SQL Compliance Manager 6.0

Table of Contents

Go to Version 5.9.x | Go to Version 5.7.x | Go to Version 5.6.x | Go to Version 5.5.x | Go to Version 5.4.x

Go to Version 5.3.x

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

- **Track and manage** SQL Server database compliance quickly and easily.
- **Audit servers, databases, and sensitive data** to see who did what. when, where, and how.
- **Monitor and alert** on suspicious activity to detect and track potential problems.
- **Satisfy audits** with configurations and reports for multiple regulatory guidelines requirements.
- **Reduce impact** on audited servers via a lightweight data collection mechanism.
- **Web-based dashboard** simplifies visibility and reporting for auditors and reviewers.

2 SQL Compliance Manager Release Notes

Designed in partnership with major auditing firms and leading security experts, IDERA 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 Compliance Manager 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

2.1 New features and fixed issues

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

> IDERA, Inc. customers are solely responsible for ensuring compliance with the laws and standards affecting their business. IDERA, Inc. does not represent that its products or services ensure 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.

2.1.1 6.0 New Features

Cloud Support Enhancements

New SQL CM Cloud Agent

SQL Compliance Manager 6.0 extends the capabilities of the current SQL CM Agent to support remote auditing on SQL servers on EC2. Allowing users to add SQL Servers active on the share network location to write/read data and support DBaaS SQL Server Instances. The Cloud Agent consists of the same behavior and functionality as the current SQL Agent, but the RDS agent is a separate agent deployed into the cloud with its own configuration auditing settings.

Add support for Amazon RDS

SQL Compliance Manager 6.0 adds support for Amazon RDS to audit servers, databases, Sensitive Data, and Activities while alerting and reporting on them. Users can select Amazon RDS as their Server Type when adding a new server in the Specify SQL Server configuration window. According to the selection, SQL CM asks to Specify Connection Credentials for the authentication, and once registered, users can begin auditing the database activity on that server.

Storage account for SQL CM on Cloud

SQL Compliance Manager 6.0 permits the creation of storage accounts to place its components within AWS. In Amazon RDS, users can audit Microsoft SQL Server databases using the built-in SQL Server auditing mechanism. For additional information on Support for SQL Server Audit, visit the SQL Server Audit User Guide.

Performance Enhancements

Improvements to the Event Collection method

Upon upgrading to SQL CM 6.0 or preparing a new installation, SQL Compliance Manager Event Collection Method Capture Default Setting changes to "SQL Server Audit Specifications". All audit logs for 'DML and Select Activities' are captured and filtered properly both for the existing CM architecture and the cloud support platform.

2.1.2 6.0 Fixed Issues

- Resolved the issue where users were mistakenly prompted for an agent upgrade. Now, if the Agent is on the latest version, the Upgrade Agent displays as a non-clickable out.

For more information about new features and fixed issues in version 5.9.x, see Previous new features and fixed issues.

2.2 Previous features and fixed issues

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

5.9 New features

There are no new features in this release.

5.9 Fixed issues

- Exporting Audit Settings now successfully includes an export of the Server Level Trusted Users configured.
- Resolved the issue where the SQL Server Properties window displayed the version as **Unknown** for registered SQL Server 2019 instances. Now, the correct version is shown.
- Resolved the issue where auditing stopped working when a user-configured Sensitive Column auditing without first selecting the DML or SELECT option caused the SQLcompliance Agent to have problems creating the **sp_SQLcompliance_AuditXE** stored procedure.
- Resolved the issue where Events were not captured for sensitive columns when SELECT and DML are not enabled at database-level audited activities on fresh and upgraded setups.
- The DML Activity (Before-After) report shows accurate results regardless of the collection method being set to Extended Events or SQL Tracing.
- The DML\SELECT filters are now working correctly when auditing SQL Server 2019 and no longer prevent DML and SELECT activities from being audited accordingly.
- The following error is no longer observed when attempting to run DML changes on a table configured for Before-After auditing in the software. **"The DELETE permission was denied on the object 'SQLcompliance_Changed_Data_Table'."**
- The retention period of the Activity Log is now configurable. It is set to a default of 60 days which can be modified in the SQLcomplianceCollectionService.exe.config file in the MAX_ACTIVITY_LOGS_AGE flag.
- Console loading times are faster now at both console startup and when navigating to the Audit Events view of the audited server or database.
- Event details on INSERT and DELETE events, audited not as INSERT INTO or DELETE FROM executions, are no longer missing the Target Object Name information, showing the name of the database object affected by the audited DML change.
- Reports deployed to SQL Server Reporting Services now show corresponding logins in the Login dropdown filter when these are set to run against an archived database.
- Reports no longer show a syntax error when executed either from the console application or SQL Server Reporting Services.
- The permissions check for the SQL Server service account permissions on the Agent Trace Files folder no longer fails when the SQL Server is running under the NETWORK SERVICE service account.
- Data types have been updated in the tables saving Before-After data to prevent the tables from filling up with event data too soon. This would have prevented new events from processing otherwise, as a result.
- The console application logging is no longer showing a collation conflict error, as shown below: **"Cannot resolve the collation conflict between "SQL_Latin1_General_CP1_CI_AS" and "Latin1_General_CI_AS" in the equal to operation."**

5.8.1 New features

There are no new features in this release.

