How to create a Query definition

DEPRECTAED as at v2.0

Queries in Open-AudIT are created in XML format. Examples can be found under the code_igniter/application/controllers/reports directory. These are the Queries that appear when the menu item Admin -> Queries -> Activate Query is chosen.

The XML definition file can be placed in the above directory and activated or copied and pasted into the text box at Admin -> Queries -> Import Query.

When a Query is activated or imported, it's definition is stored in the database. An imported Query is not stored on the filesystem as per the default queries.

Queries can be exported to XML or deleted from the database at Admin -> Queries -> List Queries.

Queries are traditionally run against an individual Group. This way users can run any activated Queries against the Groups they have access to.

A query can be run and displayed on the web page or exported to Excel, CSV, XML, JSON or RSS formats. Only Queries with a timestamp column are available as RSS format.

After reading the below, the best way to create your own query is to copy one of the existing definition files (at the above location), edit it and importing it. Try and run it against a Group. If you don't get the result you want, you can delete the Query as above, edit the XML and re-import it.

A Queries definition consists of two major sections - the details and column sections. Details is primarily concerned with retrieveing the data from the database where as the columns section concentrates on the format of the gathered data to be displayed.

The ***details section*** consists of the following values:

report_name - Quite self explanatory. This should be unique as if two queries with the same name are activated, the program will work but they will be indistinguishable in the application menu.

report_display_in_menu - Most queries will want this set to "y". A few queries are designed to be called from other queries, not directly. Examples of these queries are the Specific Software, Specific Key, Specific Server, etc.

report_sql - This is the SQL statement that is used to query the database. The attribute @group should be used so the Query is run against the particular Group in question as opposed to every item in the database (negating the User / Group / Permission security model). There is scope within the application to pass two additional parameters. These should be inserted into the SQL as a ?. The application will automatically escape the string and pass it to the query when the Query is run.

report_display_sql - This is not used for Queries. It is used for Groups. The Query and Group definitions use compatible XML files so this is simply to ensure the same attributes are present in both.

report_view_file - Some Queries may have a format that doesn't fit with the standard column data view. If you need something specific you can create your own "view" file in code_igniter/application/views/theme-tango/ and this file will be called with the data.

report_view_file_contents - Not used at present.

report_processing - Not used at present.

report_sort_column - The initial column to sort the data by. Regardless of the sort specified in the SQL statement (if any), this parameter is passed to the javascript in the web page which then sorts the output.

The ***columns section*** contains an entry for each column to be displayed in the query. The attributes are:

column_order - On the web page from left to right, which position to display this column in. I generally stick to keeping the XML columns in the XML file in the same order as I wish to see them displayed.

column_name - The header name for the column. Free form text not related to the actual attribute name.

column_variable - The attribute as selcted in the SQL statement.

column_table - If multiple tables are selected in SQL, the table from which the attribute comes from.

column_type - The type of data to be displayed in the column. This will affect the format as outputted to the web page. Valid formats are: link, image, ip_address, text, timestamp, url. These values will affect the column display thus:

- link - a link to a web page within the application is created using the value in the column_link attribute. The value in the column_secondary attribute is appended to the previous value. This is how we display a link to a System Details page (for example).
- image - The value of the column_variable attribute is used to populate the image source. It will be formatted thus - /theme-<theme>/<theme>-images/16_<column_variable>.png where <theme> is the user theme (this is "tango" by default).
- ip_address - IP Addresses are stored with padded 0's in the database to facilitate sorting. When presented in a Query, a hidden SPAN is created that contains the padded ip address, then the unpadded ip address is displayed. The javascript table sorter will then sort in correct order.
- timestamp - a date formatted field.
- url - A link to an external web page. The href attribute of the URL will contain the software_url variable and (if populated) the value of the attribute specified in the column_secondary attribute. If populated, the text of column_ternary attribute will be used to create an image as per the above column_image type.
- column_link - Used when column_type = link or url. When link, the path that is added to the base url of the application. When url, the text is used as the actual URL.

column_secondary - Used when column type = link, image or url. when link, append the value of the attribute to the href. When image, used as the image title and alt test. When url, append the value of the attribute to the href.

column_ternary - Used when column_type = url. Use as the filename for the image displayed as the link. Prepend /theme-tango/tango-images/16_ and append .png to this value.

column_align - The alignment of the data within the column. If not specified will default to left.

The default oa_group_columns are as below:

column_id	group_id	column_order	column_name	column_variable	column_type	column_link	column_secondary	column_ternary
1	0	1	Hostname	hostname	link	main/system_display/	system_id	
2	0	2	Description	man_description	text			
3	0	3	IP Address	man_ip_address	ip_address			
4	0	4	Type	man_icon	image		man_os_family	
5	0	5	OS / Device	man_os_name	text			
6	0	6	Tags	tag	text			

The columns for the "Installed Software" query are below:

column_id	group_id	column_order	column_name	column_variable	column_type	column_link	column_secondary	column_ternary
7	14	0	Package Name	software_name	link	/report /specific_software /$group_id/	software_id	
8	14	1	Type	software_comment	text			
9	14	2	Installs	software_count	text			
10	14	3	Contact	software_url	url			
11	14	4	Version	software_version	text			
12	14	5	Publisher	software_publisher	text			
13	14	6	Google Search		url	https://encrypted.google.com/search?q=	software_name	google