Audit Logging

Version: 18.1

intellicus

Dated: November 2018

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

1 Audit logging

Intellicus keeps audit logs for system administration, monitoring, problem solving, and auditing purposes. Audit logs lets you monitor the reporting activities taking place in Intellicus by enabling you to get a list of reports generated 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 Navigate > Administration > Configure > Server > Compliance.

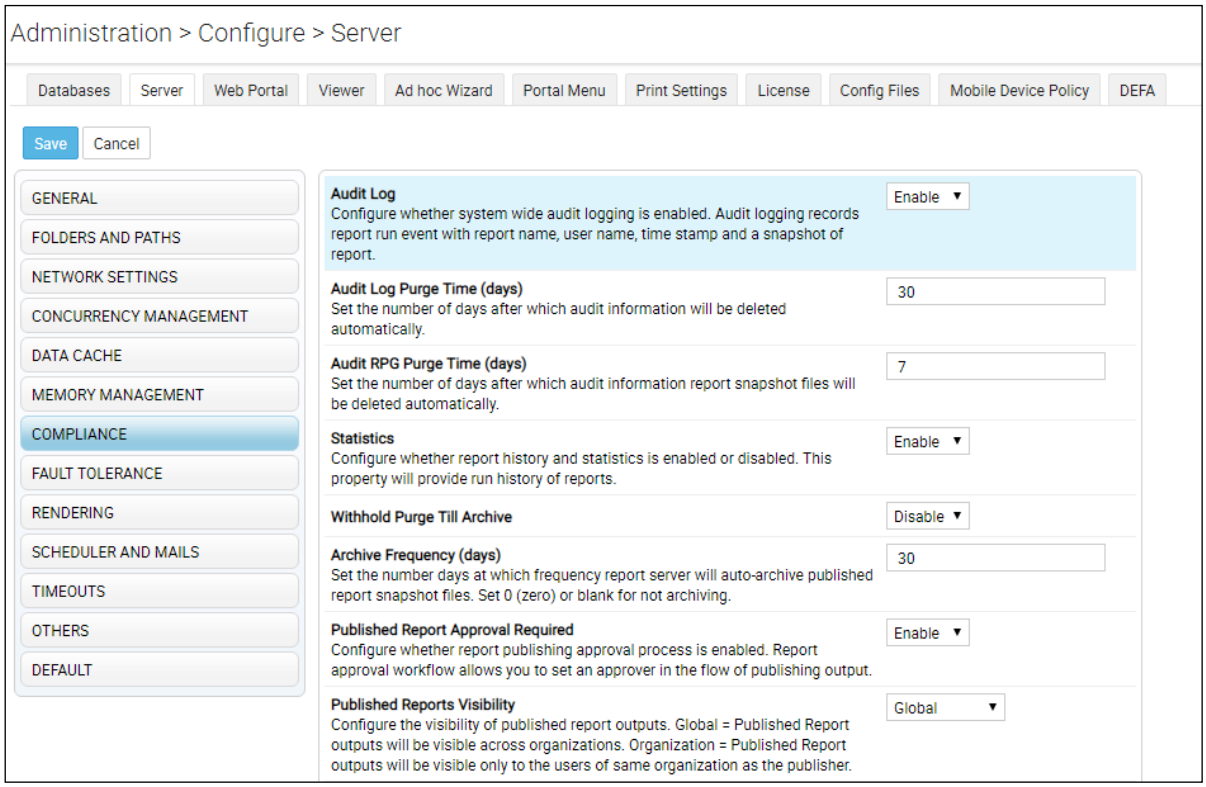

Figure 1: Audit Log server property

By default, audit log is disabled.

When audit log is enabled, Intellicus starts saving report's audit related information in repository with report name, user name, time stamp and a snapshot of report.

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 forever, 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 Logs

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

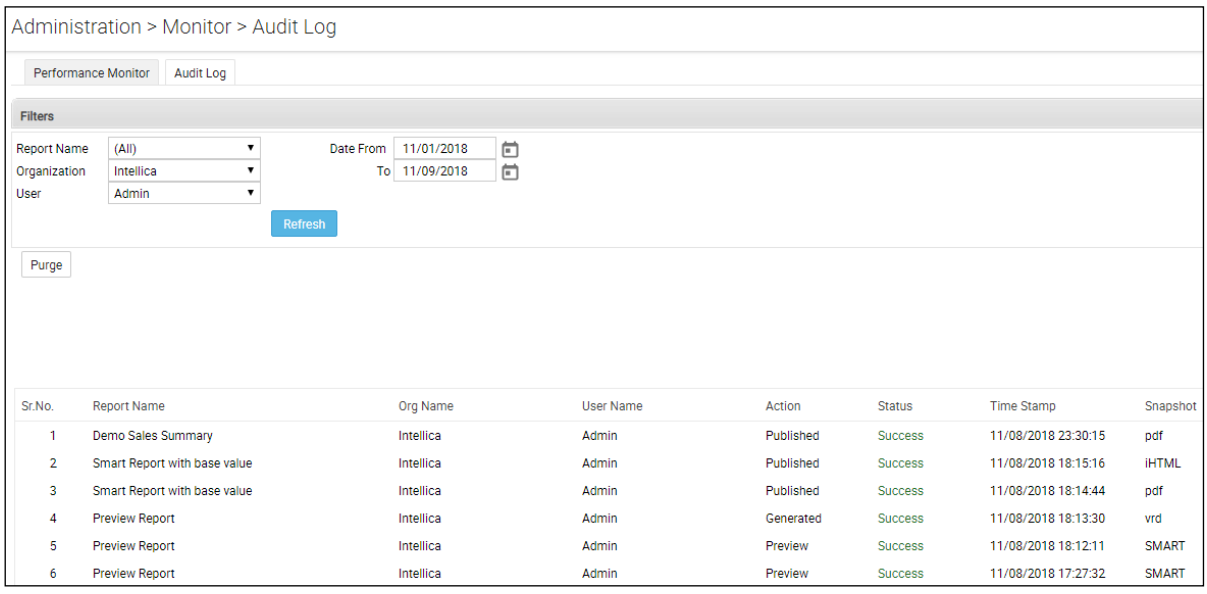

Figure 2: Audit Log tab on Monitor page

To get a log of reports generated,

1. To select a specific report, select its name under **Report Name**, or select **All** to list all the reports.
2. Select **Organization** and **User** (to get reports available to a specific organization/user) or select **All** to list reports available to all the organizations/users.
3. Optionally, specify date range in **Date From** and **To** for the time when reports were executed.
4. Click **Refresh**.

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

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

To view snapshot of a report

Each row in the table as shown in Figure 2 represents a report.

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

You can view the instance of the report when it got executed.

To purge the logs

Click **Purge** below the Refresh button to delete the audit log information. All the records listed on the Audit Log page will be deleted.