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.

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

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal