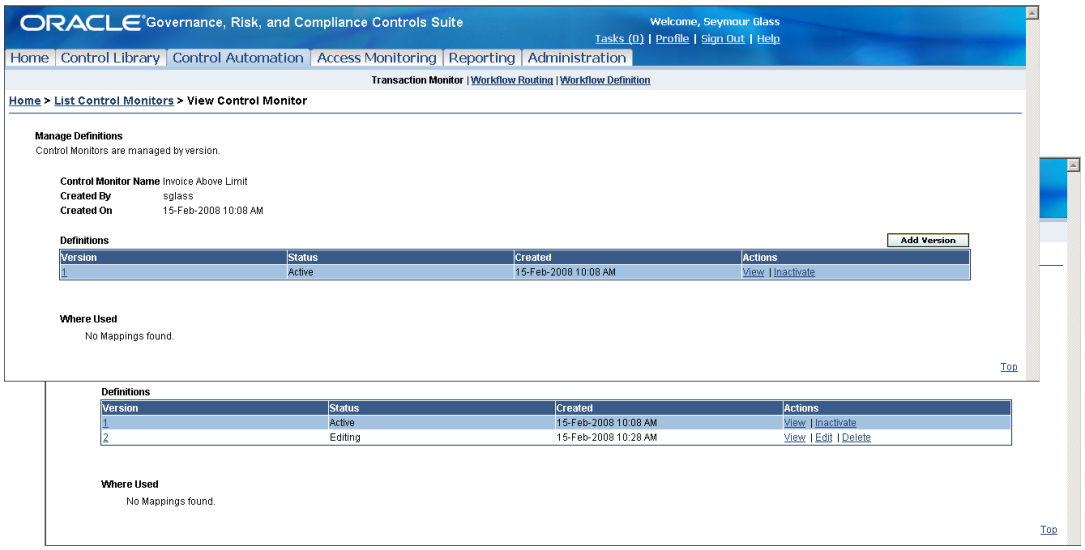
As you edit a control monitor or workflow routing, you either select values for a newly added one or modify values for an existing one. In either case, a version of the item must exist at the Editing status.

You begin to edit an item by selecting (or creating) its Editing version in a panel that lists all its versions. Or, in the same panel, you can select a version at any status to view its configuration details. The panel opens automatically for a newly created monitor or routing. For an existing monitor or routing, complete these steps to open the panel:

1. Open the List panel for control monitors or workflow routings.
2. If you are interested in monitors or workflows at a particular status, set the Status filter accordingly. Or, select All if you want to see items at more than one status.

3. The List panel presents a filtered list of control monitors or workflow routings. Click on the name of the one you want to view or change. This produces the panel that lists all existing versions of the item you've selected — View Control Monitor or View Workflow Routing.

    - If no Editing version yet exists, the panel displays an Add Version button (as shown in the top instance of the panel in the following illustration).
    - If an Editing version already exists, the panel displays a row for it (row 2 in the bottom instance of the panel in the following illustration).



From this panel, you can:

- Create an Editing version by clicking on the Add Version button. The new version is a copy of the most recent (typically Active) version.
- Open the Editing version for modification by clicking on its version number or on its Edit link. An Edit Definition panel opens.
- Open any version for viewing by clicking on its View link or, for a version at a status other than Editing, its version number. A View Definition panel opens. You cannot change any information displayed in a View Definition panel.
- Delete the Editing version by clicking on its Delete link.
- Retire the Active version by clicking on its Inactivate link.
- Rename the monitor or routing, or revise its description, by clicking on an Edit link that appears next to its name. (The link, and the renaming capability, exist only when the Editing version of the monitor or routing is selected.) This opens an Edit panel that works in the same way as the Add panel in which the monitor or routing was originally named and described.

If you have linked a version of a control monitor to one or more controls, and you select that version in the Definitions list on this panel, a Where Used grid shows the ID and name of each linked control.

Configuring a Control Monitor

A control monitor implements a series of steps. At least two steps — one each of two types — are required. A third type of step is optional.

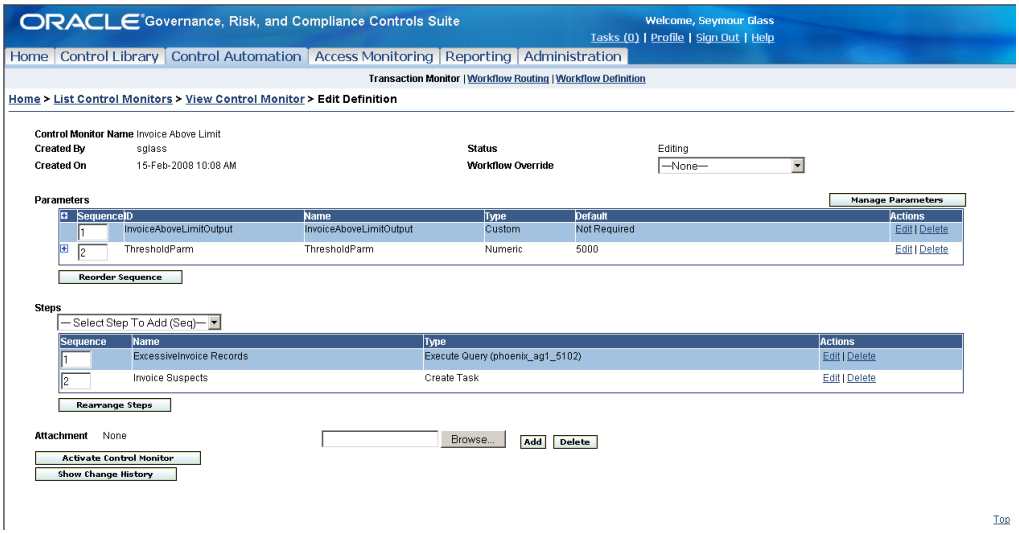
- An Execute Query step defines a SQL query and designates a parameter that stores results returned by the query. This is one of the required steps.
- A Create Task step converts each of the stored records returned by a SQL query into a "suspect task." This is the second of the required steps.
- An Update Parameter step alters the value of a parameter to the value of another parameter, to a fixed value, or to a calculated value. This is the optional step.

Thus, as you configure a control monitor you do the following:

- Create parameters — at least one per SQL query, to store the values returned by the query, and potentially others for use within queries.
- Write the SQL queries themselves.
- Incorporate queries and parameters in steps.

Optionally, you can designate a workflow routing whose members always review suspects generated by the control monitor; this removes the control monitor from review cycles implemented by workflow definitions. You can also attach a document to the control monitor (page 3-12) or review its change history (page 3-19).

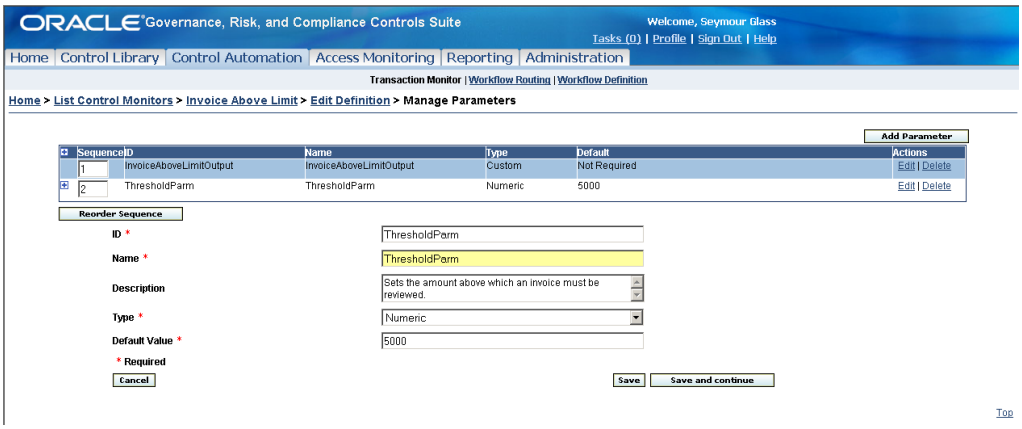
To begin, open the control monitor for editing (see "Viewing or Editing a Control Monitor or Workflow Routing" on page 3-2). An Edit Definition form appears, displaying prompts to create new parameters and steps. If parameters and steps have been created, the panel also lists them, with prompts to edit them. (The View Definition panel, if you were to open it instead, would be similar to Edit Definition, but would not allow changes.)



Configuring Parameters

To create a new parameter, click on the Manage Parameters button in the Edit Definition panel. To modify an existing parameter, click on the Manage Parameters

button or on the Edit link in the entry for the parameter you want to modify. A new panel, labeled Manage Parameters, appears:



If parameters exist, they are listed in a grid that appears above a set of data-entry fields. (It's a duplicate of the Parameters grid on the Edit Definition panel.) You can:

- Click on the Edit link corresponding to one of the parameters displayed in the grid. This fills the data-entry fields with the values configured for the parameter you've selected, so that you can modify them.
- Click on the Delete link corresponding to one of the parameters displayed in the grid, to remove it. (A confirmation dialog would appear, and you would also need to click on its OK button to delete the parameter.)
- Rearrange the order in which parameters are listed (see page 3-9).
- If you've selected an existing parameter for editing, an Add Parameter button appears. Click on it to clear the data-entry fields, so that you can enter values for a new parameter.