5.8.1 Fixed issues

- Resolved the issue where the audit configuration was not updated when new users were added to a Windows Domain group which were previously configured as Trusted Users.
- Resolved the issue where public roles were granted unnecessary permissions, such as ALTER, EXECUTE, CONTROL, TAKE OWNERSHIP, and VIEW DEFINITION, on the audit stored procedures **sp_SQLcompliance_Audit** and **sp_SQLCompliance_StartUp**.
- Resolved the issue where the Collection Server installer raised an error message requesting the removal of the newly restored **SQLcompliance** and **SQLcomplianceProcessing** databases. Currently, the migration of

the Collection Server preserves the repository databases and displays the events on the console as expected.
- Resolved the issue where users were unable to register instances that are unreachable or from an untrusted domain. Currently, users can register unreachable instances or instances from untrusted domains. Please note that while unreachable instances can be registered for auditing, it is required for the Agent service to be deployed manually on these server instances.

5.8.0 New features

- The default settings for capturing DML and Select activities were changed to Extended Events on SQL Compliance Manager 5.8. This change provides a significant performance improvement for the collection service efficiency in event collection, as well as on the performance impact on monitored instances.
- SQL Compliance Manager 5.8 introduces a new highly optimized index format where the application upgrades indexes in the background from a none compression state to a page-level compression type. This operation is done as an Online operation for supported SQL Server editions. Currently, the SQL Compliance Manager repository does not utilize the optimized indexes format. Rebuilding the indexes into the new optimized format provides a significant performance enhancement to the Management Console when viewing audited events and provides a considerable database repository size reduction resulting in less space usage on disk. For more information see Indexes rebuild operation.
- SQL Compliance Manager 5.8 modified the Collection Server and Agent to allow a mode where trace files are transferred by the Agent to the Collection Server without compression. Transferring files from the Agent to the Collection Server without compression provides a significant performance enhancement both on the server side in event collection efficiency, and it reduces the performance impact on the monitored instances. In the Agent Properties window, users with Agents in version 5.8 have the option to decide whether to compress or not compress the file transfer from the Agent directory to the Collection directory. For more information, see Agent Properties - Trace Options tab.

5.8.0 Fixed issues

There are no new features in this release.

5.7.1 New features

There are no new features in this release.

5.7.1 Fixed issues

2.2.1 General issues

- Resolved the issue where the SQL Compliance Manager did not recognize a GMSA account as a Trusted user when adding the account as part of a group.
- Resolved the issue which caused the cluster setup installation to perform a fresh installation instead of asking users to upgrade the agent service.
- Resolved the issue where SQL Compliance Manager could not establish a connection with the AG databases on the Secondary nodes where no read access is allowed. SQL Compliance Manager successfully populates the list of AG databases to be configured for auditing on the Secondary nodes.
- Resolved the issue where configuring Sensitive Column auditing caused the SQLcompliance Agent to have problems creating the **sp_SQLcompliance_Audit** stored procedure.
- Resolved the issue with the Daily Audit Activity Statistics Report which displayed an error message due to a missing component. The Daily Audit Activity Statistics Report runs successfully.

5.7.0 New features

2.2.2 General

Supports SQL Server 2019

IDERA SQL Compliance Manager 5.7 now supports the installation of the Database Repository for the Collection Server, deployment of the SQL Compliance Manager Agent, and auditing events for SQL Server 2019. For more information, see Software requirements.

Supports Windows Server 2019

The user can install IDERA SQL Compliance Manager 5.7 and deploy the SQL Compliance Manager Agent in Windows Server 2019. For more information, see Software requirements.

Reports

New Reports

SQL Compliance Manager version 5.7 includes the Server Activity Report, which allows users to view the SQL Server activity at the enterprise and at the individual instance levels. With this report, users can quickly check activity in each event category audited and view statistics of the SQL Server activity. For more information, see Server Activity Report Card.

SQL Compliance Manager version 5.7 includes the Privileged/Trusted Users Report for users to list the trusted and privileged user roles set per a specific Server or Database. Users can run this report on Privileged and Trusted users to know what these were set to during a snapshot in time. For more information, see Privileged and Trusted Users Report.

SQL Compliance Manager version 5.7 includes the Sensitive Column/BAD Users Report which lists Sensitive Columns and Before-After data audit settings applied to the servers and databases in your environment. Users can run this report on Sensitive Columns and BAD auditing to know what these were set to during a snapshot in time. For more information, see Sensitive Columns and BAD Report.

Limit Report Access to specific users

SQL Compliance Manager version 5.7 introduces the ability to restrict user access to certain SQL CM reports. As an administrator, you can grant users permission to specific reports. This way, you can tightly control permissions settings for report access for every user in your environment. For more information, see Login properties - Report Access.

Report Filter improvements

SQL Compliance Manager version 5.7 brings updates and improvements to reports by making reports more consistent and adding new filter options, such as the ability to filter reports based on a specific schema, event type, login, or multiple logins at a time. Users can also use the time range filters to report on the exact high activity time-frames or to filter out low activity time-frames.

5.7.0 Fixed issues

General issues

- The Object Activity Report no longer renders all data on a single page, and when run, the report displays the collected data correctly.

