Known issues

IDERA strives to ensure our products provide quality solutions for your SQL Server needs. The following known IDERA SQL Compliance Manager issues are described in this section. If you need further assistance with any issue, please contact Support.

Known issues in version 5.8.1

General issues

- For registered SQL Server 2019 instances, the General tab of the SQL Server Properties window displays the version as Unknown. This is only a visual issue and does not affect auditing or any other functionality.
- During the registration of an AG Listener in the Cluster Configuration Console, when naming the SQL Server instance, the underscore "_" character is not supported.
- The Audit settings Export feature does not export previously configured Server level Trusted Users. To complete the migration add the Trusted Users manually at the Server Level.

Sensitive Column issues

- Events for Sensitive Column audit data are not captured when auditing via Extended Events. When the option to capture SELECT and DML activities is configured at the server-level to capture events via the Extended Events auditing method, and the capture SELECT and DML option is not configured at database-level, but is configured to track SELECT and DML for Sensitive Column auditing. In order to capture and process Sensitive Column events correctly, change the collection method from Extended Events auditing to SQL Server Trace Files auditing.
- When you configure Sensitive Column auditing without first selecting the DML or SELECT option on the Audited Activities tab, then the SQLcompliance Agent has problems creating the **sp_SQLcompliance_AuditXE** stored procedure, and auditing stops working.

Known issues in version 5.8

General issues

- The installation wizard of the Agent service fails when running the audited SQL Server under the Local System account. In order to grant all required permissions successfully, run the **SQLcompliance-x64.exe** installer to perform a manual agent-only installation.
- ***(Fixed in version 5.8.1)*** When performing a migration of the Collection Server, while installing the new Collection Server components, the installer raises an error message that prompts for the removal of the newly restored **SQLcompliance** and **SQLcomplianceProcessing** databases. The installer locates these databases which have been restored for the purpose of the migration, on the server instance which has been designated as the new repository database server during the installation process. Do not proceed with the removal of these databases, instead, contact Support for further assistance with installation or look up the KB Article #00012649 for further instructions, in the Solutions section for the SQL Compliance Manager product in the IDERA Customer Portal.

Known issues in version 5.7.1

General issues

- ***(Fixed in version 5.8.1)*** SQL Compliance Manager presents a security concern due to unnecessary permissions such as ALTER, EXECUTE, CONTROL, TAKE OWNERSHIP, and VIEW DEFINITION, which are granted to Public roles on the audit stored procedures **sp_SQLcompliance_Audit** and **sp_SQLCompliance_StartUp**.
- When adding or editing users from the console, SQL Compliance Manager does not grant access to the Web Console Users and displays the error message "Failed to update Web Application access permission for user".
- ***(Fixed in version 5.8.1)*** SQL Compliance Manager encounters an issue when adding new users to a Windows Domain group that were previously configured as Trusted Users on a particular database. As a result, these changes are not reflected in the audit configuration stored in the .bin audit file nor on the **sp_SQLcompliance_Audit** stored procedure. Users have to manually update the audit settings in the console for the new users to display in the audit configuration.
- An Event Filter configured to exclude all activities recorded on the tables of a database, will not exclude DML and SELECT activities happening on columns that are not configured for Sensitive Column auditing, but which are part of a table with columns configured for Sensitive Column auditing. Event Filters are expected to exclude all activities these are configured to exclude, except DML and SELECT activities happening on columns configured for Sensitive Column auditing. This is by design.

Known issues in version 5.7

General Issues

- ***(Fixed in version 5.8.1)*** When running the console reports and/or the newly SSRS deployed reports, the execution fails with the following syntax error: "Query execution failed for dataset 'ReportOutput'. (rsErrorExecutingCommand) Incorrect syntax near')'.
- ***(Fixed in version 5.7.1)*** When users add a GMSA account as part of a group, SQL CM does not recognize it as a Trusted User. As a workaround, users need to specify the account and the group when configuring Trusted Users and update the audit settings each time a new GMSA account is added to the group.
- ***(Fixed in version 5.7.1)*** When users run the SQLcomplianceClusterSetup.exe to upgrade agent service deployment to 5.6.1, the cluster setup installation does not prompt users to agree to upgrade and instead it performs a fresh installation.
- ***(Fixed in version 5.7.1)*** When registering databases to the Primary node of an audited Availability Group, SQL Compliance Manager is not able to establish a connection with the AG databases on the Secondary nodes. Therefore, these databases do not get automatically register on the Secondary nodes.