Regardless of whether you are editing an existing parameter or creating a new one, complete the following steps to supply values for it:

1. In the ID field, type an identifier for the parameter. This is the label by which you must call a parameter when you use it in a SQL query.
2. In the Name field, type a name for the parameter. This is the label you use in an Execute Query step or a Create Task step to select a parameter that holds values returned by a SQL query.
3. In the Description field, type explanatory information about the parameter. (The use of this field is optional.)
4. In the Type field, select a type for the parameter. (You may wish to review "SQL Queries in Control Monitors" on page 2-5.)
    - Select *Custom* for a parameter that is to hold values returned by a SQL query. One Custom parameter is required for each Execute Query step you create.
    - Select *Numeric* for a parameter that is to represent a number within a SQL query.

- Select *Character* for a parameter that is to represent text within a SQL query. A check box appears, labeled "Surround Character Type values with single quote characters." Select or clear it as follows:

  When a SQL query is evaluated, its parameters are replaced by actual values — either defaults or values provided by the user who runs a control monitor. The actual value for each Character parameter must be placed in single quotation marks. Make this happen in either of two ways: Insert the marks around the parameter ID as you write the SQL query. If so, clear the "Surround Character" check box. Or, omit the marks as you write the query, but have Transaction Controls Governor insert them automatically around the actual value as the query is evaluated. To do so, select the "Surround Character" check box.

- Select Dimension for a parameter that is to represent a dimension value within a query.

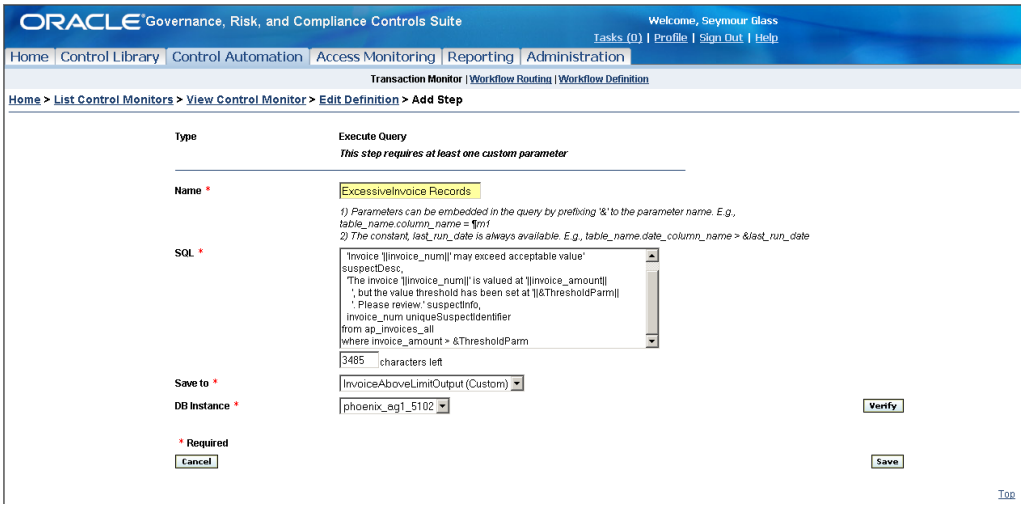
5. Set a default value for the parameter you are configuring:
   - For a Custom parameter, which has no default value, select Not Required in the Default Value field.
   - For a Numeric or Character parameter, set a number or text value to be used in place of the parameter if a user does not set a value while running the control monitor. Once again, use the Default Value field.
   - For a Dimension parameter, a Default Dimension field replaces the Default Value field. It lists all dimension values configured for your instance of Governance, Risk, and Compliance Controls Suite, each paired with the dimension for which it is a value. Select the value to be used if a user does not choose one while running the control monitor.
6. Save the parameter. Do either of the following:
   - Click on the Save and Continue button to save the parameter and keep the Manage Parameters panel open. You can then create or edit additional parameters. (The label *Save and Continue* is new for version 7.2.2; if you use version 7.2.1 or 7.2.0, this button is labeled *Add*.)
   - Click on the Save button to save the parameter and close the Manage Parameters panel.

   In either case, new parameter is added to the grid that displays parameter values, or modifications to an existing parameter are displayed in the grid.

Configuring Steps

To create or modify the steps the control monitor is to follow, click on the Select Step to Add list box in the Edit Definition panel. Then click on one of the three step types: Execute Query, Create Task, or Update Parameter. Or, click on the Edit button in the listing for an existing step.

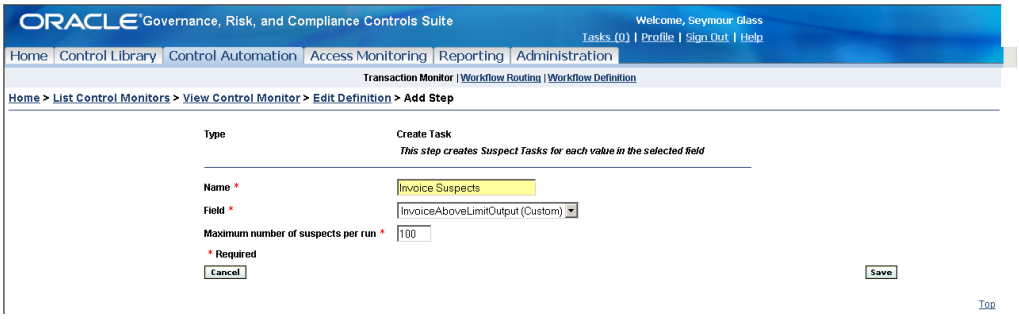
If you choose an Execute Query step (at least one is required), an Add Step form opens (as shown at the top of the next page).



1. In the Name field, type a name for the step.
2. In the SQL box, type the SQL query. (A related field counts the characters you may use.) You may wish to review "SQL Queries in Control Monitors" (page 2-5).

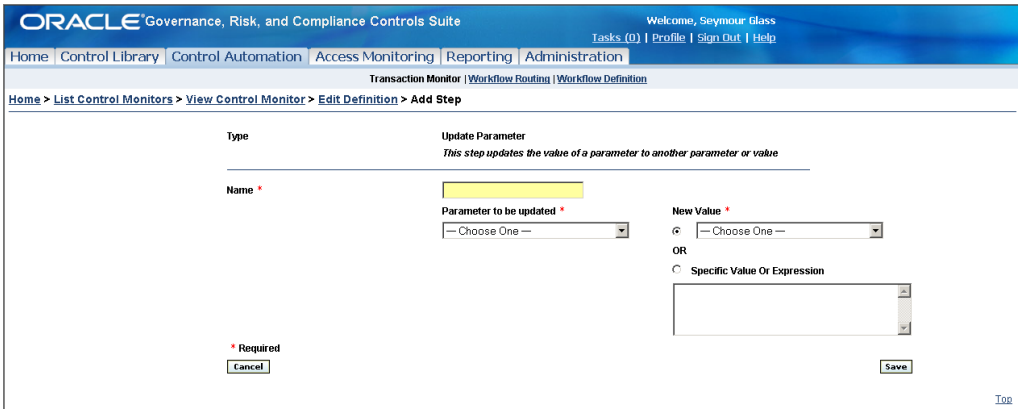
   If you include Numeric, Character, or Dimension parameters in the query, use their ID values (not their names) to identify them, and precede each ID with an ampersand (&). You must enclose the ampersand and ID value for a Dimension parameter in single quotation marks. You may or may not do so for a Character parameter, depending on whether you selected or cleared the "Surround Character Type values with single quote characters" check box as you created the parameter. Do not enclose a Numeric parameter in single quotation marks.
3. The Save To list box presents the names (not IDs) of Custom parameters you've defined for the control monitor you are creating. Select one of them.
4. The DB Instance list box presents the names of database instances to which Governance, Risk, and Compliance Controls Suite is configured to connect. Select the one at which you want to direct your query.
5. Click on the Verify button. A message appears near the top middle of this panel to inform you that the SQL either is or is not correctly parsed.
6. If the SQL contains errors, a link labeled Show Generated Sql appears next to the Verify button. Click it to see a text box that displays the generated SQL (with, for example, parameter IDs replaced by default values for the parameters).
7. Click on the Save button. The focus returns to the Edit Definition panel, which now displays a row for the step.

If you choose a Create Task step (at least one is required), the following form opens:



1. In the Name field, type a name for the step.
2. The Field list box presents the names of Custom parameters defined for this control monitor. Select one that is also named in an Execute Query step and so holds values returned by a SQL query.
3. In the Maximum Number of Suspects Per Run field, enter a number that determines how many suspects the control monitor can generate at one time. The minimum value is 1 and the maximum is 999; 100 is recommended. Without this feature, a control monitor has the potential to generate a number of suspects large enough to degrade system performance, so this feature is intended to preserve performance. If a monitor could generate more suspects than the value you set here, a message to this effect appears in a View Automation Run panel, in which the results of control-monitor runs appear. (This panel is accessible from the Control Library tab; see the *Governance, Risk, and Compliance Controls Suite Platform User Guide*.) In response to the message, you can run the monitor again.
4. Click on the Save button. The focus returns to the Edit Definition panel, which now displays a row for the step.

If you choose an Update Parameter step (which is optional), the following form opens:



1. In the Name field, type a name for the step.
2. The Parameter to Be Updated list box presents a list of parameters defined on your system. Select one whose value you want to reset.
3. Choose the value to which that parameter is to be reset. Do one of the following:
   - Click on the New Value radio button. In its list box, choose the name of a parameter that is to supply the new value. This parameter must be the same type as the parameter selected in the Parameter to Be Updated list box.
   - Click on the Specific Value or Expression radio button. Then, in the associated text box, enter either a fixed value or an expression, which may include a parameter or a SQL statement.
4. Click on the Save button. The focus returns to the Edit Definition panel, which now displays a row for the step.