5.6.1 New features

2.2.3 General

Sensitive Column Search

SQL Compliance Manager version 5.6.1 introduces the Sensitive Column Search functionality, allowing you to search all of the tables and columns on a targeted database to discover the sensitive data location that needs to be audited. For more information, see Sensitive Column Search window.

5.6.1 Fixed issues

Installation and Configuration issues

- Resolved the issue where the Stored Procedure did not get disabled for the secondary node, which caused an accumulation of trace files on the secondary node.
- Resolved the issue which caused DML/SELECT filter settings to import incorrectly.
- Resolved the issue where an error message appeared in the SQL Server Logs about an invalid call to stored procedure **master.dbo.sp_SQLcompliance_AuditXE**.

5.6.0 New features

2.2.4 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 the Server level and what is being audited at the Database level. Implementing 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 the Server level. Trusted Users designated at the 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.

2.2.5 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.

2.2.6 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.

5.6.0 Fixed issues

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.

5.5.1 New features

There are no new features in this release

5.5.1 Fixed issues

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 £.

5.5.0 New features

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 and 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 the 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.

5.5.0 Fixed issues

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.

5.4.2 New features

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.

5.4.2 Fixed issues

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.

5.4.0 New features

> 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.

5.4.0 Fixed issues

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.

5.3.1 New features

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.

5.3.1 Fixed issues

There are no fixed issues in this release.

5.3.0 New features

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.

5.3.0 Fixed issues

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.

5.0.0 New features

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.

5.0.0 Fixed issues

- 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.

2.3 Known issues

IDERA strives to ensure our products provide quality solutions for your SQL Server needs. The following known IDERA SQL Compliance Manager issues are described in this section. If you need further assistance with any issue, please contact Support.

2.3.1 Known issues in version 6.0

- Switching from Extended Events or SQL Server Traces to SQL Server Audit Specification does not stop the pre-running audit sessions and audit files. After changing the selection to SQL Server Audit Specification, fresh audit data is collected through the Audit log files.
- SQL Compliance Manager sometimes displays an error message when the Agent service hits the trace start timeout while trying to cycle one of the audit traces it's running. As soon as the audit trace has been successfully restarted, auditing continues as expected, and the audit events captured in the trace will be processed into the audit trail in Compliance Manager without issues.

  > **Note**
  >
  > This error does not affect auditing and can be safely ignored.

- For a particular Database configured to audit DML and SELECT activities via SQL Server Tracing, DML events when executed under a different Database context, produce T-SQL statements for the audited DML events showing variables over the actual values used in the transactions. DML events are captured as expected with actual parameters via SQL Server Tracing while using the same audited Database context.

2.3.2 Known issues in version 5.9

- During the registration of an AG Listener in the Cluster Configuration Console, when naming the SQL Server instance, the underscore "_" character is not supported. Because "_" isn't a supported character in FQDN names, the current behavior cannot be changed because it is an MS-documented limitation.

2.3.3 Known issues in version 5.8.1

General issues

- ***(Fixed in version 5.9)*** For registered SQL Server 2019 instances, the General tab of the SQL Server Properties window displays the version as Unknown. This is only a visual issue and does not affect auditing or any other functionality.
- ***(Fixed in version 5.9)*** The Audit settings Export feature does not export previously configured Server level Trusted Users. To complete the migration, add the Trusted Users manually at the Server Level.
- ***(Fixed in version 5.9)*** When you configure Sensitive Column auditing without first selecting the DML or SELECT option on the Audited Activities tab, then the SQLcompliance Agent has problems creating the **sp_SQLcompliance_AuditXE** stored procedure, and auditing stops working.

Sensitive Column issues

- ***(Fixed in version 5.9)***Events for Sensitive Column audit data are not captured when auditing via Extended Events. When the option to capture SELECT and DML activities is configured at the server-level to capture events via the Extended Events auditing method, and the capture SELECT and DML option is not configured at the database level but is configured to track SELECT and DML for Sensitive Column auditing. In order to capture and process Sensitive Column events correctly, change the collection method from Extended Events auditing to SQL Server Trace Files auditing.

2.3.4 Known issues in version 5.8

General issues

- The installation wizard of the Agent service fails when running the audited SQL Server under the Local System account. In order to grant all required permissions successfully, run the **SQLcompliance-x64.exe** installer to perform a manual agent-only installation.
- ***(Fixed in version 5.8.1)*** When performing a migration of the Collection Server while installing the new Collection Server components, the installer raises an error message that prompts for the removal of the newly restored **SQLcompliance** and **SQLcomplianceProcessing** databases. The installer locates these databases, which have been restored for the purpose of the migration, on the server instance, which has been designated as the new repository database server during the installation process. Do not proceed with the removal of these databases. Instead, contact Support for further assistance with installation or look up the KB Article #00012649 for further instructions in the Solutions section for the SQL Compliance Manager product in the IDERA Customer Portal.

