Oracle Fusion Cloud Risk Management

Using Advanced Controls

25D

Oracle Fusion Cloud Risk Management
Using Advanced Controls

25D

G40946-02

Author: David Christie

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 Introduction

Overview of Oracle Advanced Controls

Oracle Fusion Cloud Advanced Controls regulates activity in business applications. It includes two components:

- Oracle Advanced Access Controls identifies users with sensitive-access and separation-of-duties conflicts in your applications. Each of these users has been assigned a single role or a combination of roles whose authorizations create the potential for fraud or significant error.
- Oracle Advanced Financial Controls detects fraud, error, and other risk in transactions completed in Oracle Cloud applications, or in change tracking from the Oracle Cloud audit framework.

As you work with either of these components, you create models, then deploy controls from those models. Each model consists of filters that establish a risk logic. Each control adopts the risk logic of the model it's based on.

- Access-model filters designate roles or privileges that, individually or in combination, would allow an individual user to complete risky behaviors. They then select users assigned those points of access.
- Transaction-model filters define aspects of risk, then select transactions exhibiting the defined risk. (Models created in Oracle Advanced Financial Controls are known as "transaction models.")

A model returns temporary results: suspect records that are replaced each time the model is evaluated. Use a model to test a risk-logic definition before applying that definition in a control. Or, if you're an auditor, use models to assess the risk inherent in a system at a given moment.

A control returns permanent results: records of violations that remain available to be resolved no matter how often the control is run. Each record is known as an incident; each control names one or more result investigators, who are responsible for resolving the incidents it generates. Investigators can track the status of incidents in result-management pages.

Models and controls can analyze data from multiple data sources. By default, an Oracle Cloud data source supplies access and transaction data from Oracle Fusion ERP, SCM, HCM, and CX applications. "Synchronized" data sources provide data from other applications, but only after you set up connections to them. These sources include:

- EPM-ARCS, which provides access and transaction data from Enterprise Performance Management Account Reconciliation.
- Up to three instances of EPM-FCCS, each providing access and transaction data from a distinct "pod" in Enterprise Performance Management Financial Consolidation and Close.
- OCI, which provides access data, but not transaction data, from Oracle Cloud Infrastructure.

You can also import role-assignment data from applications, such as Workday and Salesforce, that aren't among the synchronized data sources to which you can set up connections.

Some features apply only to Oracle Advanced Access controls. These include:

- Visualizations. These are graphic depictions of paths that lead from users to roles they're assigned and ultimately to access points that models or controls define as conflicting.
- Simulations. These preview the effects of steps that may be taken to resolve access conflicts identified by controls.
- Provisioning rules. These identify pairs of conflicting roles. You can use them to prevent risky role assignments.

- Advanced Access Requests. This implements a workflow for requesting or assigning ERP roles. The workflow incorporates analysis by access controls.

Related Topics

- Set Up and Maintain Data Sources

Common Concepts

Notifications and Worklists in Advanced Controls

Worklists, notifications, and email alerts can inform users of tasks or events that require their attention.

In Oracle Fusion Cloud Advanced Controls, a worklist is a record of pending incidents returned by a control. It's also a link to the Results page for resolving the control's incidents. Each user sees only worklists concerning controls for which he or she's a result investigator. They appear on a Worklists page, which is the landing page for the Results work area.

Users may also receive notifications, email alerts, or both if your organization activates them. It can choose to activate notifications or alerts for some features, but not for others. By default, both are active for all features. (See *Activate Alerts*.)

- Notifications are available from the Notifications icon in the global header. (It looks like a bell.)
- Email alerts are sent to the email address associated with the user account for each user.

New notifications and email alerts appear with each run of a job called Advanced Controls Notification. Each provides a link to the page on which its recipient may act on its information.

One type of notification or alert informs users of controls with new incidents, or of existing incidents that have been reassigned. Each user receives notice only of controls for which he or she's a result investigator, or of incidents reassigned to him or her.

New incidents are those generated by a control after the last time the recipient was alerted. For these:

- A notification informs its recipient of a single control that's generated at least one new incident. With each run of the notification job, each user may receive multiple notifications.
- An email alert lists every control that's generated at least one new incident for which the recipient is authorized. With each run of the notification job, each user receives only one email alert.

A second type of notification or email alert announces the creation of a control. Recipients include all users authorized as owners of the newly created control (except the person who created the control).

A third type of notification or email alert concerns tasks related to Advanced Access Requests, in which users may request role assignments, or review or approve those requests:

- The person who submits a request receives confirmation that the request has been made, and later that it's been completed. If the submitter made the request on behalf of another user, that user also receives these confirmations.
- A user selected as a reviewer receives notice of requests to be reviewed. The email alert is consolidated: For each recipient, the alert lists all the user's review assignments since the user previously received an alert.
- A request approver receives notice of new requests that aren't assigned for review, requests assigned to reviewers and pending review, and requests that have been reviewed and are pending final decision. Again, email alerts are consolidated.

A fourth type reports information about error conditions, such as a job failing or concluding with errors, or a control, model, or incident lacking an eligible owner or other authorization. (To receive a message concerning an object lacking an eligible owner, a user must have a Mass Edit Security Assignments privilege. Other security-related messages go to the owners of an affected object.)

Secure Records in Advanced Controls

To work with records of models, advanced controls, or incidents, a user must be both "eligible" and "authorized" for them.

To be eligible for records of an object, a user must be assigned a role that grants privileges to work with that object. Then:

- An eligible user who creates one of these records is automatically authorized as its owner.
- The owner authorizes other eligible users as owners, editors, or viewers. An owner can edit details of the record, including its data-security configuration. An editor can't modify the security configuration, but can modify other details. A viewer can see record details, but can't change them. A user must have one of these authorizations to have access to the record.

To authorize users:

- An owner of a model clicks a Security Assignment button in the page to edit the model. This opens a Security Assignment page. (The button isn't available while the model is being created, but appears immediately after its creator saves or submits it for the first time.)
- An owner of a control configures security for it and the incidents it generates as steps in the control-deployment process. Or, in the page to edit a control, the owner expands a Security Assignment list to select either of two Security Assignment pages, one for the control and one for its incidents.
- An owner of an individual incident can open Security Assignment from the page to edit the incident. These security edits would apply to that incident, but not to others generated by its control.

In any of these cases, if you're an owner you can add individual users or user groups. A group is a set of users with an authorization for a type of object. Assigning groups to records (and users to groups) is typically the more efficient approach to managing security.

- To select an individual user, click Add in a User Assignments panel. Search for and select a user in a Name field. In an Authorized As field, select Owner, Editor, or Viewer. Then click a Save button.

  You can select less access than a user is eligible to have. For example, a user may be eligible to work with models at any of the three levels. If you select that user as a viewer for a model, he can't edit that model, even though he remains eligible to be selected as an owner or editor of other models.
- To select a user group, click Add in a Group Assignment panel. Search for and select a group, and then save that selection.

  Each group has a single authorization. As you select a group for a record, you can view the authorization, but you can't change it. You may assign multiple groups to a record, to combine authorizations.

  A group is available to be selected for a record only if at least one of its members is eligible for that record. Groups with no eligible users are excluded.

  Over time, members may be added to or dropped from groups, or their role assignments may change. This may result in a group having been assigned to a record but no longer having members who are eligible for it. If so, a warning icon appears next to the group name.

- To edit or delete a user or group, click the edit icon in its row.

Select Perspective Values in Advanced Controls

A perspective is a set of hierarchically arranged values. Each represents a context in which models, controls, and incidents exist. You relate individual perspective values to individual object records, to catalog them by organization, region, or any other concept your organization finds meaningful.

You can:

- Assign values to a model in the Perspective Assignment panel of the page to create or edit the model.
- Assign values to a control and to the incidents it generates both at once. You can do this in the Perspectives page of the control-deployment process, the page to edit a control individually, or the page to mass-edit controls. In each, you can make two selections: In Control Perspective Assignment, you select values that apply to the control itself. In Result Perspective Assignment, you select values that apply to incidents generated by the control.
- Modify the values an incident inherits from the control that generated it. Use a Result Perspective Assignment panel in the page to edit an incident individually, or to mass-edit incidents.

In any of these cases, you initially work with a single list field. Select a perspective hierarchy in that field, and the panel expands to display Available and Selected fields. Move the values you want from the Available field to the Selected field.

As you select values:

- You can type text in a Perspective Name search field to produce a list of matching perspective values. The search returns values without concern for hierarchical relationships.
- You can use View options to expand or contract the entire hierarchy or nodes within the hierarchy.

Also note the following:

- For an object's perspective-selection list field to be available, you must associate at least one perspective hierarchy with that object. You can associate perspectives with objects in the Module Perspectives page of the Setup and Administration work area.
- A hierarchy name may appear with an asterisk in the list field in which you select it for an object. That means it's required for the object; you can't save an instance of that object if no value is selected from that hierarchy. (The required designation is made when the hierarchy is associated with the object in the Module Perspectives page.)
- If two or more perspective hierarchies are associated with an object, you can assign values from any combination of them, although you select from one hierarchy at a time.

Related Topics

- Perspectives

Filter Model, Control, and Result Lists

By default, each of the pages for managing models, controls, or results filters the items it lists.

- A Models page displays models whose status is active, and a Controls page displays controls whose status is active, regardless of who created them. To do so, each implements a saved search: Active Models in the one case, and Active Controls in the other.

- A Results by Control Summary page lists controls that have generated incidents that have yet to be resolved. To do so, it implements a saved search called Pending Results.
- From the record of a control in the Results by Control Summary page, you can open a page listing the incidents generated by the control. These too are subject to the Pending Results search, which displays only incidents that have yet to be resolved.

Create Searches

In any of these pages, you can create your own searches: Click the **Show Filters** option and, in a Filters panel, select filtering values. Then click **Search**.

As you create searches, the filtering values you select generally have an AND relationship: A search returns records that satisfy all filtering criteria. In the Models page, for example, you may select yourself in the Created By search field and a range of dates in the Creation Date field. You'd then see models created by you on those dates.

However, there's an exception. You can add search fields to the default selection. Click the **Add Fields** option to do so. You can add new instances of fields that already exist, and enter distinct search criteria in these fields. Duplicated fields have an OR relationship; each returns results independently of the other. For example, two Created By fields in the Model page would specify two users, and a search would return models that each of them has created.

Save Searches

You can save your searches. After selecting filtering values in the Filters panel, select **Save**. Then:

- Enter a name for the search.
- Select or clear a **Set as Default** option. Selecting this option causes the search to run whenever you open the page it applies to. You can select this option for only one saved search in each page.

To run a saved search, select it in the **Saved Search** field of the Filters panel. Then click the **Search** button.

State and Status of Records in Advanced Controls

Models, controls, and incidents are assigned status and state values. You can use these values to filter records in pages that list object records, and in Oracle Transaction Business Intelligence (OTBI) analyses.

The application assigns status values to models. Users or the application may set control status. A regular aspect of resolving incidents is for result investigators to assign status values that indicate what, if anything, is to be done about them (although some values are set by the application). State values are typically a function of the status values assigned to objects.

Here are the status and state values that apply to object records.

Models

Model status values are **Active** and **Inactive**; model state values are **Approved** and **Invalid**. A model may be Active and Approved, or it may be Inactive and Invalid; there's no other combination of model state and status. The application sets these values for each model.

- Active status and Approved state indicate that model filters use valid and current business objects and attributes of those objects. You can use the model to generate results, and you can deploy it as a control.
- Inactive status and Invalid state indicate that model filters use at least one business object, or attribute of an object, that's obsolete. You can't use the model to generate results, or deploy it as a control.

Controls

Control status values are also **Active** and **Inactive**; control state values are also **Approved** and **Invalid**. If you make no selections, the application sets a status and state value for each control, in the same combinations and for the same reasons as it does for models.

However, if the state is Approved, you can select the status value as you deploy or edit controls. (When you deploy controls, their state is Approved by default.)

- Select Inactive for a control you want to hold in reserve, or no longer want to use. All incidents generated by the control are set to a Control Inactive status. You can't copy, export, run, or schedule an inactive control.
- Select Active for a control you want to put to use. You can copy, export, run, or schedule active controls.

If the application sets a control to the Invalid state, however, the application sets its status to Inactive and you can't change it.

Incidents

Because selecting incident status is an essential aspect of resolving incidents, a topic titled *Incident Status and State* discusses these items in detail. For reference, however, the following table shows status names, whether they can be selected by users or are set by the application, and the states they correspond to. (State values are set by the application as a function of the status selected for the incident.)

Status	Selected By	State
Assigned	Application or user	In Investigation
Remediate	User	In Investigation
Accepted	Application or user	Approved
Resolved	User	Approved
Control Inactive	Application	Closed
Closed	Application	Closed

View Model or Control Details

Each row on the Models and Controls pages provides summary information about a model or control. Here's how you can view full details.

Expand Details

Each row presents summary details about a model or control. The details you see depend on selections you make in the View Columns menu. However, you'd typically select the Name and Results Count columns, whose values serve as links to other pages. Among the columns you can select:

- Results Count, for a model, is the number of violations its most recent run discovered. For a control, it's the number of pending incidents the control has generated; in this case, however, the field reports only the incidents you (as the currently logged-on user) have access to. In either case, it's also a link to a page where you view results.
- In the Type column:
    - **Access** indicates a model or control created in Oracle Advanced Access Controls.
    - **Transaction - Pattern** indicates an Oracle Advanced Financial Controls model that uses a pattern filter to perform statistical analysis. (It may also use standard or function filters.)
    - **Transaction - Defined** indicates an Oracle Advanced Financial Controls model that uses only standard or function filters to define a risk.
    - **Transaction** indicates a control created in Oracle Advanced Financial Controls. The distinction between Pattern and Defined isn't meaningful for a control, because you can't deploy a pattern model as a control. All transaction controls are defined controls.

You can expand a row to view more detail about the object it represents. To do so, click a triangular icon in the row.

For example, Hector Lassie created a model called "Credit memos paid to a wrong pay site" on August 12, 2025. He updated it on September 17, then ran it on the same day. It returned 293 records. The row for this model might show its name, September 17 as its run date, and 293 as its results count. But if you click the triangle icon in this row, a hidden panel opens to display additional values. These include its description and its type, in this case Transaction - Defined. Details also include Hector Lassie as the person who created, updated, and ran the model, the dates these actions occurred, and its run status (Completed in this case).

View Perspective and Related-Record Values

For a model or control, the expanded display of details includes a perspective field, which shows the number of perspective values assigned to the object. A control may be related to objects created in Oracle Fusion Cloud Financial Reporting Compliance. The expanded display for the control also includes a Related Records field, which shows the number of related objects. Hover over each number to reveal the names of the perspective values (and hierarchies they belong to) or of the related objects.

For example, a model called Duplicate Payables Invoices might be assigned a single perspective value. So the number 1 would appear in the Perspectives field of its expanded-details panel. But if you place the mouse cursor over this number, a display shows the name of the perspective value and its hierarchy, for example North America in the Organization perspective.

Display Results

From the Models page, you can't run a model, but you can view the latest results of a model that has been run. From the Controls page, you can both run a control and view the results. To view results in either case, you select the Results Count value for an object.

The row for the "Credit memos" model, for example, would include a results count of 293. Click that entry to open a page in which each row represents one model violation.

Attach Documents to Controls and Incidents

You can attach any number of documents to advanced controls and incidents they generate. An attachment may, for example, be a text file, spreadsheet, or website that provides more information about a control or incident than its description contains.

To attach documents, work in a page to perform an individual or mass edit of controls or incidents. You may simply drag a file into the Attachments area of an edit page. Otherwise:

1. Click the link in the Attachments area.
2. Click Add Link or Add File.
3. Depending on your selection:
    - Type, or copy and paste, a URL into an Add Link dialog box. Then select Save and Close.
    - In a file-upload dialog, navigate to and select the file you want. Then select Open. (The title of the dialog, and the name of the option you select to complete the attachment, may depend on the web browser you use.)

To view attachments, you may:

- Select them in an Attachments field of the view or edit page for an individual control or an individual incident. Initially the page lists up to five attachments. If there are more, a Load More Items link appears. Click it to display more attachments, five at a time until all are on display. Click the link for a URL attachment, or click the Download icon for a file.
- Open them from an Attachments column of a page that lists all the incidents generated by a control. For each incident, the column entry displays the name of the first attachment; click it to open it. If there are additional attachments, the column entry also contains a phrase indicating the number of attachments beyond the first one. Hover over it to produce a list of the additional attachments, and click on the name of the one you want.

Synchronize Model Result Data for OTBI Reporting

You may use OTBI analyses to review results returned by access or transaction models. If so, run a Report Synchronization job to refresh subject areas that supply data to these analyses.

This job updates data in these subject areas:

- Risk Management Cloud - Advanced Access Models Real Time
- Risk Management Cloud - Advanced Financial Models Real Time

The typical development process involves defining a model, running it, and reviewing results. If those results include false positives, or exclude records you had expected, you revise the model, run it again, and retest. This process may include multiple iterations.

If you use an OTBI analysis to review results, you'd run the Report Synchronization job after each run of the model. You can select models as you run the job, which ensures efficiency: You synchronize data only for the models you're interested in.

To run the Report Synchronization job:

1. In the Advanced Controls work area, select the Models tab to open the Models page.

2. Select models to be synchronized. You can work from the complete list of models, or filter it. To select one model, click its row. To select a continuous set, click the first model in the set, hold the Shift key, and click the last model. To select a discontinuous set, hold the Ctrl key as you click model records.
3. Expand the Actions menu and select its **Synchronize Results in OTBI** option. A message presents a job ID. Note the ID, then close the message.
4. In the Models page, click the Monitor Jobs button. In the Monitor Jobs page, locate the row displaying the Job ID you noted, and track the progress of the synchronization.

Note: A separate Report Synchronization job, which is run from the Scheduling page in the Setup and Administration work area, doesn't update model-result data.

Import and Export

Import Models, Controls, or Conditions

You can import models, advanced controls, or global conditions. These items may have been exported to a file. Or, you may import delivered content: models (but not controls or global conditions) developed by Oracle. Delivered content is available by default for the Oracle Cloud data source, and becomes available for each synchronized data source to which you set up a connection.

A Version Limitation

A file exported from an Oracle Fusion Cloud Advanced Controls instance can be imported only into an instance at the same version or the next version. For example, if you export from a 25C instance, you can import into another 25C instance or into a 25D instance. In the export file, you can search for a <grcVersion> tag to identify the version from which the file was exported.

Begin the Import

If an import file contains controls, you can import them either as controls or as models:

- To import them as controls, select Actions > Import in the Controls page. To import them as models, select Actions > Import in the Models page.
- If you import controls as models, elements that apply only to controls, such as priority or result type, aren't imported. Neither are perspective values selected for the controls, nor the result investigator.
- Before you import controls as controls, be sure that perspective values cited in the controls exist in the target instance.

If an import file contains models, you can import them only as models. Or, if you want to import delivered-content models, there's no need to select a file at all. In either case, select Actions > Import in the Models page.

If an import file contains global conditions, you can import them only as global conditions. Select Actions > Import in the Access Global Conditions page.

Having selected an Import action, enter values in a series of import pages, selecting Next or Back to navigate among them.

Related Topics

- Perspectives

Select the Import Source

The way you select items for import depends on the type of item you're selecting.

To import controls (as controls) or global conditions, use an Import page to select a file that contains the items you want to import. Click Browse, navigate to the location of the file, and select the file name. That name then populates the File field on the Import page.

If you're importing models, an Import page provides two options.

- You can use an Import File panel to browse for a file containing exported models or controls. The procedure is the same as the one for importing controls or global conditions.
- You can use an Import from Content Library panel, from which delivered-content models are available. They're organized in libraries that support product families. In support of the Oracle Cloud data source, an Enterprise Resource Planning library, a Human Capital Management library, and other libraries contain links to access, transaction, and audit models. A library is also available for each synchronized data source you set up. Select a link to a set of models in one of the libraries.

If you use the browse option to select a file, select Next to move to a Select Items page. If you use the Import from Content Library feature in the Import page for models, the application takes you to the Select Items page automatically.

Select Items to Import

In an Import: Select Items page, review and then select from a list of the models, controls, or global conditions available for you to import.

To filter items, search by name or description. Then select the checkbox in the row for each item you want to import.

Here are some issues to consider as you select items:

- If you're importing controls, select 100 or fewer. This limit doesn't apply to models or global conditions.
- You can import only items that use business objects you're assigned access to. (An administrator uses a Business Object Security feature to assign transaction objects to users.)
- In general, if a transaction model or control calls an imported object, select the model or control for import only if the object already exists in the target instance. However, this restriction doesn't apply to delivered-content models.

Related Topics

- Work with Imported Objects

Resolve Duplicate Names

You can't import a model or control if its name matches that of a model or control already existing in your target instance. This applies both to items you select directly and items your selections depend on.

- If you select a transaction model or control with a filter that specifies a user-defined object, that object and its data set control are also selected for import automatically. (A control that generates data for a user-defined object is known as a data set control.)
- If you select an access model or control that calls entitlements, the entitlements are also selected for import.
- If you select a delivered-content transaction model that calls an imported object, that object is also selected for import.

You can resolve most duplicate-name conflicts during the import process:

- You can rename models, controls, and user-defined objects. The import process can detect whether a model and its user-defined object are revisions of an earlier version; if so, when you import the model, you're required to rename its object.
- You can't rename entitlements or imported objects. If one of these items with a matching name exists in your target instance, the item from the import file isn't imported, and you continue to use the already-existing item. You can, however, edit existing entitlements to update them. You can also use a separate import process to refresh imported objects.

Use the Import: Resolve Duplicate Name Violations page to address the naming conflicts you can resolve. The page may list models or controls individually, or may list user-defined objects and their data set controls as paired items.

You must resolve all these naming conflicts before you can move beyond the Resolve Duplicate Name Violations page. Review the Status column to determine which conflicts require your attention. For each item, select an action:

- Rename means that you'll import the item from the import file, but under a unique name that you supply. Do so in the New Record Name field.
  As you import a user-defined object and its data set control, you can rename them with distinct names. This is so even though, if you were to deploy a data set control from a model, its user-defined object would be created automatically, and the control and object would necessarily share the same name.
- Use Existing means that you won't import the item from the import file. The item already existing in your target instance will satisfy any dependency relationships with other items you import. Because there's no need to supply a new name, the New Record Name field is inactive when you select the Use Existing option.
  If you select Use Existing for either a user-defined object or its data set control, you must also select Use Existing for the other item in the pair.

In some cases, Rename is the only action available to you:

- If an import model cites a user-defined object, and the name of that model matches the name of an existing model, you must either rename the import model or remove it from the import job. You'd use the Rename option to rename the model, or return to the Select Items page to remove it.
- If the name of either a user-defined object or its data set control duplicates an existing name, but the other name is unique, you must rename both. Once again, you can give the object and its data set control distinct names.

After acting to resolve naming conflicts, click Validate. This determines whether new names for import items introduce new conflicts with existing-item names. If so, you must resolve them.

Related Topics

- Entitlements in Access Models and Controls
- Work with User-Defined Objects
- Work with Imported Objects

Resolve Data Sources

Use the Import: Resolve Data Sources page to designate the EPM-FCCS pod for which you're importing EPM-FCCS models, controls, or global conditions. This step in the import process applies only to the import of EPM-FCCS data.

You can set up as many as three EPM-FCCS data sources, each of which supplies access and transaction data from a "pod" in Oracle EPM Financial Consolidation and Close. By default, they're named FCCS 1, FCCS 2, and FCCS 3. In the Resolve Data Sources page, you can designate import targets for as many of these FCCS data sources as you've set up.

- An Imported Data Sources field identifies the pod associated with the import objects you've selected from the source environment.
- In a Mapped Data Sources field, select the FCCS pod to which you're importing the objects in your target environment.
- You can click an icon in an Impacted Objects field to see a list of the objects you're importing.

If a file contains objects from multiple FCCS data sources, the Resolve Data Source page prompts you to specify mappings to each source.

Complete the Import

In an Import: Review page, review the selections you've made.

If you want to make changes, navigate back to the appropriate page and do so. If you're satisfied with the import, select Submit. You can track the progress of the import job in the Monitor Jobs page. It's available from either the Models or Controls page.

Export Models, Controls, or Conditions

You can export models, advanced controls, or global conditions from a source instance to a file.

When you export models or controls, security assignments configured for them aren't exported with them. A user who subsequently imports them would automatically be their owner in the destination environment, and could configure additional security for them in that environment.

1. In the Models, Controls, or Access Global Conditions page, select items to export.

   You may work with your complete list of items, or filter it and work with the filtered list. To select a continuous set, click the first item, hold down the Shift key, and click the last. To select a discontinuous set, hold down the Ctrl key as you click items.
2. Select Export from the Actions menu. A message presents a job ID. Note the ID, then close the message.
3. Navigate to the Monitor Jobs page. It's available from either the Models or Controls page.

4. Locate the row displaying the job ID you noted.
5. When the status displayed in that row reaches Completed, click the Download icon.
6. A file-download window opens. In it, navigate to the folder in which you want to save the file and click the Save button. The download file is saved in JSON format.

2 Access Models

Overview of Access Models

An access model detects risk in the assignment of access points to users. Access points are roles or privileges that enable users to work with data in business applications.

A model may perform separation-of-duties analysis, identifying access points that conflict because in combination they'd allow individual users to complete transactions that may expose a company to risk. Or it may perform sensitive-access analysis, identifying a single access point that presents inherent danger, typically because it provides broad access.

