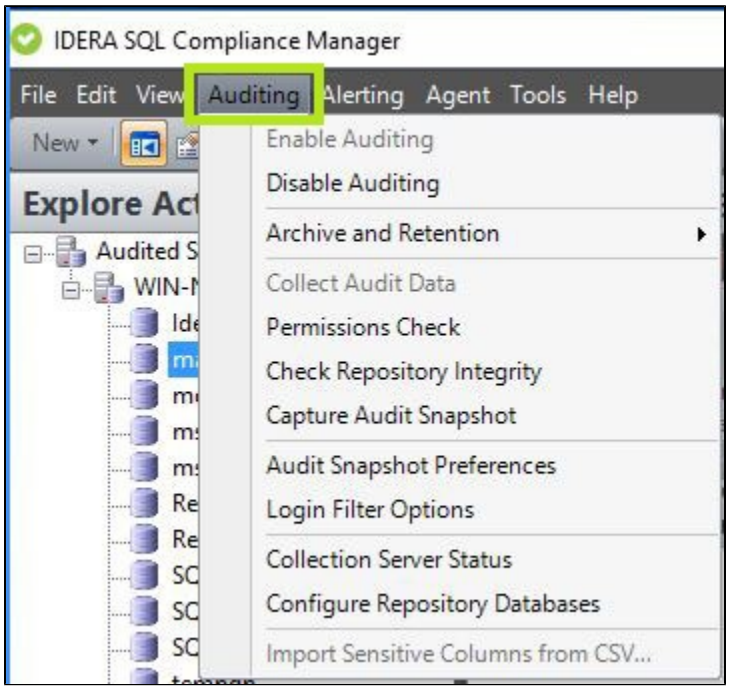
# SQL Compliance Manager Menu - Auditing

The Auditing option from the SQL Compliance Manager Menu allows users to quickly perform various auditing activities, such as to Check the Repository Integrity, Disable Auditing, Capture Snapshots or to Configure Repository Databases. Perform a Permissions Check on your audited databases and registered servers, or quickly configure your Login Filter Options using the SQL Compliance Manager Auditing Menu option.




## Available actions

### Enable Auditing

**Server level -** Auditing is enabled when you register a SQL Server instance, and allows you to capture SQL events at the server level. For more information, see Enable auditing on a SQL Server.

**Database level -** Enabling auditing on the database allows you to capture SQL events at the database level. For more information, see Enable auditing on a database.

### Disable Auditing

**Server level -** You can disable auditing on any registered SQL Server instance and the associated databases. When you disable auditing, IDERA SQL Compliance Manager stops the SQL trace but leaves the trace file directory intact. You can continue reporting on audit data stored in the Repository and archive databases. For more information, see Disable auditing on a SQL Server.

**Database level -** You can disable auditing on any database associated with a registered SQL Server instance. When you disable auditing, IDERA SQL Compliance Manager stops the SQL trace but leaves the trace file directory intact. You can continue reporting on audit data stored in the Repository and archive databases. For more information, see Disable auditing on a database.

### Archive and Retention

**Archive Audit Data Now -** Allows you to archive audit data. Archiving moves the collected audit data from the event database to an archive database for each registered SQL Server you select. If an archive database does not exist for the selected SQL Server instance, the Collection Server creates the archive database. For more information, see Archive Audit Data Now window.

**Groom Audit Data Now -** Allows you to groom audited events currently stored in the Repository databases. Grooming permanently deletes any event that is older than the age limit you specify. For more information, see Groom Audit Data Now window.

**Archive Preferences -** Allows you to set the age at which audited events are archived, configure how the archive databases are partitioned and named, and schedule archiving to run automatically. For more information, see Archive Preferences window.

## Collect Audit Data

Allows you to force the SQL Compliance Manager Agent to send trace files to the Collection Server for processing. Typically, the SQL Compliance Manager Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

## Permissions Check

Displays the results of a check of the permissions required by IDERA SQL Compliance Manager on the SQL Server instance you want to monitor. This check runs automatically each time you register a new instance. For more information, see Permission Check.

## Check Repository Integrity

Allows you to check for unexpected changes in your audit data, detecting when events are modified, added, or deleted by a script or an application other than IDERA SQL Compliance Manager. For more information, see Check Repository Integrity window.

## Capture Audit Snapshot

Allows you to manually capture an audit snapshot for all registered SQL Server instances or a specific instance. This option provides on-demand configuration data for auditing diagnostics. For more information, see Capture Audit Snapshot window.

## Audit Snapshot Preferences

Allows you to indicate whether you want IDERA SQL Compliance Manager to capture a snapshot of your audit settings at a regular interval (days). For more information, see Audit Snapshot Preferences window.

## Login Filter Options

The Login Filtering Options window allows you to set login filtering. Login filtering reduces the number of login events stored in your audit data. For more information, see Login Filtering Options window.

## Collection Server Status

Allows you to review the basic properties and status of the Collection Server. For more information, see Collection Server Properties window.

## Configure Repository Databases

Allows you to select which database recovery model you want the Collection Server to configure when creating databases to store audit data in the Repository. You can also view the status of your Repository databases and update indexes if necessary. For more information, see Configure Repository Databases window.

## Import Sensitive Columns from CSV

Allows you to import a list of sensitive columns from a .csv file to speed the process of configuring your sensitive column auditing. Note that the .csv file must have a row for each database you want to add for sensitive column auditing. For more information, see Import Sensitive Columns window.