2.3.5 Known issues in version 5.7.1

General issues

- ***(Fixed in version 5.8.1)*** SQL Compliance Manager presents a security concern due to unnecessary permissions such as ALTER, EXECUTE, CONTROL, TAKE OWNERSHIP, and VIEW DEFINITION, which are granted to Public roles on the audit stored procedures **sp_SQLcompliance_Audit** and **sp_SQLCompliance_StartUp**.
- When adding or editing users from the console, SQL Compliance Manager does not grant access to the Web Console Users and displays the error message "Failed to update Web Application access permission for user".
- ***(Fixed in version 5.8.1)*** SQL Compliance Manager encounters an issue when adding new users to a Windows Domain group that were previously configured as Trusted Users on a particular database. As a result, these changes are not reflected in the audit configuration stored in the .bin audit file nor on the **sp_SQLcompliance_Audit** stored procedure. Users have to manually update the audit settings in the console for the new users to display in the audit configuration.
- ***(Fixed in version 6.0)***An Event Filter configured to exclude all activities recorded on the tables of a database will not exclude DML and SELECT activities happening on columns that are not configured for Sensitive Column auditing but which are part of a table with columns configured for Sensitive Column auditing. Event Filters are expected to exclude all activities these are configured to exclude, except DML and SELECT activities happening on columns configured for Sensitive Column auditing. This is by design.

2.3.6 Known issues in version 5.7

General Issues

- ***(Fixed in version 5.7.1)*** When users add a GMSA account as part of a group, SQL CM does not recognize it as a Trusted User. As a workaround, users need to specify the account and the group when configuring Trusted Users and update the audit settings each time a new GMSA account is added to the group.
- ***(Fixed in version 5.7.1)*** When users run the SQLcomplianceClusterSetup.exe to upgrade agent service deployment to 5.6.1, the cluster setup installation does not prompt the user to agree to upgrade instead, it performs a fresh installation.
- ***(Fixed in version 5.7.1)*** When registering databases to the Primary node of an audited Availability Group, SQL Compliance Manager is not able to establish a connection with the AG databases on the Secondary nodes. Therefore, these databases do not get automatically registered on the Secondary nodes.

In order to register the databases on the Secondary nodes, users have to:

1. Fail over the Availability Group onto the Secondary node in order to get access to the list of databases.
2. Register the databases on the Secondary node
3. Fail over the AG back to the Primary node.

2.3.7 Known issues in version 5.6.1

General Issues

- ***(Fixed in version 5.7)*** The Daily Audit Activity Statistics Report displays an error message in the SQL CM desktop console when the **ReportViewer.DataVisualization** component is missing. To run the report correctly, close the SQL CM desktop console and install the Report Viewer 2010 program. Once the installation is complete, relaunch the SQL CM desktop console and run the report.

  To download the Report Viewer 2010 controls program, follow the link below:
  Report Viewer 2010 Controls

- In SQL Compliance Manager version 5.6.1, the Row count functionality may show as “Not Applicable”. The issue occurs when you execute a large query, and during execution, the start and the end of the SQL Statement get captured in different trace files. Since both events are located in different trace files, SQL CM is not able to map these events and therefore displays that the Row count is “Not Applicable”. Users can increase the time of collection (the default is set to 60 seconds) to capture the Row count correctly.
- ***(Fixed in version 6.0)***SQL Compliance Manager is currently allowing users to select the Upgrade Agent option, even if the Agent is already in the latest version. Upon selection, SQL CM prompts you to upgrade the agent using the full setup program.
- ***(Fixed in version 5.7.1)*** When you configure Sensitive Column auditing without first selecting the DML or SELECT option on the Audited Activities tab, then the SQLcompliance Agent has problems creating the **sp_SQLcompliance_Audit** stored procedure, and auditing stops working.

2.3.8 Known issues in version 5.6

General issues

- ***(Fixed in version 5.6.1)*** Import Database settings with DML/SELECT filters, flips import settings. When users import database audit settings and apply those settings to multiple databases, the imported settings apply only to some databases. If the user imports and applies the audit settings to the same databases again, the configuration settings get flipped, applying the import settings to the databases it did not apply to before while deleting the settings from the ones it previously applied them to.
- ***(Fixed in version 5.6.1)*** Invalid stored procedures call to sp_SQLcompliance_AuditXE. A message about an invalid stored procedure appears in the SQL Server Logs; "Could not find stored procedure **master.dbo.sp_SQLcompliance_AuditXE**". The error message appears because no stored procedure with the name "**master.dob.sp_SQLcompliance_AuditXE**" exists.
- ***(Fixed in version 5.7)*** SQL Compliance Manager Object Activity Report renders all data on a single page. When the Object Activity Report is run, the report displays all the collected data on a single page.
- ***(Fixed in version 5.6.1)*** SQL Compliance Manager traces are getting collected on the Passive nodes of an Availability Group. When a primary node becomes a secondary node, the Stored Procedure does not get disabled for the secondary node and the trace files keep gathering. This causes an accumulation of trace files on the secondary node.

Follow the steps below for the workaround to stop trace files from generating on the secondary node:

1. Launch Trace Manager from the SQL Compliance Manager Desktop Console. SQLCM Menu-bar>Tools>Trace Manager.
2. Enter the SQL Server Instance name and click the Connect button.

> ⚠ When working on a secondary node of an Availability Group, use the secondary´s instance name.

3. In the SQLcompliance Stored Procedures field, make sure to check the "_" and "_" options.
4. Click the "Drop SQLcompliance Stored Procedures" button.
5. In the Registered Traces field, from the list of running traces, select the entries related to the SQL CM traces.