An access model consists of filters that specify access points or that define conditions. Each filter cites a business object, which supplies data for analysis.

Access Point and Entitlement Filters

A filter may specify an access point or an entitlement, which is a set of related access points. The filter selects users assigned either the specified access point or any point in the specified entitlement. A model must contain at least one of these filters and, if so, returns records of users selected by the filter. But typically, a model contains two or more of these filters and returns records of users selected by defined combinations of the filters.

Condition Filters

A filter may define a condition, which grants exemptions from access analysis. First, access-point or entitlement filters return records of role assignments that involve specified access points. Then condition filters select records from that set, and so exclude the records they don't select. A condition filter may specify items, such as users or business units, to be included in analysis. Or it may require the model to consider access granted only within, or only across, individual instances of items such as business units.

> **Note:** Before you can create or run access models, you must synchronize global users at least once. This procedure assigns an ID to each person who uses business applications subject to models and controls. That ID correlates to potentially varying IDs the person may have for business-application accounts. (See *Global Users*.)

Create or Edit an Access Model

To create or edit an access model, you define the filters that select records displaying sensitive access or separation-of-duties risk. You may also select perspective values, which can serve as filtering values in lists of models.

A Models page lists the models you're authorized to work with. To reach this page, open the Risk Management springboard and, in it, select Advanced Controls. Then select a Models tab.

To create an access model, you may:

- Select Actions > Create Access Model in the Models page.

- Select the Create Access Model quick action from the Risk Management springboard. (Depending on the number of quick actions available to you, you may need to select a Show More option on the springboard.)

Either action opens a Create Access Model page. Begin by naming and describing the model.

When you create a model, you're automatically its owner. After you save the model for the first time, you can add other users as owners, editors, or viewers.

To edit a model, select its row in the Models page, then select Edit. As an alternative, click the model name to open a read-only page that provides details of the model's configuration. In that page, click the Edit button. Either action opens an Edit page, a replica of the Create page populated by values for the model you want to edit.

Related Topics

- Secure Records in Advanced Controls
- Select Perspective Values in Advanced Controls

Select Business Objects for an Access Model

As you create a model, you assign a business object to each filter you define. A business object is, in effect, a set of related values that form a subset of the data available from a data source. It provides data for the filter to evaluate. For access analysis, each data source has its own set of three business objects.

- Use an access-point business object to create a filter that specifies an access point. The filter then returns users assigned that access point.
- Use an entitlement business object to create a filter that specifies an entitlement. The filter then returns users assigned any access point in the entitlement.
- Use a condition business object to create a condition filter, which defines exemptions from analysis by a model or control.

In the Oracle Cloud data source, these business objects are called Access Point, Access Entitlement, and Access Condition. In each of the other data sources, business objects have those names prefixed with the name of the data source, for example EPM ARCS Access Point, EPM ARCS Access Entitlement, and EPM ARCS Access Condition. (Data source names for FCCS objects include the number 1, 2, or 3 to distinguish among FCCS pods.)

Each business object provides data specific to its data source. A model may include business objects from only one of the data sources, to detect access conflicts within that data source. Or a model may include business objects from more than one data source, to test for access conflicts that occur across the data sources.

In the Create Access Model page, business objects from one data source are available by default. (You can designate the objects from any data source you've set up as the defaults; see *Maintain Synchronized Data Sources*.) As you define model filters, you can use default business objects without doing anything to make them available. To use business objects from another data source, however, you have to select them. You can also remove business objects you don't need, even those that were available by default, and you can add them back if you change your mind.

To select business objects for a model:

1. Click Add in the Model Objects panel of the page to create or edit a model. A Select Business Objects page opens.
2. Select the objects you want. For each, click the plus-sign icon in its row. The icon changes to an image that displays a check mark.

3. When you finish selecting objects, click the Back icon to return to the create- or edit-model page. A representation of each object appears in the Model Objects panel. In it, you can view the attributes of the object.

Use either of two methods to remove business objects:

- As you work in the Select Business Objects page, click the check-mark icon for an object that's selected for the model. The icon becomes a plus sign, indicating that the object is no longer selected.
- Use the representation of an object in the Model Objects panel of the create- or edit-model page. There, click the deletion icon (×) in the title bar of the object.

Define Access Model Filters

Create an Access Point or Entitlement Filter

A filter may specify an access point, and return users assigned roles whose hierarchies include that access point. Or a filter may specify an entitlement, and return users assigned roles whose hierarchies include any access point in that entitlement.

To create either type of filter:

1. In the Model Logic panel, click Add Filter. A dialog box appears. Enter a name for the filter in its Name field.
2. In an Object field, select the access-point object for any data source to create an access-point filter, or the access-entitlement object for any data source to create an entitlement filter.
3. Accept default values in three fields:
    - In an Attribute field, accept Access Point Name for an access-point filter or Access Entitlement Name for an entitlement filter.
    - In a Condition field, accept Equals for either filter type.
    - In a Type field, accept Value for either filter type.
4. In a Values field, click Search. A search dialog opens. In it, search for and select an access point or an entitlement. Among search criteria:
    - Name and Description are display values identifying an access point or entitlement.
    - Access Point ID applies only to access-point filters. It's the internal name for a role or privilege, or the path to a user-defined access point.
    - Type applies only to access-point filters. Select any access-point type appropriate for the data source for which you're creating a filter.
    - As you enter search values you can use the percent symbol (%) as a wildcard.

Access-point types vary by data source:

- For the Oracle Cloud data source, an access point is any role, privilege, or user-defined access point (a path to a specific role or privilege; see *User-Defined Access Points*).
- For the EPM-ARCS data source, access points include the Service Administrator, Power User, User, and Viewer predefined roles, and application roles that apply to account reconciliation.
- For the EPM-FCCS data sources, access points include the Service Administrator, Power User, User, and Viewer predefined roles, and application roles that apply to financial consolidation and close.
- For the OCI data source, access points include OCI roles.

- For the Imported data source, access points include roles in the applications from which data has been imported.

Create an Access Condition Filter

Condition filters select from records of role assignments returned by access-point and entitlement filters. They therefore exclude the records they don't select. There are two types:

- A basic condition filter specifies a value of an attribute, and so selects records involving that value while excluding records involving other values. For example, **Business Unit Equals Consumer Electronics** selects records involving a business unit named Consumer Electronics, and so excludes records involving other business units. (However, see *How Access Conditions Work Together*.)

  Conversely, the filter might state, **Business Unit Does not equal Consumer Electronics**. It selects records involving other business units, and so excludes the Consumer Electronics unit from analysis.
- A "within same" attribute selects records only within or only across entities such as business units. For example, **Within Same Business Unit Equals Yes** would select records of assignments solely within individual business units. It would exclude records of access granted across units, for example one conflicting access point granted in a business unit named Database Servers and a second granted in the Consumer Electronics unit.

  Conversely, the filter may state **Within Same Business Unit Equals No**. It would select records of access granted across business units, but not access granted solely within individual units.

> **Note:** "Within same" conditions are for use in models that evaluate access risk in applications other than Human Capital Management. Don't use "within same" conditions in filters for Human Capital Management access models.

Although every access model must include at least one access-point or entitlement filter, condition filters are optional.

To create a filter that defines an access condition:

1. In the Model Logic panel, click Add Filter. A dialog box appears. Enter a name for the filter in its Name field.
2. In an Object field, select the condition object for a data source for which you've created one or more access-point or entitlement filters.
3. In the Attribute field, select the attribute you want to base the condition on. To create a filter that selects records and implicitly excludes others, select an attribute that names the type of entity to be included or excluded. To create a filter that directs a model to look within or across entities, select a "within same" attribute.
4. In the Condition field, select one in a set of predefined conditions. These are described below.
5. In the Type field, accept the default selection, Value. In a Value field, select or enter values that complete the condition you selected.

The only condition available to a "within same" attribute is **Equals**, and the only values you can select for it are **Yes** and **No**. For other attributes, you can select these conditions:

- **Equals** or **Does not equal**: Consider only records in which the attribute value does, or doesn't, match a value you select in the Value field.

  If a filter uses the Access Point attribute with either the **Equals** or **Does not equal** condition, it returns or excludes records in which a specified access point exists anywhere in a path. For example, suppose the Calculate Gross Earnings privilege exists in two role hierarchies, "Payroll Manager > Calculate Gross Earnings" and "Payroll Interface Coordinator > Calculate Gross Earnings." The filter **Access Point Does not equal Calculate Gross Earnings** would exclude both these role hierarchies from model analysis. (You can use path conditions to create more granular exclusions.)

- **Contains** or **Does not contain**: Consider only records in which the attribute value includes, or doesn't include, a text string you enter in the Value field. For example, **User Name Contains Super** selects a generic user called Payables Super User; an individual who uses her name, Juanita_Supera, as her user name; as well as other users whose names contain the string "Super." In this example, the condition excludes users whose names don't include "Super."

  A model that uses either of these two conditions excludes all records that don't have an attribute value for the condition to evaluate. The **Does not contain** condition therefore excludes records you may not expect it to. For example, suppose you create the condition, **Asset Book does not contain ABC**. If a record has no value for the Asset Book attribute, it doesn't have an Asset Book value containing the string "ABC," so you might expect the condition to select that record. However, it would exclude that record (and all others with no Asset Book value).

  For the **Contains** condition, the same rule applies, but doesn't have the same effect. For example, the condition **Asset Book Contains XYZ** would select records with Asset Book names containing "XYZ," and so would exclude all others, among them records with no Asset Book values.
- **Matches any of** or **Matches none of**: Consider only records in which the attribute value exactly matches one of any number of values you select in the Value field, or matches none of them. For example, **User Name Matches none of BSMITH or TJONES** excludes those users from analysis by selecting all others.

Sources of Access Condition Values

Access conditions search for values that vary from one data source to another.

In the Oracle Cloud data source:

- A condition that uses the Access Entitlement Name attribute searches for entitlements listed in the Entitlements page. Your organization may have configured these, or may have imported them along with models that use them.
- A condition that uses the Access Point, HCM Data Role, or User Name attribute searches the Security Console for records of access points, roles, or users. If a condition uses the Access Point attribute, it also searches for user-defined access points.
- The remaining condition attributes include Asset Book, Business Unit, Control Budget, Cost Organization, Data Access Set, Intercompany Organization, Inventory Organization, Ledger, Legal Entity, Manufacturing Plant, and Reference Data Set.

  These attributes correspond to "security contexts" in the Manage Data Access for Users task in Oracle Functional Setup Manager. There, security-context values are combined with user and role values; each combination determines the data access a user has when assigned a particular role. Condition filters that use the corresponding attributes cause a model to find access conflicts only when they involve role assignments with the data access defined in Manage Data Access for Users.

  For example, Manage Data Access for Users may specify that the assignment of a role to some users grants access only to records associated with a specific business unit. A model may include a condition filter that sets the Business Unit attribute equal to that unit. If so, the model finds conflicts involving that role only when it's assigned to those users.

In the EPM-ARCS, EPM-FCCS, OCI, and Imported data sources, you can create conditions that exclude users or access points from analysis. In EPM-ARCS, condition filters can also exclude entitlements.

How Access Conditions Work Together

Condition filters have an OR relationship to one another. Each operates independently, so items that seem to be excluded by one can be selected by others.

Although it's not required, it's highly recommended that filters be all-inclusive or all-exclusive to prevent conflicting logic. So if your first condition filter uses the **Equals**, **Contains**, or **Matches any of** condition, each subsequent condition filter should use any of those three conditions. If the first condition filter uses the **Does not equal**, **Does not contain**, or **Matches none of condition**, each subsequent condition filter should use any of those three conditions.

Here are some examples of how condition filters work together:

- Access-point or entitlement filters may return records in which some paths include the Accounts Payable Supervisor role and other paths include the Accounts Payable Manager role. A condition filter may state **Access Point Equals Accounts Payable Supervisor**. By itself, that filter would select records including the Supervisor role but exclude records including the Manager role. However, a second filter may state **Access Point Equals Accounts Payable Manager**. It would select the Manager records that the first filter seemed to exclude, and so model results would include records with both roles.
- User1 and User2 are assigned the Accounts Receivable Specialist role. But in Manage Data Access for Users, the assignment to User1 is defined as applying only to data appropriate for the Consumer Electronics business unit. The assignment to User2 is defined as applying to the Database Servers business unit. The condition filter **Business Unit Contains Consumer Electronics** would, on its own, select records involving Accounts Receivable Specialist as it's assigned to User1, and exclude User2. But a second filter, **Business Unit Contains Database Servers**, would select the assignment to User2, and so the model would return records involving both users.

If you use a negative condition (**Does not equal**, **Does not contain**, or **Matches none of**), take care that condition filters don't return unexpected results.

For example, you may want a model to return only assignments of the Accounts Receivable Specialist role to users working in business units other than Consumer Electronics and Database Servers. You want, therefore, to exclude the assignments to User1 and User2. So you may create the filters **Business Unit Does not contain Consumer Electronics** and **Business Unit Does not contain Database Servers**. But this would backfire: records of the Accounts Receivable Specialist assignment to each user would be selected by the filter that doesn't explicitly exclude his business unit.

To achieve the effect you want, you should instead create a filter specifying **Business Unit Matches None of Database Servers, Consumer Electronics**.

Additional considerations apply to filters that use the data-security conditions:

- Your inclusion or exclusion of one role may be inherited by a related role.

  For example, a US Accounts Payable Manager role may be both assignable to users on its own, and included in the role hierarchy of a second role, Accounts Payable North America. Manage Data Access to Users may specify that the assignment of US Accounts Payable Manager to some users grants access only to data associated with the Database Server business unit.

  The filter **Business Unit Equals Database Server** would select records involving not only US Accounts Payable, but also Accounts Payable North America, to those users.

- Although Manage Data Access for Users defines the data available to a user assigned a role, in some cases other security configuration, such as data security policies, may expand the definition created in Manage Data Access for Users.

  For example, suppose User3 is assigned the Accounts Receivable Manager role. In Manage Data Access for Users, the assignment is restricted to data associated with the business unit called AR Brazil. Suppose User3 is also assigned the Accounts Payable Manager role. In Manage Data Access for Users, the assignment is restricted to data associated with the business unit called AP Italy. Owing to data-security-policy configuration, while in an AR Receipts page, User3 would see data only for AR Brazil, but while in an AP invoice page, User3 would see data for both AR Brazil and AP Italy.

Create Path Conditions

You can create path condition filters. Each identifies one or more specific paths to access points. Such a condition filter may either exclude its specified paths from conflicts identified by a model, or include only those paths in conflicts.

To begin, create user-defined access points. Each is, in effect, a specific path to an access point. For example, one called "Payroll Manager > Calculate Gross Earnings" might provide access to the Calculate Gross Earnings privilege through a role called Payroll Manager.

Next, optionally, create an entitlement that includes user-defined access points you want to use in path conditions.

Finally, create a condition filter, either in an access model or a global condition. You may either:

- Select the Access Point attribute of the Access Condition business object, and a single user-defined access point as its value.
- Select the Access Entitlement Name attribute of the Access Condition business object. As its value, select an entitlement containing user-defined access points.

For either filter, you may:

- Select the Does Not Equal condition. Paths specified by this condition filter are excluded from the results the model can return.
- Select the Equals condition. Paths specified by this condition filter are included in the results the model can return; any other paths are excluded.

For example, assume that a model contains an access point filter that specifies the Calculate Gross Earnings privilege. The filter returns two results: Payroll Manager > Calculate Gross Earnings and Payroll Interface Coordinator > Calculate Gross Earnings.

- The condition "Access Point Does Not Equal 'Payroll Manager > Calculate Gross Earnings'" would cause the model to return the path through the Payroll Interface Coordinator role.
- The condition "Access Point Equals 'Payroll Manager > Calculate Gross Earnings'" would cause the model to return the path through the Payroll Manager role.

Related Topics

- Create an Access Condition Filter
- User-Defined Access Points
- Entitlements in Access Models and Controls

Exclusions Involving Procurement Agents

For certain privileges to grant functional access, a user must have the privilege and a corresponding "action" as a "procurement agent" for a business unit. Access models and controls exclude users granted these privileges without corresponding procurement-agent actions. (These exclusions are specific to the Oracle Cloud data source.)

For example, suppose a user is assigned a role that includes the Create Purchase Agreement privilege. To create purchase agreements within a business unit, that user must also be a procurement agent for that unit and be granted the Manage Purchase Agreements action. An access model (and a control deployed from it) would return only users assigned both the privilege and the action.

> **Note:** Use the Manage Procurement Agents task in Oracle Fusion Functional Setup Manager to set up users as procurement agents and assign them actions.

A special consideration: Models don't take into account the business units in which procurement-agent assignments are granted. So if a model contains condition filters that involve business units, those filters may allow results that should be excluded. For example:

- A user has the Create Purchase Agreement privilege. She also has the Manage Purchase Agreements procurement-agent action, but it applies only in a single business unit, BU1.
- She also has a Create Payables Invoices privilege, but it's granted only within a second business unit, BU2.
- A model includes access-point filters that place the two privileges in conflict, but also includes the condition filter "Within Same Business Unit Equals Yes."
- The condition filter should cause the model to exclude the user, because her conflict doesn't occur within one business unit. Instead, the model returns a record of the user, because it ignores her grant of the Manage Purchase Agreements action being specific to BU1.

If an access-model filter cites any of the following privileges (or a role that includes it), the filter returns only users who are also assigned the corresponding procurement-agent action:

Functional Privilege	Procurement-Agent Action
Acknowledge Purchase Agreement PO_ACKNOWLEDGE_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Cancel Purchase Agreement PO_CANCEL_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Change Purchase Agreement PO_CHANGE_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Create Blanket Purchase Agreement Line from Catalog	Manage Purchase Agreements

Functional Privilege	Procurement-Agent Action
PO_CREATE_BLANKET_PURCHASE_AGREEMENT_LINE_FROM_CATALOG_PRIV	
Create Purchase Agreement PO_CREATE_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Finally Close Purchase Agreement PO_FINALLY_CLOSE_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Freeze Purchase Agreement PO_FREEZE_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Hold Purchase Agreement PO_HOLD_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Import Blanket Purchase Agreement PO_IMPORT_BLANKET_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Import Contract Purchase Agreement PO_IMPORT_CONTRACT_PURCHASE_AGREEMENT_PRIV	Manage Purchase Agreements
Transfer Blanket Purchase Agreement to Catalog Administrator PO_TRANSFER_BLANKET_PURCHASE_AGREEMENT_TO_CATALOG_ADMINISTRATOR_PRIV	Manage Purchase Agreements
Transfer Blanket Purchase Agreement to Supplier PO_TRANSFER_BLANKET_PURCHASE_AGREEMENT_TO_SUPPLIER_PRIV	Manage Purchase Agreements
Acknowledge Purchase Order PO_ACKNOWLEDGE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Cancel Purchase Order	Manage Purchase Orders

Functional Privilege	Procurement-Agent Action
PO_CANCEL_PURCHASE_ORDER_PRIV	
Cancel Purchase Order as Procurement Requester PO_CANCEL_PURCHASE_ORDER_AS_PROCUREMENT_REQUESTER_PRIV	Manage Purchase Orders
Change Purchase Order Line Negotiated Indicator PO_CHANGE_PURCHASE_ORDER_LINE_NEGOTIATED_FLAG_PRIV	Manage Purchase Orders
Change Purchase Order PO_CHANGE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Change Supplier Site PO_CHANGE_SUPPLIER_SITE_PRIV	Manage Purchase Orders
Close Purchase Order PO_CLOSE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Create Purchase Order from Requisitions PO_CREATE_PURCHASE_ORDER_FROM_REQUISITIONS_PRIV	Manage Purchase Orders
Create Purchase Order Line from Catalog PO_CREATE_PURCHASE_ORDER_LINE_FROM_CATALOG_PRIV	Manage Purchase Orders
Create Purchase Order PO_CREATE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Finally Close Purchase Order PO_FINALLY_CLOSE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Freeze Purchase Order PO_FREEZE_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Hold Purchase Order PO_HOLD_PURCHASE_ORDER_PRIV	Manage Purchase Orders

Functional Privilege	Procurement-Agent Action
Import Purchase Order PO_IMPORT_PURCHASE_ORDER_PRIV	Manage Purchase Orders
Purge Purchasing Document Open Interface PO_PURGE_OPEN_INTERFACE_PRIV	Manage Purchase Orders
Reassign Purchasing Document PO_REASSIGN_PURCHASING_ DOCUMENT_PRIV_OBI	Manage Purchase Orders
Retroactively Price Purchase Order PO_RETROACTIVELY_PRICE_PURCHASE_ ORDER_PRIV	Manage Purchase Orders
Generate Purchase Order PO_GENERATE_PURCHASE_ORDER_PRIV	Manage Purchase Orders and Manage Requisitions
Edit Supplier Profile Change Request POZ_MAINTAIN_SUPPLIER_PROFILE_ CHANGE_REQUEST_PRIV	Manage Suppliers
Edit Supplier Registration Request POZ_EDIT_SUPPLIER_REGISTRATION_ REQUEST_PRIV	Manage Suppliers
Maintain Supplier Site POZ_MAINTAIN_SUPPLIER_SITES_PRIV	Manage Suppliers
Maintain Supplier POZ_MAINTAIN_SUPPLIER_PRIV	Manage Suppliers
Merge Supplier POZ_MERGE_SUPPLIER_PRIV	Manage Suppliers

Arrange Filters in an Access Model

Position access-point filters and entitlement filters vertically or horizontally to each other to determine how they relate to one another as they're processed.

- A vertical arrangement indicates an AND relationship: A conflict exists for users identified by filters at all levels.

  For example, an access model may contain three filters, one above another. The uppermost filter identifies users assigned one access point, the filter at the middle level identifies users assigned a second access point, and the bottommost filter identifies users assigned a third access point. A conflict exists for each user assigned all three access points, and so identified by all three filters.
- A horizontal arrangement indicates an OR relationship: Records are valid if returned by any filter or combination of filters in a horizontal set.

  For example, two filters alongside one another may be positioned above a third filter. Each filter specifies its own access point. A conflict would exist for each user assigned either the first and third access points, or the second and third access points.

A model can include access-point filters, entitlement filters, or both. There's no limit to the number of access-point filters, but for performance reasons, you can't include more than three entitlement filters.

- If a model contains access-point or entitlement filters at a single level, it performs sensitive-access analysis: Filters identify access points whose assignment is inherently worthy of review, such as super user job roles.
- If a model contains access-point or entitlement filters at two or more vertical levels, it performs separation-of-duties analysis: Access points at all levels combine to define a conflict (as in the examples above).

Condition filters work differently. Each condition filter has an OR relationship to all other filters. In effect, all condition filters are applied when a model is run, each independently of the others.

Keep these concepts in mind:

- When you add an access-point or entitlement filter, it appears by default below the lowest access-point or entitlement filter in your model hierarchy.
- When you add condition filters, they appear by default in a horizontal row beneath the access-point and entitlement filters. You can't move them from that position.
- Arrows connect the filters, indicating the flow from one filter to another as they're evaluated.
- You can drag and drop existing access-point and entitlement filters to new positions within the model: Drag a filter so that it overlays another access-point or entitlement filter. A dialog box appears; in it, click And or Or.

  If you select Or, the filter you dragged moves alongside the other filter. If you select And, the filter you dragged moves beneath the other filter. The arrows connecting the filters adjust themselves to reflect the new AND or OR relationship.

  You can't move a filter above the top filter in your model hierarchy, but you can move that top filter below any other.
- You can edit or delete a filter. Click on it and select the Edit or Delete icon in the Model Logic panel.

- You can incorporate filters into groups: First select those you want to include. You must select all the filters in a horizontal set, or adjacent filters in a vertical set. Hold down the Ctrl key as you click the filters you want. Then select Create Group. You can drag and drop groups in the same ways as individual filters.

  By default, each group you create is named "Group." To rename it, select it and click the Edit icon in the Model Logic panel.

  To dissolve a group but retain its contents as individual filters, select it and click the Remove Group button. To delete a group and the filters that belong to it, select it and click the Delete icon in the Model Logic panel.

Run an Access Model and View Results

From the Models page, or from either of the pages to create or edit a model, you can run the model or view results from its most recent run.

Access models are subject to a limit on the number of result records they can return. The default limit is 5,000, but an administrator may reduce this value in the Advanced Controls Configurations page. It's located in the Setup and Administration work area.

- A model run may return records slightly in excess of the limit. That's because once a record of a user with an access conflict is included in the record set, all records involving that user must be included. When the limit is reached, analysis may continue until records are complete for all users already included in the return set. However, no records are added for users not already included in the return set.
- A model run may fall short of the limit if global users are configured so that individual global user IDs are associated with more than one actual user.
- The create- or edit-model page includes a checkbox labeled **Override record limit and return all results for access model analysis**. It's active only if an administrator has made an appropriate selection in the Advanced Controls Configurations page. If it's active, you can have a model run return all possible results: Select the checkbox and save the model before running it. If the checkbox is inactive, you can't bypass the record limit.

To run a model, click the Run button in the page to create or edit the model, or select its row in the Models page and click Actions > Run. In either case:

- A job number is displayed; make a note of it. To check the status of the model-analysis job, select the Monitor Jobs button. In the row for the job number you noted, determine when the job status reaches Completed.
- If the model has been run before, the new run overwrites the existing results (with no prompt to save or view them).

To view model results, click the View Existing Results button in the page to create or edit the model. Or, in the Models page, a model that's been run displays the number of model violations in a Results Count column. Click that number.

