Oracle Risk Management Cloud

Using Advanced Controls Management

20A
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>i</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview of Oracle Advanced Controls Management</td>
<td>1</td>
</tr>
<tr>
<td>Common Concepts</td>
<td>1</td>
</tr>
<tr>
<td>2 Access Models</td>
<td>9</td>
</tr>
<tr>
<td>Overview of Access Models</td>
<td>9</td>
</tr>
<tr>
<td>Create or Edit an Access Model</td>
<td>9</td>
</tr>
<tr>
<td>Select Business Objects for an Access Model</td>
<td>10</td>
</tr>
<tr>
<td>Create an Access Point or Entitlement Filter</td>
<td>11</td>
</tr>
<tr>
<td>Create an Access Condition Filter</td>
<td>11</td>
</tr>
<tr>
<td>Create Path Conditions</td>
<td>13</td>
</tr>
<tr>
<td>Exclusions Involving Procurement Agents</td>
<td>14</td>
</tr>
<tr>
<td>Arrange Filters in an Access Model</td>
<td>15</td>
</tr>
<tr>
<td>View Access Model Results</td>
<td>16</td>
</tr>
<tr>
<td>Interpret Access Model Results</td>
<td>17</td>
</tr>
<tr>
<td>Eliminate False Positives</td>
<td>17</td>
</tr>
<tr>
<td>3 Access Model and Control Elements</td>
<td>21</td>
</tr>
<tr>
<td>Overview of Access Model and Control Elements</td>
<td>21</td>
</tr>
<tr>
<td>Entitlements in Access Models and Controls</td>
<td>21</td>
</tr>
<tr>
<td>Create or Edit an Entitlement</td>
<td>21</td>
</tr>
<tr>
<td>Global Conditions</td>
<td>22</td>
</tr>
<tr>
<td>Create or Edit a Global Condition</td>
<td>23</td>
</tr>
<tr>
<td>User-Defined Access Points</td>
<td>23</td>
</tr>
<tr>
<td>Create or Edit User-Defined Access Points</td>
<td>24</td>
</tr>
<tr>
<td>Audit Access Elements</td>
<td>25</td>
</tr>
</tbody>
</table>
4 Transaction Models

Overview of Transaction Models
Synchronize Data for an Individual Model
Best Practices for Transaction Model Development
Create or Edit a Transaction Model
Select Business Objects for a Transaction Model
View Business Object Relationships
Import Objects
Create a Standard Filter
Create a Function Filter
Model Filter Conditions
Advanced Options for Standard Filters
Advanced Options for Function Filters
System-Generated Objects
Create a Pattern Filter
Patterns
Arrange Filters in a Transaction Model
Define Transaction Model Results
Create Models That Support Audit
An Example of Enabling Items for Audit
View Transaction Model Results
Interpret Transaction Model Results

5 Advanced Controls

Overview of Advanced Controls
Deploy Advanced Controls
Evaluate Advanced Controls
View and Edit Individual Advanced Controls
Delete Advanced Controls
Mass-Edit Advanced Controls
### 6 Results

- Overview of Advanced Control Results
- Incident Status and State
- Work with Results by Control Summary
- Review Incidents Generated by a Control
- View and Edit Individual Incidents
- Reassign Incidents
- Mass-Edit Results

### 7 Visualizations and Simulations

- Overview of Visualizations and Simulations
- Access Visualizations
- Work with an Access Visualization
- Access Simulations
- Work with an Access Simulation

### 8 User-Defined Objects

- Overview of User-Defined Objects
- Create or Edit User-Defined Objects
- User-Defined Object Best Practices

### 9 Reports

- Advanced Controls Reports
- Run Contextual Reports
- Run Reports
- Report Parameters
- Review Scheduled Reports

### 10 Provisioning Rules

- Provisioning Rules
Preface
This preface introduces information sources that can help you use the application.

Using Oracle Applications

Help
Use help icons ? to access help in the application. 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. Not all pages have help icons. You can also access the Oracle Help Center to find guides and videos.

Watch: This video tutorial shows you how to find and use help.

You can also read about it instead.

Additional Resources

- **Community**: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.

- **Training**: Take courses on Oracle Cloud from Oracle University.

Conventions
The following table explains the text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than symbol separates elements in a navigation path.</td>
</tr>
</tbody>
</table>
Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website. Videos included in this guide are provided as a media alternative for text-based help topics also available in this guide.

Contacting Oracle

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
1 Introduction

Overview of Oracle Advanced Controls Management

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

- Oracle Advanced Access Controls enforces segregation of duties in your applications.
- 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 establishes a risk logic. Each control adopts the risk logic of the model it’s based on.

- An access model includes filters designating roles or privileges that, individually or in combination, would allow an individual user to complete risky behaviors. It then selects users assigned those points of access.
- A transaction model includes filters that define aspects of risk, then select transactions exhibiting the defined risk. (Models created in 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.

As an aid in resolving access incidents, you may create visualizations. These are graphic depictions of paths that lead from users to the roles they're assigned and ultimately to access points that models or controls define as conflicting. You may also create simulations, which preview the effects of steps taken to resolve access conflicts identified by controls. In addition, you may create provisioning rules, which identify pairs of conflicting roles. You can use them to prevent risky role assignments, and they operate completely separately from model- and control-based analysis. These features apply only to Advanced Access Controls, not to Advanced Financial Controls.

You may create perspectives; each is a set of hierarchically arranged values. Each represents a context in which models, controls, and incidents exist. You can relate individual perspective values to individual objects, thus cataloging them by organization, region, or any other concept your company finds meaningful.

Note: Advanced Access Controls also enables you certify that users' roles are appropriately assigned. Access certification features are documented separately in Oracle Risk Management Cloud: Using Access Certification.

Common Concepts
Secure Records in Advanced Controls Management

Records of models, advanced controls, and incidents are subject to data-security assignments. A user who creates a model is automatically its owner; a user who creates a control automatically owns both it and the incidents it generates. An owner of a record may select other users who can work with it.

While selecting users, an owner also authorizes each as an owner, editor, or viewer. 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, but not change, record details. 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 a step 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.

- To select an individual user, click Add in a User Assignments region. 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 region. Search for and select a group, and then save that selection. Groups have their own authorizations. You can view those authorizations as you select groups for a record, but you can’t change them.
- To edit or delete a user or group, click the edit icon in its row.

Related Topics
- Manage User Assignment Groups

Select Perspective Values

You can assign perspective values to models, advanced controls, and incidents in Advanced Controls Management, or to risks, controls, processes, and assessment batches in Financial Reporting Compliance.

Use the Perspectives region of the page you would use to create or edit any of these objects. Initially, this region displays a single list field. When you select a perspective hierarchy in that list field, the region expands to display Available and Selected fields. Move the values you want from the Available field to the Selected field.

In the Available field:

- You can type text in a search box to produce a list of matching perspective values. Entries are case-sensitive.
- A text search returns matching perspective values, regardless of hierarchy.
• Use view options to expand or contract the entire hierarchy or nodes within the hierarchy.

Also note the following:

• For the Perspectives region to appear in the create or edit page for an object, 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.

