ACTIVE Governance™

Service Pack Release Notes

Software Version 7.1

LogicalApps®

Restricted Rights Legend

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

Document Version AG005-710B

12/1/06

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

Contents

Service Packs for Active Governance 7.1

ACTIVE Governance both documents and enforces business controls, enabling users to demonstrate regulatory compliance and to promote operational efficiency. An ACTIVE Governance installation necessarily includes an ACTIVE Governance Platform, which offers documentary capability, and may include up to three modules that provide enforcement capability — ACTIVE Access Governor™, ACTIVE Policy Governor™, and ACTIVE Data Governor™.

From time to time, LogicalApps issues service packs that resolve issues concerning the performance of ACTIVE Governance. Each incorporates all service packs that have come before and addresses a new set of issues as well. Moreover, Service Pack 7.1SP2 incorporates hotfixes 710AAX01, 710AAX02, 710AAX03, and 710AG01.

Installation

While ACTIVE Governance is a web-based application that runs outside the Oracle Applications EBS environment, it works in concert with AppsRules, a LogicalApps product that runs within the Oracle environment. To run ACTIVE Governance 7.1, you must also install AppsRules version 7.1.

Issue AGM-299 (SP1)

AppsRules is installed on the database, forms, and concurrent manager servers on which Oracle Applications run. As part of the installation, a “remote compilation” procedure uses a file called laconfig.sh to make libraries resident on the concurrent manager server available to the forms server.

In a two-tier architecture — in which the forms and concurrent manager servers have different top-level directories (APPL_TOP) — the remote compilation procedure did not work properly. Although AppsRules was installed, its migration utilities (which move AppsRules data from one Oracle Applications instance to another) could not be used. Service Pack 7.1SP1 makes changes to three files called by the laconfig.sh file; as a result the remote compilation works correctly even in a two-tier architecture and the migration utilities can be used.

ACTIVE Access Governor

ACTIVE Access Governor detects segregation-of-duties conflicts within an organization, either preventing them from occurring or uncovering them so that they can be properly managed. Designed for use with Oracle Applications, ACTIVE Access Governor identifies conflicts at both the responsibility and function levels.

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

A user then "generates conflicts" — causes Access Governor to evaluate Oracle Applications users to note those whose work assignments violate SOD rules. Users may further create "simulation rules," which determine how SOD conflicts would be resolved if Oracle function and menu assignments were altered. Depending on his role, a user may also perform "remediation" — modify function, menu, and responsibility configurations to implement the simulated conditions.

Viewing, Defining, and Evaluating SOD Rules

Issue AGM-338 (SP1)

Access Governor displays a list of existing rules in a panel titled SOD Rules. In this panel, a user can limit the display to rules that satisfy filtering criteria. One of these is Approver — the user supplies the name of a workflow role, and the panel should display rules in which that role had been designated to approve or reject conflicts generated by the rules. In version 7.1, an attempt to filter rules based on Approver produced an error. Under Service Pack 7.1SP1, the error has been repaired and the Approver filter works correctly.

Issue AGM-288 (SP1)

It should be possible to create a segregation-of-duties rule that sets a function or responsibility in conflict with itself. Version 7.1 did not permit this to happen, but Service Pack 7.1SP1 restores this capability.

Working in an Add SOD Rule or Copy SOD Rule panel, an Access Governor user includes a function or responsibility (or group) in a rule by highlighting it in an Available Entities field and moving it to a Selected Entities field. In version 7.1, once the entity had been moved to the Selected field, it disappeared from the Available field.

Under Service Pack 7.1SP1, when a user moves an entity to the Selected field, a copy remains in the Available field so that it may be selected a second time.

Typically one would employ such a rule for a function or responsibility that enables a user to perform critical actions, and configure the rule to have an Approval Required "control type" — a user would be permitted access to the function or responsibility if a designated reviewer approves the access. Thus the rule would ensure that critical actions are always subject to approval.