Selecting a Workflow Override

Optionally, you can designate a workflow routing whose members have the exclusive ability to review suspect tasks generated by the control monitor you are configuring. If you do, this control monitor bypasses the ordinary workflow system, by which workflow definitions select workflow routings to be applied to suspects (as described in "Combining Priorities and Conditions in Workflow Definitions," page 2-2).

To do this, simply select the workflow routing you want from a Workflow Override list box located in the Edit Definition panel. If you select *None* (the default setting), you allow the control monitor to remain subject to the ordinary workflow system.

Rearranging Steps and Parameters

You can rearrange the order in which steps or parameters are listed in their grids on the Edit Definition panel or, in the case of parameters, on the Manage Parameters panel.

Rearranging steps actually adjusts the order in which the steps are to be completed. Rearranging parameters has no effect on how the control monitor uses them, but does determine the order in which the parameters are listed when a user adds the control monitor to a control as an automation. So it allows you to present them in an order that makes sense to that user as she supplies values for them. For example, you may group related parameters together.

To rearrange the order in which steps or parameters are to be listed:

1. In the Sequence column of the grid that lists the objects you want to rearrange, renumber the objects to reflect the sequence you want.
2. Click on the appropriate button — Reorder Sequence for parameters or Rearrange Steps for steps.

Completing the Configuration

When you finish creating a parameter, step, or workflow override, the control monitor is saved in its Editing status (because you have saved its individual components as you created or edited them). At this point, you can use the Edit Definition panel (shown on page 3-4) perform these additional actions:

- Delete an individual parameter or step by clicking on the Delete link in its entry on the Edit Definition panel.
- In the Parameters grid, click on +/- icons to display or hide the descriptions configured for parameters. (These icons appear in the left column of the Parameters grid, but only for those parameters for which descriptions have been created.)
- Promote the control monitor from Editing to Active status by clicking on the Activate Control Monitor button. The version of the control monitor that had been Active (if any) moves to the Inactive status. The Active version of a control monitor can be run only if it is attached to a control as an "automation." If a version of a control monitor is attached to a control, and you activate a new version, the newly active version of the monitor is attached automatically to the control.

Setting a Timeout Property

A suspect.query.timeout property sets the amount of time a control monitor may run before it times out. If, after control monitors are configured and attached to controls, you discover that any fail to return suspects, set a larger value for suspect.query.timeout — its unit of measurement is seconds, and its default value is 3600.

Properties can be set only by users assigned the System Administrator primary application role, through an option on the Administration tab. See the *Governance, Risk, and Compliance Controls Suite Installation Guide.*

Configuring a Workflow Routing

A workflow routing also implements a series of steps. Each selects users or groups charged with rendering approval decisions, and may designate other users or groups who receive notification when a decision is made. All receive approval requests or notifications at the Task Inbox of the Governance, Risk, and Compliance Controls Suite.

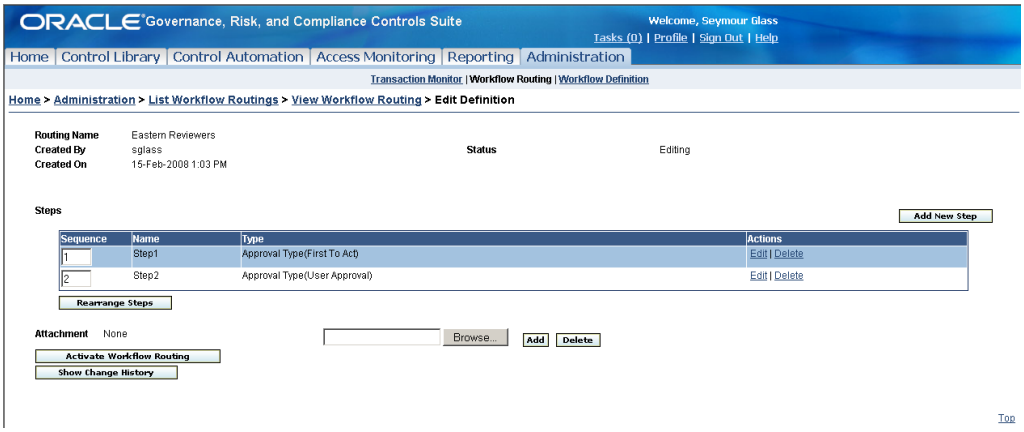
Those who review a suspect may either "pass" it (determine that the situation under review is benign) or mark it as an "exception" (find that the situation warrants correction). Those who review access requests may either approve or reject them. A suspect must be passed, or an access request be approved, at one step before it proceeds to the next. If a suspect is marked as an exception or an access request is rejected, the workflow ends; reviewers identified in subsequent steps are not sent messages.

At each step, you can select one of three types of decision-makers:

- Groups/First to Act: All members of one or more groups receive messages that a suspect or an approval request is to be reviewed, but the first member to respond acts for everyone. After the first response, other members of the groups can no longer respond.
- Groups/Requires All: All members of one or more groups receive messages that a suspect or an approval request is to be reviewed. For the item to move to the next step, all members must pass or approve it. A single exception or rejection decision causes a suspect to be marked as an exception, or an access request to be rejected, and the workflow to end.
- User: One or more users receive messages that a suspect task is to be reviewed. If two or more users are designated, all must pass a suspect or approve an access request for the workflow to proceed to its next step. A single exception or rejection decision causes a suspect to be marked as an exception, or an access request to be rejected, and the workflow to end.

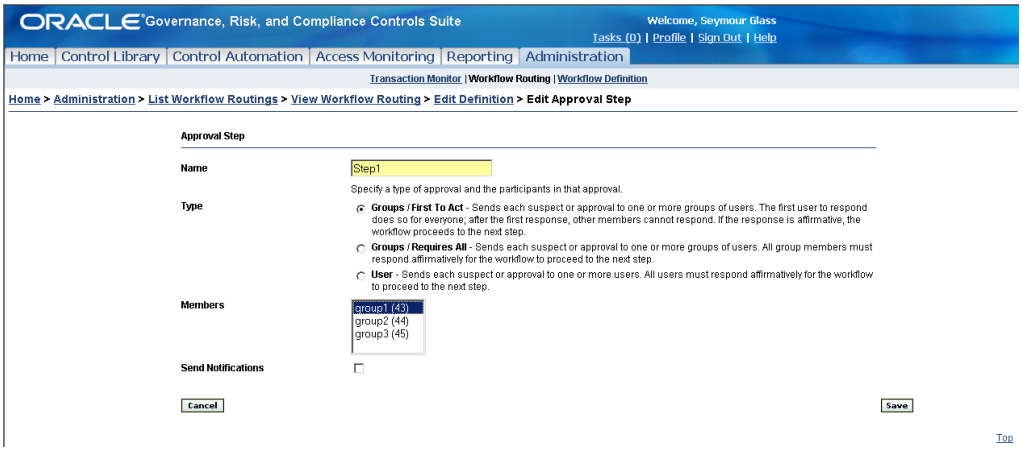
Before you configure a workflow routing, the groups or users it is to call must already have been created. (See the *Governance, Risk, and Compliance Controls Suite Platform User Guide*.)

Once this is done, create a workflow routing (page 3-2) and open its Editing version (page 3-2), or open the Editing version of an existing routing. An Edit Definition panel appears (as shown at the top of the next page), displaying a prompt to create new steps; if steps have already been created, the panel also lists them, with prompts to edit them. The Edit Definition panel also enables you to attach a document to the Editing version (page 3-12) or review change history (page 3-19) for any version.



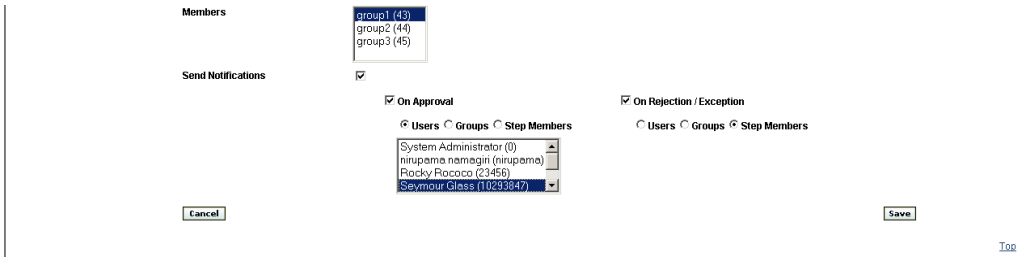
To create or modify steps that designate reviewers:

1. Click on the Add New Step button to create a new step, or click on the Edit button in the listing for an existing step to modify it. In either case, the following form opens:



2. In the Name field, type a name for the step.
3. Click on one of the Type radio buttons to determine the reviewer type.
4. A list of values appears next to the Members label, displaying either groups or users (depending on the type selection you made). Highlight those you want:
   - To highlight a single user or group, click on it.
   - To highlight a continuous selection of users or groups, click on the first one, hold down the Shift key, and click on the last one.
   - To highlight a discontinuous selection of users or groups, hold down the Ctrl key as you click on items.
5. You may or may not designate users or groups who are notified when actions are taken. If you choose not to, ensure that the Send Notifications check box is cleared and skip ahead to step 8. If, however, you want to designate recipients of notification messages, click on the Send Notifications check box and continue at step 6.

6. When you click on the Send Notifications check box, two more check boxes appear, one labeled On Approval and the other On Rejection/Exception. Click on either or both to designate those who will receive notifications of passed suspects, of exceptions, or of both.