> ⚠ Use the file path to determine the traces related to SQL CM. Or check the Agent Properties for the audited instances to verify the trace directory file path.

6. Once the desired registered trace is selected, click the Stop button. Select the record again and click the Close button.
7. Repeat steps 5 and 6 for the remaining SQL CM traces.

2.3.9 Known issues in version 5.5.1

Installation and configuration issues

- ***(Fixed in version 5.6)*** Installation or upgrade of SQL Server 2012 native client may cause the system to reboot. When installing or upgrading the version of the native client, once the process is complete, a system reboot occurs without previous warning.
- IDERA Dashboard 3.0.3 and later does not support SQL Server 2005 SP1. Users should not attempt to install SQL Compliance Manager with IDERA Dashboard 3.0.3 and later on a SQL Server 2005 SP1 as that version of SQL Server is not supported by IDERA Dashboard.

General 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.
- IDERA SQL Compliance Manager does not capture Linked Server Trace Events for SQL Server 2005. Linked server events are not present in the trace files for SQL Server 2005, therefore linked server events are not captured in IDERA SQL Compliance Manager and no alerts will trigger. Microsoft has ended extended support for this version.
- ***(Fixed in version 5.6)*** Create/Drop index events recorded as "Alter User Table" event. SQL Compliance Manager records Create/Drop index events as "Alter User Table" events.
- ***(Fixed in version 5.6)*** IDERA SQL Compliance Manager is not loading events accessed through a View. SQL Compliance Manager does not display Sensitive Column events when accessed from a view. To access the information using views gather and filter out all SELECT statements. Note that this action will cause extra collection.
- ***(Fixed in version 5.6)*** Issues loading BAD auditing information. IDERA SQL Compliance Manager is not able to capture BAD auditing information when two objects with the same name exist in the same schema.
- ***(Fixed in version 5.6)*** SQL Text is not captured for DDL Statements. When monitoring an instance for DDL event, SQL Compliance Manager is not able to capture SQL Statements for DDL activities unless a user is added to the Privileged User Group. Users can also capture SQL Text by selecting **Capture SQL statements for DDL and Security changes** at Database Level.

2.3.10 Known issues in version 5.5

General issues

- (***Fixed in version 5.5.1***) When users try to upgrade from SQL Compliance Manager 4.5 to 5.5, trace files are not processed. If you currently work with SQL Compliance Manager 4.5, before upgrading stop the Collection Service, Agent Service, and disable auditing to stop trace file processing, then proceed to upgrade to SQL Compliance Manager 5.5, and configure and enable auditing. Upon upgrading to SQL Compliance 5.5, users must upgrade all agents to a 5.x version first. For more information, see Upgrade to this build.
- (***Fixed in version 5.5.1***) The SQL Compliance Manager Collection Server is not processing trace files, or processing them slowly, causing backlog files to get accumulated in the Collection Trace Directory in large transactional databases.
  The workaround for this issue is to increase the tamper detection interval and the Collection interval.
- (***Fixed in version 5.5.1***) IDERA SQL Compliance Manager installation fails if TLS 1.0 is disabled and if SQL Server 2012 Native Client is not available. IDERA SQL Compliance Manager 5.5 installs SQL Server 2012 native client (version 11.0.2100.60) which does not support TLS 1.2 enabled as per Microsoft.
  https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server
  Users with SQL Server versions prior to SQL Server 2012 R2 SP3 need to enable TLS 1.0 or update the native client to the supported version (11.4.7001.0) following the link below:
  https://www.microsoft.com/en-us/download/details.aspx?id=50402
- (***Fixed in version 5.5.1***) SQL Compliance Manager does not process trace files generated by an older Agent after upgrading versions of the Collection Server and the Agent.

Auditing issues

- (***Fixed in version 5.5.1***) When performing an archive of a highly transactional database with SQL Compliance Manager, the application shows a “violation of PRIMARY KEY constraint” error and terminates the statement. The workaround for this issue is to rename the current archive database, along with the database files associated to it and perform a new archive operation. The operation should create a new archive database and database files.

2.3.11 Known issues in version 5.4.x

General issues

- (***Fixed in version 5.5.1***) SQL Compliance Manager does not accept user names longer than 20 characters and does not support some special characters for the user password, such as £.
- Removing databases using the Administration pane in the Management Console does not work. You can remove databases using the Explorer Activity panel.
- (***Fixed in version 5.5***) 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.

Auditing issues

- If the audit settings are configured to audit DML events for a selected table, and extended events is enabled for DML and Select on the Instance, SQL Compliance Manager collects audit data for all tables and not only the selected table. If you turn off extended events, auditing correctly collects data for the selected table only.

