Idera SQL Compliance Manager®

Version 4.5

SQL Compliance Manager 4.5 Home

Monitor, audit and alert on SQL Server user activity and data changes

- **Audit sensitive data**. See who did what, when, where, and how
- **Track and detect**. Monitor and alert on suspicious activity
- **Satisfy audits**. For PCI, HIPAA, FERPA, and SOX requirements
- **Generate reports**. 25 built-in reports to validate SQL Server audit trails
- **Minimize overhead**. Light data collection agent minimizes server impact

***SQL Compliance Manager audits all activity on your server. Learn more* > >**

Idera Website	**Products**	**Purchase**	**Support**	**Community**	**About Us**	**Resources**	**Legal**

Release Notes

Designed in partnership with major auditing firms and leading security experts, SQL Compliance Manager provides a powerful auditing and compliance solution for Microsoft SQL Server users. SQL Compliance Manager is a secure, lightweight auditing and reporting solution for Microsoft SQL Server designed to meet the needs of enterprise-scale SQL Server implementations. SQL CM provides unparalleled auditing and reporting services that help you meet the stringent requirements of today’s internal and external security standards.

To get a quick glimpse into the newest features, fixed issues, and known issues in this release of SQL Compliance Manager, review the following sections of the Release Notes:

- Learn about key new features in this release
- Review issues fixed by this release
- Review previous features and fixed issues
- See known issues
- See a list of recommended Idera Solutions

New features and fixed issues

SQL Compliance Manager provides the following new features and fixed issues.

> Idera, Inc. customers have the sole responsibility to ensure their compliance with the laws and standards affecting their business. Idera, Inc. does not represent that its products or services ensures that customer is in compliance with any law. It is the responsibility of the customer to obtain legal, accounting, or audit counsel as to the necessary business practices and actions to comply with such laws.

4.5 New features

Supports SQL Server 2014

SQL Compliance Manager supports the use of SQL Server 2014. Note that SQLcm requires the repository of the SQL Server version to be greater than or equal to the highest audited version, meaning that if you want to audit SQL Server 2012 and 2014 instances, your repository must be on SQL Server 2014 to support the highest version on your instances.

Supports Windows Server 2012 cluster deployment

This version of SQL CM allows you to install in a windows Server 2012 clustered environment. For more information about this feature, see Deploy SQL CM in a Windows Server 2012 clustered environment.

Audit the local SQL Server instance running the Collection Server on a cluster

SQL Compliance Manager allows you to audit a virtual SQL Server instance including the local instance on a cluster running the Collection Server. For more information about auditing a virtual SQL Server instance, see Audit a virtual SQL Server instance.

Schedule automatic archives

SQL Compliance Manager now allows you to schedule automatic archiving. You can select from daily, weekly, or monthly options. This feature is disabled by default. You can enable this feature and manage these settings in the Archive Preferences window.

Specify archive database drive

When setting up archiving, you can specify the drive where you want SQL CM to store the archive database. You can manage this location in the Archive Preferences window.

Receive alerts through SNMP

Users now can select to receive alerts as SNMP Trap messages to a specified destination network management console. For more information about creating a new event rule to includes SNMP Traps, see New Event Alert Rule wizard - Alert Actions tab.

Before-After data values display NULL when there is no value

After collecting data, if there is no before or after data available, SQL CM displays "NULL" in the **Before Value** and **After Value** colu mns of the Event Properties window. For more information about Before-After data, see Audited Database Properties window - Before-After Data tab.

Supports PCI DSS v3

SQL CM now supports Payment Card Industry Data Security Standard (PCI DSS) v3.0.

Improved table compression

The data type is changed in a number of highly-utilized tables from NTEXT to VARCHAR in an attempt to improve data compression.

Improved installation process

The SQL Compliance Manager installer now checks the permissions on the trace directory and the Idera folders to ensure that the service account is appropriately added with full control permissions for processing.

Improved database usage regarding failed inserts

SQL Compliance Manager includes new code that allows it to reuse event IDs in the event of a failed data insert.

4.5 Fixed issues

- SQL Compliance Manager includes new code regarding the threading library, making sure that all files in the trace directory are successfully processed. This fixes an issue that caused large trace file backlogs in the Collection Server.
- The Administrative Activities Audit Option no longer re-enables automatically after being disabled.
- Users no longer receive an error when processing the trace file due to a limited column size in the table associated with Before-After Data.
- Users upgrading from SQL CM 3.7 to 4.3 no longer receive numerous file parsing errors.
- This release fixes an issue causing incorrect dates to appear if you have SELECT and Sensitive Columns enabled in the Audited

Database Properties window. Previously, if the **Database SELECT operations** check box on the Audited Activities tab, and the Sensitive Columns tab includes **All Columns** of the **dbo.Customers** table, the dates in the summary for the associated SQL Server instance were incorrect.

- An issue that prevented new SQL CM Agent files from processing after adding a second node to a clustered repository no longer occurs.
- All failed integrity checks now includes specific events in the **Details** area of the Integrity Check Results window.
- Users no longer experience missing registry keys after re-adding monitored SQL Server instances.
- Adding an audited database to a monitored SQL Server instance no longer returns the server settings to default.
- Providing read-only access to the SQLcompliance database no longer requires that the GUEST account be enabled.

Previous features and fixed issues

This build of SQL Compliance Manager includes many fixed issues, including the following updates.

4.2 New features

New Family Educational Rights and Privacy Act (FERPA) guideline

Apply the new FERPA regulatory guideline to ensure your audited databases meet the requirements of this legislation. You can apply this guideline through the CLI or through the Import Audit Settings feature in the Console.

FERPA was introduced in 1974. This federal law mandates the confidentiality and protection of student information in any educational institution that receives funding from the Federal Government from kindergarten through the university level. FERPA generally prevents an education agency or institution from sharing student records or personally identifiable information in those records with individuals who are not authorized to view that information. In some cases authorized individuals need to be monitored to deter insider theft and unauthorized dissemination of information.

New Sarbanes Oxley (SOX) guideline

Apply the new SOX regulatory guideline to immediately enforce the right auditing settings for sensitive financial data. Collect a detailed audit trail of all access to that data and then deliver reports that prove your compliance to auditors. You can apply this guideline through the CLI or through the Import Audit Settings feature in the Console.

SOX, also known as the Corporate and Auditing Accountability and Responsibility Act, was first introduced in 2002. This legislation was put in place as a response to the corporate and accounting scandals which cost investors billions of dollars. From an information technology standpoint, security professionals and database administrators must collectively implement policies and processes that audit permissions on, and access to, financial data as well data changes such as before and after values.

New CLI actions register instances and apply audit settings

Use the new command line interface (CLI) actions to quickly and easily register large numbers of SQL Server instances and immediately apply audit settings to the hosted databases. You can choose to apply the default audit settings, custom audit settings you have exported from another audited instance, or a regulation guideline.

4.2 Fixed issues

- When the T-SQL query associated with an event cannot be parsed, SQL Compliance Manager now captures the SQL statement and indicates that it could not be parsed. This issue was mostly likely to occur when auditing sensitive column access.
- The Details tab of the Event Properties window now displays the SQL statement that is issued to SQL Server before SQL Server performs its query parameterization. This code represents the initial T-SQL query executed by the user.

4.0 New features

Offers HIPAA compliance guideline support

Collect data that helps you align with nine Health Insurance Portability Accountability Act (HIPAA) citations and one HITECH requirement via an out-of-the-box, customizable template.

Includes PCI compliance templates

Use the new, customizable auditing templates to help you comply with eight Payment Card Industry Data Security Standards (PCI DSS) requirement guidelines.

Provides Regulation Guideline reporting

The Regulation Guidelines report includes details for all of the guidelines applied to the databases on the selected SQL Server instance.

Features a new SQLcm Configuration Wizard for ease of use

The new SQL CM Configuration Wizard allows you to use a single wizard to register SQL Server instances, deploy the SQLcompliance Agent, add databases for audit, configure your audit settings for selected regulatory guidelines, and more.

4.0 Fixed issues

- SQL Compliance Manager now properly processes Grant statements.
- An issue causing SQL CM to record Create and Drop Index events as Alter User Table events no longer occurs.
- SQL CM now loads custom reports on the Archived Events page without requiring the user to select a filter.
- SQL CM now honors the DML/SELECT filters if you enable both Select auditing and Sensitive Column Auditing.
- SQL Compliance Manager now properly applies event filters for instances using non-standard ports.

3.7 New features

SQL Server 2012 compatible with experimental support

SQL Compliance Manager 3.7 is SQL Server 2012 RTM compatible. This version of SQL Compliance Manager is not certified against newer builds of SQL Server and should not be used with these builds in a production environment. Idera provides experimental support while you use your installation in a testing environment to ensure the features you rely on most are working as, or better than, expected.

3.7 Fixed issues

There are no fixed issues in this release.

3.6 New features

New sensitive column alerting

You can now receive alert notifications when someone accesses a sensitive column in your audited databases.

Improved integrity check user interface

The Integrity Check Results window now indicates when before-after data associated with `DML` events and sensitive column access data associated with `SELECT` events have been modified or deleted.

3.6 Fixed issues

The following reports now include the option to view related data from all audited SQL Server instances in your environment:

- Database Schema Change History
- Object Activity
- User Login History

3.5 New features

Sensitive column auditing

Track who has "selected" data from any number of columns in your audited tables and proactively identify malicious intent.

Transaction status auditing

Audit the status of any transaction that executes DML activity on your audited database. This audit data enhancement includes rollbacks and savepoints, allowing you to recognize suspicious activity.

3.5 Fixed issues

The Management Console now correctly imports alert rules exported from version 3.3 or earlier.

3.3 Fixed issues

- SQL Compliance Manager now supports auditing SQL Server instances located in environments that require FIPS compliance.
- The Collection Server now no longer performs duplicate processing of events collected in high-traffic environments. When this issue occurred, SQL compliance manager would write error and warning messages to the application event log, stating that it was either unable to read a trace file due to insufficient privileges or unable to delete the trace file due to a SQL Server lock.
- You can now successfully audit before-after data for DML events that occur on SQL Server databases hosted by a Windows Server Cluster.
- The DML/SELECT Filters tab of the Audited Database Properties window now allows you to successfully enable before-after auditing for DML events on specific database tables.

3.2 Hotfix 1 Fixed issues

- The SQLcompliance Agent now correctly handles a fail over that occurs on an active-active Windows cluster.
- When storing DML events collected for Before-After auditing, event processing now correctly stores each event only one time for statements that insert more than 1000 rows.

3.2 Fixed issues

- The SQLcompliance Agent now refreshes its list of DBID (database identifier) properties at each heartbeat. This fix ensures that SQL compliance manager can continue collecting audit data for a database after its ID number changes. For example, database ID numbers can change when a database is dropped, backed up, re-attached, or restored.
- The groom job now correctly deletes all events older than the specified age.
- The groom job now correctly identifies the SQL Server version, ensuring it grooms before and after data generated by DML events in SQL Server 2005 or later only. The ability to collect before and after data is not supported on SQL Server 2000 instances.
- Event Filters now support blank, empty, or null values when specifying application and host names.

3.1 Hotfix 1 Fixed issues

- When attempting to audit DML activity on specific databases, the SQLcompliance Agent would sometimes fail to collect the DML events according to your audit settings. With this hotfix, the SQLcompliance Agent correctly audits the specified databases for DML activity.
- After enabling the ability to audit Before-After data on database tables, SQL compliance manager would require accounts to have administrator privileges to the tables created by SQLcompliance in order to modify data in the audited table, potentially preventing third-party applications and other accounts from writing to these tables. This hotfix allows SQL Server logins to read and write to the audited tables per the assigned privileges.
- When attempting to groom audit data from a SQL compliance manager Repository hosted on a SQL Server 2000 instance, the grooming process would fail, returning the error “incorrect syntax near the keyword 'TOP'”. With this hotfix, you can successfully groom the Repository.
- When you attempt to update the archive database indexes using the command-line interface or the Management Console, the update process would fail. With this hotfix, you can successfully update all archive databases to the new Repository schema.
- The Management Console did not correctly format statistics with large values, resulting in an incorrect Processed Events statistic on the Explore Activity views. This hotfix resolves these formatting issues.

Known issues

Idera strives to ensure our products provide quality solutions for your SQL Server needs. The following known 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

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 has been 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 4.5

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 CM 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 SQLcm 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 CM, 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 CM 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 CM 4.5 causes an issue

Users who upgrade to SQL CM 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 CM 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 CM 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 CM 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'.

Previous known issues

Grooming alerts may result in an error when running the SQL CM 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 have been 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 not supported on databases that use SQL Server replication

You cannot audit before-after data, and their corresponding transactions, on databases that have SQL Server replication enabled. SQL Server replication is available for instances running SQL Server 2005 or later.

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 the table from being modified by UPDATE, DELETE, and INSERT operations, such as through stored procedures or third party applications. This issue is most likely to occur when you are auditing all the 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.

Recommended Idera Solutions

Idera strives to ensure our products provide quality solutions for your database needs. The following Idera Solutions have been recently added to the knowledge base at our Customer Service Portal (http://www.idera.com/support/ServiceFrame.aspx).

Number	Title
00000493	Additional service permission requirements for SQL Compliance Manager
00000361	What TCP/IP ports do the SQL Compliance Manager services communicate on?
00001481	User-defined Events: How to capture Before and After Data in SQL Compliance Manager
00001258	SQL Compliance components may not bind to the correct network adapter if a computer is configured to use multiple adapters

Get Started

Use the following checklist to get started using SQL Compliance Manager. For more information about how to best configure auditing for your environment, see the Auditing checklist.

✓	**Get started with these steps ...**
✓	Learn how auditing works.
✓	Learn about the SQL Server events that you can audit.
✓	Register the SQL Server instances you want to audit, and set your server and database settings.
✓	Apply regulation guidelines to the audited databases on your registered SQL Server instances.
✓	Track the collected SQL Server events over time and fine tune your audit settings as needed.
✓	Configure Event Alerts to notify you when suspicious events occur in your environment.
✓	Configure Status Alerts to notify you when SQL Compliance Manager experiences an issue.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Upgrade to this build

You can quickly and easily upgrade to this version of SQL Compliance Manager from version 2.0 or later. Upgrading SQL CM allows you to take advantage of the new features available in this latest version.

Upgrade checklist

✓	**Follow these steps ...**
✓	Ensure the computers on which you want to upgrade SQL Compliance Manager meet or exceed the hardware, software, and permissions requirements for this version. For example, ensure .NET Framework 2.0 or later is running on the target computer.
✓	Ensure your Windows logon account has local administrator permissions on the computers you intend to upgrade.
✓	Close all open applications on the computers running the SQL CM components.
✓	Back up your trace directories, especially the Collection Server Trace Directory.
✓	Upgrade your SQL Compliance Manager Repository, Collection Server, and Console.
✓	When prompted, schedule a time for SQL Compliance Manager to perform maintenance on your Repository databases.
✓	Ensure your product license is current. ***If you are upgrading from version 2.1 or earlier***, you will need to upgrade your license key.
✓	Upgrade your previously deployed SQLcompliance Agents.
✓	Ensure your upgrade includes any new reports by redeploying the SQL Compliance Manager reports. ***If you are upgrading from version 3.0 or earlier and you use Microsoft Reporting Services***, you must redeploy the SQL CM Reports in order to generate reports using the upgraded Repository databases as the data source.
✓	Test your upgrade by collecting and reporting on your audit data.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Upgrade the product components

You can use the setup program to upgrade all components or any individual component. The setup program detects whether SQL Compliance Manager components are running or installed on the local computer. The setup program automatically upgrades the Management Console, the Collection Server, and the SQLcompliance Agent according to your implementation.

> ⓘ The Repository must reside on a version of SQL Server that is greater than or equal to the highest audited SQL Server version.

To upgrade SQL Compliance Manager:

1. Log on with an administrator account to the computer on which you want to upgrade the Collection Server.
2. Run `SETUP.EXE` in the root of the installation kit.
3. On the Idera SQL Compliance Manager Quick Start window, click **SQL Compliance Manager** to begin the upgrade process.
4. On the Idera SQL Compliance Manager dialog, click **Yes** to start the upgrade process.
5. On the Upgrade Wizard for Idera SQL Compliance Manager window, click **Next**.
6. On the Repository Host window, select the authentication type and enter the SQL credentials, if necessary, and then click **Next**.
7. On the Setup Wizard Completed window, click **Finish** to end the upgrade process.
   Start the Management Console. When prompted, schedule a time for SQL Compliance Manager to perform maintenance on your Repository databases.
8. Upgrade your SQLcompliance Agents.

Upgrade your product license key

SQL Compliance Manager version 3.0 and later uses a new license key. ***If you are upgrading from version 2.1 or 2.0***, you will need to update your existing product license key within 45 days of upgrading to version 4.2. To request a new license, contact licensing@idera.com.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Upgrade your deployed SQLcompliance Agents

Before upgrading your SQLcompliance Agents, review the permissions requirements and how the SQLcompliance Agent works.

> ⓘ ***If you manually installed the SQLcompliance Agent on the audited SQL Server computer***, use the setup program to upgrade the agent locally.

Upgrade an agent deployed to a remote server

You can upgrade the SQLcompliance Agent remotely using the Management Console. Use this approach to upgrade agents on any registered SQL Server where you remotely installed the agent.

To upgrade a remote SQLcompliance Agent:

1. In the Navigation pane, click **Administration**, and then select **Registered SQL Servers** in the Administration tree.
2. In the view pane, right-click the SQL Server instance for which you want to upgrade the SQLcompliance Agent.
3. Select **Upgrade Agent** from the context menu.

Upgrade an agent locally

You can use the SQL Compliance Manager setup program to upgrade the SQLcompliance Agent on the local computer that is running the registered SQL Server instance. Use this approach when you are upgrading the SQLcompliance Agent on a registered SQL Server where you manually installed the agent.

Upgrade an agent in a clustered environment

You can easily upgrade a SQLcompliance Agent for a SQL Server instance located in a Windows cluster by running the setup program. Perform the following steps on each node (computer) of the cluster.

> ⚠ When you upgrade the SQLcompliance Agent, the associated CLI trigger is deleted and recreated. This update can take several minutes. During this time, the SQLcompliance Agent status will show that it is unavailable due to a CLR error. Use the Activity Log to track when the new CLI trigger install completes.

To upgrade an agent on a cluster node:

1. Log on with an administrator account to the cluster node. Start with the currently active node.
2. Bring the SQLcompliance Agent generic service for this SQL Server resource group offline.
3. Run `SETUP.EXE` in the root of the installation kit.
4. Click **INSTALL** on the Setup tab of the setup program.
5. On the Install window, click **Cluster Configuration Console**.
6. On the Idera SQL Compliance Manager Cluster Configuration dialog, click **Yes** to start the upgrade process, and then click **Next** to continue. After the upgrade completes, the Cluster Configuration Console automatically starts.
7. When prompted, specify the directory location you want SQL compliance manager to use to store CLR trigger assemblies.
8. Bring the SQLcompliance Agent generic service online.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Upgrade from SQL CM 4.0 and older in a clustered environment

Use the following steps if you are upgrading SQL Compliance Manager 4.0 or older in a clustered environment. The steps support upgrading in either a windows Server 2003 or Windows Server 2008 clustered environment.

> Be sure to back up your Repository and all databases and archives before upgrading SQL CM.

Install the SQL CM Collection Service on Cluster Nodes

You must upgrade the SQL Compliance Manager Collection Service on each cluster node for the service to work correctly when a failure occurs on the primary cluster node hosting the Collection Service.

> Before upgrading, changing, or uninstalling SQL CM on the passive node, you must delete the following registry entry: `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance\CollectionService\TraceDirectory`. This step in unnecessary for new installations.

To install the SQL Compliance Manager Collection Service on cluster nodes:

1. In the Microsoft Cluster Administrator tool (Windows Server 2003) or Microsoft Failover Cluster Management Console (Windows Server 2008), select the SQLComplianceCollectionService resource and take the service offline.
2. Log on with an administrator account to the computer on which you want to upgrade SQL CM.
3. Run `Setup.exe` in the root of the SQL CM installation kit on the first cluster node.
4. Under **Install**, click **SQL Compliance Manager**.
5. Read the Welcome window, and then click **Next**.
6. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
7. Verify that the installation folder is the same location where you initially installed SQL CM, and then click **Next**.
8. Select the **Clustered Collection Server** setup type, and then click **Next**.
9. Check the **Install the Collection Server in a Windows Cluster** check box.
10. Select whether you are upgrading the Collection Service on the **Currently Active Node** or **A Passive Node**, and then click **Next**.
11. ***If you upgrade the currently active node***, verify that the SQL CM Collection Service trace directory is the same location where you current directory resides, and then click **Next**. ***If you install on a passive node***, continue with the next step.
12. Type the service account information, and then click **Next**.
13. Verify that the Repository path is the same SQL Server instance name hosting the Repository.
14. Select the authentication method used to upgrade the Repository database and include credentials, if required, and then click **Next**.
15. In the Repository Warning dialog box, click **Preserve** to retain your current Repository. If you click **Delete**, the upgrade tool DELETES all of your current Repository databases.
16. Click **Install**.
17. In Windows Services, stop the SQL CM Collection Service and set the Startup type to **Manual**.
18. Repeat the previous steps on each cluster node. Point to the SQL CM Repository installed on the first node.
19. In the Microsoft Cluster Administrator tool (Windows Server 2003) or Microsoft Failover Cluster Management Console (Windows Server 2008), select the **SQLComplianceCollectionService** resource and bring the service online.

Welcome to SQL Compliance Manager

SQL compliance manager is a secure, lightweight auditing and reporting solution for enterprise-level Microsoft SQL Server environments.

Need help using SQL compliance manager? See the following sections:

- Start auditing events
- Alert on suspicious audit data
- Alert on SQL compliance manager status
- Report on audit data

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

What is SQL Compliance Manager?

Designed in partnership with major auditing firms and leading security experts, SQL Compliance Manager provides a powerful auditing and compliance solution for Microsoft SQL Server users. SQL CM is a secure, lightweight auditing and reporting solution for Microsoft SQL Server designed to meet the needs of enterprise-scale SQL Server implementations. SQL CM provides unparalleled auditing and reporting services that help you meet the stringent requirements of today's internal and external security standards.

SQL Compliance Manager provides many critical features:

- Low overhead data collection
- Central Repository of audit data
- Central Management Console
- Pre-defined compliance reports
- Secure ad-hoc queries for auditors
- Forensic analysis
- Efficient, secure data archival
- Comprehensive reporting to satisfy audit requirements (PCI DSS, HIPAA)

SQL Compliance Manager is the only solution that lets you quickly, easily, and securely answer the demands of on-the-spot reports, routine audits, and long-term event trending across your SQL Server environment.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

How SQL Compliance Manager helps

As a database administrator, you need a comprehensive and easy-to-use auditing and reporting solution that helps ensure continuous compliance while protecting the integrity of your audit data and SQL Server environment. SQL Compliance Manager is specifically designed to meet these requirements. SQL CM helps you meet multiple goals, whether you are fulfilling the requirements of internal auditors or simply need to feel comfortable with your database security model.

Ensure continuous compliance

SQL Compliance Manager goes beyond traditional auditing approaches by providing monitoring and auditing of all data access, updates, data structure modifications, and changes to security permissions. The audit data captured is stored in a central Repository for reporting, querying, and analysis.

You can easily configure SQL CM to audit only the events you need to track. This flexibility ensures you have a continuous stream of audit data to ensure continual compliance with internal and external security standards.

Achieve low overhead data collection

SQL Compliance Manager employs an efficient, low overhead data collection technology. A light agent monitors the SQL Server trace data stream, collects the audit data, and sends it back to the Repository. You can configure the type and detail of audit data you want to collect on an individual SQL Server instance or database. No changes to applications or production databases are required.

Leverage powerful reporting and analytics

SQL Compliance Manager is the only solution that provides secure and comprehensive reporting on and analysis of your audit data. SQL CM provides many pre-defined reports that you can immediately use to track audited events. SQL CM also leverages the flexibility and power of Microsoft SQL Server Reporting Services (Reporting Services). Through Reporting Services, you can modify the pre-defined reports or create custom reports that meet your specific auditing needs.

Protect integrity of audited data

SQL Compliance Manager leverages your existing SQL Server security model to enforce data access. You can easily and securely control who has the ability to configure, view, or report on audit data. SQL CM integrates with and conforms to your internal security policies, allowing granular access control at the database level.

SQL CM is engineered to provide a trusted, immutable source of audit data. Its powerful self-auditing features ensure that you are alerted to any changes to data collection settings or attempts to tamper with the audit data repository.

Realize rapid deployment and scalability

With DynamicDeployment™ technology, a light agent is dynamically deployed to the specific SQL Server instances you want to audit. This approach enables you to configure and deploy SQL Compliance Manager in minutes. There is no need to perform time-consuming software installs on each target server. The agent eliminates risk and increases performance by running as a separate process outside the SQL Server process space.

SQL CM is specifically designed to support large SQL Server installations. SQL CM scales from auditing a single SQL Server instance to thousands of SQL servers around the globe, from databases with only a few tables to databases with thousands of tables and large volumes of data.

Satisfy regulation requirements

When a user accesses sensitive data or when breach occurs, SQL Compliance Manager identifies the content of the event including the date, time, data accessed, and by whom, providing a clear audit trail and alerting those individuals who may need to take action.

SQL CM provides comprehensive reporting to satisfy audit requirements with regulatory and data security rules such as PCI DSS and HIPAA. SQL CM audits all SQL Server activity including login access (successful/failed) and permission activity, and provides tracking reports to help you detect abnormal access to the data. All SQL CM audit data is stored in a tamper-proof repository.

SQL Compliance Manager audits all activity on your server. Learn more > >

Find answers

This documentation set includes a comprehensive online Help system as well as additional resources that support you as you install and use the product. You can also search the Idera Solutions knowledge base, available at the Idera Customer Service Portal (http://www.idera.com/support/faq).

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Document conventions

Idera documentation uses consistent conventions to help you identify items throughout the printed online library.

Convention	Specifying
Bold	Window items
Italics	Book and CD titles Variable names New terms
Fixed Font	File and directory names Commands and code examples Text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value 1 | value 2	Exclusively command parameters where only one of the options can be specified

SQL Compliance Manager audits all activity on your server. Learn more > >

How to use this Help system

The Idera wiki includes a comprehensive online Help system as well as additional resources that support you as you install and use Idera products. You can also search multiple Idera support solutions, available at http://www.idera.com/support/faq

Additionally, Idera helps you by providing:

- 24/7 technical support for critical issues.
- Availability to report cases and access a web-based customer portal for update status.
- Access to our Knowledge center where you can find FAQs, How To's, Best Practices, and Webcasts.

This wiki includes the following Web browser minimum requirements:

- Internet Explorer 8.0
- Mozilla Firefox 4
- Google Chrome 6

You can access the Idera SQL Admin Toolset Help system through the **Help** icon on the top right section of your window or by pressing F1 on the section where you need more information.

You can print a help topic from the wiki using the Print function in your browser.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Definition of terms

Computer

Refers to the server that hosts a SQL Server, this maybe a physical or virtual server.

Database

A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields. For example, a company database may include tables for products, employees, and financial records. Each of these tables would have different fields that are relevant to the information stored in the table.

Instance

Also known as SQL Server or SQL server instance. SQL Server supports multiple “instances” or installations on the same host computer. Each instance runs independently from all others and has its own set of installation code, configuration parameters, system and user databases, memory allocation, and security configuration.

Location

The location refers to the physical or geographical location of an instance, such as Houston for example.

Owner

The owner refers to the user whom the instance belongs to. When you register an instance, Idera recommends that you register the instance owner, so later you can easily get information from this owner and his/her respective instances.

About Idera

Idera is a leading provider of application and server management solutions. We have a wide variety of performance management products for Microsoft SQL Server, and award-winning server backup solutions for both managed service providers and enterprise customers. Idera products install in minutes and start solving server problems immediately, giving administrators more time, reduced overhead and expenses, and increased server performance and reliability. We are a Microsoft Gold Certified partner, headquartered in Houston, Texas, with offices in Asia Pacific, Australia, New Zealand, Europe, Africa, and Latin America. So we're everywhere your IT needs are.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Contact Idera

Please contact Idera with your questions and comments. We look forward to hearing from you. For support around the world, please contact us or your local partner.

For a complete list of our partners, please visit our Idera website.

Sales	713.523.4433 1.877.GO.IDERA (464.3372) (only in the United States and Canada)
Sales Email	sales@idera.com
Support	713.533.5144 1.877.GO.IDERA (464.3372) (only in the United States and Canada) www.idera.com/support
Website	www.idera.com

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Idera products

Our tools are engineered to scale from managing a single server to enterprise deployments with thousands of servers. Idera products combine ease of use with a design that installs in minutes, configures in hours, and deploys worldwide in days. To learn more about Idera products, visit the Idera Web site at www.idera.com.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Legal notice

Idera, Inc. (“Idera”) makes information and products available on this web site, subject to the following terms and conditions. By accessing this web site, you agree to these terms and conditions. Idera reserves the right to change these terms and conditions, and the products, services, prices, and programs mentioned in this web site at any time, at its sole discretion, without notice. Idera reserves the right to seek all remedies available by law and in equity for any violation of these terms and conditions. THIS WEB SITE MAY INCLUDE TECHNICAL OR OTHER INACCURACIES. CHANGES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN. HOWEVER, IDERA MAKES NO COMMITMENT TO UPDATE MATERIALS ON THIS WEB SITE.

Trademark

Azure SQL Database Backup, Hyper-V VHD Explorer, Linux Hot Copy, PowerShellPlus, PowerShell Scripts for SQL Server, SQL admin toolset, SQL Backup Status Reporter, SQL check, SQL comparison toolset, SQL compliance manager, SQLcompliance, SQLcm, SQL defrag manager, SQL diagnostic manager, SQLdm, SQL doctor, SQL Elements, SQL Fragmentation Analyzer, SQL Integrity Check, SQL Job Manager, SQL mobile manager, SQL Permissions Extractor, SQLsafe, SQLsecure, SQLtool, SQL toolbox, SQL Traffic Accelerator, SQL virtual database, SQLvdb, SQL XEvent Profiler, virtual database, Idera, BBS Technologies and the Idera logo are trademarks or registered trademarks of Idera, Inc., or its subsidiaries in the United States and other jurisdictions. All other company and product names may be trademarks or registered trademarks of their respective companies. Elements of this web site are protected by trade dress or other laws and may not be imitated or reproduced in whole or in part.

Copyright

The information on this web site is protected by copyright. Except as specifically permitted, no portion of this web site may be distributed or reproduced by any means, or in any form, without Idera’s prior written consent.

Use of the Software

The software and accompanying documentation available to download from this web site are the copyrighted work of Idera. Use of the software is governed by the terms of the License Agreement, which accompanies such software. If no license accompanies the download, the terms of the license, which accompanied the original product being updated, will govern. You will not be able to use, download, or install any software unless you agree to the terms of such License Agreement.

Use of web site information

Except as otherwise indicated on this web site, you may view, print, copy, and distribute documents on this web site subject to the following terms and conditions:

1. The document may be used solely for informational, personal, non-commercial purposes;
2. Any copy of the document or portion thereof must include all copyright and proprietary notices in the same form and manner as on the original;
3. The document may not be modified in any way; and
4. Idera reserves the right to revoke such authorization at any time, and any such use shall be discontinued immediately upon notice from Idera.

Documents specified above do not include logos, graphics, sounds or images on this web site or layout or design of this web site, which may be reproduced or distributed only when expressly permitted by Idera.

Warranties and Disclaimers; Liability Limitations

EXCEPT AS EXPRESSLY PROVIDED OTHERWISE IN A WRITTEN AGREEMENT BETWEEN YOU AND IDERA, ALL INFORMATION AND SOFTWARE ON THIS WEB SITE ARE PROVIDED "AS IS" WITHOUT WARRANTY OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

IDERA ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THE INFORMATION OR SOFTWARE OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS WEB SITE.

IN NO EVENT SHALL IDERA BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION) WHETHER OR NOT IDERA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Submissions

With the exception of credit card numbers for the purchase of products and services, Idera does not want to receive confidential or proprietary information through its web site.

Any information sent to Idera, with the exception of credit card numbers, will be deemed NOT CONFIDENTIAL. You grant Idera an unrestricted, irrevocable license to display, use, modify, perform, reproduce, transmit, and distribute any information you send Idera, for any and all commercial and non-commercial purposes.

You also agree that Idera is free to use any ideas, concepts, or techniques that you send Idera for any purpose, including, but not limited to, developing, manufacturing, and marketing products that incorporate such ideas, concepts, or techniques.

Idera may, but is not obligated to, review or monitor areas on its web site where users may transmit or post communications, including bulletin boards, chat rooms, and user forums. Idera is not responsible for the accuracy of any information, data, opinions, advice, or statements transmitted or posted on bulletin boards, chat rooms, and user forums.

You are prohibited from posting or transmitting to or from this web site any libelous, obscene, defamatory, pornographic, or other materials that would violate any laws. However, if such communications do occur, Idera will have no liability related to the content of any such communications.

Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

Governing Law and Jurisdiction

You agree that all matters relating to your access to, or use of, this web site and these terms and conditions shall be governed by the laws of the state of Texas. You agree and hereby irrevocably submit to the exclusive personal jurisdiction and venue of the state courts of Texas located in Harris County, Texas, and the United States District Court for the Southern District of Texas, with respect to such matters.

Idera makes no representation that information on this web site are appropriate or available for use in all countries, and prohibits accessing materials from territories where contents are illegal. Those who access this site do so on their own initiative and are responsible for compliance with all applicable laws.

Export Control Laws

Certain Idera products, including software, documentation, services, and related technical data, available on the Idera and other web sites are subject to export controls administered by the United States (including, but not limited to, the U.S. Department of Commerce Export Administration Regulations (“EAR”)) and other countries including, controls for re-export under European Union, the Singapore Strategic Goods Control Act, and the import regulations of other countries. Diversion contrary to U.S. or other applicable law of any Idera product or service is prohibited. Export, re-export or import of products and services may require action on your behalf prior to purchase and it is your responsibility to comply with all applicable international, national, state, regional and local laws, and regulations, including any import and use restrictions. Idera products and services are currently prohibited for export or re-export to Cuba, Iran, North Korea, Sudan, Syria, or to any country then subject to U.S. trade sanctions. Idera products and services are prohibited for export or re-export to any person or entity named on the U.S. Department of Commerce Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Idera products and services are prohibited from use with chemical or biological weapons, sensitive nuclear end-users, or missiles, drones or space launch vehicles capable of delivering such weapons. By downloading or using any product from this web site, or purchasing any service, you are acknowledging that you have read and understood this notice and agree to comply with all applicable export control laws. You are also representing that you are not under the control of, located in, or a resident or national of any prohibited country, and are not a prohibited person or entity. This notice is not intended to be a comprehensive summary of the export laws that govern the products and services. It is your responsibility to consult with a legal adviser to ensure compliance with applicable laws.

United States Government Rights

All Idera products and publications are commercial in nature. The software, publications, and software documentation available on this web site are "Commercial Items", as that term is defined in 48 C.F.R.§2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R.?12.212 and 48 C.F.R. 227.7202, as applicable. Pursuant to 48 C.F.R. §12.212, 48 C.F.R.§252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-19, and other relevant sections of the Code of Federal Regulations, as applicable, Idera's publications, commercial computer software, and commercial computer software documentation are distributed and licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in the license agreements that accompany the products and software documentation, and the terms and conditions herein.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Installation and deployment

Installing SQL Compliance Manager is both quick and easy, allowing you to take immediate advantage of SQL CM auditing technologies. Use the following checklist to help you prepare your environment to successfully install and deploy SQL CM.

✓	**Follow these steps ...**
✓	Ensure the computer on which you want to install SQL Compliance Manager meets or exceeds the hardware requirements. For more information, see Hardware requirements.
✓	Ensure the computer on which you want to install SQL Compliance Manager meets or exceeds the software requirements. For more information, see Software requirements.
✓	Ensure your Windows logon account has administrator permissions on the computers where you want to install SQL Compliance Manager components.
✓	Review the supported installation scenarios to understand how to set up SQL Compliance Manager in your environment. For more information, see Implementation scenarios.
✓	Review the deployment considerations for implementation best practices. for example, if you plan to audit databases that sustain a heavy workload, install the Collection Server on a detailed computer.
✓	Identify the Windows account under which the SQLcompliance Agent should run. *Account Name:* *Password:* For more information, see Permissions requirements.
✓	Identify the Windows account under which the Collection Server should run. *Account Name:* *Password:* For more information, see Permissions requirements.
✓	Ensure you understand how licensing of your SQL Server instances works with SQL Compliance Manager. For more information, see How licensing works.
✓	Ensure you install SQL Compliance Manager as instructed. For more information, see How to install SQL Compliance Manager. ***If you are installing SQL CM on a Windows*** **cluster**, see how to audit a virtual SQL Server instance.

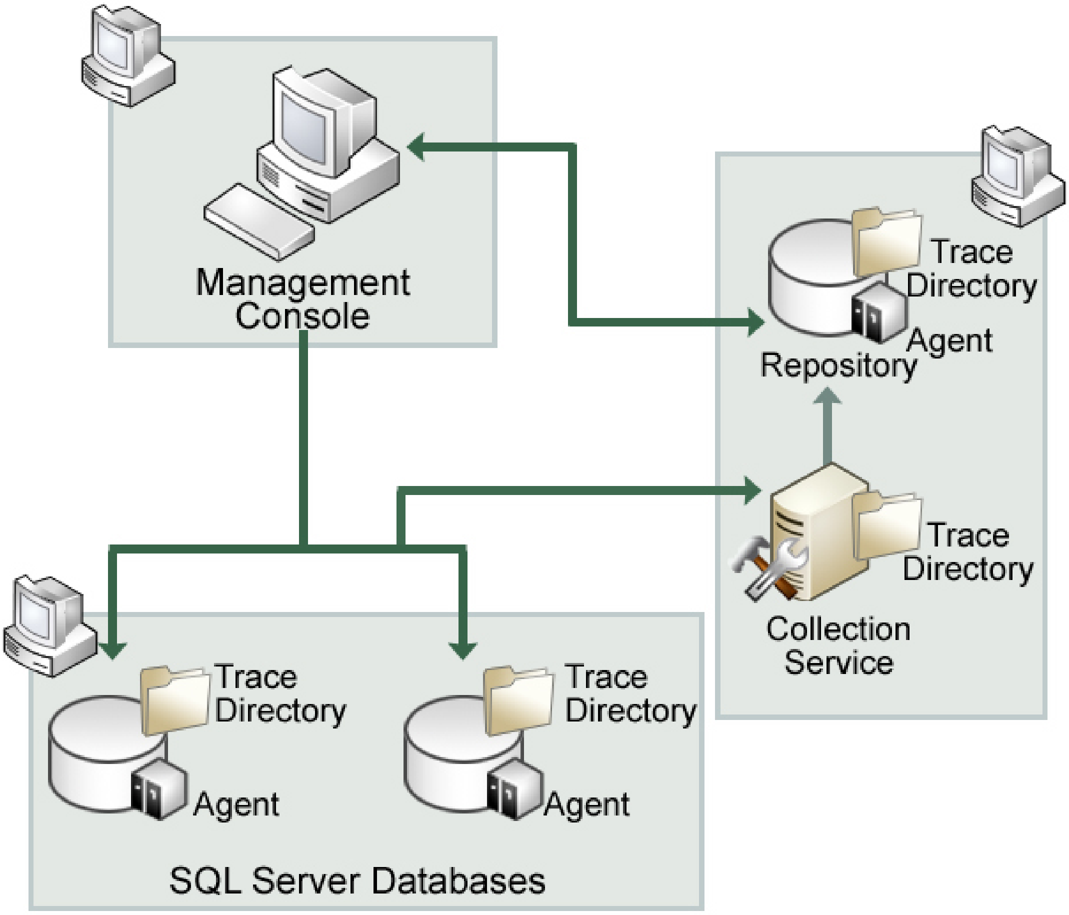
Product components and architecture

SQL Compliance Manager consists of a light, unobtrusive architecture that easily runs in your SQL Server environment with minimal configuration. All SQL CM components run outside and separate from SQL Server processes. SQL CM does not add to or modify any of your native SQL Server files or services.

Architecture

SQL Compliance Manager provides a robust, easy-to-use SQL Server audit and reporting solution. Behind a friendly user interface, SQL CM offers a unique, loosely coupled architecture that is both flexible and extremely powerful. SQL CM fits your environment, no matter how simple or complex.

The following diagram illustrates the components of the SQL Compliance Manager architecture.



Management Console

The Management Console is a centralized, intuitive user interface that allows you to easily and quickly modify audit settings, monitor events, and report on audit data. This user interface also provides the following information:

- Real-time status of audited SQL Server instances
- SQL Server login permissions
- Detailed logging of change activity
- Track and prove continual compliance using reports

Repository databases

The SQL Compliance Manager Repository is the central repository that tracks:

- SQLcompliance configurations, such as audit settings, server registrations, and console security
- Audited SQL Server events
- Alert messages

- SQLcompliance Agent activity

The Repository consists of the following databases. For more information, see How auditing works.

Repository Database Name	Description
SQLcompliance	Stores alert messages, audit settings, SQLcompliance Agent events, Activity Report Card statistics, and other SQL Compliance Manager configurations.
SQLcompliance.Processing	Stores processing event data received from the SQLcompliance Agent.
SQLcompliance.Instance	Stores processed events collected from a registered instance.
SQLcompliance.Instance_Time_Partition	Stores archived events collected from a registered instance.

Collection Server

The Collection Server processes trace files received from the SQLcompliance Agent, stores audit data in the events and archive databases, and sends audit setting updates to the SQLcompliance Agent. The Collection Server runs under the Collection Service account. By default, the Collection Server communicates with the Repository every five minutes (heartbeat) to write processed audit data to the event databases associated with the registered SQL Server instances.

SQLcompliance Agent

The SQLcompliance Agent gathers SQL Server events written to the SQL trace, caching these audited events in trace files. By default, the SQLcompliance Agent calls the Collection Server every five minutes (heartbeat) to receive audit setting updates, and sends trace files for processing every two minutes. The SQLcompliance Agent runs under the SQLcompliance Agent Service account. For more information, see How the SQLcompliance Agent works.

ⓘ Sensitive Column auditing is supported by SQLcompliance Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.

Command line interface

The command line interface (CLI) provides an interface for third-party tools so you can automate and schedule regular tasks, such as audit data archival and grooming, and perform diagnostic tasks. You can also perform integrity checks through the CLI.
The CLI supports the following operations.

CLI Operations	Description
agentsettings	Lists the settings for the SQLcompliance Agent running on a specific SQL Server instance.
archive	Archives audited events collected for registered SQL Server instances.
auditdatabase	Enables auditing on a new database, allowing to specify either a regulation guideline or a custom audit template.
checkintegrity	Verifies the integrity of audited events collected for a specific registered SQL Server instance.
collect	Collects trace data from the agent.
groom	Deletes audited events older than a specified age.
help	Displays the CLI Help.
listtriggers	Lists the CLR triggers for DML auditing on a specific registered SQL Server instance.
registerinstance	Registers a new SQL Server instance and applies audit settings.
removetriggers	Removes the CLR triggers from the subscriber table on the specific SQL Server instance.
serversettings	Lists the settings for the Collection Server.

timezones	Displays the time zones recognized by the computer hosting the Collection Server.
updateindex	Applies optimized Repository index configurations to existing events and archive databases.