• As you associate a perspective with an object, you may designate it as required. If so, the hierarchy displays an asterisk in the Perspectives region of the page to create or edit the object. You can't save an instance of the object if no value is selected for a required perspective.

• If two or more perspective hierarchies are associated with the object, you can assign values from any combination of them. To select from each, open it from the list field in the Perspectives region.

• In Advanced Controls Management, you can mass-edit controls or incidents. As you do, you select perspective values to be added to, or removed from, values already selected for each of the objects you're working with.

Related Topics

• Perspectives

• Manage Perspective Mappings

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 region, select filtering values. Then click Search.

As you create searches, the filtering values you select generally have an AND relationship. That is, 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 would 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 region, 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 region. Then click the **Search** button.

### View Model or Control Details

Each row on the Models and Controls management pages provides summary information about a model or control created in Advanced Controls Management. Here’s how you can view full details about each model or control.

#### 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 would 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 Advanced Access Controls.
  - **Transaction - Pattern** indicates an 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 Advanced Financial Controls model that uses only standard or function filters to define a risk.
  - **Transaction** indicates a control created in 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 November 12, 2017. He updated it on December 17, then ran it on the same day. It returned 293 records. The row for this model might show its name, December 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 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. Hover over that number to reveal the names of the values and of the perspective hierarchies they belong to. For example, a control developed from the "Credit memos" model might be assigned a single perspective value. So the number 1 would appear in the Perspectives field of the expanded-details panel. But if you place the mouse cursor over this number, a display shows this value, for example North America in the Organization perspective.
Display Results

From the Models management page, you can't run a model, but you can view the latest results of a model that has been run. From the Controls management 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 documents to advanced controls and to incidents generated by those controls. An attachment may, for example, be a text file, spreadsheet, or Web site that provides more information about a control or incident that its description can contain.

To attach documents, work in a page to perform an individual or mass edit of controls or incidents:

1. Click the Manage Attachments icon. An Attachments dialog opens.
2. Select a Type, either File or URL.
3. If you selected File, click Browse to navigate to, and select, the file you want. If you selected URL, enter a URL in the File Name or URL field.
4. To create additional attachments, click the Add Attachment button. Then repeat steps 2 and 3 for each attachment.
5. Click the OK button to leave the Attachments dialog.

You can open attachments in an Attachments field of the view and edit pages for an individual control or an individual incident. Or, you can open them in an Attachments column in a page that lists all the incidents generated by a control.

The Attachments field displays the name of the first attachment. Click the name to open that attachment. If there are multiple attachments, the Attachments field 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.

Related Topics

- View and Edit Individual Advanced Controls
- View and Edit Individual Incidents
- Review Incidents Generated by a Control

Import Models, Controls, or Conditions

You can import models, advanced controls, or global conditions. (Note, though, that global conditions apply only to Advanced Access Controls.) These items may have been exported from another Advanced Controls Management instance to a file. Or, you may import delivered content: models (but not controls or global conditions) developed by Oracle.

Initial Considerations

A file exported from an Advanced Controls Management instance can be imported only into an instance at the same version or the next version. For example, if you export from a 19B instance, you can import into another 19B instance or into a 19C instance. In the export file, you can search for a <grcVersion> tag to identify the version from which the file was exported.
If an import file contains controls, you can import them either as controls or as models:

- To import them as controls, select the Import action in the Controls page. To import them as models, select the Import action 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. Select the import action in the Models page. Similarly, if an import file contains global conditions, you can import them only as global conditions. Select the Import action in the Global Conditions page.

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

Select an Import Vehicle

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

If you're importing models, the Import page provides two options:

- In an Import from User-Defined File region, you can complete the same process to browse for a file containing models or controls exported from an Advanced Controls Management instance.
- In an Import from Content Library region, you can select a link to delivered-content models. For example, you may select a link to transaction models or to access models in a Human Capital Management Library or an Enterprise Resource Planning Library.

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

Select Items

In an Import: Select Items page, review a list of the models, controls, or global conditions available to you. You can import only items that use business objects your roles give you access to. You can import some or all of those items. To filter them, search by name or description. Then select the check box in the row for each item you want to import.

Note: In general, if a transaction model or control calls an imported object, don’t select it for import unless the object already exists in the target instance. However, this restriction doesn’t apply to delivered-content models.

Resolve Duplicate Names

If you're importing models or controls, you can't import an item if its name matches the name of an item of the same type already existing in your target instance. This applies not only to items you select directly, but also to 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.

• 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 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 will 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 would 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.

Complete the Import

In an Import: Review page, review the selections you have 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 management page.

Related Topics

• Entitlements in Access Models and Controls
• Overview of User-Defined Objects
• Import Objects
Export Models, Controls, or Conditions

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

1. In the Models, Controls, or Access Global Conditions management 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 management 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 offers you options to open or save the export file. Select the Save option and, in a distinct save-as dialog, navigate to the folder you want to save the file in. The download file is saved in .xml format.

Related Topics

- Manage Export Jobs
2 Access Models

Overview of Access Models

An access model defines risk in the assignment of access points, which are roles or privileges that enable users to work with data in business applications. The model may identify access points that conflict, because in combination they would allow individual users to complete transactions that may expose a company to risk. Or it may identify 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 select records for analysis. 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, and typically contains two or more, of these filters. It returns records of users selected either by a single filter or by defined combinations of multiple filters.

Condition Filters

A filter may define a condition, which grants exemptions from access analysis. A model begins with a set of records involving access points specified by access-point and entitlement filters. Condition filters select records from that set, and so exclude the records they don't select. Such a 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 or departments.

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 created in Advanced Controls Management. That ID correlates to potentially varying IDs the person may have for business-application accounts.

Related Topics

- Global Users
- Configure Global Users

Create or Edit an Access Model

As you create or edit an access model, you select business objects, which provide data from your Oracle Cloud instance for the model to evaluate. You then define filters that select risky records from that data.

You can also select perspective values for the model. These may serve as filtering values in the Models management page. If you create a model, you're automatically its owner, but you can add other users to the model as owners, editors, or viewers only after you save the model for the first time.
To work with access models, select Risk Management in the home page. Among its options, select Advanced Controls. Then select a Models tab; it opens a Models management page that lists the models you have access to.

- To create a model, select Actions > Create Access Model in the Models management page. This opens a Create Access Model page. Begin by naming and describing the model.
- To edit a model, select its row in the Models management 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
- Select Perspective Values
- Secure Records in Advanced Controls Management

Select Business Objects for an Access Model

As you create an access model, select one or more business objects for it:

- Select the Access Point business object to create a filter that specifies an access point, and returns users assigned that access point.
- Select the Access Entitlement business object to create a filter that specifies an entitlement, and returns users assigned any access point in that entitlement.
- Select the Access Condition business object to create a condition filter, which defines exemptions from analysis by a model.

Make Selections

To add objects to a model:

1. Click Add in the Model Objects section 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 in its row. Note that the plus-sign icon changes when you click it.
3. When you finish selecting objects, click Back (represented by this icon: <) to return to the create- or edit-model page. A representation of each object appears in the Model Objects section. In it, you can view the attributes of the object.