7. Beneath each selected check box, a set of three radio buttons appears: Users, Groups, and Step Members. Click on one.
   - If you select Step Members, you need make no further selections; notifications will be sent to the users or groups already chosen in the Members field.
   - If you click on Users or Groups, a field appears, displaying names of users or groups; highlight those you want. Again, to highlight a single item, click on it. To highlight a continuous selection of items, click on the first one, hold down the Shift key, and click on the last one. To highlight a discontinuous selection, hold down the Ctrl key as you click on items.
8. Click on the Save button. The focus returns to the Edit Definition panel, which now displays a row for the step.

When you finish creating steps, the workflow routing is saved in its Editing status (because you have saved its individual steps as you created or edited them). At this point, you can use the Edit Definition panel to perform these additional actions:

- Delete a step by clicking on the Delete link in its entry.
- Rearrange the order in which steps are to be completed: In the Sequence column of the Steps listing, renumber the steps to reflect the sequence you want, and then click on the Rearrange Steps button.
- Promote the workflow routing from Editing to Active status by clicking on the Activate Workflow Routing button. If a prior version was already Active, it moves to the Inactive status. A newly Active version of a routing inherits the workflow definition configured for the previously Active version.

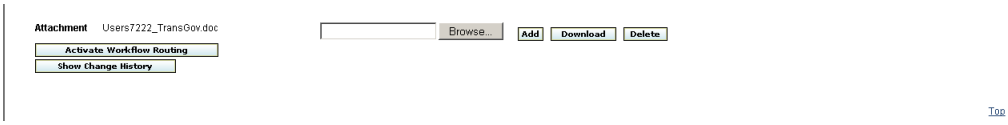
Attaching a Document

Optionally, you can attach a file to each version of a control monitor or a workflow routing, and then display the contents of the file. Typically, such a file documents what the control monitor or workflow routing does. Use a text editor, word processor, spreadsheet, or similar application to prepare the file.

You can attach only one file at a time to a given version of a monitor or routing, and only when that version exists at the Editing status. However, you can detach an existing file to make room for a new one (once again, for a version at the Editing status). You can view a file even after the version to which it is attached has been promoted to any other status.

To attach a file:

1. Navigate to the Edit Definition panel for the Editing version of a control monitor or workflow routing (see page 3-2).
2. Click on the Browse button in the Attachment area, near the lower center of the panel.
3. A Choose File dialog opens. Using standard Windows procedures, navigate to the file you want, click on its name, and then click on the Open button.
4. The path to the file appears in the text box next to the Browse button on the Edit Definition panel. Click on the Add button. The name of the attached file appears next to the Attachment label.



To detach a file, click on the Delete button. A confirmation message appears in a pop-up window; click on its Yes button.

To open and review an attached file:

1. Click on the Download button. (This button appears once a document is attached, and is the only one to remain available when the control monitor or workflow routing is at a status other than Editing.)
2. A File Download dialog appears. Click on its Open button, and the file appears in a distinct window. Alternatively, click on its Save button and, in a Save As dialog, navigate to a directory in which you want to save the file, and click on the Save button.

Copying a Control Monitor or Workflow Routing

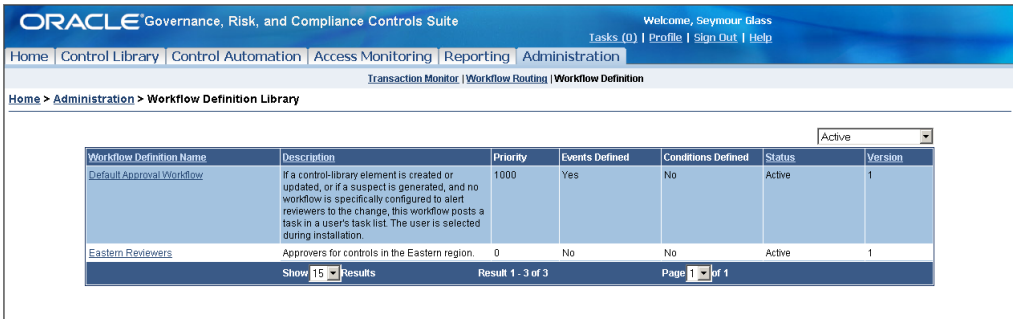
You can copy a control monitor or workflow routing under a new name, to use as a template for a new control monitor or workflow routing. As the source for such a copy operation, you can select only an object at the Active status, and its copy is created at the Editing status.

1. Navigate to the View Definition panel for the Active version of a control monitor or workflow routing (see page 3-2).
2. Click on the Create Copy button, located near the lower left of the panel.
3. The Add Control Monitor or Add Workflow Routing panel opens. (It's identical to the panel discussed in "Adding a Control Monitor or Workflow Routing" on page 3-2.) In the Name field, type a name for the copy you are creating; in the Description field, optionally type explanatory information; and click on the Save button.
4. The copied object now exists at the Editing status, identical to the source in every way except for name and status. Using standard procedures, open it and edit it as you wish.

Configuring a Workflow Definition

To create the workflow definition that applies a workflow routing to items in need of review, click on the Control Automation tab and then on the Workflow Definitions link in the Library Navigator.

A Workflow Definition Library panel displays an entry for each Active workflow routing, with its description, the priority number of its workflow definition (if one has been assigned), whether events and conditions have been assigned, its status, and its version. Click on the name of the workflow routing for which you want to configure a definition.

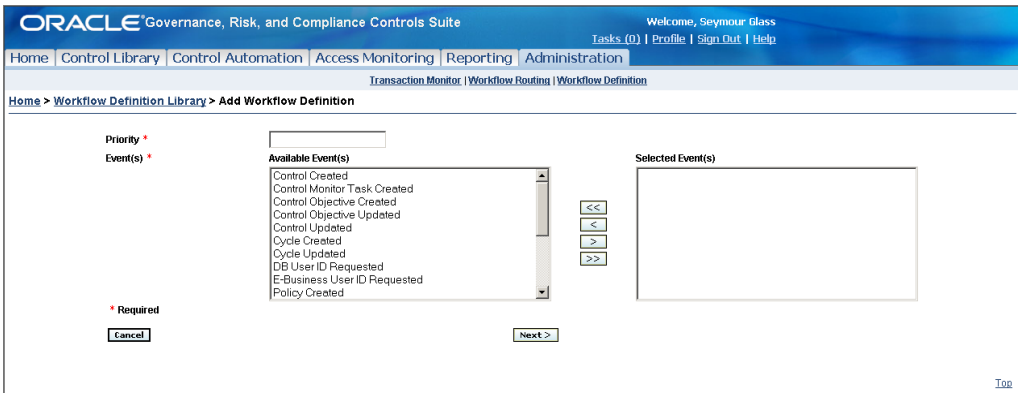


You can edit or view definitions that correspond to workflow-routing versions at the Active status. You can view, but not edit, the definitions for those workflow-routing versions as they move to the Pending Inactivation or Inactive status. To view definitions that correspond to routings at a particular status, use the Status list box (it's unlabeled, but is located above the list of workflow definitions, along the right side). You can select All or an individual status — Active, Pending Inactivation, or Inactive.

When you promote an Editing version of a workflow routing to Active, it assumes the definition configured for the version that had been Active before it. A definition for a workflow routing version at the Editing status would therefore never be used, so you cannot configure a definition for the Editing version of a workflow routing.

Selecting Priority and Events in a New Definition

If you have selected a workflow routing for which no definition yet exists, an Add Workflow Definition panel opens:



In this panel, you can select both priority and events. Do not select 0 as a priority; apart from that, you can select any number not already in use (you'll receive an error message if you do select a duplicate). You may wish to review "Combining Priorities and Conditions in Workflow Definitions" (page 2-2).

You always choose the Control Monitor Task Created event for a workflow intended to distribute suspect tasks for review. You select the E-Business User ID Requested or the DB User ID Requested to distribute Access Monitoring requests for review. If you chose to combine these events with one another (or with events that distribute control-library elements for review) in a multipurpose workflow, the combination of events determines the types of conditions you can configure. You may wish to review "Combining Events and Conditions in Workflow Definitions" (page 2-4).

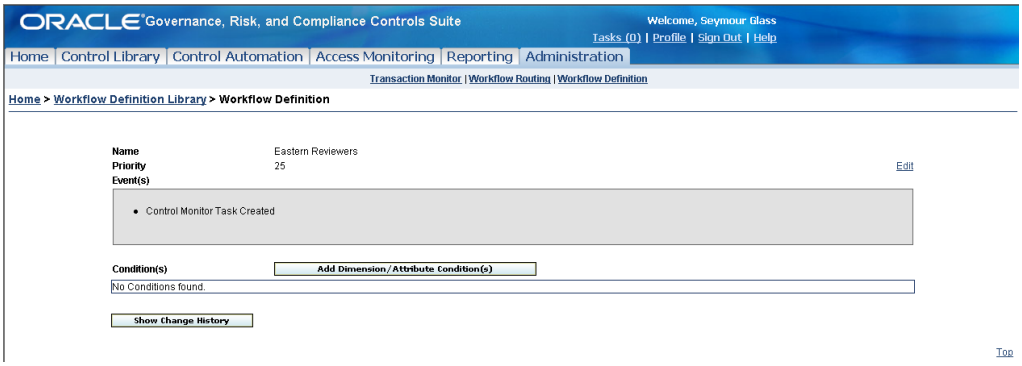
To use the Add Workflow Definition panel to select a priority and events:

1. In the Priority field, type the priority number you want.
2. In the Available Events field, highlight the events you want to select. To highlight a single event, click on it. To highlight a continuous set of events, click on the first one, hold down the Shift key, and click on the last one. To highlight a discontinuous set, hold down the Ctrl key as you click on events.
3. Click on the > button to send the events you've highlighted from the Available Events field to the Selected Events field. Or, click on the >> button to send all events to the Selected Events field, regardless of whether they are highlighted.