Trace files and the trace directory

Trace files contain audited SQL Server events collected by the SQLcompliance Agent. The SQLcompliance Agent stores these temporary files in a secure directory on the audited SQL Server instance. When the set directory size threshold is reached, the SQLcompliance Agent stops the SQL trace until the trace files are sent to the Collection Server for processing. When the set file size threshold is met, the trace file is cycled. You can configure the SQLcompliance Agent trace file directory location as well as how the SQLcompliance Agent manages these files, such as how often the agent sends trace files to the Collection Server. For more information, see How the SQLcompliance Agent works.

Hardware requirements

The following sections provide the hardware requirements for each SQL Compliance Manager component. For more information, see Product components and architecture.

Audited SQL Server

The audited SQL Server computer is the computer that hosts the SQL Server databases you want to audit. In a clustered environment with virtual SQL Servers, the audited SQL Server is the virtual SQL Server. However, each node (physical computer) in the cluster that hosts the virtual SQL Server must meet or exceed these requirements.

To achieve optimal performance, ensure each SQL Server computer meets or exceeds the following hardware requirements.

Hardware Type	Requirement
CPU	1 GHz
Memory	512 MB
Hard Disk Space	2 GB

Collection Server

The Collection Server computer is the computer that hosts the Collection Service and processes trace files. This computer also hosts the Repository databases.

To achieve optimal auditing performance and data storage, ensure the Collection Server computer meets or exceeds the following hardware requirements.

Hardware Type	Requirement
CPU	2 GHz
Memory	8 GB
Hard Disk Space	20 GB for trace directory 75 GB for Repository

Management Console

The Console computer is the computer that hosts the SQL Compliance Manager Management Console. You can install the console on the Collection Server computer, or any client computer for remote access to your audit data.

Ensure each console computer meets or exceeds the following hardware requirements.

Hardware Type	Requirement
CPU	1 GHz
Memory	512 MB
Hard Disk Space	150 MB

Permissions requirements

SQL Compliance Manager requires specific permissions and rights to successfully audit events. By default, the setup program assigns the Collection Service and SQLcompliance Agent Service accounts read and write permissions on the respective trace directory.

Management Console user permissions

Actions	Permissions Requirements
Administer SQL compliance manager and configure audit settings	sysadmin rights on the Repository databases
Generate and view audit reports	Read permissions (public rights) on the Repository databases
Deploy SQLcompliance Agent to registered SQL Server instance	Administrator permissions on the computer hosting the target instance
Connect to the SQL Server that hosts the Repository databases	SQL Server login

Operating system permissions

Actions	Permissions Requirements
Store audit settings and manage archive databases in the Repository	sysadmin rights on each Repository database
Process trace files	Read, write, and delete permissions on the Collection Server trace directory
Manage trace directory	Local Administrator permissions on the computer that hosts the Collection Service
Run as a service	Log on as a Service right on the computer that is running the audited SQL Server instance

SQLcompliance Agent service permissions

Actions	Permissions Requirements
Starting and stopping traces, and managing SQLcompliance stored procedures	sysadmin rights on the audited SQL Server instance or database
Manage trace files	Read, write, and delete permissions on the SQLcompliance Agent trace directory
Manage trace directory for an audited SQL Server instance	Local Administrator permissions on the computer that hosts the registered SQL Server
Manage trace directory for an audited virtual SQL Server	Administrator permissions on each node in the cluster hosting the virtual SQL Server
Run as a service	Log on as a Service right on the computer that is running the audited SQL Server instance

SQL Server service permissions on the Collection Server

Actions	Permissions Requirements
Load trace files so the Collection Server can process these events	Read permissions on the Collection Server trace directory

SQL Server service permissions on the registered SQL Server

Actions	Permissions Requirements
Write events to trace files for the registered SQL Server instance and audited databases	Write permissions on the SQLcompliance Agent trace directory

Using Windows Authentication

The SQL Compliance Manager Managment Console and Agent require Windows authentication. Windows authentication uses the logged on user account to establish trusted connections through the operating system. The credentials of the logged on user account are passed to the SQL Server database servers. Your database server then verifies the user matches an established SQL Server login account that has the appropriate permissions. Only after verification will a connection open.

When using Windows authentication, the account logged on to the Management Console computer must have the appropriate SQL compliance manager permissions.

Using SQL Server Authentication

The SQLcompliance Collection Service leverages existing SQL Server logins that have been granted the appropriate SQL privileges. However, SQL Compliance Manager does not support SQL Server authentication.

SQL Compliance Manager audits all activity on your server. Learn more > >

Port requirements

To ensure the SQLcompliance Agent and Collection Server can successfully audit instances in your environment, open the following ports. For more information, see Supported installation scenarios.

Environment Type	Port Requirements
Typical	• Port 5201 on the Collection Server computer • Port 5200 on each computer hosting an audited SQL Server instance
Clustered	• Port 5201 on the Collection Server computer • Port 5200 on each cluster node hosting a virtual SQL Server you want to audit
Non-trusted	• Port 5201 on the Collection Server computer • Port 5200 on each computer hosting an audited SQL Server instance in a non-trusted domain or workgroup

Software requirements

The following sections provide the software requirements for each SQL Compliance Manager component. For more information, see Product components and architecture.

Support for MS SQL Server software includes case-sensitive servers and databases. Support for Windows operating systems includes English and international versions. ***If an operating system service pack is not mentioned***, a service pack is not required for that version of the operating system.

All SQL CM components require .Net 2.0 or later.

ⓘ SQL Compliance Manager no longer allows installations on Windows 2000.

ⓘ Sensitive Column auditing is supported by SQLcompliance Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.

ⓘ This version of SQL CM does not support the Itanium processor architecture. Versions up to and including SQL CM 3.5 continue to operate with Itanium, but no Itanium support is available. SQL CM 3.7 and later support SQL Server 2012 SP1.

SQL Compliance Manager Windows cluster support

You can install SQL CM on a Windows 2003, 2008, or 2012 cluster. For more information, review the supported installation scenarios and Audit a virtual SQL Server instance.

Audited SQL Server

The audited SQL Server computer should meet or exceed the software requirements recommended by Microsoft to run and manage SQL Server databases.

In a clustered environment with virtual SQL Servers, the audited SQL Server is the virtual SQL Server. However, each node (physical computer) in the cluster that hosts the virtual SQL Server must meet or exceed these requirements.

SQL Compliance Manager supports auditing the following Microsoft SQL Server versions.

SQL Server Version	Operating System
MS SQL Server 2014	Windows Server 2008, Windows Server 2012
MS SQL Server 2012 SP1	Windows Server 2008 SP2
MS SQL Server 2008 R2 Standard and Enterprise Editions	Windows Server 2008 R2, Windows Server 2008
MS SQL Server 2008 Standard and Enterprise Editions	Windows Server 2008, Windows Server 2003, or Windows 2000 Server SP4 or later
MS SQL Server 2005 Standard and Enterprise Editions	Windows Server 2003 or Windows 2000 Server SP4 or later
MS SQL Server 2000 Standard Edition SP3 or later *	Windows Server 2003
MS SQL Server 2000 Standard Edition SP2 or later *	Windows 2000 Server SP4 or later
MS SQL Server 2000 Enterprise Edition *	Windows 2000 Server SP4 or later
** SQL Compliance Manager does not support Before-After data auditing on SQL Server 2000 instances. This feature is available only for instances using SQL Server 2005 and above*.	

Collection Server

Ensure each Collection Server computer meets or exceeds the following software requirements. The Collection Server hosts the Collection Service and the Repository databases, which store SQL CM configuration and audit data.

If you plan to audit instances running SQL Server 2005 or later, install the Collection Server on a computer hosting the highest version of SQL Server running in your environment. For example, to accept event data from audited instances running SQL Server 2012 SP1, the Repository databases must reside on a SQL Server 2012 SP1 instance.

⚠ The Repository must reside on a version of SQL Server that is greater than or equal to the highest audited SQL Server version.

Software Type	Requirement
Operating System	The Collection Server requires one of the following operating systems: • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 SP1 • Windows Server 2003 SP2 • Windows 2000 SP4 • Windows XP SP3 • Windows Vista SP2+ • Windows 7 SP1+ • Windows 8
Microsoft SQL Server	The Collection Server requires one of the following versions of Microsoft SQL Server: • MS SQL Server 2014 • MS SQL Server 2012 SP1 • MS SQL Server 2008 R2 Standard and Enterprise Editions • MS SQL Server 2008 Standard and Enterprise Editions • MS SQL Server 2005 Standard and Enterprise Editions

Management Console

Ensure each console computer meets or exceeds the following software requirements. You can install the console on the Collection Server computer, or any client computer for remote access to your audit data.

Software Type	Requirement
Operating System	The Collection Server requires one of the following operating systems: • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 SP1 • Windows Server 2003 SP2 • Windows 2000 SP4 • Windows XP SP3 • Windows Vista SP2+ • Windows 7 SP1+ • Windows 8 The Management Console computer also requires Microsoft Data Access Components (MDAC) 2.6 or later. If you plan to audit SQL Server 2005 instances, upgrade to MDAC 2.8 or later. SQL Server 2005 requires MDAC 2.8 to communicate with other applications.
Documentation	Internet Explorer 7.0 or later

Agent

Ensure the computer where the agent resides meets or exceeds the following software requirements.

Software Type	Requirement
Operating System	The agent requires one of the following operating systems: • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 SP1 • Windows Server 2003 SP2 • Windows 2000 SP4 • Windows XP SP3 • Windows Vista SP2+ • Windows 7 SP1+ • Windows 8
Documentation	Internet Explorer 7.0 or later

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Supported installation scenarios

You can install and deploy SQL Compliance Manager to meet your unique auditing and SQL Server environment needs. For example, you can select which specific databases on your SQL Server instances you want to audit.

Typical environment

The following figure illustrates a typical SQL CM implementation scenario. This configuration includes the following installations:

- Management Console on your workstation (and, optionally, the Collection Server computer)
- Collection Service and Repository on a SQL Server database server
- SQLcompliance Agents on each computer hosting databases you want to audit

Clustered environment

You can install and configure SQL Compliance Manager to audit virtual SQL Servers. A virtual SQL Server is a SQL Server running on a Microsoft failover cluster managed by Microsoft Cluster Services.
This configuration includes the following installations:

- Management Console on your workstation
- Collection Service and Repository on a SQL Server Database server
- SQLcompliance Agents on each cluster node hosting the virtual SQL Server you want to audit

For more information, see Audit a virtual SQL Server instance.

Non-trusted environment

You can install and configure SQL Compliance Manager to audit SQL Server instances running in non-trusted domains or workgroups. This configuration includes the following installations:

- Management Console on your workstation
- Collection Service and Repository on a SQL Server database server
- SQLcompliance Agents on each SQL Server instance you want to audit in a non-trusted domain or workgroup

Deployment considerations

Before implementing SQL Compliance Manager, review the following guidelines to ensure optimal performance, security, and disaster recovery. For example, ***if you anticipate collecting large numbers of events (several hundred thousand or more) in a short time period***, consider incorporating one or more of these guidelines in your SQL CM deployment.

- Identify how much audit data you expect to collect
- Use a dedicated computer for the Collection Server
- Optimize the model database settings
- Optimize the tempdb database settings
- Preserve audit data using archives
- Implement a disaster recovery strategy

Identify audit data volume

Estimate the amount of audit data your compliance needs may generate, and ensure the Collection Server computer has ample memory and database space. Consider the following examples:

- A data set of one million events may require 1 GB of database space to store the audit data
- A trace file that is 5 MB may require 100 MB of memory to process the collected events

The amount of audit data you collect and process depends on your audit settings. Test your audit settings to identify a baseline and set your memory and hardware needs accordingly.

To estimate your audit data volume, perform a test audit of your SQL Servers for 7 days, and track how much space is used by the Repository databases. Use the resultant event collection rate to estimate the database size you will need to store and process audit data over time. Also consider how often you plan to archive or groom data. For example, ***if you collect an average of 500 MB of audit data per day and you plan to archive events every 14 days***, then the database size should be set to 7 GB. Ensure you set the Repository databases to automatically grow. For more information, see Optimize tempdb settings.

Use a dedicated computer

Install the Collection Server on a dedicated physical computer running SQL Server. For optimal performance, implement the following recommended configurations:

- Configure the trace directory to use a different disk than what the operating system uses
- Run 64-bit versions of the Windows operating system and the SQL Server software
- Ensure the Repository databases are the only databases hosted on this SQL Server
- Set the default database file locations so these files are stored on a different disk than what the operating system uses

This configuration also helps you ensure minimal access to the SQL Server instance and your audit data. For more information, see Product components and architecture.

Optimize model settings

Change the following model system database properties to ensure optimal performance and complete backups of the Repository databases. The Repository databases store your audit settings and collected audit data. Whenever the Collection Server creates an events or archive database, SQL Server uses the model database as a template for the new database, applying the same property values.

Use the following guidelines to optimize performance in a typical environment. For best results, monitor your audit data collection over a period of time, and then set these model properties to reflect your needs. For more information, see Identify audit data volume.

Property Name	Benefits	Value
Automatically grow file	Allows the `tempdb` database to expand as needed, accommodating cases when the collected audit data set is larger than expected	Selected
File growth	Allows SQL Server to efficiently handle any required file growth	25%
Recovery Model	Allows you to perform full backups of the Repository database	Simple
Space allocated	Allows ample database space for audit data collection, so file growth occurs less frequently	200 MB

Optimize tempdb settings

Change the following tempdb system database properties to ensure optimal performance when the Collection Server processes and archives audit data.

Use the following guidelines to optimize performance in a typical environment. For best results, monitor your audit data collection over a period of time, and then set these tempdb properties to reflect your needs. For more information, see Identify audit data volume.

Property Name	Benefits	Value
Automatically grow file	Allows the `tempdb` database to expand as needed, accommodating cases when the collected audit data set is larger than expected	Selected
File growth	Allows SQL Server to efficiently handle any required file growth	25%
Space allocated	Allows ample database space for audit data collection, so file growth occurs less frequently	200 MB

Preserve audit data using archives

Include frequent archiving in your audit data maintenance strategy. Archiving lets you store audit data in separate databases that can be accessed for future reporting. For more information, see How archives work.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Implement a disaster recovery strategy

A disaster recovery strategy allows you to plan for unexpected outages to ensure you can continue auditing SQL Server activity and policy compliance.

When you implement SQL Compliance Manager in your production SQL Server environment, consider preparing a disaster recovery strategy to minimize audit data loss should the Collection Server become unavailable. Use the following procedures and guidelines to implement a new disaster recovery strategy or modify an existing disaster recovery strategy.

Identify how often to back up the Repository databases

The frequency at which you back up the Repository databases depends on the following factors:

- How often your audit settings change
- How often your SQL Server environment changes as you add new servers and databases or remove older servers and databases
- How much audit data you collect in a given time period
- How much risk you are willing to incur

The backup frequency should reflect your maintenance needs and allow you to meet future compliance requirements.

Schedule routine backups of the Repository databases

After you identify the appropriate backup frequency for your compliance needs, use a tool such as Idera SQL Safe to schedule routine backups of the Repository databases.

How to install SQL Compliance Manager

Before installing SQL Compliance Manager, consider the following best-practices:

- Ensure you review the hardware, software, permissions, and port requirements.
- Decide whether you should install the Collection Server on a dedicated SQL Server instance.
- ***If you plan to audit instances running SQL Server 2005 or later***, install the Collection Server on a computer hosting the highest version of SQL Server running in your environment. For example, to accept event data from audited instances running SQL Server 2012, the Repository databases must reside on a SQL Server 2012 instance.

By default, SQL CM installs with a trial license. For more information about trial licenses or upgrading your license, see Licensing.

To install SQL Compliance Manager:

1. Log on with an administrator account to the computer on which you want to install SQL CM.
2. Run `SETUP.EXE` in the root of the installation kit.
3. On the Idera SQL Compliance Manager Quick Start window, click **SQL Compliance Manager** to begin the installation process.
4. On the Welcome to the Setup Wizard for Idera SQL Compliance Manager window, click **Next**.
5. Read the Trial Software License Agreement, select **I accept the terms in the license agreement** and click **Next** to continue.
6. Accept the default folder for your SQL CM installation, or click **Browse** to specify a different folder.
7. Select whether you want the SQL CM application to be available to all users who log on to this computer, and then click **Next**.

If you select this option …	Setup configures the user logon profile to …
Anyone who uses this computer	Display icon on desktop when anyone logs onto this computer using a valid domain user account
Only for me	Display icon on desktop only when the current user account logs onto this computer

8. Select the appropriate setup type, and then click **Next.**

Setup Type	Description
Typical	Allows you to install all SQL Compliance Manager components on this computer
Console Only	Allows you to install only the SQLcompliance Management Console
Agent Only	Allows you to install only the SQLcompliance Agent
Custom	Allows you to select the individual SQL CM components you want to install

9. ***If you chose the Custom type***, select one or more SQL CM component, and then click **Next**. Using the Custom setup type, you can install SQL CM components in the following ways:
   - Collection Server and Repository with SQLcompliance Agent
   - Collection Server and Repository
   - Management Console with SQLcompliance Agent
   - Management Console only
   - SQLcompliance Agent only

   The setup program installs the Repository when you install the Collection Server.

   To install all SQL Compliance Manager components at the same time, use the **Typical** setup type.
10. ***If you chose to install the Collection Server and SQLcompliance Agent using the Typical or Custom setup***, complete the following procedure:
    a. Specify the location where you want the Collection Server to store audit data received from the SQLcompliance Agent, and then click **Next**. The specified folder is the trace file directory on the Collection Server.
    b. Specify the Windows user account that you want the Collection service and SQLcompliance Agent to run as to access the Repository, and then click **Next**.
    c. Click **Browse** to select the SQL Server instance on which you want to install the Repository. The setup program creates the Repository databases on the specified instance.
    d. Specify the authentication the setup program should use to connect to the selected SQL Server and create the Repository, and then click **Next**.
    e. ***If you want to audit the Repository or other databases associated with the selected SQL Server instance***, click **Yes**, and then click **Next**.
    f. Specify the location where the SQLcompliance Agent should store collected audit data, and then click **Next**. The specified folder will be the trace file directory on the audited SQL Server instance.
    g. Select whether you want to start the services immediately after install, and then click **Next**.
11. ***If you chose the Agent Only setup***, complete the following procedure:

   a. Specify the location where the SQLcompliance Agent should store collected audit data, and then click **Next**. The specified folder will be the trace file directory on the audited SQL Server instance.
   b. Specify the Windows user account the SQLcompliance Agent service should run as to access databases associated with the audited SQL Server instance, and then click **Next**. ***If you are installing the agent on a computer that belongs to a workgroup or non-trusted domain***, specify a valid local account (`MyComputer\AccountName`).
   c. Type the name of the computer on which the Collection Server is installed, and then click **Next**. ***If you are installing the SQLcompliance Agent on a workstation or a computer that belongs to a non-trusted domain***, the setup program is unable to validate a connection to the specified computer. Click **No** when prompted to specify another Collection Server computer.
   d. Click **Browse** to select the SQL Server instance you want to audit, specify the authentication the SQLcompliance Agent should use to connect to associated databases, and then click **Next**.
   e. Select whether you want to start the SQLcompliance Agent service immediately after install, and then click **Next**.

12. Click **Install**.
13. Click **Finish**. ***If you chose a typical setup***, select **Launch Idera SQL Compliance Manager** to begin auditing your SQL Server environment.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Deploying SQL CM in a clustered environment

SQL Compliance Manager allows you to audit and report on your clustered SQL Server environment. See the following topics for installation and configuration instructions for Windows Server 2003, Windows Server 2008, and Windows Server 2012 environments.

- Deploy SQL CM in a Windows Server 2003 clustered environment
- Deploy SQL CM in a Windows Server 2008 clustered environment
- Deploy SQL CM in a Windows Server 2012 clustered environment

Deploy SQL CM in a Windows Server 2003 clustered environment

The following instructions guide you through the installation of SQL Compliance Manager in a Windows Server 2003 based clustered environment. Before installing in this environment, note that the generic service must be in the same clustered resource group as the SQL Server. Be sure to have the following information available before creating the generic service:

- Name of the disk containing the folder
- SQL IP address
- SQL network name
- SQL Server service

Install the SQL CM Collection Service on Cluster Nodes

You must install the SQL Compliance Manager Collection Service on each cluster node for the service to work correctly when a failure occurs on the primary cluster node hosting the Collection Service.

> ⚠ Before upgrading, changing, or uninstalling SQL CM on the passive node, you must delete the following registry entry: `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance\CollectionService\TraceDirectory`. This step is unnecessary for new installations.

To install the SQL Compliance Manager Collection Service on cluster nodes:

1. Log on with an administrator account to the computer on which you want to install SQL Compliance Manager.
2. Run `Setup.exe` in the root of the SQL CM installation kit on the first cluster node.
3. Under **Install**, click **SQL Compliance Manager**.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
6. Accept the default installation folder, or click **Browse** to specify a different folder, and then click **Next**.
7. Select the **Clustered Collection Server** setup type, and then click **Next**.
8. Check the **Install the Collection Server in a Windows Cluster** check box to note that you are installing the SQL CM components in a cluster. ***If you leave this box unchecked***, the installer performs a **Typical** installation.
9. Select whether you are installing the Collection Service on the **Currently Active Node** or **A Passive Node**, and then click **Next**.
10. ***If you install on the currently active node***, specify a trace directory on a shared disk, and then click **Next**. ***If you install on a passive node***, continue with the next step.
11. Type the service account information, and then click **Next**.
12. Type the virtual SQL Server instance name hosting the Repository, or click **Browse** to specify a different server.
13. Select the authentication method used to install the Repository database and include credentials, if required, and then click **Next**.
14. Click **Install**.
15. In Windows Services, stop the SQL CM Collection Service and set the Startup type to **Manual**.

Repeat the previous steps on each cluster node. Point to the SQL CM Repository installed on the first node.

> ⓘ You cannot perform the installations concurrently, as the installers collide when checking the repository. You must perform the installations sequentially.

Create the clustered service resource

After installing the SQL Compliance Manager Collection Service on your cluster nodes, create the clustered service resource to allow SQL CM to recognize the cluster nodes.

To create the clustered service resource:

1. Log onto the currently active cluster node using an administrator account, and then start the Microsoft Cluster Administrator tool.
2. Right-click the SQL Server cluster resource group for the Collection Service, and then select **New > Resource**.
3. Type a name and description for the new resource.
4. Select the **Generic Service** resource type.
5. Verify that the correct group appears in the **Group** field, and then click **Next**.
6. Verify that the nodes in the cluster where you can use this resource appear in the **Possible owners** area, and then click **Next**.
7. Complete the following fields, and then click **Next**.
   a. Name of the disk containing the folder
   b. SQL IP Address
   c. SQL Network Name
   d. SQL Server Service
8. Type `SQLcomplianceCollectionService` in the **Service Name** field.
9. Leave the Start parameters blank.
10. Check the **Use Network Name for computer name** check box, and then click **Next**.
11. Click **Add** to add a new root registry key.

12. Type `Software\Idera\SQLcompliance`, and then click **OK**.
13. Click **Finish**.
14. Start the new generic service by bringing the resource online.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Deploy SQL CM in a Windows Server 2008 clustered environment

The following instructions guide you through the installation of SQL Compliance Manager in a Windows Server 2008 based clustered environment. Be sure to have the following information available before creating the generic service:

- Name of the disk containing the folder
- SQL IP address
- SQL network name
- SQL Server service

Install the SQL CM Collection Service on Cluster Nodes

You must install the SQL Compliance Manager Collection Service on each cluster node for the service to work correctly when a failure occurs on the primary cluster node hosting the Collection Service.

> ⚠ Before upgrading, changing, or uninstalling SQL CM on the passive node, you must delete the following registry entry: `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance\CollectionService\TraceDirectory`. This step is unnecessary for new installations.

To install SQL CM services on cluster nodes:

1. Log on with an administrator account to the computer on which you want to install SQL Compliance Manager.
2. Run `Setup.exe` in the root of the SQL CM installation kit on the first cluster node.
3. Under **Install**, click **SQL Compliance Manager**.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
6. Accept the default installation folder, or click **Browse** to specify a different folder, and then click **Next**.
7. Select the **Clustered Collection Server** setup type, and then click **Next**.
8. Check the **Install the Collection Server in a Windows Cluster** check box to note that you are installing the SQL CM components in a cluster. ***If you leave this box unchecked***, the installer performs a **Typical** installation.
9. Select whether you are installing the Collection Service on the **Currently Active Node** or **A Passive Node**, and then click **Next**.
10. ***If you install on the currently active node***, specify a trace directory on a shared disk, and then click **Next**. ***If you install on a passive node***, continue with the next step.
11. Type the service account information, and then click **Next**.
12. Accept the default SQL Server hosting the Repository, or click **Browse** to specify a different server.
13. Select the authentication method used to install the Repository database and include credentials, if required, and then click **Next**.
14. Click **Install**.
15. In Windows Services, stop the SQL CM Collection service and set the Startup type to **Manual**.

Repeat the previous steps on each cluster node. Point to the SQL CM Repository installed on the first node.

> ⓘ You cannot perform the installations concurrently, as the installers collide when checking the repository. You must perform the installations sequentially.

Create the clustered service resource

After installing the SQL Compliance Manager Collection Service on your cluster nodes, create the clustered service resource to allow SQL CM to recognize the cluster nodes.

To create the clustered service resource:

1. Log onto the currently active cluster node using an administrator account, and then start the Microsoft Failover Cluster Management Console.
2. Under Service and Applications, select the application for the SQL Server instance hosting the Repository, and then add a resource as a Generic Service.
3. Select SQL Compliance Manager Collection Service, and then complete the wizard to create the service.
4. Right-click the SQL Compliance Manager Collection Service in the Other Resources list, and then select **Properties**.
5. Type the Network Name for the SQL Server, and then click **Apply**.
6. On the Dependencies tab, complete the following fields:
   a. Name of the disk containing the folder
   b. SQL IP Address
   c. SQL Network Name
   d. SQL Server service
7. On the General tab, check the **Use Network Name for computer name** check box.
8. Click **Add** to add a new root registry key.
9. Type `Software\Idera\SQLcompliance`, and then click **OK**.
10. Start the new generic service by bringing the resource online.

Idera Website | Products | Purchase | Support | Resources | Community | About Us | Legal

Deploy SQL CM in a Windows Server 2012 clustered environment

The following instructions guide you through the installation of SQL Compliance Manager in a Windows Server 2012 based clustered environment. Be sure to have the following information available before creating the generic service:

- Name of the disk containing the folder
- SQL IP address
- SQL network name
- SQL Server service

Install the SQL CM Collection Service on Cluster Nodes

You must install the SQL Compliance Manager Collection Service on each cluster node for the service to work correctly when a failure occurs on the primary cluster node hosting the Collection Service.

> ⚠ Before upgrading, changing, or uninstalling SQL CM on the passive node, you must delete the following registry entry: `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance\CollectionService\TraceDirectory`. This step is unnecessary for new installations.

To install SQL CM services on cluster nodes:

1. Log on with an administrator account to the computer on which you want to install SQL Compliance Manager.
2. Run `Setup.exe` in the root of the SQL CM installation kit on the first cluster node.
3. Under **Install**, click **SQL Compliance Manager**.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
6. Accept the default installation folder, or click **Browse** to specify a different folder, and then click **Next**.
7. Select the **Clustered Collection Server** setup type, and then click **Next**.
8. Check the **Install the Collection Server in a Windows Cluster** check box to note that you are installing the SQL CM components in a cluster. ***If you leave this box unchecked***, the installer performs a **Typical** installation.
9. Select whether you are installing the Collection Service on the **Currently Active Node** or **A Passive Node**, and then click **Next**.
10. ***If you install on the currently active node***, specify a trace directory on a shared disk, and then click **Next**. ***If you install on a passive node***, continue with the next step.
11. Type the service account information, and then click **Next**.
12. Accept the default SQL Server hosting the Repository, or click **Browse** to specify a different server.
13. Select the authentication method used to install the Repository database and include credentials, if required, and then click **Next**.
14. Click **Install**.
15. In Windows Services, stop the SQL CM Collection service and set the Startup type to **Manual**.

Repeat the previous steps on each cluster node. Point to the SQL CM Repository installed on the first node.

> ⓘ You cannot perform the installations concurrently, as the installers collide when checking the repository. You must perform the installations sequentially.

Create the clustered service resource

After installing the SQL Compliance Manager Collection Service on your cluster nodes, create the clustered service resource to allow SQL CM to recognize the cluster nodes.

To create the clustered service resource:

1. Log onto the currently active cluster node using an administrator account, and then start the Microsoft Failover Cluster Manager.
2. Right-click the **SQL Server** role, and then select **Add Resource > Generic Service**.
3. Complete the New Resource Wizard to create the SQLcompliance Collection Service.
4. Right-click the service you just created, and then select **Properties**.
5. On the General tab, check the **Use Network Name for computer name** check box.
6. Click **Add** to add a new root registry key.
7. Type `Software\Idera\SQLcompliance`, and then click **OK**.
8. Start the new generic service by bringing the resource online.

Configure your deployment

After your initial installation and set up, you may want to perform the following tasks to further customize and streamline your deployment.

- Identify audit data volume
- Export your audit settings
- Manage the SQLcompliance Agent
- Optimize model settings
- Optimize tempdb settings
- Preserve audit data using archives
- Register your SQL Servers

Check the product version

You can check the product version at any time. The product version consists of the release number and build number assigned to SQL Compliance Manager.

To check the product version:

1. Start SQL Compliance Manager.
2. On the Help menu, click **About SQL Compliance Manager**.
3. Click **OK**.

Check the SQL Server version

You can quickly check the version of a SQL Server instance you are auditing.

To check the SQL Server version:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Right-click the SQL Server instance you want to check, and then select **Properties**.
3. On the General tab, review the SQL Server version number, and then click **OK**. For more detailed information to help troubleshoot an issue, use the native SQL Server Tools to check your SQL Server instance configuration settings.

Export your audit settings

You can export audit settings for an audited SQL Server instance or database. Exported audit settings are saved in an XML format and can be applied to other registered SQL Server instances. This flexibility saves you time when you are configuring audit settings on multiple SQL Server instances or databases, and helps ensure consistent audit settings across your environment. In addition, exporting allows you to back up your audit settings to use should you need to reinstate an audited SQL Server instance. As you configure audit settings, consider which settings you would like to save for future use, and export the settings configured for that particular SQL Server instance or database. You can later import these settings through the Console or apply them to a new registered instance and database through the CLI.

To export your audit settings:

1. Navigate to target SQL Server instance or database in the **Explore Activity** tree.
2. On the Summary tab, click either **Server Settings** or **Database Settings** to verify that the audit settings are correct.
3. Click **Export**.
4. Specify the file name or use the default name.
5. Select the location to save the output file. Considering saving the output file to a central location, such as a network share.
6. Click **Save**.

Import your audit settings

As you configure or modify audit settings for your SQL Server instances, you may want to apply the same settings across multiple SQL Server instances in your environment. You can import audit settings through previously exported XML files, allowing you to:

- Use previously configured audit settings as a baseline, or template, you deploy to multiple instances and databases so that the same events are audited across your environment
- Ensure all SQL Server databases used by regulated applications, such as SAP, are being audited consistently and held to the same level of compliance
- Streamline and automate your configuration workflow

If a user is assigned privileged status as part of the alert rule you are importing, and that user does not yet exist in the environment you are importing to, the privileged user status will apply if the user is ever added to your environment.

ⓘ To execute a T-SQL script that applies previously exported audit settings, use the auditdatabase CLI command.

Auditing the same events across multiple instances and databases

You can import previously configured audit settings to use as a baseline, or template. By deploying this baseline to multiple instances and databases, you can ensure the same events are audited across your environment.

To audit the same events across multiple instances or databases:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. On the **Registered SQL Servers** tab, click **Import**.
3. On the Select File to Import window, click **Browse** and locate the audit settings file, and then click **Open**.
4. Click **Next**.
   - ***If you want to audit events at the server level as well as events initiated by privileged users***, select these import options.
   - ***If you want to audit events at the database level***, click **Database Audit Settings**, and then select the database you want to use as your baseline or template.
5. On the Target Servers window, select the registered SQL Server instances to which you want to apply the selected audit settings, and then click **Next**.
6. On the Import Audit Settings window, select the audit settings you want to import, and then click **Next**.
7. On the Target Databases window, select the audited databases to which you want to apply the selected audit settings, and then click **Next**.
8. On the Summary window, choose whether you want your imported audit settings to overwrite the settings on the target SQL Server instances and databases or be added to the settings already present. Click **Finish** to import your audit settings.

Auditing regulated applications across your environment

You can import previously configured audit settings to ensure all SQL Server databases used by regulated applications, such as SAP, are being audited consistently and are held to the same level of compliance.

To audit regulatory applications across your environment:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. On the Registered SQL Servers tab, click **Import**.
3. On the Select File to Import window, click **Browse** and locate the audit settings file, and then click **Open**.
4. Click **Next**.
5. On the Import Audit Settings window, specify which databases have been configured with the audit settings you want to import. Complete the following steps:
   a. Click **Database Audit Settings**, and then select the **Only import for matching database names** option.
   b. Select the databases whose audit settings you want to apply.
   c. ***If you also want to audit events at the server level as well as events initiated by privileged users***, select these options, and then click **Next**.
6. On the Target Servers window, select the audited SQL Server instances you want to apply the audit settings to from the list, and then click **Next**.
7. On the Target Databases window, ensure the target database list matches the database names you specified to match. Select the audited databases to which you want to apply the imported audit settings, and then click **Next**.
8. On the Summary window, select whether you want your imported audit settings to overwrite the settings on the target SQL Server instances and databases or added to the settings already present. Click **Finish** to import your audit settings.

Manage the SQLcompliance Agent

The SQLcompliance Agent collects SQL events for the Collection Server to process. Your audit and agent property settings control which audit data is collected, and how the audit data is managed and processed. Deploy a SQLcompliance Agent to each SQL Server computer that hosts the instances and databases you want to audit.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

How the SQLcompliance Agent works

The SQLcompliance Agent runs under the SQLcompliance Agent Service account on each registered SQL Server computer that hosts the audited instances and databases. To audit events, the SQLcompliance Agent starts SQL Server traces that run on the target SQL Server. Once a trace starts, SQLcompliance copies events from the SQL trace to trace files, providing a raw audit record.

Trace files are stored in the AgentTraceFiles folder under the install directory (C:\Program Files\Idera\SQLcompliance) on the computer that hosts the SQL Server instance. This folder is secured using ACL settings. You can specify a different location for the trace directory.

The SQLcompliance Agent compresses the trace files and sends them to the Collection Server. After a trace file is successfully sent, the SQLcompliance Agent deletes the file.

You can configure how the SQLcompliance Agent manages these trace files. For example, you can set the maximum trace directory size to limit how much storage space is consumed by unprocessed audit data. When the directory size is reached, the SQLcompliance Agent stops the SQL trace until the existing trace files can be sent to the Collection Server.

By default, the SQLcompliance Agent communicates with the Collection Server every 5 minutes. This communication is a heartbeat. During a heartbeat, the SQLcompliance Agent confirms its health and receives audit setting updates. You can manually apply audit setting updates as needed using the Management Console.

If the SQLcompliance Agent continues to run without a heartbeat, SQL compliance manager considers the agent to be unattended. By setting the unattended time limit, you can control how long traces are allowed to run until SQL Server stops the trace. Use this setting to automatically stop auditing when the SQLcompliance Agent is not responding or has been deleted.

When you deploy the SQLcompliance Agent, SQLcompliance installs the SQLcompliance Agent service on the computer hosting the target SQL Server instance. You can install the agent manually through the setup program or dynamically through the Management Console.

SQLcompliance Agent version compatibility

The 3.0 or later version of the Management Console and the Collection Server supports all earlier versions of the SQLcompliance Agent. This compatibility allows you to upgrade your SQL Compliance Manager implementation in stages according to your change control policies.

Deploy the SQLcompliance Agent manually

To deploy the SQLcompliance Agent manually, run a Agent Only or Custom setup to install the agent on the physical computer that hosts the SQL Server instance or database you want to audit. Use manual deployment when you want to install the SQLcompliance Agent in a unique environment, such as on a workstation or a computer that belongs to a non-trusted domain.

If you want to audit a virtual SQL Server, use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent on each cluster node hosting the server. For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

Deploy the SQLcompliance Agent remotely

You can deploy the SQLcompliance Agent to a registered SQL Server instance using the Management Console. Deploying the agent allows you to begin auditing server and database activity on the selected SQL Server instance.

If you want to audit a virtual SQL Server, you must manually deploy the SQLcompliance Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent. For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

If you want to audit a SQL Server instance hosted by a computer that belongs to a non-trusted domain or a workgroup, you must manually deploy the SQLcompliance Agent to the host computer using the SQL Compliance Manager setup program.

To deploy the SQLcompliance Agent:

1. Navigate to **Registered SQL Servers** in the Administration tree.
2. Right-click the SQL Server instance to which you want to deploy the SQLcompliance Agent.
3. Select **Deploy Agent** from the context menu.
4. Type and confirm the account name and password. You want the SQLcompliance Agent service account to use the connect to your audited instances.
5. Specify the trace directory and click **Next**.
6. Review your settings, and then click **Finish** to deploy the SQLcompliance Agent.

Upgrade the SQLcompliance Agent locally

You can use the SQL Compliance Manager setup program to upgrade the SQLcompliance Agent on the local computer that is running the registered SQL Server instance. Use this approach when you are upgrading the SQLcompliance Agent on a registered SQL Server where you manually installed the agent. For more information, see Upgrade to this build.

Upgrade the SQLcompliance Agent remotely

You can upgrade the SQLcompliance Agent remotely using the Management Console. Use this approach to upgrade agents on any registered SQL Server where you remotely installed the agent.

If you manually installed the SQLcompliance Agent, use the SQL Compliance Manager setup program to manually upgrade the agent. For more information, see Upgrade the SQLcompliance Agent locally.

To upgrade the SQLcompliance Agent:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Right-click the SQL Server instance to which you want to upgrade the SQLcompliance Agent.
3. ***If the Agent is not up to date***, you can select **Upgrade Agent** from the context menu. ***If the Agent is up-to-date***, the option **Upgrading the Agent** is unavailable.

Ensure the SQLcompliance Agent has current audit settings

You can ensure the SQLcompliance Agent is using your most recent audit settings by performing a manual update. This update does not impact the heartbeat interval. By default, the agent receives updates every five minutes.

To ensure the SQLcompliance Agent has current audit settings:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance to which you want to update the SQLcompliance Agent.
3. Click **Update Now** on the **Audit Settings** ribbon.

Check trace file integrity

The SQLcompliance Agent manages the SQL trace that collects audit data. ***If the SQL trace is stopped, modified, paused, or deleted by another application***, the SQLcompliance Agent restarts the trace and checks the trace status. The Collection Server then logs an event indicating the current trace status.

You can set the trace tamper detection interval from the SQLcompliance Agent Properties window. For more information, see Configure how the SQLcompliance Agent manages trace files.

If an issue has occurred, one of the following events will display on the Agent Events tab of the SQL Compliance Manager Activities tab.

This Agent Event …	Means …
Trace stopped	The SQL trace was stopped but still exists on the audited SQL Server instance.
Trace missing	The SQL trace that was running no longer exists on the audited SQL Server instance. The SQLcompliance Agent started a new trace.
Trace altered	A SQL trace setting was altered.

SQL Compliance Manager audits all activity on your server. Learn more > >

Check the SQLcompliance Agent status

You can quickly check the status of a SQLcompliance Agent that is deployed to a registered SQL Server instance you are auditing. This feature provides a summary of the agent health. For more detailed information to help troubleshoot an issue, see the agent properties.

To check the SQLcompliance Agent status:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQLcompliance Agent you want to check.
3. Click **Check Agent** on the **Agent** ribbon.
4. Review the status, and then click **OK**. To obtain more detailed information about the agent, review the agent properties. To refresh the status displayed in the Registered SQL Servers tab, click Refresh on the View menu.

Check the SQLcompliance Agent version

You can quickly check the version of a SQLcompliance Agent that is deployed to a registered SQL Server instance you are auditing. The SQLcompliance Agent version consists of the release number and build number assigned to SQL Compliance Manager. The SQLcompliance Agent version should be the same as the product version. For more information, see Check the product version.

To check the SQLcompliance Agent status:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQLcompliance Agent you want to check.
3. On the Agent menu, click **Agent Properties**.
4. On the General tab, review the SQLcompliance Agent version number, and then click **OK**. For more detailed information to help troubleshoot an issue, see additional agent properties on the Deployment and Trace Options tabs.

Configure how the SQLcompliance Agent manages trace files

You can configure how the SQLcompliance Agent manages trace files. These settings include file size thresholds and how often the SQLcompliance Agent calls the Collection Server with a heartbeat.

If you specify a different location for the trace directory, ensure the SQLcompliance Agent Service account has read and write privileges on that folder. SQL Compliance Manager does not change the security settings on existing folders.

If you are auditing a virtual SQL Server, ensure the specified folder is located on a shared data disk for the specified virtual SQL Server. SQL CM applies this change to the active node in the cluster hosting the virtual SQL Server. SQLcompliance Agent properties are later replicated from the active node to the passive nodes.

To configure how the SQLcompliance Agent manages trace files:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQLcompliance Agent you want to check.
3. On the **Agent** menu, click **Agent Properties**.

If you want to …	Use this tab …
Change heartbeat interval	General
Change logging level	General
Configure trace collection settings	Trace Options
Limit trace directory size	Trace Options
Review agent status, version, and last heartbeat time	General
Review current trace directory path	Trace Options
Review how the agent was deployed on this SQL Server instance	Deployment
Review which SQL Server instances the agent audits	SQL Servers
Set how long the agent can run unattended	Trace Options
Set how long the agent waits before restarting a SQL trace that has been stopped, modified, paused, or deleted	Trace Options
Verify agent service account	Deployment

4. ***If you want to designate a different folder for the SQLcompliance Agent trace directory***, complete the following steps.
    a. On the **Agent** menu, click **Change Trace Directory**.
    b. Specify the path for the new agent trace directory location.
5. Click **OK**.

SQL Compliance Manager audits all activity on your server. Learn more > >

Licensing

SQL Compliance Manager provides an intuitive, simple to use interface for license key management. You can view the status of the license key associated with each SQL Server instance and upgrade licenses to audit additional instances. SQL Server instances are the only licensed components in the SQL CM architecture.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

How licensing works

By default, SQL Compliance Manager installs with a limited-time, limited-instance trial license key. The Management Console displays your trial license statistics in the Manage SQL Compliance Manager Licenses window.

When you decide to move from a trial implementation of SQL CM to your production environment, contact and obtain a license key from Idera. You enter the license key using the Manage SQL Compliance Manager Licenses window. This license key is stored in the Repository.

SQL Compliance Manager checks for a valid license key each time you register a SQL Server instance. ***If the SQL Server instance is not currently licensed***, and you have enough licenses to proceed, SQL CM associates the instance with an available license. ***If the attempted registration exceeds your licensed limit***, SQL CM does not register the specified instance and you cannot initiate auditing.