Modify Selections

Once you have selected objects for a model, you can remove them in either of two ways:

- Open the Select Business Objects page, click on the icon for an object you have selected, and it becomes a plus sign once again. When you finish modifying selections, click Done.
- Use the representation of an object in the Model Objects section 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 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 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.

Create an Access Point or Entitlement Filter

A filter may specify an access point, and return users who have been assigned that access point. Or a filter may specify an entitlement, and return users who have been assigned any access point included in that entitlement.

To create either type of filter:

1. In the Model Logic section, 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 have added to the model in the Model Objects section. Select Access Point for an access-point filter, or Access Entitlement for 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 Privilege, Role, or User Defined to return access points of the type you select.
   - As you enter search values you can use the percent symbol (%) as a wildcard.

Related Topics
- User-Defined Access Points
Create an Access Condition Filter

A filter may select records in which the values of an attribute satisfy a condition. A model may contain any number of these condition filters. The access-point and entitlement filters in a model define a pool of records subject to access analysis: all records involving the access points they specify. Condition filters reduce this pool, selecting records from it and therefore excluding records they don't select.

For example:

- A model may contain a single condition filter that states, "Department equals Marketing." By selecting records involving the Marketing department, it excludes all other departments from analysis.
- Conversely, the filter might state, "Department does not equal Marketing." It selects records involving all other departments, and so excludes the Marketing department from analysis.

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. For example, the condition filter "Department equals Marketing" would, by itself, exclude all other departments, among them Sales. But if you were to create a second condition filter, "Department equals Sales," the model would evaluate records involving both the Marketing and Sales departments.

A second type of condition filter uses a "Within Same" attribute to select records of access assignments only within, or only across, entities such as business units. It too would exclude the records it doesn't select from analysis by its model. For example:

- A filter may state, "Within Same Business Unit equals Yes." It would select records of access assignments solely within individual business units. It would exclude records of access granted across units: one conflicting access point granted in, say, a Database Servers unit and a second granted in a 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 section, 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 have added to the model in the Model Objects section. Select the Access Condition object.
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 does not, match a value you select in the Value field. For example (as described above), "Department equals Marketing" selects the Marketing department for analysis, and so excludes other departments.
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 user called Payables Super User for analysis, as well as other users whose names contain the string "Super," but excludes users whose names don't include this string.

- **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, "Country matches none of France or Germany" excludes those countries from analysis by selecting all other countries.

**Related Topics**
- **Global Conditions**

### 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.
Exclusions Involving Procurement Agents

For certain privileges to grant functional access, a user must be granted both the privilege and a corresponding "action" as a "procurement agent" for a business unit. For example, suppose a user is assigned a role that includes the Create Purchase Agreement privilege. That user can actually create purchase agreements within a business unit only if he or she is also a procurement agent for that unit and is granted the Manage Purchase Agreements action. If not, then even though granted the Create Purchase Agreement privilege, that user can’t create purchase agreements.

**Note:** Use the Manage Procurement Agents task in Cloud Setup and Administration to set up users as procurement agents and assign them actions.

Models created in Advanced Access Controls automatically exclude users who are granted any of these privileges but aren’t also granted the corresponding procurement-agent action. This prevents the models from returning false-positive results. You don’t need to create conditions to exclude these users.

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:

<table>
<thead>
<tr>
<th>Functional Privilege</th>
<th>Procurement-Agent Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Purchase Agreement</td>
<td>Manage Purchase Agreements</td>
</tr>
<tr>
<td>PO_CREATE_PURCHASE_AGREEMENT_PRIV</td>
<td></td>
</tr>
<tr>
<td>Import Blanket Purchase Agreement</td>
<td>Manage Purchase Agreements</td>
</tr>
<tr>
<td>PO_IMPORT_BLANKET_PURCHASE_AGREEMENT_PRIV</td>
<td></td>
</tr>
<tr>
<td>Import Contract Purchase Agreement</td>
<td>Manage Purchase Agreements</td>
</tr>
<tr>
<td>PO_IMPORT_CONTRACT_PURCHASE_AGREEMENT_PRIV</td>
<td></td>
</tr>
<tr>
<td>Change Purchase Agreement</td>
<td>Manage Purchase Agreements</td>
</tr>
<tr>
<td>PO_CHANGE_PURCHASE_AGREEMENT_PRIV</td>
<td></td>
</tr>
<tr>
<td>Create Purchase Order</td>
<td>Manage Purchase Orders</td>
</tr>
<tr>
<td>PO_CREATE_PURCHASE_ORDER_PRIV</td>
<td></td>
</tr>
</tbody>
</table>
## Functional Privilege

<table>
<thead>
<tr>
<th>Functional Privilege</th>
<th>Procurement-Agent Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Purchase Order from Requisitions</td>
<td>Manage Purchase Orders</td>
</tr>
<tr>
<td>PO_CREATE_PURCHASE_ORDER_FROM_REQUISITIONS_PRIV</td>
<td></td>
</tr>
<tr>
<td>Import Purchase Order</td>
<td>Manage Purchase Orders</td>
</tr>
<tr>
<td>PO_IMPORT_PURCHASE_ORDER_PRIV</td>
<td></td>
</tr>
<tr>
<td>Change Purchase Order</td>
<td>Manage Purchase Orders</td>
</tr>
<tr>
<td>PO_CHANGE_PURCHASE_ORDER_PRIV</td>
<td></td>
</tr>
<tr>
<td>Maintain Supplier</td>
<td>Manage Suppliers</td>
</tr>
<tr>
<td>POZ_MAINTAIN_SUPPLIER_PRIV</td>
<td></td>
</tr>
<tr>
<td>Maintain Supplier Site</td>
<td>Manage Suppliers</td>
</tr>
<tr>
<td>POZ_MAINTAIN_SUPPLIER_SITES_PRIV</td>
<td></td>
</tr>
<tr>
<td>Edit Supplier Profile Change Request</td>
<td>Manage Suppliers</td>
</tr>
<tr>
<td>POZ_MAINTAIN_SUPPLIER_PROFILE_CHANGE_REQUEST_PRIV</td>
<td></td>
</tr>
<tr>
<td>Edit Supplier Registration Request</td>
<td>Manage Suppliers</td>
</tr>
<tr>
<td>POZ_EDIT_SUPPLIER_REGISTRATION_REQUEST_PRIV</td>
<td></td>
</tr>
</tbody>
</table>

### 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: Filters at the upper level are evaluated first. Filters at the lower level analyze records returned by filters at the upper level. For the model to return results, filters at both levels must evaluate to true.

For example, an access model may contain two filters, one above the other. The upper filter identifies users assigned one access point, and the lower identifies users assigned a second access point. A conflict exists for each user identified by both 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.

You must limit the number of vertical levels:

• If a model contains access-point or entitlement filters at a single level, it performs what's known as 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 vertical levels, access points identified by filters at the first level conflict with access points identified by filters at the second level (as in the examples above).

• For performance reasons, you can't arrange access-point or entitlement filters so that they appear in three or more vertical levels.

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.

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 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. To dissolve a group, select it and click Remove Group.

By default, each group you create is named “Group.” Click the icon at the lower right corner of each group to assign it an individual name.

• You may edit or delete a filter. Right-click on it and select its Edit or Delete option. Or, to edit, you may click on a blue icon at the lower right corner of the filter.