   If you reconsider, highlight events in the Selected Events field, then click on the < button to return them to the Available Events field. Or, the << button returns all events to the Available Events field, regardless of whether they are highlighted.
4. Click on the Next button. The Add Workflow Definition panel now summarizes your selections. If you are dissatisfied with any of them, click on the Back button to return to the previous panel; edit the values it displays and click on the Next button to return to this summary panel. When you are satisfied, click on the Finish button to complete the configuration of the priority and events.

Creating Conditions for a New Definition

When you finish configuring priority and events, a Workflow Definition panel displays the values selected for the definition:



The Workflow Definition panel presents buttons you can click to configure distinct types of conditions. The assortment of buttons depends on the events you've selected:

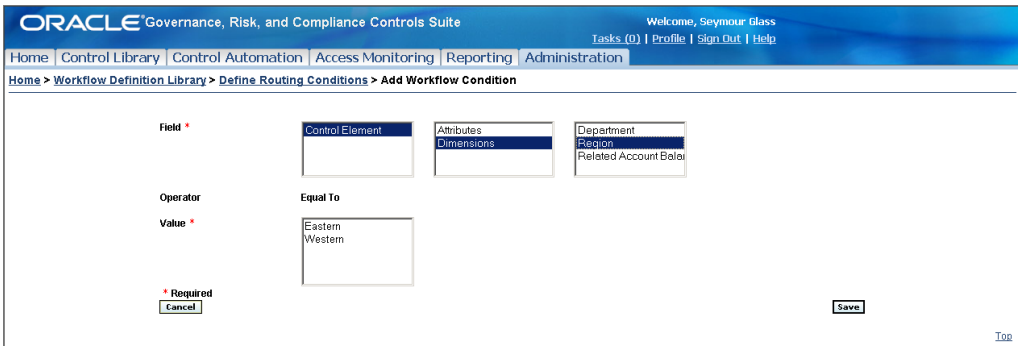
- If you have selected only the Control Monitor Task Created event, the panel offers two buttons, one for dimension/attribute conditions and the other for data conditions.
- If you have combined the Control Monitor Task Created event with a control-library event (such as Control Created), the panel presents only the dimension/attribute condition button, and you can create only that type of condition.
- If you have combined the Control Monitor Task Created event with either of the access-request events (with or without control-library events) the panel presents no condition buttons, and you cannot create conditions.
- If you have selected only "Requested" events for access requests, the panel presents the data source condition button, and you can create that type of condition.

Two or more conditions are joined by AND connectors; all must evaluate to true (and the workflow must have a higher priority than other eligible workflows) for the workflow routing associated with this definition to be used.

A single condition can have more than one right operand — for example, in a workflow devoted to access requests, DATASOURCE EQUAL TO DB1; DB2. In this case there is an OR relationship; there are implicitly as many conditional statements as there are right operands, and the condition evaluates to true if any one is true. In the example, if a request were made for access to DB1 or DB2 (and, once again, the workflow had a higher priority than other eligible workflows) the routing associated with this definition would be used. For a workflow that contains access-request events, use a single condition with any number of right operands; do not create two or more conditions.

A dimension/attribute condition states that a dimension or attribute equals a particular value; the workflow may map to a control assigned a dimension or attribute with the same value. To select dimension/attribute conditions:

1. Click on the Add Dimension/Attribute Conditions button. An Add Workflow Condition panel appears:

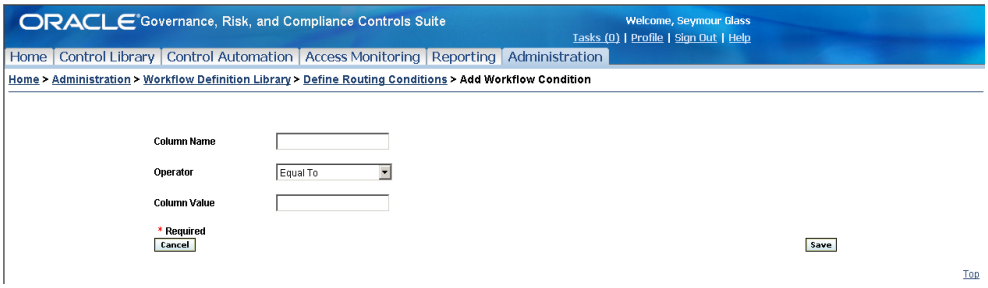


2. As a Field, select a dimension or attribute:
   - The leftmost box always reads Control Element; click on either Dimensions or Attributes in the middle box.
   - According to your selection, the rightmost box displays either the dimensions or attributes configured on your system; click on one of them.
3. Accept the default, Equal To, as the Operator value. (You cannot change it.)

4. The Value box displays the values for the dimension or attribute you selected as a Field; click on one of them.
5. Click on the Save button.

To filter the suspects returned by a control monitor, you can add data conditions. Each specifies a value that can be held in a column returned by a SQL query in the control monitor; the workflow routing may map to suspects containing that value in that column. To add a data condition:

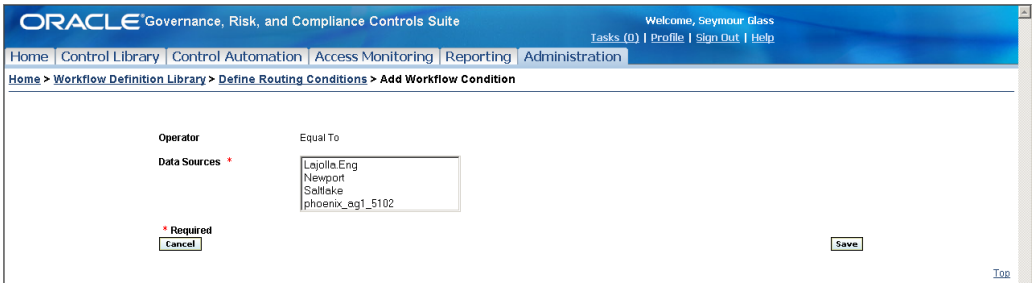
1. Click on the Add Data Conditions button, or click on the Edit link for an existing data condition. Another Add Workflow Condition panel appears:



2. In the Column Name field, type the name of a column that returns values in the SQL query for a control monitor. (Ensure that the control monitor is attached as an "automation" to controls to which this workflow definition applies.)
3. In the Operator field, choose among five values: Equal To, Less Than, Greater Than, Less Than or Equal To, or Greater Than or Equal To. Each value applies either to numeric or text values. (A text value is "less than" another if it comes earlier in alphabetic order, and "greater than" if it comes later.)
4. In the Column Value field, type the filtering value. It must, of course, be the same type (numeric or text) as values in the column specified by the Column Name field.
5. Click on the Save button.

A data source condition identifies one or more database instances in which user-access requests are to be implemented. To select data source conditions:

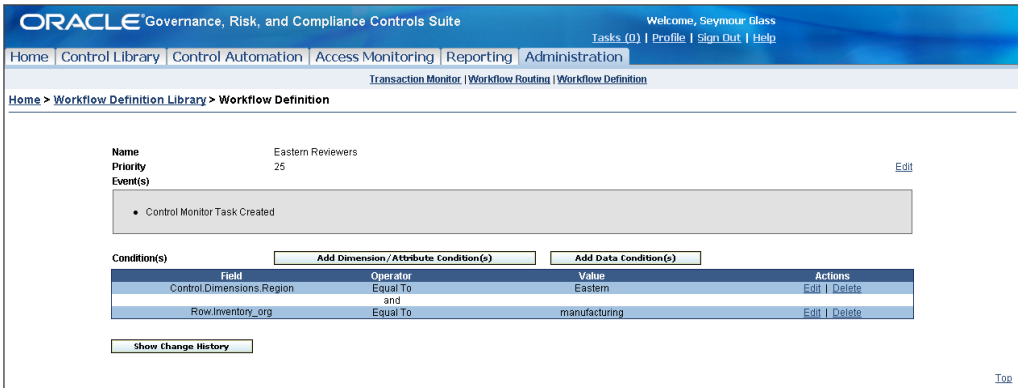
1. Click on the Add Data Source Conditions button (if you have selected access-request events for a workflow definition, and the button is therefore present in the Workflow Definition panel). A different instance of the Add Workflow Condition panel appears:



2. Accept the default, Equal To, and the Operator value (You cannot change it.)

3. In the Data Source Name field, select any number of databases. (To select more than one, hold down the Ctrl key as you click on data source names.)
4. Click on the Save button.

When you save a condition, the Add Workflow Condition panel closes; the focus returns to the Workflow Definition panel, with the new condition added to the list. Here, for example, is a workflow definition with two dimension/attribute conditions defined:



Because you have saved individual elements of the workflow definition as you created them, the definition itself requires no further saving. It is ready for use.

Editing an Existing Definition

To edit a workflow definition, select it in the Workflow Definition Library panel (page 3-14). This opens the Workflow Definition panel that displays configured values for the definition you've selected (shown in the figure above). The values are editable if the definition corresponds to an Active workflow routing, or are read-only if the definition corresponds to a Pending Inactivation or Inactive workflow routing.