When you reach your license limit, SQL Compliance Manager disallows the registration of additional SQL Server instances. ***If your license expires***, SQL CM disables all auditing of new events and disallows registration of additional SQL Server instances. You can continue to view and report on previously-collected audit data.

Upgrade your license

You may need to upgrade your license due to any number of circumstances. For example, consider the following scenarios:

- You exhaust your trial license and have decided to use SQL Compliance Manager to audit and report on database activity
- You exhaust your purchased license due to company growth or the need to audit additional SQL Server instances to remain in compliance

To upgrade your license:

1. Click **File** on the menu bar, and then select **Manage Licenses**.
2. On the Manage Licenses window, click **Add** and enter your new license key.
3. Click **OK**.

Register your SQL Servers

Registering a SQL Server instance allows you to audit this instance and the associated databases. For each database you want to audit, register the corresponding SQL Server instance. When you register the instance, you can also deploy the SQLcompliance Agent to begin auditing SQL events on this instance.

Use the Console to register your SQL Servers

1. Ensure the SQL Server instance you want to register meets the hardware and software requirements.
2. Decide which SQL Server events you want to audit on this instance.
3. Start the Management Console, and then click **New > Registered SQL Server**.
4. Specify or browse to the SQL Server instance you want to register with SQL Compliance Manager, and then click **Next**. You can also specify the description SQL CM uses when listing this instance in the Management Console.
5. ***If the SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server***, select the checkbox. Click **Next**.
6. Indicate whether you want to deploy the SQLcompliance Agent now or later, and then click **Next**. You can also choose to deploy the SQLcompliance Agent manually, allowing you to install the agent at the physical computer that is hosting the registered SQL Server instance.

   > ***If you are auditing a virtual SQL Server or a SQL Server instance running in a non-trusted domain or workgroup***, you must manually deploy the SQLcompliance Agent to the computer hosting the instance. For more information, see Deploy the SQLcompliance Agent manually.

7. ***If you chose to deploy the SQLcompliance Agent now***, specify the appropriate service account credentials for the agent, and then click **Next**. For more information, see Permissions requirements.
8. ***If you chose to deploy the SQLcompliance Agent now***, indicate whether you want the SQLcompliance Agent to use the default trace directory, and then click **Next**. By default, the trace directory path is:
   `C:\Program Files\Idera\SQLcompliance\AgentTraceFiles`
   If you designate a different directory path , ensure the SQLcompliance Agent Service account has read and write privileges on the specified folder.
9. Select the server databases you want to audit, and then click **Next**. ***If you do not want to audit any databases***, clear the **Audit Databases** check box.
10. Select the collection level of server activities you want to audit, and then click **Next**.
11. ***If you chose to create a custom audit collection***, select the server activities you want to audit, and then click **Next**. You can also indicate whether you want to audit successful or failed access checks.
12. ***If you chose to create a custom audit collection***, specify which privileged users you want to audit, and then click **Next**. ***If you are auditing a virtual SQL Server or a SQL Server instance running in a non-trusted domain or workgroup***, configure privileged user audit settings after you have deployed the SQLcompliance Agent.
13. ***If you chose to create a custom audit collection***, select the database activities you want to audit, and then click **Next**. You can also indicate whether you want to audit successful or failed access checks, capture SQL statements for DML and SELECT activity, or capture the transaction status for DML activity.
14. ***If you chose to create a custom audit collection***, specify which privileged users you want to audit, and then click **Next**.
15. Specify whether you want to grant the assigned SQL logins read access to events audited on this SQL Server instance, and then **Next**. For more information, see How Console security works.
16. Click **Finish**.

Use the CLI to register a SQL Server instance

You can use the command line interface to register a new SQL Server instance and apply audit settings. The audit settings can be configured using the Typical auditing settings or an audit template (audit settings you exported to an XML file).

Keep in mind the following requirements and limitations:

- This process requires manually deploying the SQLcompliance Agent to this instance.
- You cannot apply the built-in HIPAA or PCI regulation guidelines at the server level using the CLI.
- The `register` command supports case-sensitive named instances. Ensure you are using the appropriate case when you cite the instance name.
- The `registerinstance` command does not support registering a virtual SQL Server instance hosted on a Windows cluster.

SQL Compliance Manager includes a sample instance audit settings template (Sample_Server_AuditSettings.xml) for your convenience. Use this sample template to familiarize yourself with how specific audit settings are defined. By default, the sample template is located under `C:\Program Files\Idera\SQLcompliance`.

To register an instance and apply the Typical (default) audit settings:

1. Use the SQL CM setup program to the target instance.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance`.

To register an instance and apply a FERPA regulation guideline:

> The FERPA regulation guideline is provided as an XML template (`FERPA_Server_Regulation_Guideline.xml`) stored in the SQL CM installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the FERPA template reflects the directory you chose during installation.

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "FERPA regulation guideline file path"`.

To register an instance and apply a SOX regulation guideline:

> The SOX regulation guideline is provided as an XML template (`SOX_Server_Regulation_Guideline.xml`) stored in the SQL Compliance Manager installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the SOX template reflects the directory you chose during installation.

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "SOX regulation guideline file path"`.

To register an instance and apply a custom audit template:

1. Determine which currently audited SQL Server instance has the audit settings you want to apply to the new instance.
2. Export your audit settings from the source instance.
3. Use the SQL Compliance Manager setup program to manually deploy the SQLcompliance Agent to the target instance.
4. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "exported audit settings file path"`.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Manage the registry key

SQL Compliance Manager checks the permissions available on each SQL Server instance you want to monitor. This check runs automatically each time you register a new instance.

If the check fails, review the issue, and then access the `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance` to make the permission changes. For more information about the required permissions, see Configuration wizard - Permissions Check window.

To make a change to the registry key:

1. Start `services.msc` using the Run command. The system displays the Services window.
2. Right-click the **SQLcompliance Collection Service**, and then select **Properties**.
3. In the SQLcompliance Collection Service Properties dialog box, click the Log On tab.
4. Log on to the SQLcm Service by typing the service account credentials, and then clicking **OK**.
5. Open the registry editor by typing **regedit** in the Run command window, and then clicking **OK**. The system displays the Registry Editor window.
6. In the directory tree, expand `HKEY_LOCAL_MACHINE\SOFTWARE\Idera\SQLcompliance`.
7. Right-click the **SQLcompliance** folder, and then select **Permissions**. The system displays the Permissions for SQLcompliance dialog box.
8. On the Security tab, click **Add**. This step allows you to add a user or group.
9. In the Select Users or Groups dialog box, search for the appropriate account by clicking **Advanced > Find Now**. The Select Users or Groups dialog box displays a list of relevant results.
10. In the **Search Results** field, select the service account used by SQLcm Services, and then click **OK**. The system adds the object to the list.
11. Click **OK**. Note that the account you selected appears in the **Group or user names** field of the Permissions for SQLcompliance dialog box.
12. Select the account name, and then add the appropriate permissions by checking the **Allow** checkbox for the permission(s).
13. Click **OK** after you make your selections. You can verify the permissions by right-clicking **SQLcompliance** in the Registry Editor, selecting **Permissions**, and then viewing the allowed permissions.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Audit SQL Server Events

Auditing your SQL Server instances and databases is the first step in ensuring your SQL Server environment remains in continuous compliance with federal and corporate security and privacy policies. You can also generate reports on the audit data you collect, allowing you to demonstrate compliance on demand. For more information, see Report on Audit Data.

Auditing checklist

Use the following checklist to help you prepare your environment to successfully audit your SQL Server instances and databases. ***If you plan to audit virtual SQL Servers running in Microsoft failover clusters***, see Audit a virtual SQL Server instance for detailed installation and configuration tasks.

1. Gather the information necessary to set up your auditing.

✓	Task	Description	For more information ...
✓	Verify privileges on your Windows login account	Ensure that your Windows login account has sysadmin privileges on all SQL Server instances you want to audit.	Permissions requirements
✓	Review the list of auditable events	Review how the audit process works and which SQL events you can audit. Note that you can audit events at the server or database level.	How auditing works
✓	Identify the items you want to audit on your SQL Server instances	Identify the audit settings you want to apply to individual **instances** in your SQL Server environment. These settings should specify which server events you want to collect and report. Remember that the more data you collect, the more overhead is required. SQL Compliance Manager allows you to change your auditing settings at any time to help you make sure you collect exactly what an auditor needs.	Server-level audit settings
✓	Identify the items you want to audit on your databases	Identify the audit settings you want to apply to individual **databases** in your SQL Server environment. These settings should specify which database events you want to collect and report. Remember that the more data you collect, the more overhead is required. SQL Compliance Manager allows you to change your auditing settings at any time to help you make sure you collect exactly what an auditor needs.	Database-level audit settings
✓	Identify excluded events	Identify any events you want to exclude from your audit data.	Event Filters

2. Register your SQL Server instances.

✓	Task	Description	For more information ...
✓	Register your SQL Server instances	Register each SQL Server instance that hosts the databases you want to audit.	Register your SQL Servers

3. Enable auditing.

✓	Task	Description	For more information ...
✓	Enable server-level auditing	***If you want to audit your SQL Server instances***, enable auditing at the server level.	Enable auditing on a SQL Server
✓	Enable database-level auditing	***If you want to audit your databases***, enable auditing at the database level.	Enable auditing on a database

4. Apply regulation guidelines.

✓	Task	Description	For more information ...
✓	Apply regulation guidelines	Apply regulation guidelines to the appropriate audited databases.	Comply with specific regulations

Configure filters and test your settings.

✓	Task	Description	For more information ...
✓	Configure Event Filters	Configure the appropriate Event Filters, depending on which event category you want to exclude from your audit data.	Event Filters
✓	Test your audit settings	Test your audit settings to ensure you will collect the SQL Server events you need.	Test your audit settings

5. Monitor your settings.

✓	Task	Description	For more information ...
✓	Monitor event collection and adjust if necessary	Monitor how many events are collected on a daily basis. Depending on the growth rate of your audit data, consider creating Event Filters to better manage audit data in large environments.	Event Filters
✓	Monitor the Repository database growth	Monitor the growth of the SQL Compliance Manager Repository databases. If the databases are growing too fast, change your auditing settings to limit growth and optimize performance.	Reduce audit data to optimize performance
✓	Determine whether you need alerts	Determine whether you need to alert on the events you are collecting. SQL CM allows you to build rules that provide real-time alert notifications to help you quickly identify and resolve security issues.	Alert on Audit Data and Status
✓	Determine whether you need to capture before-and-after object values	***If you are auditing DML activity***, determine whether you want to capture the value of the database object before and after a specific transaction.	Audited Database Properties window - Before-After Data tab

✓	Determine who needs access rights to administer or report on audit data	Determine which SQL users should have access rights to administer or report on audit data. This security feature is important as both sensitive and audit data should be secure.	Secure Audit Data

6. Implement reports.

✓	**Task**	**Description**	**For more information ...**
✓	Review report implementation	Review how you can implement Reports in your SQL Server environment using SQL Server Reporting Services.	Report on Audit Data

7. Archive events.

✓	**Task**	**Description**	**For more information ...**
✓	Archive collected events	Configure how you want SQL CM to archive audit data. Note that SQL CM creates an archive database for each registered SQL Server instance.	Archive collected events

How auditing works

SQL Compliance Manager audits each registered SQL Server instance and the associated databases according to the audit settings you configure. Your audit settings should directly correlate with the SQL events you need to track in order to meet your compliance objectives. For example, you can register a SQL Server instance for auditing but not audit the hosted databases. Likewise, you can audit a single database on a registered SQL Server instance that hosts multiple databases.

Complying with regulations

If you are subject to comply with regulations such as PCI DSS or HIPAA, you can use SQL CM to configure your audit settings according to the specific guidelines of the regulation. SQL CM then collects event data based on these guidelines and can provide a report that details the section of the regulation and the data collected using SQL CM. You can apply the regulation guideline audit settings to one or more databases on a registered SQL Server instance.

Understanding traces

On each registered SQL Server instance, the SQLcompliance Agent starts a SQL Server trace to copy SQL event log entries, called audit events, to trace files. Trace files are temporary files that store audit events until these events can be sent to the Collection Server. Trace files are located in a trace file directory on the audited SQL Server computer. For more information, see How the SQLcompliance Agent works.

SQL Compliance Manager collects all events in the SQL trace that are related to the activity you want to audit. When choosing the activities you want to audit, be aware that activities performed through the SQL Server client tools, such as Management Studio, may log multiple events. For example, when you add a login to a role, the SQL trace records one event for the add login action and another event for changing the default language. In this case, SQL CM collects each event as separate audit data according to the SQL trace.

Using the Collection Server

The Collection Server stores the compressed trace files in the CollectionServerTraceFiles folder until the files can be processed. This folder is located under the install directory (`C:\Program Files\Idera\SQLcompliance`) on the computer that hosts the Collection Server. The CollectionServerTraceFiles folder is also called a trace file directory, and is secured using ACL settings. You can specify a different location for the trace directory.

The Collection Server processes the raw audit events according to your settings and then sends the results to the appropriate event database in the Repository. The Collection Server creates an event database for each registered SQL Server instance. You can specify which audit events you want to track. You can also configure how the Collection Server and SQLcompliance Agent manage the trace files.

Filtering and grooming data

For optimal data management, SQL Compliance Manager supports archiving and grooming of event data. Depending on the size of your environment, the amount of event data you audit, and your reporting cycles, you may want to archive and groom event data on a routine basis. For more information, see Manage Audit Data.

Understanding trusted and privileged users

Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited database. As these users are trusted, the events generated by accounts are removed by the SQL CM Agent from the audit trail before sending the trace file to the Collection Server for processing.

By designating trusted users, you can more efficiently audit databases used by third-party applications, such as SAP, that are self-auditing. self-auditing applications are able to audit activity and transactions initiated by their service accounts. Because service accounts can generate a significant number of login and database change events, omitting these expected events from your audit data trail lets you more easily identify unexpected activity.

When you designate trusted users, consider limiting your list to a few specific logins. This approach optimizes event processing performance and ensures you filter the intended accounts.

In comparison, privileged users are SQL Server logins and members of SQL Server roles that have certain privileges or authorization that you want to audit. You can audit individual SQL Server logins with privileged access as well as logins that belong to specific server roles. A sudden spike in privileged user activity could indicate a security breach. For more information about selecting privileged users for audit, see the Configuration wizard - Privileged Users window and the Registered SQL Server Properties window - Privileged User Auditing tab.

If you are auditing privileged user activity and the trusted user is also a privileged user, SQL CM will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted. Keep in mind that trusted users are filtered at the database level whereas privileged users are audited at the server level.

Understanding before and after data

Collect before and after data when it is critical to capture the exact data change in a table column. When this feature is enabled, you can evaluate the before value and after value for each change in the Audit Events view. Enabling this feature can impact your Collection Server and

Management Console performance.

⚠ It is important to note that the Before-After Data capture feature modifies the application schema by creating triggers on any table for which such data collection is enabled.

Audit collection levels

When you add a database to audit, you can select the Default, Custom, or Regulation audit collection level. Use the audit collection level to control which SQL Server events you audit at the database level.

Default collection level

Allows you to collect the SQL Server events most commonly requested by auditors. This collection level audits the following activities and SQL events:

- Security changes
- Database Definition (DDL)
- Administrative activities
- Successful operations only (operations that pass the SQL access check)

Custom collection level

Allows you to select the specific activities and SQL events you want to audit on these databases. The Custom collection level is recommended for advanced users, or for cases in which only one type of data is required for compliance. Before using the Custom collection level, review the event data gathered by the Default collection level.

Regulation

Configures your audit settings to collect the event data required by specific regulatory guidelines Comply with specific regulations, such as PCI DSS or HIPAA. You can review a list of the collected events on the Regulation Guidelines window of the SQL Compliance Manager Configuration wizard. On the Summary window at the end of the wizard, click **View the Regulation Guideline Details** to review a summary of all the regulation guidelines applied to the selected database.

SQL Server events you can audit

SQL Compliance Manager allows you to audit specific types of SQL Server event data, and distinguish between successful operations and failed operations. Whether an operation succeeds or fails is dependent upon whether the login permissions are correct.

Data types and corresponding events

SQL Compliance Manager captures the following types of event data.

Data Type	Events Audited	Description
Logins	• Successful logins • Failed logins Impersonation	Audits login activity if an access check is performed and the event status is recorded (success or failure) at the server level
Administration	• Backups Restores • DBCC • Change server settings • Alter trace Database operation	Audits common administrative tasks on the SQL Server instance
Security	• Add login • Add role • Grant, Revoke, Deny • Change role password • Change login properties • Change owner	Audits all SQL security model activity
Database Definition (DDL)	• Derived permission • SQL statement permission • Database access	Audits create, drop, and alter operations performed on SQL Server objects, database objects, and schema object
DML	Object permissions	Audits common database operations, such as: • UPDATE • INSERT • DELETE
Select	SELECT	Audits all SELECT statements executed on database table
Privileged User	All	Audits all privileged user activity at any level ***If the privileged user is also a trusted user***, SQL Compliance Manager continues to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted.
User defined	All	Audits all custom events generated using the `sp_trace_generateevent` stored procedure

Data levels

You can capture different event data at one or more of the following levels:

- SQL Server instance
- Database
- Database object, such as a table

This flexibility allows you to achieve precise and granular compliance. For example, you can configure different audit settings for multiple databases hosted on a single registered SQL Server instance.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Database-level audit settings

You can specify which SQL events you want to audit at the database level. SQL Compliance Manager applies these settings to the audited database on the registered SQL Server instance.

You can configure database audit settings when you add a new database or later as your auditing needs change. For more information about individual SQL events, see Microsoft SQL Server Books Online.

SQL CM audits the following SQL events at the database level.

Event class	SQL Server version	Description
Audit Add DB User	SQL Server 2000 only	Records when a database user is added or dropped from the audited database. In SQL Server 2005 and later, this event class is Audit Database Principal Management
Audit Add Member to DB Role	SQL Server 2000 and later	Records when users are added to or removed from a database role
Audit Add Role	SQL Server 2000 only	Records when a database role is added to or removed from the audited database. In SQL Server 2005 and later, this event class is Audit Database Principal Management
Audit App Role Change Password	SQL Server 2000 and later	Records all application password changes
Audit Backup/Restore	SQL Server 2000 and later	Records BACKUP and RESTORE operations, including backups and restores performed through SQLsafe
Audit DBCC	SQL Server 2000 and later	Records all DBCC commands executed on the audited database
Audit Database Object Access	SQL Server 2005 and later	Records when an operation, login, or application accesses a database object
Audit Database Object GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements on the audited database object
Audit Database Object Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on database objects In SQL Server 2000, this event class is Audit Object Derived Permission
Audit Database Object Take Ownership	SQL Server 2005 and later	Records when ownership of an audited database object changes
Audit Database Operation	SQL Server 2005 and later	Records all operations executed on an audited database
Audit Database Principal Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on database principals
Audit Database Scope GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements on the audited database In SQL Server 2000, this event class is Audit Statement GDR
Audit Object Derived Permission	SQL Server 2000 only	Records ALTER, CREATE, and DROP commands executed on a database object, such as CREATE TABLE or ALTER TABLE In SQL Server 2005 and later, this event class is Audit Database Object Management and Audit Schema Object Management
Audit Object GDR	SQL Server 2000 only	Records all GRANT, REVOKE, or DENY actions on user permissions for a database object In SQL Server 2005 and later, this event class is Audit Schema Object GDR

Audit Object Permission	SQL Server 2000 only	Records whether a user is authorized to execute the following commands on a database object: • SELECT ALL • UPDATE ALL • REFERENCE ALL • INSERT • DELETE • EXECUTE (stored procedures only) In SQL Server 2005 and later, this event class is Audit Schema Object Access
Audit Schema Object Access	SQL Server 2005 and later	Records whether a user is authorized to execute the following commands on a schema object: • SELECT ALL • UPDATE ALL • REFERENCE ALL • INSERT • DELETE • EXECUTE (stored procedures only) In SQL Server 2000, this event class is Audit Object Permission
Audit Schema Object GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on user permissions for a schema object In SQL Server 2000, this event class is Audit Object GDR
Audit Schema Object Management	SQL Server 2005 and later	Records ALTER, CREATE, and DROP commands executed on a server object In SQL Server 2000, this event class is Audit Object Derived Permission and Audit Statement Permission
Audit Schema Object Take Ownership	SQL Server 2005 and later	Records when the ALTER AUTHORIZATION statement is used to change ownership of a schema object
Audit Statement GDR	SQL Server 2000 only	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements on the audited database In SQL Server 2005 and later, this event class is Audit Database Scope GDR
Audit Statement Permission	SQL Server 2000 only	Records when a user is authorized to execute a T-SQL statement on the audited database In SQL Server 2005 and later, this event class is Audit Schema Object Management
SQL Transaction	SQL Server 2000 and later	Records the status of explicit and implicit DML transactions executed in T-SQL scripts, including: • Begin • Commit • Rollback • Savepoint

Server-level audit settings

You can specify which SQL events you want to audit at the server level. SQL Compliance Manager applies these settings to the registered SQL Server instance. These settings are not applied to the hosted databases.

You can configure server audit settings when you register a new SQL Server instance or later as your auditing needs change. For more information about individual SQL events, see Microsoft SQL Server Books Online.

Event class	SQL Server version	Description
Audit Add Login	SQL Server 2000 only	Records when a SQL Server login is added to or dropped from a registered SQL Server instance In SQL Server 2005 and later, this event class is Audit Server Principal Management
Audit Add Login To Server Role	SQL Server 2000 and later	Records when a login is added to or removed from a server role
Audit Change Database Owner	SQL Server 2005 and later	Records when the ALTER AUTHORIZATION statement is used to specify a different database owner
Audit Database Management	SQL Server 2005	Records all DROP, ALTER, and CREATE operations on a database
Audit Login	SQL Server 2000 and later	Records all successful logins on the registered SQL Server instance
Audit Login Change Password	SQL Server 2000 and later	Records all password changes for logins on the registered SQL Server instance
Audit Login Change Properties	SQL Server 2000 and later	Records changes in default database and language properties for all logins on the registered SQL Server instance
Audit Login Failed	SQL Server 2000 and later	Records all logins that failed an access check on the registered SQL Server instance
Audit Login GDR	SQL Server 2000 only	Records all GRANT, REVOKE, or DENY actions on Windows 2000 user account login rights In SQL Server 2005 and later, this event class is Audit Server Principal Management
Audit Object Derived Permission	SQL Server 2000 only	Records CREATE and DROP commands executed on a server object, such as CREATE DATABASE or DROP DATABASE In SQL Server 2005 and later, this event class is Audit Database Management
Audit Server Alter Trace	SQL Server 2005 and later	Records when an ALTER TRACE permission check is executed for a T-SQL statement that creates, configures, or filters a SQL trace
Audit Server Object GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements on the audited schema object, such as a table or function
Audit Server Object Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on server objects
Audit Server Object Take Ownership	SQL Server 2005 and later	Records when ownership of an audited server object changes
Audit Server Operation	SQL Server 2005 and later	Records all security operations executed on the audited server
Audit Server Principal Impersonation	SQL Server 2005 and later	Records when impersonation is used to access or act on a server object
Audit Server Principal Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on server principals

Audit Server Scope GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements that change the server scope, such as creating a login
Audit Statement Permission	SQL Server 2000 only	Records when a user is authorized to execute a T-SQL statement on the registered SQL Server instance In SQL Server 2005 and later, this event class is Audit Database Management

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

User-defined events

You can audit, alert on, and filter user-defined events. User-defined events are SQL events generated by the `sp_trace_generateevent` stored procedure. Use this stored procedure to create custom SQL events that track data that may not be available in a standard SQL trace. For more information, see Microsoft Books Online.

Comply with specific regulations

SQL Compliance Manager audits and identifies events that affect SQL Server objects and data. By selecting a specific regulation guideline set, SQL CM applies audit settings to your selected databases according the corresponding data security rules. This audited data is collected and securely stored for forensic analysis and reporting. SQL CM also provides tamper-proof data security features as well as methods for watching events without exposing account information.

You can apply a regulation guideline when you register a new SQL Server instance or audit a database though the Console or CLI. The following tables list each section of a regulation and the associated SQL Server events that SQL CM audits, as well as specific audit features.

> Idera, Inc. customers have the sole responsibility to ensure their compliance with the laws and standards affecting their business. Idera, Inc. does not represent that its products or services ensures that customer is in compliance with any law. It is the responsibility of the customer to obtain legal, accounting, or audit counsel as to the necessary business practices and actions to comply with such laws.

FERPA Compliance

Section	Summary	Associated Audit Events and Features
99.2	**What is the purpose of these regulations?** The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.	Server Events: • Successful and Failed Logins • Security changes Database Events: • Security changes
99.31(a)(1)	**School officials** Institutions that allow "school officials, including teachers, within the agency or institution" to have access to students' education records, without consent, must first make a determination that the official has "legitimate educational interests" in the information. The list of officials must be included in the annual FERPA notification.	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • SELECT statements • Security changes • Sensitive Columns
99.31(a)(1)(ii)	**Controlling access to education records by school** Institutions are now required to use "reasonable methods" to ensure that instructors and other school officials (including outside service providers) obtain access to only those education records (paper or electronic) in which they have legitimate educational interests. Institutions are encouraged to restrict or track access to education records to ensure that they remain in compliance with this requirement. The higher the risk, the more stringent the protections should be (e.g., SSNs should be closely guarded).	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • DDL • DML • SELECT statements • Sensitive Columns • Before-After Data auditing

99.31(a)(2)	**Student's new school** An institution retains the authority to disclose and transfer education records to a student's new school even after the student has enrolled and such authority continues into the future so long as the disclosure is for purposes related to the student's enrollment/transfer. After admission, the American Disabilities Act (ADA) does not prohibit institutions from obtaining information concerning a current student with disabilities from any school previously attended by the student in connection with an emergency and if necessary to protect the health or safety of a student or other persons under FERPA. A student's previous school may supplement, update, or correct any records it sent during the student's application or transfer period and may identify any falsified or fraudulent records and/or explain the meaning of any records disclosed previously to the new school.	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • SELECT statements • Sensitive Columns • Before-After Data auditing
99.32(a)(1)	**What record keeping requirements exist concerning requests and disclosures?** An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in § 99.31(a)(3) that may make further disclosures of personally identifiable information from the student's education records without consent under § 99.33(b)(2). The agency or institution shall maintain the record with the education records of the student as long as the records are maintained.	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • SELECT statements • Sensitive Columns • SELECT statements

HIPAA Compliance

Section	Summary	Associated Audit Events and Features
164.306 (a, 2)	**Security Standards** Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • DML • Sensitive Columns
164.308 (1, i)	**Security Management Process** Implement policies and procedures to prevent, detect, contain and correct security violations.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • None

164.308 (B)	**Risk Management** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Server Events: • Failed Logins • Security Changes • DDL • Privileged User activity Database Events: • None
164.308 (D)	**Information System Activity Review** Implement procedures to regularly review records of information system activity such as audit logs, access reports and security incident tracking reports.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • Security • DDL • Administrative activities • DML • Sensitive Columns
164.308 (3, C)	**Termination Procedures** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.	Server Events: • Security Changes Database Events: • Security
164.308 (5, C)	**Implementation Specifications** Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Server Events: • Logins • Failed Logins Database Events: • None
164.312 (b)	**Technical Standard** **Audit controls**. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Server Events: • Failed Logins • Security Changes • DDL • Administrative activities Database Events: • Security • DDL • Administrative activities • DML • Sensitive Columns

164.404 (a) (1) (2)	**Security and Privacy** **General rule**. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. **Breaches treated as discovered**. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Server Events: • None Database Events: • Security • Sensitive Columns
164.404 (c) (1) (A), (B)	**Security and Privacy** (c) Implementation specifications: Content of notification (1) Elements. The notification required by (a) of this section shall include, to the extent possible: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information.	Server Events: • None Database Events: • Sensitive Columns
HITECH 13402 (a) (f), (1), (2)	**Notification In the Case of Breach** (a) In General. A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. (f) Content of Notification. Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following: (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known. (2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).	Server Events: • None Database Events: • Sensitive Columns

PCI DSS Compliance

Section	Summary	Associated Audit Events and Features
8	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.	Server Events: • Failed Logins • Security Changes • DDL • Administrative activities • Privileged Users Database Events: • Security • DDL • Administrative activities • DML • SQL statements • Sensitive Columns
8.5.4	Immediately revoke access for any terminated users.	Server Events: • Security Changes • Administrative activities Database Events: • Security
10	Track and monitor all access to network resources and cardholder data- Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.	See subsections
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user).	Server Events: • Failed Logins • Administrative activities • Privileged Users activity Database Events: • None
10.2	Implement automated audit trails for all system components to reconstruct the following events: • 10.2.1 All individual user accesses to cardholder data • 10.2.2 All actions taken by any individual with root or administrative privileges • 10.2.3 Access to all audit trails • 10.2.4 Invalid logical access attempts • 10.2.5 Use of identification and authentication mechanisms • 10.2.6 Initialization of audit logs • 10.2.7 Creation and deletions of system-level objects	Server Events: • Failed Logins • DDL Database Events: • DDL • DML • Sensitive Columns
10.3	Record at least the following audit trail entries for all system components for each event: • 10.3.1 User identification • 10.3.2 Type of event • 10.3.3 Date and time • 10.3.4 Success or failure indication • 10.3.5 Origination of event • 10.3.6 Identify or name of affected data, system component, or resource	Server Events: • Failed Logins • Privileged Users activity Database Events: • Security • DDL • DML • Sensitive Columns
10.5	Secure audit trails so they cannot be altered.	SQL CM Repository

10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	Enable archive and groom to retain Repository data for a minimum of one year

SOX Compliance

Section	Summary	Associated Audit Events and Features
404	A statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and management's assessment, as of the end of the company's most recent fiscal year of the effectiveness of the company's internal control structure and procedures for financial reporting, Section 404 requires the company's auditor to attest to , and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board. (Source: Securities and Exchange Commission.) **What does this mean from an Information Technology standpoint?** The key is reliability of financial reporting. Financial information resides in the database and it is the responsibility of IT to ensure the right personnel have access to that data at the right time. Any changes to the permissions must be tracked. Additionally, all access to that data (select, insert, update, and delete operations, plus before and after changes) must be audited down to the actual user and stored. If the need arises to determine where an individual has violated the accuracy of the financial data, an audit trail of activity will help to prove that the user: • Accessed the data • Changed permissions • Changed the data	Server Events: • Successful and Failed Logins • Security • DDL • Privileged User activity Database Events: • Security changes • Administrative activities • DML • SQL statements • SELECT statements on all DB objects • SELECT statements on specific tables • Before-After Data auditing • Sensitive Columns • Alerting

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Audit snapshots

Audit snapshots provide a summary of the audit settings for each audited database hosted on the registered SQL Server instances. Routinely reviewing audit snapshots allows you to ensure audit settings are applied correctly and consistently across your SQL Server environment.

You can schedule audit snapshots on a regular basis (in days) or you can capture an audit snapshot to meet an immediate need.

Capture an audit snapshot

You can take a snapshot of your audit settings on demand, to meet immediate audit needs or diagnose issues.

To capture an audit snapshot:

1. Click **Auditing** on the menu bar, and then select **Capture Audit Snapshot**.
2. Specify whether you want a snapshot of audit settings for all registered SQL Server instances or for a specific instance, and then click **OK**.
3. Review the newly captured snapshot.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Schedule an audit snapshot

You can schedule SQL Compliance Manager to take a snapshot of your audit settings at a routine interval (in days), or you can configure SQL CM to not take a snapshot.

To schedule a routine audit snapshot:

1. Click **Auditing** on the menu bar, and then select **Audit Snapshot Preferences**.
2. Specify how often SQL Compliance Manager should take a snapshot of your audit settings, and then click **OK**.

View the audit snapshot

You can view any audit snapshot you have previously captured. SQL Compliance Manager displays audit snapshots as entries in the SQL CM Change Log.

To view the audit snapshot:

1. Select **Change Log** in the **Administration** tree.
2. Locate the audit snapshot you want to view.
3. Right-click the audit snapshot, and then select **Properties** from the context menu.
4. Review the audit snapshot contents, and then click **OK**.

SQL Compliance Manager audits all activity on your server. Learn more > >

Control access to audit data

You can control who can access audit data by granting the appropriate SQL Compliance Manager permissions. You can grant these permissions using the Management Console. You can also create new SQL Server logins on-the-fly to address different auditing demands. For more information, see Secure Audit Data.

Enable auditing on a database

Enabling auditing on the database allows you to capture SQL events at the database level. You can enable database-level auditing when you register the SQL Server instance. For more information, see Register your SQL Servers.

When you enable auditing on a database, you can control the Audit collection levels per each database, choosing whether to apply the built-in default audit settings, enforce a regulatory guideline, or define custom audit settings.

> ⓘ After you enable auditing on your databases, set up the audited database properties to enable more advanced auditing, such as Sensitive Columns and Before-After Data in tables.

If you disable auditing for any reason, you can easily re-enable database-level auditing. On the **Explore Activity** tree, expand the SQL Server instance on which the database resides. Right-click the name of the database on which you want to enable auditing, and then select **Enable Auditing**. This action enables auditing at the server and database levels.

Use the SQL CM Configuration wizard to enable auditing on a database

You can use the SQL Compliance Manager Configuration wizard to add a database and apply one of the following audit settings:

To enable database auditing through the Configuration wizard:

1. In the **Explore Activity** tree, select the SQL Server instance that hosts the new database.
2. Select **Audited Database** from the **New** drop-down.
3. Select the user databases you want to audit, and then click **Next**.
4. Select which audit collection level you want to use, and then click **Next**.
5. ***If you chose to use the Custom audit collection level***, select the appropriate audit settings for these databases, and then click **Next**. SQL CM audits only the activities and results you select. For information, see Database-level audit settings.
6. ***If you chose to use the Custom audit collection level and you are auditing DML and SELECT events***, select the objects SQL CM should audit for these events, and then click **Next**.
7. ***If you chose to use the Custom audit collection level***, select any trusted users you do not want to audit, and then click **Next**.
   - Trusted users are database users, SQL Server logins, or members of SQL Server roles that you trust to read, update, or manage a particular audited database. SQL CM does not audit trusted users. Trusted users are designated on the Add Trusted Users window of the New Audited Database wizard.
   - ***If you are auditing privileged user activity and the trusted user is also a privileged user***, SQL CM continues to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted.
8. Click **Finish**.

Use the import audit settings feature to apply audit settings to a database

You can use the Import your audit settings feature to apply an audit template you previously exported from an audited database. To successfully apply the template, first add the database to SQL Compliance Manager.

Use the CLI to enable auditing on a database

You can use the command line interface to enable auditing on a new database and apply audit settings. The audit settings can be configured using a specific regulation or an audit template (audit settings you exported to an XML file).
Keep in mind the following requirements and limitations:

- This process requires manually deploying the SQLcompliance Agent to the instance that hosts this database.
- The auditdatabase command does not support enabling auditing of a database that belongs to a virtual SQL Server instance hosted on a Windows cluster.
- The auditdatabase command supports case-sensitive named instances. Ensure you are using the appropriate case when you cite the instance and database names.
- The CLI does not support configuring Before-After data auditing.
- You can apply either a built-in regulation guideline or an XML template file.

SQL Compliance Manager includes sample database audit settings templates (`Sample_Database_AuditSettings.xml`) for your convenience. Use this sample template to familiarize yourself with how specific audit settings are defined. By default, the sample template is located under `C:\Program Files\Idera\SQLcompliance`.

To enable database auditing and apply the Typical (default) audit settings:

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] auditdatabase instance database`.

To enable database auditing and apply a HIPAA or PCI regulation guideline:

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.

2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] auditdatabase instance database -Regulation {PCI | HIPAA | PCI, HIPAA}`.

To enable database auditing and apply a FERPA regulation guideline:

> The FERPA regulation guideline is provided as an XML templates (`FERPA_Database_Regulation_Guideline.xml`) stored in the SQL Compliance Manager installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the FERPA template reflects the directory you chose during installation.

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] auditdatabase instance database -config "FERPA regulation guideline file path"`.

Use the CLI to enable auditing on a database

To enable database auditing and apply a SOX regulation guideline:

> The SOX regulation guidelines is provided as an XML template (`SOX_Database_Regulation_Guideline.xml`) stored in the SQL Compliance Manager installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the SOX template reflects the directory you chose during installation.

1. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] auditdatabase instance database -config "SOX regulation guideline file path"`.

To enable database auditing and apply a custom audit template:

1. Determine which currently audited database has the audit settings you want to apply to the new database.
2. Export your audit settings from the source database.
3. Use the SQL CM setup program to manually deploy the SQLcompliance Agent to the instance that hosts the target database.
4. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] auditdatabase instance database -config "exported audit settings file path"`.

Enable auditing on a SQL Server

Auditing is enabled when you register a SQL Server instance, and allows you to capture SQL events at the server level. For more information, see Register your SQL Servers. You can configure server audit settings during registration or later as your auditing needs change. For more information, see Server-level audit settings.

If you disable auditing for any reason, you can easily re-enable server-level auditing. On the **Explore Activity** tree, right-click the SQL Server instance on which you want to re-enable auditing, and then select **Enable Auditing**.

Event Filters

You can use Event Filters to improve scalability, remove unwanted events from the audit data stream, and increase the granularity of your audit settings. Event Filters let you filter raw audit data from the collected trace files before processing begins. Use Event Filters to improve scalability and remove unwanted events from the audit data stream.

Event Filters allow you to further customize your audit data collection. For example, you can configure Event Filters to accommodate the following auditing needs:

- Exclude "noise" events and events generated from expected business activity, such as `INSERTS` and `DELETES` performed on a Sales database by a standard application
- Provide more precise data about specific database activity, such as collecting DDL and DML events for one table but only collecting DDL events for another table

How Event Filters work

Event Filters determine which collected SQL events should be kept for processing by the Collection Server. Like your audit settings, the Event Filters should correlate with the SQL events you need to track in order to meet your compliance objectives.

After receiving the trace files from the SQLcompliance Agent, the Collection Server applies your Event Filters. Any matching events are permanently deleted and eliminated from the data stream. All remaining events are processed for alerts and stored in the appropriate Repository database.

> ⓘ When you enable Sensitive Column auditing on a table, the Collection Server preserves all SELECT events associated with the audited columns even though you may have created an event filter to exclude SELECT events.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Create an Event Filter

An Event Filter allows you to exclude specific events from your audit data. This approach helps you collect only the audit data you need. Event Filters can also help performance by reducing the size of the Repository databases and the processing load on the Collection Server.

To create an Event Filter:

1. Navigate to **Event Filters** in the **Administration** tree.
2. Click **New Event Filter** on the **Actions** ribbon.
3. Select the type of event (event category) that you want to exclude from your audit data, and then click **Next**.
4. Select the type of object affected by the selected event type, and then click **Next**. By default, the event filter will exclude events that occur on any registered SQL Server instance, database, or database object. Use the links provided in the filter details pane to narrow your event filter to specific objects or objects that match a naming convention.
5. Select the software application or SQL Server login that originates the event you want to filter, and then click **Next**.
6. Specify a name and description for this filter, review the summary, and then click **Finish**. By default, the new event filter is enabled.

Use an Event Filter as a template

You can create a new Event Filter by using an existing filter as a template. Event filter templates allow you to more efficiently create multiple filters against the same instance, database, application, or SQL Server login. You can also use event filter templates to apply consistent filter criteria across multiple instances and databases. When you choose to use an Event Filter as a template, SQL Compliance Manager copies the existing filter criteria to the new filter. You can then use the Edit Event Filter wizard to customize the new filter.

To use an Event Filter as a template:

1. Navigate to **Event Filters** in the **Administration** tree.
2. In the Event Filter tab, select the filter you want to use as a template, and then click **Use as Filter Template**, on the **Actions** ribbon.
3. On each wizard window, specify the criteria you want to use for this new filter, and then click **Next**.
4. On the Finish Event Filter window, specify a name and description for this filter, review the summary, and then click **Finish**. By default, the new filter is enabled.

Export your Event Filters

Exported event filter settings are saved in an XML format and can be applied to other registered SQL Server instances. This flexibility saves you time when you are configuring Event Filters on multiple SQL Server instances, and helps ensure consistent Event Filters across your environment. In addition, exporting allows you to back up your Event Filters to use should you need to reinstate an audited SQL Server instance. As you configure your Event Filters, consider what you would like to save for future use, and export the filters for that particular SQL Server instance or database.

To export your Event Filters:

1. Navigate to **Event Filters** in the **Administration** tree.
2. Click **Export Filters** on the **Event Filters** ribbon.
3. Specify a file name or use the default name.
4. Select the location to save the output file. Consider saving all Event Filters to a centralized location such as a network share.
5. Click **Save**.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Import your Event Filters

As you configure or modify Event Filters for your SQL Server instances, you may want to apply the same filters across multiple SQL Server instances in your environment. You can import Event Filters through previously exported XML files and streamline your configuration workflow while reducing errors.

To import your Event Filters:

1. Navigate to **Event Filters** in the **Administration** tree.
2. Click **Import Filters**.
3. Locate the event filter you want to import and click **Open**. By default, the imported Event Filters are disabled.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Change which audit data the filter excludes

Based on the criteria defined in your Event Filters, SQL compliance manager excludes events from your audit data stream. You can exclude events based on the event type (category), the SQL Server instance or database object affected by the event, or the software application or SQL Server login that initiated the event. For more information, see How Event Filters work.

By changing the filter criteria, you can change the type of audit data that is excluded. You can also copy an existing Alert Rule and use it as a template to create a new rule.

To change the type of audit data that an event filter excludes:

1. Navigate to **Event Filters** in the **Administration** tree.
2. Select the filter you want to change, and then click **View Details** from the **Action** ribbon.
3. Select the type of event (event category) that you want to exclude from your audit data, and then click **Next**.
4. Select the type of object affected by the selected event type, and then click **Next**. By default, the event filter will exclude events that occur on any registered SQL Server instance, database, or database object. Use the links provided in the filter details pane to narrow your event filter to specific objects or objects that match a naming convention.
5. Select the software application or SQL Server login that originates the event you want to filter, and then click **Next**.
6. Click **Finish**.

Enable an Event Filter

You can enable filtering on audit data from a specific SQL Server instance or database. By default, filtering is enabled when the event filter is created.

To enable an Event Filter:

1. Navigate to **Event Filters** in the **Administration** tree.
2. On the **Event Filters** tab, select the filter you want to enable, and then click **Enable Filter**.

Disable an Event Filter

You can disable filtering on audit data from a specific SQL Server instance or database. When you disable filtering, SQL compliance manager stops excluding the specified events from your audit data and leaves the event filter intact. SQL compliance manager continues auditing SQL Server events on the specified instances and databases.

To permanently remove an Event Filter from the Repository, delete the filter.

To disable an Event Filter:

1. Navigate to **Event Filters** in the **Administration** tree.
2. On the **Event Filters** tab, select the filter you want to enable, and then click **Disable Filter**.

Disable auditing on a database

You can disable auditing on any database associated with a registered SQL Server instance. When you disable auditing, SQL compliance manager stops the SQL trace but leaves the trace file directory intact. You can continue reporting on audit data stored in the Repository and archive databases.

Although alert rules that monitor this database will remain enabled, no alert messages will be generated because no new audit data will be collected.

