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`

SQL Compliance Manager 5.0 no longer supports Microsoft Windows Server 2000 or the .NET 2.0 framework

SQL Compliance Manager 5.0 does not support Windows Server 2000 or the .NET 2.0 framework. While SQL Compliance Manager 4.5 and prior versions continue to operate with Windows Server 2000, SQL Compliance Manager 5.0 and later require the .NET 4.0 Full framework to take advantage of the additional features. For additional information about supported versions, see the SQL Compliance Manager Software requirements.

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.

Upgrading from 2.1 to 3.3 or later results in SQL Server trace error

When you upgrade from SQL Compliance Manager version 2.1 to version 3.3 or later, you may receive warnings indicating that the trace is altered unexpectedly. This issue is most likely to happen when:

- Collection Server resides on a SQL Server 2005 instance
- SQL Compliance Manager is configured for self-monitoring

These warnings are incorrect and do not indicate a problem with your upgrade.

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 5.0

Users experience some AlwaysOn Availability Group issues when the listener uses any port other than the default

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.

Users receive error when installing SQL Compliance Manager after installing SQL BI if both use the same IDERA Dashboard

Users who install SQL BI Manager product before installing the SQL Compliance Manager product, both registering with the same IDERA Dashboard, may receive an error message.

Audit Events tab may display incorrect user account

The Audit Events tab may display an incorrect user name in the Login column when auditing start and stop server events.

Some SQL Server instances do not trigger a Column Value Changed alert

Case-sensitive SQL Server instances do not trigger a Column Value Changed alert when a column that is set up for Before-After Data auditing is changed.

Previous known issues

Net Time value not updated in recurring schedules

Users who have recurring archive schedules may notice an issue that prevents the archive process from executing. While the first scheduled archive does occur, the second scheduled archive does not. The workaround in this situation is to restart the Collection Service, and then wait until the next time the archive scheduler runs.

SELECT statements appear as DML events

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.

Already Deployed option is unavailable

When you attempt to add a new SQL Server instance to SQL Compliance Manager, the Deployment dialog box does not default to **Already Deployed** on instances where the Agent was manually installed on the machine where the SQL Server instance specified is located.

Guest user is enabled after installation

After installing SQL Compliance Manager 4.5, the Guest user is enabled in the SQLcompliance repository while it is disabled in the SQLcompliance event databases. You can disable this account in the repository using Microsoft SQL Server Management Studio.

Filtering Before-After data can cause event duplication

SQL Compliance Manager may duplicate some Before-After data events on the Audit Events tab of a database if you use the Filter by Table option to view your results. This issue does not occur with other filtering options.

Login Activity event alerts display as Security Changes in the Edit Event Alert Rule window

When you access the Edit Event Alert Rule window for a Login Activity event alert, SQL Compliance Manager defaults to the Security Changes option instead of the Login Activity option.

Changing archive preferences to Daily after upgrading to SQL Compliance Manager 4.5 causes an issue

Users who upgrade to SQL Compliance Manager 4.5, and then modify the archive preferences to **Daily** may experience that the subsequent archives fail and display a primary key constraint violation error message. In addition, SQL Compliance Manager does not store the events in the Events table of the Archive database.

Re-adding a virtual (clustered) instance previously deleted does not re-add a sub-key to the registry

When you install the SQLcompliance Agent on an audited instance, a Windows Registry sub-key called "Instances" is created in `HKEY_LOCAL_MACHINE\SOFTWARE\Idera\SQLcompliance\SQLcomplianceAgent`. This sub-key specifies the name of the SQL Server instance that you want to audit. In a clustered environment, the sub-key is created for each node. This issue occurs when you remove a virtual instance from the SQL Compliance Manager console, thereby deleting the sub-key from the active node registry, and then you re-add the virtual instance to the console. The sub-key "Instances" is not re-added to the registry and SQL Compliance Manager stops auditing data.

Archiving may fail on remote agents

Some users may experience an issue that causes archiving on a remote agent to fail. Associated error messages include:

- Exception: Invalid attempt to call Read when reader is closed.
- Exception: Unable to cast object of type 'System.Int32' to type 'System.String'.

Grooming alerts may result in an error when running the SQL Compliance Manager Console on Windows 2012 and Windows 8

Users running the SQL Compliance Manager Console on Windows 2012 and Windows 8 may receive an exception error when attempting to groom alerts. As a workaround, you can create a SQL script that deletes alerts directly from the repository.

Invalid events may appear for the custom Server role on a SQL Server 2012 instance

Users who create a custom Server role and give it permissions on a SQL Server 2012 instance may see events appearing as Invalid.

Issues can occur when a table name contains a period (.)

The following issues can occur if you have tables containing a period (.) in the name:

- Columns may not appear in the Before-After Data selection.
- Importing audit configuration containing Before-After Data settings may fail.
- Users cannot select Before-After Data and Sensitive Columns for audit.

Auditing sensitive columns does not capture events executed by encrypted stored procedures or linked servers

The Collection Server is unable to process SELECT events that were executed by encrypted stored procedures or queries from linked servers. This issue is most likely to affect the audit data trail for specific, sensitive columns.

Column-level auditing is limited to tables

Auditing of SELECT events at the column level is limited to columns located in tables. For example, you cannot audit specific columns located in views. However, to audit SELECT commands performed on views, you can enable SELECT auditing at the database level and choose to capture the corresponding T-SQL statements.

Auditing of before-after data is supported on a limited basis for databases that use SQL Server replication

IDERA provides limited support for before-after data auditing of the publisher database in SQL Servers with replication. However, this scenario is supported only when the publisher database with transaction replication is set to replicate data tables ONLY and no other objects. ***If the target database uses SQL Server replication set to replicate more than data tables*** , do not enable before-after auditing. Before and after data collection does not support SQL Server replication in that situation. For more information, see Microsoft Books Online for the version of SQL Server you are using.

Events statistics may not display in charts

SQL Compliance Manager now displays event statistics on the new Enterprise, SQL Server Instance, and Database Summary tabs. Because this information was not collected in previous versions, the new graphs does not display event statistics for audit data collected by SQL Compliance Manager 2.1 or earlier.

Filters do not support audit data collected by version 2.1 or earlier

SQL Compliance Manager includes many new filters in the enhanced Management Console views. These filters will not sort or filter events collected with SQL Compliance Manager version 2.1 or earlier.

Encrypted trace files not supported

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.

Alerts include raw variable data if undefined

SQL Compliance Manager now includes alert messages for all alerts. ***If you have not defined an alert message and an alert is generated*** , the alert message will display raw variable information without any corresponding values. Configuring your alert messages and defining the variables to include will allow you to customize what you see in alert messages.Adding BLOB data type to table definition prevents updates

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.