For Active definitions, you can always modify the priority assigned to a workflow (providing that the new priority value is not already taken by another workflow). However, once you have configured an original set of events for a workflow definition, you cannot subsequently add or remove events if you have also configured conditions for the definition. To edit the selection of events for a workflow definition, you must first delete its conditions. To do this, click on the Delete link in the row for each condition.

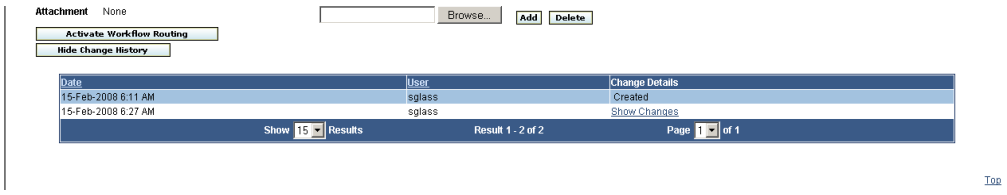
To edit priority or events, click on the Edit link in the Workflow Definition panel. (This link is toward the upper right of the panel, aligned horizontally with the Priority field). This opens an Edit Workflow Definition panel; apart from its label, it's the same as the Add Workflow Definition panel, except that it shows the values already selected for the definition, and the event fields are read-only if you have not deleted the conditions associated with the definition. Use the Edit Workflow Definition panel as you would the Add Workflow Definition panel (see page 3-14).

To edit a condition, click on the Edit link in its row on the Workflow Definition panel. This opens one of two Edit Workflow Condition panels — one for data conditions and the other for dimension/attribute conditions. Each of these, label aside, is the same as the corresponding Add Workflow Condition panel except, once again, that it displays the values already configured for the condition. Use these panels as you would the Add Workflow Condition panels (see page 3-15). You can also delete conditions (as discussed above) or use the Add buttons to add new conditions.

Reviewing Change History

For each version of a control monitor, workflow routing, or workflow definition, you can view a history of the changes made to the item:

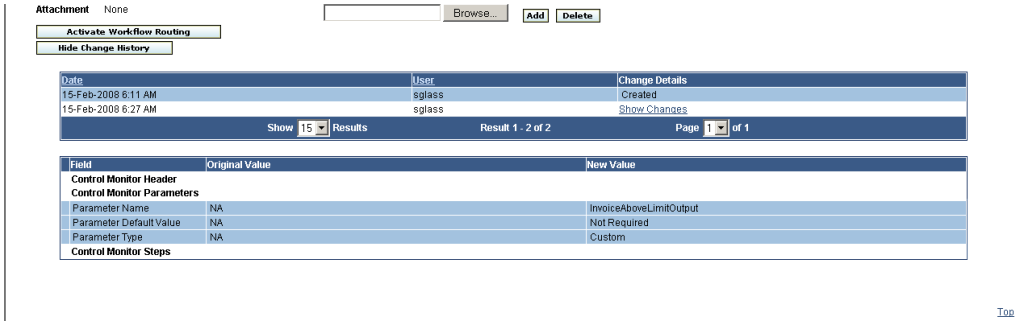
1. Open the panel from which change history can be viewed:
   - For a control monitor or a workflow routing, this is the Edit Definition panel (for a version at the Editing status) or the View Definition panel (for a version at any other status). See "Viewing or Editing a Control Monitor or Workflow Routing" (page 3-2) for information on opening these panels.
   - For a workflow definition, this is the Workflow Definition panel (shown on page 3-18, and opened from the Workflow Definition Library panel, shown on page 3-14.)
2. Click on the Show Change History button. A grid appears at the bottom of the panel, displaying a row for each time changes were saved for a control monitor, workflow routing, or workflow definition. Each row shows the date and time on which changes were saved, and identifies the user who made the changes.



Top

3. The first row in the grid documents the creation of the item; it's read-only, and it displays a static value, "Created," in a Change Details Column. Each subsequent row documents a change, which may in fact involve modifications to several related fields. To view details about such modifications, click on the Show Details link in the Change Details column for one of these rows.

   A second grid appears, displaying the old and new values for each modified field associated with the row you selected.



Top

   This grid categorizes the changes according to whether they have been made to the "header" (the name and status of an item), the parameters, the steps, or other miscellaneous items (such as attachments).

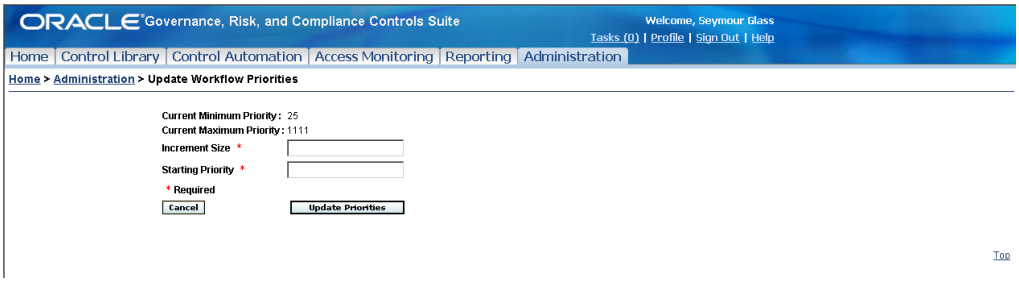
4. Click on Show Details in other rows to view values for changes saved at other moments. Or, to close both grids, click on the Hide Change History button.

Updating Priority Values

You may create a large number of workflows, each, of course, incorporating a definition that includes a unique priority number. You may then identify a need to create a new workflow whose priority must be set at some point amid the values that have already been taken. This may require that the priorities assigned to many workflows be reset (if, for example, one thousand existing workflows have consecutive priority numbers, and you need to create a new workflow with a priority of, say, 15).

Transaction Controls Governor enables you to reset the priorities of any number of workflows at once, rather than edit individual workflow definitions. To do so:

1. Click on the Administration tab in the Governance, Risk, and Compliance Controls Suite. This opens an Administration Home panel; in it, locate the Workflow Administration section and click on the Manage Workflow Priorities link. An Update Workflow Priorities panel appears:



2. Review information about your current priority configuration:
   - The Current Minimum Priority field shows the smallest priority value (and therefore actually the highest priority) assigned to an existing workflow definition.
   - The Current Maximum Priority field shows the largest priority value (and therefore the lowest priority) assigned to an existing workflow definition.
3. In the Starting Priority field, type the existing number of the first priority you want to reset to a new value. In the example above, you want to create a new workflow at priority 15. So the first priority you need to reset is for the workflow currently at 15. It and subsequent priorities will increase by an amount to be determined in the next step.
4. In the Increment Size field, type the number of openings you want to create at the starting point.

   In the example above, you're creating one new workflow, so you need one opening for it, and would enter the value 1 in the Increment Size field. The workflow whose priority was originally at 15 would move to 16, and subsequent priorities would also be increased by one.

   But if, instead, you had two new workflows to create and wanted to assign them priorities 15 and 16, you would enter 2 here; the existing number 15 would then become 17, and subsequent priorities would be renumbered accordingly.
5. Click on the Update Priorities button.

4

Access Monitoring

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

Requests must be approved. Governance, Risk, and Compliance Controls Suite provides workflows that route requests to approvers, as well as a Task Inbox at which approvers receive the requests and respond to them. A user is prevented from creating a request if workflows are configured so that he is an approver for the request.

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

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

- Database tables must be audit-enabled, regardless of whether they are to be accessed directly or through a responsibility. A set of tables is typically audit-enabled during system installation. Moreover within Oracle EBS a user can open an Access Monitoring Content form to view tables (and columns) that are already audit-enabled, and add to them.
- Database user IDs must be created. Access Monitoring maintains a set of 30 IDs for responsibility-access requests; as each user's access expires, his ID can be reused. However, a distinct set of IDs applies to database-table access, and a database administrator must create these database user IDs.
- Workflows must be configured to route access requests to approvers. For instructions on configuring them, see "Creating Workflows" in the *Governance,*

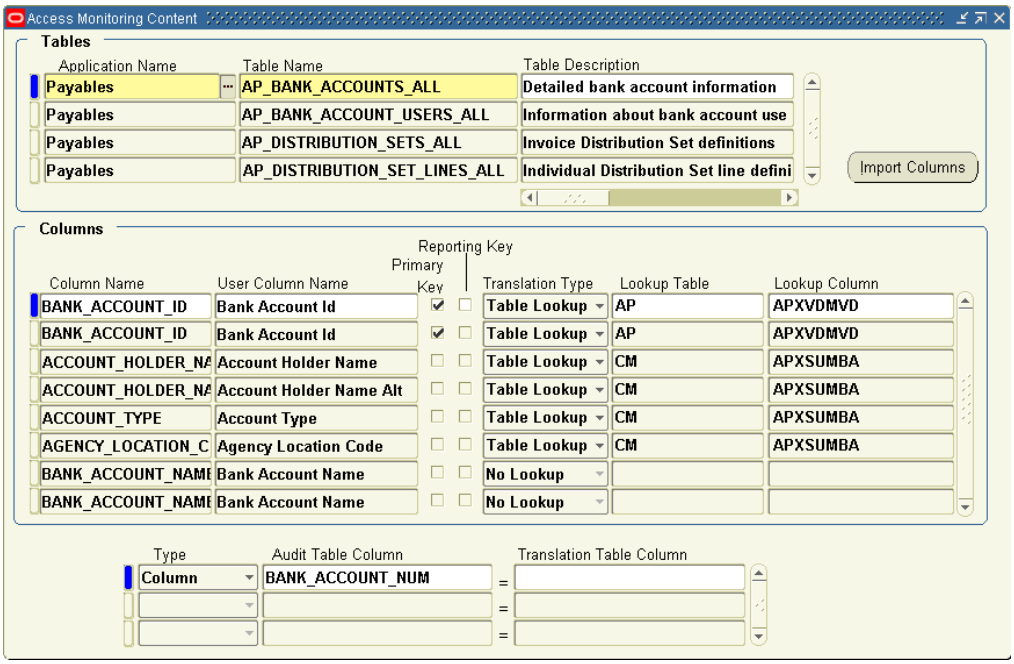
Risk, and Compliance Controls Suite Platform User Guide. As you review this information, note that the E-Business User ID Requested event pertains to the review of responsibility access requests, the DB User ID Requested event applies to the review of database access requests, and the Request SQL Created event is not used.

