Report Audit and Tracking

Overview

Yellowfin has a complete audit facility for tracking which users are accessing data from your data sources. Each time a report is run, a unique instance of that report definition and timestamp is saved.

As an administrator you will be able to run reports against the Yellowfin database to determine your usage statistics and track access to specific data sources and views.

Should we maintain unique user logins?

For security and audit purposes, it is vital that each user be given unique access logons to the system. If users use shared accounts, your ability as an administrator to manage security and audit reporting use will be compromised.

What data is stored in the report audit?

Each time a report is run a record is created that stores the details of that report.

Item	Description
Reader's User ID	Which user accessed the report
Report ID	Unique instance of a report definition
SQL Statement*	The SQL that was generated and passed to the database
Time Stamp	When the report was run
Duration	How long did the query take
Number of Rows Returned	How many rows were returned
Source System Accessed *	Which source system was accessed
View Accessed *	Which view was accessed as part of the query

*Derived fields

By accessing the administration view and reporting your usage statistics, you will be able to track and audit all users' access to the application and your public data.

Using prebuilt content

Get the free "Audit Content" file from Yellowfin's Github and upload it to your instance through the Import module, for a quick means of analyzing your system usage by using already generated reports and dashboards.