A model may contain a filter that specifies an access point from the Imported Access Point business object. After the model is created, the role assignments supporting that access point may be removed from a new data import. If so, the access point remains in the model, but becomes inactive; an attempt to run the model prompts an "Access point not found" error. If another data import reactivates the access point, subsequent runs of the model return results correctly.

In the page to review results, you can select any number of records, then click an Export to Excel button to export the records to an Excel file. (See *Manage Export Jobs*.)

> **Note:** When you edit an access model, any results already returned for the model are deleted. You must rerun the model to produce new results.

Interpret Access Model Results

An access model returns a grid. Each row consists of information about the path through which a user is assigned one of the access points involved in a conflict. Typically, a single access conflict involves assignments documented in more than one row.

In each row, results include these values:

- An Incident Information column reports the path to the access point that's the focus of the result record. It uses display names to identify roles in the path, but display names may not be unique.
- An Incident Information Codes column reports the same access path, but it uses role codes to identify roles in the path. Every role code is unique.
- A Group column identifies any access points that conflict with the Incident Information access point.
- Role and Conflicting Roles columns identify the roles that grant access to these access points.
- A Data Source column identifies the data source in which the Incident Information path exists.

Other columns are self-explanatory. You may find that some of the columns you want to see are hidden by default. Click View > Columns to select the columns appropriate for your purposes.

In some cases, the assignment of a single role grants rights to access points a model defines as conflicting. You can filter the model results to display only those conflicts. Click the **Conflicts within a single role** checkbox.

Eliminate False Positives

As you review access model results, you may determine that some records are false positives: although they meet the model's risk definition, they don't pose actual separation-of-duties risk. This may be true, for example, in either of these cases:

- A model defines a conflict between two access points, but a user's access to one of them is read-only. In particular, the conflict may involve a privilege whose path includes an aggregate privilege that grants read-only access.

  An aggregate privilege is a predefined role that combines one function security privilege with related data security policies. In some cases, the policies stipulate read-only access to data. For example, users may have access to a Manage Work Terms and Assignment privilege. That access would be read-only if granted through an aggregate privilege called View Work Terms and Assignment, but write-enabled if granted through a duty role called Manage Work Terms and Assignment.
- A model defines a conflict between two access points, and one of them exists in the hierarchy of a role with "stripes." Modifications to striped roles may cause an access point to exist within a hierarchy but not actually grant access.

  Role stripes are versions of a role that apply to specific modules of Oracle Fusion Cloud. For example, there's a predefined Payables Invoice Creation duty role: ORA_AP_PAYABLES_INVOICE_CREATION_DUTY. There are also stripes of this role: ORA_AP_PAYABLES_INVOICE_CREATION_DUTY_OBI and ORA_AP_PAYABLES_INVOICE_CREATION_DUTY_CRM. They're used with Oracle Business Intelligence and Customer Resource Management, respectively.

Note that you can no longer modify role stripes, so these false positives would be of concern only for modified stripes inherited from R12 or earlier.

To eliminate false positive results, create conditions to exclude them. Path conditions, for example, work well with false positives generated when users gain access to privileges through read-only aggregate privileges. The process involves these steps:

1. Having run an access model, review its results to identify false-positive records. For example, look for paths that include aggregate privileges you know to be read-only. Or, look for paths including roles with stripes.
2. Confirm that a given record is a false positive. Then create a condition to exclude it. For example, you might:
    - Create a user-defined access point that specifies the exact path of a false positive involving a read-only aggregate privilege. Then create a path condition to exclude that user-defined access point.
    - Create a conventional condition that uses the Access Point attribute, the Does not equal condition, and the name of a role that you know grants read-only access. For example, that role might be the View Work Terms and Assignment aggregate privilege. This would exclude records in which the role occurs anywhere in a path.
3. Consider including related condition filters as elements of a global condition. For example, a global condition might contain all the path-condition filters that identify false positives involving read-only aggregate privileges. That way, each condition filter applies whenever any model would return the false positive it excludes.
4. Rerun the model. You should find that it returns fewer records, and all of them pertain to genuine conflicts.

Read-only aggregate privileges and role stripes are only two examples of what may cause false-positive results. Ask questions about your setup whose answers suggest condition filters that can eliminate other false-positive results. Here are some samples.

If you answer yes to either of the following, you may want to add a Within Same equals Yes condition:

- Do you consider it a risk if someone can both create and pay an AP invoice, but only in the same business unit?
- Do you consider it a risk if someone can create and post to a journal, but only in one data access set?

If you answer yes to any of the following, you may want to create a user-defined access point, and then create a path condition to exclude it:

- Have you disabled the ability to quick pay for a particular role?
- Have you hidden the bank accounts tab on the supplier site?
- Have you modified data security policies associated to a role, so that the role doesn't have certain access? Possibly even through use of custom SQL?

If you answer yes to either of the following, you may want to create a condition that excludes a role:

- Are you in a development instance, and want to exclude users with super-user roles?
- Do you want to exclude the supplier portal role because it returns only external users who are expected to create their own suppliers and invoices?

Related Topics

- Create an Access Condition Filter
- User-Defined Access Points
- Create Path Conditions
- Global Conditions

3 Access Model and Control Elements

Overview of Access Model and Control Elements

Access models and controls may use elements that are configured separately from the models and controls themselves. These include entitlements, global conditions, and user-defined access points.

An entitlement is a set of related access points. A global condition defines exemptions from access analysis that apply to all models and controls. User-defined access points trace specific paths to access grants.

In addition, you must establish global user IDs before you can create or run access models or controls. (See *Global Users*.)

Entitlements in Access Models and Controls

An entitlement is a set of related access points that exist within a data source. You may select an entitlement as you create a filter for an access model. If so, the filter identifies users assigned any access point in the specified entitlement.

You're advised to keep the number of access points in each entitlement as small as you can while still meeting your risk-analysis requirements. That's because large entitlements have a negative impact on performance. When a model or control uses entitlement filters, the number of access-point combinations it must analyze is the number of access points in each entitlement multiplied by one another. (And that product would be multiplied by the number of individual access points specified in any access-point filters.) For example, suppose a model or control consists of three filters that call entitlements, and each entitlement includes 30 access points. This would require the analysis of 27,000 access-point combinations (30 times 30 times 30).

In addition to creating entitlements manually, you can import them. More precisely, when you import models or controls that use entitlements, you also import any of these entitlements that don't already exist in your target instance.

When you edit an entitlement, be aware that adding or deleting access points necessarily changes the risk logic of models and controls that use the entitlement. When you run a control after editing an entitlement it uses, you may cause existing incidents to be closed automatically.

Create or Edit an Entitlement

To build an entitlement is to name it, activate or inactivate it, and add or remove access points.

1. Open the Access Entitlements page. Select Risk Management > Advanced Controls > Models > Actions > Access Entitlements.

2. Each row of the Access Entitlements page provides summary information about an existing entitlement. In this page, you may:
    - Select Create to build an entirely new entitlement.
    - Click the row for an entitlement you want to edit, then click the Edit icon. As an alternative, click the entitlement name to open the page that displays full details about it, then click the Edit button in that page.
3. Select values that characterize the entitlement:
    - Enter or modify a name of up to 250 characters and, optionally, a description.

      Consider creating a naming convention to distinguish entitlements that support access models and controls from those that support certification campaigns created in the Oracle Fusion Cloud Access Certifications application. A description may explain briefly the organizing principle or business purpose of the entitlement.
    - Select a status, Active or Inactive.
    - Under Comments, review any existing comments or click Add Comments to add a new one.
4. Select a data source. (Oracle Cloud is the default.) Only access points from the data source you select are available for inclusion in the entitlement. You can select the data source only as you create the entitlement, not when you edit it.
5. Add access points:
    - In the Selected Access Points grid, click the Add option.
    - In a Search and Add dialog, filter the list of access points. Among search criteria:
        - Name and Description are display values identifying an access point. The Access Point ID is an internal name for a role or privilege, or the path to a user-defined access point.
        - Access Point Type values include Role, Privilege, and User Defined.
        - As you enter search values, you can use the percent symbol (%) as a wildcard.
    - Select access points from the filtered list.

      To select one, click its row. To select a continuous set, click the first point in the set, hold the Shift key, and click the last point. To select a discontinuous set, hold the Ctrl key as you click access points.
    - When you're satisfied with your selections, click Apply. Your selections appear in the Selected Access Points grid.
    - You may then enter new search parameters and select other access points, or close the Search and Add dialog.
6. Potentially, delete access points:
    - In the Selected Access Points grid, select the rows for the access points you want to delete. Again, use the Shift or Ctrl key to select multiple rows.
    - Click the Delete option.
7. Save the entitlement.

An entitlement for the Imported data source may contain access points that become inactive because a new data import doesn't include role assignments that support those access points. As long as the entitlement contains other access points that are valid, however, it continues to function without error. The effect of an access point being invalid is that it doesn't contribute to the results returned by a model or control that uses the entitlement. It would resume doing so if a subsequent data import were to restore the access point.

Global Conditions

A global condition defines exclusions from access analysis that apply across all access models and controls.

A given model or control defines a pool of records subject to access analysis: those involving access points specified by its access-point and entitlement filters, minus those excluded by condition filters specific to the model or control. A global condition implements a further exclusion: from the pool for each model or control, it selects records, and so excludes all it doesn't select.

However, each global condition is specific to a data source. So it actually acts upon only models and controls that analyze data supplied by that data source.

A single global condition may contain any number of condition filters. A given filter selects exactly the same records as it would in an access model.

- An ordinary condition filter may select records of access assignments in which the values of an attribute satisfy a condition, such as "Business Unit equals Consumer Electronics."
- A "Within Same" condition filter selects records of access assignments only within, or only across, entities such as business units.

Be aware that creating, editing, or inactivating a global condition may add or remove exclusions to models and controls in your environment. When you run controls after creating or modifying global conditions, you may cause existing incidents to be closed, or closed incidents to be reopened at the Assigned status, automatically.

In the pages to create and edit access models, an Access Global Conditions panel displays the global conditions that are active in your environment. These are display-only. You can't create or edit global conditions in these pages.

To work with global conditions, select Access Global Conditions in the Actions menu on the Models page. In an Access Global Conditions page, each row provides summary information about a global condition. Click the name of a global condition to open a page that displays full details of its configuration.

Create or Edit a Global Condition

The process of creating a global condition is comparable to creating an access model that contains only condition filters. However, all filters in a global condition have an OR relationship to one another. There's no need to arrange the positions of filters to define their relationships to one another.

To create or edit a global condition:

1. In the Access Global Conditions page, either:
    - Select the Create icon.
    - Click the row for a global condition you want to edit, then click the Edit icon. As an alternative, click the global condition name to open the page that displays details about it, then click the Edit button in that page.

2. Select values that characterize the global condition:
    - Enter or modify a name and, optionally, a description.
    - Select a status, Active or Inactive. Once you create a global condition, you can't delete it, but you can inactivate it.
3. Select a data source. The condition business object appropriate for the data source you select becomes the only one available for you to use as you create filters. From it, you can use only condition attributes and related values specific to the data source. You can select the data source only as you create the global filter, not when you edit it.
4. Create one or more condition filters. The procedure is the same as the one for creating condition filters in access models. (See *Create an Access Condition Filter*.)

    > **Note:** All conditions available to model-specific filters are also available to global-condition filters. However, filters that use the **Contain** and **Does not contain** conditions exclude all records that don't have an attribute value for the condition to evaluate. They may therefore exclude records you intend to include. Use these conditions rarely, if ever, at the global-condition level.

5. Save the global condition.

A global condition for the Imported data source may contain filters with access points that become inactive because a new data import doesn't include role assignments that support those access points. As long as the global condition contains other filters that are valid, however, it continues to function without error. But it doesn't exclude records that would have been excluded if the inactive access points were active. It would restore those exclusions if a subsequent data import were to restore the access points.

User-Defined Access Points

Whether an access point constitutes an element of a separation-of-duties conflict may depend on how a user reaches it. So instead of an access point, you may want to include an access path in a model filter.

A user-defined access point is precisely that: a specific path to an access point. You can create user-defined access points only for Oracle Cloud data; other data sources don't support them.

For example, an Oracle Cloud privilege may present risk if a user can reach it by way of a path that grants write access. However, it may be innocuous if it's available through a path that grants only read access. You can create a user-defined access point that specifies the path granting write access.

Once created, a user-defined access point belongs to the Access Point business object. You'd select it for use in a model filter or an entitlement as you'd select any other access point. Its name is the path you've defined for it.

Be aware that if you edit a user-defined access point, you change the risk logic of any model or control that uses the access point. When you run such a control after editing its user-defined access point, you may cause existing incidents to be closed automatically.

To work with user-defined access points, select User-Defined Access Points from the Actions menu of either the Models or Controls page. In a User-Defined Access Points page, each row provides summary information about a user-defined access point. Click the name of one to open a page that displays full details of its configuration.

Create or Edit a User-Defined Access Point

To create or edit a user-defined access point:

1. In the User-Defined Access Points page, either:
    - Select the Create icon.
    - Click the row for a user-defined access point you want to edit, then click the Edit icon. As an alternative, click the user-defined access point name to open the page that displays details about it, then click the Edit button in that page.
2. In a Data Source field, accept the default, Oracle Cloud. (Other data sources don't support user-defined access points.)
3. Search for and select an access point that constitutes one element in the path you're defining. You may, for example, be tracing the path from a job role to a privilege, and one of its elements might be the job role. As you search, note that:
    - Access Point Type values include Role, Privilege, and User Defined.
    - For a role or privilege, the Name search parameter value is the item's display name, and the Description parameter value is its internal name.
    - For a user-defined access point, each of the Name and Description parameters is the path that defines the access point. The Name parameter uses display values to express that path, while the Description parameter uses internal values.
4. Click in the row for the access point you want, and then click Add to Selected. The access point appears in a Selected Access Points grid.
5. Repeat these steps for other access points that are elements of the path you're defining. These may, for example, be a duty role that descends from a job role, a duty role subordinate to another duty role, a privilege within a role, or a user-defined access point that fits anywhere within a path.
6. Ensure that the access points are listed in the order that correctly defines the path you want to create. In an Order column, click move-up or move-down icons to move a given access point to its correct position.
7. Click Save and Close.

As you create or edit a user-defined access point, you can delete an access point you've selected as an element of its path. Click its Delete icon in the Selected Access Points grid. You can also delete a user-defined access point, providing that you've first removed it from all models and entitlements that use it. In the User-Defined Access Points page, click the row for the access point, then click the Delete icon.

4 Transaction Models

Overview of Transaction Models

A transaction model uncovers transactions that might involve error or fraud, or otherwise present risk.

It consists of filters that define aspects of risk and select records that satisfy their definitions. A combination of these filters defines a complete risk, with each filter evaluating records returned by filters that precede it.

Filters cite business objects and attributes of those objects, which supply data for analysis. Oracle provides "delivered" business objects. Each is a set of related fields from a business application, and an attribute is one field within the set. You can create other types of object: An imported object is data imported via an XML file. A user-defined object is data returned by a specially configured advanced control. A system-generated object is data returned by certain transaction filters.

Standard Filters

A standard filter selects records containing an attribute whose values satisfy a condition. For example, a standard filter may state: Payment Amount (an attribute of the Payment business object) is greater than 5,000 dollars. As you create the filter, you:

- Specify the attribute (and the object it belongs to).
- Select the condition from a set of predefined conditions. (In the example, "is greater than" is the condition.)
- Specify elements that complete the condition. These elements may be one or more constant values or another attribute of an object. (The example uses a single constant value, "5,000 dollars.")

Certain conditions enable a standard filter to gather attribute values into groups. For example, a filter may use a Similar condition to find invoices with similar supplier names. It would return sets of records, each set containing invoices that meet a similarity standard in a distinct way. The filter in this example may serve to identify duplicate invoices with slightly different renderings of a supplier's name.

Function Filters

A function filter, like a standard filter, creates a formula that specifies how attribute values must satisfy a condition. However, it also incorporates a function that operates on the attribute term, for example taking the average of a set of attribute values. It can create groups of records for the function to operate on, or it can use groups created by a standard filter.

For example, a function filter might group records by supplier. It may then calculate an average payment amount for each supplier, then determine whether each average amount exceeds a threshold value.

Pattern Filters

A pattern filter performs statistical analysis. As you create the filter, you select a pattern (a statistical function) from a predefined set, and you select one or more attributes whose values are subject to analysis. For example, a Mean pattern calculates the average for a set of numeric attribute values, and identifies values too far above or below the average. Each model can use only one pattern filter.

Best Practices for Transaction Model Development

You may shorten the time required for model analysis by following best practices.

- Consider making your first filter one that creates the smallest data set for subsequent filters to analyze. For example, your first filter might apply a relative value on a date attribute to select only the most recent month's worth of data.
- Apply simple filters early in your model logic. For example, a model may analyze records of invoices, but include a simple filter that limits analysis to a specific set, such as those that haven't been canceled (Canceled Date attribute of the Payables Invoice business object is blank). Or it may establish thresholds (for example, an amount greater than a fixed value) or select transactions of a specific type.
- The attribute for a simple filter may be available both in a delivered object and a user-defined object. If so, create two filters for your model, one for each object. For example, suppose you're creating a model, and it includes a filter that states "Payables Invoice.Amount is greater than 100." Suppose also that you created a user-defined object, called Specialty Invoice. It's developed from a data-set control based on the Payables Invoice object, and it includes the Amount attribute. You should include a second filter, "Specialty Invoice.Amount is greater than 100," in your model.
- Function filters, or filters that apply a **Related to** condition to user-defined objects, are best applied after simple filters.
- You may create more than one filter that uses an **Equals** condition to arrange records into groups. If the filters call the same business object, place them one after the other (if your model logic permits).
- A filter may use a **Similar** (or **Similar to**) condition to establish groups of similar records. You can include more than one of these filters in a model. However, place them after other filters (if your model logic permits).
- The language you select as you log on to Oracle Cloud becomes the "source language" for transaction models you create. For some business objects, attribute values are translated into multiple languages. So that models return appropriate results, make sure model filters that use translated objects search for attribute values in your source language. Or, whenever possible, use ID attributes in model filters, rather than corresponding name attributes.

  For example, the Business Operating Unit object is translated into multiple languages. A user working in Spanish creates a model with a filter that searches for unit names that contain "norte." Later, a user working in English copies the model as the basis of a new one. Unless that user changes "norte" to "north," the filter returns no results. As an alternative, the creator of either model could have searched for organization-ID values, which are the same in any language, rather than name values.

  To identify the source languages of the models you can access, select View > Columns in the Models page, and select the Source Language column.
- Use a step process to develop models. Add a filter, save the model, and run it to confirm that results are as you expect. Then add another filter and test again. Continue until your model is fully developed. This greatly simplifies troubleshooting should the model return unexpected results.
- Use a known data set to develop models. In addition to using the step process when designing models, consider restricting your data set by first adding a simple filter that selects a small set of known test data. For example, use conditions such as **Equals**, **Contains**, or **Matches any of** against attributes like invoice number, supplier name, or person name. This approach helps facilitate model-logic design and evaluate required filters.
- Most patterns return graphical as well as tabular results. These patterns are for use only in models. Don't use them in a model that you intend to deploy as a control. There are two exceptions: The Normalize and Lexical

Tokenization patterns don't produce graphs and so are appropriate for use in models that are to be deployed as controls.

Create or Edit a Transaction Model

To create or edit a transaction model, you select business objects, which provide data for the model to evaluate. From that data, you define both the filters that select risky records and the results that the model returns.

A Models page lists the models you're authorized to work with. To reach this page, open the Risk Management springboard and, in it, select Advanced Controls. Then select a Models tab.

To create a transaction model, you may :

- Select Actions > Create Transaction Model in the Models page.
- Select the Create Transaction Model quick action from the Risk Management springboard. (Depending on the number of quick actions available to you, you may need to select a Show More option on the springboard.)

Either action opens a Create Transaction Model page. Begin by naming and describing the model.

When you create a model, you're automatically its owner. After you save the model for the first time, you can add other users as owners, editors, or viewers.

To edit a model, select its row in the Models page, then select Edit. As an alternative, click the model name to open a read-only page that provides details of the model's configuration. In that page, click the Edit button. Either action opens an Edit page, a replica of the Create page populated by values for the model you want to edit.

Every transaction model must include a selection of business objects. Even so, no delivered, user-defined, or imported business objects are initially available to you. An administrator must use a Business Object Security feature to assign you business objects you can use. As you create a model, you can select only among the objects you've been assigned. Even if you're authorized to work with a model, you can open it for viewing or editing only if you're assigned all the objects it uses. If you're not, a Missing Business Objects Access icon appears next to the model name. When you click on the name, a message identifies the objects you lack.

Related Topics

- Secure Records in Advanced Controls
- Select Perspective Values in Advanced Controls
- Secure Business Objects

Select Business Objects for a Transaction Model

A business object is, in effect, a set of related values that form a subset of the information available from a data source. For a transaction model, select business objects that include attributes you'll use in the model's risk definition. Also select business objects that supply result values the model returns.

For example, if a model is to include the filter "Payment Amount is greater than 5,000 dollars," you'd select the Payment business object, because it includes the Payment Amount attribute. While Payment Amount might also serve as a result attribute, so might other attributes that belong to other business objects. For example, you might use the Supplier

Name attribute of the Supplier business object to identify the supplier to which the payment has been made. So you'd select the Supplier business object as well.

You can select delivered business objects; each is a set of related fields in a business application, and each field is an attribute of the object. In addition, you can select imported objects (data imported from a file) or user-defined objects (data returned by a specially configured advanced control). A model may also use system-generated objects, but you create filters that define them, so they're not available to be selected.

> **Note:** "Approvals" business objects provide both archived and completed approval records created from workflow tasks. To do so, each of these objects depends on an Extract Workflow Tasks for Archive job, which is scheduled to run once a day. If you select any of these objects for a model, you may want to run the job manually before evaluating the model, to ensure data is freshly updated. Navigate to Tools > Scheduled Processes to run the job. These business objects include Cash Advance Approvals, Expense Report Approvals, Journal Approvals, Payables Invoice Approvals, Purchase Order Approvals, Salary Approvals, and Supplier Approvals.

Make Selections

To add business objects to a model:

1. Click Add in the Model Objects panel of the page to create or edit a model. A Select Business Objects page opens. In it, each row displays the name of an object as well as these values:
    - A label identifying the category to which the business object belongs. Categories generally indicate the type of data the business object provides, such as transaction, audit, or configuration setup. An "Other" category consists of user-defined objects.
    - A label that identifies the source of the business object. This may be the name of a data source, "Internal" (managed within the application, such as a user-defined object), or "Imported" (created from an import file).
2. Search for objects. You can use the Search field to search by business-object name. Or, click Show Filters, then filter the list of objects by name, category, or product (to select among business objects that support the product you specify).
3. Select the objects you want. For each, click the plus sign in its row. The icon changes to an image that displays a check mark.

    > **Note:** For transaction analysis, each EPM data source (ARCS and FCCS 1 through 3) has a single delivered business object. The name of each is "User Activity" preceded by the data source name. All other delivered objects belong to the Oracle Cloud data source. Transaction business objects for data sources are mutually exclusive. If you select an object from one source, you can't select objects from the others.

4. When you finish selecting objects, click the Back icon to return to the create- or edit-model page. A representation of each object appears in the Model Objects panel. In it, you can view the attributes of the object.

Modify Selections

You can also remove business objects you don't need:

- As you work in the Select Business Objects page, click the check-mark icon for an object that's selected for the model. The icon becomes a plus sign, indicating that the object is no longer selected.
- Use the representation of an object in the Model Objects panel of the create- or edit-model page. There, click the x icon in the title bar of the object.

Create Attributes

You can create attributes for an object. Each applies only to the model it's created in (and a control developed from the model).

1. In the representation of an object, click the Add icon. An Add Configurable Attribute dialog opens.
2. In an Attribute Name field, create a name for the new attribute.
3. In a Base Attribute field, select one of the existing attributes.
4. In a Modifier field, select a mathematical operator: + (addition), - (subtraction), * (multiplication), / (division), or the ampersand symbol (creates a comma-delimited text string of the combined values). You can select only among modifiers appropriate for the base attribute you selected in step 3. For example, you can subtract dates, but you can't multiply them.
5. In a Type field, select Value or Object.
6. If you selected Value, enter a value to be combined with the base attribute, as defined by the modifier. If you selected Object, select a second attribute, whose values are combined with those of the base attribute, as defined by the modifier.
7. Click the OK button.

For example, suppose a model returns records of employee expense reports that include duplicate expenses. Among the model's result attributes, you want to include the number of days between the start and end dates on the expense line. You can use one of the model's business objects, Expense Report Details, to create two new attributes, the first serving as an attribute on which the second is based.

Start with a calculation involving two delivered attributes: End Date minus Date ("Date" being the name of the attribute that reports the start date). Select the icon in the Expense Report Details object to open its Add Configurable Attribute dialog. Give the new attribute a name (for example, 1NumberOfDays), select End Date as the base attribute, the minus sign as the modifier, Object as the type, and finally the Date attribute.

But this calculation separates the start date from the period to which it belongs, so you need a second calculation that adds 1 to the result of the first calculation. Reopen the Add Configurable Attribute dialog and give your second new attribute a name (for example, 2NumberOfDays). This time, select 1NumberOfDays as the base attribute, the plus sign as the modifier, Value as the type, and 1 as the value. Then select 2NumberOfDays as a result attribute for the model.