In order to register the databases on the Secondary nodes, users have to:

1. Fail over the Availability Group onto the Secondary node, in order to get access to the list of databases.
2. Register the databases on the Secondary node
3. Fail over the AG back to the Primary node.

Known issues in version 5.6.1

General Issues

- ***(Fixed in version 5.7)*** The Daily Audit Activity Statistics Report displays an error message in the SQL CM desktop console when the **ReportViewer.DataVisualization** component is missing. To run the report correctly, close the SQL CM desktop console and install the Report Viewer 2010 program. Once the installation is complete, relaunch the SQL CM desktop console and run the report.

  To download the Report Viewer 2010 controls program follow the link below:
  Report Viewer 2010 Controls

- In SQL Compliance Manager version 5.6.1 the Row count functionality may show as “Not Applicable”. The issue occurs when you execute a large query and during execution the start and the end of the SQL Statement get captured in different trace files. Since both events are located in different trace files, SQL CM is not able to map these events and therefore displays that Row count is “Not Applicable”. Users can increase the time of collection (default is set to 60 seconds) to capture Row count correctly.
- SQL Compliance Manager is currently allowing users to select the Upgrade Agent option, even if the Agent is already in the latest version. Upon selection, SQL CM prompts you to upgrade the agent using the full setup program.
- ***(Fixed in version 5.7.1)*** When you configure Sensitive Column auditing without first selecting the DML or SELECT option on the Audited Activities tab, then the SQLcompliance Agent has problems creating the **sp_SQLcompliance_Audit** stored procedure, and auditing stops working.

Known issues in version 5.6

General issues

- ***(Fixed in version 5.6.1)*** Import Database settings with DML/SELECT filters, flip import settings. When users import database audit settings and apply those settings to multiple databases, the imported settings apply only to some databases. If the user imports and applies the audit settings to the same databases again, the configuration settings get flipped, applying the import settings to the databases it did not apply to before while deleting the settings from the ones it previously applied them to.
- ***(Fixed in version 5.6.1)*** Invalid stored procedures call to sp_SQLcompliance_AuditXE. A message about an invalid stored procedure appears in the SQL Server Logs; "Could not find stored procedure **master.dbo.sp_SQLcompliance_AuditXE**". The error message appears because no stored procedure with the name "**master.dob.sp_SQLcompliance_AuditXE**" exists.
- ***(Fixed in version 5.7)*** SQL Compliance Manager Object Activity Report renders all data on a single page. When the Object Activity Report is run, the report displays all the collected data on a single page.
- ***(Fixed in version 5.6.1)*** SQL Compliance Manager traces are getting collected on the Passive nodes of an Availability Group. When a primary node becomes a secondary node, the Stored Procedure does not get disabled for the secondary node and the trace files keep gathering. This causes an accumulation of trace files on the secondary node.

Follow the steps below for the workaround to stop trace files from generating on the secondary node:

1. Launch Trace Manager from the SQL Compliance Manager Desktop Console. SQLCM Menu-bar>Tools>Trace Manager.
2. Enter the SQL Server Instance name and click the Connect button.

> ⚠ When working on a secondary node of an Availability Group, use the secondary´s instance name.

3. In the SQLcompliance Stored Procedures field, make sure to check the "_" and "_" options.
4. Click the "Drop SQLcompliance Stored Procedures" button.
5. In the Registered Traces field, from the list of running traces, select the entries related to the SQL CM traces.

> ⚠ Use the file path to determine the traces related to SQL CM. Or check the Agent Properties for the audited instances to verify the trace directory file path.

6. Once the desired registered trace is selected, click the Stop button. Select the record again and click the Close button.
7. Repeat steps 5 and 6 for the remaining SQL CM traces.

Known issues in version 5.5.1

Installation and configuration issues

- ***(Fixed in version 5.6)*** Installation or upgrade of SQL Server 2012 native client may cause the system to reboot. When installing or upgrading the version of the native client, once the process is complete, a system reboot occurs without a previous warning.
- IDERA Dashboard 3.0.3 and later does not support SQL Server 2005 SP1. Users should not attempt to install SQL Compliance Manager with IDERA Dashboard 3.0.3 and later on a SQL Server 2005 SP1 as that version of SQL Server is not supported by IDERA Dashboard.