View Access Model Results

From either of the pages you use to create or edit a model, you can also run the model. From either of those pages or from the Models management page, you can view results from the most recent run of the model.
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.
- Or, if global users are configured so that individual global user IDs are associated with more than one actual user, the model run may fall short of the limit.
- The create- or edit-model page includes a check box 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 check box and save the model before running it. If the check box is inactive, you can’t bypass the record limit.

In the page to create or edit a model, you have two results options:

- Run: The model runs, and the page remains open. 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).
- View Existing Results: A results page displays the results generated in the most recent run of the model. This option is available only if the model has been run at least once.

From the Models page, any model that’s been run displays the number of model violations in a Results Count column. Click that number to generate the display of the most recent model results.

**Related Topics**

- **Performance Configuration for Advanced Controls Management**

**Interpret Access Model Results**

An access model returns a grid. Each row is a record of an access-point assignment to a user that the model defines as risky. Results include these values:

- An incident Information column reports the path to the access point that’s the focus of the result record.
- 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.

Other columns are self-explanatory. You may find that some of the columns you want to see are hidden by default. Use the Columns tool 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** check box.
Eliminate False Positives

As you review model results, you may determine that some records are false positives: although they meet the model's risk definition, they don't pose actual segregation-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 Cloud. For example, there is 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 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.

A final word: The two examples, of false positives involving read-only aggregate privileges and those involving role stripes, are only examples. Your models may generate false positives for other reasons. For example, you may create roles that grant read-only access, and you may create models that return those roles in result records. One element of eliminating false positives is to know how to recognize them, which involves taking care as you create roles and models.
Related Topics

- User-Defined Access Points
- Global Conditions
3 Access Model and Control Elements

Overview of Access Model and Control Elements

Access models and controls may make use of elements that are configured separately from the models and controls themselves. These include entitlements, which are sets of related access points; global conditions, which define exemptions from access analysis; and user-defined access points, which trace specific paths to access grants.

In addition, you must establish global user IDs before you can create or run access models or controls.

Related Topics

- Global Users
- Configure Global Users

Entitlements in Access Models and Controls

An entitlement is a set of related access points. 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.

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:
   - If you’re working in the Advanced Controls work area, select Access Entitlements in the Actions menu on the Models page.
   - If you’re an owner working in Access Certifications, select the Access Entitlements tab.

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 and, optionally, a description.
     Consider creating a naming convention to distinguish entitlements created for Access Certification from those created for use with Advanced Access Controls models and controls. A description may explain briefly the organizing principle or business purpose of the entitlement.
   - Select a status, Active or Inactive. Once you create an entitlement, you can't delete it, but you can inactivate it.
   - In a Comments region, review any existing comments or click Add Comments to add a new one.

4. 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.

5. 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.

6. Save the entitlement.

---

Global Conditions

A global condition defines exclusions from access analysis that apply to 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.

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 "Department equals Marketing."
• 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 automatically.

In the pages to create and edit access models, an Access Global Conditions region 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.
• Only one business object provides attributes appropriate for a global condition. That business object, Access Condition, is selected by default. There's no need to select a business object for a global condition.

To create or edit a global condition:

1. In the Access Global Conditions page, either:
   o Select the Create icon.
   o 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:
   o Enter or modify a name and, optionally, a description.
   o Select a status, Active or Inactive. Once you create a global condition, you can't delete it, but you can inactivate it.
3. Create one or more condition filters. The procedure is the same as the one for creating condition filters in access models.
4. Save the global condition.

Related Topics
- Create an Access Condition Filter

User-Defined Access Points

Whether an access point legitimately constitutes an element of a segregation-of-duties conflict may depend on how a user can reach it. For example, a 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.
Thus, rather than include an access point in an access model or control, you may want to include an access path. A user-defined access point is precisely that: a specific path to an access point.

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

**Related Topics**
- Create an Access Point or Entitlement Filter
- Create Path Conditions

**Create or Edit User-Defined Access Points**

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. 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, and the Description parameter uses internal values, to express the path.
3. 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.
4. 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.
5. 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.
6. Click Save and Close.

As you create or edit a user-defined attribute, you can delete an access point you have 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 have 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.
Audit Access Elements

You can use the Oracle Cloud audit framework to track changes to entitlements, global users, and user-defined access points. For example, if access points are added to or removed from an entitlement, you can run a report to see what changed, who changed it, and when.

First, enable auditing for attributes you want to track. To do this, you must be a user with rights to the Setup and Maintenance work area of Oracle Cloud.

1. Open Oracle Cloud Setup and Maintenance. In its Search Tasks field, search for the Manage Audit Policies task. Then select that task in the Tasks list.
2. In the Manage Audit Policies page, locate the row for Oracle Fusion Applications. In its Audit Level field, select Auditing.
3. Click the Configure Business Object Attributes button in that row.
4. In a Configure Business Object Attributes page, select Risks and Controls in the Product field.
5. An Objects region presents a hierarchical list of business objects. Select one that contains attributes you want to track, such as Access Entitlement Access Point.
6. In an Audited Attributes region, click Create (a plus icon). In a Select and Add Audit Attributes dialog, click the check box for each attribute you want to track, for example Access Point Name. Then click OK.
7. When you complete your selections, click Save and Close.

Next, run reports that capture changes made after auditing is enabled. To do this, you must be a user with rights to the Tools work area of Oracle Cloud.

1. Select Navigator > Tools > Audit Reports.
2. In the Search area, select Risks and Controls in the Product field. Also enter a date value in the Date field, for example "Before" and the current date. You may enter other search parameters as well.
3. Click Search. A Search Results area displays records of inserts, updates, and deletions for the attributes you enabled.
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. A business object is, in effect, a set of related data fields from a business application. An attribute is one field within the set. However, other object types are available: An imported object is a set of data imported from an xml file. A system-generated object is data returned by certain transaction filters. A user-defined object is data returned by a specially configured advanced control.

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.
Note: Before you run models, you must run data synchronization, a process that copies data from your Oracle Cloud data source to Risk Management. You can synchronize data as you add a business object to an individual model, or to support all transaction models and controls.

Related Topics
- Synchronize Data

Synchronize Data for an Individual Model

From the Models page, you can select a transaction model and synchronize the data it uses. This process loads data only for business objects that both are used in the selected model and have never been synchronized before. This option enables you to add new objects as you create or edit a model, and then load the data you need for model testing.

1. In the Models grid, select the row for the transaction model whose data you want to update.
2. Select the Synchronize action.
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.

You can instead synchronize all data used by all current transaction models and controls. You would use options available in the Advanced Controls Configurations page of the Setup and Administration work area.

Best Practices for Transaction Model Development

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

- 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.
- A filter may use an Equals condition to arrange records into groups. You may create more than one filter that uses the Equals condition in this way. 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. Place such a filter last (if your model logic permits).
• 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 includes 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

As you create or edit a transaction model, you perform several tasks: You select business objects, which provide data from your Oracle Cloud instance for the model to evaluate. You define filters that select risky records from that data. And you select result values the model is to return for each risky transaction it finds.

You can also select perspective values for the model. These may serve as filtering values in the Models management page. If you create a model, you’re automatically its owner, but you can add other users to the model as owners, editors, or viewers only after you save the model for the first time.