Note that the names of these attributes incorporate numbers for two reasons. First, you can create similar names for two closely related attributes, but nevertheless distinguish between them. Second, because the names begin with numbers, they're listed ahead of other attributes of the object, and so are easy for you to locate.

Related Topics

- Work with System-Generated Objects
- Work with Imported Objects
- Work with User-Defined Objects

Define Transaction Model Filters

Create a Standard Filter

To create a typical standard filter for a transaction model:

1. In the Model Logic panel, click Add Filter. A dialog box appears. Enter a name for the filter in its Name field.

2. An Object field lists the business objects you've added to the model in the Model Objects panel. Select the one that includes the attribute you want to use in the filter. Then select that attribute in the Attribute field. For an example that's to be extended over the next several steps, suppose you select the Payment business object and its Payment Amount attribute.
3. In a Condition field, select a predefined condition. For the example, suppose you select the Greater Than condition.
4. Select the type of item that completes the condition. Then specify an item of that type. For text or numeric attributes, there are two options:
    - Select Value in a Type field. Then enter a fixed value in a Value field. Your filter might, for example, set the Payment Amount attribute to be greater than a fixed number, to select records with payment amounts that exceed the number.
    - Select Object in the Type field. Then, in Object and Attribute fields, select a business object and one of its attributes. This might, for example, be the Cleared Amount attribute of the Payment business object. The filter would return records with a payment amount value greater than the cleared amount value.

    The same options apply to date attributes, with one adaptation. If your filter uses one of the greater-than or less-than conditions, a value may be fixed or relative. For the former, you'd select a specific date. For the latter, you'd select a number of days, weeks, or months from the moment the model or control containing this filter is run.
5. If appropriate, open the Advanced Options panel and select advanced options. You'll see only options that apply to the filter you created.

Certain conditions present special cases: A filter that uses the **Is blank** or **Is not blank** condition doesn't require a term to complete the condition. In a filter that uses the **Is not related to** condition, you specify business objects both to the left and right of the condition, but no attributes.

Related Topics

- Model Filter Conditions
- Advanced Options for Standard Filters

Create a Function Filter

A function applies a calculation to groups of attribute values, then determines whether each calculated value poses a risk.

A function filter can group records on its own. Or, a standard filter can create a system-generated object, and the function filter can use the groups defined for that object. If a standard filter is to define groups, create it first, then create the function filter in an AND relationship with (below) the standard filter.

To create a function filter:

1. In the Model Logic panel, expand the Add Filter option, then select Function. A dialog box appears. Enter a name for the filter in the Name field.
2. In a Grouping Value line, use Object and Attribute fields to gather records into groups:
    - If the function filter is to create groups on its own, select a business object in the Object field. Then select one of its attributes in the Attribute field. In each group the function filter creates, values for that attribute match exactly.
    - If the function filter is to use a system-generated object, select the name of that object in the Object field. Then select one of its attributes in the Attribute field. This creates subgroups: records in each group defined by the system-generated object are further sorted on the values of the attribute you select.

3. In a When line, use a Function field to select the calculation that's to be performed on grouped attribute values. Select among:
    - Average: Calculates the average of the attribute values.
    - Count: Determines how many attribute values exist.
    - Sum: Adds the attribute values together.
    - Rank: Arranges attribute values in ascending order. (A Display in Descending Order advanced option may reverse this order.)
    - Exclusive: Returns records of groups whose rows are missing any in a set of text strings that should belong together. (If you group records by expense report, for example, you can find expense reports that lack any in a set of complementary values, such as rental car but no gasoline expenses.)
    - Inclusive: Returns records of groups whose rows include all in a set of text strings that should not belong together. (If you group records by expense report, for example, you can find expense reports that contain conflicting values, for example gasoline purchases and taxi expenses.)
4. For any function other than Count, select the attribute that provides values for the function to operate on. Use Object and Attribute fields in the When line to do this. (For the Inclusive or Exclusive function, only text attributes are available for you to select.)

    The Count function operates on the attribute you selected (in the Grouping Value line) to group records. It removes the option to select another object and attribute.
5. In the remaining fields of the When line, select a condition and values that complete the condition.

    For the Inclusive and Exclusive functions, only the **Matches any of** condition is available. Specify values that should or shouldn't belong together. Use either a comma or a semicolon to delimit values. A full match isn't required. For example, "car" would return "rental_car."

    For the Rank and Count functions, the value must be a positive integer.

    For the Rank function, the condition and value specify one or more ranks, and the filter returns records at those ranks. For example, Equals 4 returns one record for each group, containing the fourth-ranking value of the attribute. Or, Less than 4 returns three records for each group, containing the first- through third-ranking values.
6. Optionally, open the Advanced Options panel and select options that refine the attribute-condition formula you created.

An example: Group payables invoices by supplier, calculate the average payment to each supplier, and find average amounts that exceed a threshold.

- To group records, use the Grouping Value line to select the Payables Invoice object and Supplier ID attribute.
- To evaluate grouped records, use the When line to select the Average function. Then select the Payables Invoice object and its Amount attribute. Finally select the greater than condition and whatever value you want as a threshold.

A second example: Group payables invoices by supplier. Then identify suppliers that have generated large numbers of invoices.

- To group records, use the Grouping Value line to select the Payables Invoice object and Supplier ID attribute.
- To evaluate the grouped records, use the When line to select the Count function. The dialog refreshes so that the Object and Attribute fields disappear. Select the greater than condition and whatever value you want as a threshold. These selections apply to the Supplier ID attribute.

Related Topics

- Model Filter Conditions
- Advanced Options for Function Filters

Model Filter Conditions

A model filter specifies an attribute of an object, then selects records with attribute values that satisfy a condition. You select the condition and elements that complete it: one or more constant values, or another attribute of an object.

For example, this is a filter that uses a condition involving a constant value: the Payment Amount attribute of the Payment business object is greater than 5,000 dollars.

Select among the following conditions as you create filters for transaction models. Each condition is available only to attributes it's appropriate for.

- **Mathematical operators**: The filter returns results if the value of one attribute equals, doesn't equal, is less than, is less than or equal to, is greater than, or is greater than or equal to either a constant value or another attribute value. For a date attribute, "less" means "earlier," and "greater" means "later."

  You can set an attribute of a business object equal to itself. The filter returns groups of records. In each group, the attribute equals a specific value. If the attribute were Supplier ID, for example, all records for supplier ID 1234 would form one group, all records for ID 2345 would form another group, and so on.

- **Similar** and **Similar to**: The Similar condition checks for similarity in the values of one attribute. The Similar to condition checks for similarity in two attributes; a value of either may be similar to other values of the same attribute or to values of the other attribute.

  For either condition, define a standard of similarity. The filter then collects records into groups. In each group, attribute values meet your standard in a distinct way.

  - Text: Enter a percentage. Strings are similar if the number of characters they share is at least that percentage of total characters. For example, six-character strings are 50 percent similar if they contain three matching characters.

    Values with distinct sets of matching characters form distinct groups. For example, one group might contain strings with abc, and another strings with xyz.

    Characters in one string need not be consecutive to match characters in another string. By default, the filter checks whether entire strings are similar. You can select a Similar Word advanced option to check for similarity in any single word in each string.
  - Number: Enter a percentage. This sets a lower limit. An upper limit is the same number of points above 100 percent as your percentage is below. For example, if you enter 85 percent, you establish two limiting values, 0.85 and 1.15.

    The filter takes the average of numbers already included in a group, multiplies it by the limiting values to create a range, and admits a new value if it falls within the range. Each time a new value is added, the group average changes, and so does the range for admitting new values.

    In the 85 percent example, one group might include 22 and 20. Another might include 9 and 8. Although 7 is one apart from 8, just as 8 is from 9, 7 wouldn't be similar to 9 and 8. That's because the average of 9 and 8 is 8.5, the 85 percent range around 8.5 is 7.225 to 9.775, and 7 falls outside that range.
  - Date: Enter a number of days. Dates are similar if they fall within this span.

  By default, a record belongs only to the group it qualifies for first. (Text strings are evaluated in ascending alphabetic order; numeric values in descending numeric order.) You can set a Generate Results for Similar Groups advanced option to have records belong to all groups they qualify for.

  The filter excludes records that don't qualify for any of the groups it creates. You can select an Include Unique Data Rows advanced option to get records the filter would otherwise exclude.
- **Different than**: Get records that the Similar to condition would exclude. Criteria for these two conditions are the same.
- **Between**: The filter returns results if the value of an attribute falls between two constant values that you select.
- **Is blank** and **Is not blank**: The filter returns records that either have no value, or any value, for a specified attribute. The filter consists only of the attribute and the Is blank or Is not blank statement, because these two elements are sufficient to define the filter.
- **Is not related to**: Specify two business objects to identify records existing in one, but not the other. For example, an invoice that's never been on hold should not appear in the Payables Invoice Hold object. So the filter "Payables Invoice Is not related to Payables Invoice Hold" returns records of invoices that have never been on hold.
- **Contains** and **Does not contain**: A Contains filter returns results if the value of a text attribute includes either a text string you specify or a value of another text attribute you identify. A Does not contain filter returns results if the value of a text attribute doesn't include specified text; in effect, it returns all records that a Contains filter wouldn't.

- **Matches any of** and **Matches none of**: The filter returns results if the value of an attribute is a text string, number, or ID that matches any in a specified set of values, or matches none of them. Use either a semicolon or a comma to delimit values. The match must be exact. (The Matches any of condition behaves a little differently in a filter that uses the Inclusive or Exclusive function. See *Create a Function Filter*.)
- **Starts with** and **Ends with**: The filter returns results if the value of an attribute begins or concludes with a specified string of alphabetic or numeric characters. You may specify a constant value or another attribute that returns text values.
- **Expresses**: The filter finds records in which the value of a specified attribute is a text string containing any term in a dictionary. This dictionary must exist as an imported object. Supply the name of that imported object in the Object field to the right of the Expresses condition, and **Word** in the Attribute field. (See *Create an Object as a Dictionary for the Expresses Condition*.)
- **Related to**: Establish a join relationship between an attribute of a user-defined object and an attribute of any other delivered, imported, or user-defined object. Or, establish a join relationship between an attribute of a "stand-alone" object and an attribute of any other delivered object. (A stand-alone object is a delivered object with no default relationship to other objects.) Specify the attribute of the user-defined or stand-alone object to the left of the Related-to condition, and the attribute of the other object to the right.

  This join relationship is valid only for the model or control it exists in. A user-defined or stand-alone object can have only one dynamic join relationship per model. If the attribute to the left of the condition is a date, the attribute to the right must also be a date; otherwise, attribute types need not match. Use the Business Object Visualizer to determine whether a business object is stand-alone.

Advanced Options for Standard Filters

You may set advanced options that refine the basic formula of a standard filter. The availability of each option depends on the attribute or condition you select for the filter.

An **Exclude** option is common to all conditions. Clear it to get records that satisfy a filter's attribute-condition formula. Select it to exclude those records and get all others.

Similar and Similar To Options

The following options are available if you use the Similar or Similar To condition:

- **Include Unique Data Rows**: Clear to exclude records that don't qualify for any group the filter creates. Select to have the filter return the groups it would ordinarily return, plus the records it would otherwise exclude.
- **Generate Results for Similar Groups**: Clear to include a given record only in the first group it qualifies for. Select to include each record in all groups it qualifies for.
- **Similar Word**: Clear to require full text strings to meet the similarity threshold established by the filter. Select to allow any word in one string to be similar to any word in another.
- **Apply Condition Across the Same Data Row**: This option applies only to a Similar To filter that specifies two attributes belonging to a single business object. Clear to compare values across all rows of the object, so that a given attribute value may be similar to values of either attribute. Select to consider each row individually, so that a value of one attribute can be similar only to a value of the other attribute.

Other Standard Filter Options

The following options are also available to standard filters:

- **Include Empty Row**: This option applies to the Expresses condition. Clear to get only records that include terms in a dictionary. Select to have all records returned; those without dictionary terms have a relevance score of 0. Use this option only if the dictionary (an imported object) includes a row with these settings: the **Word** attribute is null, and **Relevance** equals 0.
- **Match Case**: In searches for matching text values, clear to ignore capitalization or select to consider capitalization.
- **Ignore After Floating Point**: Clear to consider, or select to ignore, digits after a decimal point in number values. For example, if this option were selected, a filter specifying "Payment Amount ends with 5" would return the value 25.67.
- **Include Time with Date**: Clear to ignore, or select to consider, time while you look for matches in date values. As you create a date filter, you specify an absolute or relative date value, but you can't specify a time value. So if you select the Include Time with Date option, the filter uses the exact time of day, to the second, that you run the model containing the filter (or run a control developed from the model).

  Some examples: You select a Created Date attribute for a filter, and you specify a date on which four records were created, two in the morning and two in the afternoon. You run the model containing the filter exactly at noon on some subsequent date. If your filter uses the Equals condition and you clear the Include Time with Date option, the filter returns all four records. But if you select the Include Time with Date option, the filter returns none of those records (because none were created at noon). If you use the Greater Than condition, the filter returns only the two records created in the afternoon.
- **Apply Range of Time**: Find matches for records that fall within a time range you define.
- **Apply Day of Week**: Find matches for records worked only on days you select.

Related Topics

- Model Filter Conditions

Advanced Options for Function Filters

You may be able to set advanced options that refine the basic formula of a function filter. The availability of each option may depend on the function or attribute you select for the filter.

An **Exclude** option is common to all conditions. Clear it to get records that satisfy a filter's attribute-condition formula. Select it to exclude those records and get all others.

Other options include:

- **Generate Subgroups**: This option applies when a function uses groups created by a system-generated object, and typically when the Count function is selected. Clear it to count the number of subgroups that belong to each group. Select it to count either of the following:
  - The number of records in each subgroup, if the attribute in the Filter line is also selected as a result attribute.
  - The number of records in each parent group, if the attribute in the Filter line isn't a result attribute.

- **Over Interval**: This option applies when a function organizes groups by date. Clear it to have each group contain records generated on a distinct date. Select it to have each group contain records whose dates fall within a time period. You define the period:
    - Specify Overlap to define overlapping periods. For example, two-day periods may include Monday and Tuesday, then Tuesday and Wednesday, then Wednesday and Thursday.
    - Specify Successive to define distinct periods. In the two-day-period example, periods might be Monday and Tuesday, then Wednesday and Thursday, then Friday and Saturday.
    - Having selected Overlap or Successive, select a number of days, weeks, or months, then set start and end dates.
- **Display in Descending Order**: This option applies to the Rank function. Clear it to rank values in ascending order. Select it to rank values in descending order.

Related Topics

- Model Filter Conditions
- Work with System-Generated Objects

Create a Pattern Filter

You can add one pattern filter to a given transaction model. For that filter, you select a statistical function, define one or more sets of data the function applies to, and set parameters that focus the results.

Before you can create a pattern filter, you must select at least one business object for the model that has at least one attribute that provides data patterns can operate on. If not, then as you attempt to create the filter, an error message informs you that no patterns are associated with the business objects you've selected. (The EPM-ARCS User Activity and EPM-FCCS User Activity business objects don't support pattern filters.)

To create a pattern filter:

1. In the Model Logic panel, expand the Add Filter option, then select Pattern. A dialog box appears. Enter a name for the filter in the Name field.
2. Select one of the following patterns in the Pattern field:
    - Mean
    - Benford
    - Clustering
    - Anomaly Detection
    - Absolute Deviation
    - Pareto
    - Normalize
    - Lexical Tokenization
3. Under Model Objects, identify an attribute whose values are subject to analysis by the pattern. Select its business object in the Object field, and the attribute itself in the Attribute field.

    You can select more than one object-attribute pair: click the Add icon to generate additional selection fields. The fields display only objects and attributes your selected pattern can operate on.
4. Under Parameters, select parameter values. These vary by pattern.

Patterns

As you create a pattern filter for a transaction model, you can select among the following patterns.

- **Mean**: This pattern calculates the mean for the values of an attribute. It also calculates means for subsets of those attribute values, and identifies those that are too far above or below the overall mean. For example, the pattern may calculate an average for the Amount attribute of the Expense Report Details business object. It may then calculate the average amount for each person who's submitted an expense report, and identify amounts for individual people that are outliers from the overall average. Parameters include:
    - Greater Than and Less Than: Set percentages above and below the overall mean at which values are considered outliers.
    - Variance: Select an attribute that determines how records are grouped into subsets. In the current example, this would be the Person Identifier attribute of the Expense Report Details business object.
- **Benford**: Benford's Law states that even in widely varied sets of numeric data, the frequency distribution of leading digits is predictable. For example, approximately 30 percent of values begin with the digit 1 (if values are expressed in base 10).

  This pattern compares the distribution of leading digits in sets of numbers with the distribution predicted by Benford's Law, and identifies discrepancies. To define the data sets, specify one or more attributes that return number values. Discrepancies are values that are some percentage above or below the Benford values. Set Greater Than and Less Than parameters to define these percentages.
- **Clustering**: This pattern distributes data records into clusters. It applies K Means analysis to attribute values: it distributes values into a number of clusters (that number being expressed by the variable k) so that each value belongs to the cluster with the nearest mean. For best results, select attributes that return large data sets.

  The pattern determines how many clusters to create based on the number of records it evaluates. However, you can influence this number by setting a Resolution parameter, whose values are Very High, High, Medium, Low, and Very Low. The Very High value results in the most clusters, and the Very Low value in the fewest clusters.
- **Anomaly Detection**: This pattern calculates a normal distribution of values for a specified attribute, then compares it with the actual distribution of values. Pattern results appear in a graph. In it, you can identify anomalies: actual values that stand out sharply from the expected (normal-distribution) values. For best results, specify attributes that return large data sets.
- **Absolute Deviation**: This pattern calculates absolute deviations for values of an attribute. Absolute deviation is the difference (expressed as a positive number) between each value in a set of values and the average for all values within that set.

  The pattern actually defines multiple sets, and returns deviations for each set. To define sets, you select an attribute for an Aggregation Pivot parameter and another attribute for a Categorization parameter. The pattern then calculates absolute deviation per Categorization value within each Aggregation Pivot value.

  For example, suppose you want to apply the pattern to expenses incurred by employees within each business unit of a company. Begin by selecting the Amount attribute of the Expense Report Details business object. Select Person Identifier for the Categorization parameter and Business Unit for the Aggregation Pivot parameter.

  The result is a scatter plot. Its x axis represents Aggregation Pivot values (business units in the example), and its y axis represents absolute deviation values. Each point on the graph is a count of the records per aggregation pivot/absolute deviation value.

Other parameters for this pattern include Scale and Sensitivity. Typically select Linear for the Scale parameter. When values are widely spread, however, you may choose one of the Logarithm options for better graphing. The Sensitivity parameter enables you to choose whether to plot all results or a subset ranging from normal to highly anomalous.

- **Pareto**: The Pareto Principle asserts that, for many events, roughly 80 percent of the effects come from 20 percent of the causes. This pattern uses the Pareto Principle to divide a set of records into ever-smaller groups.

  It sorts an initial set of records so that values of an attribute you select (or derivatives of those values) are in descending order. It selects the top 20 percent of those records. It performs repeated iterations, with each selecting 20 percent of the records remaining from the previous iteration. The second iteration, for example, creates a group that consists of 4 percent of the original set (20 percent of the first 20 percent); the group created in the first iteration therefore retains 16 percent of the original data set.

  The pattern determines how many iterations to perform based on the number of records it evaluates. However, you can influence this number by setting a Resolution parameter, whose values are Very High, High, Medium, Low, and Very Low. The Very High value results in the largest number of iterations, and the Very Low value in the smallest number of iterations.

  You may also set a Derivative parameter, which determines whether the pattern works with attribute values or with derivatives of those values. Derivative options include:

  - None: The pattern sorts attribute values from high to low, then begins the process of selecting records for groups.
  - First Derivative: The pattern sorts attribute values from high to low, subtracts each value from the value immediately above it, sorts the resulting values, and then begins the process of selecting records for groups.
  - Second Derivative: The pattern uses first-derivative values to perform a second derivative calculation before selecting records for groups.

- **Normalize**: This pattern establishes a common scale for values measured initially on differing scales. It sorts input attribute values in ascending order, then assigns a normalized score to each value: the ratio of individual rank to maximum rank. The pattern then multiplies each normalized score by a user-specified multiplier. To use the pattern, select one or more attributes that supply long, int, float, or double data types, and specify a multiplier value.
- **Lexical Tokenization**: This pattern separates the values of a specified attribute into parts. It adds columns to the values returned by the filter that cites the pattern. Each reports one of the parts that attribute values are separated into. Typically, a model that uses this pattern in one filter would contain at least one more filter that cites values in one of the columns that the Lexical Tokenization pattern creates.

  For example, the Address: Postal Code attribute of the Supplier Site Location business object may contain nine-digit postal codes, with the first five digits separated from the last four by a hyphen. You may want to work only with the first five digits. The Lexical Tokenization pattern can specify the hyphen as a delimiter; results would include one column reporting only the first five digits, and another column reporting only the last four digits, of each postal code.

  Parameters include the following:

  - Delimiter determines the point where attribute values are separated. This may be a character (such the hyphen in the postal code example) or a regular expression (its use requires some knowledge of software coding languages and conventions).
  - Maximum Limit sets the number of columns that attribute values should be separated into.

- Prefix sets a text value that appears in the heading for each return column the pattern creates. (For each column, this prefix is followed by a sequential number that distinguishes it from other return columns.)
- Type specifies whether return values should be formatted as text, number, or date.

Arrange Filters in a Transaction Model

As you add filters to a transaction model, position each vertically or horizontally with respect to others to determine their processing order:

- A vertical arrangement indicates an AND relationship: Filters at one level are evaluated before those at the level below it, the topmost first and the bottommost last. Presuming that processing at any vertical level returns records, processing continues on those records at the next level. Records selected at the final vertical level constitute the model results.
- A horizontal arrangement indicates an OR relationship: If any one filter within a horizontal set returns results, processing moves to the next vertical level.

Keep these concepts in mind:

- When you add a filter, it appears by default below the lowest filter in your model hierarchy. Arrows connect filters, indicating the flow from one filter to another as they're evaluated.
- You can drag and drop existing filters to new positions within the model: Drag a filter so that it overlays any other filter. A dialog box appears; in it, click And or Or.

  If you select Or, the filter you dragged moves alongside the other filter. If you select And, the filter you dragged moves beneath the other filter. The arrows connecting the filters adjust themselves to reflect the new AND or OR relationship.

  You can't move a filter above the top filter in your model hierarchy, but you can move that top filter below any other.
- You can edit or delete a filter. Click on it and select the Edit or Delete icon in the Model Logic panel.
- You can define filters so that one depends on another. For example, a function filter may use groups defined by a standard filter. You can't delete a filter if another filter depends on it. In the example, you can't delete the standard filter until you first delete the function filter. A padlock icon indicates a filter others depend on.
- You can incorporate filters into groups: First select those you want to include. You must select all the filters in a horizontal set, or adjacent filters in a vertical set. Hold down the Ctrl key as you click the filters you want. Then select Create Group. You can drag and drop groups in the same ways as individual filters.

  By default, each group you create is named "Group." To rename it, select it and click the Edit icon in the Model Logic panel.

  To dissolve a group but retain its contents as individual filters, select it and click the Remove Group button. To delete a group and the filters that belong to it, select it and click the Delete icon in the Model Logic panel.

Define Transaction Model Results

As you create a transaction model, select result attributes. When the model is run, it returns the values of these attributes for each risky transaction it finds.

A model may incorporate derived attributes. These are calculations performed by the model. One example is a label applied to each group by a filter that uses the Equals or Similar condition to create groups. Another example is the sum, average, or count in a function filter that performs one of these calculations. Model results automatically include derived attributes, and you can't remove them.

You must actively select any other attribute to include it among the model results. The limit for user-selected result attributes is 25. This limit doesn't include derived attributes; a model can include up to 25 attributes selected by its creators or editors, plus any number of derived attributes.

Be careful to select attributes that reflect the level of detail you want to see in your results. For example, a model may use a function filter that calculates the sum of invoice amounts for each supplier. The sum value, a derived attribute, is included automatically in the result set.

Your model logic would have used the Amount attribute of the Payables Invoice business object. Even so, this attribute isn't included automatically in the result set. If you opt to include it, results would contain a row for each invoice, which would be required to display the amount for each invoice. (Each row would also display the sum of its supplier's invoices.) If you don't, the results include many fewer rows: only one for each supplier, displaying the sum of that supplier's invoices.

You may intend for controls to supply information to analyses, reports, or dashboards created in Oracle Transaction Business Intelligence (OTBI). Those controls inherit result attributes from the models on which they're based. Here are some things to consider as you select result attributes for those models:

- An analysis or report can include values from only the first 25 result attributes in a control. Derived attributes come after the attributes you actively select. For example, if a model includes a function filter that calculates a sum, and you actively select 25 result attributes for the model, the derived attribute containing the sum is result attribute 26, and so wouldn't be available for reporting. If you want to use a derived attribute in an analysis or report, be sure to leave room for it.
- You may want to include amount values that are to be summarized in a reporting instrument. If so, position the amount attribute second among the result attributes. You may also want to include a date related to the amount; if so, position the date attribute third among the result attributes. Examples of such attributes are Amount and Date in the Payables Invoice business object.

