Audit Logging

Intellicus Enterprise Reporting and BI Platform

intellicus
Enterprise Reporting and
Business Insights Platform

info@intellicus.com
www.intellicus.com

Dated: - September 2010.

Acknowledgements

Intellicus acknowledges using of third-party libraries to extend support to the functionalities that they provide.

For details, visit: http://www.intellicus.com/acknowledgements.htm .

Contents

Audit logging

Audit logs lets you monitor the reporting activities taking place in Intellicus by enabling you to get a list of reports generated in Intellicus by different users and view the report outputs.

Configuring Audit Log functionality

To enable Audit Log functionality, set report server property **Audit Log** to *Enable*. To set this property, you need to navigate to Navigation > Administration > Configure > Server.

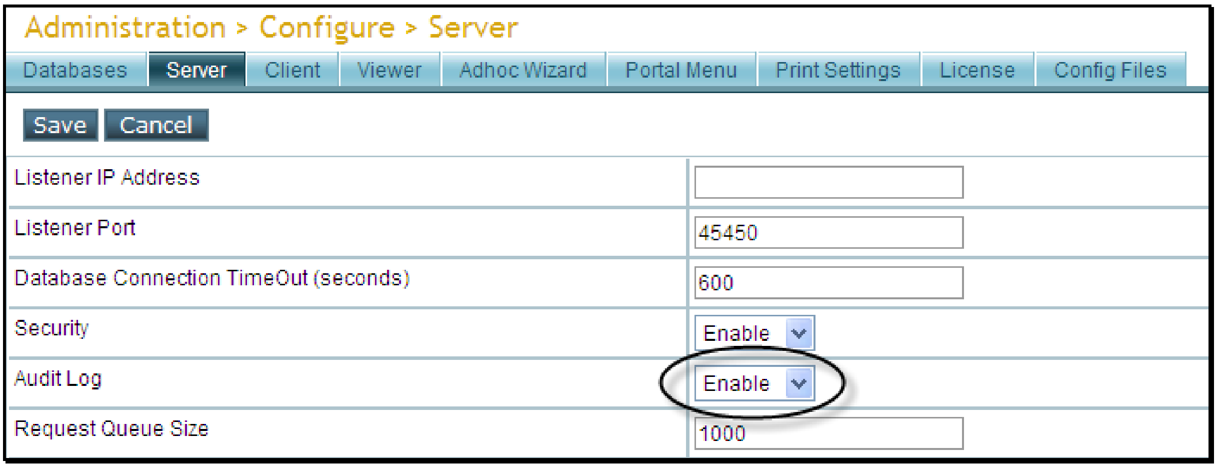

Figure 1: Audit Log server property

By default, Audit log is *Disable*.

When audit log is enabled, Intellicus starts saving report's audit related information in repository.

Number of days for which this information should be maintained is set in a report server property **Audit Log Purge Time**. For example, to maintain audit details for 45 days, set 45 as property value. By default it is 30 (days).

When a user generates an Intellicus report, intermediate report files (known as RPG files), are created and stored at server. When you view snapshot of a report, report is generated from its RPG file. The duration for which RPG files can be retained (so that report's snapshot can be viewed) depends on value set in a report server property **Audit RPG Purge Time**. By default it is 7 days.

If **Audit Log Purge Time** is less than **Audit RPG Purge Time**, then all audit information will be deleted as per **Audit Log Purge Time**, but RPG file will not be purged.

When an RPG will be purged?

Purging of an RPG file depends on many server properties. For example, if value of **Audit RPG Purge Time** is 7 days, but if that report is published for "ever", such an RPG will never be purged. However, this file will not be available for audit after corresponding log purge time is over.

Viewing Audit log

To get a list of reports that were generated within a date range go to Audit Log page. Click **Navigation** > **Administration > Monitor > Audit Log**.

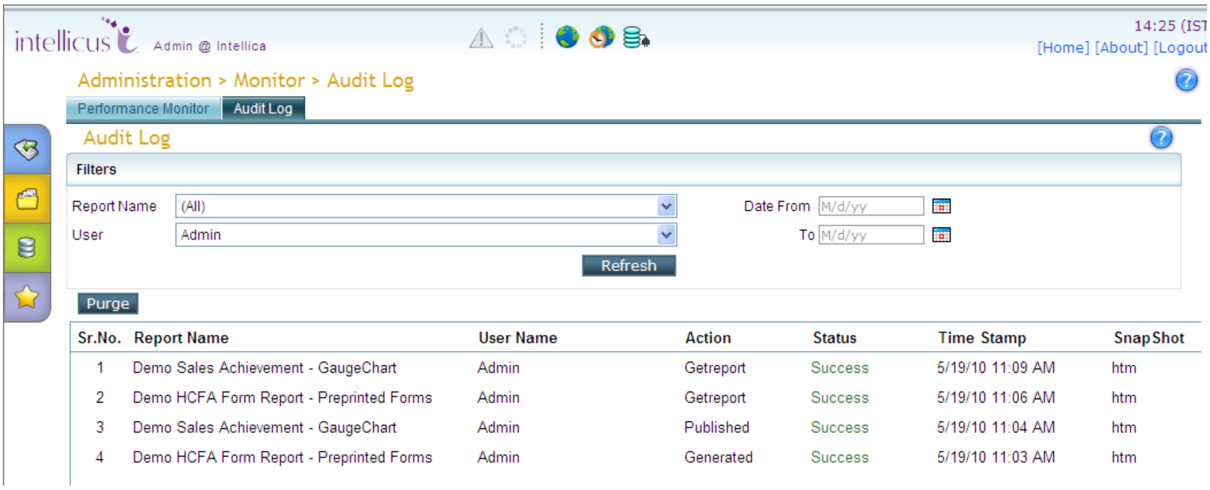

Figure 2: Audit Log tab on Monitor page

To get a log of reports generated,

1. To select a specific report select its name, or **All** to list all the reports.
2. Select **User** (to get reports requested by a specific user) or select **All** to list reports requested by all the users.
3. Optionally, specify Date range in **Date from** and **Date To**.
4. Click **Refresh**.

All the reports generated that meets the specified criteria will be listed. For each report, following detail is listed:

- Report Name
- User Name
- Action
- Status
- Time Stamp
- Snapshot

To view Snapshot or a report

Each row in the table represents one report.

1. Click the link in the **Snapshot** column of the row. The link indicates the output type.
2. In **View Options** dialog, select options for the snap shot.
3. Click **OK** to proceed.

To purge the log

Click **Purge** button to delete audit log information.