To work with transaction models, select Risk Management in the home page. Among its options, select Advanced Controls. Then select a Models tab; it opens a Models management page that lists the models you have access to.

• To create a model, select Actions > Create Transaction Model in the Models management page. This opens a Create Transaction Model page. Begin by naming and describing the model.

• To edit a model, select its row in the Models management 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
• Select Perspective Values
• Secure Records in Advanced Controls Management

Select Business Objects for a Transaction Model

As you create a model, select one or more business objects for it.

For a transaction model, each business object is a set of related transaction, master-data, setup data, or audit-data fields. Each field within the set is known as an attribute of the object. Select business objects that provide data pertinent to the transaction risk your model is to define. In addition to business objects, you may select imported objects or user-defined objects.

Note: Initially, you have no access to transaction business objects. An administrator must use a Business Object Security feature to assign you the business objects you’re able to use. Business Object Security is available in the Risk Management Data Security work area.
Make Selections
To add objects to a model:

1. Click Add in the Model Objects section of the page to create or edit a model. A Select Business Objects page opens.
2. Search for objects. You can use the Search field to search by name. Or, click Show Filter, then filter the list of objects by name, category, or type.

Each row displays not only the name of an object, but also its category and type. In general, category is a label describing the data an object contains, such as Transaction (records of actual transactions), Operational (master-data records) or Configuration (setup records). Type indicates an activity or product offering that the object supports.
3. Select the objects you want. For each, click the plus sign in its row. Note that the plus-sign icon changes when you click it.
4. When you finish selecting objects, click Back (represented by this icon: <) to return to the create- or edit-model page. A representation of each object appears in the Model Objects section. In it, you can view the attributes of the object.

Modify Selections
Once you have selected objects for a model, you can remove them in either of two ways:

• Open the Select Business Objects page, click on the icon for an object you have selected, and it becomes a plus sign once again. When you finish modifying selections, click Done.
• Use the representation of an object in the Model Objects section 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 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 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.
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 Select Business Objects 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 have typed. You can click on a name to select its object or type. To return to the home page, click All in a bread-crum 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.

**Import 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.
Import-File Format

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 (records of actual transactions), Operational (master-data records), and Configuration (setup records). 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:PM, or MM/DD/YYYY HH:MM:SS (Military Time).

If you refresh an existing imported object, you can:

- Add, edit, or delete rows of values.
- Add columns to the object, providing that you define the column headings as attributes in the Attribute Definitions sheet.
- Change or delete most keys defined in the BO Definitions sheet. You can’t alter BO Key1.
- Modify BO Category values established in the BO Definitions sheet.

You can’t delete columns or update attribute names already existing in columns.

### Dictionary for the Expresses Condition

A transaction filter may contain an Expresses condition. It determines whether text fields in a specified business or imported object contain any term in a dictionary. For this condition to be used, 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.

### Upload an Object File

To upload an object file:

1. Open the Select Business Objects page: As you create or edit a model, click Add in the Model Objects region of the Create Model page or the Edit Model page.
2. Select the Import icon.
3. Click the Browse button. Navigate to, and select, the file you want to import. The file name then populates the File field.
4. 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.

You can delete an imported object if it isn't used in a model or control. Select the x icon in its row in the Select Business Objects page.
Create a Standard Filter

To create a typical standard filter for a transaction model:

1. In the Model Logic section, 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 have added to the model in the Model Objects section. 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, you have 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.

   You have the same options for 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 would select a specific date. For the latter, you would 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 section and select advanced options. You will see only options that apply to the filter you have 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.

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 section, 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.
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.

   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, use only the Matches any of condition, and specify the strings that either should or should not belong together as semicolon-delimited values of that condition. 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 section and select options that refine the attribute-condition formula you have 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.
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 that matches any in a specified set of values, or matches none of them. You may specify only constant, text-string values, delimited by semicolons. The match must be exact.
- **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.
- **Related to**: Establish a join relationship between an attribute of a user-defined object and an attribute of a business, imported, or user-defined object. Specify the attribute of the user-defined 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 object can have only one dynamic join relationship per model.

### 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 Leading and Trailing Spaces**: In principle, this option determines whether leading and trailing spaces are to be ignored in searches for matching text values. In practice, however, these spaces are always ignored regardless of whether you select or clear this option.

- **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.

### 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.

---

**System-Generated Objects**

In transaction models (and controls), a filter that uses the Equals, Similar, or Similar To condition may return records sorted into groups. These records serve as a system-generated object: they may 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 **Payables Invoice 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 would 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 **Payables 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 Payables Invoice Invoice ID is the same. The object contains sets of records; in each, all records have the same invoice ID.
- A second filter states that the Supplier ID attribute of the Payables Invoice 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’t state that an attribute of a business object doesn’t equal itself. A filter can state that an attribute of a system-generated object doesn’t equal itself.

A filter can’t state that an attribute of a business object differs from itself. However, an attribute of a system-generated object can differ from itself, if that object is created by a Similar or Similar To filter.

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.
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 have selected.

To create a pattern filter:

1. In the Model Logic region, 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. For the model to return any results, every vertical level must evaluate to true.

- **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 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. To dissolve a group, select it and click Remove Group.

By default, each group you create is named "Group." Click the icon at the lower right corner of each group to assign it an individual name.

- You may edit or delete a filter. Right-click on it and select its Edit or Delete option. Or, to edit, you may click on a blue icon at the lower right corner of the filter.
- You may 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.

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.

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 Transaction Business Intelligence Enterprise analyses, reports, or dashboards. Such a control may provide amount values that are to be summarized in one of these reporting instruments. If so, position the amount attribute so that it's second among the result attributes. (You would do this as
you create the model that the control is to be based on.) The control may also provide a date related to the payment; if so, position the date attribute so that it's third among the result attributes. Examples of such attributes include Amount and Date in the Payables Invoice business object.

Use the Result Display section 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 models you create in Advanced Financial Controls 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. The audit framework also tracks event types, and therefore so do Advanced Financial Controls audit business objects. These types 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 Advanced Financial Controls version, but you need to enable those you want to use in a model. (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 would do this for each audit model you create or import.

- When you run data synchronization, you update the Advanced Financial Controls 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 Advanced Financial Controls audit 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 region, enter or modify a cutoff date in the Audit Events Created as Of field.

To clarify further, audit-model analysis in Advanced Financial Controls 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 Advanced Financial Controls. Audit data is then available in the Advanced Financial Controls 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, you would 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 the Setup and Maintenance work area of Oracle Cloud.

1. In Advanced Financial Controls, 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 Advanced Financial Controls 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. Open Oracle Cloud Setup and Maintenance. In its Search Tasks field, search for the Manage Audit Policies task. In its Tasks 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 Advanced Financial Controls 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 an Advanced Financial Controls 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. Open the Manage Audit Policies task in Setup and Maintenance.
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 of Advanced Financial Controls.)
4. In an Audit column of the Objects region, select check boxes 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 check boxes 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.

**View Transaction Model Results**

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

In the page to create or edit a model, you have two results options:

- **Run:** The model runs, and the page remains open. 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).
- **View Existing Results:** A results page displays the results generated in the most recent run of the model. This option is available only if the model has been run at least once.