Use the Result Display panel to define results:

1. An Available box lists the attributes of all business objects included in the model, organized by object. The naming format for each attribute is [Object Name].[Attribute Name]. Search for attributes you want.
2. Move attributes you want from the Available box to the Selected box. Or, if need be, move attributes you don't want from the Selected box to the Available box.

Create Models That Support Audit

You can create models that use audit data to uncover risk revealed by changes to data over time.

For example, a model (and a control developed from it) may analyze frequent supplier site changes by counting the number of records for each supplier with more than two updates per month.

To create change-tracking models, you use audit-enabled business objects. The name of each begins with the word "Audit," for example "Audit - Supplier Sites." Each of these is a parallel version of a distinct object existing in the Oracle Cloud audit framework. For example, the Audit - Supplier Sites object for use in transaction models you create is a version of an object called "Supplier Sites" in the Oracle Cloud audit framework.

Both versions of an audit object capture not only current values for a given attribute, but also past values. Both versions also track event types, which include whether a value is newly created, updated from an earlier value, or deleted.

However, there are differences between the two versions:

- The Oracle Cloud audit framework version of an audit object consists of a set of attributes. All of these attributes appear to be available in the version you use to create transaction models, but you need to enable those you want to use. (The procedure for this comes in a moment.) Attributes that aren't enabled don't provide any information.

  > **Note:** If you were to enable attributes you don't need, performance would be impacted negatively. So you want to enable only the attributes you need. You'd do this for each audit model you create or import.

- When you run data synchronization, you update your local version of audit objects with data that has accumulated in the Oracle Cloud audit framework version. So if you haven't synchronized data, there may be a data mismatch between the two versions of an audit object.
- Oracle Cloud audit framework objects may contain older records that are excluded from your local version of these objects. That's because the latter are subject to a cutoff date. It limits the audit-object records that can be synchronized to those added or updated on or after a date you specify. To set that date, navigate to the Setup and Administration work area and select the Advanced Controls Configurations tab. In its Transaction and Audit Performance Configuration panel, enter or modify a cutoff date in the Audit Events Created as Of field.

To clarify further, audit-model analysis depends on audit data existing in the Oracle Cloud audit framework. Once data is captured in audit-framework business objects, you can synchronize those objects with parallel objects in Oracle Advanced Financial Controls. Audit data is then available in the objects for use in model filters that identify anomalies.

In all other respects, you use the same procedures to create audit models as you do to create conventional models.

For example, to create the model that tracks frequent supplier site changes, select the Audit - Supplier Sites business object, then create these filters:

- First, a standard filter selects recent data. It sets the Date attribute greater than or equal to a relative value, one month.
- A second standard filter returns records of all updates in that month. To do so, it sets the Event Type attribute to Update.
- Finally, a function filter identifies supplier sites with excessive changes. Its Grouping Value line specifies the Supplier ID attribute to group the records of updates by supplier. Its When line selects the Count function, the greater-than condition, and the value two, to return records for each supplier with more than two updates.

To enable the audit business objects and attributes you want to use, you must be a user with rights to Oracle Fusion Functional Setup Manager.

1. Open the model and review it to determine which audit objects and attributes it uses, both to define model logic and to define results the model returns. These are local audit business objects and attributes that correspond to Oracle Cloud audit framework objects and attributes.

   Also note the Type value for the audit business object. It's displayed along with the object name in the page you use to select objects for a model.

2. In the Navigator, select My Enterprise > Setup and Maintenance. Search for the Manage Audit Policies task. In the task list, select that task.
3. In the Manage Audit Policies page, locate the row for Oracle Fusion Applications. In its Audit Level field, select Auditing.
4. Click the Configure Business Object Attributes button in that row.
5. In a Configure Business Object Attributes page, use a Product field to select the product whose data you want to audit. Typically, this value correlates to the Type value you noted in step 1 for a business object your model uses.
6. An Objects region presents a hierarchical list of business objects. Select the object your model uses. To do so, you must also select its parent objects.
7. In an Audited Attributes region, click Create (a plus icon). Select the Oracle Cloud audit framework attributes that correlate to the local attributes you noted in step 1. Then click OK.
8. When you complete your selections, click Save and Close.

After completing this procedure, you can verify your configuration by running Audit Reports. You can select among search parameters to decide the type of audit history report you require. To access the Audit Reports work area, select Navigator > Tools > Audit Reports.

An Example of Enabling Items for Audit

As an example of the process for identifying and enabling Oracle Cloud audit framework objects and attributes for audit data collection, consider the delivered-content model 60002: Frequent Changes to Supplier Bank Accounts.

- The model analyzes bank-account update events to find suppliers whose bank-account records have been updated more than twice over the course of a year from the date you run the model.
- For each update by each of these suppliers, the model returns old and new values for account name, account type, account number, bank name, description, and whether international payments are allowed. All these are attributes of a business object called Audit - Supplier Bank Accounts.

The model logic uses audit-event attributes, but these are included automatically in audit business objects. You don't need to enable them. However, Account Name, Account Type, Account Number, Bank Name, Description, and Allow International Payments are result attributes you must enable for auditing. They belong to a business object in the Oracle Cloud audit framework called Supplier Bank Accounts. It's a child of a Supplier object.

To enable these items:

1. In the Navigator, select My Enterprise > Setup and Maintenance. Open the Manage Audit Policies task.
2. Ensure that Auditing is selected in the Audit Level field in the Oracle Fusion Applications row. Then click its Configure Business Object Attributes button.
3. In the Product field, select Supplier Model, which is the correct value for the Supplier Bank Accounts object. (Note that it matches the Type value displayed for that object in the Select Business Objects page.)
4. In an Audit column of the Objects region, select checkboxes that define a hierarchical path to this object: Audit Top Node > Supplier Audit Setup > Supplier > Supplier Bank Accounts. Then click in the Supplier Bank Accounts row.
5. In the Audited Attributes region, click Create.
6. A Select and Add Audit Attributes window opens. In it, select the checkboxes for the six attributes your model uses: Account Name, Account Type, Account Number, Bank Name, Description, and Allow International Payments. Click OK to close the window.
7. Select Save and Close in the Configure Business Object Attributes page.

Synchronize Transaction Data

To ensure that transaction models (and controls) evaluate current data, a Transaction Data Source Synchronization job uploads new and modified records from your Oracle Cloud data source.

For the most part, this happens in the background. Using features available in the Advanced Controls Configuration page of the Setup and Administration work area, an administrator schedules the job to run regularly (and may also run it on demand). With each run, it updates all business objects used by all current transaction models and controls. (See *Schedule or Run Data Synchronization*.) The job must run at least once before you can evaluate transaction models.

But there's a special case: As you create or edit a model, you may add one or more business objects that have never been synchronized before. If so, you can synchronize those objects only, to load the data you need for model testing.

1. In the Models page, select the row for the transaction model whose data you want to update.
2. Select Actions > Synchronize Business Objects.
3. A message presents a job number. Note the number, then close the message.
4. Check the status of the synchronization job: Click the Monitor Jobs button in the Models page. In a Monitor Jobs page, locate the row displaying the job number you noted, and look for the status value to update to Completed. Then click the Back button to return to the Models page.

Run a Transaction Model and View Results

From the Models page, or from either of the pages to create or edit a model, you can run the model or view results from its most recent run.

To run a model, click the Run button in the page to create or edit the model, or select its row in the Models page and click Actions > Run. In either case:

- A job number is displayed; make a note of it. To check the status of the model-analysis job, select the Monitor Jobs button. In the row for the job number you noted, determine when the job status reaches Completed.
- If the model has been run before, the new run overwrites the existing results (with no prompt to save or view them).

To view model results, click the View Existing Results button in the page to create or edit the model. Or, in the Models page, a model that's been run displays the number of model violations in a Results Count column. Click that number.

In the page to review results, you can select any number of records, then click an Export to Excel button to export the records to an Excel file. (See *Manage Export Jobs*.)

> **Note:** When you edit a transaction model, any results already returned for the model are deleted. You must rerun the model to produce new results.

Interpret Transaction Model Results

The results returned by a transaction model depend on whether that model includes a pattern filter.

Defined Models

If the model doesn't include a pattern filter, it returns a grid. Each row is the record of a transaction that violates the model, although a single violation may encompass multiple rows. For example, a model that detects duplicate invoices would return one row for each of the duplicated invoices.

Each record contains values for the result attributes selected for the model, and for any derived attributes the model may calculate. The grid may also contain these columns:

- Incident Information. For each record, this is the value of the first attribute among those selected to characterize the suspect transaction.
- Group and Grouping Value. Values for these columns vary:
  - A filter may use the Equals condition to set an attribute of a business object equal to itself. The Group filter reports the business object and attribute. The Grouping Value field reports the value of the attribute.
  - A filter may find transactions with similar values for a specified attribute. The Group field displays the word "Similar" and the specified attribute. The Grouping Value field displays the value of the attribute.
  - A function filter may calculate a value for a specified attribute across a group of transactions. The Group field identifies the function and the specified attribute. The Grouping Value field displays the calculated value.

Pattern Models

If the model contains a pattern filter, it typically generates both graphic and tabular results. The graph depicts the statistical pattern generated by the model, and the table displays data represented in the graph. (The Normalize and Lexical Tokenization patterns are exceptions. Each generates only tabular results.)

For example, the graph for a model that uses the Mean pattern displays two plots: One represents the mean of the values of an attribute. The other tracks means for specified subsets of those values, with outliers evident by their distance from the overall mean.

If a pattern analysis uses multiple attributes, the results page generates multiple result tabs. Each presents a graph and a table related to one of the attributes. If you hold the mouse cursor over a data point in a graph, a box displays the values defining that point. If you click on the data point, the table refreshes to display only values for the data point you've selected.

5 Transaction Business Objects

Overview of Business Objects

Transaction model filters cite business objects and attributes of those objects, which supply data for analysis. There are several types of business object.

- Oracle provides "delivered" business objects. Each is a set of related data fields from a business application, and each field is an attribute of the object.
- You can supplement these with imported objects (data imported via an XML file), user-defined objects (data returned by a specially configured advanced control), and system-generated objects (data returned by certain transaction filters).

Generally, you have access to delivered, imported, and user-defined objects only if they're assigned to you. An administrator uses a Business Object Security feature, available in the Risk Management Data Security work area, to assign objects you can use. Exceptions: You automatically have access to objects you import and to user-defined objects generated by controls you deploy. Also, object security doesn't apply to system-generated objects because each is necessarily specific to the model or control that defines it.

Business objects may be related to other business objects, and an understanding of those relationships can help you to select objects as you create or edit models. In a Business Object Visualizer, you can generate graphic representations of the relationships between objects.

Work with Imported Objects

Create an Import File for Business Objects

For transaction models, you can import any set of data and use it as if it were a business object. An import file may contain data for any number of objects, and it may organize related objects into groups.

Use Excel 2003 or later to create an import file and save it in XML format. You may then import the XML file or a ZIP compression of the file. The maximum size of the XML or ZIP file is 1 megabyte. Construct the file to contain the following worksheets:

- Title the first sheet "BO Group Definitions." Include a row for each group the file is to create. You may create any number of groups, but must create at least one. In each row, provide values in these columns:
    - A column headed "BO Group Name" contains a value that serves as a collective name for a set of objects the file is to create. (A set may consist of only one object.)
    - A "BO Group Type" column provides a label that characterizes the content of its group. A type label might, for example, be Financials or Procurement.

- Title the second sheet "BO Definitions." Include a row for each object the file is to create, providing values in these columns:
  - A column headed "BO Group Name" contains the name of the group this object belongs to. This is a name established in the BO Group Definitions sheet.
  - A "BO Name" column contains the name of an object the file is to create. Each name must be unique. It can't match the name of another object in its group, an object in any other group, or an object already existing in the application.
  - A "BO Category" column includes a label describing the data an individual object is to contain. You may use labels that apply to standard business objects, such as Transaction, Operational Master Data, and Configuration Setup Data. You may, however, use any other value.
  - Additional columns contain the names of attributes that serve as key fields for the object. These columns are headed "BO Key1," "BO Key2," "BO Key3," and so on. You must supply a value for BO Key1. You may create as many additional keys as you need. However, all but BO Key1 are optional. As you create key column headers, don't leave gaps in the numbering. However, these columns may appear in any order.
- Title the third sheet "Attribute Definitions." This sheet lists all attributes for all objects the file is to create. Establish three columns: "BO Name," "Attribute Name," and "Attribute Datatype." In each row, supply:
  - The name of one of the objects established in the BO Definitions sheet.
  - The name of an attribute of that object. The attribute name must not match the name of the object it belongs to.
  - The data type for that attribute. Valid data types include String, Integer, Time stamp, Double, and Long.
- Include a sheet for each object the file is to create. Each of these sheets may have any title. A suggestion is "Data-[Object Name]," with the name of an object, established in the BO Definitions sheet, replacing the "[Object Name]" placeholder.
  - In the first cell of the first row, provide the name of the object as a header.
  - In the second row, as column headers, provide the object's attribute names, as established in the Attribute Definitions sheet.
  - All remaining rows contain attribute values.
  - For the attribute you defined as BO Key1, no value can be blank.
- Observe the following formatting standards:
  - Cells may contain absolute values, formulas, or reference links. (A reference link enables a cell in one worksheet to be populated with the value of a cell in another worksheet.)
  - Remove any total-amount rows not directly tied to specific data attributes.
  - Remove numeric formatting (such as dollar signs). Use the Format Cells - General option.
  - To indicate negative amounts, use a negative sign, not open and close parentheses.
  - For date values, use any of the following formats: MM/DD/YYYY, MM/DD/YY HH:MM AM, MM/DD/YYYY HH:MM PM, or MM/DD/YYYY HH:MM:SS (Military Time).

Edit an Import File

Once you've imported a file to create objects, you can modify the file and import it again to refresh those objects. Rather than refresh an object, you can replace it. In either case, there are limits to the changes you can make, and those limits depend on which action you take.

To refresh an object, you must begin with an import file that specifies the BO Group Name, BO Name, attributes, and relationships that are current for the object. It's strongly recommended that you export the object you want to refresh from the application, so you can be certain its file initially contains no changes that would cause an import to fail.

Here's what you can and can't do for a refresh:

- BO Group Definitions sheet: Don't delete existing groups or change their names. You can modify BO Group Type values.
- BO Definitions sheet: Don't delete the row for an existing object. Don't change the name, the group, or the BO Key1 value for an existing object. You may modify BO Category values. You may add keys, and you may modify or delete keys other than BO Key1. You may add rows to create new objects.
- Attribute Definitions sheet: Don't delete the row for an existing attribute. Don't change the name of an existing attribute, or change the business object it belongs to. If the data type of an attribute was originally Integer, Long, or Double, you can change from the original value to either of the other two. But if the data type was String or Time stamp, you can't change it. You may add rows that define new attributes; for each, you must also add columns to the appropriate Data-[Object Name] sheet to provide values for the new attribute.
- Data-[Object Name] sheet: You may add, edit, or delete rows of values. You may add columns to the object, providing you define the column headings as attributes in the Attribute Definitions sheet. Don't delete columns or update attribute names in existing columns.
- A file may define more than one object, or more than one group. When you select an object to export, you actually export the file that created that object and potentially any number of other objects. You must retain the data that applies to objects and groups you don't want to modify.

You may want to replace an object because one or more of its attributes are no longer appropriate. You have two options:

- You can import a new object and allow the older object to remain. In the file for the new object, you must provide unique BO Group Name and BO Name values. Beyond that, the basic rules for creating a file apply, regardless of whether you're creating a new file or editing a copy of the old one that serves as a template.
- If you want to replace an object that belongs to an import file that contains no other objects, you can delete the original, then import a new object as a replacement. Follow standard procedure to create the new object. If you delete the old object before importing the new one, you can reuse the BO Group Name and BO Name values.

Import, Export, or Delete Objects

You import or export business-object files, or delete imported objects, from the Select Business Objects page. To open it, click Add in the Model Objects panel of the Create Model page or the Edit Model page.

To import an object file:

1. Click the Import button in the Select Business Objects page.
2. Click the Browse button. Navigate to, and select, the file you want to import. The file name then populates the File field.
3. With the file selected, click the OK button.

> **Note:** Although you import an object file as you create or edit a specific model, you may use its objects with any model.

To export an object file:

1. In the Select Business Objects page, locate the row for the object you want to export.

2. Click the Export icon in that row.
3. A file-download window opens. Navigate to the folder in which you want to save the file and click the Save button. The file is saved in XML format.

Although you select an individual object to export, you actually export the file it belongs to. If that file contained multiple objects or groups when it was imported, the file you export also contains all those objects or groups.

You can delete an imported object if it meets two conditions: It isn't used in a model or control, and it belongs to an import file that includes no other objects. Select the x icon in its row in the Select Business Objects page.

Create an Object as a Dictionary for the Expresses Condition

An Expresses condition determines whether text fields in a specified business object contain any term in a dictionary. For you to use this condition in a transaction-model filter, the dictionary must be created as an imported object.

- At minimum, this object must contain a Word attribute (String format) and a Relevance attribute (Double format). The Word attribute lists terms that the Expresses condition searches for. The Relevance attribute rates their relative importance.
- You may include other attributes as well. These may be selected for the results displayed for incidents generated by a model or control that uses the Expresses condition.
- An Include Empty Row advanced option is available to the Expresses condition. For it to be useful, include one row in the imported object that leaves the Word value null and sets the Relevance value to 0.

Related Topics

- Model Filter Conditions

Work with User-Defined Objects

Create or Delete a User-Defined Object

A user-defined object is a set of data returned by a specially configured advanced control. You can use the data set as a business object, with each result column serving as an attribute of the object.

To create a user-defined object, simply deploy the control that supplies data to the user-defined object. Doing so automatically creates the object itself:

- Either an access control or a transaction control can provide data to a user-defined object.
- A control can generate incidents, or it can provide data to a user-defined object, but it can't do both. You determine which purpose a control serves by selecting an appropriate value in a Result Type field as you create the control. **Data set** is the value to select for a control that supplies data to a user-defined object.
- A user-defined object has the same name as the control it's based on. You can't change this name. As you create a data-set control, ensure that its name is meaningful as the name of an object a user would select while creating a model.

Once user-defined objects are created:

- They're listed in a User-Defined Objects page. You can open the page from the Actions menu of either the Models or the Controls page.

- If you deploy the control that creates a user-defined object, you automatically have access to that object. However, you can access other user-defined objects only if they're assigned to you. An administrator must use a Business Object Security feature, available in the Risk Management Data Security work area, to assign objects you can use.
- Only a transaction model (or a control developed from it) can contain filters that cite user-defined objects.
- Before you use one of these objects in a transaction model or control, you must run its data-set control. Otherwise, no results are generated. Each time the source control is run, the data available in the user-defined object is refreshed.
- User-defined objects have no join relationship to other objects. You must expressly define a relationship between a user-defined object and another object it may work with in a model or control. When you cite a user-defined object in a model filter, you use a **Related to** condition in a subsequent filter to create this join relationship.

You may delete a user-defined object, but only if it isn't used in any control or model. In the row for the user-defined object, an Actively Used field indicates whether this is the case. If not, select the Delete icon in the row.

Related Topics

- Deploy Advanced Controls
- Model Filter Conditions

Edit a User-Defined Object

You can edit user-defined objects:

1. From the User-Defined Objects page, locate the row for a user-defined object you want to edit. You can use search features to filter the list of objects. Select the Edit icon in the row you locate.
2. Enter or modify appropriate values in these fields:
    - Description: Optionally enter a brief description of the object.
    - Product: By default, the Product value is Other. You can select a value that identifies a product about which the object supplies information, for example Procurement.
    - Category: By default, the Category value is Other. You can select among three other values. Transaction is appropriate for an object that contains records of actual transactions. These records are expected to be updated frequently. Operational Master Data and Configuration Setup are appropriate for records that are expected to change infrequently, such as setup-data records.
    - Status: By default, the Status is Active. You can change this to Inactive.
    - State: This field is read-only, because the status you select determines the state value.
3. Save the object.

Best Practices for User-Defined Objects

As you create user-defined objects, follow these performance guidelines:

- Limit the amount of data returned by user-defined objects, or by models or controls that consume them, to as few rows as possible. Add filters during model-logic definition to ensure acceptable performance.

- The smaller the number of business objects joined to a user-defined object, the better the performance. (For example, you might relate a user-defined object to only one or two business objects.)
- When applying the **Related to** (join) filter condition, use the most unique (or primary) attribute for better logic processing. Examples of primary attributes in transaction business objects include Invoice ID in Payables Invoice and Expense Report Identifier in Expense Report Information.
- For reusability, keep user-defined objects as generic as possible. However, don't allow this approach to result in an excessively large data set.
- Be sure to select only key attributes in the model used for a user-defined object. For example, select those required to establish join relationships, to create attributes, or to be returned as results. The number of selected attributes can impact performance. The limit for result attributes is 25, not including derived attributes.

Work with System-Generated Objects

A system-generated object is unlike the other types: Rather than select it for a model, you create filters that define it. The object doesn't exist outside of the model that defines it (or a control deployed from that model).

Specifically, if a filter uses the **Equals** condition to set an attribute equal to itself, or if a filter uses the **Similar** or **Similar to** condition, it returns records sorted into groups. These records may then be used in subsequent filters as if they were a business object.

Naming

As you create any filter, you give it a name. The name of the filter that defines a system-generated object serves also as the name of the object itself, as you select it in a subsequent filter. For example, a filter may set the Invoice ID attribute of the Payables Invoice business object equal to itself. It would return an object that groups records by invoice. You may name the filter **Invoice ID is the same**, and that would also serve as the name of the system-generated object.

You may create more than one of these filters, citing distinct attributes of a single business object. Typically, you'd create one after another, so that they produce one object with records sorted into multidimensional groups. In that case, the name of the system-generated object is the name of the last of the filters that define the object.

For example, one filter may set the Invoice ID attribute of the Payables Invoice business object equal to itself, and a second filter may set the Amount attribute equal to itself. In the resulting object, each group would contain records with the same invoice ID and amount. If the second filter were named **Invoice Amount is the same**, that would also be the name of the system-generated object defined by the two filters.

Use Cases

When a filter produces a system-generated object, a subsequent filter can apply a function to each group defined by the object.

In another common usage, one filter applies the **Equals** condition to create a system-generated object. A second filter applies the **Does not equal** condition to identify discrepancies within each group created by the system-generated object. For example:

- A filter states that the Invoice ID attribute of the Payables Invoice business object equals itself. The filter, and therefore its object, are named **Invoice ID is the same**. The object contains sets of records; in each set, all records have the same invoice ID.

- A second filter states that the Supplier ID attribute of the **Invoice ID is the same** object doesn't equal itself. This identifies distinct suppliers in each set. The overall result is records of distinct suppliers who have been issued duplicate invoice IDs.

The filter that creates the system-generated object may use the **Similar** or **Similar to** condition. If so, the filter that identifies discrepancies within groups would use the **Different than** condition.

Limitations

A filter can state that an attribute of an object doesn't equal itself only if that attribute belongs to a system-generated object, and not if it belongs to any other type of business object.

Similarly, for a filter to state that an attribute of an object differs from itself, the attribute must belong to a system-generated object created by a **Similar** or **Similar to** filter. If an attribute belongs to any other type of business object, a filter can't state that it differs from itself.

Once you create a filter that calls a system-generated object, the filter that creates the system-generated object is locked. It displays an icon that looks like a padlock, and if you hover over the icon, the word "Dependency" appears. You can edit the filter that creates the system-generated object only if you first delete its dependent filters. To locate them, click the padlock icon; all dependent filters are highlighted. To remove the highlighting, right-click and then select a Clear Highlight option.

Parent and Child Sets

Filters can generate parent and child sets of records with a common attribute. A model matches values in the two sets to determine which sets to include among results. For example:

- Create filters that use the Payables Invoice business object: the Invoice ID attribute equals itself, and the Amount attribute equals itself. The result is an object that contains groups of invoices; in each, all invoices have the same ID and same amount.
- Create a filter specifying that the Supplier ID of that system-generated object doesn't equal itself. The result is parent sets of invoices. In each, invoice ID and amount are the same, but at least one supplier ID differs from the others. (If all supplier IDs are the same within a set, it's discarded.)
- Create a fourth filter: equate the Taxpayer ID attribute of the Supplier business object with itself. Its result is a new, child set of sets. In each set, the taxpayer ID is the same for all records, but it may correlate to any number of supplier IDs. The model would compare parent and child sets, and keep only those parent sets with matching Supplier ID values.

Related Topics

- Model Filter Conditions
- Create a Function Filter

View Business Object Relationships

You can use a Business Object Visualizer to view diagrams depicting the relationships of business objects to one another.

It's a view-only tool; you can't use it to modify objects or their relationships to other objects. However, an understanding of object relationships can help you to select objects as you create or edit models.

Note: In the Visualizer, you can select among all business objects even though some of them, such as audit business objects, have no relationships to other objects.

Getting Started

In the Advanced Controls work area, click a Business Object Visualization tab to open the Business Object Visualization page. The home page displays listings for both business objects and business-object types:

- Type indicates an activity or product offering that a set of objects supports, for example Financials. Each type listing has an icon depicting a hierarchical structure. Click either the icon or the type name to open a page listing the objects of its type. Click any object name to view its relationships to other objects.
- The listing for a business object displays its name and the type it belongs to. Click the name to view the object's relationships to other objects.

The home page, as well as those that display objects that belong to a type, offer two views:

- A list view displays rows, each of which represents one object or one type. This is the default view. If it's not in use, click the List View icon to restore it.
- A card view presents "cards" (rectangular spaces), each representing one object or one type. Click the Card View icon to use it.