Issue AGM-371 (SP2)

A "global subscriber" is a menu, function, data group, operating unit, or user configured to be exempt from conflict rules. When a menu is named as a global subscriber, and an exclusion for the same menu is configured within a responsibility (through the use of standard Oracle functionality), Access Governor would recognize conflicts involving functions available from the exempted menu, even though it should not. Service Pack 7.1SP2 corrects code so that Access Governor no longer generates spurious conflicts involving functions belonging to menus that are both named as global subscribers and excluded from responsibilities.

Issue AGM-372 (SP2)

Within an Oracle menu hierarchy, a given submenu may be excluded, and functions available from that submenu should no longer be available to users and so should no longer figure in conflicts. If, however, the submenu exists in more than one branch of menus descending from the root menu, Access Governor would consider an exclusion to apply to one instance of the submenu, but not to others, and so would continue to generate conflicts involving functions from other instances of the submenu. In Service Pack 7.1SP2, Access Governor recognizes a submenu exclusion as applying to instances of the submenu in all branches descending from the root menu, and so no longer generates conflicts involving functions available from the submenu.

Issue AGM-485 (SP2)

An Export/Import Groups and Rules program enables users to export entity groups and SOD rules from an ACTIVE Access Governor instance to CSV files (one file each for groups and for rules), and then import the data from the files to a second ACTIVE Access Governor instance. In version 7.1, a user could select an imported function group for use in an SOD rule and save the rule; although a message would indicate "SOD rule successfully created," the rule in fact would not be. This was because the import operation improperly added trailing spaces to the imported group name. When called from within an SOD rule, therefore, the now-misnamed group returned no function values. Service Pack 7.1SP2 corrects the Export/Import program so that it imports function-group names correctly, without the trailing spaces. Note that for an import operation to work, the group file must contain a record of at least one entity group and the rule file must contain a record of at least one SOD rule.

Resolving Conflicts

Issue AGM-37 (SP2)

An SOD rule may be created to have the Approval Required control type and to involve a responsibility in a conflict (either set functions available from it in conflict or set it in conflict with another responsibility). If a user has already been assigned that responsibility and so now has a conflict, one way to resolve it is to end-date his assignment to the responsibility.

To do so, an Access Governor user would query for the conflict user in the Oracle User's form, and from it use LogicalApps-specific forms to set an end date, initiate conflict analysis, and submit the revised assignment.

In earlier versions, this would launch an approval flow (because the control type of the rule is Approval Required), even though approval is unnecessary (because the effect of the change in responsibility assignment is to resolve a conflict). In Service Pack 7.1SP2, if the new end date is the current date or any date earlier than the previous end date, no approval flow is launched. If the new end date is later than the previous end date, an approval flow is launched (because the change has extended access and therefore perpetuated the conflict).

Mass Update

A Mass Update feature displays a list of conflicts generated by SOD rules that designate the user who is currently logged on to Access Governor as the approver. The user can filter the list of conflicts, select a set of them, and approve or reject the selection all at once.

Issue AGM-360 (SP2)

When the pagination.show.all property (see issue OC-2464 on page 5) is set to null, an attempt to open the Mass Update panel produces an error. The property should be set to a value greater than 50; in Service Pack 7.1SP2, the value is set by default to 1,000, and the error no longer occurs.

Issue AGM-405 (SP2)

The Mass Update panel should display only conflicts for which the user currently logged on to Access Governor is the approver. In version7.1, however, the panel might display no results, or display conflicts for which other users were the designated approvers. Service Pack 7.1SP2 resolves these issues and correctly displays only conflicts appropriate for the current user.

Issue AGM-424 (SP2)

In the Mass Update panel, a user can click on an Approve All button to approve all of the conflicts available for him to review. In version 7.1, however, the use of this button would produce no result other than to display the message "Successfully approved 0 results." Service Pack 7.1SP2 corrects the approve-all feature so that it does in fact approve the conflicts assigned to the user, and the message correctly reports the number of approved conflicts.

Simulation

A simulation rule may propose that a function or menu be excluded from a responsibility, or that a function or submenu be removed from, or included in, a menu. One evaluates simulation rules by running a "background program" that creates two "snapshots" — the first is a set of conflicts that are generated with functions, menus, and responsibilities as they are actually configured, and the second is a set that would be generated under the simulated conditions. ACTIVE Access Governor compares the two and presents results — a list of conflicts that would no longer exist, as well as those that would be newly generated.