From the Models page, any model that’s been run displays the number of model violations in a Results Count column. Click that number to generate the display of the most recent model results.

**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:

- If a transaction model doesn't include a pattern filter, it returns a grid. Each row is a record of a transaction. That record contains values for the result attributes selected when the model was created or edited. It may also contain Incident Information, Group, and Grouping Value results, which are the same as they would be for an
incident generated by a control. If the results include date values, you can select a Display Time Stamp option to show time values with the dates.

- A pattern transaction model 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 have selected.

Related Topics

- Review Incidents Generated by a Control
5 Advanced Controls

Overview of Advanced Controls

An advanced control typically defines access or transaction risk, and 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, the perspective values and users (associated with those values) who can resolve incidents, 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 management page, which initially lists controls you can access.

Deploy Advanced Controls

You can deploy any number of 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.

Select the Deploy Transaction Controls action or the Deploy Access Controls action in the Controls management page. Enter values in a series of control-deployment pages, selecting Next or Back to navigate among them.

Select Models

On a Deploy Controls: Select Models page, search for and select active models you want to deploy as controls. Search by model name or description. You can review the risk logic for each of the models your search returns: click the Control Logic icon in its row. However, you can’t modify the logic. Select the check box in the row for each model you want to deploy.

Note: If you’re deploying transaction controls, 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.

Set 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.

### Select Perspective Values

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.

### Secure Controls and Their Incidents

In a Deploy Controls: Control Security Assignment page, grant access to the controls you're deploying. Authorize users as owners, editors, or viewers, or select user groups. Then click Next and, in a Deploy Controls: Result Security Assignment page, make a second grant of access to the incidents generated by the controls. Again, authorize users as owners, editors, or viewers, or select user groups.

### Select Worklist Recipients

In a Deploy Controls: Worklist Assignment page, determine which result investigator receives worklist notifications when a control generates incidents. In a Result Investigator field, you may:

- Select Search. A Search and Select Investigator dialog opens, listing users you have 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 worklist notifications, any of the investigators you have selected can work with incidents in Results management pages.
- Select All Eligible Users. All potential investigators receive worklist notifications when a control generates incidents.

### Relate Controls to Financial Reporting Compliance Objects

In a Deploy Controls: Related Records page, relate the advanced controls you're creating to processes, risks, or controls defined in Financial Reporting Compliance.

Once relationships are created:

- In Advanced Controls Management, the page for viewing or editing an advanced control includes a Related Records region. It lists the Financial Reporting Compliance objects you select here. You can click on a related record to view its definition.
- Also in Advanced Controls Management, the page for viewing or editing an incident includes a Related Records region. It lists the 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 Financial Reporting Compliance, the management page for an object may include a Results tab. It displays incidents generated by the advanced controls it's related to. For this tab to appear, you must ensure that the Result option is selected in the Manage Configuration Options page of the Setup and Administration work area.
To create relationships:

1. Select the type of 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 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.

Complete the Controls

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.

Related Topics

- Manage Perspective Mappings
- Select Perspective Values
- Overview of User-Defined Objects
- Reassign Incidents
- Secure Records in Advanced Controls Management

Evaluate Advanced Controls

You can analyze any selection of advanced controls. 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 management 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:

- Evaluate 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

- Synchronize Data
- Configure Global Users
View and Edit Individual Advanced Controls

For each control, you can open a page that displays its full details. Or, you can open an edit version of that page to modify some configuration details, add comments, or revise perspective and worklist-recipient assignments.

To open a control in view mode, click its name in the Controls management 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 management 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 the assignments of users to the control or the incidents it generates. Or you can view those assignments if you’re an editor or viewer.
- 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 section 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 check box 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 check box is labeled, "Before this control runs, also run the user-defined objects that supply it with data."

This section 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 sections 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 section 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.
- A Related Records section displays Financial Reporting Compliance processes, risks, and controls that are related to the advanced control. (Incidents generated by the advanced control are associated with these Financial Reporting Compliance objects.) In the edit-mode page, you can add or remove Financial Reporting Compliance objects as you would if you were deploying a control.

Related Topics

- Select Perspective Values
Delete Advanced Controls

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, and related records.

1. Select the controls you want to modify on the Controls management 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.
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 perspectives section, 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.
   - In a Related Records section, select Financial Reporting Compliance objects to be added to, or removed from, those already selected for each control you're editing. These objects may be processes, risks, or controls. Incidents generated by each advanced control are associated with its Financial Reporting Compliance objects.
4. To complete the edits, click the Submit button.

Related Topics

- Select Perspective Values
- Attach Documents to Controls and Incidents
6 Results

Overview of Advanced Control Results

An incident is a record of a grant of access or a transaction 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 other investigators assign them to you.

The actual resolution of incidents occurs outside of Advanced Controls Management. 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 segregation-of-duties conflict. In Advanced Controls Management, you can:

- Review the details of incidents assigned to you.
- Set the status of those incidents to reflect whether anything should be, or has been, done about them.
- Reassign them to other incident reviewers.

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 that initially lists 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

Initially, incidents are set to an Assigned status, which means that result investigators have been designated to address them. If you’re one of the result investigators, you can update an Assigned incident to any of the following statuses:

- Accepted means you have determined that nothing need be done to resolve the incident.
- Remediate means you have decided that some action must be taken to resolve the incident.
- Resolved means you have confirmed that the remedial action has been carried out.

Advanced Controls Management may set other statuses:

- Control Inactive means that an incident is no longer of concern because the control that generated it has been inactivated.
- Closed means an incident has been resolved in the business application, so a subsequent evaluation of controls finds the incident need no longer be addressed.

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.

An incident may be closed, but later reintroduced. In that case, a new incident isn't generated. Instead, the status of the original incident is reset to Assigned, and its state is reset to In Investigation.

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 would typically select the Name and Results 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 have been authorized to see. The heading for this page is the word "Results" followed by the control name.

Related Topics

- Filter Model, Control, and Result Lists
- View and Edit Individual Advanced Controls

Review Incidents Generated by a Control

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

The following are among the values displayed for each incident:

- Result ID: 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 the incident, then click Edit to go directly to the edit page for the incident.)
- For a transaction control, values for the attributes that characterize the incident. These are results attributes selected for the model that served as the source for the control that generated the incident.
- Incident Information:
  - For an access incident, the path that grants a particular user rights to an access point. The control has identified this access point as inherently risky or has defined a conflict between it and other access points.
  - For a transaction incident, the value of the first attribute among those selected to characterize the suspect transaction.
• Group and Grouping Value:
  o For an access incident, Group identifies one or more access points the control has defined as conflicting with the incident information access point. The Grouping Value field is always blank for access-control results.
  o For transaction incidents, results vary:
    A filter in a control 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 filter reports the business object and attribute. The Grouping Value field reports the common value of this attribute.
    A filter in a control 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 in a control 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.

• Attachments: Links to documents or URLs attached to the incident, if any attachments exist. Click a link to view its attachment. (You add attachments to an incident in the page that opens from the Result ID link. You can't add attachments in this page.)

