# Previous features and fixed issues

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

## General

### Capture Logout Events

Currently SQL Compliance Manager captures Logins and Failed Logins, with SQL CM version 5.6 users have the ability to capture Logouts as a separate tracking option for their registered servers and for their configured Server Level Privileged Users.

### Default Audit Configuration Settings

SQL Compliance Manager provides users with the capability to set up a single Server default setting and a single Database default setting. Allowing users to set up newly added Servers and Databases with their exact desired settings. Users also have the ability to apply those default settings to already registered Servers and Databases. By default, SQL CM provides users with the Idera Default Settings, which are a set of basic settings to help users start auditing from the moment a Server is registered. For more information about this feature, see Default Audit Settings

### Add Databases Automatically

SQL Compliance Manager version 5.6 provides users with the ability to enable their Server Instances to automatically add any new database that is created on an audited server. For more information about this feature, see Registered SQL Server Properties - Advanced tab.

### Configurations Clarifications

Compliance Manager version 5.6 improved the configurations setting to help users have a clear understanding of what is being audited at Server level and what is being audited at Database level. With the implementation of a new logic that shows items checked and unavailable for deselection at the Database level since those items are already selected at the Server level.

> Please note that it is possible that with the setting inheritance you may collect more data, to avoid doing so, please review your settings to ensure that all items all collected as you expect.

### Server Level Trusted Users

SQL Compliance Manager version 5.6 allows users to configure Trusted Users at Server level. Trusted Users designated at Server level will apply across all databases in the selected server, giving users a greater control over who is monitored at what level. For more information, see Trusted Users at Server level.

### Sensitive Columns Auditing

SQL Compliance Manager version 5.6 updated the Sensitive Column functionality in order to alert users if PII data is selected or altered. To know if such data has been accessed, users can choose to collect information for Select Only, Selects and DML or for All Activity.

### Web Console Updates

SQL Compliance Manager version 5.6 removed all the configuration settings from the Web Console, to help users have a greater control over who can change audit data while still allowing granted users to view the information being audited. Centralizing the setting configurations to the Desktop Console only, makes the Web Console a place where Auditors and Executives can easily use Reports and Alerts to see the information that they need to see.

### Log File

SQL Compliance Manager version 5.6 includes a new Log file that keeps track of the product s versions and upgrades. The new Log file, found in the SQL CM installation folder, help users track the timelines for upgrade versions.

### Non-sysadmin

SQL Compliance Manager version 5.6 provides users with the ability to register a non-sysadmin role with permission to run the Compliance Manager Agent and permission to access the trace files.

### Increase the number of threads processed

SQL Compliance Manager version 5.6 added the option to adjust the number of threads that can be used to process trace files at a time.

## Regulatory Guidelines

### GDPR Regulation

SQL Compliance Manager version 5.6 added the General Data Protection Regulation (GDPR) guideline to the selectable list of regulatory guidelines, providing users with the option to select GDPR guideline and comply with their auditing needs. For more information about this feature, see Comply with Specific Regulations.

## Reports

### Configuration Check Report

SQL Compliance Manager version 5.6 implemented the Configuration Check Report, which allows users to compare the settings configured on the registered servers and databases with the previously defined default settings. This report allows users to quickly identify where settings may vary from what is defined as the default settings as well as to identify the differences in the configurations across your registered servers and databases. For more information about this feature, see Available Reports.

### Regulation Compliance Check Report

SQL Compliance Manager version 5.6 implemented the Regulation Compliance Check Report, which allows users to review the configurations set for all registered servers and databases and determine if settings comply with the selected Regulatory Guideline. This report compares the server and database configured settings to the predefined settings for any IDERA supported Regulation Guideline. For more information about this feature, see Available Reports.