To disable auditing on a database, select the database in the **Explore Activity** tree, and then click **Disable Auditing** in the Summary tab. This action disables auditing at the database level only.

Disable auditing on a SQL Server

You can disable auditing on any registered SQL Server instance and the associated databases. When you disable auditing, SQL compliance manager stops the SQL trace but leaves the trace file directory intact. You can continue reporting on audit data stored in the Repository and archive databases.

Although alert rules that monitor this instance will remain enabled, no alert messages will be generated because no new audit data will be collected.

To disable auditing on a SQL Server instance, select the instance in the **Explore Activity tree**, and then click **Disable Auditing** in the Summary tab. This action disables auditing at the SQL Server instance level for all databases.

Fine tune your audit settings

SQL compliance manager provides a lot of flexibility for your audit settings, allowing you to collect a wide range of SQL Server events. However, extensive auditing requires sufficient disk space, processing time, and a very stable network connection. Your environment may not provide the resources necessary to audit every event that occurs on a particular SQL Server instance.

The following auditing options can be resource-intensive and cause significant growth in the Repository databases, thereby decreasing the performance of SQL compliance manager. For more information, see Reduce audit data to optimize performance.

Auditing System Administrators or sa login as a privileged user

Many SQL Server environments are not hardened around the sysadmin fixed role. Consequently, when you audit this role as a privileged user, you will likely collect a significant number of events initiated by benign applications simply because they have been designed to operate using a login in this role. ***If you want to continue auditing System Administrator activity***, consider defining Event Filters to exclude the benign operations you do not need to monitor.

Auditing the system databases for DML or SELECT activity

Gathering events directly from the system databases is only useful under very specific circumstances in an audited environment. Internal operations of SQL Server may be accidentally collected when you audit DML or SELECT events, causing unnecessary data to be collected and stored. ***If you want to continue auditing system databases***, consider archiving or grooming your event databases on a routine basis.

Auditing login events at the server level

Some third-party applications perform a login to the SQL Server instance before any individual operation is initiated. This can cause a very large number of login events to be collected for your audit data trail. ***If you have this type of activity in your environment***, consider specifying a privileged user status to those logins whose activity you need to collect. Note that auditing the Login Failed event category does not result in the same level of data and can remain enabled.

Monitor SQLcompliance Agent activities

You can monitor SQL compliance manager change activity and SQLcompliance Agent events. By default, SQL compliance manager automatically monitors changes applied to the Repository databases as well as SQLcompliance Agent updates.

To track additional activities, such as failed logins, audit the Repository and archive databases. For more information, see Register your SQL Servers.

To monitor SQLcompliance activities:

1. Select the SQL Server instance you want to monitor from the **Explore Activity** tree.
2. View the SQL Server activity summary on the Summary tab and view Alerts, Audit Events, and Archived Events information from each of the respective tabs.

Reduce audit data to optimize performance

Use the following checklist to help you optimize SQL compliance manager performance by fine tuning your auditing settings to prevent excess data collection.

As SQL compliance manager collects audit data and stores this information in the Repository, the event databases grow. When SQL compliance manager is configured to audit all SQL Server events, the event databases can grow very large (up to several gigabytes) in a single 24-hour period, especially in larger environments or environments with high-volume traffic. For more information about event databases in the Repository, see Product components and architecture.

✓	**Follow these steps ...**
✓	Archive or groom stale audit data from the event databases on a regular basis. Archiving allows you to move older events whereas grooming allows you to delete older events. For more information, see How archives work and How grooming works.
✓	Re-index and shrink each event database from which you have archived or groomed data. You can use native Microsoft SQL Server tools or other third-party tools such as Idera SQL defrag manager.
✓	Carefully choose the events you need to audit. The growth and overall size of the event databases is a direct result of the auditing configuration you define. For more information, see Fine tune your audit settings.
✓	Consider configuring Event Filters. Event filters prevent unwanted events from being collected and stored. For example, you can use Event Filters to exclude specific applications and operations that perform benign activities, and therefore do not require auditing, from your audit trial. For more information, see Event Filters.
✓	Consider configuring trusted user filters. Trusted user filters sift out events initiated by specific user accounts on an individual database. In general, a trusted user filter will be more resource-efficient than an event filter when excluding non-useful or benign events from your audit data collection.

Enable self-auditing and monitoring

Auditing your SQL Compliance Manager implementation is called self-auditing. Self-auditing consists of regularly checking the integrity of the Repository databases. You can also audit the Repository databases. For example, you can audit specific events, such as logins, on the Repository. For more information, see Registering Your SQL Servers and Verifying Audit Data Integrity.

Tracking SQL CM activities is called monitoring. By default, the Collection Server gathers specific event data on the Repository databases. SQL CM automatically monitors change activity as well as SQLcompliance Agent events. SQL Compliance Manager lists these activities and events in the Activity and Change Logs. For more information, see Monitoring SQLcompliance Activities.

Using these built-in features, you can ensure your audit settings and data remain secure and uncompromised. You can also ensure your SQL CM implementation complies with your internal and external policies.

Test your audit settings

You can test your audit settings whenever you apply a change. Testing helps ensure you collect the audit data you need to maintain continuous compliance with internal and external standards.

To test your audit settings:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance on which you want to test your audit settings.
3. Ensure the SQLcompliance Agent for the target SQL Server instance is using your most recent audit settings.
4. On the **Auditing** menu, click **Collect Audit Data**. This action will collect SQL Server events based on your current auditing settings.

Verify audit data integrity

SQL compliance manager allows you to verify the integrity of your audit data. This integrity check runs a validation algorithm that determines whether data in your Repository and archive databases has been added, deleted, or modified since the last verification. The integrity check analyzes all collected events as well as additional data for Before-After and Sensitive Column auditing.

Use this integrity check to help ensure your audit data has not been compromised. Consider running an integrity check on a routine basis, depending on the volume or sensitivity of your audit data.

When you run an integrity check, SQL compliance manager logs the event in the Change Log.

You can also run an integrity check using the command line interface. For more information, see Use the CLI to verify audit data integrity.

To verify audit data integrity:

1. Select **Check Repository Integrity** from the **Auditing** drop-down.
2. Select the Repository on which you want to run an integrity check, and then click **Check**.
3. Review the integrity status. ***If your audit data fails the integrity check***, decide whether you want to mark each compromised event in the audit data. Marking these events changes the event class to reflect the type of compromise (event was inserted, modified, deleted) and changes the event category to Integrity Check. For more information, see the online Help for the corresponding window.

View audit data

You can view audit data from the Management Console and Reports.

View the Activity Summary

Select a SQL Server instance in the **Explore Activity** tree. The Activity Summary appears on the **Summary** tab.

View recent audit events

Select a SQL Server instance in the **Explore Activity** tree. Recent audit events appear on the **Summary** tab.

View audited events before archiving

Select a SQL Server instance in the **Explore Activity** tree, and then select the **Audit Events** tab.

View archived events

Select a monitored SQL Server instance or database from the **Explore Activity** tree and then select the **Archived Events** tab. For more information, see Attach existing archives.

Report on events

To report on events, click **Reports** in the console tree pane, and then select the report you want to view. For more information, see Report on Audit Data.

Use custom views

SQL compliance manager allows you to customize the way data is displayed on the Alerts tab, the Audit Events tab, and the Archived Events tab. These customized views can be saved and displayed later to allow you to more efficiently check for important alerts and audit events.

Custom views allow you to edit and save the following:

- Select which columns you want to display
- Select the order you want to group columns by
- Select the sort order of your columns
- Select the width of each column displayed
- Filter the data displayed

Tabs that support custom views

Alerts tab

You can customize the alerts view using the Views, Filters, and Group ribbons at the top of the tab. For example, consider creating a custom Alerts view to filter for severe alerts that have occurred today.

Audit Events tab

You can customize the Audit Events view using the Views, Filters, and Group ribbons at the top of the tab. For example, consider creating a custom Audit Events view to display events created that have a particular login.

Archived Events tab

You can customize the Archived Events view using the Archives, Views. Filters, and Group ribbons at the top of the tab. For example, you can customize your Archived Events tab to limit what is displayed to a particular login so that you can quickly locate problems.

Add a custom view

To add a custom view:

1. Select the grid and filter options using the **Views** ribbon.
2. Click **Save As**.
3. Enter a name for your custom view in the field provide on the View Name window, and then click **OK**.
4. Select your custom view from the view drop-down list on the ribbon.

Edit a custom view

To edit a custom view:

1. Select the custom view you want to edit from the drop-down list on the **Views** ribbon at the top of the view.
2. Select the grid and filter options you would like to use, and then click **Save**.

SQL Compliance Manager audits all activity on your server. Learn more > >

View your activity summary

SQL compliance manager allows you to view the summary across SQL Server activity on your enterprise, on individual SQL Server instances, and on individual databases. These summary tabs allow you to quickly check your compliance status and indicates whether any potential problems exist so that you can investigate them more thoroughly.

You can view the following summary tabs:

Audited SQL Servers Summary

Displays the overall system status, the Enterprise Activity Report Card, and a breakdown of alert activity on all the SQL Server instances registered with SQL compliance manager.

Instance Summary

Displays the overall server status, the Server Activity Report Card, audit configuration, and recent audit events that have occurred on the selected SQL Server instance.

Database Summary

Displays the event distribution, recent database activity, audited activity, and recent audit events for the selected database.

Alert on Audit Data and Status

You can receive alerts when SQL Compliance Manager detects a specific event or operational status Alerting on event data collected from your audited SQL Server instances and databases provides the information you need to immediately correct issues that threaten your compliance with federal and corporate security and privacy policies. Alerting on operational status allows you proactively identify performance issues before your SQL Compliance Manager deployment is impacted.

You can also generate reports on alert activity, allowing you to provide forensic information and demonstrate policy enforcement. For more information, see Report on Audit Data.

Event alerting checklist

Use the following checklist to help you prepare your environment to successfully use Event Alerts to analyze audit data collected from your SQL Server instances and databases.

✓	**Follow these steps ...**
✓	Ensure your Windows logon account has sysadmin privileges on the SQL Server instances hosting the Collection Server. For more information, see Hardware requirements.
✓	Review how the alert process works and which SQL events you can detect using alerts. For more information, see How Event Alerts work.
✓	Identify the types of audit data you want to be alerted on. Determine which events should generate alerts and the conditions under which the alert should be generated. Also consider whether you want an alert message written to the event log or emailed to a specific account. For more information, see Use Event Alerts to analyze audit data.
✓	For each type of audit data you want to alert on, create an alert rule using the criteria you identified. For more information, see Create an Event Alert rule.
✓	***If you want to receive alert notifications through your email account***, test your email configuration settings to ensure SQL Compliance Manager can access your SMTP server. For more information, see Receive alerts through email.
✓	Review how you can implement Reports in your SQL Server environment. For more information, see Report on Audit Data.

Status alerting checklist

Use the following checklist to help you prepare your environment to successfully use Status Alerts to identify performance or operational issues in your SQL Compliance Manager deployment.

✓	**Follow these steps ...**
✓	Ensure your Windows logon account has sysadmin privileges on the SQL Server instances hosting the Collection Server. For more information, see Hardware requirements.
✓	Review how the alert process works and which SQL events you can detect using alerts. For more information, see How Status Alerts work.
✓	Identify the product components whose status you want to audit.
✓	For each type of status data you want to alert on, create an alert rule using the criteria you identified. For more information, see Create a Status Alert.
✓	***If you want to receive alert notifications through your email account***, test your email configuration settings to ensure SQL Compliance Manager can access your SMTP server. For more information, see Receive alerts through email.
✓	Review how you can implement Reports in your SQL Server environment. For more information, see Report on Audit Data.

Use Event Alerts to analyze audit data

You can use Event Alerts to identify any type of SQL Server event data you are currently auditing. Event Alerts allow you to track suspicious events collected in your audit data stream. You can use these alerts to warn about potentially malicious activity or record routine activity on an audited instance or database.

For example, when a suspicious event is discovered, you can be notified by email so you can immediately diagnose and resolve the issue. You can also configure SQL compliance manager to write a custom message to the application event log so you have an ongoing record.

Event Alert rule examples

Use the following examples to help you identify the alert criteria you need to define in the corresponding Event Alert rule to monitor a specific action.

Data you want to alert on …	Type of Event Alert rule criteria to set …
When a login fails to access a database containing customer information	• Failed Logins • Instance named SalesServer • Database named Customers
When any login performs a password change	• Security Changes • Any SQL Server instance • Successful Event is true • Exclude certain event types
When a non-privileged user attempts to add a login to role	• Security Changes • Any SQL Server instance • Successful Event is false • Privileged User is false • Exclude certain event types
When a login other than HR01 changes the Salary table	• Data Manipulation • Instance named HRServer • Database object named Salary • Login Name is not HR01 • Successful Event is true • Exclude certain event types

How Event Alerts work

SQL Compliance Manager can generate an event alert when it finds a suspicious event in your audit data. Alert rules define what a suspicious event is and how SQL CM should respond. For example, you can create a rule to alert on DML events that occur on a sensitive database. You can configure SQL CM to write a custom alert message to the application event log and send an alert email notification to your corporate and personal SMTP accounts when the alert is triggered. For more information, see Use Event Alerts to analyze audit data.

SQL Compliance Manager only alerts on the events you select for an audited SQL Server instance or database. After the Collection Server processes the raw event data sent by the SQLcompliance Agent, the Collection Server uses the criteria defined by your alert rules to search for suspicious events. When a matching event is found, the alert is triggered. ***If you specified a message for this alert***, SQL CM saves the alert message in the SQLcompliance Repository database. You can view alert messages and the corresponding events using the Event Alerts tab on the Select SQL Server Instance view.

Depending on the amount of alert activity your environment generates, you may want to groom alert messages on a routine basis. For more information, see Groom alerts from Repository.

Create an Event Alert rule

Creating an Event Alert rule allows you to begin generating alerts on audit data across your SQL Server environment. To successfully generate an alert, the alert rule criteria you select must match SQL Server event data you are currently auditing on the specified instance or database. For more information, see Use Event Alerts to analyze audit data.

To create an Event Alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Click **Event** on the **New Rule** ribbon.
3. Select the type of event (event category) that you want to alert on, and then click **Next**.
4. Select the type of object you want to alert on for the selected event type, and then click **Next**. By default, the alert rule will generate an alert when the selected event occurs on any registered SQL Server instance, database, or database object. Use the links provided on the rule details pane to narrow your alert rule to specific objects or objects that match a naming convention.
5. Define the criteria under which the alert should trigger, and then click **Next**. Use the criteria to narrow your alert rule to generate alerts only under specific conditions. To specify values that the event should match, use the links provided on the rule details pane.
6. Select the action you want SQL compliance manager to take when this alert triggers, and then click **Next**. To configure the email notification message or event log entry, use the links provided on the rule details pane.
7. Specify a name and appropriate alert level for this alert, review the summary, and then click **Finish**. By default, the new alert rule is enabled.

Change which event triggers the alert

Based on the criteria defined in your alert rules, SQL compliance manager generates alerts against your audit data stream for events that occur on a specified SQL Server instance, database, or database object. ***If a SQL Server instance, database, or database object is not specified***, the alert rule criteria is applied against all audit data collected from your SQL Server environment.

You can change the type of audit data that triggers an alert. For example, you can alert on a different event type or a different database. You can also copy an existing alert rule and use it as a template to create a new rule. For more information, see Use an alert rule as a template.

To change the type of audit data that triggers an alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Right-click the rule for the alert you want to change, and then select **Properties** on the context menu.
3. On the SQL Server Event Type window, select the type of event (event category) that you want to alert on, and then click **Next**.
4. On the SQL Server Object Type window, select the type of object you want to alert on for the selected event type, and then click **Next**. By default, the alert rule will generate an alert when the selected event occurs on any registered SQL Server instance, database, or database object. Use the links provided on the rule details pane to narrow your alert rule to specific objects or objects that match a naming convention.
5. On the Additional Event Filters window, define the criteria under which the alert should trigger. Use the criteria to narrow your alert rule to generate alerts only under specific conditions. To specify values that the event should match, use the links provided on the rule details pane.
6. Click **Finish**.

View the event that triggered an alert

You can use the Management Console to view the properties of the SQL Server event that triggered a given alert.

To view the event data for an alert:

1. Select **Audited SQL Servers** or an individual SQL Server instance in the **Explore Activity** tree.
2. On the **Alerts** tab, right-click the alert for which you want to view event details, and then select **Event Properties** on the context menu.
3. Review the event details, and then click **Close**.

Use Status Alerts to ensure compliance

You can use Status Alerts to identify issues and potential disruptions in your SQL compliance manager deployment. By enabling Status Alerts, you can:

- Confirm that your SQL Server instances are available to be audited.
- Ensure the SQLcompliance Agent and Collection Server are operating as expected.
- Proactively know when the event databases are growing too large so you can archive or groom your audit data before too much disk space has been consumed.

Status Alerts best practices

Alert	What it means	What is the risk	What might be wrong
Agent cannot connect to audited instance	The SQLcompliance Agent was unable to connect to the audited SQL Server instance. This alert is sent immediately after the failed connection occurs.	You are in danger of filling the trace directory and losing important audit data. Updated audit settings will not be applied to the SQL trace that is collecting events, and you will fail to collect the events you want. SQL Server will continue to write trace files to the SQLcompliance Agent trace directory, but the agent will not be able to send these files to the Collection Server. When the trace directory is full, auditing will cease, and the SQL Server performance will be impacted. ***If the database id changes***, the agent will not be able to detect this update, causing the SQL trace to stop. ***If communications between the agent and the instance are "down" for more than 7 days***, the SQL trace will automatically stop.	• The audited SQL Server instance may be offline or unable to respond. • The SQLcompliance Agent service account does not have the required permissions to access the target SQL Server instance.
Agent heartbeat was not received	The Collection Server has not received a heartbeat from the SQLcompliance Agent within the specified heartbeat interval.	Auditing is not immediately affected by this issue; however, you cannot apply updated audit settings. Trace files will continue to queue in the trace file directory until the SQLcompliance Agent Service is able to send these trace files to the Collection Server.	• The computer hosting the SQLcompliance Agent may be offline. • Network firewall settings may be blocking communication between the SQLcompliance Agent and the Collection Server. • The SQLcompliance Agent may have been stopped.
Agent trace directory reached size limit	The trace directory folder on the SQL Server computer where the SQLcompliance Agent is deployed has exceeded the disk space percentage allocated in the alert rule.	You are in danger of filling the trace directory and losing important audit data. When the trace directory reaches its specified maximum size, the SQLcompliance Agent will cease auditing the target instances. The SQL traces are stopped, and no subsequent events are collected. The size of the trace directory could also impact the performance of the SQL Server instances on this computer.	• The Collection Server may be offline, preventing the SQLcompliance Agent from sending the trace files. • Network firewall settings may be blocking communication between the SQLcompliance Agent and the Collection Server. • Your audit settings may be collecting more SQL Server events than you expected. • SQL Server traffic may have unexpectedly increased, causing more events to be collected and resulting in larger trace files.

Collection Server trace directory reached size limit	The trace directory folder on the computer where the Collection Server is installed has exceeded the disk space limit specified in the alert rule.	You are in danger of filling the trace directory, which can impact the performance of the Collection Server, such as delaying alerts. In turn, a full trace directory on the Collection Server can cause the SQLcompliance Agent trace directory to fill as the trace files queue up to be sent. When the SQLcompliance Agent trace directory reaches its specified maximum size, the agent will cease auditing the target instances. The SQL traces are stopped, and no subsequent events are collected.	• The Collection Service may have been manually stopped, preventing the trace files from being processed. • The Collection Service may not be able to access the Repository, due to inadequate permissions or the Repository database being offline. • Your audit settings may be collecting more SQL Server events than you expected. • A third-party application, such as an anti-virus scanner, may be preventing the Collection Service from accessing the trace directory.
Event database is too large	The event database for an audited SQL Server instance is larger than the size limit specified in the alert rule.	Large event databases can significantly impact the performance of the Repository, and the SQL Server instance hosting the Repository.	• Your audit settings may be collecting more SQL Server events than you expected. • SQL Server traffic may have unexpectedly increased, causing more events to be collected and resulting in larger trace files. • You may need to archive or groom events.

How Status Alerts work

SQL compliance manager can generate a Status Alert when it receives a status update from the Collection Server or SQLcompliance Agent that is unsafe and could disrupt your ability to audit your SQL Server instances. Alert rules define what type of status is considered unsafe and how SQL compliance manager should respond. You can configure SQL compliance manager to write a custom alert message to the application event log and send an alert email notification to your corporate and personal SMTP accounts when the alert is triggered. For more information, see Use Status Alerts to ensure compliance.

There are two categories of Status Alerts: alerts that track the Collection Server status and alerts that track the SQLcompliance Agent status. In general, when the Collection Server or SQLcompliance Agent communicates at their heartbeat intervals, each service confirms its health and compares its status information against the alert rules you have defined. An alert message is generated when the status is deemed unsafe. By default, each heartbeat occurs in 5 minute intervals.

Depending on the amount of alert activity your environment generates, you may want to groom alert messages on a routine basis. For more information, see Groom alerts.

Create a Status Alert

Creating a Status Alert rule allows you to proactively identify potential issues in your SQL compliance manager deployment that could disrupt your ability to continue auditing. For more information, see Use Status Alerts to ensure compliance.

To create a Status Alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Click **Status** on the **New Rule** ribbon.
3. Select the type of SQL compliance manager status that you want to alert on.
4. In the **Edit rule details** pane, define the criteria under which the alert should trigger, and then click **Next**.
5. Select the action you want SQL compliance manager to take when this alert triggers, and then click **Next**. To configure the email notification message or event log entry, use the links provided on the rule details pane.
6. Specify a name and appropriate alert level for this alert, review the summary, and then click **Finish**. By default, the new alert rule is enabled.

Use Data Alerts to perform forensics

You can use Data Alerts to track access to specific table columns that contain sensitive data, such as Social Security numbers. For example, when a user accesses a sensitive column, SQL compliance manager can notify you by email so you can immediately diagnose and resolve the issue. You can also configure SQL compliance manager to write a custom message to the application event log so you have an ongoing record.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

How Data Alerts work

SQL compliance manager can generate a Data Alert when it finds a suspicious data manipulation in your audit trail. Alert rules define what a suspicious data manipulation is and how SQL compliance manager should respond. For example, you can create a rule to alert you when data in sensitive columns has been accessed. You can configure SQL compliance manager to write a custom alert message to the application event log and send an alert email notification to your corporate and personal SMTP accounts when the alert is triggered. For more information, see Use Data Alerts to perform forensics.

SQL compliance manager only alerts on the data you select for an audited SQL Server instance and database. After the Collection Server processes the raw event data sent by the SQLcompliance Agent, the Collection Server uses the criteria defined by your alert rules to search for suspicious manipulations. When a matching event is found, the alert is triggered. ***If you specified a message for this alert***, SQL compliance manager saves the alert message in the SQLcompliance Repository database. You can view alert messages and the corresponding events using the Data Alerts tab on the Select SQL Server Instance view.

Depending on the amount of alert activity your environment generates, you may want to groom alert messages on a routine basis. For more information, see Groom alerts.

Create a Data Alert

Creating a Data Alert rule allows you to begin generating alerts on audit data across your SQL Server environment. To successfully generate an alert, the alert rule criteria you select must match SQL Server event data you are currently auditing on the specified instance or database. For example, to alert on sensitive column access, first enable auditing on sensitive columns.

To create a Data Alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Click **Data** on the **New Rule** ribbon.
3. On the **Data Alert Type** window, note that you are creating an alert for sensitive column access, and then click **Next**.
4. Select the type of object you want to alert on, and then click **Next**. By default, the alert rule will generate an alert when the selected data is collected for an instance, database, table, or column. Use the links provided on the rule details pane to narrow your alert rule to specific objects or objects that match a naming convention.
5. Select the action you want SQL compliance manager to take when this alert triggers, and then click **Next**. To configure the email notification message or event log entry, use the links provided on the rule details pane.
6. Specify a name and appropriate alert level for this alert, review the summary, and then click **Finish**. By default, the new alert rule is enabled.

Change the action an alert performs

Based on the criteria defined in your alert rules, SQL Compliance Manager will write a custom alert message to the application event log or email a custom alert message to the specified addresses when an alert is triggered. You can change which action SQL CM takes when the event or Status Alert is triggered.

If you want to receive alert email notifications, ensure you have configured SQL Compliance Manager to connect to your SMTP server. For more information, see Receive alerts through email.

To change the action an alert performs:

1. Select **Alert Rules** in the **Administration** tree.
2. Right-click the rule for the event or Status Alert you want to change, and then select **Properties** on the context menu.
3. Click **Next** to navigate to the Alert Actions window.
4. Select the action you want SQL Compliance Manager to take when this alert triggers. To configure the email notification message or event log entry, use the links provided on the rule details pane.
5. Click **Finish**.

Disable an alert

Disabling an alert allows you to temporarily stop alerting on a specific event or status. For example, you can disable alerting on audit data from a specific SQL Server instance or database by disabling the corresponding Event Alert rule. When you disable alerting, SQL compliance manager stops generating alerts against the audit data or operational status specified by the alert rule criteria but leaves the alert rule and previously generated alert messages intact. For example, SQL compliance manager continues auditing SQL Server events on the specified instances and databases.

To permanently remove an alert rule from the Repository, delete the rule.

To disable an alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Select the rule you want to disable, and then click **Disable** on the **Rule Management** ribbon.

Enable an alert

You can resume alerting on audit data or status by enabling the corresponding alert rule. By default, alerting is enabled when the Event or Status Alert rule is created.

To enable an alert:

1. Select **Alert Rules** in the **Administration** tree.
2. Select the rule you want to enable, and then click **Enable** on the **Rule Management** ribbon.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Export your alert rules

Exported alert rules are saved in an XML format and can be applied to other registered SQL Server instances. This flexibility saves you time when you are configuring Event and Status Alert rules on multiple SQL Server instances, and helps ensure consistency across your environment. In addition, exporting allows you to back up your alert rules to use should you need to reinstate an audited SQL Server instance. As you configure alert rules, consider which settings you would like to save for future use, and export the rules configured for that particular SQL Server instance or database.

To export your alert rules:

1. Select **Alert Rules** in the **Administration** tree.
2. Click **Export Rules**.
3. Enter a file name or use the default.
4. Select the location to save your alert rules file.
5. Click **Save**.

Groom alerts

You can remove stale alert data and manage your alert storage requirements by grooming alert messages from the Repository databases. When you groom alerts, you can use an age threshold to delete alert messages you no longer need. Grooming ensures your alert reports reflect the current state of your environment without compromising your database resources. For more information, see How grooming works and Groom alerts.

Import your alert rules

As you configure or modify alert rules for your SQL Server instances, you may want to apply the same rules across multiple SQL Server instances in your environment. You can import Event and Status Alert rules through previously exported XML files to streamline your configuration workflow while reducing errors.

To import your alert rules:

1. Select **Alert Rules** in the **Administration** tree.
2. Click **Import Rules**.
3. Locate the alert rules file you want to import.
4. Click **Open**.

Receive alerts through email

You can configure SQL compliance manager to email custom alert messages to yourself or others. To successfully receive alert messages through an email client, configure SQL compliance manager to connect to your SMTP server, and then configure the Event or Status Alert rule to send an email when the alert is triggered.

To receive alerts through email:

1. On the **Alerting** menu, click **Configure Email Settings**.
2. Specify the following settings according to your SMTP server configuration:
    - Name of the physical computer hosting the SMTP server
    - Port used to connect to the SMTP server
    - Whether the SMTP server requires authentication to accept a connection from another computer or application
    - Whether the SMTP server uses Secure Sockets Layer (SSL)
    - Address that should display in the From field of the alert email
3. To verify that SQL compliance manager can connect to your SMTP server using the specified settings, click **Test**.
4. Click **OK**.
5. Depending on the alert rule type, use the either Edit Event Alert Rule or the Edit Status Alert Rule wizard to enable email notification, specify recipient addresses, and create a custom alert message for existing alerts. For more information, see Change the action an alert performs.

SQL Compliance Manager audits all activity on your server. Learn more > >

Report on alerts

You can use Report Cards to identify compliance problems, or track alert activity over a time period up to 30 days. When you identify spikes in alert activity, or potential issues, you can generate reports to view in-depth information on the associated alerts. This feature allows you to gather forensic information or demonstrate policy enforcement. For more information, see Report on Audit Data.

Use an alert rule as a template

You can create a new alert rule by using an existing event or status rule as a template. Alert rule templates allow you to more efficiently create multiple rules against the same instance or database. You can also use alert rule templates to apply consistent alert criteria across multiple instances and databases. When you choose to use an alert rule as a template, SQL compliance manager copies the existing alert rule criteria to the new rule. You can then use the Edit Alert Rule wizard to customize the new rule.

To use an alert rule as a template:

1. Select **Alert Rules** in the **Administration** tree.
2. Select the event or status rule you want to use as a template, and then click **From Existing** on the **New Rule** ribbon.
3. On each wizard window, specify the criteria you want to use for this new rule, and then click **Next**.
4. On the Finish Alert Rule window, specify a name for this alert, review the summary, and then click **Finish**. By default, the new alert rule is enabled.

View alerts

You can use the Management Console to view messages for previously generated alerts. To successfully view an alert message, the corresponding alert rule must be set to email the alert message or write the alert message to the application event log. For more information, see Change the action an alert performs.

To view alert messages:

1. Select **Audited SQL Servers** or an individual SQL Server instance in the **Explore Activity** tree.
2. Select the **Alerts** tab, right-click the alert for which you want to view the alert message, and then select **Alert Message** on the context menu.
3. Review the alert message, and then click **Close**.

Secure Audit Data

SQL Compliance Manager allows you to control access to your audit data by leveraging the native SQL Server security model. The Management Console authenticates SQL Server login credentials and privileges to determine who can administer audit data and who can view audit data. SQL Compliance Manager seamlessly integrates with your existing SQL Server security settings, complying with your network security policies. This approach allows you to safely and securely deploy SQL Compliance Manager throughout your SQL Server environment with little or no configuration.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

How Console security works

SQL compliance manager controls user access by leveraging the SQL Server logins that exist on the SQL Server instance hosting the Repository databases. When you start the Management Console, SQL compliance manager automatically attempts to connect to the Repository. The Management Console validates your SQL Server privileges and restricts your access to the appropriate features. To be able to configure audit settings or report on audit data, your login must have the appropriate SQL Server privileges on the Repository databases.

Security and existing logins

An existing Windows authentication login that is a member of the built-in Administrators group in SQL Server can configure and view audit data. Likewise, an existing SQL authentication login, such as the sa account, that is a member of the sysadmin fixed server role can configure and view audit data.

An existing Windows authentication login that is a member of the Public role on the SQL Server instance that hosts the Repository databases can view audit data.

Security and login permissions

Ensure each SQL Compliance Manager user has a SQL Server login. When you grant SQL CM permissions to a login, SQL CM assigns either the System Administrators role or read privileges on the Repository databases. You can quickly and easily grant these permissions using the Management Console.

The System Administrators role allows the user to perform administrative activities in SQL Compliance Manager, such as:

- Registering SQL Server instances
- Enabling or disabling auditing
- Configuring audit settings

Read privileges allow the user to view collected audit data and generate reports on audited events.

You can also set default permissions on the registered SQL Server instance or an individual archive database. For more information, see Understanding default permissions.

Understanding default permissions

If your security policies require more granular access control, you can grant or deny SQL compliance manager permissions on each audited SQL Server instance and archive database. These permissions determine whether a user can view audited events and the corresponding SQL statements by default.

You can set default permissions when you register a SQL Server instance to audit. When you set default permissions, SQL compliance manager grants read privileges to the guest account on the selected Repository databases. This setting allows a SQL Server login to view audit data collected from that registered SQL Server instance only.

You can also specify the appropriate permissions on each archive database that contains audit data. You can grant or deny access per database. When you set default permissions, SQL compliance manager grants read privileges to the guest account on the selected archive database only.

As you assign permissions, keep in mind that permissions granted to a login are applied along side any default permissions you set at the server or database level.

How to implement logins

Use the following checklist to help you implement and configure logins that meet your auditing and SQL Server security needs.

☑	**Follow these steps ...**
□	Ensure your Windows logon account has sysadmin privileges on the SQL Server instance that hosts the Repository databases. For more information, see Permissions requirements.
□	Review how SQL Compliance Manager enforces your native SQL Server security model. For more information, see How Console security works.
□	Review the SQL Server privileges granted with SQL compliance manager permissions. For more information, see Available login permissions.
□	Create a login for each person who should generate reports using the Management Console, and then apply the Can view and report on audit data permission to each login. For more information, see Create a login.
□	Create a login for each person who should administer auditing in the Management Console, and then apply the Can configure settings and view audit data permission to each login. For more information, see Cr eate a login.

Available login permissions

SQL Compliance Manager permissions allow a user to access specific SQL CM features. When you assign a SQL CM permission, SQL Compliance Manager applies specific SQL Server privileges to the login.

SQL Compliance Manager provides the following levels of permission:

Can configure SQL Compliance Manager settings and view audit data

Allows the selected login to perform any administrative task in the Management Console. Administrative tasks include:

- Configuring audit settings and event filters
- Managing alerts
- Managing logins
- Monitoring SQL CM activities
- Archiving and grooming audit data
- Enabling auditing on SQL Servers and databases

Logins with this permission can also view and report on audit data.

When you assign this permission, SQL CM grants the System Administrators role to the selected login. This role is granted on the SQL Server instance that hosts the Repository databases, applying this role along side any default permission settings.

Can view and report on audit data

Allows the selected login to view and report on audited data using the Management Console. When you assign this permission, SQL CM grants read privileges to the selected login. These privileges are granted on the SQL Server instance that hosts the Repository databases, applying these privileges along side any default permission settings.

Create a login

Consider creating a login for each security administrator, database administrator, or auditor who uses the Management Console. Creating multiple logins allows you to enforce more granular security. When you create a login, SQL compliance manager also creates a SQL Server login on the SQL Server instance that hosts the Repository databases.

Assign the new login the appropriate SQL compliance manager permissions and database access rights. For more information, see Available login permissions.

To create a console login:

1. Select **Logins** in the **Administration** tree, and then click **New Login**.
2. Specify the name of a valid Windows user account and whether this account should have access to audit data, and then click **Next**. You can grant or change access later.
3. Specify which level of SQL compliance manager permissions you want to grant this login, and then click **Next**. For more information, see Available login permissions.
4. Review the summary, and then click **Finish**.

Assign permissions to a login

You can assign SQL Compliance Manager permissions to any login. When you assign SQL Compliance Manager permissions, SQL CM applies the appropriate SQL Server privileges to the login. For more information, see Available login permissions.

Because you are granting SQL Server privileges, applying permissions to a login also applies the same permissions in SQL Server. You can assign login permissions when you create a login, or modify permissions for existing logins. The following procedure allows you to modify permissions for existing logins.

To assign SQL Compliance Manager permissions:

1. Select **Logins** in the Administration tree.
2. Select the login you would like to assign permissions to in the list and click **View Login Properties**.
3. On the General tab, select the appropriate permissions.
4. ***If your internal security policies require more granular access control***, use the Database Access tab to select the appropriate permissions on each database that contains audit data.
5. Click **OK**.

Report on Audit Data

SQL Compliance Manager Reports provides several built-in reports that allow you to quickly and easily meet the demands of on-the-spot audits, routine audits, and long-term event trending. Each report gives detailed information about events in your SQL Server environment. Use SQL Compliance Manager Reports to track compliance on demand and provide self-service reporting to third-party auditors.

How reports work

The Audit Reports window contains a reporting interface that allows you to generate audit reports. Each report is based on a template file that is stored in the Reports folder in the SQLcompliance installation directory. When you generate a report, you are able to determine what is displayed by selecting from the options on each individual report. This allows you to generate reports tailored to your needs.

In addition, report template files can be integrated into Microsoft SQL Server Reporting Services (Reporting Services) to allow you to further customize your reports when necessary. For more information, see Customize reports.

Available reports

The following report categories are included with SQL compliance manager. The activity, change, and history reports list events that passed the SQL Server access check. To audit events that failed the SQL Server access check, generate the Permission Denied Activity report for the appropriate SQL Server instance.

Audit Reports

The Daily Audit Activity Statistics report lists the amount of activity that occurred on the SQL Server instance or designated database, on an hourly basis, for the dates specified. Use this report to audit overall activity levels on your SQL Server instances and databases.

Alerts Reports

The Alert Activity report lists alert details, such as target object, event, and time of the alert. Use this report to audit alerts triggered over a specified time period.

Application Audit Reports

These reports list activity details, such as login, event, and time of activity, per application and database. Use these reports to audit activity across multiple applications and databases.

- Application Activity
- Application Activity Statistics

Database Object Audit Reports

The Backup and DBCC Activity report lists backup, restore, DBCC, and database object activities on specific databases. Use these reports to audit mass data movement or database object activity, such as SELECT or UPDATE, across multiple databases.

DDL Audit Reports

The Database Schema Change History report lists schema changes applied to audited databases. Use these reports to audit data definition language (DDL) statements, such as dropped tables, executed against one or more databases on a SQL Server instance.

DML Audit Reports

The DML Activity (Before-After) report lists DML events for which before and after data is available. Use this report to audit UPDATE, INSERT, and DELETE activity on critical or sensitive databases.

Host Audit Reports

The Host Activity report lists all host computers from which specific logins executed an action. Use this report to audit user behavior from multiple client computers, identifying the host computer from which an activity request originated.

Policy Audit Reports

These reports list changes and updates applied to the SQLcompliance Agent deployed on a specific SQL Server, and any integrity violations in your audit data. Use these reports to diagnose audit data integrity issues and track agent configuration changes as well as agent activities, such as SQLcompliance Agent service restarts.

- Agent History
- Alert Rules
- Audit Control Changes
- Integrity Check

Regulation Audit Reports

The Regulation Guidelines report lists all of the regulations and their individual guidelines applied to one or more databases. Use this report to audit the regulatory guidelines applied to your SQL Server instance.

Security Audit Reports

These reports list permission changes by object type as well as unauthorized attempts to execute activities. Use these reports to audit your SQL Server security settings and identify misconduct.

- Change History (by object)
- Change History (by user)
- Permission Denied Activity
- User Login History

SELECT Audit Reports

The Sensitive Column report lists all SELECT events that were initiated by applications to read specific columns that contain sensitive data. This report also includes the T-SQL statements that executed the corresponding commands. Use this report to audit columns that require high security, such as employee Social Security numbers (SSNs).

User Audit Reports

These reports list user activities performed on a specific SQL Server instance, and provide a history of login creations and deletions. Use these reports to audit user behavior and login management.

- Login Creation History
- Login Deletion History
- Server Login Activity Summary
- User Activity History

Customize reports

You can customize any of the integrated audit reports or develop new reports that fit your unique auditing needs. First, deploy the SQL compliance manager Reports to your existing Microsoft Reporting Services. Then select which reports you want to customize from the corresponding RDL files (by default, these files are stored in the Anytime folder under the SQL compliance manager Reports root folder on the Report Server). ***If you decide to customize these reports***, consider the following best practices:

- Save your new and modified reports to a separate folder
- Use a different filename for modified reports

For more information about deploying SQL compliance manager Reports, see Generate reports with Reporting Services. For more information about developing custom reports, see the Reporting Services Books Online.

Generate reports in the Console

SQL compliance manager includes many common audit reports. These reports are created from the Audit Reports view in the Management Console. You can select the SQL Server instances, date range, and other report specific criteria to generate reports that meet your needs. Once generated, you can print the report or save it to Excel or PDF.

To generate a report:

1. Select **Audit Reports** in the console tree.
2. Select the appropriate report from the **Audit Reports** list.
3. Click **Run**.

Generate reports with Reporting Services

You can integrate the reports included with SQL compliance manager into your Reporting Services Server using the Reports Installer accessible from the Audit reports view. Integrating the SQL compliance manager audit reports with Microsoft SQL Server Reporting Services (Reporting Services) gives you the ability to completely customize your reports to fit your particular needs.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Reporting Services requirements

SQL compliance manager allows you to use Microsoft SQL Server Reporting Services (Reporting Services) to provide on-the-spot reporting on your audit data. The Report Server computer should meet or exceed the hardware and software requirements recommended by Microsoft to run and manage the Reporting Services components.

To successfully use Reporting Services in your SQL Server 2000 environment, deploy Reporting Services version 1.0 SP1 or later (SP2 recommended). For SQL Server 2005 or later environments, deploy the Reporting Services components released with the current version of SQL Server.

To successfully integrate SQL compliance manager reports with Microsoft Reporting Services, ensure your logon account has Content Manager Rights on the Report Server.

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Deploy reports to Reporting Services

The Deploy Reports wizard allows you to integrate SQL compliance manager reports into Microsoft Report Services. Perform this deployment for each Repository that contains data you want to audit using Microsoft Reporting Services. The following procedure guides you through a remote install.

If the Repository databases are located in a non-trusted domain, deploy the reports to the same physical computer that is hosting the Repository databases (by default, this computer is also the Collection Server). To ensure successful authentication, ensure the target computer is running a local install of Microsoft Reporting Services.

To install reports:

1. Ensure your environment includes supported installations of Microsoft Report Services, and note the configuration settings. For more information, see Reporting Services requirements.
2. Start the Management Console and navigate to the **Audit Reports** view.
3. Under **ReportingServices**, click **Deploy Reports**.
4. On the Welcome window, click **Next**.
5. Specify the name of the Report Server computer hosting Microsoft Reporting Services and any advanced configuration settings, such as a dedicated port, and then click **Next**.
6. Specify the following Repository connection settings, and then click **Next**.
   - Name of the SQL Server instance that is hosting the target Repository
   - Credentials of the Windows account the Report Server should use to connect to the Repository databases
7. Specify the name of the virtual folder Reporting Services will use to store the reports (RDL files) and choose whether to overwrite any previously deployed reports, and then click **Next**.
   - ***If you choose to not overwrite reports***, the wizard deploys only the new reports included in this release. The wizard will not deploy updated reports.
8. On the Summary window, click **Next**.
9. Review the progress. When deployment is complete, click **OK**.
10. To start using the deployed reports, click **View Deployed Reports** under Reporting Services on the Audit Reports view. This link opens the Report Manager interface on the Report Server.

Test report deployment

Once you have integrated SQL compliance reports into Microsoft Reporting Services, you should test your installation by loading Microsoft Reporting Services and generating each report. This will allow you to ensure that when you start generating reports, you get the results you anticipate.

For more information on generating reports in Microsoft Reporting Services, see the Reporting Services Books Online.

Change the Reporting Services data source

Reporting Services leverages the Repository as the data source when generating reports. To use Reporting Services to report on your audit data, ensure the data source has been correctly configured, allowing Reporting Services to find and connect to the Repository.

For example, when you migrate the Collection Server to another computer, the Repository location changes accordingly, causing the data source configuration to become invalid.

You can configure Reporting Services using the Report Manager Web interface.

Use reports to analyze trends over time

You can use SQL compliance manager reports to track activity trends over a period of time. This allows you, for example, to check peaks in activity to be sure that they are only occurring in expected periods of time. If you use Microsoft Reporting Services, you can automate the generation of daily, weekly, monthly, and quarterly reports.

Using SQL compliance manager reports to track trends over time also allows you to see potential problems that are occurring with a higher frequency over time, and might require your attention. This can be a useful way to reinforce SQL Server compliance policies and catch problems before they become a bigger issue.

