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 (www.idera.com/support).

Installation and configuration issues

The SQL Compliance Manager 5.0 installation kit default extraction path is the same as previous versions and may cause issues if the previous files still reside at that location. Before launching the SQL Compliance Manager 5.0 upgrade, either select a different installation location or delete the files from the following location:

`c:\Program Files\Idera\SQLcompliance x64 Installation Kit` or `c:\Program Files (x86)\Idera\SQLcompliance x86 Installation Kit`

IDERA Dashboard 3.0.3 does not support SQL Server 2005 SP1

Users should not attempt to install SQL Compliance Manager with IDERA Dashboard 3.0.3 on a SQL Server 2005 SP1 as that version of SQL Server is not supported by IDERA Dashboard.

SQL Compliance Manager 5.3 remote Agent cannot be upgraded using the Management Console or Web Console

An issue in SQL Compliance Manager 5.3 prevents users from upgrading a remote Agent using the SQL Compliance Manager Management Console or the Web Console. For more information about upgrading to this release, see Upgrade from SQL Compliance Manager 4.5 to version 5.3+.

Verify SQL Compliance Manager repository database size before upgrading

It is important to check the size of the SQL Compliance Manager repository databases on the Collection Server before proceeding with an upgrade. There are four databases created by SQL Compliance Manager: SQLcompliance; SQLcompliance.Processing; SQLcompliance.<*Instance*>; SQLcompliance.<*Instance*>_Time_Partition. Each database should be under 20 GB to complete a successful upgrade. In order to avoid problems during the upgrade due to database size, IDERA recommends that you regularly archive the repository data to maintain the audit history. For more information about archiving, see Manage Audit Data. If archiving the data through SQL Compliance Manager is not an option at the time of the upgrade, it is recommended to back up the repository databases and delete unneeded records from the Events and EventSQL tables of the event databases.

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.

Agent-Only installation does not create a trace directory when you use a different destination folder

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.

Known issues in version 5.4.x

General issues

- 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.

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.
- 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.
- 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.
- Before-After data does not appear for Binary Collation SQL Server instances when extended events is enabled.
- (***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.
- Audit settings at an instance level take precedence over database-level settings for a Privileged User.
- Agent trace folder permissions are overwritten when the Agent is deployed.
- SQL Compliance Manager attempts to contact the Agent (heartbeat check) on attached archive databases.
- 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.

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.
- 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.