- (***Fixed in version 5.5***) Execute events are captured when extended events is enabled. There may be some extra events captured and shown through the Extended Events auditing than the events shown through the Trace method.
- (***Fixed in version 5.4.2***) Cannot insert duplicate key row in object 'dbo.Events' with unique index 'IX_Events_eventId'.
- (***Fixed in version 5.4.2***) DatabaseName appears as empty for Login Events. SQL Compliance Manager 5.4 traces do capture the DatabaseID, but do not include the database name.
- (***Fixed in version 5.5***) Applying a regulation guideline does not work when there is a Privileged User defined.
- (***Fixed in version 5.4.2***) Case-sensitive collation may prevent some trusted and privileged users from being captured.
- (***Fixed in version 5.4.2***) Auditing an AlwaysOn database using the Node method causes the Registered SQL Servers list to display both nodes as Secondary.
- Audit Snapshot does not include setting to capture DDL SQL statements.
- Before-After data does not appear for Binary Collation SQL Server instances when extended events is enabled.
- (***Fixed in version 5.4.2***) Audit settings at an instance level take precedence over database-level settings for a Privileged User.
- (***Fixed in version 5.5***) Agent trace folder permissions are overwritten when the Agent is deployed.
- (***Fixed in version 5.4***) SQL Compliance Manager attempts to contact the Agent (heartbeat check) on attached archive databases.
- (***Fixed in version 5.5***) Users who export reports to Microsoft Excel fail when the SQL text contains more than 32,767 characters.
- (***Fixed in version 5.4.2***) Some SQL Server startup/stop events may cause the integrity check to fail.
- The Audit Events tab may display an incorrect user name in the Login column when auditing start and stop server events.
- (***Fixed in version 5.4.2***) A known SQL Server issue causes some SQL Compliance Manager SELECT statements to appear as DML events. This issue occurs when a user audits both SELECT and DML. SQL Compliance Manager captures many events when certain columns are selected from certain system tables from a single SELECT statement query and shows them as individual DML events.
  Specifically, the SELECT statement which uses the `permissions()` function generates only DML event traces and not a SELECT event trace. This step results in SQL Compliance Manager reporting the SELECT statement as a DML event. In addition, the `permissions()` function is deprecated. Microsoft recommends in MSDN documentation that users implement the `Has_Perms_By_Name()` function instead of the `permissions()` function. The difference between these two functions is that the `permissions()` function always generates the DML event traces while the `Has_Perms_By_Name()` function generates event traces according to permission type used. For example, SELECT event traces for SELECT permission types, and DML event traces for EXECUTE or DELETE permission types.
- (***Fixed in version 5.4.2***) Users who change the default port for the AlwaysOn Availability Group from the default may experience the following issues. to avoid these issues, change the listener to the default port.
  - SQL Compliance Manager does not accept the name format when attempting to add the listener name using the Cluster Configuration Console.
  - If the port is not added, the agent cannot connect to the SQL Server instance. You can manually add the port to the registry setting later and it will then connect to the instance after restarting the SQLcomplianceAgent.
  - Users cannot connect to the SQL Server instance even when adding the listener with the port in the SQL CM console.
  - The Permissions Check also fails.
- When you change the definition of a table you are auditing to include BLOB data types, the Before-After data trigger prevents UPDATE, DELETE, and INSERT operations from modifying the table, such as through stored procedures or third-party applications. This issue is most likely to occur when you are auditing all columns

in the target table. This issue occurs because Before-After auditing does not support BLOB data types (such as text, image data, or XML code). To correct this issue, change the data definition of the table.
- SQL Compliance Manager 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.
- After removing a server from auditing and leave registered databases archived, the user is able to right-click the archived database 'server' and register databases to audit.
- Users can select "Capture SQL statements for DDL activities" only if the "Database Definition DDL" option is saved first.

Alerting issues

- Filtering by time does not work properly on the Alerts view.
- Some status alerts including Agent trace directory reached size limit and Collection Server trace directory reached size limit do not display properly in the Web Console.
- Status alerts are not generated for alert rules of the **Agent cannot connect to audited instance** Rule Type.
- (***Fixed in version 5.5***) SQL Statement is not captured or displayed when viewing Event Properties for Create SQL Login and Create Windows Login events.
- (***Fixed in version 5.4.2***) A Column Value Changed data alert is generated twice for each Before-After audit event.

Reporting issues

- (***Fixed in version 5.4.2***) The DML Activity (Before-After) report, when deployed to SQL Server Reporting Services, does not run properly. You can view the report in the Console.

3 Welcome to SQL Compliance Manager

IDERA 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

3.1 What is SQL Compliance Manager?

Designed in partnership with major auditing firms and leading security experts, IDERA 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 Compliance Manager 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.

3.2 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. IDERA SQL Compliance Manager is specifically designed to meet these requirements. SQL Compliance Manager 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.

3.2.1 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 Compliance Manager 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.

3.2.2 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.

3.2.3 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 Compliance Manager provides many pre-defined reports that you can immediately use to track audited events. SQL Compliance Manager 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.

3.2.4 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 Compliance Manager integrates with and conforms to your internal security policies, allowing granular access control at the database level.

SQL Compliance Manager 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.

3.2.5 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 Compliance Manager is specifically designed to support large SQL Server installations. SQL Compliance Manager 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.

3.2.6 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 Compliance Manager provides comprehensive reporting to satisfy audit requirements with regulatory and data security rules such as PCI DSS and HIPAA. SQL Compliance Manager 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 Compliance Manager audit data is stored in a tamper-proof repository.

3.3 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.

3.3.1 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

3.3.2 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 in the IDERA Customer Service Portal.