Issue AGM-276 (SP1)

In version 7.1, the background program that evaluates simulation rules ran slowly. For Service Pack 7.1SP1, indices were created in the database tables that contain actual and simulated snapshots, with the result that performance is improved significantly.

Issue OC-2464/AGS-454 (SP1)

After creating and running simulation rules, a user can open a Simulation Results panel to view a list of all conflicts that would be resolved or newly created by the simulated changes, or all users or responsibilities that would be affected by the changes. In version 7.1, the Simulation Results panel could take an excessively long time to load. Service Pack 7.1SP1 addresses this issue in several ways:

- Two SQL queries select records for display in the Simulation Results panel — one returns records of conflicts that would be resolved, and the other those that would be created. The columns targeted by WHERE clauses in these queries are now indexed, with a resultant performance improvement.
- In version 7.1, the Simulation Results panel presented records of all conflicts that would be affected by simulation rules. It also provided fields that one could use to filter these records after they were initially displayed. Service Pack 7.1SP1 alters this behavior: The Simulation Results panel displays no records until a user has entered filtering criteria. Because those criteria would typically reduce the number of records to be fetched from the database, performance improves.
- In the footer row of the lists, one can select a number in a 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 chosen for display.) In the Show Results list box, one can choose the value *All*. In version 7.1, the Simulation Results panel would then attempt to list all records, no matter how many, in a single page. In Service Pack 7.1SP1, a pagination.show.all configuration parameter sets a limit on the number of records returned when a user selects the Show All Results option in a list. (The parameter is available from the Manage Configuration Properties link of the Administration tab in the ACTIVE Governance Platform.) Because this parameter reduces the number of records to be displayed at once, performance improves.

Issues AGM-277 and AGM-303 (SP1)

In version 7.1, the Simulation Results panel could show incorrect results. It might show unresolved conflicts as resolved, or fail to show those that would be resolved. It could show new conflicts that would not actually be created, or fail to show new conflicts that would. Service Pack 7.1SP1 refines the SQL queries that select records for display in the Simulation Results panel, and these incorrect results are eliminated.

Issue AGM-322 (SP1)

After evaluating simulation rules, a user may run remediation, which causes Access Governor actually to implement the simulated function, menu, and responsibility changes in the Oracle EBS environment. The remediation background program generates a log file that contains a record of each requested change — each exclusion of a function or menu from a responsibility, or removal or inclusion of a function or submenu in a menu. Beginning with Service Pack 7.1SP1, each record in the log indicates either that the change has been made successfully or that it could not be made (typically because after a simulation run but before remediation, a user's manual change in the Oracle system duplicated a change proposed in a simulation rule, and so nothing remained to be done for that rule).

Access Monitoring

In version 7.1, ACTIVE Access Governor added an Access Monitoring feature, which enabled users to request temporary access (for themselves or others) to database tables or Oracle responsibilities. 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 to the requested objects, and a reason why access is sought. Each request is subject to approval, and if approval is granted, the resulting access is continually audited.

Issues AGM-343 (SP1) and AGM-366 (SP2)

The Access Monitoring feature automatically generates a logon password for a user granted access to an Oracle responsibility. In version 7.1, this password was five characters in length. A client had set its Oracle Signon Password Length profile option to eight; because the password generated by Access Monitoring was shorter, an approved access request resulted in a message stating that the request had failed.

Service Pack 7.1SP1 introduced a temporary fix: the automatically generated Access Monitoring password was increased to eight characters in length.

Service Pack 7.1SP2 replaces this with a permanent fix: The Access Monitoring feature reads the Signon Password Length profile option and generates a password of the length that it sets (or, if the option is not set, generates a password of eight characters). As a result, the password-length-related failure to grant access to an Oracle responsibility no longer occurs.

Issue AGM-425 (SP2)

ACTIVE Governance enables users to configure workflows that distribute access requests to approvers. In version 7.1, these requests appeared only in the Task Inbox of the ACTIVE Governance Platform, and so approvers were required to log on to ACTIVE Governance in order to know they had access requests to approve. In Service Pack 7.1SP2, an approver receives access requests not only in the Task Inbox, but also by email. He is therefore alerted to access requests even if he is not logged on to ACTIVE Governance, although he must log on to approve requests.