## Installation and Configuration issues

- SQL Compliance Manager version 5.6 resolved the issue where the Compliance Manager Windows Console rebooted after installing or upgrading the SQL Server 2012 Native client version.
- Resolved an issue where SQL Compliance Manager recorded Create/Drop index events as “Alter User Table” events.
- SQL Compliance Manager version 5.6 implemented updates in the Sensitive Column functionality which resolved the issue where Sensitive Column events were not displayed if accessed from a view.
- Resolved an issue where SQL Compliance Manager was not capturing BAD auditing information when two objects with the same name exist in the same schema.
- SQL Compliance Manager version 5.6 resolved the issue where SQL Statements for DDL activities was not getting captured.
- SQL Compliance Manager version 5.6 resolved the issue which did not allow users to remove a database from the Administration pane.
- Resolved an issue where users were able to register active audited databases to archived SQL Servers.
- Resolved an issue where the **Capture SQL statements for DDL activities and Security Changes** option could not be selected unless the **Database Definition (DDL)** option was saved first.
- Resolved the issue where no events got captured for traces performed by non-privileged users.
- Resolved the issue where using encrypted credentials to deploy SQL Compliance Manager performing a silent installation returned an authentication error message.
- Resolved the issue where SQL Compliance Manager was not able to process alerts when a Group of users is set as a Privileged User.

There are no new features in this release

## Administration issues

- IDERA SQL Compliance Manager 5.5.1 process version 4.5 traces files. After upgrading the Collection Server to version 5.5.1, the agent must be upgraded to the same version. Once both the Agent and the Collection Server upgrades are complete, SQL Compliance Manager will process trace files. For more information, see Upgrade to this build.

- Resolved an issue in which the SQL Compliance Manager Collection Server was not processing trace files, or was processing them slowly, causing backlog files to get accumulated in the Collection Trace Directory in large transactional databases.
- IDERA SQL Compliance Manager 5.5.1 installation no longer fails if TLS 1.0 is disabled and if SQL Server 2012 Native Client is not available.

- IDERA SQL Compliance Manager 5.5.1 no longer shows the "Violation of PRIMARY KEY constraint" error nor terminates the statement when performing an archive of a highly transactional database.
- Integrity check runs for archived databases performed through stored procedures.
- IDERA SQL Compliance Manager 5.5.1 installation no longer fails due to an error setting up permissions if the username used special characters (e.g. ",", space characters, etc.).

- IDERA SQL Compliance Manager 5.5.1 supports user names longer than 20 characters as well as special characters for the user's password, such as £.

## Includes updated and new regulation guidelines

IDERA SQL Compliance Manager 5.5 includes updates on PCI DSS and HIPAA regulation guidelines templates. It also includes new sets of regulation guidelines, allowing users to perform data audits according the corresponding security rules.

The new regulation guidelines are the following:

- Defense Information Security Agency (DISA STIG)
- North American Electric Reliability Corporation (NERC)
- Center for Internet Security (CIS)
- Sarbanes-Oxley Act (SOX)
- Family Educational Rights and Privacy Act (FERPA)

For more information about this feature, see Comply with specific Regulations.

## Auditing available via SQL Server Audit Logs

IDERA SQL Compliance Manager 5.5 includes the ability to track your alerts via SQL Server Audit Logs for Agents running on SQL Server 2017 or above. Users can now decide if they want to track events via Trace Files, Extended Events (SQL Server 2015 and above) or Audit Logs (SQL Server 2017 or above). This new feature is supported in both the Web console and the Windows Management Console.

For more information about this feature, see Using SQL Server Audit Logs.

## Includes a Row Count feature

IDERA SQL Compliance Manager 5.5 includes the row count feature which captures and reports on the frequency that users access Event types and SQL Statements, alerting database administrators about suspicious behavior.

> As part of the row count functionality in SQL Compliance Manager 5.5 and above, we are now capturing Statement Completed instead of Statement Start. In some cases, if a SQL statement is run but not executed (e.g. SET SHOWPLAN_XML), SQL Compliance Manager may pick up those events.

For more information about this feature, see Control data access - Row count.

## Enable SQL Extended Events Auditing from the Windows Management Console

SQL Extended Events auditing can now be enabled from both the Web Console and the Windows Management Console.

For more information about this feature, see Using SQL Server Extended Events.

## Supports SQL Server 2017

IDERA SQL Compliance Manager 5.5 now supports installation of the Database Repository for Collection Server, deployment of the SQL Compliance Manager Agent, and auditing events for SQL Server 2017.

For more information, see Software requirements.

## Supports Windows Server 2016

The user can install IDERA SQL Compliance Manager 5.5 and deploy the SQL Compliance Manager Agent in Windows Server 2016.

For more information, see Software requirements.

