

Explore Activity - Database Summary tab

The IDERA SQL Compliance Manager Database Summary tab displays the status of audit activity for a particular database hosted by the selected SQL Server instance. Use the statistics and graphs on this tab to quickly and easily identify database-level issues so you can continue to ensure the correct level of compliance.

Understanding Event Distribution

The Event Distribution pane tracks the distribution of audited activity during the selected time span. This pie chart displays how recently collected events are distributed across the commonly audited event categories. You can mouse-over a slice of the pie to see the exact number of events in this category and the percentage of total events this category represents. To verify which event categories you are auditing, see the Audited Activity pane.

Understanding Audited Activity

The Audited Activity pane provides a brief summary of the audit settings configured for the selected database. For more detailed information, review the database audit settings (available from the task ribbon).

Regulation Guideline

Lists the regulation guideline(s) applied to this database.

Database

Lists the event categories currently audited on this database. This list includes auditing settings configured at the database level only.

Before-After

Lists which tables are audited for before and after data.

Sensitive Columns

Lists which tables are audited at the column level for SELECT events.

Trusted Users

Displays the number of trusted users that are excluded from the audit trail.

Event Filters

Displays the number of Event Filters that are created to streamline audit data collected from this database, and the event properties used by these filters. Events that match the listed properties are omitted from the audit data trail for this database.

Understanding Recent Database Activity

The Recent Database Activity pane tracks the level of activity during the selected time span. This graph plots the number of recently collected audit events per the commonly audited event categories.

Understanding Recent Audit Events

The Recent Audit Events pane lists the most recent audit events collected for this database during the specified time span. This list displays up to 100 events. To see more details about a specific event, double-click the listed event. To view all audited events collected since your last archive, use the Audit Events tab.

Available actions

Configure Alerting

Opens the Alert Rules tab under Administration, allowing you to configure alerting to track specific activity on this database or other SQL Server instances across your environment.

Configure Event Filters

Opens the Event Filters tab under Administration, allowing you to configure Event Filters that exclude specific types of events from your audit trail, allowing you to eliminate unnecessary events before they are processed by the Collection Server.

Remove Database

Allows you to unregister the selected SQL Server database(s). When you remove a SQL Server database, SQL Compliance Manager disables all auditing for this specific database on the SQL Server instance. Auditing of other databases on this instance continues.

Disable Auditing

Allows you to disable auditing on the selected SQL Server database. When you disable auditing, the SQL Compliance Manager Agent stops collecting new event data for this database and stops the corresponding SQL trace running against that database. You can continue to view and report on previously audited events or archived events.

Disabling auditing at the database level does not disable auditing at the server level or auditing of other databases hosted on the SQL Server instance.

To re-enable auditing, right-click the database from the Explore Activity tree, and then click **Enable Auditing** on the context menu.

Database Settings

Allows you to change the audit settings for the selected SQL Server database.

Apply Regulation Guideline

Allows you to select one or more regulations to apply to this audited SQL Server database. If you want to apply regulation guidelines to all audited databases on a SQL Server instance, use the **Apply Regulation Guideline** feature from the [Explore Activity - Instance Summary](#) tab.

Trusted Users

Allows you to change which SQL Server logins or roles are considered trusted users on the selected SQL Server database. Logins designated as trusted users are not audited at the database level. All events resulting from trusted user activity are filtered from the audit trail before the trace file is sent to the Collection Server for processing.

Import

Allows you to import audit settings previously exported from another audited instance or database.

Export

Allows you to export audit settings for this SQL Server database to an XML file. This file includes audit settings configured at the database level. You can later use this file to import audit settings across multiple databases, ensuring consistent auditing and compliance on a given instance or throughout your environment.

Span

Allows you to change the number of days (time span) for which the Summary tab displays status, events, and activity. By default, this tab displays data for the last seven days.

SQL Compliance Manager monitor, audit and alert on SQL user activity and data changes.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)