Use reports to establish and maintain compliance

You can use SQL Compliance Manager reports to show that SQL Server compliance policies are being followed or that the procedures you have developed are having a positive impact on the way that SQL Server is being used in your environment.

Once compliance is established, SQL CM Reports allow you to track activity and identify problems so that they can be resolved and compliance can be maintained. In addition to being able to generate compliance reports on your SQL Server environment, you can also assign read-only access to SQL CM to designated users so they can generate the reports they need.

Idera Website | **Products** | **Purchase** | **Support** | **Resources** | **Community** | **About Us** | **Legal**

Use report cards to track SQL Server activity

SQL compliance manager includes several Activity Report Cards that display up to 30 days of SQL Server activity. Activity Report Cards allow you to view the SQL Server activity at the enterprise and individual SQL Server instance levels. These report cards allow you to quickly check activity in each event category audited, view SQL Server activity statistics, and short-term activity trends. Activity Report Cards can be used to identify problems that might require more in-depth analysis.

To view report cards:

1. Select **Audited SQL Servers** from the **Explore Activity** tree to see the Enterprise Activity Report Card. The Enterprise Activity Report Card allows you to review the status of your audited SQL Servers and the recent activity that has occurred on them.
2. Select any SQL Server instance from the **Explore Activity** tree to see the Server Activity Report Card. The Server Activity Report Card allows you to review the activity status and recent audit event history on your SQL Server instance.
3. Select any database from the **Explore Activity** tree to see Recent Database Activity Summary. The Recent Database Activity Summary allows you to review the recent database activity and a listing of recent audit events that have occurred on the selected database.

Manage Audit Data

You can optimize auditing performance and preserve your compliance history through SQL Compliance Manager archives. Archiving allows you to off-load collected and processed events from the Repository databases to an archive database. Your audit data remains available for reporting and viewing without impacting your collection and processing performance. To view or report on archived events, simply attach the archive database.

If your environment requires more aggressive data management, consider implementing a maintenance plan for your archive databases to meet your storage and performance needs. Consider using tools such as Idera SQL Safe to quickly and securely back up archive databases so that you maintain optimal performance on the host SQL Server instance. Also consider grooming older event data. You can groom audited events from selected archive databases using the Management Console.

How archives work

When you archive audit data, the Collection Server moves audited events from the Repository (typically, the event database) to an archive database. SQL compliance manager creates an archive database for each registered SQL Server instance, according to the file naming conventions and event age limit you specify. Each archive database contains events collected from the audited databases hosted on the SQL Server instance. You can archive event data across all registered SQL Server instances or for a selected instance.

To ensure you are archiving uncompromised audit data, SQL compliance manager allows you to check the integrity of the collected events. ***If the audit data fails this integrity check***, SQL compliance manager does not archive the data.

During the archival process, the audited events are temporarily written to the tempdb before being stored in the appropriate archive database. ***If you are archiving a large number of events, such as one million events***, the tempdb may run out of available space, resulting in an incomplete archive.

To ensure optimal event handling and performance, archive your audit data frequently. Monitor your Repository database consumption over the first few days of collecting audit data, so you can develop a maintenance strategy that best suits your needs. For more information, see Back up and restore archive databases.

For more information on how to archive events, see Archive collected events.

Also consider grooming older audit data. Grooming allows you to minimize your storage requirements and ensure your audit data remains relevant to your compliance needs. For more information, see How grooming works.

How grooming works

Grooming allows you to permanently delete event data from the Repository databases. You can groom Repository databases for all registered SQL Server instances or for specific SQL Server instances.

Use grooming to ensure your Repository databases contain only the event data you need. You can delete events and alerts older than a specified age (in days).

To increase storage on the host SQL Server instance, also consider archiving your audit data. Archiving provides additional storage flexibility and security. For example, you can back up archive databases, storing the backup files on a dedicated backup server computer, and then remove the archive databases. When you need to report on the archived data, you can use tools such as Idera SQLsafe to easily and quickly restore the archive databases, and then attach the archives.
For more information on how to groom events, see Groom audit data.

Archive collected events

When you archive your registered SQL Server instances, SQL compliance manager moves audited events from the Repository databases to an archive database. You can archive event data for all registered SQL Server instances or a particular SQL Server instance.

You can archive events using the Management Console or the CLI. Note that SQL compliance manager does not automatically shrink the Repository databases after an archive is performed. After each archive operation, re-index and shrink the corresponding event databases in the Repository so that SQL Server can reclaim the space that had been allocated due to the previous growth.

Use the Management Console to archive events

When you archive events using the Management Console, SQL compliance manager can also perform the following actions:

- Check the integrity of the collected events to ensure you are archiving uncompromised data. ***If the audit data for the selected SQL Server instance fails this integrity check***, SQL compliance manager does not archive the data.
- Log the event in the Change Log.

You can also perform an integrity check using the command line interface (CLI), allowing you to schedule and automate your archive workflow.

To archive events using the Management Console:

1. Set your archive preferences. To set archive preferences, click **Auditing** on the menu bar, and then select **Archive and Retention > Archive Preferences**.
2. Click **Auditing** on the menu bar, and then select **Archive and Retention > Archive Audit Data Now**.
3. Choose whether you want to archive events for all registered instances. You can select a specific SQL Server instance.
4. To generate a CLI command that uses your archival preferences, click **Generate Script**. From the View Script window, you can save the command as a batch file or copy the command to another application.
5. To archive your audit data now, click **OK**.

Use the CLI to archive events

You can use the command line interface to archive audited events for registered SQL Server instances across your environment.

The archive operation supports the following syntax:

```
SQLcmCmd [-host CollectionServer] [-port number] archive {instance | all} [numberofdaysold] [-prefix phrase] [-partition {quarter | month | year}] [-timezone timezonename] [-nointegrity]
```

If you do not specify an optional parameter, the Collection Server will use the settings you selected in your archive preferences. An integrity check will be performed unless you use the –nointegrity parameter in your command.

Attach existing archives

Attaching an archive allows you to view audited events that have been moved to an archive database. When you attach an archive, the Collection Server loads the database so you can view and report on the events. The audited events remain in the archive database, allowing you to manage the archived events without impacting the Repository databases.

By default, SQL compliance manager automatically attaches an archive when the corresponding database is created. ***If you are not reporting on audit data contained in an archive***, consider detaching the archive to prevent unwanted access. When you detach an archive, SQL compliance manager continues to audit the associated SQL Server instance and databases.

When you attach an archive database generated with an earlier version of SQL compliance manager, you can choose whether to update the database now or schedule a time off-hours. Updating the archive database allows you to take advantage of performance enhancements, such as optimized indexes.

To attach archives:

1. Select the SQL Server instance you want to attach an archive from the **Explore Activity tree**.
2. Click **File** on the menu bar, and then select **Attach Archive Database**.
3. Specify the appropriate settings, and then click **OK**.

Automate audit data management

SQL compliance manager supports the automation of audit data management activities such as archiving, grooming, and verifying data integrity. Use the corresponding command line interface operations to integrate these activities into your existing workflows.

SQL Compliance Manager audits all activity on your server. Learn more > >

Groom alerts from Repository

You can groom alerts from the Repository. When you groom alerts, SQL compliance manager deletes all alert messages that are older than the age (in days) you specify. You can groom alerts generated by events from all registered SQL Server instances or from selected instances. Grooming ensures that the Repository contains only the alert data you need.

To groom alerts:

1. Click **Alerting** on the menu bar, and then select **Groom Alerts Now**.
2. Specify the appropriate settings, and then click **OK**.

Groom audit data

You can groom audited SQL events from the event databases in the Repository. When you groom audit data, SQL compliance manager deletes all events that are older than the age (in days) you specify. You can groom audit data collected from all registered SQL Server instances or from selected instances. Grooming ensures the Repository contains only the audit data you need.

If your auditing needs require long-term storage, consider implementing a maintenance plan. For more information, see Manage Audit Data.

You can groom events using the Management Console or the CLI. Note that SQL compliance manager does not automatically shrink the Repository databases after a groom is performed. After each groom operation, re-index and shrink the affected Repository databases so that SQL Server can reclaim the space that had been allocated due to the previous growth.

Use the Console to groom events

When you groom events using the Management Console, SQL compliance manager also performs the following actions:

- Checks the integrity of the collected events to ensure you are grooming uncompromised data. ***If the audit data for the selected SQL Server instance fails this integrity check***, SQL compliance manager does not groom the data.
- Logs the event in the Change Log.

To groom archived events:

1. Click **Auditing** on the menu bar, and then select **Archive and Retention > Groom Audit Data Now**.
2. Specify the appropriate settings, and then click **OK**.

Use the CLI to groom events

You can use the command line interface to groom audited events for registered SQL Server instances across your environment.

The groom operation supports the following syntax:

```
SQLcmCmd [-host CollectionServer] [-port number] groom {instance | -all} [numberofdaysold]
[-nointegrity]
```

For example, to groom audited events older than 90 days for all registered instances without performing an integrity check, use the following command:

```
SQLcmCmd -host SERVER01 -port 5201 groom -all 90 -nointegrity
```

Maintain the Repository databases

Maintaining the Repository databases helps you achieve optimal performance and ensure long-term audit data integrity. Repository database maintenance includes backup and restore operations, and should coincide with your established disaster recovery strategies.

Before you implement a disaster recovery strategy for the Repository databases, review the following supported recovery model settings.

Repository Database	Supported Recovery Model
SQLcompliance	Recovery model set for the model system database
SQLcompliance.Processing	Simple
SQLcompliance_Instance	Simple, or recovery model set for the model system database
SQLcmArchive_instance_Time_Partition	Simple, or recovery model set for the model system database

You can perform backups on a routine basis as a scheduled job or manually on an as-needed basis. Refer to your established disaster recovery strategies when implementing a backup or restore policy for the Repository databases. Tools such as Idera SQLsafe allow you to schedule fast, secure backups using optimized compression and encryption settings.

Back up event databases

Consider backing up the event databases frequently, depending on the volume of audit data you collect and your established disaster recovery strategies. For best results, use the following guidelines:

- Perform a full backup, including the transaction logs
- Schedule the backup during off-hours, or times when you expect the least audit activity
- Back up all event databases during the same backup procedure
- Save each database to a separate backup file
- Back up the SQLcompliance database during the same backup procedure to ensure audit data integrity remains intact

To back up the event databases:

1. Use SQL Server Enterprise Manager or Management Studio to take the SQLcompliance database offline. ***If you cannot take the SQLcompliance database offline***, stop the Collection Service.
2. Use a tool such as Idera SQLsafe to perform a full backup, including transaction logs, of the SQLcompliance database.

For each event database, perform a full backup, including the transaction logs. Each registered SQL Server instance has a corresponding event database. For more information, see Product components and architecture.

1. Use SQL Server Enterprise Manager or Management Studio to bring the SQLcompliance database online.

Back up and restore archive databases

To ensure optimal audit performance while minimizing storage requirements, consider implementing a maintenance plan to backup your archive databases on a routine basis. Each archive database is independent, and can be maintained on a different schedule.

Once you back up the archive, you can drop it from the SQL Server instance that hosts the Collection Server. When you need to access older audit data, restore the archive database to the Collection Server, and then attach it using the Management Console. For more information, see Attach existing archives.

When you restore an archive database that was generated by a previous version of SQL compliance manager version, consider updating the database to use optimized indexes. Optimizing indexes enhances performance when working with larger archive databases. For more information, see Update your archive databases.

Change the Repository recovery model

You can select which database recovery model you want the Collection Server to configure when creating databases to store audit data in the Repository. Typically, the recovery model is set on the model system database on the host SQL Server instance.

Changes made to the recovery model used by the Repository databases should reflect your disaster recovery strategies. You may need to change the Repository recovery model to address the following situations:

- You are moving SQL compliance manager into a production environment and now need to implement a full recovery model
- You no longer need to back up transaction logs for the Repository databases and can use a simple recovery model

Configure the model system database before installing the Repository. For more information, see Deployment considerations. By default, the setup program installs the Repository on the Collection Server computer.

To change the Repository recovery model:

1. Click **Auditing** on the menu bar, and then select **Configure Repository Databases**.
2. Specify the appropriate recovery model, and then click **OK**. For more information, see Microsoft SQL Server Books Online.

Restore event databases

Restore the event databases to recover lost or damaged audit data, according to your established disaster recovery strategies. For best results, use the following guidelines:

- Perform a full restore, including the transaction logs
- Schedule the restore during off-hours, or times when you expect the least audit activity
- Restore all event databases during the same restore procedure
- Restore the SQLcompliance database during the same restore procedure to ensure audit data integrity remains intact

To restore the event databases:

1. Use SQL Server Enterprise Manager or Management Studio to close any open connections to the SQLcompliance database.
2. Use SQL Server Enterprise Manager or Management Studio to take the SQLcompliance database offline. ***If you cannot take the SQLcompliance database offline***, stop the Collection Service.
3. Use a tool such as Idera SQLsafe to restore the SQLcompliance database using the appropriate backup file, including transaction logs.
4. Use a tool such as Idera SQLsafe to restore each event database using the appropriate backup file, including the transaction logs. Each registered SQL Server instance has a corresponding event database. For more information, see Product components and architecture.
5. Use SQL Server Enterprise Manager or Management Studio to bring the SQLcompliance database online.

Update your archive databases

Updating your archive databases allows you to take advantage of the performance enhancements provided by optimized indexing in the latest version. When you update an archive database, SQL compliance manager locks the Repository and applies the new indexing scheme to the specified database.

You can update your archive databases using the Management Console or the command line interface (CLI).

Update your archive database using the Management Console

To update archive databases using the Management Console:

1. Attach existing archives.
2. Select **Auditing > Configure Repository Databases**.
3. On the Configure Repository Databases window, select the **Databases** tab.
4. Select the databases you want to update, and then click **Update Now**.

Update your archive databases using the CLI

To update your archive databases using the CLI:

1. From a DOS prompt, navigate to your SQL compliance manager installation directory.
2. Enter the following at the prompt:

```
SQLcmCMD updateindex –all
```

Use the CLI to verify audit data integrity

You can use the command line interface to verify and resolve the integrity of audited events for a specific registered SQL Server instance.

The checkintegrity operation supports the following syntax:

```
SQLcmCmd [-host CollectionServer] [-port number] checkintegrity instance [-fixintegrity]
```

For example, to verify the integrity of audited events for the test01\STD_SQL_2005 registered instance, use the following command:

```
SQLcmCmd –host TEST01 –port 5201 checkintegrity TEST01\STD_SQL_2005
```

Management Console User Interface

The SQL Compliance Manager Management Console online Help provides context-sensitive Help for user interface windows, wizards, tabs, and views in the Management Console. For Help on a specific window, expand this section, and then select the appropriate topic. You can also access these window descriptions from the Management Console by pressing F1 or using the **?** button.

Activity Log Properties window

This window allows you to view details about an individual event in the Activity Log. You can view the following information:

- Date and time the event occurred
- Type of event
- SQL Server instance on which the event occurred

To scroll from one event to the next, use the up and down arrows.

To copy the event details to another application, click **Copy**. This action copies the event details to your clipboard, allowing you to paste the contents into another application such as Microsoft Word.

Activity Log tab

This tab lists events and alerts initiated by the SQL Compliance Manager components, allowing you to monitor SQL CM operations and diagnose issues.

Available actions

View activity details

To view detailed information about a particular event, double-click the event entry in the Activity Log.

View system alerts

To view detailed information about a system alert, double-click the event entry in the Activity Log. SQL compliance manager generates the following types of system alerts.

System Alert	Caused by ...	Resolves when ...
Agent Configuration Error	Error saving the SQLcompliance Agent configuration file (.bin) Error loading the new configuration	File is successfully saved SQLcompliance Agent configuration is successfully updated
Collection Service Connection Error	Collection Server is offline or the SQL Server instance hosting the Repository is offline	Connection to the collection service is established
CLR Error	Error when enabling CLR, creating or modifying the before-after data trigger, or performing a health check	SQLcompliance Agent configuration update or health check is successful
Server Connection Error	Error when connecting to the audited instances, due to invalid permissions or the SQL Server instance being offline	Connection is established
SQL Trace Error	Error when starting or stopping the audit traces	Audit traces are started or stopped
Trace Directory Error	Error when creating trace directory or when reaching the maximum size allocated for the trace directory	Trace directory is created or the trace files are transferred to the Collection Server for processing

Page through activities

Allows you to page through the list of activities. Use the previous and next arrows to navigate from page to page, up and down the list.

Filters

Allows you to filter the listed activities by time span (for example, last seven days).

Enable Groups

Allows you to group activities by a specific property, such as the computers on which the activities occurred or the times the activities occurred. Enable groups when you want to sort the activities or focus on a particular activity attribute.

Refresh

Allows you to update the activity list with current data.

Available columns

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

SQL Server

Provides the name of the SQL Server instance, using the format SQLServerName\InstanceName.

Event

Provides the type of event that occurred.

Details

Displays the first line of the event details.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Add Privileged Users window

This window allows you to specify which privileged users you want to audit. You can specify privileged users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQLcompliance Agent collects events generated by any login who is a member of that role.

Select the logins or fixed server roles you want to audit, and then click **Add**. You can specify both individual logins and roles.

Add User Tables window - Before and after data

This window allows you to specify which user tables you want to audit for before and after data. This setting is available when you choose to audit before and after data at the database level.

Select the user tables you want to audit, and then click **Add**.

If a table contains BLOB data, then you must specify which columns you want to audit. Tables that include BLOB data are displayed in bold type. Note that SQL Compliance Manager does not support auditing BLOB data types. BLOB data includes:

- binary
- images
- ntext
- text
- varbinary
- XML code

Add User Tables window - DML and SELECT statements

This window allows you to specify which user tables you want to audit for DML and SELECT statements. This setting is available when you choose to audit DML or SELECT statements at the database level. You can audit DML and SELECT events on one or more user tables.

Select the user tables you want to audit, and then click **Add**.

Add User Tables window - Sensitive columns

This window allows you to specify which user tables you want to audit for sensitive columns. This setting is available when you choose to audit sensitive columns at the database level.

Select the user tables you want to audit, and then click **Add**.

Alert Message Template window

This window allows you to define a custom alert message. When an alert is triggered, SQL Compliance Manager writes this message to the application event log or emails this message to the specified addresses, depending on your alert rule criteria.

The alert message consists of variables that display specific alert and event properties, such as the alert timestamp, the event ID, and the database affected by the triggering event.

You can accept the default alert message or compose a custom message using the provided variables.

Alert Rules tab

This SQL Compliance Manager tab allows you to create new alert rules and manage existing alert rules. An alert rule is a set of criteria that determines when an alert should be generated as the Collection Server processes SQL Server events collected from your audited instances. Use alert rules to detect events that occur on specific databases, users, or instances.

Available actions

View alert rule description

Use the **Rule Description** pane to quickly see which parameters are configured as criteria for this alert.

Set alert criteria

Use the links in the **Rule Description** pane to change the value or setting of a specific rule criterion.

New Event Alert Rule

Allows you to create a new alert using the New Event Alert Rule wizard. SQL CM stores this alert rule in the Repository.

New Status Alert Rule

Allows you to create a new alert using the New Status Alert Rule wizard. SQL CM stores this alert rule in the Repository.

New Data Alert Rule

Allows you to create a new alert using the New Data Alert Rule wizard. SQL CM stores this alert rule in the Repository.

Create new alert rule from an existing rule

Allows you to create a new alert using the selected rule as a template. This action launches the New Alert Rule wizard, each window populated with alert criteria from the selected rule. You can change any alert criterion to meet the goals of your new alert rule. SQL CM stores the new alert rule in the Repository. The selected rule remains unchanged.

Enable Alert Rule

Allows you to enable the selected rule. When an alert rule is enabled, SQL CM processes audited events using the selected criteria in this rule. ***If an event matches the alert criteria and an alert action is configured***, SQL CM writes an alert message to the application event log or email it to the specified addresses. Alert messages are also available using the Alerts tab.

Disable Alert Rule

Allows you to temporarily stop using the selected rule. SQL CM no longer uses this alert rule when processing events. All alert messages previously generated by this rule will remain available through the Management Console and the application event log, if event log notification was configured. To reinstate this alert, enable the alert rule.

Import Rules

Allows you to import alert rules previously exported from another SQL Server instance. By default, the imported alert rules are disabled.

Export Rules

Allows you to export all previously-created alert rules to an XML file. You can later use this file to import alert rules across multiple SQL Server instances, ensuring consistent alerting on activity throughout your environment.

View Details

Allows you to view or change the alert criteria for the selected rule.

Delete

Allows you to permanently delete the selected rule. Deleting an alert rule removes the rule from the Repository. SQL CM no longer uses this alert rule when processing events. All alert messages previously generated by this rule will remain available through the Management Console and the application event log, if event log notification was configured. ***If you want to temporarily stop using an alert rule***, disable the alert rule.

Refresh

Allows you to update the Alert Rules list with current data.

Available columns

Rule

Provides the name you specified when you created each alert rule. By default, SQL CM names each new rule **New Rule**.

Rule Type

Indicates whether this rule generates an Event Alert or a Status Alert.

SQL Server

Provides the name of the registered SQL Server instance associated with this alert rule. By default, Event and Status Alerts apply to all registered SQL Server instances. For better focused Event Alerts, you can specify a different target SQL Server using the Edit Alert Rule wizard.

Level

Provides the alert level, such as High. Depending on the rule type, you can change the alert level using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

Email

Indicates whether the alert rule criteria includes email notification. When email notification is configured, SQL CM sends an alert message to the specified addresses. Depending on the rule type, you can set up email notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

Event Log

Indicates whether the alert rule criteria includes event log notification. When event log notification is configured, SQL CM writes an alert message to the application event log. Depending on the rule type, you can set up event log notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

Archive Audit Data Now window

This window allows you to archive audit data (collected SQL Server events). Archiving moves the collected audit data from the event database to an archive database for each registered SQL Server you select. ***If an archive database does not exist for the selected SQL Server instance***, the Collection Server creates the archive database. You can continue to report on all audited events that you archive.

Your archive preferences determine which data is moved. Check your preferences before archiving the audit data.

When you archive audit data, you can choose to check the integrity of the collected events. ***If the audit data for the selected SQL Server instance fails this integrity check***, SQL Compliance Manager does not archive the data.

To change your archive settings, click **Archive Preferences**.

To generate a CLI command that includes your archive preferences, click **Generate Script**.

To archive collected audit data now, select the appropriate SQL Servers, and then click **OK**.

Available actions

Archive Preferences

Allows you to set the age at which audited events are archived, specify the time zone the Collection Server uses to determine when to partition an archive database, configure how the archive databases are named, and choose whether to perform an integrity check of the audit data. The Collection Server applies these settings whenever an archive operation is performed.

Generate Script

Creates a CLI command that includes your archive preferences. You can save the command to a batch file or copy the command to another application. Use this command to schedule and automate your archive workflow through a third-party tool.

Available fields

Select SQL Servers to Archive

Allows you to archive audit data across all registered SQL Server instances or on a particular registered SQL Server instance.

Archive Preferences window

This window allows you to set the age at which audited events are archived, configure how the archive databases are partitioned and named, and schedule archiving to run automatically. You can continue to report on all audited events that you archive. SQL Compliance Manager uses these settings each time you archive audited events collected for a registered SQL Server instance.

Available fields

Archive Options

Allows you to configure the following options to control which audit data is archived:

- How old events must be before they are moved to an archive database.
- Which time zone the Collection Server uses to determine when to partition an archive database

You can also skip the integrity check SQL CM usually performs before archiving your collected events. ***If the audit data for the selected SQL Server instance fails this integrity check***, SQL CM does not archive the data.

Archive Schedule

Allows you to configure the following options to control when archiving runs:

- The **Once Daily at** option lets you select the time of day you want archiving to run. The default value is 1:30 AM.
- The **Every week(s) on** options allow you to select one or more days of the week when you want archiving to run as well as the time archiving begins. Note that you cannot schedule different times for different days.
- The **Monthly** options allows you to select a specific day of a specific month and the time when you want archiving to run.

Archive Database Creation

Allows you to configure the following options to control how the archive database is created:

- How often the archive database is partitioned (by month, quarter, or year)
- Naming conventions for the archive databases
- Location where you want the archive database to reside

By default, the Collection Server creates a new archive database at midnight (GMT) when the specified time period (month, quarter, year) ends. For example, if you set archive creation to occur every month, the Collection Server creates a new archive database at midnight on the first day of each month. Each archive database represents a separate data set. You can report on audited events from each archive database.

Archive Properties Window - Default Permissions tab

This tab lets you control the default permission settings at the archive database.

Available fields

Default Database Permissions

Allows you to set the default permissions on the selected archive database. Keep in mind that login permissions will be applied along with the permissions you grant at the archive database level. You can select one of the following default permissions:

- Grant permission to view events and associated SQL statements
- Grant permission to view events only
- Deny permission to view events or SQL statements

Archive Properties Window - General tab

This tab provides the basic properties for the selected archive database. You can specify a different display name or description.

Available fields

SQL Server

Provides the name of the SQL Server instance whose audit data the selected archive contains. This field uses the format `SQLServerName\InstanceName`.

Display Name

Allows you to specify the name you want the Management Console to use when referencing this archive database. By default, the archive name reflects the archive frequency (quarter, month, year) you specified when setting the archive preferences. Consider updating the name to include the type of audit data the archive contains, such as Houston Sales Logins 2005 Q2.

Description

Allows you to specify a description for the selected archive. By default, the archive description reflects the archive preferences you set. Consider updating the description to include more information about the type of audit data the archive contains, such as All attempted logins (failed and successful) on Houston Sales db for the 2005 Q2 period.

Archive database summary

Database Name

Provides the name of selected archive database. This name is automatically generated using the naming conventions you specified in your archive preferences.

Event Time Span

Provides the date and time of the first and last events stored in this archive database.

Database Integrity

Indicates whether the last integrity check performed on this archive database passed or failed.

Last Integrity Check

Provides the date and time an integrity check was last performed on this archive database.

Last Integrity Check Result

Summarizes the results of the last integrity check, such as **Passed** or **Problems found and marked in audit data.**

Archived Events tab

This tab allows you to read previously collected audit data that has been moved to an archive database for storage.

Available actions

Page through events

Allows you to page through the list of events. Use the previous and next arrows to navigate from page to page, up and down the list.

Update databases to use optimized indexes

Allows you to update archive and event databases generated with earlier versions of SQL compliance manager. Updating the databases applies optimized indexes that improve the Management Console performance.

To update the databases, click the provided link. Be aware that this update process requires free disk space, may be resource-intensive, and may take some time to complete. Consider performing database updates during non-peak hours.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Attach

Allows you to load audit data stored in the archive database so you can view and run reports on the events. By default, SQL Compliance Manager loads events from the most recently created archive database.

Detach

Allows you to remove the selected archive database. Removing the archive prevents users from viewing and running reports on the audit data stored in the database.

Filters

Allows you to filter the listed events by time span (for example, last seven days) or event category (for example, security).

Enable Groups

Allows you to group events by a specific property, such as the audited SQL Servers affected by the events or the times the events occurred. Enable groups when you want to sort the events or focus on a particular event attribute.

Archives Properties

Allows you to view details about the selected archive database.

Refresh

Allows you to update the Archives list with current data.

Event Properties

Allows you to view details about the selected event.

Default columns

Icon

Provides a visual indication of the event category so you can quickly scan the listed event for a specific event type, such as security events.

Category

Provides the category SQL Server assigns to this event.

Event

Provides the type of SQL action that caused this event, such as CREATE USER.

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Login

Provides the SQL Server login of the user whose actions generated this event.

Database

Provides the name of the database on which the event occurred.

Target Object

Provides the name of the database object targeted by the T-SQL statement associated with this event.

Details

Provides the text description of the event.

Additional columns

You can add any of these columns to this tab using the **Select Column** action. After you add a new column, you can save the tab as a custom view to reference later.

Access Check

Indicates whether this event passed or failed the SQL Server access check.

Application

Provides the name of the application that initiated this event.

Database User

Provides the name of the database user who executed this event.

Host

Provides the name of the computer where the event was initiated.

Object

Provides the name of the database object affected by this event

Owner

Provides the name of the owner of the database affected by this event.

Privileged User

Indicates whether the user who initiated this event was a privileged user.

Role

Provides the type of SQL Server role assigned to the user who initiated this event.

Server

Provides the name of the SQL Server affected by this event.

Session Login

Provides the login credentials used to open the corresponding session with SQL Server.

SPID

Provides the SQL Server internal process ID of the object affected by the event.

Target Login

Provides the name of the SQL Server login targeted by the T-SQL statement associated with this event.

Target User

Provides the name of the database user targeted by the T-SQL statement associated with this event.

Attach Archive Database window

This window allows you to open an archive database so you can view and report on previously collected audit data.

Available fields

Archive Database

Allows you to select which archive database you want to attach. To view all available databases on the registered SQL Server instances, click **Show all databases**.

Archive Information

Provides general information about the archive database you selected, such as the name of the corresponding SQL Server instance and the last date the archive was updated.

Audit Events tab

This tab allows you to sort and analyze SQL events collected from the SQL Server instances and databases you are auditing.

Available actions

View Before-After data

Allows you to view before and after data for DML events, according to the affected table or column. You can also change the display from a multi-level grid to a flat grid by clicking **Flatten Data**.

For more information about collecting before and after data, see the Before-After Data tab on the Audited Database Properties window.

Page through events

Allows you to page through the list of audited events. Use the previous and next arrows to navigate from page to page, up and down the list.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Filters

Allows you to filter the listed events by time span (for example, last seven days) or event category (for example, security).

Enable Groups

Allows you to group events by a specific property, such as the audited SQL Servers affected by the events or the times the events occurred. Enable groups when you want to sort the events or focus on a particular event attribute.

Refresh

Allows you to update the events list with current data.

Event Properties

Allows you to view details about the selected event.

Default columns

Icon

Provides a visual indication of the event category associated with the event so you can quickly scan the listed events for a specific type, such as a security event.

Category

Provides the name of the event category. The event category corresponds to the activity you are auditing. For example, if you are auditing EXECUTE events on stored procedures, the event category is DML.

Event

Provides the type of event that occurred.

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Login

Provides the name of the SQL login that applied the change, using the format DomainName\LogonName.

Database

Provides the name of the database on which the event occurred.

Target Object

Provides the name of the database object targeted by the T-SQL statement associated with this event.

Details

Provides the text description of the event.

Before-After audit columns

Action

Provides the type of DML event that caused the table column to change (UPDATE, INSERT, or DELETE).

Date

Provides the date that the change occurred.

Time

Provides the time that the change occurred.

Columns Updated

Provides the number of columns that were changed by this event.

Audited Updates

Provides the number of updated columns for which audit data was collected. To collect different data, change audit settings.

Primary Key

Provides the name of the column that uniquely identifies this table. For more information about primary keys, see Microsoft Books Online.

Table

Provides the name of the table affected by this event.

After Value

Provides the value before this column was changed.

Before Value

Provides the value after this column was changed.

Column

Provides the name of the column affected by the event.

Login

Provides the name of the SQL login that applied the change, using the format DomainName\LogonName.

Sensitive Column audit columns

Action

Displays the SELECT event that read the table column.

Application

Provides the name of the application that initiated this event.

Database

Provides the name of the database on which the event occurred.

Date

Provides the date that the change occurred.

Time

Provides the time that the change occurred.

Column

Provides the name of the column affected by the event.

Login

Provides the name of the SQL login that read the column, using the format DomainName\LogonName.

Host

Provides the name of the computer where the event was initiated.

Additional columns

You can add any of these columns to this tab using the **Select Column** action. After you add a new column, you can save the tab as a custom view to reference later.

Access Check

Indicates whether this event passed or failed the SQL Server access check.

Application

Provides the name of the application that initiated this event.

Database User

Provides the name of the database user who executed this event.

Host

Provides the name of the computer where the event was initiated.

Object

Provides the name of the database object affected by this event.

Owner

Provides the name of the owner of the database affected by this event.

Privileged User

Indicates whether the user who initiated this event was a privileged user.

Role

Provides the type of SQL Server role assigned to the user who initiated this event.

Server

Provides the name of the SQL Server affected by this event.

Session Login

Provides the login credentials used to open the corresponding session with SQL Server.

SPID

Provides the SQL Server internal process ID of the object affected by the event.

Target Login

Provides the name of the SQL Server login targeted by the T-SQL statement associated with this event.

Target User

Provides the name of the database user targeted by the T-SQL statement associated with this event.

Audit reports view

This view allows you to generate audit reports using the built-in Microsoft SQL Server Reporting Services Report Viewer (Report Viewer). Each report lets you view and track audited events stored in your event databases and archive files. Use these reports to confirm regulatory compliance, enforce security policies, and capture activity history.

Available actions

Generate a report now

Use the **Audit Reports** tree to navigate to the appropriate report, and then specify your criteria in the report view.

Deploy reports to Microsoft Reporting Services

In the **Reporting Services** pane, click **Deploy Reports**. Starts the Reports Installer, allowing you to deploy individual SQL Compliance Manager reports to your existing Reporting Services server and customize the report.

View which reports have been deployed

In the **Reporting Services** pane, click **View Deployed Reports**. Opens the Report Manager on the Reporting Services server, allowing you to see which SQL CM reports you have deployed.

Available reports

Alert Reports

These reports list alert details, such as target object, affected SQL Server instance, the event, and time of the alert. Use these reports to audit Event and Status Alerts triggered over a specified time period.

- Alert Activity - Events
- Alert Activity - Status

Audit Reports

The Daily Audit Activity Statistics report lists the amount of activity that occurred on the SQL Server instance or designated database, on an hourly basis, for the dates specified. Use this report to audit overall activity levels on your SQL Server instances and databases.

Application Audit Reports

These reports list activity details, such as login, event, and time of activity, per application and database. Use these reports to audit activity across multiple applications and databases.

- Application Activity
- Application Activity Statistics

Database Object Audit Reports

These reports list backup, restore, DBCC, DML, and database object activities on specific databases. Use these reports to audit mass data movement or database object activity, such as SELECT or UPDATE, across multiple databases.

- Backup and DBCC Activity
- DML Activity (Before-After)
- Object Activity

DDL Audit Reports

The Database Schema Change History report lists schema changes applied to audited databases. Use these reports to audit data definition language (DDL) statements, such as dropped tables, executed against one or more databases on a SQL Server instance.

Host Audit Reports

The Host Activity report lists all host computers from which specific logins executed an action. Use this report to audit user behavior from multiple client computers, identifying the host computer from which an activity request originated.

Policy Audit Reports

These reports list changes and updates applied to the SQLcompliance Agent deployed on a specific SQL Server, and any integrity violations in your audit data. Use these reports to diagnose audit data integrity issues and track agent configuration changes as well as agent activities, such as SQLcompliance Agent service restarts.

- Agent History
- Alert Rules
- Audit Control Changes
- Integrity Check

Security Audit Reports

These reports list permission changes by object type as well as unauthorized attempts to execute activities. Use these reports to audit your SQL Server security settings and identify misconduct.

- Change History (by object)
- Change History (by user)
- Permission Denied Activity
- User Login History

User Audit Reports

These reports list user activities performed on a specific SQL Server instance, and provide a history of login creations and deletions. Use these reports to audit user behavior and login management.

- Login Creation History
- Login Deletion History
- Server Login Activity Summary
- User Activity History

Audit Snapshot Preferences window

Allows you to indicate whether you want SQL Compliance Manager to capture a snapshot of your audit settings at a regular interval (days). Each snapshot includes current audit settings for all registered SQL Server instances and audited databases. Captured snapshots are listed on the Change Log tab. By default, SQL CM does not capture audit snapshots.

To schedule audit snapshot captures, specify the appropriate frequency, and then click **Capture Audit Snapshots**.

Audited Database Properties window - Audited Activities tab

This tab allows you to change which types of SQL Server events you want to audit on the selected databases. Use the Audit Events tab to see your collected data.

Available fields

Audited Activities

Allows you select the type of activity you want to audit. Based on your selections, SQL Compliance Manager collects and processes the corresponding SQL Server events.

Access Check Filter

Allows you to refine your audit trail for SQL Server login data by collecting events that better reflect your auditing requirements for security and user processes.

SQL Server validates login permissions and access rights when a user attempts to execute an operation or SQL statement on the audited

SQL Server instance. ***If the access check filter is enabled for a database on a registered instance*** , SQL CM collects access check events at the database level.

Select this filter to help identify logins that may have inappropriate access rights or permissions. This filter may also help reduce the size of your audit data.

Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL server
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Audited Database Properties window - Before-After Data tab

This tab allows you to select the tables for which you want to collect before and after data. You can collect before and after data for DML events generated by DELETE, INSERT, and UPDATE commands.

Collect before and after data when it is critical to capture the exact data change in a table column. When this feature is enabled, you can evaluate the before value and after value for each change in the Audit Events view. Enabling this feature can impact your Collection Server and Management Console performance.

If you want to collect before and after data, verify that you are auditing DML events on this database and that common language runtime (CLR) is enabled on the corresponding SQL Server instance. ***If the target database uses SQL Server replication***, do not enable before-after auditing. Before and after data collection does not support SQL Server replication. For more information, see Microsoft Books Online.

> ⓘ To successfully audit specific columns on a table, ensure the table name does not contain the following special characters: \ / : * ? "

Available actions

Specify tables for before and after data collection

Use **Add and Remove** to specify the tables for which you want to collect before and after data.

Specify which columns to audit

Use **Edit** to specify which columns you want to audit. You can audit all columns or individual columns that do not contain BLOB data.

Select the maximum number of rows to collect

Use **Edit** to select the number of rows per transaction that you want to audit from this table. For example, if you select 100 rows, the SQLcompliance Agent will capture the first 100 rows of each DML transaction, and collect all column updates for each captured row. By default, the first 10 rows per DML transaction are captured.

Enable Now

Allows you to enable CLR on the instance hosting this database.

CLR is required by .NET Framework to access details about DML events on the SQL Server database. For more information, see Microsoft Books Online.

Available fields

Table Name

Provides the name of the table you are auditing on this database.

Maximum Rows

Provides the maximum number of rows that the SQLcompliance Agent will capture of each DML transaction.

Columns

Indicates the status of the columns associated with the audited tables. Typically, this field will display **All Columns** or list the individual columns that are being audited for before and after data.

If the audited table contains BLOB data and individual columns have not yet been selected, the status will display as **Not Configured**. SQL Compliance Manager does not support auditing BLOB data. To audit data changes on this table, click **Edit** and then choose the available columns that do not contain BLOB data.

Set up auditing before and after data

Auditing before and after data is an extension of DML event auditing at the table column level.

1. Ensure Database Modification (DML) activity is selected on the Audited Activities tab.
2. Ensure the appropriate tables are specified on the DML/SELECT Filters tab.
3. On the Before-After Data tab, click **Add** to choose which audited tables should also be audited at the column level for before and after data.
4. Choose the appropriate tables, and then click **OK**. By default, all columns are audited.
5. ***If you want to audit specific columns***, select the table, and then click **Edit**.

Audited Database Properties window - DML/SELECT Filters tab

This tab allows you to change which database objects you want to audit for DML and SELECT statements. These settings are available when you choose to audit DML or SELECT statements on the selected databases. You can audit all database objects or specific database objects, such as user tables and stored procedures.

For example, if you chose to audit SELECT statements on user tables, the Collection Server retrieves SQL Server events that comprise of SELECT operations run on user tables in the audited database.

> ⓘ To successfully audit before and after data, ensure you select the target user tables.

Available actions

Add

Allows you to enable auditing of DML and SELECT events on one or more user tables.

Remove

Allows you to remove the selected user table from the list of audited user tables. When you remove the user table, the SQLcompliance Agent will no longer collect DML and SELECT events recorded for that user table.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Audited Database Properties window - General tab

This tab allows you to view the general properties of the selected database, and specify a description.

Available fields

Server instance

Provides the name of the registered SQL Server instance that is hosting the selected database.

Database name

Provides the name of the selected database you are auditing.

Description

Allows you to specify a description for this database. The Management Console uses this description when you view properties or report on audit data. Consider including information about the data stored on this database, or the organization to which this database belongs.

Auditing status

Indicates whether auditing is currently enabled on this database.

Date created

Provides the date and time when the database was added for auditing. By default, auditing is enabled when the database is added.

Last modified

Provides the date and time when audit settings were last modified for this database.

Last change in auditing status

Provides the date and time when the auditing status of this database changed.

Audited Database Properties window - Sensitive Columns tab

This tab allows you to choose the table columns for which you want to audit SELECT events. This data tells you which third-party application or database user accessed and read the specified columns.

Audit access to sensitive columns when it is critical to capture whether someone read the data in a specific table column. When this feature is enabled, you can review the SELECT events in the Audit Events view. Enabling this feature can impact your Collection Server and Management Console performance. You can audit sensitive columns on specific tables without enabling SELECT statement auditing at the database level.

ⓘ To successfully audit specific columns on a table, ensure the table name does not contain the following special characters: \ / : * ? "

ⓘ Sensitive Column auditing is supported by SQLcompliance Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.

Available actions

Specify tables for before and after data collection

Use **Add and Remove** to specify the tables for which you want to access to specific sensitive columns.

Specify which columns to audit

Use **Edit** to specify which columns you want to audit. You can audit all columns or individual columns.

Available fields

Table Name

Provides the name of the table you are auditing on this database.

Columns

Indicates the status of the columns associated with the audited tables. Typically, this field will display **All Columns** or list the individual columns that are being audited for SELECT events.

Set up auditing sensitive columns

Sensitive column auditing occurs independently from your other database-level audit settings.

1. On the Sensitive Columns tab, click **Add** to choose which audited tables should also be audited at the column level when a user attempts to access this column.
2. Choose the appropriate tables, and then click **OK**. By default, all columns are audited.
3. ***If you want to audit specific columns***, select the table, and then click **Edit**.

Audited Database Properties window - Trusted Users tab

Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited database. The SQLcompliance Agent removes events generated by trusted users from the audit trail before sending the trace file to the Collection Server for processing. This exclusion occurs for all auditing, including DML and SELECT events related to sensitive columns and before and after data.

By designating trusted users, you can more efficiently audit databases used by third-party applications, such as SAP, that are self-auditing. Self-auditing applications are able to audit activity and transactions initiated by their service accounts. Because service accounts can generate a significant number of login and database change events, omitting these expected events from your audit data trail lets you more easily identify unexpected activity.

When you designate trusted users, consider limiting your list to a few specific logins. This approach optimizes event processing performance and ensures you filter the intended accounts.

If you are auditing privileged user activity and the trusted user is also a privileged user, SQL Compliance Manager will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted. Keep in mind that trusted users are filtered at the database level whereas privileged users are audited at the server level.
To omit, or filter, events generated by specific logins and roles from your audit data trail, click **Add**, and then select the SQL Server login or role you want to trust.

> ⓘ When you want to specify multiple accounts as trusted users, consider creating a Windows group that contains only those users. This approach allows you to better manage your trusted users and ensures you do not accidentally trust additional accounts due to unexpected group membership (such as through nested groups). Creating a unique group for trusted users prevents unintended omissions in your audit data.

