

Using SQL Server Audit Logs

Starting IDERA SQL Compliance Manager 6.0 and above, the SQL Compliance Manager default Event Collection method is SQL Server Audit Specifications. Use the SQL Server Audit Logs feature to track specific events occurring in your monitored environment. SQL Server Audit Logs is an event-handling system that helps you reduce the size of data gathered and deliver performance gains over the default SQL trace method. In SQL Compliance Manager 5.5 and later, only SELECT and DML events for SQL Server 2017 and later versions are supported by this feature.



Upon version upgrade or new installation, the SQL Compliance Manager Event Collection method setting changes to "SQL Server Audit Specifications" by default. Users can manually change the collection method.



Before and After Data is not supported on the RDS instance due to the limitation of creating trusted assemblies using SQL script. BAD operations are removed from the properties, reports, alerts, and summary tabs.

To manually change the capturing events method, go to:

- The [Registered SQL Server Properties window - Audited Activities tab](#) in the Windows Management Console.

Prerequisites and conditions for enabling auditing using Audit Logs

IDERA SQL Compliance Manager supports Audit Logs based auditing for SQL Server 2017 and above. The following prerequisites and conditions are required to switch auditing based on Audit Logs.

- While enabling Audit Logs from Web or Windows Management console.
 - SQL Compliance Manager checks for the following conditions, which all must be met to successfully enable Audit Logs:
 - The Agent is reachable.
 - SQL Server 2017 or above.
 - SQL Compliance Agent 5.5 or above.

Enable Audit Logs mode using the Windows Management Console

Users wanting to take advantage of SQL Server Audit Logs auditing capabilities can do so by completing the following steps:

1. Right-click the instance you want to audit and select **Properties**.
2. In the **Registered SQL Server Properties** window, select the **Audited Activities** tab.
3. Under the **Capture DML and Select activities** options, select the **Via SQL Server Audit Specifications** option.
4. Click **OK**.

For more information about enabling this feature using the Windows Management Console, see [Registered SQL Server Properties window - Audited Activities tab](#).