Issue AGM-426 (SP2)

Temporary user IDs should not be available to be assigned to two or more users at once. In version 7.1, in most cases, they were not: When a user saved an access request, the user ID selected for the request disappeared from the field in which IDs can be selected. In one case, however, they could: Two or more users could begin to generate access requests simultaneously. As long as none had yet saved the request, all could select a common ID. Then all would be able to save their requests and, if they were approved, the ID would improperly be assigned to more than one user.

Service Pack 7.1SP2 corrects this flaw: When two or more users select an ID simultaneously, the first user to save the request gets the ID. When the others try to save their requests, they receive a message stating that the ID is already in use and they must select another.

Issue AGM-432 (SP2)

A temporary ID for access to an Oracle responsibility should be reusable: When the assignment of an ID to a user has expired, the ID should become available for assignment to another user. Earlier, the first assignment of an ID to a user worked correctly, but the second time it was assigned, the new user would receive an error message when she attempted to log on to her temporary responsibility. Service Pack 7.1SP2 corrects this problem: When an ID is first assigned to a user, that user is able to log on. When the assignment expires and the ID is given to another user, that user is able to log on as well.

Access Governor Reports

Issue AGM-297 (SP1)

A Responsibilities with Conflicts Report lists responsibilities for which conflicts exist, and identifies the components of each conflict as well as the SOD rule that defines it. As a parameter to the report, a user can select a responsibility from a list to view only conflicts for that responsibility. In version 7.1, ACTIVE Access Governor took an excessive amount of time to generate the list of responsibilities from which one could set this parameter. Service Pack 7.1SP1 alters the query that generates the list, so that the list is presented to the user much more rapidly.

Issue AGM-309 (SP1)

Several reports — Conflict Summary, Conflicts by Responsibility or Application, Responsibilities with Conflicts, Responsibility Menu, User Conflicts, and User Conflicts Trend Analysis — allow the user to select a snapshot name as a parameter. Each then presents results only for that snapshot (a set of conflicts created at a given moment, as distinct from other sets generated at other moments). If more than one snapshot were generated on a given day, some reports enabled the user to select only the first snapshot from that day, and others only the last. Under Service Pack 7.1SP1, the Conflicts by Responsibility or Application report offers (by design) only the last snapshot generated on each day; all the other reports offer all snapshots generated on each day.

Issue AGM-186 (SP1)

Three Oracle EBS Security reports provide information about the responsibilities, menus, and functions to which users have access. One of the reports presents results by user, another by function, and the third by responsibility. All gather results from a database table that is refreshed by a background program called LAA Populate User Access Data Table. In version 7.1, this program provided incorrect APPL_ID (application identifier) values. Service Pack 7.1SP1 corrects this error.

Issue AGM-433 (SP2)

In earlier versions, the LAA Populate User Access Data Table program took an excessive time to run. Service Pack 7.1SP2 significantly reduces the time in which the program runs.

Issue AGM-290 (SP1)

Service Pack 7.1SP1 enhances the Oracle EBS Security reports as follows:

- All three reports include a new parameter — Show Menu/Function Exclusions — that enables the person running the report to determine whether it should display results for menus and functions that are excluded from responsibilities, for menus and functions that are not excluded, or both.
- In all three reports, an Active Responsibilities parameter should have enabled the person running the report to choose whether it displayed results for active responsibilities (and menus and functions available from them), inactive responsibilities, or both. In version 7.1 it did not work properly, but in Service Pack 7.1SP1, it does.
- In all three reports, a Grant parameter should have enabled the person running the report to choose whether it displayed results for submenus and functions for which the Grant check box is selected or cleared. In version 7.1 it did not work properly, but in Service Pack 7.1SP1, it does.
- Owing to an error in code that joined "subreports," the Oracle EBS User Details Report did not run. In Service Pack 7.1SP1, the error has been corrected and the report runs correctly.
- In the Oracle EBS User Details Report, one could select the users about which it returned results either by selecting *All* for a User parameter or by typing the names of users in an Enter a Value field. In Service Pack 71.SP1, the User parameter displays a list of users, from which the person running the report can make selections; the Enter a Value field is no longer available.
- The Oracle EBS Responsibility Details Report should have provided a parameter that enabled a person running the report to select the responsibilities about which it displayed results. In version 7.1 it improperly provided a parameter for selecting users; Service Pack 7.1SP1 replaces that parameter with a Responsibility Name parameter, which presents a list of responsibilities from which the person running the report can select.
- In the Oracle EBS Function Details Report, one can select functions (and the applications to which they belong) about which the report should return results. In version 7.1, the report did not return results for all users or responsibilities associated with the functions selected for the report. In Service Pack 7.1SP1, it does.