Other columns are self-explanatory. You may find that some of the columns you want to see are hidden by default. Use the Columns tool 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.

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** check box.

**Related Topics**

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

### View and Edit Individual Incidents

For each incident, you can open a page that displays its full details. Or, you can open an edit version of that page and set the incident's status, write comments, reassign the incident to other users, or add attachments.

From the Results by Control Summary page, click the Results Count value for a control to open the Results page specific to it. In that list of incidents, click the Result ID value for one of these incidents to open its view-only page. To open an incident in edit mode:

• In the incident list, select the row representing an incident, then select the Edit icon.
• 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.
  
  o In the Details section, view details that define the incident. You can't edit these values.
  
  o In the Result Perspective Assignment section, view the current perspective assignments that apply to the incident. In edit mode, you can modify these values
  
  o In the Worklist Assignment section, 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.
  
  o In the Related Records section, view Financial Reporting Compliance objects related to this incident. These relationships are indirect. Financial Reporting Compliance 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 have selected. You can't edit these records, nor modify the selection of Financial Reporting Compliance objects at the incident level.

Related Topics
• Attach Documents to Controls and Incidents
• Secure Records in Advanced Controls Management

Reassign Incidents

To resolve an incident, you must be its owner or editor, and so have authorization to edit its record (reset its status). Only an owner of an incident can modify the selection of users who serve as its owners and editors, so only an owner can reassign an incident to a new selection of investigators. 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 Results

You can modify certain settings for multiple incidents at once. These settings include status, comments, perspective assignments, and worklist assignments.

1. Generate a list of incidents: Locate a control in the Results by Control Summary page, then select the Results Count value for that control.
2. Select from the list. You may work with your complete list of incidents or set search parameters to filter it. In either case, you can:
   - Select a continuous set of incidents. Click the first incident, hold down the Shift key, and click the last.
   - Select a discontinuous set. Hold down the Ctrl key as you click incidents.
3. Select Edit.
4. 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 section, select perspective values to be added to, or removed from, values already selected for each of the incidents you’re working with.
   - In the Worklist Assignment region, select a user, or all eligible users, to receive worklist notifications concerning the incidents.
5. Select Submit.

Related Topics

- Attach Documents to Controls and Incidents
7 Visualizations and Simulations

Overview of Visualizations and Simulations

As an aid in resolving access incidents, you may create visualizations. These are graphic depictions of paths that lead from users to the roles they’re assigned and ultimately to conflicting access points. You may also create simulations, which 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 have no application 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. You reach 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.

1. 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.
2. Click the Visualize icon.

Node Labels

You can enlarge or reduce a visualization, either by expanding or collapsing nodes or by zooming 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, and P for 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.

Nodes for each type of item are depicted in a distinct shape and color, so that item types are easily distinguished.

Expand or Collapse Nodes
To expand a node is to reveal roles, privileges, or users it connects to. To collapse a node is to hide those items. To perform these actions:

1. Select a node and right-click.
2. Select one of these options:
   - Expand reveals nodes with direct connections to the selected node, and Collapse hides those nodes.
   - Expand All reveals all generations of connecting nodes, and Collapse All hides those nodes.

Alternatively, double-click a collapsed node to expand it, or an expanded node to collapse it.

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. (Nodes that you have expanded remain expanded.)
• 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.

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.

Use Path Filters
Click a node in the visualization and click Apply Path Filter to have the result page for the model or control display rows only for results that involve the user, role, or privilege whose node you selected.
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 management 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 management 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 region 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 region, 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 you 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 Done. You’re returned to the Create Access Simulation page, and each pair of access points you have 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 region, 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 region, 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 Count region 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 simulation results.

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.

Edit Simulations

You can edit or rerun simulations. To open a simulation for editing, select its row in the Access Simulations management page, and then select Edit. Or, click the simulation name to open the page that displays details about it, 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.
8 User-Defined Objects

Overview of User-Defined Objects

A user-defined object is a set of data returned by an advanced control that's used as if it were a business object. Each column in the results returned by one of these specially configured controls serves as an attribute of the user-defined object generated from the control.

Either an access control or a transaction control can supply data to a user-defined object. However, only a transaction model (and a control developed from it) can contain filters that cite user-defined objects.

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 as you create it, by selecting an appropriate value for a Result Type field: Incident for a control that generates incidents, or Data set for a control that supplies data to a user-defined object.

A user-defined object has no join relationship to any other object. You must expressly define a relationship between the 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.

Related Topics
- Model Filter Conditions

Create or Edit User-Defined Objects

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. It's listed, along with other user-defined objects, in a User-Defined Objects page. You can open the page from the Actions menu of either the Models or the Controls management page.

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.

You must run the control before you use the object in a transaction model or control. Otherwise, no results are generated. Each time the source control is run, the data available in the user-defined object is refreshed.

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.
   - Domain: By default, the Domain value is Other. You can select a value that characterizes the object, 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 is appropriate for master-data records, and Configuration is appropriate for setup records. These records are expected to change infrequently.
   - Status: By default, the Status is Active. You can change this to Inactive.
3. Save the object.

You may also 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.

User-Defined Object Best Practices

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.
9 Reports

Advanced Controls Reports

You can run the following reports about Advanced Controls Management.

### Advanced Controls Reports

Advanced controls reports include:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions Report</td>
<td>Provides information about both control-specific conditions and global conditions. Control-specific conditions are filters created for models the controls were based on. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Entitlement Report</td>
<td>Lists access points belonging to each in a set of entitlements. This report applies only to Advanced Access Controls.</td>
</tr>
</tbody>
</table>

### Result Reports

Result reports include:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point Report</td>
<td>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. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Access Violations by User Report</td>
<td>Lists ten users with the greatest number of conflicts, the number of conflicts for each, and information about those conflicts. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Access Violations within a Single Role (Intra-Role) Report</td>
<td>Lists roles you can’t assign individually to any user without a conflict occurring, because each role contains privileges that controls define as conflicting. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Intra-Role Violations by Control Report</td>
<td>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. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Global Users Report</td>
<td>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. This report applies only to Advanced Access Controls.</td>
</tr>
<tr>
<td>Report Title</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Result Summary Extract Report</td>
<td>Lists incidents generated by controls, providing summary details for each. This report applies to both Advanced Access Controls and Advanced Financial Controls.</td>
</tr>
<tr>
<td>Result by Control Summary Extract Report</td>
<td>Lists controls that have generated pending incidents, and provides information about each control. This report applies to both Advanced Access Controls and Advanced Financial Controls.</td>
</tr>
<tr>
<td>Users with Access Violations by Control Report</td>
<td>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. This report applies only to Advanced Access Controls.</td>
</tr>
</tbody>
</table>

### Administrative Reports

Administrative reports include:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inaccessible Records Report</td>
<td>Lists data records that can't be accessed by any user, owing to how Risk Management security is defined. This report applies to both Advanced Access Controls and Advanced Financial Controls.</td>
</tr>
<tr>
<td>Pending Worklist Items Report</td>
<td>Displays the outstanding worklist items by user. This report applies to both Advanced Access Controls and Advanced Financial Controls.</td>
</tr>
</tbody>
</table>

### Run Contextual Reports

From each of the Results by Control Summary and Results pages, you can run reports about the items each page lists.