Preparing Tables for Auditing

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

Selecting Audit Tables and Columns

To add to the selection of tables, columns, and translations available for access requests, open your instance of Oracle E-Business Suite and select the GRC Controls responsibility. From the available applications, select Access Monitor Content. An Access Monitoring Content form appears:



In it, select a table.

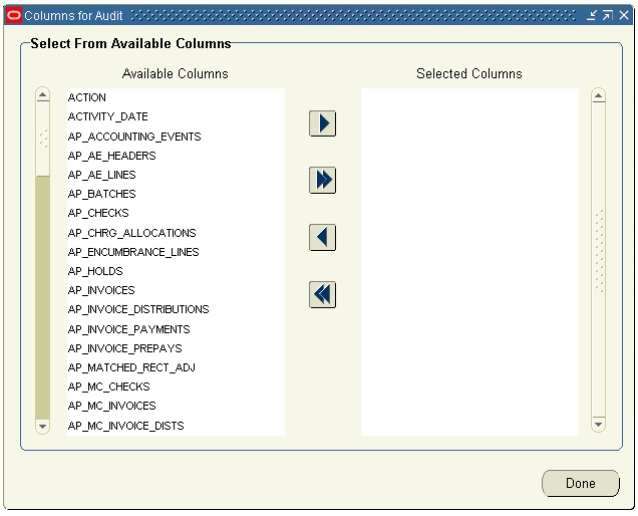
If you know a table is already audit-enabled (and you want to edit or add to the audit columns selected for it), use the Oracle query feature to load its record in the Tables block. Doing so also loads entries in the Columns block for columns in the table that have been selected for auditing. Or, you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

If a table is not yet audit-enabled:

1. In a blank row of the Tables block, select an application in the Application Name list of values (LOV).
2. The Table Name LOV can now display only tables that support the application you've chosen. Select one of them. Not only does the Table Name field display your selection, but the Table Description field also displays the description configured for it.
3. Optionally, use the scroll bar located beneath the Table Description field to scroll to the right and enter values in additional fields:
   - Form Name: Enter the internal name for the form supported by the table you selected. (For example, APXVDMVD is the internal name for the Enter Vendors form.)
   - User Form Name: This field automatically displays the external name for the form whose internal name you selected. You cannot enter a value directly in this field.
   - Block Name: Enter the internal name for the block that both exists on the form you selected and is supported by the table you selected.

Next, choose the columns you want to audit.

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



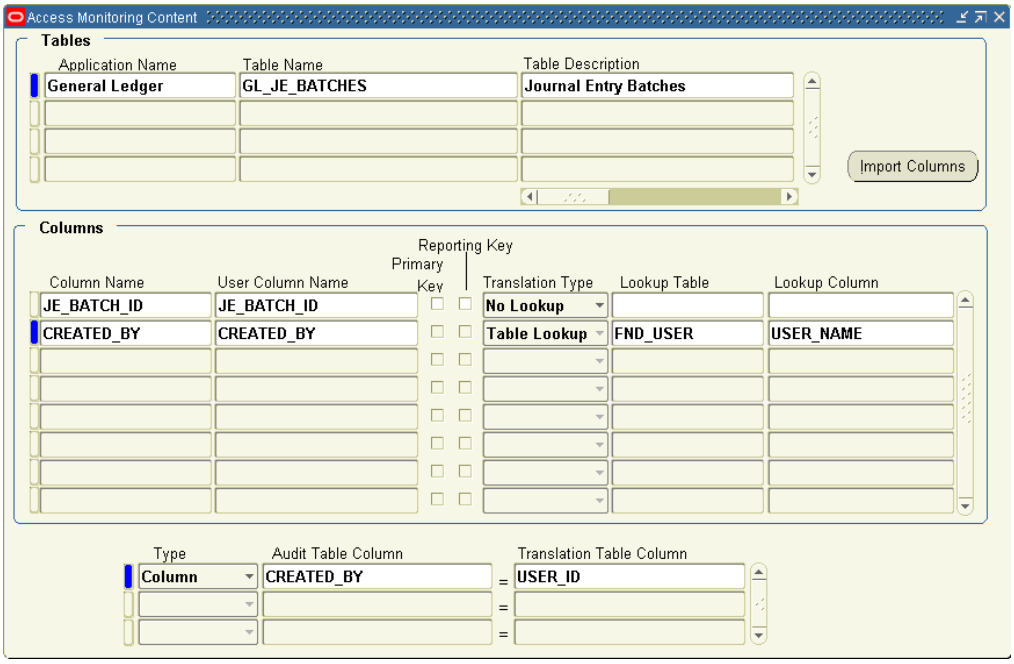
2. Select the columns individually or collectively:
   - In the Available Columns box, click on the name of a column you want to audit. Then click on the right-pointing single-arrow button to move it to the Selected Columns box. Repeat for each column you want.
   - Alternatively, click on the right-pointing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

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

Setting Up Translations

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

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



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

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

To set up this linkage:

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

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

Saving Your Work

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

Creating Database IDs

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

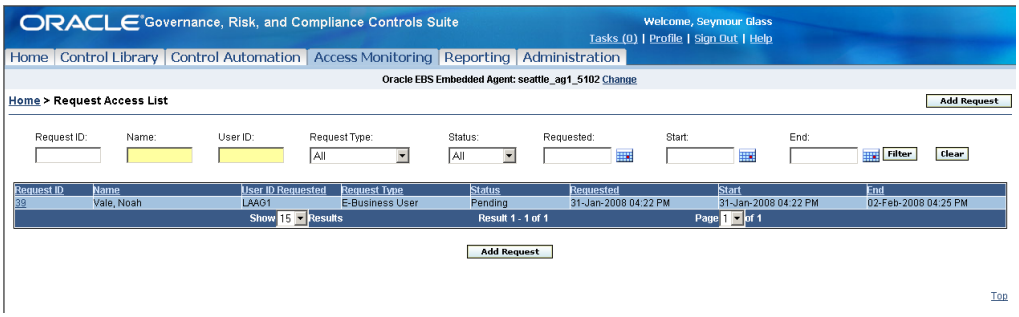
After the IDs are created, a concurrent request, called Access Monitor — DB Users Synchronization Process, must be run in the GRC Controls responsibility of Oracle E-Business Suite; this enables Access Monitoring to recognize the IDs and display them so that they are available for selection. The request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

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

Displaying a List of Access Requests

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

the dates on which the user's access is proposed to start and end. Finally, it displays the status of the request — Pending, Approved, or Rejected.



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

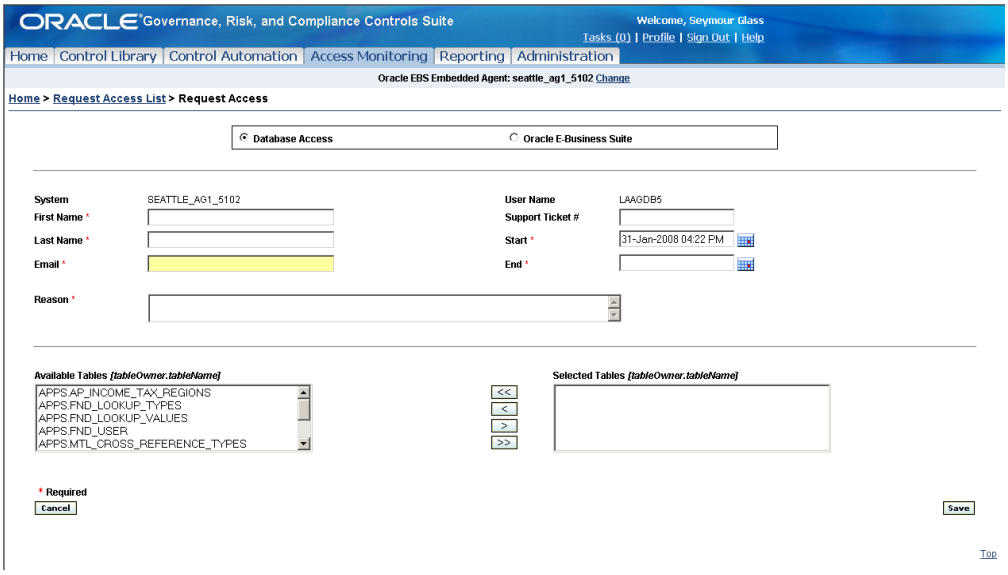
Creating a New Request

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

Starting the Request

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

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



2. Your request applies to the database instance to which you are logged on, and the System field displays the name of the instance. You cannot change this field

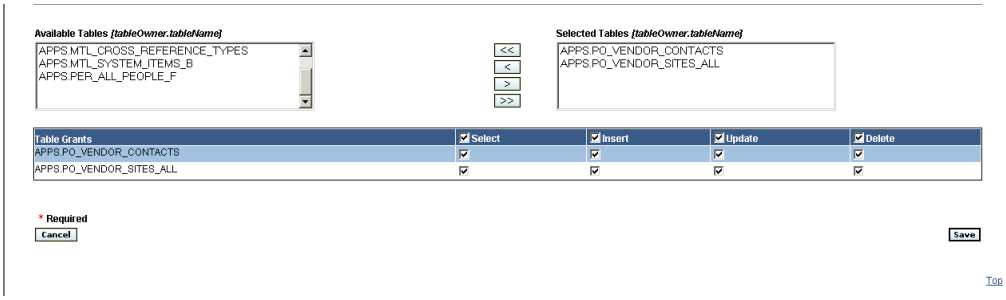
value directly. If you want to request access to another database instance, use the Change link (at the upper right of the panel) to log on to that instance.