Issues AGM-450 and AGM-443 (SP2)

Four reports that present information about conflicts that have been generated now accept Set of Books and Operating Unit as parameters. A user running one of the reports can select a set of books or an operating unit to view conflicts generated in that set of books or operating unit. For either value, the user can instead select any number of operating units or sets of books, to view conflicts for that selection, or choose all to view items from all operating units or sets of books. The four reports are User Conflicts, Responsibilities with Conflicts, User Conflicts Master CSV, and Conflict Summary.

Issue AGM-379 (SP2)

The User Conflicts Master CSV Report produces a CSV (text) file that contains data about conflicts and about the SOD rules that generated them. The data is intended for export to an Excel file. In version 7.1, the CSV file contained errors, and Service Pack 7.1SP2 makes the following corrections:

- Each of two columns contained the name of a user affected by a conflict. One of these duplicate columns is deleted; the other remains under the label USER_NAME.
- A misaligned MENU_NAME column heading now appears correctly above the column containing menu names.
- Two columns — REVIEWER_EMPLOYEE_NUMBER and REVIEWER_FULL_NAME — contained the workflow role designated as an approver for conflicts generated by a rule. One of these duplicate columns is deleted, and the other is renamed REVIEWER.

ACTIVE Policy Governor

ACTIVE Policy Governor implements “control monitors,” each of which uses structured query language (SQL) statements to select records of actions subject to control and marks them as “suspect tasks.” A control monitor is attached as an “automation” to a control created in the ACTIVE Governance Platform, and is either run manually, or scheduled to be run automatically, from the Platform. ACTIVE Policy Governor also enables users to configure workflows that distribute suspect tasks to reviewers.

Issues AGM-224 and AGM-310 (SP1)

LogicalApps provides a set of “prepackaged” control monitors, which clients may import and use in place of, or in addition to, the monitors they create in Policy Governor. The SQL statements in these prepackaged monitors call functions contained in a file called la_cm_pkg1.plb, and use database views defined by a file called la_cm_views.sql. Both files contained flaws that prevented them from loading properly during installation. Service Pack 7.1SP1 corrects both files; they now load properly and the prepackaged control monitors run as intended.

ACTIVE Data Governor

ACTIVE Data Governor applies change control to Oracle Applications form fields. It implement rules — one for each field — that apply “control types”: an Audit rule tracks changes to fields, and presents a history of those changes in reports. A Reason Code rule tracks changes as well, but also requires a user to supply a reason for a change and may send notification to another person or rule. An Approval rule both tracks change and requires a reason, but also requires that a specified person or rule approve the change.

Issue AGM-431 (SP2)

Through the use of concurrent requests called LA AppsControl Data Export and LA AppsControl Data Load, one can migrate change control rules from one instance of Oracle Applications (with ACTIVE Data Governor installed) to another. Because the

LA AppsControl Data Export request did not capture “audit translations” properly, the rules were corrupted in the destination instance. Service Pack 7.1SP2 modifies the LA AppsControl Data Export request so that migrated rules now run correctly on the destination instance.

Issue AGM-430 (SP2)

A Change History report shows the old and new value for each change made to a field subject to change control. A Request Date parameter to the report enables users to specify starting and ending dates, and the report should display data for changes that occurred between the dates. In version 7.1, however, the report displayed only data for changes that occurred since the last time the report was run, no matter how the Request Date parameter was set. Service Pack 7.1SP2 corrects underlying code so that the report properly displays data for all changes made in the period defined by the Request Date parameter.