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 9.0
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

You can access the IDERA SQL Compliance Manager 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.

4 Getting started

Use the following checklist to get started using IDERA 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.

4.1 Upgrade to this build

You can quickly and easily upgrade to the current version of IDERA SQL Compliance Manager from version 4.5 and later. All versions prior to 4.5 must upgrade to version 4.5 before upgrading to the current version. Upgrading SQL Compliance Manager allows you to take advantage of the new features available in this latest version.

⚠ For IDERA SQL Compliance Manager 5.5, you must upgrade to version 4.5 and then to 5.0 before upgrading to this version.

ⓘ SQL Compliance Manager 5.0 and later requires you to upgrade the SQL Compliance Manager Agents to the same version, i.e. version 5.0 requires Agent version 5.0.

4.1.1 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 4.0 or later is running on the target computer.
✓	Ensure your Windows logon account has the following permissions: • Permission to agent and collection trace file directories • Permission to uninstall/install a windows service • Permission to start a service (Logon as a service)
✓	Close all open applications on the computers running the SQL Compliance Manager 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.
✓	Upgrade your license key.
✓	Upgrade your previously deployed SQL Compliance Agents.
✓	Ensure that 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 Compliance Manager Reports in order to generate reports using the upgraded Repository databases as the data source.
✓	Ensure that the computers on which you want to upgrade SQL Compliance Manager have VC redistributable 2010 installed. ***You can download*** the Microsoft Visual C++ 2010 Redistributable Package for 32 Bit OS (x86) here.
✓	Ensure that the computers on which you want to upgrade SQL Compliance Manager have the latest version of Microsoft Windows Installer Driver installed. ***You can find and download*** the latest Windows Installer here.
✓	Test your upgrade by collecting and reporting on your audit data.

4.1.2 Upgrade from SQL Compliance Manager 4.5 to version 5.0

IDERA SQL Compliance Manager has unique instructions for upgrading from version 4.5 to version 5.0. If you have any installation issues, please contact Support.

Preparing to upgrade

Request a new license key

IDERA SQL Compliance Manager version 5.0 and later use a new license key. You must update your existing product license key to complete the installation of IDERA SQL Compliance Manager 5.0 or later. To request a new license, contact licensing@idera.com. Provide the hostname of the server/SQL Server instance hosting IDERA SQL Compliance Manager. If using the default name MSSQLSERVER for SQL, simply provide the server hostname.

Key notes

- **Verify .NET 4x is installed on all your servers.*** All IDERA SQL Compliance Manager 5.0 and later versions require .NET 4.0 components. Previous versions of IDERA SQL Compliance Manager require at least .NET 3.5. * Beginning with version 5.0, IDERA SQL Compliance Manager does not support Windows Server 2000 or the .NET 2.0 framework. While IDERA SQL Compliance Manager 4.5 and prior versions continue to operate with Windows Server 2000, IDERA SQL Compliance Manager 5.0 and later require the .NET 4.0 Full framework to take advantage of the additional features. For additional information about supported versions, see the IDERA SQL Compliance Manager Software requirements.
- **You must upgrade the Agent.** IDERA SQL Compliance Manager 5.0 and later require that you upgrade the IDERA SQL Compliance Manager Agents to the same version, i.e. version 5.0 requires Agent version 5.0.
- **You do not have to enable the default trace or use ID 1.** IDERA SQL Compliance Manager 5.0 requires that the default trace is enabled and it is also ID 1. This requirement was removed for IDERA SQL Compliance Manager 5.3.x. Contact Support if you have any questions.

Upgrade

To upgrade IDERA SQL Compliance Manager:

1. Close the IDERA SQL Compliance Manager Management Console, if running.
2. Stop the SQL Compliance Collection Service.
3. Back up all of the SQLcompliance databases.
    a. `SQLcompliance` and `SQLcompliance.Processing` are the core databases.
    b. `SQLcompliance_[instance name]` contains the live audit data.
    c. `SQLcmArchive_[instance name]_[date]` contains the archive data.
4. Check the `CollectionServerTraceFiles` folder on the collection server for trace files.
    a. ***If there are any files***, make a copy in another location.
    b. ***If there are lots of files older than 1 day***, please contact support for help with these older trace files.
5. Run the `setup.exe` for IDERA SQL Compliance Manager using **Run as Administrator.**
    a. The `setup.exe` is a two-part installer.
        i. The IDERA Dashboard is installed first.
        ii. The SQL Compliance Manager upgrade will be started after the Dashboard installation has completed.
    b. To bypass installing the IDERA Dashboard, run the `SQLcompliance-x64.exe` found in the Installation kit x64 folder. (default location: C:\Program Files\IDERA\SQLcompliance x64 Installation Kit\Full\x64.

6. Run the IDERA SQL Compliance Manager Management Console. Verify the console loads and the servers and data are displayed.
7. Manually update the SQL Compliance Agent on the audited servers.
    a. No agents have been updated yet, so all the servers will report as DOWN (except for the SQL Compliance Agent that is running on the IDERA SQL Compliance Manager Collection server).
    b. Run the `SQLcompliance-x64.exe` using **Run as Administrator** (not setup.exe).
    c. Follow the prompts then select **Agent Only** install.

