

# 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 \(www.idera.com/support\)](http://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 5.3 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.x](#).

## SQL Compliance Manager 5.0 and later do not support Microsoft Windows Server 2000 or the .NET 2.0 framework

Beginning with version 5.0, SQL Compliance Manager 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 5.3

### Installation and upgrade issues

- If you change the **Display Name** of IDERA SQL Compliance Manager during an upgrade, the installer perceives that you want an ADDITIONAL installation of SQL Compliance Manager rather than an upgrade of the previous version. This action results in TWO SQL CM TABS and does not upgrade the product in your environment. To upgrade SQL Compliance Manager, type the name displayed on the Web Console tab for your current installation.
- IDERA SQL Compliance Manager 5.3 does not support SQLcomplianceAgent silent installation.

- The Collection Trace directory is not created when choosing a non-default path during installation. Use the default installation path to avoid this issue.

## IDERA Dashboard issues

- Users who upgrade from a previous version of IDERA SQL Compliance Manager that supports the IDERA Dashboard may notice two issues with the widgets on the Dashboard Overview. First, duplicate SQLCM Environment Alerts widgets appear. Second, the Audited Instances widget may not display any data.

## Enterprise Activity Report Card issues

- The Overall Activity view of the Enterprise Activity Report Card included on the Home view of the Web Console and in the Windows Console displays all events processed by the system rather than only those generated as event alerts, failed logins, privileged user activity, DDL activity, and security alerts.

## Instance issues

- **If you use the IDERA SQL Compliance Manager Web Console to edit existing Threshold Notifications**, you may notice that the current settings are not properly displayed. They are correctly saved in the database and are simply not properly displayed in the Web Console.
- Users cannot register a new instance using the IDERA SQL Compliance Manager Web Console. This feature does work properly in the IDERA SQL Compliance Manager Windows Console.
- After you use the IDERA SQL Compliance Manager Windows Console to delete a SQL Server instance that includes Archived events:
  - an error occurs when you attempt to view your registered instances in the Web Console.
  - an "Agent heartbeat was not received" event occurs on every heartbeat check.

## Auditing issues

- Security changes and DDL events are not captured when Capture SQL Statements for DDL is enabled.
- While the IDERA SQL Compliance Manager Web Console Audit Event Filters view displays **Enable** or **Disable** in the **Status** column, the exported file displays only a 1 in that same column and for both statuses.
- After registering an AlwaysOn Availability Group server for auditing using the Listener method, IDERA Compliance Manager:
  - allows auditing of all databases for the Primary node, including those that are not part of the AG. Note that if the primary node changes, the non-AG databases will not be available.
  - (Cluster Agent configured on nodes) returns an error after running the update query with one column of a table selected for Before and After auditing OR when you select **Audit Selected Columns** with all columns selected instead of checking **Audit All Columns**. While the data is updated in the table, no Before and After data is collected.
- If you select **Custom** for the **Audit Collection Level** and attempt to add privileged users when adding a new database for auditing, an error occurs when you click **Add**. To avoid this issue, add the new database without selecting any privileged users, and then go back and edit the properties for the audited database and add a privileged user.
- When adding or removing a database role for a user on SQL Server 2008 R2, the audited event does not capture the SQL statement.
- If you have two tables in the same database that have the same name but different schemas, auditing fails on those two tables.
- When **Capture Transaction Status for DML Activity** is enabled for auditing on the database, capturing SQL Statements will have variables instead of values.
- Some SQL Server startup/stop events may cause the integrity check to fail.
- Case-sensitive collation may prevent some trusted and privileged users from being captured.

## Alerting issues

- **If you use the IDERA SQL Compliance Manager Windows Console to edit an existing Alert Rule**, you may notice that the current settings are not properly displayed. They are correctly saved in the database and are simply not displayed in the Windows Console. This feature does work properly in the IDERA SQL Compliance Manager Web Console.
- **If you use the IDERA SQL Compliance Manager Web Console to create an Alert Rule including Sensitive Column Accessed or Column Value Changed**, you may notice that the alerts are not generated when these events occur. This feature does work properly in the IDERA SQL Compliance Manager Windows Console.
- **If you use the IDERA SQL Compliance Manager Web Console to create an Event or Status Alert Rule**, you may notice that the alerts are generated when these events occur, but no corresponding email notifications are sent. This feature does work properly in the IDERA SQL Compliance Manager Windows Console.

## Previous known issues

### 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.

## 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_Permis_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_Permis_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.

SQL Compliance Manager audits all activity on your server. [Learn more](#) > >

<a href="#">IDERA Website</a>	<a href="#">Products</a>	<a href="#">Purchase</a>	<a href="#">Support</a>	<a href="#">Community</a>	<a href="#">About Us</a>	<a href="#">Resources</a>	<a href="#">Legal</a>
-------------------------------	--------------------------	--------------------------	-------------------------	---------------------------	--------------------------	---------------------------	-----------------------