Available actions

Add a trusted user or role

Allows you to select which SQL Server logins or roles you want to trust on this database. When a login or role is designated as trusted, the SQLcompliance Agent omits all database-level activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

Allows you to designate a previously trusted user or SQL Server role as non-trusted. When a login or role becomes non-trusted, SQL Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

Capture Audit Snapshot window

This window allows you to manually capture an audit snapshot for all registered SQL Server instances or a specific instance. This option provides on-demand configuration data for auditing diagnostics. Audit snapshots include current audit settings for the registered SQL Server instances and audited databases. Captured snapshots are listed on the **Change Log** tab.

Select the type of audit snapshot you want to capture, and then click **OK**.

If you want to capture audit snapshots on a routine basis, consider scheduling snapshots.

Change Log Properties window

This window allows you to view details about an individual event in the Change Log. You can view the following information:

- Date and time the event occurred
- Type of event
- SQL Server instance on which the event occurred
- User who executed the event

To scroll from one event to the next, use the up and down arrows.

To copy the event details to another application, click **Copy**. This action copies the event details to your clipboard, allowing you to paste the contents into another application such as Microsoft Word.

Change Log tab

This tab lists changes and events initiated through the Management Console and the Collection Server, allowing you to monitor SQL Compliance Manager operations and diagnose issues.

Available actions

Page through activities

Allows you to page through the list of activities. Use the previous and next arrows to navigate from page to page, up and down the list.

Filters

Allows you to filter the listed activities by time span (for example, last seven days).

Enable Groups

Allows you to group activities by a specific property, such as the computers on which the activities occurred or the times the activities occurred. Enable groups when you want to sort the activities or focus on a particular activity attribute.

Refresh

Allows you to update the activity list with current data.

Available columns

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Event

Provides the type of event that occurred.

User

Provides the name of the user who applied the change, using the format DomainName\LogonName.

SQL Server

Provides the name of the SQL Server instance, using the format SQLServerName\InstanceName.

Description

Provides the text description of this event.

Check Repository Integrity window

This window allows you to check for unexpected changes in your audit data, detecting when events have been modified, added, or deleted by a script or an application other than SQL Compliance Manager.

Select the Repository database you want to verify, and then click **OK**. To perform an integrity check on an archive database, click **Show archive databases**.

Collection Server Properties window

This window allows you to review the basic properties and status of the Collection Server. You can review the following items:

- Whether the Collection Server is available (up and running)
- Official status
- Name of the computer that hosts the Collection Server
- Port the Collection Server is using to communicate with the Management Console and the SQLcompliance Agent
- Version of Collection Server software (should be the same as the SQL compliance manager build and version number)
- Data and time last heartbeat was received from the SQLcompliance Agent
- Logging levels set at the Collection Server and the SQLcompliance Agent
- Collection Server heartbeat interval
- Location of trace file directory

Available actions

Change Collection Server log level

Allows you to select the logging level at which the Collection Server writes events to the Application log on the host computer.

Change heartbeat interval

Allows you to specify the interval (in minutes) at which the Collection Service processes any status alerts associated with the Collection Server. These alerts are written to the Repository. It also manages any SQL compliance manager maintenance activities, such as re-indexing the Repository databases. By default, the heartbeat interval is 5 minutes.

Start Service

Allows you to restart the Collection Service from the Management Console. Use this feature if the Collection Service has stopped running on the Collection Server computer and requires a manual restart.

Stop Service

Allows you to stop the Collection Service from the Management Console. You can use this feature to stop the Collection Service currently running on the Collection Server computer.

Refresh Status

Allows you to refresh the status fields with the most recent data from the Collection Server.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - Add Databases window

This window allows you to select one or more user databases to audit. When you choose to audit a database, SQL Compliance Manager collects and processes SQL Server events on the database according to your audit settings.

Available actions

Audit Databases

Allows you to enable auditing by capturing SQL events at the database level. After you enable auditing on your databases, set up the audited database properties to enable more advanced auditing, such as sensitive columns and before-and-after data in tables.

Select All

Selects all user databases.

Unselect All

Clears all user database selections.

Available fields

User Databases

Allows you to choose target databases from a list of available databases hosted by this SQL Server instance. This list does not include databases you are currently auditing or databases on which you disabled auditing.

Configuration wizard - Add Server window

This window allows you to specify the SQL Server instance you want to register with SQL Compliance Manager.

Available fields

SQL Server

Allows you to specify the name of the target SQL Server instance, using the format `SQLServerName\InstanceName`. You can also browse for available SQL Server instances in your domain.

Description

Allows you to specify a description for this instance. The Management Console uses this description when you view SQL Server properties or report on audit data. Consider including information about the databases hosted on this instance, or the organization to which this instance belongs.

Configuration wizard - Apply Regulation window

This window allows you to apply regulation guidelines to the selected, audited databases. SQL Compliance Manager configures your audit settings according to the selected guidelines. Note that if you already have audit settings configured, applying new regulation guidelines overrides the existing settings.

After selecting your regulation guidelines and completing the wizard, you must then configure the following audit settings, if not already set:

- Privileged users
- Privileged user audited activity
- Sensitive columns

Check the box for the regulation guidelines you want to enforce, and SQL CM displays a description of that guideline and what it can do for your organization.

Select the regulation guideline(s) you want to apply, and then click **Next**.

Available fields

PCI DSS

Allows you to apply regulation guidelines for the Payment Card Industry Data Security Standard (PCI DSS).

HIPAA

Allows you to apply regulation guidelines for the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - Audit Collection Level window

This window allows you to choose whether to use the default, custom, or regulation audit settings (audit collection levels) for the databases you selected for audit in SQL Compliance Manager.

Select the audit collection level you want to use, and then click **Next**.

Available fields

Default

The **Default** audit collection level allows you to collect the SQL Server events most commonly requested by auditors. This collection level audits the following activities and SQL events:

- Security changes
- Database definition (DDL)
- Administrative activities
- Successful operations only (operations that pass the SQL access check)

Custom

Choosing the **Custom** audit collection level allows you to specify the activities and SQL events you want to audit on these databases. You can also audit system tables. The **Custom** collection level is recommended for advanced users, or for cases in which only one type of data is required for compliance. Before using this collection level, review the event data gathered by the **Default** collection level.

Regulation

The **Regulation** audit collection level configures your audit settings to collect the event data required by specific regulatory guidelines, such as PCI DSS or HIPAA. You can review a list of the collected events on the Regulation Guidelines window of the SQL Compliance Manager Configuration Wizard. On the Summary window at the end of the wizard, click View the Regulation Guideline Details to review a summary of all the regulation guidelines applied to the selected database.

Configuration Wizard - Database Audit Settings window

This window allows you to specify which types of SQL Server events you want to audit on the selected databases in SQL Compliance Manager. This window is available when you choose the Custom audit collection level.

Available fields

Audited Activity

Allows you select the type of activity you want to audit. Based on your selections, SQL CM collects and processes the corresponding SQL Server events.

Access Check Filter

Allows you to refine your audit trail for SQL Server login data by collecting events that better reflect your auditing requirements for security and user processes.

SQL Server validates login permissions and access rights when a user attempts to execute an operation or SQL statement on the audited SQL Server instance. ***If the access check filter is enabled for a database on a registered instance***, SQL CM collects access check events at the database level.

Select this filter to help identify logins that may have inappropriate access rights or permissions. This filter may also help reduce the size of your audit data.

Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL Server
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Configuration wizard - Default Permissions window

This window lets you specify the default permission settings on the Repository databases that contain audit data for this SQL Server instance in SQL Compliance Manager. Keep in mind that login permissions specified at the database take precedence over the default permissions set on this page. This window is available only when you are registering a SQL Server instance with SQL CM for the first time.

Available fields

Grant right to read events and their associated SQL statements

Grant users the right to read events and their associated SQL statements on the database containing audit data for this SQL Server instance.

Grant right to read events only

Grant users the right to read events only. Users cannot read the associated SQL statements when you select this option. To allow users to view the associated SQL statements, you can explicitly grant users read access to the database containing audit data for this SQL Server instance.

Deny read access by default

Deny users the right to read events or their associated SQL statements by default. To allow users to view events and the associated SQL statements, you can explicitly grant users read access to the database containing audit data for this SQL Server instance.

Configuration wizard - DML and SELECT Audit Filters window

This window allows you to specify which database objects you want to audit for DML and SELECT statements in SQL Compliance Manager. These settings are available when you choose to audit DML or SELECT statements on the selected databases, and you are using the Custom audit collection level. You can audit all database objects or specific database objects, such as user tables and stored procedures.

For example, if you chose to audit SELECT statements on user tables, the Collection Server retrieves SQL Server events that comprise of SELECT operations run on user tables in the audited database.

Select the database objects you want to audit, and then click **Next**.

Configuration wizard - Enforce Regulation Guidelines window

This window displays additional information regarding the regulation guideline selections for the audited databases on your SQL Server instance. SQL Compliance Manager provides a list of the information scheduled for collection.

After selecting your regulation guidelines and completing the wizard, you must then configure the following audit settings, if not already set:

- Privileged users
- Privileged user audited activity
- Sensitive columns

After reviewing this information, click **Next**.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - Existing Audit Data window

This window indicates that an event database already exists for this SQL Server instance in SQL Compliance Manager. This database most likely contains previously audited event data. Keeping this audit data ensures you maintain compliance and preserve a record of all audited activities on this SQL Server instance.

Specify whether you want to keep the previously collected audit data and use the existing event database, and then click **Next**.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - Existing Incompatible Database window

This window allows you specify how you want to resolve this situation in SQL Compliance Manager.

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Configuration wizard - License Limit Reached window

This window indicates that you have registered the maximum number of SQL Server instances allowed by your SQL Compliance Manager license. You cannot register any additional instances.

To successfully register additional SQL Server instances, upgrade your license or remove a registered SQL Server instance from SQL CM. For more information, contact Idera Support.

Configuration wizard - Permissions Check window

This window displays the results of a check of the permissions required by SQL compliance manager on the SQL Server instance you want to monitor. This check runs automatically each time you register a new instance.

If the check fails, review the issue, make the required change to the target SQL Server instance, and then click **Re-check**. Once the check in complete, click **Next** to continue.

Required permissions include:

- Collection Service must have rights to the Repository databases
- Collection Service must have rights to read the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance`
- Collection Service must have permissions to the collection trace directory
- Agent Service must have permissions to the agent trace directory
- Agent Service must have rights to read the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance`
- Agent Service must have rights to the SQL Server instance
- SQL Server must have permissions to the agent trace directory
- SQL Server must have permissions to the collection trace directory

ⓘ You can make changes to the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance` to update permissions for your services. for more information about the registry key, see Manage the registry key.

Available actions

Re-check

Allows you to re-check the required permissions after making an update to the target SQL Server instance in case the preliminary check fails.

Available fields

Progress

Displays an icon that shows whether the check is in progress, passed, or failed.

Check

Displays the list of permissions checked in this step.

Status

Displays the current status of the associated check. All checks display **Waiting** until run.

Configuration wizard - Permissions Check Failed window

SQL compliance manager displays the Permissions Check Failed window if one or more permissions check fails.This window includes the number of failed permissions and the steps necessary for you to resolve the issue.

The Configuration wizard runs automatically each time you register a new instance. You can also run this wizard using the menu options if you want to check one or more audited instance. SQLcm then runs these checks on the Collection Service and each Agent for all of the selected SQL Server instances.

> ⓘ While Idera recommends that you do not continue adding this SQL Server instance to SQLcm without all permissions checks passing, you are not forced to delay configuration.

Available actions

Ignore and Continue

Allows you to continue with configuration even when a permission check fails.

Stay and Re-check

Allows you to leave the window open, make any necessary changes to the SQL Server instance permissions, and then runs the permissions audit again.

Configuration wizard - Privileged Users Audited Activity window

This window allows you to specify which activities (events) you want to audit when the selected privileged users perform certain actions. You can choose to audit event categories and user defined events using SQL Compliance Manager. An event category includes related SQL Server events that occur at the server level. A user-defined event is a custom event you create and track using the sp_trace_generateevent stored procedure.

For example, you can audit all activities or only the activities related to specific types of events and actions, such as logins or database modifications (DMLs).

You can also audit activities that either failed or passed the required access check. For example, auditing failed activities allows you to track when a privileged user attempts to execute an action for which the login does not have the appropriate permissions.

Select the activities you want to audit, and then click **Next**.

Available actions

Audit all activities done by privileged users

Allows you to audit all activities involving your privileged users.

Audit selected activities done by privileged users

Allows you to select the privileged user activities you want audited.

Available fields

Audited Activity

Allows you to specify which activities (events) you want to audit for the selected privileged users.

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Configuration wizard - Privileged Users window

This window allows you to select which privileged users you want to audit using SQL Compliance Manager. You can audit individual SQL Server logins with privileged access as well as logins that belong to specific server roles.

To successfully configure privileged user audit settings, the Management Console must have trusted access to the physical computer hosting the target SQL Server instance.

If you are auditing a virtual SQL Server, configure privileged user audit settings after you have deployed the SQLcompliance Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent. For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

If you are auditing a SQL Server instance running in a non-trusted domain or workgroup, configure privileged user audit settings after you have deployed the SQLcompliance Agent to the computer hosting the instance.

Available actions

Add

Allows you to select one or more privileged users to audit. You can select privileged users by login name or by membership to a server role.

Remove

Allows you to remove the selected SQL Server login or server role from the list of audited privileged users. ***If you remove the login or role***, the SQLcompliance Agent will continue collecting events recorded for that login or the role members when these events belong to an audited event category. For example, if you are auditing DML events, any DML event initiated by a privileged user will be included in your audit trail.

Configuration wizard - Regulation Details window

This window displays a table containing all of the regulation guidelines applied to the selected database(s) and what events are affected. You can scroll through the table, sorted by regulation number. If you have more than one set of regulations applied, SQL Compliance Manager displays each set on a tab for ease of use.

You can access this window by clicking the link available on the SQL CM Configuration Wizard Summary window.

Configuration wizard - Sensitive Column window

This window allows you to select the table columns you want SQL Compliance Manager to audit for sensitive column access using SELECT events. This information is important to track whether a third-party application or database user read data in a specific table column.

Enable this feature on a database to review the SELECT events in the Audit Events view. Note that this feature can the performance of your Collection Server and Management Console. You can audit sensitive columns on specific tables without enabling SELECT statement auditing at the database level.

Sensitive column auditing is not available until you deploy an agent to audit the server and a heartbeat is received.

> ⓘ Sensitive Column auditing is supported by SQLcompliance Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.

Available actions

Add

Allows you to select one or more database tables to audit for sensitive columns.

Remove

Allows you to remove the selected database table from the list of audited tables.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - Server Audit Settings window

This window allows you to specify which types of SQL Server events you want to audit on the selected instance. SQL Compliance Manager audits these events at the server level only.

Available fields

Audited Activity

Allows you select the type of activity you want to audit. Based on your selections, SQL CM collects and processes the corresponding SQL Server events. You can choose to audit event categories and user defined events. An event category includes related SQL Server events that occur at the server level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

Access Check Filter

Allows you to refine your audit trail for SQL Server login data by collecting events that better reflect your auditing requirements for security and user processes.

SQL Server validates login permissions and access rights when a user attempts to execute an operation or SQL statement on the audited SQL Server instance. ***If the access check filter is enabled for a registered instance***, SQL CM collects access check events at the server level.

Select this filter to help identify logins that may have inappropriate access rights or permissions. This filter may also help reduce the size of your audit data.

Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL Server
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - SQL Server Cluster window

This window allows you to confirm whether the SQL Server instance you want to audit through SQL Compliance Manager is hosted by a Microsoft failover cluster (managed through Microsoft Cluster Services). A SQL Server instance running in a cluster is a virtual SQL Server. You can audit server and database events for a virtual SQL Server. Use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent.

If you want to audit events on a virtual SQL Server, select the confirmation checkbox, and then click **Next**.

For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

Configuration wizard - SQLcompliance Agent Deployment window

This window allows you to choose when and how you want to deploy the SQLcompliance Agent to the target SQL Server instance. You can deploy the SQLcompliance Agent now or later using the SQL Compliance Manager Management Console, or manually using the setup program.

If you are auditing a virtual SQL Server, you must manually deploy the SQLcompliance Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent. For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

If you are auditing a SQL Server instance hosted by a computer that belongs to a non-trusted domain or a workgroup, you must manually deploy the SQLcompliance Agent to the host computer using the SQL compliance manager setup program.

Choose the deployment option that is appropriate for your environment, and then click **Next**.

Available fields

Deploy Now

Installs the SQLcompliance Agent when you complete the wizard. You must have a connection between the SQL Server that you want to audit and the Management Console.

Deploy Later

Does not install the SQLcompliance Agent. Select this option when you plan to install the SQLcompliance Agent later using the Management Console, such as installing during off-hours.

Manually Deploy

Does not install the SQLcompliance Agent. Select this option when you want to manually install the agent directly on the physical computer hosting the SQL Server instance. Note that this option is required for virtual SQL Server instances and instances located across a domain trust boundary.

Already Deployed

Display only. Informs you that the SQLcompliance Agent is already deployed on the computer hosting this SQL Server instance.

Configuration wizard - SQLcompliance Agent Service Account window

This SQL Compliance Manager window is available when you choose to deploy the SQLcompliance Agent now, and allows you to specify the credentials of the account under which the SQLcompliance Agent Service runs. The SQLcompliance Agent Service uses this account to stop and start SQL Server traces, execute stored procedures, manage trace files, and communicate with the Collection Server. Ensure you specify a valid Windows account that has SQL Server System Administrator privileges on the target SQL Server instance as well as read and write access to the specified trace directory.

Type the account name and password, confirm the password, and then click **Next**.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Configuration wizard - SQLcompliance Agent Trace Directory window

This SQL Compliance Manager window is available when you choose to deploy the SQLcompliance Agent now and allows you to accept the default path for the agent trace directory or specify a different path. The default path is c:\Program Files\Idera\SQLcompliance\AgentTraceFiles. The SQLcompliance Agent stores SQL Server trace files in this directory until the files are sent to the Collection Server.

When SQL CM creates the default trace directory, the directory is secured using ACL settings. Only local administrators have read and write access to this folder.

If you specify a different directory path, ensure the SQLcompliance Agent Service account has read and write privileges on that folder. SQL CM does not change the security settings on existing folders.

Choose whether you want to use the default path for the agent trace directory, and then click **Next**.

Configuration wizard - Summary window

Review the provided summary, and then click **Finish**. When you finish this wizard, SQL Compliance Manager enables auditing on the selected databases. The Collection Server uses the settings you specified to process the raw audit data (SQL Server events) collected from the SQL Server instance.

If you want to change a setting now, click **Previous** to return to the appropriate window. You can also change audit settings later using the Audited Database Properties window.

Click **View the Regulation Guidelines Details** link to view a list of the regulations applied to the selected database(s) for this SQL Server instance.

Configuration wizard - Trusted Users window

Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited database. The SQL Compliance Manager Agent removes events generated by trusted users from the audit trail before sending the trace file to the Collection Server for processing.

By designating trusted users, you can more efficiently audit databases used by third-party applications, such as SAP, that are self-auditing. self-auditing applications are able to audit activity and transactions initiated by their service accounts. Because service accounts can generate a significant number of login and database change events, omitting these expected events from your audit data trail lets you more easily identify unexpected activity.

When you designate trusted users, consider limiting your list to a few specific logins. This approach optimizes event processing performance and ensures you filter the intended accounts.

If you are auditing privileged user activity and the trusted user is also a privileged user, SQL CM will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted. Keep in mind that trusted users are filtered at the database level whereas privileged users are audited at the server level.

To omit, or filter, events generated by specific logins and roles from your audit data trail, click **Add**, and then select the SQL Server login or role you want to trust.

Available actions

Add a trusted user or role

Allows you to select which SQL Server logins or roles you want to trust on this database. When a login or role is designated as trusted, the SQLcompliance Agent omits all database-level activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

Allows you to designate a previously trusted SQL Server login or role as non-trusted. When a login or role becomes non-trusted, SQL CM begins auditing database-level activity generated by this login or role, based on your current audit settings.

Configure Email Settings window

This window allows you to configure SQL Compliance Manager to connect to your mail server. This configuration is required to send alert email notifications.

Available actions

Test your configuration settings

Allows you to verify that SQL CM can connect to your mail server using the specified settings. This test does not verify whether your mail server successfully sent the alert email notification to the specified recipients.

Available fields

SMTP Server

Allows you to specify the name of the computer on which your mail server is running.

Port

Allows you to specify which port your mail server uses for incoming communications.

Requires Authentication

Allows you to indicate whether the mail server requires authentication to connect to the server. ***If authentication is required***, provide the user name and password SQL CM should use to access the mail server.

SSL

Allows you to indicate whether the mail server is configured to use Secure Sockets Layer (SSL) for network communications.

Sender Address

Allows you to specify the email address SQL CM should use to send the alert email notification.

Configure Repository Databases window - Databases tab

This tab allows you to view the status of your Repository databases and update event and attached archive databases created by earlier versions of SQL Compliance Manager.

Available actions

Edit Schedule

Allows you to change the specified scheduled for Repository maintenance activities such as rebuilding indexes.

Update indexes now

Allows you to update archive and event databases generated with earlier versions of SQL Compliance Manager. Updating the databases applies optimized indexes that improve the Management Console performance.

To update the databases, select the appropriate database, and then click **Update Now**. Be aware that this update process requires free disk space, may be resource-intensive, and may take some time to complete. Consider performing database updates during non-peak hours.

Available fields

Database Name

Provides the name of an individual Repository database.

Type

Indicates the type of database, such as an event database or an archive database.

Status

Indicates whether a Repository database should be updated to use the optimized indexes.

Configure Repository Databases window - Recovery Model tab

This tab allows you to select which database recovery model you want the Collection Server to configure when creating databases to store audit data in the Repository. You can choose either the simple model or the default model. The Collection Server applies this setting to new event databases created for each audited SQL Server instance and new archive databases.

A database recovery model controls whether transaction logs are backed up for each database. The simple model does not allow you to back up transaction logs for a database. The default model does allow you to back up transaction logs for a database. The default model is the recovery model configured for the model database. Typically, when a database is created, SQL Server applies the model database properties to the new database. The model database properties on the SQL Server that hosts the Repository should reflect your overall backup and disaster recovery strategies. Before choosing the default recovery model setting, verify that the model database properties are correct.

If you are auditing SQL Servers in a trial environment or have not implemented a backup strategy for the Repository databases, select the simple recovery model.

If you are auditing production SQL Servers and have implemented a backup strategy for the Repository databases, select the default recovery model.

Select the appropriate database recovery model, and then click **OK**.

You can change your selection at any time. When you select a different database recovery model, your change affects new databases only. Ensure you manually change the database recovery model used on each existing Repository database.

Configure Table Auditing window

This window allows you to choose which columns you want to audit from the selected table.

Available actions

Specify how many rows of data to include in the audit stream

Specify how many rows of data you want to capture for each audited column. A single DML transaction can contain multiple rows of data, depending on the modification performed. Consider selecting a low number of rows until you can identify exactly which data you need to audit from the transaction.

Select the columns to audit

Choose whether you want to **Audit All Columns** or **Audit Selected Columns**. You can select any column that does not contain BLOB data.

Connect to Repository window

This window allows you to connect to a different installation of the SQL Compliance Manager Repository. You can type the name of the SQL Server instance that hosts the Repository databases or browse for the instance. ***If the target SQL Server instance is not listed***, verify that the instance is available.

Specify the appropriate SQL Server instance, and then click **OK**.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Console Preferences window - Alert Views window

This window allows you to define the number of alerts that display per view page. Specify the appropriate value, and then click **OK**.

Available actions

Restore Defaults

Allows you to restore the console settings to the default values.

Console Preferences window - Event Views window

This tab allows you to configure how the Management Console displays events in the Audited Events tab. You can also sort events by age, time period, or user by using the event filter provided on the view.

Specify the appropriate value for each setting, and then click **OK**.

Available actions

Restore Defaults

Allows you to restore the console settings to the default values.

Available fields

Event time display

Allows you specify which local time (SQL Server computer time or current system time) the Management Console should use to display event times. By default, the Management Console uses the current system time.

Event view limits

Allows you to specify how you want the Management Console to load events in a view, such as the Audited Events tab. You can configure the view page size (how many events are displayed on a single "page" of the view). You can improve Management Console performance by specifying smaller page sizes.

Data Alerts Tab

This tab allows you to view previously generated Data Alerts. A Data Alert is generated when the Collection Server processes a SQL Server event that matches the alert rule criteria. Use Data Alerts to identify and investigate data manipulation on specific databases, tables, or columns.

> ⓘ The Collection Server generates one alert per SELECT event, even though the query may have accessed multiple audited columns.

Available actions

Page through alerts

Allows you to page through the list of alerts. Use the previous and next arrows to navigate from page to page, up and down the list.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Filters

Allows you to filter the listed alert messages by time span (for example, last seven days) or alert level (for example, high).

Enable Groups

Allows you to group alerts by a specific property, such as the audited SQL Servers affected by the alerts or the times the alerts occurred. Enable groups when you want to sort the alerts or focus on a particular alert attribute.

Event Properties

Allows you to view details about the SQL Server event that triggered this alert. This option is available from the right-click context menu. You can also view event properties by double-clicking an alert from the list.

Alert Message

Allows you to view the message SQL Compliance Manager generated when this alert was triggered. Depending on your alert rule criteria, this message is written to the application event log and emailed to the specified email addresses. The Management Console displays an alert message only when the corresponding alert rule is configured to generate a message.

This action is available from the right-click context menu only.

Refresh

Allows you to update the Data Alerts list with current data.

Default columns

Icon

Provides a visual indication of the alert level so you can quickly scan the listed alerts for a specific alert type, such as a severe alert.

Date

Provides the date when the alert was generated.

Time

Provides the time when the alert was generated.

Level

Indicates the type of alert, such as Severe or Low. Use the alert level to help you identify critical issues, sort alerts by severity, and understand the overall health of your environment. You can define the alert using the Edit Data Alert Rule wizard.

Source Rule

Provides the name of the alert rule that generated this alert.

Event

Provides the name of the audited event that triggered this alert.

SQL Server

Provides the name of the audited SQL Server instance where this event occurred.

Additional columns

You can add any of these columns to this tab using the **Select Column** action. After you add a new column, you can save the tab as a custom view to reference later.

Details

Provides the first line of the alert message associated with this alert.

Subject

Provides the subject line of the alert message associated with this alert.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Deploy SQLcompliance Agent wizard - SQLcompliance Agent Services Account window

This window allows you to specify the credentials of the Windows user account under which the SQLcompliance Agent Service runs. The SQLcompliance Agent Service uses this account to stop and start SQL Server traces, execute stored procedures, manage trace files, and communicate with the Collection Server. Ensure you specify a valid Windows account that has SQL Server System Administrator privileges on the target SQL Server instance.

Type the account name and password, and then click **Next**.

Deploy SQLcompliance Agent wizard - SQLcompliance Agent Trace Directory window

This window allows you to accept the default path for the agent trace directory or specify a different path. The default path is `C:\Program Files\Idera\SQLcompliance\AgentTraceFiles`, and is secured using ACL settings. The SQLcompliance Agent stores SQL Server trace files in this directory until the files can be sent to the Collection Server.

If you specify a different directory path, ensure the SQLcompliance Agent Service account has read and write privileges on that folder. SQL Compliance Manager does not change the security settings on existing folders.

Choose whether you want to use the default path for the agent trace directory, and then click **Next**.

Deploy SQLcompliance Agent wizard - Summary tab

Review the provided summary, and then click **Finish**. When you finish this wizard, SQL Compliance Manager installs the SQLcompliance Agent on the computer that hosts the selected SQL Server instance, and starts the SQLcompliance Agent Service.

When you enable auditing on this SQL Server instance, the SQLcompliance Agent begins managing SQL Server traces and trace files according to the settings you specified.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change agent settings later using the SQLcompliance Agent Properties window.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Deploy Reports wizard - Connect to Reporting Services tab

This tab allows you to specify the Report Server to which you want to deploy the SQL Compliance Manager Reports. The Deploy Reports wizard automatically applies connection settings based on a default Microsoft Reporting Services installation. You can use the default connection settings, or specify custom connection settings.

To specify connection settings, click **Show advanced connection options**, and then enter the appropriate settings.

Click **Next** to continue.

Deploy Reports wizard - Report Deployment Location tab

This tab allows you to specify the name of the folder where the reports should be stored. This folder belongs to the Virtual Directory specified in the Reporting Services connection settings, and is displayed when you access the reports using the Report Manager interface.

You can also specify whether you want to overwrite existing reports. By overwriting existing reports, you ensure all deployed reports are current. ***If you decide not to overwrite existing reports***, the Deploy Reports wizard installs only the reports that are new or updated in this version of SQL Compliance Manager.

Deploy Reports wizard - SQL Compliance Manager Repository tab

This tab allows you to specify which Windows user account SQL Compliance Manager should use to connect to the Repository. You can use the same account that the Collection Service runs under, or you can specify a different account.

Specify the name of the SQL Server instance that hosts the Repository, enter the appropriate account credentials, and then click **Next**.

Deploy Reports wizard - Summary tab

Review the provided summary, and then click **Finish**. When you finish this wizard, SQL Compliance Manager installs the corresponding RDL files in the specified virtual directory on your Report Server.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change your deployment settings later through the Report Manager interface installed with Microsoft Reporting Services.

Deploy Reports wizard - Welcome tab

You can deploy the SQL Compliance Manager Reports to your existing Microsoft Reporting Services installation. SQL CM supports Reporting Services version 2005 or later. If you previously deployed SQL Compliance Manager Reports, verify which version of Reporting Services is currently running in your environment.

For more information, see Reporting Services requirements.

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Edit Data Alert Rule wizard - Alert Actions tab

This tab allows you to change the action you want this alert rule to perform when an audited data matches the specified criteria. Depending on the actions you select, SQL Compliance Manager will write an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL CM is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the Edit Data Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Data Alert Rule wizard - Data Alert Type tab

This tab allows you to change the criteria of this alert rule by editing its parameters in the **Edit rule details** pane.

Available actions

Edit rule details

Allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the Edit Data Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Data Alert Rule wizard - Finish Alert Rule tab

Use the rule details pane to review your changes, and then click **Finish**. When you finish this wizard, SQL Compliance Manager applies your changes.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the alert.

Specify alert level

Allows you to set the severity alerts generated by this rule should have. SQL CM tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL CM to begin monitoring audit data using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your new alert rule. To edit previously set criteria, click the corresponding setting.

Edit Data Alert Rule wizard - SQL Server Object Type tab

This tab allows you to change the type of SQL Server object that should be monitored by this alert rule. You can generate alerts for objects on currently audited databases and SQL Server instances.

Available actions

Select the object that triggers this alert

Allows you to specify the SQL Server object type that should trigger this alert. When the Collection Server processes audit data associated with the specified object type, the alert rule is run to see whether the identified data matches the other alert rule criteria.

By default, the alert rule will apply your alert criteria against audit data from any audited SQL Server instance.
You can control the level at which you want SQL compliance manager to apply this alert:

- SQL Server instance
- Database
- Table
- Column

For example, you can specify the following objects:

- Any column in any table on any database hosted by the Chicago instance
- Any column in any table on the HR01 database hosted by the Chicago instance
- Any column in the Employees table on the HR01 database hosted by the Chicago instance
- The SSN column in the Employees table on the HR01 database hosted by the Chicago instance

Edit rule details

Allows you specify which SQL Server objects the alert rule should use to identify audit data to alert on.

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Data Alert Rule wizard, the rule details grows to include these additional settings.

To edit previously set criteria, click the corresponding setting.

Edit Event Alert Rule wizard - Additional Event Filters tab

This tab allows you to change when the selected event should trigger this alert rule. You can specify more than one condition.

Available actions

Select when this alert should be triggered

Allows you to select the condition under which the alert should trigger. For example, you can specify that the alert rule look for security changes performed by privileged users or only alert on events that are successful.

Edit rule details

Allows you to specify a value for the selected condition, such as true or false.

The rule details pane also allows you to change your specified alert rule criteria at any time as you edit your alert rule. As you specify criteria using the Edit Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Event Alert Rule wizard - Alert Actions tab

This tab allows you to change the action you want this alert rule to perform when an audited event matches the specified criteria. Depending on the actions you select, SQL Compliance Manager will write an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL CM is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you edit your alert rule. As you specify criteria using the Edit Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Event Alert Rule wizard - Finish Alert Rule tab

Use the rule details pane to review your changes, and then click **Finish**. When you finish this wizard, SQL Compliance Manager applies your changes.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the rule, such as AllFailedLogins.

Specify alert level

Allows you to set the severity of alerts generated by this rule should have. SQL Compliance Manager tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL CM to begin monitoring audited events using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your edits. To edit previously set criteria, click the corresponding setting.

Edit Event Alert Rule wizard - SQL Server Event Type tab

This tab allows you to change the type of SQL Server event on which you want to alert.

Available actions

Select type of event that triggers this alert

Allows you to select the SQL Server event type that should trigger this alert. When the Collection Server processes an audited event that matches the specified event type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

You can also select a specific event or a user defined event. A specific event can be any supported SQL Server event that occurs at the server or database level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

Edit rule details

The rule details pane also allows you to change your specified alert rule criteria at any time as you edit your alert rule. As you specify criteria using the Edit Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Event Alert Rule wizard - SQL Server Object Type tab

This tab allows you to change the type of SQL Server object that should be monitored by this alert rule. You can generate alerts for objects on currently audited databases and SQL Server instances.

Available actions

Select the object that triggers this alert

Allows you to specify the SQL Server object type that should trigger this alert. When the Collection Server processes an audited event associated with the specified object type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

By default, the alert rule will generate alerts for matching events on all audited SQL Server instances.
You can specify one or more objects:

Type of Object	You can specify ...
SQL Server instance	• Any instance • A specific instance by name
Database	• A specific database by name • Any database whose name matches a naming convention or phrase
Database object	• A specific database object by name • Any database object whose name matches a naming convention or phrase

For example, you can specify the following objects:

- Any database whose name contains the word test on the LABSERVER instance
- The model database on any audited instance
- The Salary table in the HR01 database hosted by the Chicago instance

Edit rule details

Allows you specify the word or phrase the alert rule should use to identify events associated with the object you want to alert on.

The rule details pane also allows you to change your specified alert rule criteria at any time as you edit your alert rule. As you specify criteria using the Edit Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Event Filter wizard - Finish Event Filter tab

Use the filter details pane to review your changes, and then click **Finish**. When you finish this wizard, SQL Compliance Manager applies your changes.

Available actions

Specify filter name

Allows you to name your event filter. Consider using a unique name that reflects the purpose of the rule.

Specify filter description

Allows you to provide a description for this event filter. Consider including detailed information that can help you diagnose issues later.

Enable filter now

Indicates that you want SQL compliance manager to begin filtering events using this rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review filter details

Allows you to change your specified event filter rule criteria before applying your edits. To edit previously set criteria, click the corresponding setting.

Edit Event Filter wizard - SQL Server Event Object Type tab

This tab allows you to change the type of SQL Server object affected by the filtered event. You can filter events that occur on specific audited databases and SQL Server instances.

Available actions

Select the object that is affected by this event

Allows you to specify the SQL Server object type that is affected by the event you want to filter. For example, you can filter out all DDL activity on a specific database. When the Collection Server processes an audited event associated with the specified object type, the filter run to see whether the identified event matches the other filter criteria.

By default, the filter will apply your criteria against events on any audited SQL Server instance.

You can specify one or more objects:

Type of Object	You can specify ...
SQL Server instance	• Any instance • A specific instance by name
Database	• A specific database by name • Any database whose name matches a naming convention or phrase
Database object	• A specific database object by name • Any database object whose name matches a naming convention or phrase

For example, you can specify the following objects:

- Any database whose name contains the word test on the LABSERVER instance
- The model database on any audited instance
- The Salary table in the HR01 database hosted by the Chicago instance

Edit filter details

Allows you specify the word or phrase the filter should use to identify objects affected by the event you want to filter from your audit data.

The filter details pane also allows you to change your specified criteria at any time as you edit your new filter. As you specify criteria using the Edit Event Filter wizard, the filter details change to include these new settings. To edit previously set criteria, click the corresponding setting.

Edit Event Filter wizard - SQL Server Event Source tab

This tab allows you to change which user (SQL Server login) or application is initializing the SQL Server event you want to filter from your audit data.

Available actions

Select the user or application to filter from your audit data

Allows you to select the specific software application, computer, or SQL Server login you want to filter from your audit data. You can also filter privileged user events.

When the Collection Server processes an audited event that was initiated by the specified application, computer, or user, the filter is run to see whether the identified event matches the other filter criteria.

Edit filter details

Allows you to change your specified criteria at any time as you edit your filter. As you specify criteria using the Edit Event Filter wizard, the filter details change to reflect these new settings. To edit previously set criteria, click the corresponding setting.

Edit Event Filter wizard - SQL Server Event Type tab

This tab allows you to change the type of SQL Server event you want to filter from your audit data.

Available actions

Select type of event to filter from your audit data

Allows you to select the specific SQL Server event category or type you want to filter from your audit data. When the Collection Server processes an audited event that matches the specified event type, the filter is run to see whether the identified event matches the other filter criteria.

Edit filter details

Allows you to change your specified criteria at any time as you edit your filter. As you specify criteria using the Edit Event Filter wizard, the filter details change to reflect these new settings. To edit previously set criteria, click the corresponding setting.

Edit Status Alert wizard - Alert Actions tab

This tab allows you to change the action you want this alert rule to perform when the SQL Compliance Manager status matches the specified criteria. Depending on the actions you select, SQL CM will write an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL CM is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the Edit Status Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Edit Status Alert wizard - Finish Status Alert Rule tab

Specify a name for the different alert rule, review the rule details, and then click **Finish**. When you finish this wizard, SQL Compliance Manager applies your changes.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the alert.

Specify alert level

Allows you to set the severity alerts generated by this rule should have. SQL CM tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL Compliance Manager to begin monitoring the product component status using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your new alert rule. To edit previously set criteria, click the corresponding setting.

Edit Status Alert wizard - Status Alert Type tab

This tab allows you to change the type of SQL Compliance Manager status you want to alert on.

Available actions

Select type of SQL Compliance Manager status that triggers this alert

Allows you to select the product component status that should trigger this alert. When the Collection Server receives a status that matches the specified type, the alert rule is run to see whether the status matches the other alert rule criteria.

Edit rule details

Allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the Edit Status Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Event Alerts tab

This tab allows you to view previously generated Event Alerts. An Event Alert is generated when the Collection Server processes a SQL Server event that matches the alert rule criteria. Use Event Alerts to identify and investigate suspicious activity on specific databases, users, or instances.

Available actions

Page through alerts

Allows you to page through the list of alerts. Use the previous and next arrows to navigate from page to page, up and down the list.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Filters

Allows you to filter the listed alert messages by time span (for example, last 7 days) or alert level (for example, high).

Enable Groups

Allows you to group alerts by a specific property, such as the audited SQL Servers affected by the alerts or the times the alerts occurred. Enable groups when you want to sort the alerts or focus on a particular alert attribute.

Event Properties

Allows you to view details about the SQL Server event that triggered this alert. This option is available from the right-click context menu. You can also view event properties by double-clicking an alert from the list.

Alert Message

Allows you to view the message SQL Compliance Manager generated when this alert was triggered. Depending on your alert rule criteria, this message is written to the application event log and emailed to the specified email addresses. The Management Console displays an alert message only when the corresponding alert rule is configured to generate a message.

This action is available from the right-click context menu only.

Refresh

Allows you to update the Event Alerts list with current data.

Default columns

Icon

Provides a visual indication of the alert level so you can quickly scan the listed alerts for a specific alert type, such as a severe alert.

Date

Provides the date when the alert was generated.

Time

Provides the time when the alert was generated.

Level

Indicates the type of alert, such as Severe or Low. Use the alert level to help you identify critical issues, sort alerts by severity, and understand the overall health of your environment. You can define the alert using the Edit Alert Rule wizard.

Source Rule

Provides the name of the alert rule that generated this alert.

Event

Provides the name of the audited event that triggered this alert.

SQL Server

Provides the name of the audited SQL Server instance where this event occurred.

Additional columns

You can add any of these columns to this tab using the **Select Column** action. After you add a new column, you can save the tab as a custom view to reference later.

Details

Provides the first line of the alert message associated with this alert.

Subject

Provides the subject line of the alert message associated with this alert.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Event Filters tab

This tab allows you to filter out specific SQL events in the audit data collected from the SQL Server instances and databases you are auditing. Use audit Event Filters to refine your audit data trail so that it contains only the events you need to track.

Available actions

Set filter criteria

Use the links in the **Filter Description** pane to change the value or setting of a specific filter criterion.

New Event Filter

Allows you to create a new event filter using the New Event Filter wizard. SQL Compliance Manager stores this event filter in the Repository.

Use Filter as Template

Allows you to create a new event filter using the selected filter as a template. This action launches the New Event Filter wizard, each window populated with event criteria from the selected filter. You can change any event criterion to meet the goals of your new filter. SQL CM stores the new event filter in the Repository. The selected filter remains unchanged.

Enable Filter

Allows you to enable the selected event filter. When an event filter is enabled, SQL Compliance Manager processes audited events using the selected criteria in this filter. ***If an event matches the filter criteria***, SQL CM removes the event from the audit data. Use the Audit Events tab to see the resultant set of processed events.

Disable Filter

Allows you to temporarily stop using the selected event filter. SQL Compliance Manager will no longer use this filter when processing events. All previously processed audit data stored in the Repository remains intact. To reinstate this filter, enable it.

Import Filters

Allows you to import Event Filters previously exported from another SQL Server instance. By default, the imported Event Filters are disabled.

Export Filters

Allows you to export Event Filters created for this SQL Server instance to an XML file. You can later use this file to import Event Filters across multiple SQL Server instances, ensuring consistent filtering of specific events throughout your environment.

View Details

Allows you to view or change the criteria for the selected filter.

Delete

Allows you to permanently delete the selected event filter. This option removes the filter from the Repository. SQL Compliance Manager will no longer use this filter when processing events. All previously processed audit data stored in the Repository remains intact.

Refresh

Allows you to update the Audit Event Filters list with current data.

Available columns

Filter

Provides the name of the audit event filter. You can specify a new name when you create or edit an audit event filter.

SQL Server

Provides the name of the registered SQL Server instance for which audited events are being excluded by this filter.

Description

Provides a brief description of the event filter. You can specify the filter description when you create or edit an event filter.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Event Properties window - Data Change tab

This tab allows you to review how column values changed as a result of the selected event.

This tab is available only when you are collecting before and after data. For more information about collecting before and after data, see Audited Database Properties window - Before-After Data tab.

To scroll from one event to the next, use the up and down arrows.

To copy the event details to another application, click **Copy**. This action copies the event details to your clipboard, allowing you to paste the contents into another application such as Microsoft Word.

Available columns

Row #

Provides the ordered number of the change in the data change set. For example, a DML operation results in seven rows changing. In the **Row #** field, these rows are numbered 1-7 in the order in which each change occurred. You can limit the number of recorded changes for a given operation in the Configure Table Auditing window.

Primary Key

Provides the name of the column that uniquely identifies this table. For more information about primary keys, see Microsoft Books Online.

Column Name

Provides the name of the column affected by the event.

Before Data

Provides the value before this column changed.

After Data

Provides the value after this column changed.

Event Properties window - Details tab

This tab allows you to view details collected for an individual event.