You can search for records by object or type name. As you begin to type in the Search field, a window presents the names of objects and types that contain the letters you've typed. You can click on a name to select its object or type. To return to the home page, click All in a bread-crumb path in the header area of the page.

View Object Relationships

When you select a business object, you open a page displaying an image that consists of nodes representing your focal object and objects related to it. Arrows connect these nodes to indicate that objects either feed data to your focal object or receive data from it. You can choose between views that arrange these nodes in differing ways:

- Layers: The nodes form up to three rows. Your focal object occupies the middle row. Above it, a row may contain objects that feed data to the focal object (known as "In" objects). Below, a row may contain objects that receive data from the focal object (known as "Out" objects). This view is the default.
- Radial: Nodes for related objects form a circular pattern around the focal object. A Radial diagram that includes both In and Out objects looks similar to the Layers diagram, with In objects above, and Out objects below, the focal object. But the related objects from a more curved pattern around the focal object. If all related objects are of one type, In or Out, they form a circle around the focal object.

Use the Control Panel

In a Control Panel, use the Switch Layout option to select the view you want. You can also use these options:

- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.
- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.
- Zoom to Fit: Center the image and size it so that it's as large as it can be while fitting entirely in its display window.
- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area beneath the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.

- Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.
- Control Panel: Hide or expose the Control Panel.

View Information About Objects

In either the Layers or Radial view, each node displays the name of the object it represents and the number of objects it relates to. Hover over any node to review this information about its object:

- Once again, its name and the total number of objects it relates to.
- A Link value, which reveals the point of contact between the object and the one it's connected to.
- The numbers of In and Out relationships of this object to all other objects (not only those depicted in the diagram).

You can also view the attributes that belong to the focal business object. Click the Attributes icon. Or, right click on the focus node and select See Attributes.

Use the Legend

Nodes vary in shape and color to distinguish the focal object from the objects that relate to it. A Legend tells which shapes and colors correspond to which objects. You can take the following actions:

- Hover over an entry to highlight objects of its type (by graying out other entries).
- Hide or expose the Legend by clicking its button.

Use the Overview

Click the Overview icon to open a thumbnail sketch of the diagram. Click any area of the thumbnail to focus the actual diagram on that area. Alternatively, you can click the background of the visualization and drag the entire image in any direction.

Refocus the Image

You can select any node in a diagram as the focal point for a new diagram: Right-click a node, then select Pivot.

6 Advanced Controls

Overview of Advanced Controls

An advanced control defines access or transaction risk and, typically, generates incidents. These are records of access assignments or of transactions that satisfy a control's risk criteria.

A control may instead define a set of data that's incorporated into a user-defined object. That object may then be used as if it were a business object in transaction models and transaction controls.

You base each control on a model, adopting its risk criteria (filtering logic). As you deploy the control, you add information needed for it to be applied. This includes whether it generates incidents or a data set, users who can work with the control itself and can resolve the incidents it generates, a priority, and more.

To begin working with controls, select Risk Management in the home page. Among its options, select Advanced Controls. Then select a Controls tab; it opens a Controls page, which lists controls you can access.

Deploy Advanced Controls

Control Deployment Overview

You can deploy up to 100 models as controls at once. If you deploy multiple controls, their risk logic, names, and descriptions remain distinct. Other values are the same for all the controls you deploy at once.

In the Controls page, select either of two options in the Actions menu, Deploy Transaction Controls or Deploy Access Controls. Enter values in a series of control-deployment pages, selecting Next or Back to navigate among them.

Select Models to Deploy as Controls

On a Deploy Controls: Select Models page, search for and select active models you want to deploy as controls.

- You can search by model name or description.
- You can select up to 100 models you're authorized to own, edit, or view. However, the Select Models page initially lists only 25. To expand the initial list, click the Load More Items option.
- Optionally, review the risk logic for each model you're considering. Click the Control Logic icon in its row. However, you can't modify the logic.
- Finally, select the checkbox in the row for each model you want to deploy. Or, click a Select All checkbox. Note, though, if more than 100 models are available for selection, the Select All checkbox is disabled. You can filter the model list to contain 100 or fewer models, and then use the Select All option.

If you're deploying transaction controls:

- A transaction model is available for selection only if every one of its objects (delivered, imported, or user-defined) is assigned to you. Object assignments are made in Business Object Security, which is available in the Risk Management Data Security work area.
- Don't select any model incorporating a pattern that returns graphic results. Only the Normalize and Lexical Tokenization patterns are appropriate for use in a control.
- As you select transaction models to be deployed as controls, ensure that each has 25 or fewer user-selected result attributes. (See *Define Transaction Model Results*.)

Set Control Details

In a Deploy Controls: Details page, set the priority, status, and result type for your controls.

- Priority expresses the importance of a control in relation to others. The value must be a number. Your company should establish a set of priority values and enforce consistent usage.
- Status is Active or Inactive.
- For Result Type, select **Incident** if controls are to generate incidents, or **Data set** if controls are to supply data to user-defined objects.

The Details page also lists the names and descriptions of the models you selected. You may accept these as the names and descriptions of the controls you're creating, or replace them with new values.

When you create a control that supplies data to a user-defined object (one whose Result Type is **Data set**), you also automatically create the user-defined object itself. The user-defined object has the same name as the control it's based on. You can't change the object's name. As you create a data-set control, ensure that its name is meaningful as the name of an object a user would select while creating a model.

If descriptive flexfield segments have been defined for the Advanced Control object, these appear as fields in an Additional Information panel. Provide values for these fields.

Related Topics

- Work with User-Defined Objects

Assign Perspective Values to Controls and Their Incidents

In a Deploy Controls: Perspectives page, you may select two sets of perspective values. These may be useful in filtering lists of controls or incidents.

- Control Perspective Assignment values apply to the controls themselves.
- Result Perspective Assignment values apply to incidents generated by controls, but you select them as you deploy the controls. Make selections here if you selected **Incident** as the result type in the Details page. Result perspective values serve no purpose for a control whose type is **Data set**.

Related Topics

- Select Perspective Values in Advanced Controls

Secure Controls and Their Incidents

In a Deploy Controls: Control Security Assignment page, grant access to the controls you're deploying. You're automatically their owner, but you can authorize other users as owners, editors, or viewers. Or you can select user groups.

For transaction controls, you can select only users assigned the business objects that supply data to the models you're deploying as controls, or groups whose members are assigned these objects. This limitation doesn't apply to access controls.

If you selected **Incident** as the result type in the Details page, use a Deploy Controls: Result Security Assignment page to grant access to the incidents generated by the controls. Again, you're automatically their owner, but you can authorize other users as incident owners, editors, or viewers, or select user groups. Business-object security doesn't apply to incidents. You can select any eligible users or groups.

You can't assign result security for a control whose result type is **Data set**, since it doesn't generate incidents for result investigators to review.

Related Topics

- Secure Records in Advanced Controls
- Secure Business Objects

Select Worklist Recipients

If you selected **Incident** as the result type in the Details page, use a Deploy Controls: Worklist Assignment page to determine which result investigator receives worklists when a control generates incidents.

In a Result Investigator field, you may:

- Select Search. A Search and Select Investigator dialog opens, listing users you've selected as owners or editors in the Result Security Assignment page. Search for and select one of them. Although this user would be the only one to receive worklists, any of the investigators you've selected can work with incidents in Results pages.
- Select All Eligible Users. All potential investigators receive worklists when a control generates incidents.

Worklist assignments serve no purpose for a control whose result type is **Data set**, since it doesn't generate incidents that would appear in worklists.

Related Topics

- Notifications and Worklists in Advanced Controls

Relate Controls to Financial Reporting Compliance Objects

If you selected the **Incident** result type in the Details page, you may use a Deploy Controls: Related Records page to relate the advanced controls you're creating to processes, risks, or controls defined in Oracle Fusion Cloud Financial Reporting Compliance.

Once relationships are created:

- In Oracle Fusion Cloud Advanced Controls, the page for viewing or editing an advanced control includes a Related Records panel. It lists the Oracle Financial Reporting Compliance objects you select here. You can click on a related record to view its definition.
- Also in Oracle Advanced Controls, the page for viewing or editing an incident includes a Related Records panel. It lists the Oracle Financial Reporting Compliance objects selected for the control that has generated the incident. Again, you can click on a related record to view its definition.
- In Oracle Financial Reporting Compliance, object records include an Advanced Controls tab. It displays the advanced controls to which a process, risk, or control is related. From the record of each control, you can display its incidents.

To create relationships:

1. Select the type of Oracle Financial Reporting Compliance object you want to relate to the advanced controls you're deploying. You may select Process, Risk, or Control.
2. Select Add Related Object.
3. In a Search dialog, supply parameter values to list a filtered set of Oracle Financial Reporting Compliance objects. Click Search to list the objects that satisfy your search parameters.
4. From the list, select any number of objects, then click OK.
5. As needed, select another type (repeat step 1) and add objects of that type (repeat steps 2 through 4).

Relating Oracle Financial Reporting Compliance objects serves no purpose for a control whose result type is **Data set**, since it doesn't generate incidents to be displayed with these objects.

Complete the Control Deployment

On a Deploy Controls: Review page, review your selections. If you want to make changes, navigate back to the appropriate page and do so. If you're satisfied, select Submit.

Run Advanced Controls

You can run any selection of advanced controls for which you're authorized as an owner or editor. Depending on the result type selected for each control, you may generate incidents or compile data sets for user-defined objects.

To begin, select the controls you want to run on the Controls page. You may work with your complete list of controls, or set search parameters to filter it, then work with the filtered list. In either case, you can:

- Select a continuous set of controls. Click the first, hold down the Shift key, and click the last.
- Select a discontinuous set. Hold down the Ctrl key as you click controls.

Then, do either of the following:

- Run the selected controls once, immediately. Select Actions, then Run.
- Schedule the selected controls to run regularly. Select Actions, then Schedule. Enter values that set a name for the schedule, when it starts, how regularly controls are evaluated, and when (if at all) the schedule expires. Then click the Schedule button.

Consider synchronizing data before evaluating transaction controls, or synchronizing global users before evaluating access controls. If you evaluate controls manually, you can synchronize manually first. If you schedule control analysis,

you can also create a coordinated schedule for synchronization. In either case, you synchronize data from the Advanced Controls Configurations page, or global users from the Global Users page, of the Setup and Administration work area.

Related Topics

- Schedule or Run Data Synchronization
- Configure Global Users

View or Edit an Advanced Control

Depending on your authorization for a control, you can open a page to view its full details or to edit some details.

If you're authorized at any level to work with a control, you can open a view-only page that displays its details. Or, if you're the owner or editor of a control, you can also open an edit version of that page. In it, you can modify some configuration details, add comments, or revise perspective and worklist-recipient assignments.

Even if you're authorized to work with a transaction control, you can open it for viewing or editing only if you're assigned all the delivered, user-defined, and imported business objects it uses. If you're not, a Missing Business Objects Access icon appears next to the control name. When you click on the name, a message identifies the objects you lack. An administrator must use a Business Object Security feature, available in the Risk Management Data Security work area, to assign you the missing objects.

To open a control in view mode, click its name in the Controls page. To open a control in edit mode, do either of the following:

- Open a control in view mode, then click Edit in the view page.
- In the Controls page, click in the row for the control you want to edit, and select the Edit icon.

In each of these pages:

- Expand the Security Assignment button, then select Control Security Assignment or Result Security Assignment. If you're an owner, you can then modify security assignments for the control or for the incidents it generates. Or you can view those assignments if you're an editor or viewer. Bear in mind, though:
    - Result security applies only to incident controls. The Result Security Assignment option is inactive if you're working with a data-set control.
    - A result-security edit applies only to incidents generated after the edit is made. Each incident generated before the edit continues to use the security configuration in force at the moment it was generated.
- Click a Control Logic tab to display the filters that define the processing logic of the control. These are arranged in the order they're analyzed in. You can't edit these elements.
- Click a Comments tab to display existing comments. When the page is in edit mode, you can add a comment.

- Click a Definition tab to review a full record of the current control configuration. In this tab:
    - Review the name and description of the control or, in edit mode, modify them.
    - A Details panel displays the status and priority of the control. You can modify those values in the edit-mode page.

      In the view-mode page, you can view documents attached to the control. In the edit-mode page, you can both view and add attachments to the control.

      A transaction control that generates incidents may cite one or more user-defined objects. For such a control only, a checkbox appears. In the edit-mode page, select it to cause data-set controls to refresh the user-defined objects automatically each time, and immediately before, the incident control runs. This checkbox is labeled, "Before this control runs, also run the user-defined objects that supply it with data."

      This panel also displays information you can't edit, including the following: The control type and result type; dates the control was created, most recently run, and most recently updated; and the people who performed these operations.
    - Control and Result Perspective Assignments panels display perspective values currently assigned to the control itself and to incidents it generates. In edit mode, you can modify these as you would if you were deploying a control.
    - A Worklist Assignment panel identifies the person assigned to receive worklist notifications to investigate incidents generated by the control. Or it selects all eligible users. In edit mode, you can modify this selection as you would if you were deploying a control.
    - If descriptive flexfield segments have been defined for the Advanced Control object, these appear as fields in an Additional Information panel. You can view values selected for the control or, in the edit-mode page, modify them.
    - A Related Records panel displays Process, Risk, and Control object records related to the advanced control. (Incidents generated by the advanced control are associated with these records.) In the edit-mode page, you can add or remove object records as you would if you were deploying a control.

  Options involving incident results apply only to incident controls. So result-perspective-assignment, worklist-assignment, and related-record options are inactive if you're working with a data-set control.

Related Topics

- Attach Documents to Controls and Incidents
- Secure Records in Advanced Controls
- Select Perspective Values in Advanced Controls

Delete an Advanced Control

You can delete advanced controls, although only one at a time.

The control must be at the Inactive status. If you delete an incident control, you also delete all incidents the control has generated. If you delete a data set control, you also delete its results and the user-defined object based on it.

1. Edit the control you want to delete to set its status to Inactive.
2. Navigate to the Controls page. In it, select the row for the control you want to delete.
3. Select the Delete option from the Actions menu.

Mass-Edit Advanced Controls

You can modify certain settings for multiple controls at once. These settings include priority, status, comments, perspective values, worklist assignment, additional-information fields, and related records.

1. Select controls you want to modify on the Controls page. You may work with your complete list of controls, or set search parameters to filter it, then work with the filtered list. In either case, you can:
    - Select a continuous set of controls. Click the first control, hold down the Shift key, and click the last.
    - Select a discontinuous set. Hold down the Ctrl key as you click controls.
2. Select the Edit icon. A Mass Edit page opens.
3. Modify any or all of the following:
    - Enter a new value for priority (a number value), status (Active or Inactive), or comment. You can also view or add attachments. The controls retain their original values for any of these fields you don't edit.
    - In each of the Control Perspective Assignment and Result Perspective Assignment panels, select perspective values to be added to, or removed from, those already in place for each control you're editing. Control perspectives apply to the controls you're editing, and result perspectives apply to incidents they generate.
    - Decide whether to select a result investigator to receive worklist notifications. By default, the field is blank. If you make no selection, each control retains the result investigator originally assigned to it. Or, a control adopts the All Eligible Users value if its original investigator has been invalidated. If you make a selection, it applies to all the controls you're editing.
    - If descriptive flexfield segments have been defined for the Advanced Control object, these appear as fields in an Additional Information panel. For each field, any value you enter applies to all the controls you're editing. Or, if you make no selection a field, each control retains the value originally set for the field.
    - In a Related Records panel, select Process, Risk, and Control object records to be added to, or removed from, those already selected for each control you're editing. Incidents generated by each advanced control are associated with these object records.

    Your selection of controls may include both incident and data-set controls. Your edits of result-perspective assignments, worklist-notification assignments, and related records are accepted for incident controls, but ignored for data-set controls.
4. To complete the edits, click the Submit button.

Related Topics

- Attach Documents to Controls and Incidents
- Select Perspective Values in Advanced Controls

7 Results

Overview of Advanced Control Results

An incident is a record of a transaction or a grant of access that's exceeded the risk defined by an advanced control. Incidents may be assigned to you because controls that generate them identify you as a result investigator, or because incident owners assign them to you.

The actual resolution of incidents occurs outside of Oracle Fusion Cloud Advanced Controls. For example, you may use the Financials application to cancel a purchase order if a transaction control shows it to be suspect. Or, you may revise the assignment of roles to a user if an access control uncovers a separation-of-duties conflict. In Oracle Advanced Controls, you can:

- Review the details of incidents assigned to you.
- Set the status of incidents for which you're authorized as an owner or editor. Status reflects whether anything should be, or has been, done about the incidents.
- Reassign incidents for which you're authorized as an owner.

To begin, select Risk Management in the home page. Among its options, select Results. Then select any of three tabs: Worklists displays your result-related worklist assignments. Results by Control Summary opens a page listing controls that have generated incidents assigned to you. Simulations takes you to a page to manage simulations, which preview the effects of steps you take to resolve violations of access controls.

Incident Status and State

If you're a result investigator for an incident, you can update status values to indicate the progress made toward the incident's resolution. These values include:

- Assigned: Result investigators have been appointed to address the incident. With one exception, this is the initial, default status for an incident.
- Accepted: Nothing need be done to resolve the incident.

  This is the one exception. A role assignment may be approved in Advanced Access Requests despite having violated an access control. If so, it generates incidents for which Accepted is the initial, default status. In any other circumstance, this status is available for you to select as an update to an earlier status.
- Remediate. Some action must be taken to resolve the incident.
- Resolved: Remedial action has been taken on the incident.

These status values suggest natural progressions, for example Assigned to Accepted, or Assigned to Remediate to Resolved. However, when an incident is at any of these statuses, you can select any of the others. For example, if you determine that an Accepted incident needs to be looked into, you can update it to Assigned.

The application may set additional statuses:

- Control Inactive: An incident is no longer of concern because the control that generated it has been inactivated.

- Closed: An incident has been resolved in the business application, so a subsequent evaluation of controls finds the incident need no longer be addressed.

A Closed incident may be reopened if circumstances warrant.

- To close an incident generated by an access control, a security administrator may adjust a user's role assignments to reduce that user's access to an application. Later, the user's access may be restored. If so, when the control runs again, a new incident isn't generated. Instead, the status of the original incident is reset to Assigned.
- Closed incidents that are reopened through a request in Advanced Access Requests are assigned the Accepted status. For each, the incident record includes comments written by the request reviewer and the request approver.

Not only does an incident have status, but it also exists in one of three states: In Investigation, Approved, or Closed. You can't directly set the state of an incident. When you change its status, however, the state may change:

- If the status of an incident is Assigned, or you submit it at the Remediate status, its state is In Investigation.
- If you submit an incident at the Accepted or Resolved status, its state is Approved.
- If the status of an incident is Closed or Control Inactive, its state is Closed.

State matters because by default Results pages show pending results, which are defined as those at the In Investigation state. Use standard search features to cause Results pages to display incidents at the Approved or Closed state, if your roles give access to data at those states.

Work with Results by Control Summary

The Results by Control Summary page displays a list of controls that have generated incidents. It presents summary information about each control.

The details you see depend on selections you make in the View Columns menu. However, you'd typically select the Name, Results Count, and User Count columns, whose values serve as links to other pages.

You can set parameters to filter the list of controls. In the row for any control in a complete or filtered list, you can:

- Click a triangle icon to open a hidden panel that displays additional details about that control.
- Click the control name to open pages to view or edit the control. These are the same as the view and edit pages available from the Controls tab of the Advanced Controls work area.
- Click the Results Count value to open a page that lists the control-generated incidents you've been authorized to see. In this page, you can mass-edit incidents or open incident records individually. The heading for this page is the word "Results" followed by the control name.
- In the record of an access control, click the User Count value to open a Results by Control and User page. It's the first in a series of pages that enable you to work with sets of access incidents generated by a control, but filtered by user and role. This feature applies only to access controls. For records of transaction controls, the User Count column contains no value.

Related Topics

- Filter Model, Control, and Result Lists
- View or Edit an Advanced Control

Review Incidents Generated by a Control

The Results page for a control displays a grid in which each row represents an incident the control has generated. By default, the page displays pending incidents (those at the In Investigation state), but if you have rights to view incidents at other states, you can search for them.

You can select any number of records, then click an Export to Excel button to export the records to an Excel file. (See *Manage Export Jobs*.)

Apart from those discussed below, columns are self-explanatory. You may find that some columns you want to see are hidden by default. Click **View > Columns** to select the columns appropriate for your purposes. If the results include date values, you can select a Display Time Stamp option to show time values with the dates.

Review Transaction Incidents

Each transaction incident is the record of a transaction that violates the control. However, a single violation may generate multiple incidents. For example, a control that detects duplicate invoices would generate an incident for each of the duplicated invoices.

Default columns include Result ID, Status, Group, Grouping Value, result attributes selected for the model from which the control was deployed, and any derived attributes.

- Result ID is an identifying value that serves as a link to pages where you can view or edit the incident. As an alternative, you can select the row for an incident, then click Edit to go directly to the edit page for the incident.
- Group and Grouping Value display information that varies:
  - A filter may use the Equals condition to set an attribute of a business object equal to itself. For each incident generated by that control, the Group field reports the business object and attribute. The Grouping Value field reports the common value of this attribute.
  - A filter may find transactions with similar values for a specified attribute. For each incident generated by that control, the Group field displays the word "Similar" and the specified attribute. The Grouping Value field displays the value of that attribute.
  - A function filter may calculate a value for a specified attribute across a group of transactions. For each incident generated by that control, the Group field identifies the function and the specified attribute. The Grouping Value field displays the calculated value.
- Incident Information displays the value of the first attribute among those selected to characterize the suspect transaction. It's not available by default, but you can select it for display.

Review Access Incidents

Each access incident consists of information about the path through which a user is assigned one of the access points involved in a conflict. Typically, a single access conflict involves multiple incidents, presenting information about multiple assignments that the control defines as conflicting.

Default columns include Global User, User First Name, User Last Name, Role, Access Entitlement, Access Point, Incident Information, Conflicting Roles, Group, Investigator, Comments, and Attachments. Rows are sorted by global user.

- Access Point identifies an access point that the control defines as inherently risky or conflicting with other access points. Its assignment to an individual user is the focus of the result record.

- Incident Information reports the path to that focal access point. However, there are actually two incident-information columns:
  - The Incident Information column is included by default in access-control results, and it uses display names to identify roles in the path. But display names may not be unique.
  - Incident Information Codes uses role codes to identify roles in the path, and every role code is unique. Although this column isn't included among the results by default, you can select it for display.
- Global User, User First Name, and User Last name identify the person assigned the Incident Information access point.
- Access Entitlement identifies the entitlement (if any) that's named in the control and includes the Incident Information access point.
- Group identifies one or more access points that the control defines as conflicting with the Incident Information access point.
- Role identifies the role that grants the user access to the Incident Information access point.
- Conflicting Roles identifies roles that grant the user access to the Group access points.
- Data Source identifies the data source in which the Incident Information path exists.
- Result ID isn't available by default, but you can select it for display. If you do, it serves as a link to pages where you can view or edit the incident. As an alternative, you can select the row for an incident, then click Edit to go directly to the edit page for the incident.

For access controls, it's sometimes true that the assignment of a single role grants rights to the access points a control defines as conflicting. You can filter the incidents generated by an access control to display only those conflicts. Click the **Conflicts within a single role** checkbox.

An access control may contain a filter that specifies an access point from the Imported Access Point business object. After the control has generated incidents, the role assignments supporting that access point may be removed from a new data import. If so, the access point remains in the control, but its incidents are closed automatically. Records of the incidents include the comment "Incident closed due to inactive access points." Similarly, incidents are closed automatically, with the comment "Incident closed due to inactive user," if a new data import removes all records of the user involved in the incidents. If a subsequent data import restores the access point or user, the incidents are reopened.

Related Topics

- Define Transaction Model Results
- Attach Documents to Controls and Incidents

View or Edit an Incident

Depending on your authorization for an incident, you can open a page to view its full details or to edit details.

If you're authorized at any level to work with an incident, you can open a view-only page that displays its details. Or, if you're an owner or editor of an incident, you can also open an edit version of that page. In it, you can set the incident's status, write comments, or add attachments.

Having opened the Results page specific to a control, click the Result ID value for one of the incidents it lists. This opens its view-only page. The Result ID column is available by default for transaction incidents. For access incidents, it's not available by default but you can click View > Columns to select it for display.

To open an incident in edit mode:

- In the incident list, select the row representing an incident, then select the Edit icon, which looks like a pencil. This icon is active only if you select a single incident. (It's distinct from the Mass Edit button, which enables you to edit multiple incidents at once. A separate topic later in this chapter covers mass editing.)
- Open the view-mode page for an incident, then click its Edit option.