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 fields, select the report you want to run. Also select Excel as its format. This is the only format available for a contextual report. It produces a file for export to Excel.
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.
6. A file-download window offers you options to open or save the export file. If you select Open, the report opens in a Microsoft Excel instance. If you select Save, use a distinct save-as dialog to navigate to the folder where you want to save the file.
Run Reports

You can run reports on demand or schedule them to be run at intervals over a period you define. The reporting management page saves the scheduled reports it generates, enabling you to view them at any time.

1. From the home page, open the springboard for the module whose reports you want to run, Financial Reporting Compliance or Advanced Controls Management. Then select the Reports icon. Or, open the Navigator and select the reporting option for either module.
2. Open the Related Links panel tab and select a category of reports.
3. The reporting management page lists reports belonging to the category you selected. Click in the row for the report you want to run.
4. Click the Run Now action or the Schedule action.
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, you would select among the same values.

For example, a Control Details Report enables you to select among values you would set as you work with Financial Reporting Compliance controls. You can filter by name; select controls with specific method, frequency, or stratification values; designate controls associated with particular perspective 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 management 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 check box to make the set of parameters available, or hide it, in the Select Saved Report Parameters field.
- Select or clear a Default Report Parameter check box 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 management 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

Provisioning Rules

You can create provisioning rules, which identify roles that you consider to conflict with one another. You can use their results to prevent the assignment of Oracle Cloud roles to users in risky combinations. For each rule, you can also select a risk level: High, Medium, or Low. You use your judgment to select roles for each rule. This enables you to focus on risks that are important to you.

You can use these rules in two ways:

- As you create or edit a role in the Security Console, you can evaluate provisioning rules in a Segregation 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.

Provisioning rules operate entirely separately from, but may complement, the rigorous segregation-of-duties analysis performed by access models and controls. It’s recommended that you use both provisioning rules and model- and control-based analysis to mitigate access risk.

Create or Edit Provisioning Rules

To create or edit provisioning rules:

1. In the Advanced Controls work area, click the Provisioning Rules tab.
2. In the Provisioning Rules page, click Add. Or, locate the row defining a rule you want to edit, and select its Edit option.
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 Save.

Once the rule is saved, you can repeat the process to create new rules. Or, use a list field to select among options to edit or delete the rule, or view information about its creation and updates. You can also sort rules by risk level, Role values, or Conflicts With values.

Use REST APIs to Evaluate Rules

To build an application that evaluates provisioning rules as you assign roles to users, use a runUserRoleCheck method, which is available in the Provisioning Rules REST API.

- Your application would pass in a user name and the names of roles requested for that user.
• The API returns the user name and the requested roles, and identifies already-assigned or requested roles that rules define as conflicting with a requested role. Or, if no rules were violated, it 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 in which you supply basic information, define function security policies and data security policies, define a role hierarchy, and assign the role to users. In between the role-hierarchy and role-assignment stops, there is now a Segregation of Duties stop.

To use it, you must first enable it: In Setup and Maintenance, 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.

SOD analysis and all other aspects of the role-creation process are covered in a guide titled Securing Risk Management.

Related Topics

• Create Risk Management Roles in the Security Console
Glossary

access point
A role or privilege that enables users to work with data in a business application. In an access model, a filter may select an access point and return users assigned that access point. In an access certification, a filter may select an access point and return assignable roles that are its hierarchical parents.

attribute
An individual field within a business object.

business object
A set of related fields in a data source subject to models and controls created in Advanced Controls Management. While creating a model, a user selects one or more business objects that supply data for evaluation.

condition
An operator for use in risk-definition formulas contained in model filters. As you create a model filter, you select from a set of predefined conditions.

condition filter
An Advanced Access Controls filter that defines an exclusion from analysis. It may exclude records from analysis by an access model or control, if it appears in that object. It may exclude records from analysis by all access models or controls if it appears in a global condition. Or it may exclude records from an access certification if it appears among the certification's scoping filters.

data source
The supplier of data to business objects cited in models and controls created in Advanced Controls Management. For most business objects, this is your Oracle Cloud instance. However, an Internal data source corresponds to the Advanced Controls Management instance in which you're working, and supplies data to business objects such as User and Access Entitlement. Imported Business Object is a data source name that applies to business objects imported in .xml files.

data synchronization
A process to copy transaction data from a business application to Advanced Financial Controls, for analysis by models and controls. A standard synchronization involves only records that have been newly created or updated since the previous synchronization. Data synchronization doesn't apply to Advanced Access Controls.

entitlement
A set of related access points. In an access model, one type of filter selects an entitlement and returns users assigned any access point in that entitlement. In a scoping job for an access certification, one type of filter selects an entitlement and returns every assignable role that's a parent of an access point in the entitlement.
**function filter**
An element of a model or advanced control that specifies an attribute of a business object, applies a function to groups of attribute values, then determines whether values calculated by the function satisfy a condition. For example: Group records by supplier, calculate the average payment amount for each supplier, and select records for which the average amount exceeds a threshold.

**global condition**
A set of filters that define exclusions from access analysis. These exclusions apply to all access models and controls. Global conditions don't apply to transaction models and controls.

**global user**
An identifier assigned to each user of business applications subject to models and controls created in Advanced Controls Management. It correlates to potentially varying identifiers each person may have for business-application accounts. Global user IDs apply only to Advanced Controls Management, not to Financial Reporting Compliance.

**imported object**
A specialized type of business object, consisting of data imported from a file for analysis by transaction models and advanced controls. Access models and controls don't use imported objects.

**incident**
A record of a transaction or access assignment that's exceeded the risk defined by an advanced control.

**panel tab**
A tab that provides supplemental information or functionality for the page. Each panel tab is on the right side of the page, has an icon as the tab label, and slides out when you open the tab.

**pattern filter**
An element of a transaction model that applies any in a predefined set of statistical operators to the values of an attribute. Most pattern filters return both graphic and tabular results. Pattern filters that return graphic results are for use in models, but not controls.

**perspective hierarchy**
A set of related, hierarchically organized values. You assign perspective values to Risk Management objects to define a context they exist in. In Financial Reporting Compliance, these objects include processes, risks, and controls. In Advanced Controls Management, objects include models, advanced controls, and incidents. These can serve as filtering values.

**simulation**
A preview of the effects of changes you may make to your security model to resolve incidents identified by access controls.
standard filter
An element of a model or advanced control that specifies an attribute of a business object, defines a condition, and selects records in which attribute values satisfy that condition. For example: Payment Amount (an attribute of the Payment business object) is greater than 5,000 dollars.

system-generated object
Data organized into groups by a model or control filter. Within that model or control, the data may be used as a business object in a subsequent filters.

user-defined access point
A specific path to a role or privilege. You may select that path as an access point in an access model. Whether the role or privilege is involved in access conflicts therefore depends on how the user can reach it.

user-defined object
A specialized type of business object, consisting of data returned by a specially configured advanced control, for analysis by models or other advanced controls. Either an access or transaction control may provide data to a user-defined object, but only a transaction model or control can call a user-defined object.

visualization
A graphic depiction of paths by which users gain access to roles or privileges identified in incidents generated by access models or controls.