General issues

- Case-sensitivity required when specifying the Repository database name. When specifying the location and name of your Repository database, SQL Compliance Manager requires that you use proper capitalization.
- IDERA SQL Compliance Manager does not capture Linked Server Trace Events for SQL Server 2005. Linked server events are not present in the trace files for SQL Server 2005, therefore linked server events are not captured in IDERA SQL Compliance Manager and no alerts will trigger. Microsoft has ended extended support for this version.
- ***(Fixed in version 5.6)*** Create/Drop index events recorded as "Alter User Table" event. SQL Compliance Manager records Create/Drop index events as "Alter User Table" events.
- ***(Fixed in version 5.6)*** IDERA SQL Compliance Manager is not loading events accessed through a View. SQL Compliance Manager does not display Sensitive Column events when accessed from a view. To access the information using views gather and filter out all SELECT statements. Note that this action will cause extra collection.

- ***(Fixed in version 5.6)*** Issues loading BAD auditing information. IDERA SQL Compliance Manager is not able to capture BAD auditing information when two objects with the same name exist in the same schema.
- ***(Fixed in version 5.6)*** SQL Text is not captured for DDL Statements. When monitoring an instance for DDL event, SQL Compliance Manager is not able to capture SQL Statements for DDL activities unless a user is added to the Privileged User Group. Users can also capture SQL Text by selecting **Capture SQL statements for DDL and Security changes** at Database Level.

Known issues in version 5.5

General issues

- (***Fixed in version 5.5.1***) When users try to upgrade from SQL Compliance Manager 4.5 to 5.5, trace files are not processed. If you currently work with SQL Compliance Manager 4.5, before upgrading stop the Collection Service, Agent Service, and disable auditing to stop trace file processing, then proceed to upgrade to SQL Compliance Manager 5.5, and configure and enable auditing. Upon upgrading to SQL Compliance 5.5, users must upgrade all agents to a 5.x version first. For more information, see Upgrade to this build.

- (***Fixed in version 5.5.1***) The SQL Compliance Manager Collection Server is not processing trace files, or processing them slowly, causing backlog files to get accumulated in the Collection Trace Directory in large transactional databases.

  The workaround for this issue is to increase the tamper detection interval and the Collection interval.
- (***Fixed in version 5.5.1***) IDERA SQL Compliance Manager installation fails if TLS 1.0 is disabled and if SQL Server 2012 Native Client is not available. IDERA SQL Compliance Manager 5.5 installs SQL Server 2012 native client (version 11.0.2100.60) which does not support TLS 1.2 enabled as per Microsoft.

  https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

  Users with SQL Server versions prior to SQL Server 2012 R2 SP3 need to enable TLS 1.0 or update the native client to the supported version (11.4.7001.0) following the link below:

  https://www.microsoft.com/en-us/download/details.aspx?id=50402
- (***Fixed in version 5.5.1***) SQL Compliance Manager does not process trace files generated by an older Agent after upgrading versions of the Collection Server and the Agent.

Auditing issues

- (***Fixed in version 5.5.1***) When performing an archive of a highly transactional database with SQL Compliance Manager, the application shows a “violation of PRIMARY KEY constraint” error and terminates the statement. The workaround for this issue is to rename the current archive database, along with the database files associated to it and perform a new archive operation. The operation should create a new archive database and database files.

Known issues in version 5.4.x

General issues

- (***Fixed in version 5.5.1***) SQL Compliance Manager does not accept user names longer than 20 characters and does not support some special characters for the user password, such as £.
- Removing databases using the Administration pane in the Management Console does not work. You can remove databases using the Explorer Activity panel.
- (***Fixed in version 5.5***) During an Agent-only installation, if you accept the default destination path for SQL Compliance Manager, and then select a different destination drive and use a sub-folder in the Agent Trace Directory dialog box, the installer does not create the Agent Trace Directory during installation. If this issue occurs, reinstall the Agent specifying a folder instead of a sub-folder as the destination path or use the default path specified in the installer.