## Allows users to create Sensitive Column data sets

IDERA SQL Compliance Manager 5.5 allows users to create Sensitive Column data sets that can be monitored as a group of sensitive information. Users can also add Sensitive Column data sets to any regulation guideline applied in servers or databases.

For more information, see Sensitive Column window.

## BAD Alerts

IDERA SQL Compliance Manager 5.5 allows users to add Host Name, Login, and Before-After data values to the alert message templates.

## Agent Deployment method

IDERA SQL Compliance Manager 5.5 allows users to see the agent deployment method in the Registered SQL Servers window of the Administration view.

## Allows users to install or upgrade on a non default drive

IDERA SQL Compliance Manager 5.5 allows users to install and/or upgrade in a non default drive path.

## Administration issues

- Audit thresholds appear enabled in the ReportCard even after removing and/or archiving an instance.
- SQL Compliance Manager 5.5 no longer fails to reach the Collection service on the active node after a successful failover in a clustered environment.
- Resolved the issue preventing SQL Scripts files with Supplementary Characters to work on the Collation SQL Server.
- Resolved the issue causing unexpected behavior during the manual upgrade of the SQL Compliance Manager Agent on a remote machine.
- Resolved an issue causing overwritten permissions on the Agent Trace folder after deploying the SQL Compliance Manager Agent.

## Auditing issues

- SQL Compliance Manager Agent no longer recreates stored procedures every second.
- Resolved an issue in which SQL Compliance Manager was not showing Before-After data when enabling capture DML events using Extended Events.
- Resolved an issue causing DDL Events to display twice for the same event.
- Resolved an issue in which SQL Compliance Manager was not saving changes made in privileged users when applying regulation guidelines.
- Resolved the issue preventing the user to capture SQL Statements for DDL and Security changes.
- Resolved the issue preventing the capture of Before-After Data when using Extended Events auditing to capture DML events.

## Reporting issues

- Email notifications for Event Alerts now display the date and time in the Collection Server time zone.
- SQL Compliance Manager alerts users about the limit of SQL Statements when exporting reports.
- Resolved an issue preventing users to view and report on audit data or see events.

IDERA SQL Compliance Manager 5.4 and later depend on certain Microsoft components that did not ship with SQL Server versions prior to SQL Server 2012 SP1. ***If you are installing SQL Compliance Manager's Collection Service on a Repository running on SQL Server 2012 or below,*** you must install these components manually. For more information about this process, see Important installation steps for SQLCM 5.4.x and above.

## Supports TLS 1.2 with SQL CM 5.4.2

IDERA SQL Compliance Manager 5.4.2 includes support for Transport Layer Security (TLS) version 1.2. The TLS protocol provides encryption, authentication, and data privacy and integrity when transferring information over a network, including VPN, VOIP, and instant messaging.

## Administration issues

- Resolved an issue causing both Primary and Secondary nodes to list the AlwaysOn database as Secondary.
- Resolved an issue preventing email from working for certain servers and types of events.

## Auditing issues

- Resolved an issue preventing audit of the Availabiity Group listener if a non-default port is used.
- Database-level Privileged User Auditing settings are no longer overwritten by instance-level Privileged User Auditing settings.
- Resolved the following integrity check issues:
  - users received an integrity check issue message although the scheduled integrity checks all passed
  - SQL Server startup events caused an integrity check failure
  - Integrity checks didn't match the Audit events in the SQLCM Repository
- Resolved an issue causing the database name to return blank for Login Events in some places.
- SELECT statements no longer appear as UPDATE statements.
- Resolved an error that occurred when the eventId reached the max limit of Integer. The error was, "Cannot insert duplicate key row in object 'dbo.Events' with unique index 'IX_Events_eventId'.
- No longer generates the Column Value Changed Data alert twice for Before-After auditing events.
- Resolved an issue causing an error when updating a table that contains an image and the table name contains a hyphen.
- The default Events view now displays data for a single day rather than 30 days.
- Resolved an issue preventing the proper function of the Exporting/Importing Database DML Filter audit settings.

## Archiving issues

- During archiving, users no longer receive a "Violation of PRIMARY KEY" error during archiving.

## Reporting issues

- Resolved an issue that prevented users from running the DML Activity (Before-After) report.