To scroll from one event to the next, use the up and down arrows.

To copy the event details to another application, click **Copy**. This action copies the event details to your clipboard, allowing you to paste the contents into another application such as Microsoft Word.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Event Properties window - General tab

The General tab allows you to view high-level information about an individual event.

You can view the following information:

- Date and time the event occurred
- Type and category of event
- Application where the event occurred
- Database and target object on which the event occurred
- User who executed the event
- Summary of rows and columns changed by this event (if collected)
- Corresponding SQL statement (if audited)

To scroll from one event to the next, use the up and down arrows.

To copy the event details to another application, click **Copy**. This action copies the event details to your clipboard, allowing you to paste the contents into another application such as Microsoft Word.

Explore Activity - Audited SQL Servers Summary tab

The Audited SQL Servers Summary tab displays the status of audit activity across your SQL Server environment. Use the statistics and graphs on this tab to quickly and easily identify issues so you can continue to ensure the correct level of compliance.

Understanding System Status

The System Status pane displays the overall status of your SQL Server environment.

Status

Indicates whether SQL Compliance Manager has encountered any issues while auditing your SQL Server environment.

Clicking the status link opens the more detailed Registered SQL Servers tab under Administration. Use this tab to see the status of audited databases on this instance, validate audit settings, and check the SQLcompliance Agent status.

Status Type	Possible Causes
Alert/Error	• **The Repository is installed on a SQL Server 2000 instance but a SQLcompliance Agent has been deployed to a SQL Server 2005 or later instance.** For example, to audit activity on instances running SQL Server 2005, install a second Repository on a SQL Server 2005 instance. • **A version 1.1 SQLcompliance Agent has been deployed to a SQL Server 2005 or later instance.** Version 1.1 does not support auditing SQL Server 2005 instances. To continuing auditing SQL Server 2005 instances, upgrade the agents to the latest version. • **The SQLcompliance Agent has missed every heartbeat over the last 24 hours.** This issue occurs when the SQLcompliance Agent service is stopped, the Collection Server is offline, the computer hosting the agent is offline, or network availability is lost. • **The SQLcompliance Agent service is no longer running.** The SQLcompliance Agent service is stopped by a SQL Server login or a third-party application. • **A system alert has been triggered.** System alerts notify you when the health of your SQL Compliance Manager deployment may be compromised. For more information, see the Activity Log tab.
OK	SQL Compliance Manager is performing as expected.
Warning	• **No SQL Server instances have been registered with SQL Compliance Manager.** SQL CM cannot begin auditing your environment until instances are registered, SQLcompliance Agents are deployed, and audit settings are configured. • **The SQLcompliance Agent has not yet been deployed to an instance that is registered with SQL Compliance Manager.** S QL CM cannot audit this instance until an agent is deployed and audit settings are configured. • **A deployed SQLcompliance Agent has not yet contacted SQL Compliance Manager.** This issue occurs when the SQLcompliance Agent service is stopped, the computer hosting the agent is offline, or network availability is lost. • **A deployed SQLcompliance Agent has missed two sequential heart beats.** This issue occurs when the SQLcompliance Agent service is stopped, the computer hosting the agent is offline, or network availability is lost.

Registered SQL Servers

Displays the number of SQL Server instances that are registered with SQL CM.

Audited SQL Servers

Displays the number of instances currently being audited. This number does not include instances where auditing is not yet configured or is disabled.

Audited Databases

Displays the number of databases currently being audited. These databases are hosted by SQL Server instances that are registered with SQL CM. This number does not include databases where auditing is not yet configured or is disabled.

Processed Events

Displays the number of audit events stored in the Repository event databases for the selected time span. This number does not include events that were previously archived or groomed.

Understanding the Enterprise Activity Report Card status

Each tab of the Enterprise Activity Report Card provides an auditing status for the corresponding event category. You can use this status to help you determine whether you are effectively auditing events in your environment.

You can also use auditing thresholds to display critical issues or warnings should a particular activity, such as privileged user events, be higher than expected. These thresholds can notify you about issues related to increased activity levels, such as a security breach, that may be occurring on this instance. Use thresholds to supplement the alert rules you have configured for your environment.

Status Type	Indication	Meaning
Audited without thresholds	gray check	This event category is being audited on instances in your environment but auditing thresholds are not set for this event category. Consider setting audit thresholds so you can track peaks in activity and identify any suspicious events.
Critical	red icon	The event activity during the selected time span is higher than the defined critical threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.
OK	green check	This event category is being audited on instances in your environment and auditing thresholds are set for this event category.
Not audited	red icon	This event category is not being audited on instances in your environment even though auditing thresholds are set for this event category. To track this activity, change your audit settings to include the corresponding event category. To ignore this activity, disable the auditing threshold set for this event category.
Not audited and no thresholds set	gray circle	This event category is not being audited on any instances in your environment. Auditing thresholds are not set for this event category. Review whether you need to audit and track this activity on any of your SQL Server instance.
Warning	yellow icon	The event activity during the selected time span is higher than the defined warning threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.

Understanding the Enterprise Activity Report Card tabs

The Enterprise Activity Report Card tabs (Report Card) chart recent activity for each of the common audit event categories and provide the status of each registered SQL Server instance. This activity and status is calculated for the selected time span from the processed audit events stored in the Repository event databases.

Use the Report Card to track the rate of activity in specific event categories and identify when exceptional activity occurs. Auditing thresholds can also help you track and identify activity that could reflect a SQL Server performance or security issue.

To get more detailed information about a particular SQL Server instance, use the provided link.

Understanding Recent Alerts

The Recent Alerts pane displays the number of alerts that are generated for each alert category in the selected time span. ***If you see an unexpected number of alerts***, consider reviewing the current alert messages and then modifying your alert rules to better fit your compliance and auditing needs.

For more information about specific alerts, see the Alerts tab. You can view which alerts have been generated from multiple instances across your environment or from a particular instance.

Available actions

Register SQL Server

Starts the New Registered SQL Server wizard, allowing you to enable and configure auditing on another SQL Server instance.

Monitor

Opens the Change Log tab under Administration, allowing you to monitor what types of changes have been made to audit settings across your environment.

Configure Access

Opens the SQL Logins tab under Administration, allowing you to control who has access to view and report on audit data or change configuration settings.

Self-Audit

Allows you to perform an integrity check on the audit data currently stored in Repository.

Configure Alerting

Opens the Alert Rules tab under Administration, allowing you to configure alerting to track specific activity on SQL Server instances across your environment.

Span

Allows you to change the number of days (time span) for which the Summary tab displays status, alerts, and activity. By default, this tab displays data for the last seven days.

Explore Activity - Database Summary tab

The SQL Compliance Manager Database Summary tab displays the status of audit activity for a particular database hosted by the selected SQL Server instance. Use the statistics and graphs on this tab to quickly and easily identify database-level issues so you can continue to ensure the correct level of compliance.

Understanding Event Distribution

The Event Distribution pane tracks the distribution of audited activity during the selected time span. This pie chart displays how recently collected events are distributed across the commonly audited event categories. You can mouse-over a slice of the pie to see the exact number of events in this category and the percentage of total events this category represents. To verify which event categories you are auditing, see the Audited Activity pane.

Understanding Audited Activity

The Audited Activity pane provides a brief summary of the audit settings configured for the selected database. For more detailed information, review the database audit settings (available from the task ribbon).

Regulation Guideline

Lists the regulation guideline(s) applied to this database.

Database

Lists the event categories currently audited on this database. This list includes auditing settings configured at the database level only.

Before-After

Lists which tables are being audited for before and after data.

Sensitive Columns

Lists which tables are being audited at the column level for SELECT events.

Trusted Users

Displays the number of trusted users that are being excluded from the audit trail.

Event Filters

Displays the number of Event Filters that have been created to streamline audit data collected from this database, and the event properties being used by these filters. Events that match the listed properties are omitted from the audit data trail for this database.

Understanding Recent Database Activity

The Recent Database Activity pane tracks the level of activity during the selected time span. This graph plots the number of recently collected audit events per the commonly audited event categories.

Understanding Recent Audit Events

The Recent Audit Events pane lists the most recent audit events collected for this database during the specified time span. This list displays up to 100 events. To see more details about a specific event, double-click the listed event. To view all audited events collected since your last archive, use the Audit Events tab.

Available actions

Configure Alerting

Opens the Alert Rules tab under Administration, allowing you to configure alerting to track specific activity on this database or other SQL Server instances across your environment.

Configure Event Filters

Opens the Event Filters tab under Administration, allowing you to configure Event Filters that exclude specific types of events from your audit trail, allowing you to eliminate unnecessary events before they are processed by the Collection Server.

Remove Database

Allows you to unregister the selected SQL Server database(s). When you remove a SQL Server database, SQL Compliance Manager disables all auditing for this specific database on the SQL Server instance. Auditing of other databases on this instance continues.

Disable Auditing

Allows you to disable auditing on the selected SQL Server database. When you disable auditing, the SQLcompliance Agent stops collecting new event data for this database and stops the corresponding SQL trace running against that database. You can continue to view and report on previously audited events or archived events.

Disabling auditing at the database level does not disable auditing at the server level or auditing of other databases hosted on the SQL Server instance.

To re-enable auditing, right-click the database from the Explore Activity tree, and then click Enable Auditing on the context menu.

Database Settings

Allows you to change the audit settings for the selected SQL Server database.

Apply Regulation Guideline

Allows you to select one or more regulations to apply to this audited SQL Server database. If you want to apply regulation guidelines to all audited databases on a SQL Server instance, use the **Apply Regulation Guideline** feature from the Explore Activity - Instance Summary tab.

Trusted Users

Allows you to change which SQL Server logins or roles are considered trusted users on the selected SQL Server database. Logins designated as trusted users are not audited at the database level. All events resulting from trusted user activity are filtered from the audit trail before the trace file is sent to the Collection Server for processing.

Import

Allows you to import audit settings previously exported from another audited instance or database.

Export

Allows you to export audit settings for this SQL Server database to an XML file. This file includes audit settings configured at the database level. You can later use this file to import audit settings across multiple databases, ensuring consistent auditing and compliance on a given instance or throughout your environment.

Span

Allows you to change the number of days (time span) for which the Summary tab displays status, events, and activity. By default, this tab displays data for the last seven days.

Explore Activity - Instance Summary tab

The SQL Compliance Manager Instance Summary tab displays the status of audit activity for a particular SQL Server instance in your environment. Use the statistics and graphs on this tab to quickly and easily identify server-level issues so you can continue to ensure the correct level of compliance.

Understanding Server Status

Status

Indicates whether SQL CM encountered any issues while auditing this SQL Server instance. ***If a system alert is triggered***, the status displays as critical. System alerts notify you when the health of your SQL CM deployment may be compromised. For more information, see the Activity Log tab.

Last Heartbeat

Provides the most recent date and time that the SQLcompliance Agent deployed for this instance contacted the Collection Server.

Last Archived

Provides the most recent date and time that events collected for this instance were archived.

Processed Events

Displays the number of audit events stored in the Repository event databases for the selected time span. This number does not include events previously archived or groomed.

Recent Alerts

Displays the number of alerts generated for events collected from this instance during the specified time span.

Understanding the Server Activity Report Card status

Each tab of the Server Activity Report Card provides an auditing status for the corresponding event category. You can use this status to help you determine whether you are effectively auditing events on this SQL Server instance.
You can also use auditing thresholds to display critical issues or warnings should a particular activity, such as privileged user events, be higher than expected. These thresholds can notify you about issues related to increased activity levels, such as a security breach, that may be occurring on this instance. Use thresholds to supplement the alert rules you have configured for this instance.

Status Type	Indication	Meaning
Audited without thresholds	gray check	This event category is being audited on instances in your environment but auditing thresholds have not been set for this event category. Consider setting audit thresholds so you can track peaks in activity and identify any suspicious events.
Critical	red icon	The event activity during the selected time span is higher than the defined critical threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.
OK	green check	This event category is being audited on instances in your environment and auditing thresholds have been set for this event category.
Not audited	red icon	This event category is not being audited on instances in your environment even though auditing thresholds have been set for this event category. To track this activity, change your audit settings to include the corresponding event category. To ignore this activity, disable the auditing threshold set for this event category.

Not audited and no thresholds set	gray circle	This event category is not being audited on any instances in your environment. Auditing thresholds have not been set for this event category. Review whether you need to audit and track this activity on any of your SQL Server instance.
Warning	yellow icon	The event activity during the selected time span is higher than the defined warning threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.

Understanding the Server Activity Report Card tabs

The Server Activity Report Card tabs chart recent activity for each of the common audit event categories and provide the status of this registered SQL Server instance. This activity and status is calculated from the processed audit events stored in the Repository event databases for the selected time span.

Use the Report Card to track the rate of activity in specific event categories and identify when exceptional activity occurs. Auditing thresholds can also help you track and identify activity that could reflect a SQL Server performance or security issue. Using the yellow and red lines that display when warning and critical auditing thresholds are exceeded, you can pinpoint the exact time at which the violations occurred.

When reviewing the Report Card, consider guidelines such as the following tips:

- Too many alerts and failed logins can indicate serious issues
- A sudden spike in privileged user activity could indicate a security breach
- Setting your Overall Activity threshold at 20% above the benchmark activity can warn you when unexpected traffic or database growth occurs

To get more detailed information about a particular increase in activity, use the Recent Audit Events pane to see which events correlated to this activity.

Understanding Audit Configuration

The Audit Configuration pane provides a brief summary of the audit settings configured for the selected SQL Server instance.

For more detailed information, review the properties of the registered instance.

Server

Lists the event categories currently audited on this SQL Server instance. This list includes auditing settings configured at the server level.

Privileged Users

Displays the number of privileged users who are being audited, and the audit settings currently configured to track their activity.

Databases

Indicates the number of databases hosted by this SQL Server instance that are being audited.

Event Filters

Displays the number of Event Filters that have been created to streamline audit data collected from this SQL Server instance, and the event properties being used by these filters. Events that match the listed properties are omitted from the audit data trail for this instance.

Understanding Recent Audit Events

The Recent Audit Events pane lists the most recent audit events collected for this SQL Server instance during the specified time span. This list displays up to 100 events.

To see more details about a specific event, double-click the listed event.

To view all audited events collected since your last archive, use the Audit Events tab.

Available actions

Configure Alerting

Opens the Alert Rules tab under Administration, allowing you to configure alerting to track specific activity on this instance or other SQL Server instances across your environment.

Remove Server

Allows you to unregister the selected SQL Server instance. When you remove a SQL Server instance, SQL Compliance Manager disables all auditing at the server and database levels on the SQL Server instance. ***If the selected instance is the last instance to be audited on this SQL Server***, SQL CM also uninstalls the SQLcompliance Agent. ***If you manually deployed the SQLcompliance Agent***, you must manually uninstall it from the SQL Server computer.

Add Audited Databases

Starts the New Audited Database wizard, allowing you to enable auditing on additional databases hosted by this SQL Server instance.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQLcompliance Agent stops collecting new event data, and stops the corresponding SQL trace. You can continue to view and report on previously audited events or archived events.

To re-enable auditing, right-click the instance from the **Explore Activity** tree, and then click **Enable Auditing** on the context menu.

Server Settings

Allows you to change the audit settings for the selected SQL Server instance.

Apply Regulation Guideline

Allows you to select one or more regulations to apply to all of the audited databases within this SQL Server instance. If you want to apply regulation guidelines only to specific databases, use the **Apply Regulation Guideline** feature from the Explore Activity - Database Summary tab. This option is unavailable if you have no databases selected for audit.

Privileged Users

Allows you to change how privileged user activity is audited on the selected SQL Server instance.

Import

Allows you to import audit settings previously exported from another SQL Server instance. Using the Import Audit Settings wizard, you can specify whether you want to import settings at the server or database level.

Export

Allows you to export audit settings for this SQL Server instance to an XML file. This file includes audit settings configured at the server and database level. You can later use this file to import audit settings across multiple SQL Server instances, ensuring consistent auditing and compliance throughout your environment.

Collect Audit Data

Allows you to force the SQLcompliance Agent to send trace files to the Collection Server for processing. Typically, the SQLcompliance Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

Agent Properties

Allows you to view or change the properties, such as the heartbeat interval and the collection interval, of the SQLcompliance Agent deployed to the selected SQL Server instance.

Span

Allows you to change the number of days (time span) for which the Summary tab displays status, alerts, and activity. By default, this tab displays data for the last 7 days.

Groom Alerts Now window

This window allows you to groom alert messages currently stored in the Repository databases. Grooming permanently deletes any alert message that is older than the age limit you specify.

Available fields

SQL Servers

Allows you to select which SQL Server instance you want to groom. You can groom alerts for all registered SQL Server instances or for a particular SQL Server instance.

Grooming Options

Allows you to specify the age (in days) at which an alert message should be groomed. The Collection Server will not groom alert messages that are younger than the specified age.

Groom Audit Data Now window

This window allows you to groom audited events currently stored in the Repository databases. Grooming permanently deletes any event that is older than the age limit you specify. To improve the Collection Server performance while maintaining audit data for later analysis, consider archiving your audit data.

Available actions

Generate Script

Creates a CLI command that includes your groom settings. You can save the command to a batch file or copy the command to another application. Use this command to schedule and automate your audit data maintenance through a third-party tool.

Available fields

SQL Servers

Allows you to select which SQL Server instance you want to groom. You can groom audit data for all registered SQL Server instances or for a particular SQL Server instance.

Grooming Options

Allows you to specify the age (in days) at which an audited event should be groomed and choose whether you want to skip the integrity check.

The Collection Server will not groom events that are younger than the specified age.

When you groom audit data, you can choose to check the integrity of the collected events. ***If the audit data for the selected SQL Server instance fails this integrity check***, SQL Compliance Manager does not groom the data.

Import Audit Settings wizard - Import Audit Settings window

This window allows you to select which type of audit settings you want to import from the selected XML file.

Available actions

Select server-level audit settings

Allows you to import all server-level audit settings from the selected XML file. This action is available when the selected XML file contains audit settings that were exported at the server level.

Select privileged user audit settings

Allows you to import the privileged user settings from the selected XML file. This action is available when the selected XML file contains audit settings that were exported at the server level.

Select database audit settings

Allows you to import database-level audit settings previously configured for a specific database, using the selected database as a baseline or template. You can import these settings to multiple databases or limit your import to target databases whose names match the baseline database.

For example, if you want to import the audit settings you configured for the HR database, select HR from the database list.

Import Audit Settings wizard - Select File to Import window

The Select File to Import window allows you to specify which audit settings you would like import by selecting the corresponding XML file.

Previously exported audit settings are saved to XML files in the designated folder. By default, the audit settings file names are InstanceName_AuditSettings.xml (for a registered instance and all databases hosted on that instance) and InstanceName_DatabaseName_AuditSettings.xml (for a specific database on a registered instance). These files are stored in the My Documents folder of the user who exported the settings.

Import Audit Settings wizard - Summary window

The Summary window allows you to choose whether to append or overwrite the existing audit settings for the target SQL Server instance or database.

To complete your import, click **Finish**. The Management Console updates the SQLcompliance Agent at the next heartbeat.

Available actions

Add to current audit settings

Appends the existing audit settings the SQLcompliance Agent is using to audit the target SQL Server instance or database with the settings you have chosen to import. The SQLcompliance Agent will use the previous settings and the imported settings to collect events from this instance or database.

Overwrite current audit settings

Overwrites the existing audit settings the SQLcompliance Agent is using to audit the target SQL Server instance or database with the settings you have chosen to import. The SQLcompliance Agent will use only the imported settings to collect events from this instance or database.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Import Audit Settings wizard - Target Databases window

The Target Databases window allows you to select which databases you would like to audit using the imported settings.

You can import audit settings to any audited database. To successfully collect audit data from the target database, ensure auditing is enabled at the database level.

If you previously choose to import audit settings to target databases that matched the names of the source databases, this window will only list the matching databases. To import audit settings to all databases, return to the Import Audit Settings window and clear the Only import for matching database names option.

Available actions

Clear All

Clears all audited databases.

Select All

Selects all audited databases.

Import Audit Settings wizard - Target Servers window

The Target Servers window allows you to select which registered SQL Server instances you would like to audit using the imported settings.

You can import audit settings to any registered SQL Server instance. To successfully collect audit data from the target SQL Server instance, ensure auditing is enabled at the server level.

Available actions

Clear All

Clears all registered SQL Server instances.

Select All

Selects all registered SQL Server instances.

Integrity Check Results window

The Integrity Check Results window allows you to review the results of your audit data integrity check.

If your audit data fails the integrity check, the integrity check returns a list of events that have been inserted, modified, or deleted from the selected Repository or archive database. These events are considered compromised. The integrity check also analyzes the additional data associated with Before-After and Sensitive Column auditing of DML and SELECT events, and indicates whether this data has been compromised as well.

The integrity check results indicate:

- How many individual event entries have been compromised
- How many entries of Before-After change data and column data has been compromised
- How many Sensitive Column entries have been compromised

You can choose whether to mark each compromised event entry in the audit data. Marking these events changes the event class to reflect the compromise and changes the event category to Integrity Check. Use the marked audit data to help diagnose the issues and begin a forensic analysis.

Type of Compromise	New Event Class	New Event Category
Events were added to the audit data stream after archival, using another application	Events inserted	Integrity Check
Events stored in the selected Repository or archive database were modified using another application	Events modified	Integrity Check
Events previously stored in the selected Repository or archive database were deleted using another application	Missing events	Integrity Check

To mark the compromised events as they occur in the audit data, click **Mark Events**.

Login Filtering Options window

The Login Filtering Options window allows you to set login filtering. Login filtering reduces the number of login events stored in your audit data. When login filtering is enabled, the Collection Server searches the trace files sent by the SQLcompliance Agent for duplicate logins that occurred within the specified time period. Duplicate logins are logins with matching user, application, or host names. The Collection Server consolidates these logins into a single event entry in your audit data.

Login filtering is enabled when you audit login events on specific SQL Server instance. By default, the Collection Server searches for duplicate events with time stamps that are within an hour of each other.

Use login filtering to better audit login activity on SQL Server instances where applications, such as SQL Server 2005 Enterprise Studio, frequently open and close connections to SQL Server.

To set login filtering, select the provided checkbox, and specify the appropriate time period.

Login Properties window - Database Access tab

The Database Access tab allows you to specify access on each Repository database. Use this tab if your environment requires permissions settings that tightly control database access. For example, you can deny access to the Repository databases by default, but grant a login access to a specific Repository database.

Select the Repository database on which you want to set permissions, and then select the appropriate permissions.

Your selections are applied along with any default permissions you set when you registered the corresponding SQL Server instance.

Login Properties window - General tab

The General tab allows you to change the security access and SQL Compliance Manager permissions for the selected SQL Server login.

Available fields

Security access

Allows you to specify whether this login should have access to the SQL Server instance that hosts the Repository databases.

Permissions within SQL Compliance Manager

Allows you to indicate which SQL CM permissions this login should have. You can grant the login permission to configure audit settings or view audit data. By default, all logins on the Repository SQL Server instance have read access to audit data. Read access allows the user to view and report on audit data stored in the Repository and archive databases.

Manage SQL Compliance Manager Licenses window

The Manage SQL Compliance Manager Licenses window allows you to view details about your SQL compliance manager product license. You can view the following information:

- Current license key
- Type of license (trial or production)
- Number of SQL Server instances allowed to be licensed with this key
- Expiration date of license

Available actions

Add

Allows you to upgrade an existing product license key or specify a new product license key. Copy the license key into the provided field, and then click **OK**.

Delete

Allows you to permanently decommission a license key. This action removes the license key from the Repository.

New Data Alert Rule wizard - Alert Actions tab

The Alert Actions tab allows you to select the action you want this alert rule to perform when an audited data matches the specified criteria. Depending on the actions you select, SQL Compliance Manager writes an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL CM is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log, emailed to a specific address or distribution list, or send SNMP Trap messages to a specified network management console. SQL CM uses the same alert message content for all notifications.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed
- Server address, port number, and community name of the network management console

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Data Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Data Alert Rule wizard - Data Alert Type tab

The Data Alert Type tab allows you to start setting up an alert that tracks when someone accesses a sensitive column.

Available actions

Edit rule details

Allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Data Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Data Alert Rule wizard - Finish Alert Rule tab

The finish Alert rule tab allows you to specify a name for the new Data Alert rule, review the rule details, and then click **Finish**. When you finish this wizard, SQL Compliance Manager enables the alert rule and begins applying your alert criteria against audit data associated with the selected objects.

If you want to change a setting now, use the rule details pane. You can also change alert rule settings later using the Edit Data Alert Rule wizard.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the alert.

Specify alert level

Allows you to set the severity alerts generated by this rule should have. SQL CM tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL CM to begin monitoring audit data using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your new alert rule. To edit previously set criteria, click the corresponding setting.

New Data Alert Rule wizard - SQL Server Object Type tab

The SQL Server Object Type tab allows you to specify the type of SQL Server object that should be monitored by this alert rule. You can generate alerts for objects on currently audited databases and SQL Server instances.

> ⓘ When you choose to alert on access to specific columns, your choice is limited to the columns you previously selected for Sensitive Column auditing. For example, if you chose to audit only the salary column, you can alert on access to the salary column only. Likewise, if you chose to audit all columns in a table, you can alert on access to any column in that table, but not specific columns.

Available actions

Select the object that triggers this alert

Allows you to specify the SQL Server object type that should trigger this alert. When the Collection Server processes audit data associated with the specified object type, the alert rule is run to see whether the identified data matches the other alert rule criteria.

By default, the alert rule will apply your alert criteria against audit data from any audited SQL Server instance.
You can control the level at which you want SQL compliance manager to apply this alert:

- SQL Server instance
- Database
- Table
- Column

For example, you can specify the following objects:

- Any column in any table on any database hosted by the Chicago instance
- Any column in any table on the HR01 database hosted by the Chicago instance
- Any column in the Employees table on the HR01 database hosted by the Chicago instance
- The SSN column in the Employees table on the HR01 database hosted by the Chicago instance

Edit rule details

Allows you specify which SQL Server objects the alert rule should use to identify audit data to alert on.

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Data Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Alert Rule wizard - Additional Event Filters tab

This tab allows you to define when the selected event should trigger this alert rule. You can specify more than one condition.

Available actions

Select when this alert should be triggered

Allows you to select the condition under which the alert should trigger. For example, you can specify that the alert rule look for security changes performed by privileged users, or only alert on events that are successful.

Edit rule details

Allows you to specify a value for the selected condition, such as true or false.

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Alert Rule wizard - Alert Actions tab

The Alert Actions tab allows you to select the action you want this alert rule to perform when an audited event matches the specified criteria. Depending on the actions you select, SQL Compliance Manager writes an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL CM is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

New Event Alert Rule wizard - Finish Alert Rule tab

The Finish Alert Rule tab allows you to specify a name for the new Event Alert rule, review the rule details, and then click **Finish**. When you finish this wizard, SQL Compliance Manager enables the alert rule and begins applying your alert criteria against audited events associated with the selected objects.

If you want to change a setting now, use the rule details pane. You can also change alert rule settings later using the Edit Event Alert Rule wizard.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the alert.

Specify alert level

Allows you to set the severity alerts generated by this rule should have. SQL Compliance Manager tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL CM to begin monitoring audited events using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your new alert rule. To edit previously set criteria, click the corresponding setting.

SQL Compliance Manager audits all activity on your server. Learn more > >

New Event Alert Rule wizard - SQL Server Event Type tab

The SQL Server Event Type tab allows you to specify on which type of SQL Server event you want to alert.

Available actions

Select type of event that triggers this alert

Allows you to select the SQL Server event type that should trigger this alert. When the Collection Server processes an audited event that matches the specified event type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

You can also select a specific event or a user defined event. A specific event can be any supported SQL Server event that occurs at the server or database level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` sto red procedure.

Edit rule details

Allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Alert Rule wizard - SQL Server Object Type tab

The SQL Server Object Type tab allows you to specify the type of SQL Server object that should be monitored by this alert rule. You can generate alerts for objects on currently audited databases and SQL Server instances.

Available actions

Select the object that triggers this alert

Allows you to specify the SQL Server object type that should trigger this alert. When the Collection Server processes an audited event associated with the specified object type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

By default, the alert rule applies your alert criteria against events on any audited SQL Server instance.
You can specify one or more objects:

Type of Object	You can specify …
SQL Server instance	• Any instance • A specific instance by name
Database	• A specific database by name • Any database whose name matches a naming convention or phrase
Database object	• A specific database object by name • Any database object whose name matches a naming convention or phrase

For example, you can specify the following objects:

- Any database whose name contains the word test on the LABSERVER instance
- The model database on any audited instance
- The Salary table in the HR01 database hosted by the Chicago instance

Edit rule details

Allows you specify the word or phrase the alert rule should use to identify events associated with the object you want to alert on.

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Filter wizard - Finish Event Filter tab

The Finish Event Filter tab allows you to specify a name for the new event filter, review the filter details, and then click **Finish**. When you finish this wizard, SQL Compliance Manager enables the event filter and begins applying your filter criteria against audited events associated with the selected objects.

If you want to change a setting now, use the filter details pane. You can also change event filter settings later using the Edit Event Filter wizard.

Available actions

Specify filter name

Allows you to name your event filter. Consider using a unique name that reflects the purpose of the rule.

Specify filter description

Allows you to provide a description for this event filter. Consider including detailed information that can help you diagnose issues later.

Enable filter now

Indicates that you want SQL Compliance Manager to begin filtering events using this rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review filter details

Allows you to change your specified event filter rule criteria before applying your edits. To edit previously set criteria, click the corresponding setting.

New Event Filter wizard - SQL Server Event Source tab

The SQL Server Event Source tab allows you to specify which user (SQL Server login) or application is initializing the SQL Server event you want to filter from your audit data.

Available actions

Select the user or application to filter from your audit data

> Allows you to select the specific software application, computer, or SQL Server login you want to filter from your audit data. You can also filter privileged user events.
>
> When the Collection Server processes an audited event that was initiated by the specified application, computer, or user, the filter is run to see whether the identified event matches the other filter criteria.

Edit filter details

> Allows you to change your specified criteria at any time as you create your new filter. As you specify criteria using the New Event Filter wizard, the filter details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Filter wizard - SQL Server Event Type tab

The SQL Server Event Type tab allows you to specify the type of SQL Server event you want to filter from your audit data.

Available actions

Select type of event to filter from your audit data

Allows you to select the specific SQL Server event category or type you want to filter from your audit data. When the Collection Server processes an audited event that matches the specified event type, the filter is run to see whether the identified event matches the other filter criteria.

Edit filter details

Allows you to change your specified criteria at any time as you create your new filter. As you specify criteria using the New Event Filter wizard, the filter details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Filter wizard - SQL Server Object Type tab

The SQL Server Object Type tab allows you to specify the type of SQL Server object affected by the filtered event. You can filter events that occur on specific audited databases and SQL Server instances.

Available actions

Select the object that is affected by this event

Allows you to specify the SQL Server object type that is affected by the event you want to filter. For example, you can filter out all DDL activity on a specific database. When the Collection Server processes an audited event associated with the specified object type, the filter is run to see whether the identified event matches the other filter criteria.

By default, the filter will apply your criteria against events on any audited SQL Server instance.
You can specify one or more objects:

Type of Object	You can specify …
SQL Server instance	• Any instance • A specific instance by name
Database	• A specific database by name • Any database whose name matches a naming convention or phrase
Database object	• A specific database object by name • Any database object whose name matches a naming convention or phrase

For example, you can specify the following objects:

- Any database whose name contains the word test on the LABSERVER instance
- The model database on any audited instance
- The Salary table in the HR01 database hosted by the Chicago instance

Edit filter details

Allows you specify the word or phrase the filter should use to identify objects affected by the event you want to filter from your audit data.

The filter details pane also allows you to change your specified criteria at any time as you create your new filter. As you specify criteria using the New Event Filter wizard, the filter details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New SQL Server Login wizard - SQL Compliance Manager Permissions tab

The SQL Compliance Manager Permissions tab allows you to specify which level of permissions this login should have within SQL Compliance Manager. A login can configure audit settings, change console security, view audit data, and run reports.

To allow a login to configure audit settings and console security, SQL CM adds the login to the Systems Administrator (sysadmin) fixed server role on the SQL Server instance that hosts the Repository databases.

Select the appropriate SQL Compliance Manager permission, and then click **Next**.

New SQL Server Login wizard - SQL Server Windows Authentication tab

The SQL Server Windows Authentication tab allows you to specify which Windows user account should be used when creating the SQL Server login to access SQL Compliance Manager. You can also grant or deny security access to the SQL Server instance that hosts the Repository databases.

Type the log name of the Windows user account `(DomainName\UserName)`, select the appropriate security access, and then click **Next**.

New SQL Server Login wizard - Summary tab

The Summary tab allows you to review the provided summary, and then click **Finish**. When you finish this wizard, SQL Compliance Manager creates a SQL Server login with the specified permissions on the SQL Server instance that hosts the Repository databases.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change login settings later using the Login Properties window.

New Status Alert wizard - Alert Actions tab

The Alert Actions tab allows you to select the action you want this alert rule to perform when the SQL Compliance Manager status matches the specified criteria. Depending on the actions you select, SQL CM writes an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL Compliance Manager is configured to connect to your mail server. For more information, see the Configure Email Settings window.

Available actions

Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Status Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Status Alert wizard - Finish Status Alert Rule tab

The Finish Status Alert Rule tab allows you to specify a name for the new alert rule, review the rule details, and then click **Finish**. When you finish this wizard, SQL Compliance Manager enables the alert rule and begins applying your alert criteria against status updates about the specified product component.

If you want to change a setting now, use the rule details pane. You can also change alert rule settings later using the Edit Status Alert Rule wizard.

Available actions

Specify rule name

Allows you to name your alert rule. Consider using a unique name that reflects the purpose of the alert.

Specify alert level

Allows you to set the severity alerts generated by this rule should have. SQL compliance manager tallies the alerts by severity on the Audited SQL Servers Summary tab.

Specify rule description

Allows you to provide a description for this alert rule. Consider including detailed information that can help you diagnose issues later.

Enable rule now

Indicates that you want SQL Compliance Manager to begin monitoring the product component status using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

Review rule details

Allows you to change your specified alert rule criteria before applying your new alert rule. To edit previously set criteria, click the corresponding setting.

New Status Alert wizard - Status Alert Type tab

The Status Alert Type tab allows you to choose the type of SQL compliance manager status you want to alert on.

Available actions

Select type of SQL compliance manager status that triggers this alert

Allows you to select the product components status that should trigger this alert. When the Collection Server receives a status that matches the specified type, the alert rule is run to see whether the status matches the other alert rule criteria.

Edit rule details

Allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Status Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

Registered SQL Server Properties window - Advanced tab

The Advanced tab allows you to configure the following settings:

- Control the default permission settings on the databases that contain audit data for this SQL Server instance.
- Indicate whether collected SQL statements should be truncated if they pass the specified character limit. This option is only available if you are auditing SQL statements executed at the server level on this instance.

Available fields

Default Database Permissions

Allows you to set the default permissions on the databases that contain audit data for this instance. Keep in mind that login permissions specified at the database are applied along with the default permissions you set here. You can select one of the following default permissions:

- Grant permission to view events and associated SQL statements
- Grant permission to view events only
- Deny permission to view events or SQL statements

SQL Statement Limit

Allows you to specify whether you want to truncate collected SQL statements associated with audited events. You can set the character limit for collected SQL statements. By default, this limit is 512 characters. The Collection Server truncates SQL statements that are longer than the specified character limit.

Registered SQL Server Properties window - Audited Activities tab

The Audited Activities tab allows you to change which types of SQL Server events you want to audit on the selected instance. SQL Compliance Manager audits these events at the server level only.

Available fields

Audited Activity

Allows you select the type of activity you want to audit. Based on your selections, SQL CM collects and processes the corresponding SQL Server events.

You can choose to audit event categories and user defined events. An event category includes related SQL Server events that occur at the server level. A user defined event is a custom event you create and track using the sp_trace_generateevent stored procedure.

Access Check Filter

Allows you to refine your audit trail for SQL Server login data by collecting events that better reflect your auditing requirements for security and user processes.

SQL Server validates login permissions and access rights when a user attempts to execute an operation or SQL statement on the audited SQL Server instance. ***If the access check filter is enabled for a registered instance***, SQL CM collects access check events at the server level.

Select this filter to help identify logins that may have inappropriate access rights or permissions. This filter may also help reduce the size of your audit data.

Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL Server
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

SQL Compliance Manager audits all activity on your server. Learn more > >

Registered SQL Server Properties window - Auditing Thresholds tab

The Auditing Thresholds tab allows you to set auditing thresholds to identify unusual activity on the selected SQL Server instance. SQL Compliance Manager reports threshold violations through the Activity Report Cards on the Summary tabs.

Use auditing thresholds to display critical issues or warnings when a particular activity, such as privileged user events, is higher than expected. These thresholds can notify you about issues related to increased activity levels, such as a security breach, that may be occurring on this instance. Auditing thresholds can also inform you when an audited SQL Server instance is becoming non-compliant. Use thresholds to supplement the alert rules you have configured for your environment.

Available fields

Warning

Allows you to specify the number of events you expect to occur in a given event category for the selected time period. When the warning threshold is exceeded, this violation indicates an unusually high number of events. A warning threshold violation can lead to a non-compliant database or SQL Server instance.

Critical

Allows you to specify the maximum number of events that should occur in a given event category for the selected time period. When the critical threshold is exceeded, this violation indicates a serious issue, such as a security breach, which is compromising your ability to remain in compliance with your corporate and regulatory policies.

Period

Allows you to set an acceptable rate, or time span, for the warning and critical thresholds. For example, you may expect overall activity to be no more than 200 events per day on this instance.

Enabled

Allows you to enable (select) or disable (clear) auditing thresholds for a particular event category.

Registered SQL Server Properties window - General tab

The General tab allows you to change the description of this registered SQL Server instance, and view general properties such as audit settings.

Available actions

Update now

Allows you to send audit setting updates to the SQLcompliance Agent running on this SQL Server instance. This action is available when you update audit settings between heartbeats, and the Collection Server has not yet sent your changes to the SQLcompliance Agent.

To diagnose SQLcompliance Agent issues, check the SQLcompliance Agent status and review the SQLcompliance Agent properties.

Available fields

SQL Server instance

Provides the name of the selected SQL Server instance. ***If you are auditing a local instance***, the SQL Server instance name is the name of the physical computer hosting this instance.

Version

Provides the version number of SQL Server running on this registered instance.

Description

Allows you to specify a description for this instance. The Management Console uses this description when you view SQL Server properties or report on audit data. Consider including information about the databases hosted on this instance, or the organization to which this instance belongs.

Status

Provides the current status of this instance. The current status indicates whether SQL Server is available and the SQLcompliance Agent Service and Collection Service are running. Use the Registered SQL Servers tab to see an overview of the status of all registered SQL Server instances.

Date created

Provides the date and time when this instance was registered. By default, auditing is enabled when the instance is registered with SQL Compliance Manager.

Last modified

Provides the date and time when audit settings were last modified on this instance.

Last heartbeat

Provides the date and time when the SQLcompliance Agent auditing this instance contacted the Collect Server. This communication is called a heartbeat. Typically, the SQLcompliance Agent receives audit setting updates during a heartbeat.

Events received

Provides the date and time when the Collection Server last received audited events (SQL trace files) from the SQLcompliance Agent.

Audit Settings

Provides the following information about the status of your audit settings:

- Whether auditing is enabled on this instance
- When the SQLcompliance Agent auditing this instance received the last audit setting updates
- Whether the audit settings are current

If the audit settings are not current, you can send your updates to the SQLcompliance Agent by clicking **Update now**.

Event Database Information

Provides the following information about audited events collected on this instance:

- Name of the database where audited events processed by the Collection Server are stored
- Whether the Repository databases passed the last audit data integrity check
- When the last audit data integrity check was performed

Time of Last Archive

Provides the date and time when audited events collected for this SQL Server instance were last archived.

Last Archive Results

Provides the results of the data integrity check. SQL CM automatically performs a data integrity check each time you archive audited events from the Repository databases.

Registered SQL Server Properties window - Privileged User Auditing tab

The Privileged User auditing tab allows you to change the audit settings currently applied to privileged users on this SQL Server instance. You can choose to audit event categories and user defined events. An event category includes related SQL Server events that occur at the server level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

For example, you can audit individual SQL Server logins with privileged access, logins that belong to specific fixed server roles, all activities, or specific activities.

When you update audit settings to audit privileged user activities, these changes are not applied until the SQL trace is refreshed. The SQL trace is refreshed when the SQLcompliance Agent sends the trace files to the Collection Server. To ensure an immediate application of your new audit settings, click **Update Audit Settings Now** on the Agent menu.

Available actions

Add

Allows you to select one or more privileged users to audit. You can select privileged users by login name or by membership to a fixed server role.

Remove

Allows you to remove the selected SQL Server login or fixed server role from the list of audited privileged users. When you remove the login or role, the SQLcompliance Agent no longer collects events recorded for that login or the role members.

Available fields

Privileged users and roles to be audited

Lists the audited privileged users by login name or fixed server role. ***If you are auditing privileged users in a fixed server role***, the SQLcompliance Agent collects activities executed by all members of the selected role.

Audited Activity

Allows you to specify which activities (events) you want to audit for the selected privileged users.

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Registered SQL Servers tab

The Registered SQL Servers tab lists the SQL Server instances that are registered for SQL Compliance Manager to audit. This list includes the following types of registered servers:

- SQL Server instances running in trusted domains
- SQL Server instances running in non-trusted domains or workgroups
- Virtual SQL Servers hosted by Microsoft failover clusters (Microsoft Cluster Services)

Registering a SQL Server instance allows you to audit events at the server and database levels. You can configure audit settings for each registered instance and hosted database.

This tab lists the registered SQL Server instances you have audited. Auditing allows you to collect specific events from the SQL Server trace. This list contains SQL Servers you are currently auditing. ***If you disabled auditing on a SQL Server instance***, this window continues to list the server until you remove the server.

Available actions

Register New Server

Allows you to register an additional SQL Server instance with SQL CM.

Register New Database

Allows you to enable auditing and configure audit settings for a database on the selected SQL Server instance. To manage settings for a database you are currently auditing, use the Audited Database Properties window.

Enable Auditing

Allows you to enable auditing on the selected SQL Server instance. When you enable auditing, the SQLcompliance Agent begins collecting events on the selected SQL Server instance, and sends the SQL trace files to the Collection Server.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQLcompliance Agent stops collecting new event data, and stops the corresponding SQL trace. You can continue to view and report on previously audited events or archived events.

Server Settings for Audited Server Activities

Allows you to view and modify audit settings for the selected SQL Server instance.

Server Settings for Privileged Users

Allows you to view and modify which privileged users are audited on the selected SQL Server instance.

Database Settings for Audited Database Activities

Allows you to view and modify audit settings for the selected database. This action is available when you select a database from the **Audited Databases** list.

Database Settings for Trusted Users

Allows you to view and modify which users are considered trusted users on the selected database. Trusted users are not audited.

Import

Allows you to import audit settings previously exported from another SQL Server instance or database.

Export

Allows you to export audit settings configured for this SQL Server instance to an XML file. You can later use this file to import audit settings across multiple SQL Server instances or databases, ensuring consistent alerting on activity throughout your environment.