3. In the First Name and Last Name fields, enter the given name and surname of the user for whom you are requesting access.
4. In the Email field, enter the email address of the user for whom you are requesting access. This is the address at which the user is notified of his new access rights, logon ID, and password. (Your own confirming email message goes to the address configured for you in the Add User panel of the Governance Risk and Compliance Controls Suite.)
5. The Support Ticket # field is for use if you are requesting access in response to a notification from an issue-tracking system. If so, enter the number assigned to the issue in the tracking system. (Any format is acceptable.) If not, leave the field blank.
6. The Start field displays the date and time at which you create the request, and the End field is blank. If you want the user to receive access immediately upon approval of the request, retain the default Start value; otherwise specify a later date and time. The access you are requesting is necessarily temporary, so you must supply an End date and time. The default Start value is read from the Oracle E-Business Suite server to which you are requesting access, and values you enter should be appropriate to that server.

   You can insert a date and time manually in either field (use the format *DD-Mon-YYYY HH:MM AM/PM*). Alternatively, you can click on the icon next to either field, and a pop-up calendar appears. In it, click on the < or > symbol surrounding a month name or year to display an earlier or later month or year; then, in the calendar, click on the date you want. The pop-up window closes, and the date you selected appears in the field, together with the time of day at the moment you select the date. You can edit the time.
7. In the Reason field, type an explanation for the user's being given the access you've requested.

Completing a Request for Database-Table Access

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



Complete the following steps:

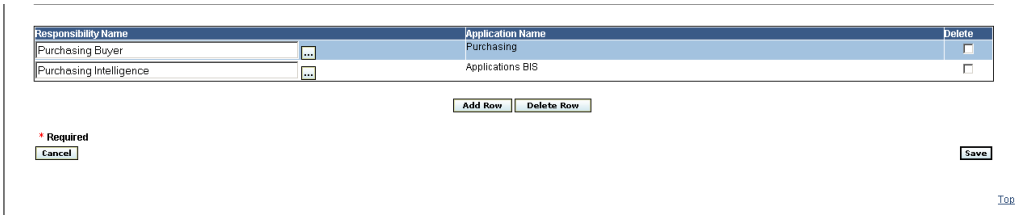
1. Select tables by moving them from the Available Tables field to the Selected Tables field:
   - Highlight tables you intend to select. Click on a table to highlight it. Or, to highlight a continuous group of tables, click on the first one, hold down the Shift key, and click on the last one. To highlight a discontinuous group, hold the Ctrl key as you click on tables.
   - Click on the > button to move highlighted tables from the Available field to the Selected field. Or, click on the >> button to send all values in the Available field (regardless of whether you've highlighted them first) to the Selected field.
   - If you reconsider, click on the < button to return highlighted values from the Selected field to the Available field. Or, click on the << button to return all values in the Selected field to the Available field.
2. When you select a table, a Table Grants grid appears; it generates a row for each table you select. For each table, select the check boxes corresponding to the privileges you want to assign — Select, Insert, Update, and Delete. Or choose any of these privileges for all tables by selecting its check box in the header row of the grid.
3. Click on the Save button. A pop-up window prompts to submit the request. Click on the OK button. The request is submitted, and the Request Access List panel is restored, with a new entry for the request you've made.

Completing a Request for Responsibility Access

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

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

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



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

1. For each responsibility you want to select, click on the Add Row button.

2. In each row that you add, the Responsibility Name field is a list of values. In each, select a responsibility. In each row, Access Monitoring automatically populates the Application Name field with the application to which the selected responsibility belongs; you cannot change this value.

3. If you have selected responsibilities you do not want to request for the user, or you have created more rows that you need, select the Delete check box in the rows you no longer want, and then click on the Delete Row button.

No matter release you are using, click on the Save button when you are satisfied with your selection. A pop-up window prompts you to submit the request; click on its OK button. The request is submitted, and the Request Access List panel is restored, with a new entry for your request.

Viewing Requests

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

1. Specify filtering criteria by entering complementary values in any combination of the fields that run horizontally above the list of requests:

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

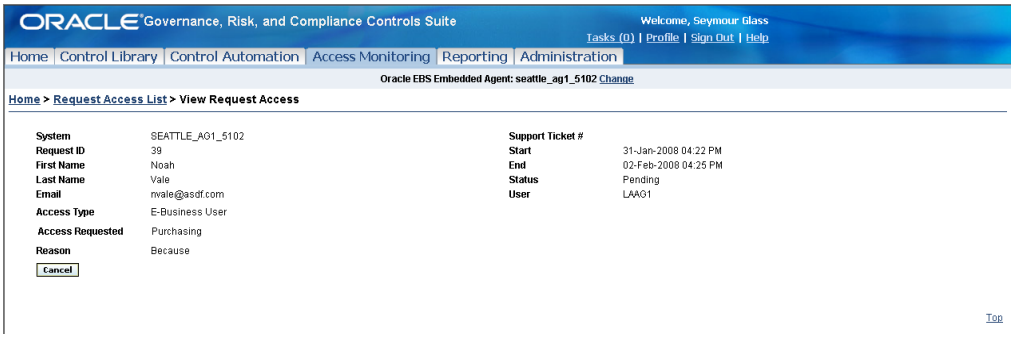
   The three date filter fields display time of day as well as date, but the time is not significant. When you execute the filter, the panel displays all requests created

on the selected date, or for which the date is the start or end date. As before, you can enter a date manually or select it from a pop-up window.

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

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

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



Access Monitoring Reports

To view reports of Access Monitoring requests, click on the Reporting tab to display a Reports panel. In a Folders area to the left of this panel, select Public Folders, then Report Center, and then Access Monitoring.

Exporting a Report

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

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

Access Monitor Request Report

The Access Monitor Request Report lists requests for database or responsibility access generated through use of the Access Monitoring feature. For each user for

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

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

- AG Source Data: Select the database for the GRCC instance whose Access Monitoring requests you wish to view. If you follow naming conventions, this instance contains the value *XXLAAPPS_AG*. You supply this value twice, first to generate a list of the remaining parameters and then, within that list, to generate the report itself.
- System: Select one or more Oracle E-Business Suite instances to have the report list requests made on those instances.
- Access Type: Select E-Biz User to have the report list requests for access to responsibilities, Database User to have the report list requests for access to database tables, or both.
- Access Requested: Select any number of responsibilities or database tables to have the report list requests for access to those items. This parameter lists only items for which access requests have been made, and depending on you selection in the Access Type parameter, may list only responsibilities, only database tables, or both.
- User: Select one or more users to have the report list requests to grant those users access. This parameter lists Access Monitoring user IDs.
- Approver: Select any number of users to see requests for which those users are designated to be approvers by Governance, Risk, and Compliance Controls Suite workflows.
- Status: Select statuses — Approved, Rejected, Failed, or Pending — to see requests at those statuses, or select All to see requests at all statuses.
- Request Date: Define a period the report should cover. You may enter dates in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the Start date and select the No Lower Value check box to start with the earliest existing request, or omit the End date and select the No Upper Value check box to finish with the latest existing request.

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

Access Monitoring User Activity Report

The Access Monitoring User Activity Report lists transactions completed by users as they implement rights granted to them through the Access Monitoring feature. In

this context, a “transaction” is a change to a value in a database table, made via direct access to that table or to a responsibility supported by the table. For each user, the report presents the user’s name, her temporary Access Monitoring logon ID, the database instance in which she is working, the start and end dates of her temporary access, the responsibility or database tables to which she has been granted access, and her transactions. For each transaction, the report presents its date and time, the action taken (select, insert, delete, or update), the name of the table and its primary key column, the column in which the change has been made, and the old and new values.

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

- Oracle ERP Agent Source Data: Select the database instance in which you want to view monitored transactions. The instance you select holds data generated by an “embedded agent” that implements Access Monitoring in an instance of Oracle E-Business Suite. If you follow naming conventions, its name contains the value *XXLAAPPS*. You supply this value twice, first to generate a list of the remaining parameters and then, within that list, to generate the report itself.
- User Type: Select the value Database User to view results for users granted direct access to database tables, Ebiz User to view results for users granted access to Oracle responsibilities, or both.
- User Name: Select the users whose transactions you want to review.
- Action Type: Select any combination of three transaction types to review: INSERT, UPDATE, or DELETE.
- Transaction Date Range: Define a period in which transactions must have occurred to be included in the report. You may enter dates and times in the Start and End fields; in that case, clear the No Lower Value and No Upper Value check boxes. Or you may omit the start date and select the No Lower Value check box to start with the earliest existing transaction, or omit the end date and select the No Upper Value check box to finish with the latest existing transaction.

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

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