IDERA SQL Compliance Manager 5.4 depends on certain Microsoft components that did not ship with SQL Server versions prior to SQL Server 2012 SP1. ***If you are installing SQL Compliance Manager's Collection Service on a Repository running on SQL Server 2012 or below,*** you must install these components manually. For more information about this process, see Important installation steps for SQLCM 5.4.x and above.

## Improves archiving through the availability of SQL Server Extended Events

IDERA SQL Compliance Manager 5.4 includes support for event handling with SQL Server Extended Events. This optional feature is available for use in auditing instead of using SQL Trace. Running Extended Events offers a performance improvement over the default SQL Trace audit event gathering system and is available for instances running SQL Server 2012 and later. For more information about using the Extended Events option, see Using SQL Server Extended Events.

## Includes new Sensitive Column Search

Included in this release is integration with a free tool from IDERA called SQL Column Search. Available from the IDERA SQL Compliance Manager Instance Details view, this feature allows you to search tables and columns on a targeted database to discover the location of sensitive data needing to be audited. For more information about using the Sensitive Column Search, see Sensitive Column Search window.

## Offers SQL Compliance Manager Windows Console functionality in the Web Console

The following features previously available only through the IDERA SQL Compliance Manager Windows Console now are available in the Web Console as well:

- Importing sensitive columns
- Importing audit settings including instance and database templates
- Exporting audit settings including instance and database templates

## Includes updated regulatory guideline templates

IDERA SQL Compliance Manager includes a number of regulatory guideline templates for customer use. IDERA SQL Compliance Manager 5.4 includes updates for these templates. For more information about this feature, see Comply with specific regulations.

## Installation and upgrade issues

- Enabled **Capture Transaction Status for DML Activity** no longer replaces SQL statement values with variables.
- This release resolves an issue that prevented auditing when two tables has the same name but different schema
- An error no longer occurs while updating the audit configuration file due to duplicate database IDs.
- Improves Collection Server performance while processing trace files.
- Corrects an issue preventing the Collection Trace directory from being created when the user chooses a non-default installation path.
- IDERA SQL Compliance Manager 5.3 now supports SQL Compliance Manager Agent silent installation.
- Resolves an issue causing heartbeat alerts for instances after they are archived.
- Resolves an error that appeared when a user added privileged users while applying a custom Audit Collection Level.
- Fixed an error causing the collection of non-audited database data when **Capture SQL statements for DML and SELECT activity** is enabled.
- Before-After data now works during an update when auditing selected columns.
- Non-AlwaysOn Availability Group databases can no longer be added to an AG server for auditing.
- Resolves an issue causing an invalid object name error with 'sys.dm_os_window_info' for SQL Server 2005 agents.

**Supports SQL Server 2016**

IDERA SQL Compliance Manager 5.3.1 and later support audited and collection servers using Microsoft SQL Server 2016. For more information about supported platforms, see Software requirements.

There are no fixed issues in this release.

## Expanded the SQL Compliance Manager Web console to provide a richer set of capabilities online

IDERA SQL Compliance Manager 5.3 continues to build on the work developed by prior versions to bring a richer set of capabilities to the web console. New web capabilities include:

- an ability to set up notifications for auditing thresholds; allowing a user to set up a threshold and select the delivery method such as email, Windows event log, or SNMP traps.
- additional views such as the Enhanced Audited Database, Enhanced Alert, and New Logs views.
- the ability to export views to PDF, CSV, and XML formats.
- additional new widgets that show different activities and audited SQL Server instances.

## Integration with IDERA Dashboard 2.2

IDERA Dashboard integration began with SQL Compliance Manager 5.0, which centralizes the common administration, tasks, and views across all IDERA SQL products. This release of SQL Compliance Manager expands this integration by supporting IDERA Dashboard 2.2, which includes the following widgets specific to SQL Compliance Manager:

- **SQL Compliance Manager Audited Instances Widget**. Displays a list of audited SQL Server instances.
- **SQL Compliance Manager Enterprise Activity Report Card**. Displays your SQL Compliance Manager enterprise activity in a line graph.

For more information about using SQL Compliance Manager widgets within the IDERA Dashboard, see Overview tab.

## Limited Support for SQL Server 2016

IDERA supports installation of SQL Compliance Manager 5.3 on Microsoft SQL Server 2016 with limited technical support. Full technical support is available a short period after SQL Server 2016 is generally available.