Update Now

Allows you to send your audit setting changes to the SQLcompliance agent immediately. Typically, the Collection Server sends audit setting updates at each heartbeat communication from the SQLcompliance Agent. By default, a heartbeat occurs every five minutes. To view the SQLcompliance Agent heartbeat details, use the General tab on the SQLcompliance Agent Properties window.

Collect Audit Data Now

Allows you to force the SQLcompliance Agent to send trace files to the Collection Server for processing. Typically, the SQLcompliance Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

Agent Properties

Allows you to view and modify settings for the SQLcompliance Agent that is auditing the selected SQL Server instance.

Check Agent Status

Allows you to check the status of the SQLcompliance Agent on the selected SQL Server instance, such as whether or not the agent is active.

Deploy Agent

Allows you to deploy the SQLcompliance Agent to one or more registered SQL Server instances. Deploying the agent installs the SQLcompliance Agent Service on the target instance, and allows you to begin auditing events.

Upgrade Agent

Allows you to upgrade the SQLcompliance Agent on the selected SQL Server instance to the current version. This option is available if the agent was remotely deployed through the Management Console. To upgrade an agent that was manually deployed, run setup.exe from the SQL compliance manager installation kit on the target SQL Server computer.

Change Agent Trace Directory

Allows you to specify a different trace directory for the SQLcompliance Agent. The agent uses the specified folder to store trace files before sending these files to the Collection Server for processing.

Refresh

Allows you to update the Registered SQL Servers list with current information.

Remove

Allows you to unregister the selected SQL Server instance. When you remove a SQL Server instance, SQL Compliance Manager disables all auditing at the server and database levels on the SQL Server instance. ***If the selected instance is the last instance to be audited on this SQL Server***, SQL CM also uninstalls the SQLcompliance Agent. ***If you manually deployed the SQLcompliance Agent***, you must manually uninstall it from the SQL Server computer.

Available columns

SQL Server

Provides the name of the SQL Server instance, using the format SQLServerName\InstanceName.

Status

Indicates whether SQL Compliance Manager detected an auditing or configuration issue. For example, if the selected SQL Server instance is unavailable, SQL CM displays an error.

If a system alert has been triggered, the **Status** column displays the alert type. System alerts notify you when the health of your SQL Compliance Manager deployment may be compromised. For more information, see the Activity Log tab.

Audit Status

Indicates whether auditing is enabled on the selected SQL Server instance. When auditing is disabled, the SQL trace is stopped and the SQLcompliance Agent no longer collects events.

If a system alert is triggered, the Audit Status column instruct you to view the Activity Log to determine which event triggered this alert.

Last Agent Contact

Provides the date and time when the SQLcompliance Agent last received audit setting updates from the Collection Server (also called a heartbeat). To view the SQLcompliance Agent heartbeat details, use the General tab on the SQLcompliance Agent Properties window.

Select SQL Server window

This window allows you to select the SQL Server instance you want to register with SQL Compliance Manager. Choose the appropriate instance from the provided list, and then click **OK**.

If the list does not contain the target SQL Server instance, the instance may not be available or may be located in a non-trusted domain. Ensure the instance is available and accessible from the Management Console computer.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Set Maintenance Schedule window

This window allows you to specify when SQL Compliance Manager should perform maintenance tasks on the Repository, such as rebuilding indexes in the event and archive databases. Because these tasks can be resource-intensive and require extra disk space, consider specifying a time period with slow activity.

Each day, during the specified time, SQL CM continues to execute the required maintenance tasks on any event databases or attached archive database that has not yet been maintained, until all databases are maintained. These tasks are performed as background processes during the allotted time period.

You can view the status of your databases on the Configure Repository Databases window - Databases tab. You can also choose to manually update a database.

> ⓘ Collection Server heartbeat intervalSpecify a duration time that is larger than the . By default, the Collection Server heartbeat is five minutes.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

SNMP Configuration window

This window allows you to specify the server address, port number, and community name of the network management console that you want to receive a SQL CM alert notification as SNMP Trap messages.

Type the appropriate server address, port, and community name in the provided fields, and then click **OK**.

Click **Test** to verify that you entered the proper information for the network management console.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	**Products**	**Purchase**	**Support**	**Resources**	**Community**	**About Us**	**Legal**

Specify Addresses window

This window allows you to specify who should receive an alert email notification. You can specify one or more email addresses for each rule.

Type the appropriate email address in the provided field, and then click **Add**.

Specify Alert Criteria windows

These windows allow you to use words, phrases, and wildcards to further define your alert rule criteria. For example, you can use this window to find and alert on all databases in your environment that use a naming convention such as dbname01.

Available actions

Alert on objects whose names match the listed words, phrases, or wildcards

To alert on objects with specific names or naming conventions, click **listed**, and then specify the words, phrases, or wildcards the object names should match. You can add more than one criterion.

Alert on objects whose names are not listed

To alert on objects whose names are not listed, click **except those listed**, and then specify the words, phrases, or wildcards the object names should not match. You can add more than one criterion.

Available fields

Match all <alert criteria>

Allows you to indicate whether the alert rule should generate alerts for objects that match the listed names, phrases, or wildcards.

Specify <alert criteria> to match

Allows you to define match criteria. Match criteria can include exact names, words, phrases, or wildcards. For each match criterion you want to define, type the appropriate word, phrase, or wildcard in the provided field, and then click **Add**.

Use the following examples to help you define wildcard match criteria. Note that wildcard matches are not case-sensitive.

If you want to match …	Use …	Examples		
One digit	#	*You want:* All databases with name of testNN	*You specify:* test##	*You get:* Test00Test01test#1
One character	?	*You want:* All databases with name of testXX	*You specify:* test??	*You get:* Test00Test01TEST?htester
Any character	*	*You want:* All databases that start with test	*You specify:* test*	*You get:* Test00Test01test0101test4metest#1TEST?htest*devtestertest

<Alert criteria> to match

Allows to you change the list of match criteria. You can add a new criterion or remove an existing criterion.

Specify Event Filter Criteria windows

These windows allow you to use words, phrases, and wildcards to further define your audit event filter criteria. For example, you can use this window to filter out events that occur on all databases in your environment that use a naming convention such as dbname01.

Available actions

Filter events on objects whose names match the listed words, phrases, or wildcards

To filter events on objects with specific names or naming conventions, click **listed**, and then specify the words, phrases, or wildcards the object names should match. You can add more than one criterion.

Filter events on objects whose names are not listed

To filter events on objects whose names are not listed, click **except those listed**, and then specify the words, phrases, or wildcards the object names should not match. You can add more than one criterion.

Available fields

Match all <event filter criteria>

Allows you to indicate whether the event filter should generate alerts for objects that match the listed names, phrases, or wildcards.

Specify <alert criteria> to match

Allows you to define match criteria. Match criteria can include exact names, words, phrases, or wildcards. For each match criterion you want to define, type the appropriate word, phrase, or wildcard in the provided field, and then click **Add**.

Use the following examples to help you define wildcard match criteria. Note that wildcard matches are not case-sensitive.

If you want to match …	Use …	Examples		
One digit	#	*You want:* All databases with name of testNN	*You specify:* test##	*You get:* Test00Test01test#1
One character	?	*You want:* All databases with name of testXX	*You specify:* test??	*You get:* Test00Test01TEST?htester
Any character	*	*You want:* All databases that start with test	*You specify:* test*	*You get:* Test00Test01test0101test4metest#1TEST?htest*devtestertest

<Event filter criteria> to match

Allows to you change the list of match criteria. You can add a new criterion or remove an existing criterion.

SQL Logins tab

This tab allows you to manage the SQL Server login accounts associated with the Repository databases. Use this window to configure SQL Server security access and designate permissions within SQL Compliance Manager.
SQL Compliance Manager leverages the SQL Server security model, using SQL Server logins to authenticate access to the Repository databases and your audit data.

This tab does not list the following logins, which have read access to audit data stored in the Repository databases:

- SQL authentication logins, such as the sa account, who are members of the sysadmin fixed server role
- Windows authentication logins who are members of the local Administrators group

Available actions

New Login

Allows you to create a SQL Server login. SQL compliance manager creates this login at the SQL Server instance that hosts the Repository databases.

View Login Properties

Allows you to view details about permissions settings and database access.

Delete

Allows you to delete the selected SQL Server login. Deleting a login removes the login from the SQL Server instance that hosts the Repository databases. This login will no longer be able to view or report on audit data, and the Windows user account associated with this login will no longer be able to access the Management Console.

Refresh

Allows you to refresh the Logins list with current information.

Available columns

Name

Provides the logon name of the SQL Server login account.

Type

Indicates whether the login is a Windows user or group.

Server Access

Indicates whether security access is permitted or denied to the SQL Server instance that hosts the Repository databases.

Permissions in SQL Compliance Manager

Indicates which SQL Compliance Manager permission the selected login has on the Repository databases.

SQLcompliance Agent Properties window - Deployment tab

This tab allows you to verify how the SQLcompliance Agent was deployed on the selected SQL Server instance. You can view the account used by the SQLcompliance Agent Service as well as the deployment method used.

Available fields

SQLcompliance Agent Service

Provides the name of the user account under which the SQLcompliance Agent is running on this SQL Server instance. The displayed account name uses the format `DomainName\LogonName`.

SQLcompliance Agent Deployment

Indicates which deployment method (automatic or manual) was used to install the SQLcompliance Agent on this SQL Server instance.

SQLcompliance Agent Properties window - General tab

This tab allows you to monitor the health of the SQLcompliance Agent that is auditing the selected SQL Server instance.

If you modifying properties for a SQLcompliance Agent that is auditing a virtual SQL Server, SQL compliance manager applies your changes to the active node in the cluster hosting the virtual SQL Server. SQLcompliance Agent properties are later replicated from the active node to the passive nodes.

Available actions

Update now

Allows you to send any audit setting changes to the SQLcompliance Agent. The SQLcompliance Agent service applies your updates immediately.

Available fields

SQLcompliance Agent Computer

Provides the name of the computer on which the SQLcompliance Agent is installed. This computer hosts the selected SQL Server instance and audited databases.

Agent Status

Provides the status of the agent, such as OK or Not deployed.

Agent version

Provides the version number for the agent. This version number should reflect the product version number.

Agent port

Provides the port number used by the agent to communicate with the Collection Server.

Last heartbeat

Provides the last date and time when the agent successfully communicated with the Collection Server.

Heartbeat interval

Allows you to specify the interval (in minutes) at which the SQLcompliance Agent calls the Collection service and receives audit setting updates. By default, the heartbeat interval is 5 minutes.

Logging level

Allows you to select the logging level at which the SQLcompliance Agent writes events to the Application log on the computer hosting the registered SQL Server instance.

Last agent update

Provides the last date and time when the agent received audit setting updates.

Audit settings status

Indicates whether the agent is using the most current audit settings available.

Audit settings level at agent

Provides the version of the audit settings applied at the agent. ***If the agent audit settings level does not match the current audit settings level***, consider performing an immediate update.

Current audit settings level

Provides the version of the audit settings available at the Collection Server.

SQLcompliance Agent Properties window - SQL Servers tab

This tab allows you to verify which SQL Server instances are currently audited by the SQLcompliance Agent. This list includes instances that are virtual SQL Servers or are running in non-trusted domains and workgroups.

Available columns

SQL Server

Provides the name of the SQL Server instance, using the format `SQLServerName\InstanceName`.

Description

Provides the description you specified when you registered the selected SQL Server instance.

SQLcompliance Agent Properties window - Trace Options tab

This tab allows you to configure how the SQLcompliance Agent manages the trace files that contain collected events for auditing.

If you are modifying properties for a SQLcompliance Agent that is auditing a virtual SQL Server, SQLCompliance Manager applies your changes to the active node in the cluster hosting the virtual SQL Server. SQLcompliance Agent properties are later replicated from the active node to the passive nodes.

Available fields

SQLcompliance Agent Trace Directory

Provides the directory path under which the SQLcompliance Agent stores trace files.

Trace Collection Options

Allows you to specify the following settings:

- The rollover size (MB) at which the SQLcompliance Agent should send the current trace file to the Collection Server, and create a new trace file to continue collecting events
- Time interval (minutes) at which the SQLcompliance Agent should send full trace files to the Collection Server
- Maximum time (minutes) that should elapse before the SQLcompliance Agent sends existing trace files to the Collection Server (if no trace files have been received during the normal collection interval)
- Maximum time (seconds) that should elapse before the SQLcompliance Agent's attempt to stop or start a trace file times out and returns a failure. By default, the timeout value is 30 seconds. Ensure this setting does not exceed the specified collection interval.

Trace Tamper Detection Options

Allows you to specify the amount of time (seconds) that should pass before the SQLcompliance Agent automatically restarts the SQL trace. The SQLcompliance Agent detects whether the trace has been stopped, modified, paused, or deleted by another application. After the specified tamper detection interval, the SQLcompliance Agent restarts the trace and records the trace status to the application event log.

Trace Directory Size Limit

Allows you to specify the maximum size threshold (GB) for the directory where you are storing the trace files. The directory size is checked at each heartbeat. To effectively manage the directory size, ensure you allow ample room to accommodate your auditing needs and set the SQLcompliance Agent heartbeat interval at a low frequency.

Unattended Auditing Time Limit

Allows you to specify the maximum time threshold (days) for allowing the SQLcompliance Agent to run without receiving a heartbeat.

SQLcompliance Agent Trace Directory window

This window allows you to change the location of the agent trace directory. The SQLcompliance Agent temporarily stores collected SQL Server events in the trace directory until the files can be sent to the Collection Server. To optimize performance, consider specifying a directory that is not located on the local disk drive that hosts the databases of the audited SQL Server instance.

If you specify a different directory path, ensure the SQLcompliance Agent Service account has read, write, and delete privileges on that folder. SQL Compliance Manager does not change the security settings on existing folders.

If you are auditing a virtual SQL Server, ensure the specified folder is located on a shared data disk for the selected virtual SQL Server. SQL CM applies this change to the active node in the cluster hosting the virtual SQL Server. SQLcompliance Agent properties are later replicated from the active node to the passive nodes.

To change the trace directory, type the path of the preferred trace directory location, and then click **OK**.

Status Alerts tab

This tab allows you to view previously generated Status Alerts. A Status Alert is generated when the status of the specified product components matches the alert rule criteria. Use Status Alerts to identify and investigate possible issues with SQL compliance manager operations, such as deployed agents that may have stopped running.

Available actions

Page through alerts

Allows you to page through the list of alerts. Use the previous and next arrows to navigate from page to page, up and down the list.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Filters

Allows you to filter the listed alert messages by time span (for example, last 7 days) or alert level (for example, high).

Enable Groups

Allows you to group alerts by a specific property, such as the audited SQL Servers affected by the alerts or the times the alerts occurred. Enable groups when you want to sort the alerts or focus on a particular alert attribute.

Alert Message

Allows you to view the message SQL compliance manager generated when this alert was triggered. Depending on your alert rule criteria, this message is written to the application event log and emailed to the specified email addresses. The Management Console displays an alert message only when the corresponding alert rule is configured to generate a message.

This action is available from the right-click context menu only.

Refresh

Allows you to update the Status Alerts list with current data.

Default columns

Icon

Provides a visual indication of the alert level so you can quickly scan the listed alerts for a specific alert type, such as a severe alert.

Date

Provides the date when the alert was generated.

Time

Provides the time when the alert was generated.

Level

Indicates the type of alert, such as Severe or Low. Use the alert level to help you identify critical issues, sort alerts by severity, and understand the overall health of your environment. You can define the alert using the Edit Alert Rule wizard.

Source Rule

Provides the name of the alert rule that generated this alert.

Rule Type

Provides the type of Status Alert that triggered this alert, such as a Collection Server or SQLcompliance Agent rule.

Computer Name

Provides the name of the SQL Server computer hosting the affected instance. For example, if the SQLcompliance Agent or Collection Server trace directory has reached its size limit, this column displays the name of the computer on which the trace directory folder resides.

SQL Server

Provides either the name of the audited SQL Server instance affected by this alert. For example, if the Collection Server has not received a heartbeat from the SQLcompliance Agent, this column displays the name of the registered instance to which the agent was deployed.

Update Indexes window

This window confirms whether you want to update indexes in the selected Repository databases now or later. Updating indexes optimizes performance when viewing and managing event data.

Before updating the indexes, ensure the selected database has sufficient free space to accommodate these changes. For example, if the current database is 1MB in size, the updated database may grow to 2 MB. In this case, the update process would require 1MB of free space.

Also be aware that this update process may be resource-intensive and may take some time to complete. Consider performing database updates during non-peak hours.

Available actions

Update now

Click **Yes** to update the indexes in all available Repository databases, including event and archive databases.

Update later

Click **Later** to schedule a time when the index updates should be performed.

SQL Compliance Manager audits all activity on your server. Learn more > >

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Cluster Configuration Console User Interface

The SQL Compliance Manager Cluster Configuration online Help provides context-sensitive Help for user interface windows and wizards in the Cluster Configuration Console. For Help on a specific window, expand this section, and then select the appropriate topic. You can also access these window descriptions from the Cluster Configuration Console by pressing F1 or using the **?** button.

Add SQLcompliance Agent Service wizard - Collection Server tab

This tab lets you to specify which computer is currently hosting the Collection Server. The SQLcompliance Agent Service receives audit settings from the Collection Server and sends collected SQL events to the Collection Server for processing. Ensure the SQLcompliance Agent Service has access to the Collection Server computer.

Specify the Collection Server to which the SQLcompliance Agent Service should connect, and then click Next.

Add SQLcompliance Agent Service wizard - General tab

This tab lets you to specify which virtual SQL Server you are planning to audit. The virtual SQL Server is any SQL Server instance hosted by this cluster node. Specifying a virtual SQL Server allows you to begin auditing SQL events generated by activity on this instance. Use the Management Console to specify which server and database events you would like to audit.

Specify the virtual SQL Server you want to audit, and then click **Next**.

Idera Website	Products	Purchase	Support	Resources	Community	About Us	Legal

Add SQLcompliance Agent Service wizard - SQLcompliance Agent Service Account tab

The SQLcompliance Agent Service Account tab lets you specify the account credentials the SQLcompliance Agent Service account should use to connect to the Collection Server and the virtual SQL Server. The SQLcompliance Agent Service also uses this account to stop and start SQL Server traces, execute stored procedures, and manage trace files. Ensure you specify a valid Windows account that has the following permissions:

- SQL Server System Administrator privileges on the target virtual SQL Server
- Administrator permissions on each node in the cluster hosting the virtual SQL Server
- Read and write access to the trace directory you specify

Specify the account the SQLcompliance Agent Service should run under, and then click **Next**.

Add SQLcompliance Agent Service wizard - SQLcompliance Agent Trace Directory tab

The SQLcompliance Agent Trace Directory tab lets you specify which folder should be used for the SQLcompliance Agent trace directory. The SQLcompliance Agent stores SQL Server trace files in this directory until the files can be sent to the Collection Server for processing. The specified folder must be located on a shared data disk for the specified virtual SQL Server. Ensure you specify the same directory path for each node in the cluster hosting the virtual SQL Server.

You can specify an existing folder or a new folder that the Cluster Configuration Console will create for you. When the Cluster Configuration Console creates the trace directory, the directory is secured using ACL settings. Only local administrators have read and write access to the new folder. Ensure the SQLcompliance Agent Service account has read and write privileges on that folder. The Cluster Configuration Console does not change the security settings on existing folders.

Specify the folder where the SQLcompliance Agent should store SQL Server trace files, and then click **Next**.

Add SQLcompliance Agent Service wizard - CLR Trigger Location tab

The CLR Trigger Location tab lets you specify which folder should be used to store the CLR trigger assembly files required to audit before and after data. These assemblies are created by SQL Compliance Manager when you enable before-after auditing for a specific SQL Server database. The SQLcompliance Agent uses the CLR trigger to collect the before and after values of a database object affected by an audited DML event.

Because you are auditing databases hosted by instances running on Windows server cluster nodes, the CLR trigger assemblies must be associated with the same cluster resource group as the audited SQL Server so that before-after auditing can continue when a failover occurs. Thus, the specified folder must be located on a shared data disk for the specified virtual SQL Server. Ensure you specify the same directory path for each node in the cluster hosting the virtual SQL Server.

Specify the folder where the SQLcompliance Agent should store CLR trigger assembly files, and then click **Next**.

Add SQLcompliance Agent Service wizard - Summary tab

Review the provided summary, and then click **Finish**. When you finish this wizard, the Cluster Configuration Console installs the SQLcompliance Agent Service on this cluster node.

When you enable auditing on the virtual SQL Server, the SQLcompliance Agent begins managing SQL Server traces and trace files according to the settings you specified.

If you want to change a setting now, click **Back** to return to the appropriate window. You can also change these settings later using the **Properties** button on the Cluster Configuration Console window.

Cluster Configuration Console window

The Cluster Configuration Console window lets you install and configure the SQLcompliance Agent Service on a cluster node that hosts the virtual SQL Server you want to audit. The cluster node is the physical computer on which you are running the Cluster Configuration Console. When you installed the Cluster Configuration Console, the setup program also installed the SQLcompliance Agent.

Available actions

Add Service

Allows you to install and configure the SQLcompliance Agent Service on this cluster node. When you install the service, you specify which virtual SQL Server will be audited by this service and configure the trace directory folder and service account credentials.

Properties

Allows you to view a subset of properties for the SQLcompliance Agent Service that is auditing the selected virtual SQL Server. To view all properties of the SQLcompliance Agent installed on this cluster node, use the Management Console.

Remove Service

Allows you to uninstall the SQLcompliance Agent Service from this cluster node.

Available fields

SQLcompliance Agent Version

Provides the version number of the SQLcompliance Agent installed on this cluster node.

SQLcompliance Agent Details window

The SQLcompliance Agent Details window lets you view a subset of SQLcompliance Agent properties. To view all properties for the SQLcompliance Agent, use the Management Console.

- Name of the virtual SQL Server audited by this SQLcompliance Agent
- Name of the Collection Server computer that is processing events collected by the SQLcompliance Agent
- Name and location of the trace directory where the SQLcompliance Agent is storing trace files
- Name and location of the CLR trigger assemblies used to collect before and after data for audited DML events
- Name of the SQLcompliance Agent Service under which the SQLcompliance Agent is running
- Name and path of the SQLcompliance Agent Service registry key that is replicated across the cluster nodes

Available actions

To copy either the SQLcompliance Agent Service name or the registry key, click the copy button beside the corresponding field, and then click **OK**
.

Copy the SQLcompliance Agent Service name

> Allows you to copy the name of the SQLcompliance Agent Service to your clipboard. Use this feature to specify the service name when registering the SQLcompliance Agent Service through Microsoft Cluster Administrator. You can paste the copied service name into the required field.

Copy the SQLcompliance Agent Service registry key

> Allows you to copy the path of the SQLcompliance Agent Service registry key that will be replicated across the cluster nodes. The registry path is copied to your clipboard. Use this feature to specify registry replication when registering the SQLcompliance Agent Service through Microsoft Cluster Administrator. You can paste the copied service name into the required field.

Specify CLR Trigger Directory window

This window lets you specify which folder should be used to store the CLR trigger assembly files required to audit before and after data. These assemblies are created by SQL Compliance Manager when you enable before-after auditing for a specific SQL Server database. The SQLcompliance Agent uses the CLR trigger to collect the before and after values of a database object affected by an audited DML event.

Because you are auditing databases hosted by instances running on Windows server cluster nodes, the CLR trigger assemblies must be associated with the same cluster resource group as the audited SQL Server so that before-after auditing can continue when a failover occurs. Thus, the specified folder must be located on a shared data disk for the specified virtual SQL Server. Ensure you specify the same directory path for each node in the cluster hosting the virtual SQL Server.

For each audited instance, specify the folder where the SQLcompliance Agent should store CLR trigger assembly files, and then click **OK**.

Upgrade SQL Server in your audited environment

You can choose one of the following SQL Compliance Manager upgrade strategies. Each strategy meets different goals and auditing needs. Before choosing a strategy, review how you intend to deploy a newer version of SQL Server in your audited environment.

How to use your current installation

Allows you to use your current SQL Compliance Manager installation to audit instances running on multiple versions of SQL Server at the same time in a single environment. This strategy supports a heterogeneous environment and provides a seamless approach to upgrading. As you deploy SQL Server to production servers, you can upgrade the SQLcompliance Agent to support SQL Server 2005 or later event collection.

However, you will need to stop auditing SQL Server events during the time required to upgrade the Collection Server and Repository databases to the new SQL Server version. To prevent potential audit data loss, upgrade the Collection Server and Repository databases during off-hours or other times when there is little or no SQL Server activity.

How to deploy a second installation

Allows you to audit separate homogeneous environments of SQL Server instances, such as a SQL Server 2005 environment and a SQL Server 2008 environment. This strategy requires two installations of SQL Compliance Manager, one in each environment. You can also use this strategy to perform test auditing of SQL Server instances before you deploy the latest SQL Server version on production servers.

Although you can continue auditing your current environment as you deploy the second SQL Compliance Manager installation, you may want to move your audit settings to the new Repository.

Upgrade SQL Server on the Collection Server

You can upgrade the SQL Server software running on the existing Collection Server when you use your current SQL Compliance Manager installation to audit instances running on multiple versions of SQL Server at the same time in a single environment. Use the following checklist and instructions to successfully upgrade the SQL Server software.

Upgrade checklist

☑	**Follow these steps ...**
□	Determine whether you want to upgrade to the latest version of SQL Compliance Manager. To verify whether you are running the latest version, click **Check for Updates** on the Help menu.
□	Choose the appropriate upgrade strategy for your environment and your auditing needs.
□	Ensure your Windows logon account has administrator permissions on the Collection Server computer and sysadmin rights on the SQL Server instance hosting the Repository.
□	Back up your trace directories, especially the Collection Server Trace Directory.
□	Run the Microsoft SQL Server Upgrade Advisor utility on the target instance. For example, for more information about upgrading to SQL Server 2008, see **Upgrade** on the Microsoft Solutions web site at http://www.microsoft.com/sqlserver/2008/en/us/solutions.aspx .

Upgrade instructions

1. ***If you want to use the latest version of SQL Compliance Manager***, Upgrade to this build.
2. Disable auditing on a SQL Server at the server level.
3. Stop the SQLcompliance Agent service. Use the Microsoft Services administrative tool to stop the SQLcompliance Agent service (SQLcompliance Agent) running on the Collection Server computer.
4. Stop the Collection Server service. Use the Microsoft Services administrative tool to stop the Collection Server service (SQLcompliance Collection Service) running on the Collection Server computer.
5. Upgrade SQL Server on the Collection Server computer.
6. Restart the Collection Server service. Use the Microsoft Services administrative tool to restart the Collection Server service (SQLcompliance Collection Service) running on the Collection Server computer.
7. Restart the SQLcompliance Agent service. Use the Microsoft Services administrative tool to restart the SQLcompliance Agent service (SQLcompliance Agent) running on the Collection Server computer.
8. ***If you upgraded SQL Compliance Manager to the latest version***, also upgrade the SQLcompliance Agent remotely.
9. Upgrade the SQL Server software on the computers hosting your audited instances.
10. Begin auditing any new SQL Server instances.

Deploy second Collection Server

Deploy a second Collection Server when you need to audit separate homogeneous environments of SQL Server instances, such as a SQL Server 2005 environment and a SQL Server 2008 environment. For example, you could deploy one Collection Server to dedicated SQL Server 2005 instance in one environment and a second Collection Server to a dedicated SQL Server 2008 instance in another environment. Use the following checklist and instructions to successfully deploy a second Collection Server.

Deployment checklist

☑	**Follow these steps ...**
□	Determine whether you want to upgrade to the latest version of SQL Compliance Manager. To verify whether you are running the latest version, click **Check for Updates** on the Help menu.
□	Choose the appropriate upgrade strategy for your environment and your auditing needs.
□	Ensure the computer that will host the new Collection Server: • Has trusted access to the computers hosting the SQL Server instances you want to audit. • Hosts the same version of SQL Server as the upgraded instances. For example, if some instances were recently upgraded to SQL Server 2008, install the Collection Server on computer hosting SQL Server 2008. • Meets the product hardware, software, and permissions requirements.

Deploy new Collection Server after the SQL Server on an audited instance has been upgraded

1. ***If you want to use the latest version of SQL Compliance Manager***, upgrade your deployment.
2. Use Custom install in the SQL CM setup program to install the new Collection Server.
3. ***If you upgraded SQL Compliance Manager to the latest version***, also upgrade the compliance Agents deployed to the upgraded instances you are auditing.
4. Configure the SQLcompliance Agent to communicate with the new Collection Server.

Deploy new Collection Server to audit new instances

1. ***If you want to use the latest version of SQL Compliance Manager***, upgrade your deployment.
2. Use the Custom install in the SQL CM setup program to install the new Collection Server.
3. Register the instances you want to audit.
4. Begin auditing your new SQL Server instances.

Migrate the Collection Server

You can execute a migration strategy that addresses one of the following situations:

- The Collection Server requires maintenance, such as new hardware or a software upgrade (Microsoft Windows or SQL Server Service Pack).
- The Collection Server becomes permanently unavailable.
- The Collection Server is being decommissioned and replaced.

Establishing a migration strategy for the Collection Server allows you to preserve existing audit settings and collected SQL Server events. You can also continue auditing your SQL Server environment to meet your compliance requirements with minimal disruption.

What is the Collection Server?

The Collection Server is the computer that hosts the Collection Service and the Repository databases. For more information, review the Product components and architecture.

Migration checklist

Use the following checklist to help you migrate your Collection Server.

☑	**Follow these steps ...**
□	Prepare for your migration.
□	Execute your migration by: • Restoring the Repository databases • Deploying the new Collection Server • Configuring the SQLcompliance Agent connection
□	***If you use Microsoft Reporting Services to generate reports about your audit data*** , change the Reporting Services data source to use the restored Repository databases.
□	Test your new Collection Server deployment and setup.

Migration best practices

Before you execute your migration strategy, decide whether you will want to permanently move the Collection Server to another computer.

If you expect to replace the Collection Server , ensure you have an available SQL Server that can be a dedicated host for the Collection Server. This computer should meet or exceed the product requirements.

If you expect to repair the original Collection Server computer , ensure your strategy includes plans to reinstate the original computer once it is repaired. Consider the following guidelines:

- To minimize audit data loss, plan to backup the Repository databases on the temporary Collection Server immediately before reinstating the original Collection Server
- Use these migration procedures to reinstate the Collection Server on the original computer, configure the SQLcompliance agents, and configure Reporting Services
- To verify all components were reinstated correctly, test your implementation
- Uninstall the Collection Server you previously implemented on the temporary computer

Prepare for your migration

A migration strategy moves the Collection Server components to another SQL Server instance, thereby replacing the original Collection Server. You can use a migration strategy to respond to an immediate maintenance need. Use the following procedures and guidelines to implement a new migration strategy or modify an existing migration strategy.

Verify the configuration of the target SQL Server

When identifying the new SQL Server instance that will host the Collection Server, ensure this instance meets or exceeds the product hardware, software, and permissions, as well as these specific requirements:

- The target instance is running the same version or higher of the SQL Server software that is currently running on the existing Collection Server computer
- The current Collection Service account can access the target instance and has the correct permissions on the target instance

Back up the Repository databases

Use a tool such as Idera SQL Safe to perform a full backup of the Repository databases, including transaction logs. You can back up event and archive databases separately from the SQLcompliance databases. However, for best results during a disaster recovery, fully restore all Repository databases at the same time.

Restore the Repository databases

To recover lost or damaged audit data, restore the Repository databases. For best results, use the following guidelines:

- Perform a full restore, including the transaction logs
- Schedule the restore during off-hours, or times when you expect the least audit activity
- Restore all Repository databases during the same restore procedure to ensure audit data integrity remains intact

To restore the Repository databases:

1. Use the SQL Server client tools to close any open connections to the SQLcompliance database.
2. Use the SQL Server client tools to take the SQLcompliance database offline. ***If you cannot take the SQLcompliance database offline***, stop the Collection Service.
3. Use a tool such as Idera SQL Safe to restore the SQLcompliance database using the appropriate backup file, including transaction logs.
4. Use a tool such as Idera SQL Safe to restore each event and archive database using the appropriate backup file, including the transaction logs. Each registered SQL Server instance has a corresponding event database. The number of archive databases depends on your archive preferences and your archive frequency.
5. Use SQL Server client tools to bring the SQLcompliance database online.

Deploy the new Collection Server

Ensure you review the Collection Server requirements before installing. By default, SQL Compliance Manager installs with a trial license. Update the license key to reflect your current production license.

To install the Collection Server:

1. Log on with an administrator account to the computer on which you want to install the Collection Server.
2. Run Setup.exe in the root of the installation kit.
3. Click **Begin Setup** on the Setup tab of the setup program.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking I accept the terms in the license agreement, and then click **Next**.
6. Accept the default folder for your SQL Compliance Manager installation, or click **Change** to specify a different folder, and then click **Next**.
7. Select the **Custom** setup type, and then click **Next**.
8. Select the Collection Server component, and then click **Next**.
9. Specify the location where the Collection Server should store audit data received from the SQLcompliance Agent, and then click **Next**. The specified folder will be the trace file directory on the Collection Server.
10. Specify the Windows user account the Collection service and SQLcompliance Agent service should use to access the Repository, and then click **Next**.
11. Click **Browse** to select the SQL Server instance on which you restored the Repository databases.
12. Specify the authentication the setup program should use to connect to the selected SQL Server, and then click **Next**.
13. Indicate that you want to use the existing Repository databases, and then click **Next**.
14. ***If you want to audit the Repository or other databases associated with the selected SQL Server instance***, click **Yes**, and then click **Next**.
15. Specify the location where the SQLcompliance Agent should store collected audit data, and then click **Next**. The specified folder will be the trace file directory on the audited SQL Server instance.
16. Select whether you want to start the services immediately after install, and then click **Next**.
17. Click **Install**.
18. Click **Finish**.

Configure the SQLcompliance Agent connection

To ensure you successfully continue auditing your registered SQL Servers, configure each SQLcompliance Agent to communicate with the new Collection Server.

Apply this update by changing the Server value of the following registry key on the computer that hosts the registered SQL Server instance:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Idera\ SQLcompliance\SQLcomplianceAgent
```

You can manually apply this update at each registered SQL Server or automate this update using a script. This procedure demonstrates how to use a script, such as a Visual Basic script, to configure the SQLcompliance Agent to communicate to the new Collection Server.

Use this procedure to develop a script that suits your environment. You can run a script locally to update one agent at a time, or remotely to update all agents at the same time.

To configure the SQLcompliance Agent using a script:

1. Define variables for the computers that host the SQLcompliance Agent and the new Collection Server. For example, if you plan to run a Visual Basic script locally on the computer that hosts the SQL Server, your script may include the following code:
   ```
   ' Define the SQL compliance manager Agent server
   strComputer = "SQLServer01"
   strNewCollectionServer = "CollectionServer02"
   ```

2. Declare the SQLcompliance Agent and registry objects. For example, if you plan to run a Visual Basic script locally on the computer that hosts the SQL Server, your script may include the following code:
   ```
   ' Get the SQLcompliance Agent and registry objects
   Set objComplianceAgent = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" _
   & strComputer & "\root\cimv2:Win32_Service='SQLcomplianceAgent'")
   Set objReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\" _
   & strComputer & "\root\default:StdRegProv")
   ```

3. Stop the SQLcompliance Agent Service. For example, if you plan to run a Visual Basic script locally on the computer that hosts the SQL Server, your script may include the following code:
   ```
   ' Stop the SQLcompliance Agent Set flgStopStatus = objComplianceAgent.ExecMethod_("StopService")
   ```

4. Change the registry key. For example, if you plan to run a Visual Basic script locally on the computer that hosts the SQL Server, your script may include the following code:
   ```
   ' Change the location of the Collection Server in the registry
   const HKEY_LOCAL_MACHINE = &H80000002
   strRegAgentPath = "SOFTWARE\Idera\SQLcompliance\SQLcomplianceAgent"
   strServerValName = "Server"
   objReg.GetStringValue HKEY_LOCAL_MACHINE, strRegAgentPath, strServerValName, strOldServer
   objReg.SetStringValue HKEY_LOCAL_MACHINE, strRegAgentPath,strServerValName, strNewCollectionServer
   WScript.Echo "Changed collection server from " & strOldServer & " to " & strNewCollectionServer
   ```

5. Start the SQLcompliance Agent Service. For example, if you plan to run a Visual Basic script locally on the computer that hosts the SQL Server, your script may include the following code:
   ```
   ' Restart the SQLcompliance Agent Set flgStartStatus = objComplianceAgent.ExecMethod_("StartService")
   ```

6. Using an administrator account, run your script to update each SQLcompliance Agent deployed to your registered SQL Servers.

Audit a virtual SQL Server instance

SQL Compliance Manager supports auditing a virtual SQL Server instance including the local instance on a cluster running the Collection Server. Use the following checklist to help you deploy and configure SQL Compliance Manager in a clustered environment.

☑	Follow these steps ...
□	Install SQL Compliance Manager.
□	Identify which virtual SQL Server instances you want to audit.
□	Identify which cluster nodes host each virtual SQL Server instance. Make sure that you identify the currently active node as well as any passive nodes in the same cluster.
□	On each cluster node, open port 5200 for SQLcompliance Agent communication.
□	For each cluster node, identify the folder you want to use for the SQLcompliance Agent trace directory. ***If a cluster node hosts more than one virtual SQL Server instance*** , identify a trace directory for each additional instance you want to audit.
□	For each cluster node, identify the account you want to use for the SQLcompliance Agent Service. Verify that this account can access the computer where you installed the Collection Server. Also make sure that this account belongs to the Administrators group on each node. Review the SQLcompliance Agent Service permission requirements.
□	Deploy the SQLcompliance Agent to each cluster node using the Cluster Configuration setup program.
□	Add the SQLcompliance Agent Service on each cluster node using the Cluster Configuration Console.
□	Register the SQLcompliance Agent Service as a generic service using the Microsoft Cluster Administrator tool.
□	Register each virtual SQL Server instance with SQL Compliance Manager using the Management Console. Note that you must choose manual deployment for the SQLcompliance Agent.
□	Specify the SQL Server events you want to audit on each registered virtual SQL Server instance using the Management Console.
□	Run SQL Compliance Manager. Use report cards and the Audit Events tab to ensure you are auditing the correct SQL Server events.

Deploy SQLcompliance Agent to cluster nodes

Deploying the SQLcompliance Agent allows you to audit SQL traces written by the virtual SQL Server instance. Complete the following procedure on each cluster node that hosts a virtual SQL Server instance, including the currently active node as well as any passive nodes in the same cluster.

This task installs the SQLcompliance Agent and the Cluster Configuration Console.

To deploy the SQLcompliance Agent:

1. Log on to the cluster node using an administrator account. Remember that you must repeat these steps on each cluster node that hosts a virtual SQL Server instance.
2. Run Setup.exe in the root of the installation kit.
3. Under the Install heading, click **Cluster Configuration Console**.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
6. Accept the default installation folder, or click **Change** to specify a different folder.
7. Select whether you want the Cluster Configuration Console to be available to all users who log on to this computer, and then click **Next**.
8. Click **Install**.
9. The Cluster Configuration Console starts. Use this console to add the SQLcompliance Agent service to the cluster node.

Add SQLcompliance Agent Service

Adding the SQLcompliance Agent Service allows the SQLcompliance Agent to communicate with the virtual SQL Server instance and the Collection Server. Complete the following procedure on each cluster node that hosts the virtual SQL Server instance, including the currently active node as well as any passive nodes in the same cluster.

By default, the SQLcompliance Agent Service is named Idera SQLcompliance Agent$*VirtualServerName*.

To add the SQLcompliance Agent Service:

1. Log on to the cluster node using an administrator account.
2. Start the Cluster Configuration Console.
3. Click **Add Service**.
4. Specify or browse to the virtual SQL Server instance you want to audit, and then click **Next**. This instance must be hosted by the current cluster node.
5. Specify the name of the computer where you installed the Collection Server, and then click **Next**.
6. Specify the credentials of the Windows account under which the SQLcompliance Agent Service should run, and then click **Next**.
7. Specify the directory path you want to use for the default trace directory location, and then click **Next**. The trace directory must be located on a shared data disk for the specified virtual SQL Server instance. Specify the same directory path for each node in the cluster hosting the virtual SQL Server instance.
8. Review the summary, and then click **Finish**.

Register the SQLcompliance Agent Service

Registering the SQLcompliance Agent Service with the Microsoft Cluster Administrator allows the Microsoft Cluster Service to manage the SQLcompliance Agent Service in failover situations. This configuration ensures the SQL trace continues to be audited during a failover and no audit data is lost.

Complete the following procedure on one cluster node hosting the virtual SQL Server instance. You can perform this task on the currently active node or on any passive node in the same cluster. The Microsoft Cluster Administrator tool replicates your completed configuration to the remaining nodes in the cluster.

To register the SQLcompliance Agent Service:

1. Log on to the cluster node using an administrator account.
2. ***If this is a Windows Server 2003 cluster*** , start the Microsoft Cluster Administrator tool. ***If this is a Windows 2008 cluster*** , start the Microsoft Failover Cluster Administrator tool.
3. Add the SQLcompliance Agent Service as a generic service.

   Specify the following dependencies:
   - Disk where the SQLcompliance Agent trace directory is located
   - SQL network name
   - SQL Server

   Specify the following generic service permissions:
   - Specify a friendly name for the generic service.
   - Specify the name of the SQLcompliance Agent Service (as displayed in the Services Manager tool), but leave the parameters unspecified. Use the SQLcompliance Agent Details window in the Cluster Configuration Console to copy the service name to your clipboard. Paste the name in the provided field.
   - Clear the start parameter setting.
   - Select to use the network name.
4. Agree to replicate registry entries, and then specify the registry key for the SQLcompliance Agent Service. Use the SQLcompliance Agent Details window in the Cluster Configuration Console to copy the registry key path to your clipboard. Paste the name in the provided field.
5. Bring the generic service online.
6. Ensure the SQLcompliance Agent is running on the active cluster node.

Start auditing the virtual SQL Server

After you install and configure the SQLcompliance Agent on each node of the Microsoft failover cluster where the virtual SQL Server instance is running, you can test your configuration and begin auditing the instance.

To audit the virtual SQL Server:

1. Verify that the SQLcompliance Agent is running.
2. Use the Registered Server Properties window to modify the existing audit settings or configure additional audit settings for server-level events.
3. Use the New Audited Database wizard to configure the audit settings for all databases hosted by the virtual SQL Server instance.

Stop auditing the virtual SQL Server

When you decide to stop auditing a virtual SQL Server instance, use the following procedure to remove your configuration settings and uninstall the SQLcompliance Agent.

To stop auditing the virtual SQL Server:

1. Use the Microsoft Cluster Administrator tool to remove the registered generic service you created for the SQLcompliance Agent Service. You can perform this task on any node of the cluster hosting the virtual SQL Server instance.
2. Use the Cluster Configuration Console window to remove the SQLcompliance Agent Service. This action deletes the SQLcompliance Agent Service. Be sure to perform this task on each node of the cluster hosting the virtual SQL Server instance.
3. Use Add/Remove Programs to uninstall the Cluster Configuration Console and the SQLcompliance Agent. You must perform this task on each node of the cluster hosting the virtual SQL Server instance.
4. Use the Management Console to remove the registered SQL Server instance.