In each of these pages:

- Click the Security Assignment button to modify the assignments of users to the incident if you're an owner, or to view those assignments if you're an editor or viewer.
- Review the control name and description, incident status, and any attachments to the incident in the header area of the page. In edit mode, you can assign a new status to the incident. If you then submit the incident, the new status may also change the incident state. In edit mode, you can also attach files to the incident.
- Click a Result Attributes tab to view values for the attributes that characterize the incident. For a transaction incident, these are results attributes selected for the model that served as the source for the control that generated the incident. For an access incident, these identify an access point and a user it's assigned to. The access point presents risk either in itself or because it conflicts with other access points. You can't edit these values.
- Click a Comments tab to display existing comments. When the page is in edit mode, you can add a comment.
- Click a Definition tab to view a full record of the incident.
    - In the Details panel, view details that define the incident. You can't edit these values.
    - In the Result Perspective Assignment panel, view the current perspective assignments that apply to the incident. In edit mode, you can modify these values
    - In the Worklist Assignment panel, view the person currently assigned to receive worklist notifications that apply to the incident. In edit mode, you can select another user or all eligible users.
    - In the Related Records panel, view records of Process, Risk, and Control objects related to this incident. These relationships are indirect. The objects are actually related directly to the advanced control that generated the incident. Select Process, Risk, or Control to populate the grid with records of the type of object you've selected. You can't edit these records, nor modify the selection of objects at the incident level.
    - If descriptive flexfield segments have been defined for the Incident Result object, these appear as fields in an Additional Information panel. You can view values selected for the incident or, in the edit-mode page, modify them.

Related Topics

- Incident Status and State
- Attach Documents to Controls and Incidents
- Secure Records in Advanced Controls

Review Access Incidents by Control, User, and Role

An access control may generate thousands of incidents. Rather than review them all at once, you can separate them into manageable sets that apply to individual users, or even sets that apply to roles assigned to each of those users.

In the Result by Control Summary page, click the User Count value in the record of an access control to open a Results by Control and User page. In it, each row identifies a user involved in incidents generated by the control you selected and the number of pending incidents applying to that user.

In that page, you can click a user's number of pending-incident paths to open a Results by Control, User, and Role page. Each of its rows identifies a role assigned to the selected user and involved in the incidents generated by the selected control. Each row also displays the number of pending incidents applying to its role.

From there, you can click on a role's number of pending-incident paths to open a Results page filtered to display the incidents that apply to the user and role you've selected. Except for the filtering, this is the same as the page you'd open by clicking the Results Count value for a control in the Result by Control Summary page. You can use it in the same way to mass-edit incidents, open incident records for individual review or editing, create visualizations, or run contextual reports.

In the Control-User and Control-User-Role pages, you can:

- Mass-edit all the incidents that apply to a user in the Control-User page. Or, mass-edit all the incidents that apply to a role assigned to a user in the Control-User-Role page. In either case, click the pencil icon in a record to edit the incidents associated with that record. Among other things, mass-editing enables you to resolve a set of incidents by updating their status. (See the *Mass-Edit Incidents* topic for more information.)
- Search among the users or roles the page lists. As you begin to type in the Search field, a window presents the names of items that contain the letters you've typed. You can click on a name to select that item. Or, in the Control-User page, click Show Filters to create filters on these user attributes: Manager, Location, Department, Country, Job, Email, and Business Unit. (To view the attribute values assigned to a user record, expand its row.)
- Sort records. In either page, Pending Incident Paths is the default; it sorts records in descending order of the number of incidents they contain. In the Control-User page you can sort by user, and in the Control-User-Role page you can sort by role, to list records in ascending alphabetic order of item names. Select the sort you want in a Sort By field.
- Export the content of the page to a spreadsheet. Select Actions > Export. A message presents a job ID. Use it to identify the record of that job in the Monitor Jobs page. When the job status is Complete, download the file from the job record.
- Refresh the page, to capture the latest records and counts based on the most recent run of a Record Count Update job. Select Actions > Refresh.
- Display "user cards," which show additional information about the users to whom incidents apply. Hover over a user's picture until an ellipsis appears. Then click on the ellipsis.

Note: These features apply only to access controls and the incidents they generate. Transaction-control records in the Result by Control Summary page don't contain User Count values, and for them you can't open the Results by Control User page or the pages it drills down to.

Related Topics

- Access Visualizations
- Run Contextual Reports

Reassign an Incident

Only an owner of an incident can reassign it to a new selection of investigators.

That's because a user must be an owner or editor of an incident to have the authorization to edit its record (reset its status). Only an incident owner can modify the selection of users who serve as owners and editors. To do this, the owner would select the Security Assignments option in the record of the incident, and make changes.

However, either an owner or an editor of an incident can modify its Result Investigator setting, which determines whether all eligible investigators receive worklist notifications of the incident, or whether only one does, and if the latter, which one.

Mass-Edit Incidents

You can modify certain settings for any number of incidents at once. These settings include status, comments, additional-information fields, perspective assignments, and worklist assignments. You can also reconfigure incident security.

Select Incidents from the Results Page

To begin, produce a complete list of pending incidents generated by an access or transaction control: Click the Results Count value in the record of that control. You can find that record either in the Results by Control Summary page of the Results work area, or in the Controls page of the Advanced Controls work area. A Results page then displays incident records.

Next, use any of the following three methods to determine which of those incidents you want to edit. Then click the Mass Edit button.

- Accept the full list: don't filter it or select from it at all. In this case, all the incidents are considered for edit. (But see What You Can Edit, below.)
- Filter the list to include only the incidents you want to edit, but make no selections from the filtered list. In this case, all the incidents in your filtered list are considered for edit.
- In either a filtered or unfiltered list, select incidents. To select a continuous set of incidents, click the first one, hold down the Shift key, and click the last one. Or to select a discontinuous set, hold down the Ctrl key as you click on records. In this case, only the incidents you select are considered for edit.

Here are two additional considerations:

- A Results page displays a maximum of 500 incidents, but its control may have generated more. The page also reports the number of incident records that match filtering criteria. (If you haven't applied filters, this is the total number of incidents the control has generated.) If that number is greater than 500, you're updating all incidents that match filtering criteria, not just the 500 on display.
- When you work in the Results page, the Edit icon, which looks like a pencil, applies only if you've selected a single incident to be edited. The Edit icon is disabled, and you'd use the Mass Edit button, if you've selected no incidents (and so intend to edit a full or filtered list) or if you've selected two or more incidents.

Select Filtered Sets of Access Incidents

These alternatives apply only to access controls and the incidents they generate: Click the User Count value in the record of the control. You can find access-control records containing this value only in the Results by Control Summary page of the Results work area. Then, in the Results by Control and User page, click the Edit (pencil) icon in the record of the user whose incidents you want to edit.

Or, click the pending-incident path value for that user. In the Results by Control, User, and Role page, click the Edit icon in the record of a role assigned to the user, to edit the incidents involving that role.

Or, click the pending-incident path value for the role to open a Results page filtered to display the incidents that apply to the user and role you've selected. There, you can once again update the entire list, filter it to update only the records that remain, or select from a full or filtered list. In this page, you'd once again click the Edit icon if you've selected a single incident or click the Mass Update button to edit multiple incidents.

What You Can Edit

No matter how you produce a set of incidents for mass edit, you may include records for which you're an owner, editor, or viewer:

- For records you own, all updates are accepted, including security updates.
- For records for which you're an editor, security updates are ignored, but updates of other details are accepted.
- For records for which you're a viewer, all updates are ignored.

Update the Incidents

Once you've selected records, a Mass Edit page opens:

1. In a Mass Edit Selection panel, determine what you want to update: click either Mass Edit Details or Mass Edit Security.
2. Enter update values in the fields you want to edit. These are described below.
3. Select Submit.

As you edit details, do any of the following. Incidents retain their original values for any of these features that you leave unedited.

- Select a status you want to assign to the selected incidents.
- Write a comment, or attach a file or URL.
- In the Perspective Assignment panel, select perspective values to be added to values already selected for each of the incidents you're working with. If you're updating records you've explicitly selected, you can also remove perspective values. This capability isn't available for if you're updating a full or filtered list, to safeguard against a performance issue that can be expected with large jobs.
- In the Worklist Assignment panel, select a user, or all eligible users, to receive worklist notifications concerning the incidents.
- If descriptive flexfield segments have been defined for the Incident Result object, these appear as fields in an Additional Information panel. Make any appropriate modifications to field values.

As you edit security configuration, you can add users; authorize users as owners, editors, or viewers; or remove users. You can also add or remove user groups. You can complete these tasks in the same way that you'd work with the Mass Edit Security Assignment tool.

Related Topics

- Incident Status and State
- Filter Model, Control, and Result Lists
- Attach Documents to Controls and Incidents
- Use the Mass Edit Security Assignment Tool

8 Visualizations and Simulations

Overview of Visualizations and Simulations

As an aid in resolving access incidents, you may create visualizations and simulations.

Visualizations are graphic depictions of paths that lead from users to the roles they're assigned and ultimately to conflicting access points. Simulations preview the effects of steps you may take to resolve access conflicts. These items may be related to one another: a simulation can focus on the resolution of conflicts involving access points depicted in a visualization.

Visualizations and simulations are for use only in understanding and resolving access incidents. They don't apply to transaction incidents.

Access Visualizations

You can create an image that shows how users are granted conflicting access points. The image may display results returned by an access model or incidents generated by an access control.

Each image consists of nodes that represent users, roles, and privileges. Arrows connect these nodes to define user-to-privilege access paths. You can choose between views that arrange these nodes in differing ways:

- Layers: The nodes form rows. Nodes in the highest row represent users. Those at the next level represent job roles assigned to those users. Those at lower levels represent subordinate access points, extending down to duty roles and then privileges that enable a user to view or modify data.
- Flow: User-to-privilege paths flow generally from left to right. When paths for multiple users involve common roles or privileges, however, some arrows connecting nodes may extend up or down, curving to the right. (In some cases, individual paths may overlap. You may need to drag nodes representing users to positions that enable you to view all nodes.)

Work with an Access Visualization

Create a visualization from a page that lists either results generated by an access model or incidents generated by an access control.

1. Navigate to that page by clicking the Results Count value for a model in the Models page or for a control in the Results by Control Summary page.
2. Select up to 25 results to include in a visualization. To select one result, click in the row representing it. To select a continuous set, click the first row, hold the shift key, and click the last row. To select a discontinuous set of rows, hold the Ctrl key as you click rows.
3. Click the Visualize icon.

Use the Legend

Nodes for each object type are depicted in a distinct shape and color, so that you can distinguish them easily. A Legend tells which shapes and colors correspond to which objects. You can take the following actions:

- Hover over an entry to highlight objects of its type (by graying out other types of object).
- Hide or expose the Legend by clicking its button.

Node Labels

You can use a Control Panel to zoom in or out of the image. As you do, the labels identifying nodes change:

- If the image is large enough, each node displays the name of the item it represents.
- If the image is smaller, symbols replace the names: U for user, R for role, S for predefined role, P for privilege, and A for aggregate privilege.
- If the image is smaller still, the nodes are unlabeled.

Regardless of labeling, you can hover over a node to display the name and description of the user, role, or privilege it represents.

Use Control Panel Tools

A Control Panel contains these tools:

- Change Layout: Select a view for the image, either Layers or Flow.
- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.
- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.
- Zoom to Fit: Center the image and size it so that it's as large as it can be while fitting entirely in its display window.
- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area beneath the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.
- Search: Enter text to locate nodes whose names contain matching text. The search uses a "contains" operator, selecting nodes whose names include the search string at any position.
- Control Panel: Hide or expose the Control Panel.

If you right-click on a node, an Options menu presents the same tools as the Control Panel. Although you use a specific node to reach this menu, its options apply to the visualization as a whole.

Use the Overview

At the lower right of the image, click a plus sign to open the Overview, a thumbnail sketch of the visualization. In it, click any area of the thumbnail to focus the actual visualization on that area.

As an alternative, click the background of the visualization, then drag the entire image in any direction.

Simplify the Result Display

You can simplify either the visualization itself or the display of result records in the results page from which you generated the visualization.

- In a panel titled Choose the Simplification, use a Level field to remove nodes from the visualization. Select Hide User to remove user nodes and retain role and privilege nodes. Select Hide User and Role to retain only the privilege nodes. Or click Show All to restore the full visualization.
- Click a node in the visualization. Only nodes in the direct path to the one you selected remain "active"; others are dimmed. Also, the name of the node you selected appears next to an Apply button in the Choose the Simplification panel. Click that button to return to the results page and have it display records only of results that involve the user, role, or privilege whose node you selected. (Before clicking the Apply button, you can undo your selection: Click a user at the top of the visualization hierarchy, then click the background of the visualization.)

Access Simulations

Simulation previews the effects of changes you might make in your security model to resolve incidents identified by access controls.

A simulation consists of remediation steps; each hypothesizes the removal of an access point from a role hierarchy. Incidents involving that access point (reached from within that hierarchy) would be resolved if the access point were actually removed.

You can create a simulation from a visualization of control incidents. This permits you to use the access points it depicts as the focus of remediation steps. This is preferred, because the simulation job is based on a single control, and so requires less time to run.

Or, you can begin from an Access Simulations page. This is typically not preferred, because the simulation job encompasses all controls, and so requires more time to run. This option, however, may be desirable if you want to simulate across controls, or if you know the access points to include in remediation steps and their relationships to access points in their role hierarchies.

To reach the Access Simulations page, select the Access Simulations tab in the Results work area. Each row in the page provides summary information about an existing simulation. Click the name of one to open a page that displays full details of its configuration.

Work with an Access Simulation

To create a simulation, determine whether you want to base it on a visualization. If so, create the visualization, then click its Create Simulation button. If not, open the Access Simulations page and click its Create option.

In either case, a Create Access Simulation page opens. If you're basing the simulation on a visualization, a Remediation Steps panel of this page includes a Visualize icon. If not, this icon doesn't appear. Begin by creating a name and, optionally, a description for the simulation.

Create Remediation Steps

Each remediation step names two access points:

- A "Remove" access point is one involved in an access incident. Your purpose is to simulate what would happen if you were to remove it from a role hierarchy.
- A "From" access point should always be the immediate parent of the Remove access point in a role hierarchy.

If you're basing the simulation on a visualization, you may use the following method to select pairs of access points for remediation steps. This method isn't available if you opened the create page from the Access Simulations page.

1. In the Remediation Steps panel, click the Visualize icon. A Visualization page opens, displaying the visualization you're basing the simulation on.
2. Click on a solid arrow connecting any two access points in the visualization. With the arrow highlighted, right-click and select Remove. The solid arrow becomes dashed, indicating that the access points are selected for a remediation step.
3. If other pairs of access points are appropriate for your simulation, repeat the previous step to select them.
4. If necessary, cancel selections: Click on a dashed arrow. With that arrow highlighted, right-click and select Reset. The dashed arrow becomes solid once again.
5. Select the Back icon. You're returned to the Create Access Simulation page, and each pair of access points you've selected appears in a row of the Remediation Steps grid. For each pair, the parent access point occupies a From Access Point field, and the child access point occupies a Remove Access Point field.

A second method of selecting access-point pairs for remediation steps is available no matter how you create the simulation.

1. In the Remediation Steps panel, select Add. A row appears in the grid.
2. In the Remove Access Point field, click Search. In a Search and Add dialog, search for and select an access point involved in an access incident.
    - If you're basing the simulation on a visualization, the Search and Add dialog limits you to access points that both appear in the visualization and have parent access points.
    - If you aren't basing the simulation on a visualization, the Search and Add dialog enables you to select among all access points.
3. A From Access Point field becomes active only after you make a selection in the Remove field. Click Search in the From field.
    - If you're basing the simulation on a visualization, a Search and Add dialog limits you to access points that are parents of the Remove access point, each in a distinct role hierarchy. Select one.
    - If you aren't basing the simulation on a visualization, the Search and Add dialog enables you to select among all access points. However, be sure to select an immediate parent of your Remove access point in a role hierarchy.
4. Repeat these steps as necessary to select other pairs that are appropriate for your simulation. You can also delete pairs. Select a row and click Delete.

When you finish creating remediation steps, save your simulation.

Run a Simulation and Review Results

In the Remediation Steps panel, click the Run Simulation button.

A message displays a job number. Make a note of it. You can track the progress of the job in the Monitor Jobs page; click the Monitor Jobs button. Click the Back icon in the Monitor Jobs page to return to the simulation.

Once the job is complete, an Impacted Incident Path Counts panel presents results. In a View By field, select User, Control, or Role. A grid then displays the numbers of current and remaining incidents for each user, control, or role affected by the simulation, as well as the difference between these amounts.

- Current is defined as the number of pending incidents that actually exist.
- Remaining is defined as the number that would exist if the simulated changes were implemented.

An Overall Pending Incidents graph provides slightly different results: the current and remaining values for all pending incidents, both those affected by, and those unaffected by, the simulation.

Optionally, select Run Remediation Report to save or print the remediation steps and results of the simulation you're working in. Or, use a Simulation Remediation Plan dashboard to select simulations and view their remediation-plan steps and their results. The dashboard is available in the Oracle Business Intelligence Catalog.

A User and Role Impact page lists the users and roles that would be affected by the simulated changes. To reach this page, click the User and Role Impact button.

- This page displays records only of paths that would no longer grant access to users. For example, suppose a control defines a conflict between two privileges, P100 and P200. A user has access to both. A remediation step simulates the removal of P100 from the role hierarchy that grants the user access to it. The User and Role Impact page would show a record of the user's access to P100, but not of the user's access to P200.
- The removal of an access point from its immediate parent may not only resolve incidents. Some users may have legitimate access to the removed access point, and implementation of the remediation plan would shut off that legitimate access. The User and Role Impact page lists both types of user, those with resolved control violations and those with lost legitimate access. It documents the roles that would no longer grant access if the simulation were implemented.

Related Topics

- Use Predefined Dashboards

Edit a Simulation

You can edit or rerun a simulation: Select its row in the Access Simulations page, then select Edit. Or, click the simulation name to open its details page, then click the Edit button in that page.

However, if you initially based a simulation on a visualization, that visualization is no longer associated with the simulation as you edit it. So you can't use the procedure that involves selecting the connectors between access points in a visualization.

Thus no matter how you created a simulation, as you edit its remediation steps you must search for values in the Remove Access Point and From Access Point fields of rows in the Remediation Steps grid:

- As you select a value for the Remove Access Point field, the Search and Add dialog enables you to search among all access points.
- As you select a value for the From Access Point field, the Search and Add dialog enables you once again to search among all access points. Once again, however, be sure to select an immediate parent of your Remove access point in a role hierarchy.

9 Reports

Advanced Controls Reports

You can run the following reports about Oracle Fusion Cloud Advanced Controls.

Result Reports

Result reports include:

Report Title	Description
Access Point Report	Lists paths to access points involved in conflicts. Each record in the report isn't a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
Access Violations by User Report	Lists ten users with the greatest number of conflicts, the number of conflicts for each, and information about those conflicts.
Access Violations within a Single Role (Intra-Role) Report	Lists roles you can't assign individually to any user without a conflict occurring, because each role contains privileges that controls define as conflicting.
Intra-Role Violations by Control Report	Lists access controls that generate conflicts involving privileges granted within individual roles. It identifies roles that have violated each control, and it lists incidents at the Assigned, Remediate, or Accepted status.
Global Users Report	Provides information about global users: IDs, each identifying one person and correlating to any number of potentially varying IDs that person may have in business applications subject to advanced controls.
Result by Control Summary Extract Report	Lists access and transaction controls that have generated pending incidents, and provides information about each control.
Users with Access Violations by Control Report	Lists access controls that have generated incidents at the Assigned, Remediate, or Accepted status. For each control, it lists users whose work assignments have violated the control.

Business Intelligence Analyses

Apart from these reports, predefined dashboards provide analyses (displays of real-time data) that track change history, identify records that aren't accessible by any user, and identify perspective hierarchies and values that aren't assigned to any object. These dashboards are available in the Oracle Business Intelligence Catalog. (See *Use Predefined Dashboards*.)

Run Contextual Reports

From the Results by Control Summary page, or from the Results page for an access control, you can run reports about access controls or incidents.

1. In either of these pages, filter the list of items to include only the controls or incidents you want the report to cover. For example, you can filter a list to include controls at a particular priority, or incidents at a particular status.
2. In the Run Report field, select the report you want to run. Also select its format.
3. Click the Go button. A message identifies a job number. Note the number, then close the message.
4. Click the Monitor Jobs button to open the Monitor Jobs page.
5. Locate the row representing the job whose number you noted. When the status displayed in that row reaches Completed, click the Download icon.

Related Topics

- Filter Model, Control, and Result Lists

Run Reports

You can run reports on demand or schedule them to be run at intervals over a period you define. Scheduled reports are saved, so you can view them at any time.

1. From the Risk Management springboard, open the work area for the reports you want to run: Advanced Controls Reports or Financial Compliance Reports. Or, open the Navigator and select either reporting option.
2. In the Financial Compliance Reports work area, open the Related Links panel tab and select a category of reports. The reporting page lists reports belonging to the category you selected. (In the Advanced Control Reports work area, there's only one category, and so no selection to be made.)
3. Click in the row for the report you want to run.
4. Click Actions > Run Now or Actions > Schedule.
5. A Parameters dialog opens. In it, select parameter values to focus the content of the report.
6. If you selected Run Now, the Parameters dialog displays a Submit button. Click it to generate the report.

   If you selected Schedule, this button is replaced by a Schedule Information button. Click this button to produce a Schedule Parameter dialog. Enter values that set a name for a schedule, the date and time it should start, how regularly the report should run, and the date and time (if any) the schedule should expire. Then click the Schedule button.

Report Parameters

You can select parameter values that focus the content of reports you generate.

Parameters vary from one report to another. In general, they correspond to the selections users make as they work with the object you're reporting on. As you set parameters, select among the same values.

For example, a Control Details Report enables you to select among values you'd set as create or edit controls in Oracle Fusion Cloud Financial Reporting Compliance. You can filter by name; select controls with specific method, frequency, or stratification values; or select other values that apply to controls. You may also select a report format, either PDF (Adobe Acrobat file) or CSV (a text file for export to another application, such as a spreadsheet).

Select parameter values in the Parameters dialog that opens as you run or schedule reports.

Save Parameter Values

You can save sets of parameter values, so that you can select them easily as you run reports:

1. In the Parameters dialog that opens when you select the Run Now option in the reporting page, select a set of parameter values. Then click the Save Report Parameters button.
2. A Create Saved Report Parameters dialog opens. In it, create a name for the set of parameter values, and click the OK button.

To use a set of saved parameter values, select it in the Select Saved Report Parameters field, which appears in the Parameters dialog as you run or schedule a report.

In this field, you can select a Personalize option. This opens a Personalize Saved Report Parameters dialog. Select one of the sets of saved parameters. Then do any of the following:

- Click the Delete button to delete the set of saved parameters.
- Select or clear a Show in Saved Report Parameters checkbox to make the set of parameters available, or hide it, in the Select Saved Report Parameters field.
- Select or clear a Default Report Parameter checkbox to apply the set of parameters each time you run the report. (Select this option for only one set of parameters per report. Clear the existing selection before setting this option for a new set of parameters.)

Select the Apply button in the Personalize Saved Report Parameters dialog to implement your selections, and the OK button to close the dialog.

Review Scheduled Reports

If you schedule a report to run, the reporting page can display a row for each generation of the report. Or, it can display a row for each schedule configured for the report.

To view a report generated on a schedule:

1. Click the title of the report you want to see.
2. Click Display, then Report History.
3. Click the row representing the instance of the report you want to see. Then select the View Report action.

(To remove an instance of a report, click its row and then select the Delete action.)

To view or modify a report's schedule:

1. Click the title of the report whose schedule you want to see.
2. Click Display, then Scheduled Reports.
3. Click the row representing a current schedule. (Schedules that have reached their end dates are removed from the list.) Then select the Manage Report Job Schedule action. The Schedule Parameters dialog reopens. You can:

- Enter modified schedule values and select a Reschedule button.
- Discontinue the schedule by selecting a Cancel Schedule button.

10 Provisioning Rules

Overview of Provisioning Rules

Provisioning rules enable you to prevent the assignment of Oracle Cloud roles in combinations that cause separation-of-duties conflicts.

Each rule identifies two roles that conflict with one another. Rule results can inform decisions you make as you create roles or as you grant roles to users.

You can create these rules manually, focusing on role conflicts that are important to you. Or you can run a Generate Provisioning Rules job to generate rules automatically. It evaluates all your active access controls to create rules, one for each pair of conflicting roles identified by each control. (For each run, the Monitor Jobs page displays not only a listing for the Generate Provisioning Rules job, but also one or more listings for a related Auto Provisioning job.)

Once you've created provisioning rules, you can use them in two ways:

- As you create or edit a role in the Security Console, you can evaluate provisioning rules in a Separation of Duties page. This enables you to avoid creating roles that have inherent conflicts. Analysis in the Security Console returns conflicts when roles named in a provisioning rule exist anywhere in the role hierarchy of the role you're creating or editing.
- You can integrate rules with your user-provisioning workflow or process. To do that, you use a method available in an Oracle REST API. This method returns conflicts only when roles named in each provisioning rule are directly assigned to, or requested for, a user; it doesn't search through role hierarchies.

Autogenerate Provisioning Rules

To identify pairs of conflicting roles, the Generate Provisioning Rules job evaluates all active access controls in your environment, regardless of whether the person who runs the job is authorized to work with them.

To autogenerate rules:

1. In the Advanced Controls work area, click the Provisioning Rules tab.
2. In the Provisioning Rules page, click the Generate Provisioning Rules button. A message reports a number identifying the job; make a note of it.
3. Click the Monitor Jobs button to navigate to the Monitor Jobs page. In the row for the number you noted, determine when the Generate Provisioning Rules job status reaches Completed.
4. Click the Back icon in the Monitor Jobs page to return to the Provisioning Rules page.