Auditing issues

- If the audit settings are configured to audit DML events for a selected table, and extended events is enabled for DML and Select on the Instance, SQL Compliance Manager collects audit data for all tables and not only the selected table. If you turn off extended events, auditing correctly collects data for the selected table only.
- (***Fixed in version 5.5***) Execute events are captured when extended events is enabled. There may be some extra events captured and shown through the Extended Events auditing than the events shown through the Trace method.
- (***Fixed in version 5.4.2***) Cannot insert duplicate key row in object 'dbo.Events' with unique index 'IX_Events_eventId'.
- (***Fixed in version 5.4.2***) DatabaseName appears as empty for Login Events. SQL Compliance Manager 5.4 traces do capture the DatabaseID, but do not include the database name.
- (***Fixed in version 5.5***) Applying a regulation guideline does not work when there is a Privileged User defined.
- (***Fixed in version 5.4.2***) Case-sensitive collation may prevent some trusted and privileged users from being captured.
- (***Fixed in version 5.4.2***) Auditing an AlwaysOn database using the Node method causes the Registered SQL Servers list to display both nodes as Secondary.
- Audit Snapshot does not include setting to capture DDL SQL statements.
- Before-After data does not appear for Binary Collation SQL Server instances when extended events is enabled.
- (***Fixed in version 5.4.2***) Audit settings at an instance level take precedence over database-level settings for a Privileged User.
- (***Fixed in version 5.5***) Agent trace folder permissions are overwritten when the Agent is deployed.
- (***Fixed in version 5.4***) SQL Compliance Manager attempts to contact the Agent (heartbeat check) on attached archive databases.
- (***Fixed in version 5.5***) Users who export reports to Microsoft Excel fail when the SQL text contains more than 32,767 characters.
- (***Fixed in version 5.4.2***) Some SQL Server startup/stop events may cause the integrity check to fail.
- The Audit Events tab may display an incorrect user name in the Login column when auditing start and stop server events.
- (***Fixed in version 5.4.2***) A known SQL Server issue causes some SQL Compliance Manager SELECT statements to appear as DML events. This issue occurs when a user audits both SELECT and DML. SQL Compliance Manager captures many events when certain columns are selected from certain system tables from a single SELECT statement query and shows them as individual DML events. Specifically, the SELECT statement which uses the `permissions()` function generates only DML event traces and not a SELECT event trace. This step results in SQL Compliance Manager reporting the SELECT statement as a DML event. In addition, the `permissions()` function is deprecated. Microsoft recommends in MSDN documentation that users implement the `Has_Perms_By_Name()` function instead of the `permissions()` function. The difference between these two functions is that the `permissions()` function always

generates the DML event traces while the `Has_Perms_By_Name()` function generates event traces according to permission type used. For example, SELECT event traces for SELECT permission types, and DML event traces for EXECUTE or DELETE permission types.

- (***Fixed in version 5.4.2***) Users who change the default port for the AlwaysOn Availability Group from the default may experience the following issues. to avoid these issues, change the listener to the default port.
    - SQL Compliance Manager does not accept the name format when attempting to add the listener name using the Cluster Configuration Console.
    - If the port is not added, the agent cannot connect to the SQL Server instance. You can manually add the port to the registry setting later and it will then connect to the instance after restarting the SQLcomplianceAgent.
    - Users cannot connect to the SQL Server instance even when adding the listener with the port in the SQL CM console.
    - The Permissions Check also fails.
- When you change the definition of a table you are auditing to include BLOB data types, the Before-After data trigger prevents UPDATE, DELETE, and INSERT operations from modifying the table, such as through stored procedures or third-party applications. This issue is most likely to occur when you are auditing all columns in the target table. This issue occurs because Before-After auditing does not support BLOB data types (such as text, image data, or XML code). To correct this issue, change the data definition of the table.
- SQL Compliance Manager does not support collecting and processing events from encrypted SQL Server trace files. This issue is most likely to occur in environments that use third-party encryption software. For example, some applications can be configured to automatically encrypt all new files created on a specific computer. If you are running encryption software in your SQL Server environment, verify the encryption settings to ensure the application does not encrypt trace files on the audited SQL Server instances.
- After removing a server from auditing and leave registered databases archived, the user is able to right-click the archived database ‘server’ and register databases to audit.
- Users can select “Capture SQL statements for DDL activities” only if the “Database Definition DDL” option is saved first.

Alerting issues

- Filtering by time does not work properly on the Alerts view.
- Some status alerts including Agent trace directory reached size limit and Collection Server trace directory reached size limit do not display properly in the Web Console.
- Status alerts are not generated for alert rules of the **Agent cannot connect to audited instance** Rule Type.
- (***Fixed in version 5.5***) SQL Statement is not captured or displayed when viewing Event Properties for Create SQL Login and Create Windows Login events.
- (***Fixed in version 5.4.2***) A Column Value Changed data alert is generated twice for each Before-After audit event.

Reporting issues

- (***Fixed in version 5.4.2***) The DML Activity (Before-After) report, when deployed to SQL Server Reporting Services, does not run properly. You can view the report in the Console.