## General

- Resolved an issue that did not properly update group permissions after modification and honored group settings over the individual user account in some situations.
- Improved Permissions Check functionality to prevent false or inconsistent results.

## Installation

- Renamed the SQL Compliance Processing database from `SQLCompliance.Processing` to `SQLComplianceProcessing`.
- Corrected an issue preventing the **...** button from properly working in the Add SQL Compliance Manager Agent Service window on Windows 2012/2012 R2 installations.

## Licensing

- Resolved an issue causing users with AlwaysOn Availability Groups to receive a message that the maximum number of servers is reached while they actually had less than that limit.

## Services

- Improved the Collection Service performance to be able to process a substantially large number of trace files.

## Auditing

- SQL Compliance Manager now can log events that are accessed through a view.
- Sensitive column traces no longer include events from databases not configured for sensitive column auditing.
- Resolved an issue that prevented SQL Compliance Manager from discovering and auditing new users added to the list of Trusted Users / Privileged Users within a domain group without manually updating the audit settings.
- Exported audit settings now include database level privileged users.

## Fully supports the SQL Server AlwaysOn Availability Groups feature

SQL Compliance Manager 5.0 now allows DBAs to monitor their availability groups, availability replicas, and availability databases through AlwaysOn Availability in SQL Server 2012 and newer. AlwaysOn automatically switches auditing from the primary to the secondary replica in the event of failure as well as failback to primary when it comes back online. This advantage prevents a loss of audit data trail in the event of failure.

Support for this feature also comes with:

- An Availability Group Statistics report that allows you view the historical health of your availability groups, availability replicas, and availability databases.
- An Availability Group Topology report that allows you to view the current topology of your availability groups configuration.
- Monitoring of key metrics specific to the AlwaysOn Availability Groups feature.
- Queue Size and Transfer Rates charts.

For additional information on SQL Compliance Manager and the AlwaysOn Availability Groups feature, see Enable automatic failover using AlwaysOn Availability Groups.

## Offers a technology preview of a new web-based SQL Compliance Manager Dashboard

Along with the integration of the IDERA Dashboard, SQL Compliance Manager 5.0 includes a preview of a newly-designed web console that offers quick views of key audit trail activities on your SQL Servers from any web browser. Identify key compliance issues quickly and provide an easy access point to non-DBAs without giving them access to the entire Management Console.

## Added integration with the IDERA Dashboard

SQL Compliance Manager 5.0 now integrates with the IDERA Dashboard, a common technology framework designed to support the IDERA product suite. Users are able to obtain an overview of the status of their SQL Servers and hosted databases all in a consolidated view and navigate to individual product dashboards for details. The IDERA Dashboard provides a central set of services for managing users, product registry, instance registry, aggregated alerts across IDERA applications, a central web server, and tags for grouping instances. For more information about the IDERA Dashboard, see Navigate the IDERA Dashboard web console.

## Moved to the Windows .NET 4.0 framework

SQL Compliance Manager 5.0 supports Microsoft Windows operating systems using .NET 4.0. Note that .NET 4.0 or later must be installed on the audited server. For more information about requirements, see Software requirements.

- Active Trace is now properly cleared when necessary.
- A change to the SQL Compliance Manager login filter settings from minutes to seconds fixes an issue that allowed new user events such as failed login attempts to be missed in reports.
- You can now view Reports in .CSV format.
- SQL Compliance Manager 5.0 includes an update that clarifies alert email triggers when users to have two alert rules for Sensitive Columns.
- SQL Compliance Manager no longer displays conflicting data by including a fix that forces the collection of object names while processing trace file records.
- Regular user accounts are no longer able to capture SQL text used in admin activities without enabling additional options.

- When you have multiple columns selected for a particular table in Before-After Data (BAD), SQL Compliance Manager no longer labels events that update other columns as BAD events.
- SQL Compliance Manager now includes descriptions for ALTER ANY SCHEMA and ALTER ANY USER in the tracejob.cs file.
- The permissions check process is updated in SQL Compliance Manager 5.0 to avoid any issues when performing a check.
- Event types 158 and 258 now include expanded details that display when these types of events occur.
- SQL Compliance Manager Integrity Check now properly tracks and reports on deleted rows.