When the Generate Provisioning Rules job finishes running, the Provisioning Rules page displays an Autogenerated Rules panel, which contains a row for each access control that generated rules. Each row:

- Reports the control name.
- Reports the number of rules generated for the control. Each control may define multiple conflicts, for example among multiple access points included in entitlements. Paths to these access points may involve numerous roles. Since each provisioning rule involves only two conflicting roles, each control may generate many rules. Rules may define conflicts between job roles, between duty roles, and between job and duty role combinations.

- Permits you to export rule data to a spreadsheet. Click the Export to Excel icon. A file-download window opens. Navigate to the folder in which you want to save the file and click the Save button. The file documents pairs of conflicting roles identified by the control whose row you're exporting from.

You can sort the control list by control name or by rule count; you can also use a search field to search for controls by name. A field beneath the search field reports the date and time of the most recent run of the Generate Provisioning Rules job.

The Generate Provisioning Rules job has no effect on any provisioning rules you create or edit manually.

Create or Edit Provisioning Rules Manually

To create or edit a provisioning rule manually:

1. In the Advanced Controls work area, click the Provisioning Rules tab.
2. If no rules exist yet, click Add to create one. Otherwise, work in the Manual Rules panel of the page: To create a rule, click Create. Or to edit a rule, select the row defining the rule you want to edit, and click Edit. An add-rules dialog opens.
3. In two fields, Role and Conflicts With, enter the names of roles the rule defines as conflicting.
    - You can enter either the display name or the internal name for a role.
    - As you type, a Roles window presents the display and internal names of roles that match the string you're typing. You can click on a role to select it for the field you're working in.
4. In a Risk Level field, select High, Medium, or Low.
5. Click OK.

Once the rule is saved, you can repeat the process to create or edit more rules. Or, use a delete option to delete a selected rule, or an About This Record option to view information about a selected rule. You can also sort rules by risk level, Role values, or Conflicts With values.

Use REST APIs to Evaluate Provisioning Rules

To build an application that evaluates provisioning rules as you assign roles to users, use a method called **Create a rules check for role assignments** (whose technical name is **runUserRoleCheck**). It's available in the Provisioning Rules REST API.

- Your application would pass in a user name and the codes for roles requested for that user.
- The API returns codes for roles that meet two requirements: First, they're requested for, or already assigned to, the user identified in the request. Second, provisioning rules define the roles as conflicting. Or, if no rules were violated, the API returns "No Violations."

Your application can also use other REST APIs to provide user information in addition to the user name. For example, among Common Features REST APIs, a Users task provides a **Get a user** method.

See REST API documentation for more information.

Run SOD Analysis in the Security Console

As you create or edit roles in the Security Console, you work through a series of pages. One of them, Separation of Duties, evaluates provisioning rules to uncover separation-of-duties conflicts in the role you're working with.

In summary, as you create or edit a role you supply basic information, define function security policies and data security policies, define a role hierarchy (a set of subordinate roles from which the role you're creating inherits functional access), and assign the role to users. Once you've defined the role hierarchy, you use the Separation of Duties page to determine whether the hierarchy contains roles that violate your provisioning rules.

To use the Separation of Duties page, however, you must first enable it: In Oracle Fusion Functional Setup Manager, open the Manage Administrator Profile Values page. (You can use the Search option, available in the panel tab, to search for this page.) In the Profile Option Code field, enter ASE_SEGREGATION_OF_ DUTIES_SETTING, then click Search. Set the site-level value for this option to Yes.

Related Topics

- Create Risk Management Roles in the Security Console
- Create ERP Roles in the Security Console

11 Advanced Access Requests

Overview of Advanced Access Requests

Advanced Access Requests implements a self-service workflow for requesting and assigning ERP roles. As steps in this workflow, access controls may perform separation-of-duties and sensitive-access analysis, and a review-and-approval process takes place.

Your current provisioning process might involve four manual steps: First, use the Security Console to assign Fusion roles to ERP users. Second, use the Manage Data Access for Users task in Functional Setup Manager to set data security for the role assignments. Third, check for SOD and sensitive-access policy violations. And last, document business-owner approvals, for example via email. But Advanced Access Requests replaces these steps. Here's how it works:

You request one or more roles, either for yourself or for another user. You can request any role that can be assigned directly to a user, such as a job, data, or abstract role. The request can be for a standard assignment, or for a temporary assignment to address ad hoc tasks such as IT troubleshooting or period-end transactions. A temporary assignment has a specified end date, and a standard assignment does not.

Along with the role, you may request data permissions, which define a set of data records the user can create or work with. For example, these might be records associated with a business unit you specify. If the request were to be granted, the user's authorization for the role would apply only to those records.

Your request and those of other requesters accumulate until an Advanced Access Request job processes them. The job runs on a schedule, although you can also run it on demand in the Scheduling page of Risk Management Setup and Administration.

- The job runs access controls to uncover SOD and sensitive-access issues. This analysis applies to requests for standard assignments, and only if one or more access controls are active. Requested roles may conflict either with each other or with a user's already-assigned roles. When the job finishes running, Advanced Access Requests reports the number of control violations for each role request. It also names the controls that have found violations, identifies the roles that conflict, and provides related data.
- The job bypasses access analysis for temporary-access requests even if access controls are active, or for any requests if no access controls are active.

In either case, a review-and-approval process ensues. The person who makes final decisions about requests is known as a "request approver." Before deciding on a given request, the approver may select a reviewer for it. This person judges whether the risk (or the absence of risk analysis) is acceptable, and therefore if the request should be granted or refused. By default the reviewer is the manager of the user for whom the role has been requested. However, the request approver may select another person with an interest in the work the user would be doing. In any case, the reviewer's judgment isn't binding, and the review process is optional.

Regardless of whether the review step takes place, the request approver determines whether to approve or reject the role for the user. For each approved role, Advanced Access Requests automatically completes these tasks:

- Updates the user's record in the Security Console to add the requested role. This happens whenever a role assignment is approved.
- Creates a new record in the Manage Data Access for Users task of Functional Setup Manager. This record associates the user, role, and data permissions with one another. This happens only when an approved request includes a data definition.
- Creates incidents in the Results work area to track control violations, if the request has generated any.

The request approver can also remove roles from users to whom they're assigned. The approver may be responding to requests by business owners or to removal reports generated by analysis in Oracle Fusion Cloud Access Certifications.

> **Note:** Some role customization is necessary for the majority of users (all but request approvers) to request roles. (See *Modify Security for Advanced Access Requests*.)

Use Dashboards to Work with Role Requests

Among the work areas in the Risk Management springboard, three apply to Advanced Access Requests. Access to them depends on the roles users are assigned. The landing page for each is a dashboard.

- A My Access Requests dashboard presents records of requests you've made for yourself or for others, as well as requests others have made on your behalf.
- An Access Request Reviews dashboard displays records of requests you've been selected to review.
- An Access Request Approvals dashboard contains records of requests for which you're an eligible request approver.

Each record in a dashboard shows the name of a user for whom a request has been made, an ID number for the request, and a "badge" that displays the number of controls that have been violated. (A badge might state "Queued" if the request is so new that the Advanced Access Request Analysis job hasn't yet run against it, "Analyzing" if analysis is under way, or "No active controls" if no access controls were active when the job was run.)

Records are categorized by status. You click a filtering option to view request records that include roles whose approval has reached the status you select. (See "Filtering," below.)

View Request Summaries

To view summary information about a request, click its request ID in a dashboard.

The summary record displays the name of the user for whom the request is made, the request ID and date, and its justification (a brief statement written when the request was made). For each requested role, it displays the role name, a security context (more on security contexts a little later), and a badge showing the number of access controls the role assignment would violate.

A special case: For certain privileges that grant access to Procurement functionality, a user must have both the privilege and a corresponding action as a procurement agent for a business unit. If a requested role includes such privileges, a field labeled Procurement Agent Access appears in the summary record available to approvers and reviewers, beneath the Request Date field. For more on this, see *Review a Role Request* and *Assign Reviewers and Approve Role Requests*.

Even though a summary record applies to a single request, it also provides status-based filtering options. That's to accommodate multiple-role requests.

Filtering

A single request may be for more than one role, and the approval process for those roles may be at more than one status. You filter by status for the requests you want to work with.

- In the My Access Requests, Access Request Reviews, and Access Request Approvals dashboards, the filter for a given status returns all records of role requests at that status. This means that the record for a multiple-role request ID may be selected by more than one filter.

  For example, suppose that a request includes two roles. The result approver has assigned one to a reviewer, but has not yet done anything with the other. A record of the request would appear if you were to select either the New Requests filter or the Pending Review filter.
- In a summary record, you can filter by status for roles included in the single request whose summary you're viewing, enabling you to revisit requests on which you've already worked. For example, a summary record opened from the Access Request Reviews dashboard has three filters, not only Pending Review but also Accepted Risks and Declined Risks.

View Request Details

From a summary record, you can open a drawer that displays details for a role you select. If the role you want to work with isn't already on display, select a status filter that returns it. Then click on its name. The drawer opens with the requested role as its heading.

Click tabs to view types of information you want to see. When you select a tab, its name is underlined and boldfaced. **Approvals** and **Data Permissions** tabs are available in records opened from any dashboard. Additional tabs are available only in records opened from the Access Request Reviews and Access Request Approvals dashboards. These include **Control Violations**, **Conflicting Roles**, and **Worker Info**, and may include **Security Briefing**.

- **Approvals** is the default tab when you open a drawer. In this view, you initially see a list of request approvers (all users assigned the Access Request Security Administrator role). Any one of them may act on the request. When one does, that approver takes responsibility for the request, and other approvers are removed.

  From then on, the Approvals tab displays rows that form a history of work on the request. Each row identifies an approver or a reviewer, and displays a badge indicating the status of an action that person is responsible for. When that person completes the action, another row is added, identifying the next person with a task to perform. Each row shows the date and time when an action occurred, and comments written by the actor.

- Select **Data Permissions** to see the data-security definition configured for the role request. At minimum, a request for data permissions consists of two components.
    - A "security context" may be any of these labels: Asset Book, Business Unit, Control Budget, Cost Organization, Data Access Set, Intercompany Organization, Inventory Organization, Ledger, Legal Entity, Manufacturing Plant, or Reference Data Set.
    - A "security value" is an item appropriate for one of these contexts, configured by your organization. If the role request were approved, it would grant access only to data associated with the security value.

  For example, if a role request includes the Business Unit context and the name of a business unit as its security value, it would apply only to data pertaining to that unit.

  However, data permissions can be more complex. First, the person who requests a role can select any number of security values for a security context. The role would then provide access to data records associated with any of the values.

  Second, the requester can select any number of security contexts, with values appropriate to each. To do so, the requester creates multiple requests for a role, each selecting security values for a distinct security context. The role would then provide access to data records that satisfy values selected for any of the contexts. However, this isn't a common occurrence. Typically, a single security context is appropriate for a role.
- Select **Control Violations** to see the names of the access controls violated by the role request. You'll also see counts of the violated controls and the total number of evaluated controls. Or, if no access controls were evaluated when the Advanced Access Request Analysis job was run for the request, an entry tells you so.
- Select **Conflicting Roles** to see a list of roles that would conflict with the requested role if the request were approved. The entry for each conflicting role includes a description. A long description may be truncated, but you can hover over it to see it in full. Or, if no access controls were active when the Advanced Access Request Analysis job was run for the request, an entry tells you so.

  Two things to note:
    - Because a control may detect more than one conflict, the number of conflicting roles may (and often does) differ from the number of controls that have found conflicts.
    - It's possible for a requested role to conflict with itself. This is known as an "intrarole" conflict: A role on its own includes access points that an access control defines as conflicting. When this occurs, the requested role appears both in the heading of the tab and in the list of conflicting roles.
- Select **Worker Info** to see information about two people. On the left, this view identifies the user for whom the role is requested, and on the right, that user's manager. For each, it displays the first and last name, job title, email address, and telephone number. For the user, the view also displays the legal employer, business unit, and department. All of this information is taken from the user's employee record in Human Capital Management. If a request approver decides to submit this request for review, the manager is the default selection for reviewer.
- Select **Security Briefing** to display data that informs the approval decision. (This tab appears only if setup steps have been completed. See *Activate Security Briefings for Advanced Access Requests*.)
    - A **Highlights** section presents an AI-generated paragraph that summarizes what the role's privileges enable a user to do. It also presents a list of statements about the user-role combination that's the focus of the record in which you opened the briefing. The list presents salient facts selected from the remaining sections.
    - A **Summary of privileges by functional category** section uses AI to define categories into which the role's privileges fit, and to describe what the privileges in each category enable a user to do.

- An **Elevated privileges** section tells whether the role is, is similar to, or includes a role from a set of IT roles that provide sensitive access. If so, it identifies the IT role. The role being requested for assignment is similar to an IT role if it includes 75 percent of the IT role's privileges.
- An **Unusual privileges** section tells whether the role contains privileges that aren't typically appropriate for the job title or position of the user whose role request is being considered. Typically, the role contains sensitive IT privileges, but the job title suggests the role isn't IT-related. If the role includes unusual privileges, the message includes the job title, position, or both (as appropriate). If the job title and position are unavailable, a message reports that no determination can be made.
- A **Related data access permissions** section documents the data-security definition configured for the role request.
- A **Usage in the organization** section reports numbers of users assigned the role that's been requested. Counts include users throughout your organization, users who report directly or indirectly to the manager of the user for whom the role is requested, and users who report directly to that manager. Also, a set of tests determines whether the user for whom the role's requested is likely to be nonhuman. If so, this section reports that judgment. (This section makes no comment if the tests suggest that the user is likely to be human.)
- An **Access certification history** section reports the number of users certified to keep the role this briefing is concerned with, and the number for whom role removal was recommended, in the last 12 months. Certifications are performed in the Access Certifications application.
- An **Inherent risks and incident history** section gives the numbers of access risks, both intrarole and across-role, that would result if the role were assigned to the user.
- A **Complete list of privileges** section presents a list of all the privileges included in the role this briefing is concerned with.

To close the details drawer, click its deletion (×) icon. To return from a summary page to a dashboard, click the View Dashboard button.

Make a Role Request

To request one or more roles, either for yourself or for another user, complete these steps.

1. Open the My Access Requests dashboard. In it, click the **Request Access** button. A Request Access page opens.
2. Your user name appears by default in a field labeled **Who is this request for**. Accept this if you want to request one or more roles for yourself.

   Or, to request one or more roles for another user, delete the default entry and search for that user's first name, last name, or user name. To search, begin to enter text. After you type a few characters, the application presents a list of values that include the text you've typed. You can then select one user from that list. (All fields in which you enter values use this search capability.)

   In your search text, a space is treated as one of the characters to be contained in return values. Some examples: "mark " ("mark" with a trailing space) would return "Mark Tayler" and "Mark Webb," but not "Marketing_Mgr"; "mark t" would return "Mark Taylor" but neither "Mark Webb" nor "Marketing_Mgr"; "mark" (no space) would return all three values.
3. In the field labeled **Why is additional access required**, enter a justification for your role request. This is a mandatory field.
4. To answer the question **Which roles and data would you like to request**, click the **Add Role** button. An Add Role drawer opens. In its **Role Name** field, search for and select a role you're requesting. You can search on the role's display name or internal name.

5. Still in the Add Role drawer, optionally request data permissions to be defined in the Manage Data Access for Users task of Functional Setup Manager.

    - In the **Security Context** field, select one of these labels: Asset Book, Business Unit, Control Budget, Cost Organization, Data Access Set, Intercompany Organization, Inventory Organization, Ledger, Legal Entity, Manufacturing Plant, or Reference Data Set.
    - A **Security Value** list presents items configured by your organization that are appropriate for the context you selected. Click checkboxes for any number of them. Or, click the Select All box. For example, if you select the Business Unit context, you can select any number of your company's business units.

    Together, these selections define data records the user would have access to while using the role you're requesting, for example records associated with any in a set of business units you've specified.

    Keep these considerations in mind:

    - A request for data permissions is optional because some roles, such as data roles, define their own data security. So you wouldn't request data permissions for them. For any other role, however, you must request data permissions. Otherwise the user for whom the role is requested would be granted the role, but have no access to data.
    - For certain privileges that grant access to Procurement functionality, a user must have both the privilege and a corresponding action as a procurement agent for a specified business unit. You may request a role containing such privileges, and the user who's to be assigned the role may have no earlier role assignment that recognizes him or her as a procurement agent.

      In that case, you must select the Business Unit security context and, as its security value, the appropriate business unit. If not, a message alerts you of this requirement, and you can't submit the request until you configure the data security correctly.
6. Click the **Add** button in the Add Role drawer. The drawer closes, and the Request Access page includes a row that displays the name of the role you've added, the name of the security context you've selected for it, and the number of security values you've selected for that context.
7. You may want to add roles to your request.

    - You may select a role you've already requested, so that you can request security values from a security context other than the one in your original request. However, this isn't common; often, only a single context is appropriate for a role. If you make multiple data-permissions requests for a role, a request approver may approve or reject each independently of the others. A role approved with multiple data-permission requests provides access to data associated with any of its contexts.
    - You may select a role you haven't already requested.

    In either case, repeat steps 4 through 6. You can request any number of roles. You can also remove a populated row by clicking its **Withdraw** icon (it looks like a trash can) or edit it by clicking its **Edit** icon (it looks like a pencil).
8. To answer the question **Is this access request temporary**, click **No** for a standard request (one that doesn't specify an end date). Or click **Yes** to request a brief assignment to complete ad hoc tasks on an urgent basis. Examples might be IT troubleshooting or period-end transactions. When you click Yes, a field labeled **Number of days access is needed** appears. Use its **Increase** and **Decrease** buttons to set the number of days the role will be granted to the user; the assignment ends automatically after that time passes. When you click Yes, the temporary assignment isn't subject to access analysis.
9. Click the **Submit** button. The focus returns to the My Access Requests dashboard, where the New Requests filter is active by default and a record of your request appears.

For any given user, only one request can exist at a time, although that request can be for any number of roles. This is the case no matter whether the user makes the request or someone else makes it on the user's behalf. If you select a user for whom a request is pending, an error message appears.

One response is to wait until a request approver has accepted or rejected all roles included in the pending request. But if you have access to the pending request (if you made it or it was made on your behalf), you can withdraw it and replace it with another. To withdraw a request:

1. In the Request Access page, click **Cancel** to return to the My Access Requests dashboard.
2. Click the ID for the request you want to withdraw.
3. In the summary page for that request, the record for each role includes a **Withdraw** icon. Click the icon for each role. When you have withdrawn all of the roles included in the request, the request itself is withdrawn.

Review a Role Request

A request approver may not have immediate knowledge of the person for whom a role is requested. So the purpose of a review is for an informed person, such as the user's manager, to provide input to the request approver. However, the reviewer's input is purely advisory; the request approver isn't bound by it.

The approver may make a final decision on the request without selecting a reviewer, and if so the review process is skipped. You can review a role request only if a request approver selects you as its reviewer.

A request for a given user may consist of a single role with a single security context; multiple assignments of a single role, each with a distinct security context; or multiple roles. When a review requires multiple judgments, you can make them collectively or one by one. (In particular, although requests for a single role with multiple security contexts may be related, you can accept or decline them independently of one another.)

To review a role request:

1. Open the Access Request Reviews dashboard. From the Pending Review list, click the ID for the request you want to review.
2. In the summary record of the request, click the name of a role you're reviewing to open its details drawer. Look over information about the data-permission request associated with the role and the user to whom the role is to be assigned. Also, if access controls were active when the request was made, go over the controls that have been violated and the conflicting roles those controls have identified. Then close the details drawer for the request you're reviewing.
3. A requested role may contain privileges that grant access to Procurement functionality. If so, a user must have both the privilege and a corresponding action as a procurement agent for a business user.

   In this case, a Procurement Agent Action field appears in the summary record. Click its Edit link to open a drawer. Review procurement-agent actions selected automatically by the application, and potentially edited by the approver. When you finish, close the drawer.
4. In the summary record, accept or decline the risk.
   - You may review a single-role request, or review multiple requests individually. For each, click the **Accept Risk** icon (a check mark in a circle) or the **Decline Risk** icon (the × symbol in a circle). A drawer opens; in it, write a justification for your decision (this is mandatory) and click either an **Accept Risk** or **Decline Risk** button.
   - If the request is for multiple assignments, you may choose to accept or decline all of them at once. Expand the **Actions** menu and select its **Accept All** or **Decline All** option. This opens the same Accept or Decline drawer, which you'd complete in the same way. But, of course, your decision would apply to all the requested roles.

5. Depending on your decision, you can click the Accepted Risks or Declined Risks filter to review your work. Or, for a multiple-role request, click the Pending Review filter to list roles you've yet to act on.

Assign Reviewers and Approve Role Requests

Every role request must be accepted or rejected by a request approver, even if it hasn't generated control violations. Review is optional, but if the request is to be reviewed, the request approver assigns the reviewer. The two processes are similar (and both are similar to the review process).

For a given user, you may be considering whether to approve or assign a single role with a single security context; multiple assignments of a single role, each with its own security context; or multiple roles. When a request requires multiple judgments, you can make them collectively or individually. (In particular, although requests for a single role with multiple security contexts may be related, you can approve, reject, or assign them to reviewers independently of one another.)

1. Open the Access Request Approvals dashboard and click the ID for a request you want to work with.

    - If you select among records at the New Requests status, you can assign a reviewer, or accept or reject the request without subjecting it to review.
    - If you select among records at the Pending Approval status, you'll make an approval decision on a request that's already been reviewed.

    In either case, you can't approve a request you've made for yourself or on behalf of another user.
2. In the summary record of the request, click the name of each role you're considering for approval to open its details drawer. Go over information about the request.

    - If it's been reviewed, the reviewer's accept-or-decline recommendation and the justification for that recommendation appear in the work history available in the Approvals tab.
    - Regardless of whether a review has occurred, click tabs to see the data-permission request associated with the role and the user to whom the role is to be assigned. Also, if access controls were active when the request was made, go over the controls that have been violated and the conflicting roles those controls have identified.

    When you finish, close the details drawer for the request you're considering for approval.
3. A requested role may contain privileges that grant access to Procurement functionality. If so, a user must have both the privilege and a corresponding action as a procurement agent for a business user.

    In this case, a Procurement Agent Action field appears in the summary record. Click its Edit link to open a drawer. You can review procurement-agent actions selected automatically by the application, and you can edit them. When you finish, close the drawer.
4. In the summary record, approve or reject requests, or assign them to reviewers:

    - A request may consist of a single record (one role with one security context) or multiple records that you want to consider individually. If you've selected a request at the New Requests status, you have three options for each role: **Approve**, **Reject**, and **Assign**. If you've selected a request at the Pending

Approval status, you have only the **Approve** and **Reject** options. You select among these options slightly differently.

When you have three options, the request record includes a **More Actions** menu, which looks like an ellipsis. Click it to select among the three options. When you can only approve or reject, icons representing those two options appear in the request record.

In any case, select the option you want, and a drawer opens. If you're assigning a reviewer, accept the default (the user's manager) or search for and select the name of another person. Add comments for the reviewer to consider, and click the **Assign** button. If you're approving or rejecting the role request, write a justification for your decision and click the **Approve** or **Reject** button. No matter which action you're completing, the comments to a reviewer or the approval-decision justification is mandatory.

- If the request consists of multiple records, you may choose to assign a reviewer for, approve, or reject all of them at once. Expand the **Actions** menu and select among its **Approve All**, **Reject All**, and **Assign All** options. This opens the same Approve, Reject, or Assign drawer, which you'd complete in the same way. But, of course, your decision would apply to all the requested roles.

5. Depending on the action you've taken, you can click the Pending Review, Approved, or Rejected filter to review your work. Or, for a multiple-role request, click the New Role Requests or Pending Approval filter to list roles you've yet to act on.

Remove Roles

If you're a request approver, you can also remove roles from users to whom they're assigned. Typically, you would do this in response to requests by business owners, or to removal reports generated by analysis in Oracle Fusion Cloud Access Certifications.

1. Open the Access Request Approvals dashboard. In it, click the Manual Access Removals tab at the bottom of the dashboard. A Manual Access Removals page opens.
2. Click the Remove Access button. A Remove Access page opens.
3. In a field labeled **Who would you like to remove roles from**, search for the user whose role assignment is to be ended. You can search by first name, last name, or user name.
4. In a field labeled **Give interested stakeholders your rationale for removing the access**, explain why the role is to be removed from the user.
5. Once you've entered values in these fields, a list of the user's current roles appears under the heading **Which roles would you like to remove**.
    - For each role, optionally click a **Data security** icon to open a drawer that displays the security context and security values associated with the role.
    - Select checkboxes for any number of roles you want to remove. Or, click a select-all checkbox, which is located next to a **Role Name** heading.
6. Click the Update button.

The focus returns to the Manual Access Removals page, where a record of the removal now appears. In that record, the user name is a link to a page that lists all removals for the user. The Manual Access Removals page displays records of role removals performed by all request approvers. As they accumulate, you can filter them by time periods, and you can sort them.

To return to the Access Request Approvals dashboard, click the Access Request Approvals tab at the bottom of the page.

Export Requests

From either the Access Request Reviews or Access Request Approvals dashboard, you can export records of role requests to an Excel spreadsheet. These may serve as reports of role-request history.

1. From either dashboard, filter the requests to produce a set you want to include in a report, for example Approved and Rejected.
2. Click the **Export** icon.
3. An information message reports a process number. Make a note of the number and close the message.
4. Navigate to Risk Management > Setup and Administration > Monitor Jobs.
5. Locate the row for the job whose process number you noted. When it reaches completion, click the Download File Attachment icon to download the file.