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

4.1.3 Upgrade the product components

These instructions are only valid for upgrades from 4.5 to the current version. All versions prior to 4.5 must first upgrade to version 4.5, and then to the current version.
If you are upgrading to SQL Compliance Manager version 5.5, you must first upgrade to version 4.5 and then to 5.0 before upgrading to 5.5.
For upgrade instructions for version 4.5, see Upgrade from SQL Compliance Manager 4.5 to 5.0.

You can use the setup program to upgrade all components or any individual component. The setup program detects whether IDERA 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 SQL Compliance 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 from SQL Compliance Manager 4.5 and later to current version:

1. Log on with an administrator account to the computer on which you want to upgrade IDERA SQL Compliance Manager components.
2. Run `SQLCMInstall.EXE` in the root of the installation kit.
3. The IDERA SQL Compliance Manager welcome window shows you the components you can upgrade to the current version or the ones that require a fresh installation. Click **Next** to begin the upgrade process.
4. On the Repositories window, select the authentication type and enter the SQL credentials, if necessary, and click **Next**.
5. Type the appropriate credentials in the provided fields under which the IDERA Dashboard services run, and then click **Next**.
6. Review the installation settings and click **Install**.
7. Start the Management Console. When prompted, schedule a time for SQL Compliance Manager to perform maintenance on your Repository databases.
8. Upgrade your SQL Compliance Agents

If you currently use the latest version of IDERA SQL Compliance Manager, it is not possible to upgrade the IDERA Dashboard only. To upgrade the IDERA Dashboard only, you need to use the CWF installer.
For more information, see IDERA Dashboard.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

4.1.4 Upgrade your deployed SQL Compliance Agents

Before upgrading your SQL Compliance Agents, review the permissions requirements and how the SQL Compliance Manager Agent works.

Consider the scenarios described below for SQL Compliance Manager Agent installation and upgrade.

If the SQL Compliance Manager Agent is:

- installed and deployed via SQL Compliance Manager console, it has to be upgraded using the application console. Alternatively, it can be upgraded via command line.
- installed and deployed with the main installer, it has to be upgraded using the main installer.
- installed and deployed manually using the install command line, it has to be upgraded using the upgrade command line.

⚠ To upgrade the agent manually with the command line, it is required to use **only** the SQL Compliance Manager Agent **MSI**.

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.

ⓘ If you deployed an agent on a remote server via the SQL Compliance Manager console and want to upgrade it to this build, you can also use the upgrade command of the SQL Compliance Manager silent installer.

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 with a command line

To upgrade the IDERA SQL Compliance Manager Agent for versions 5.5 and later, use the following command:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
```

```
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

To upgrade the IDERA SQL Compliance Manager Agent from 4.5 to this version and later, use the following command:

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" AllUsers=1 /qb+
```

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 `SQLCMInstall.EXE` in the root of the installation kit.
4. After completing the upgrade on a clustered environment, go to the SQL Compliance Manager install path. Unless you have specified a different path, the one by default is `C:\Program Files\IDERA\SQLCompliance.`
5. Run `SQLcomplianceClusterSetup.EXE.`
6. The installer displays a confirmation message. Click **Yes** if you want to upgrade the IDERA Cluster Configuration Console.
7. Once the setup wizard launches, click the **Next** to complete the upgrade.
8. After the upgrade completes, the **Cluster Configuration Console** automatically starts.
9. When prompted, specify the directory location you want SQL compliance manager to use to store CLR trigger assemblies.
10. In Windows Services, stop the SQL Compliance Manager Agent service and set the Startup type to **Manual**.
11. Open Microsoft Failover Manager, right-click the SQL Compliance Manager Agent service, and select **Properties**.
12. Go to the **Registry Replication** tab, set the Root Registry Key to `Software\Idera\SQLCM`, save the changes and close the **Properties** window.
13. Right-click the SQL Compliance Manager Agent service and bring the generic service online.

4.1.5 Upgrade to the latest SQL Compliance Manager version in a clustered environment

To upgrade SQL Compliance Manager 4.0 or later in a clustered environment using Windows Server 2003 or later, follow the steps below.

Be sure to back up your Repository and all databases and archives before upgrading SQL Compliance Manager.

Upgrade the SQL Compliance Manager 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 Compliance Manager 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 upgrade 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 and later), 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 Compliance Manager.
3. Run `SQLCMInstall.exe` in the root of the SQL Compliance Manager installation kit on the first cluster node.
4. Review the information you need to start the upgrade and click **Next.**
5. Select the **SQL Compliance Manager** setup type and uncheck the **IDERA Dashboard** setup type. Review and accept the license agreement by selecting the ***I accept the terms and conditions of the End User License Agreement*** checkbox.
6. Specify if you want to register SQL Compliance Manager with an existing IDERA Dashboard.
   If you select Yes, you need to provide the IDERA Dashboard location and administrator credentials.
   If you want to use the IDERA Dashboard, see how to Deploy the IDERA Dashboard in clustered environments.
7. Specify the location in which you want to upgrade SQL Compliance Manager.
8. Enable the **Clustered Environment** checkbox and select whether you are upgrading SQL Compliance Manager in an active or a passive node.
   Verify that the repository is the same SQL Server Instance name hosting the current repository and **specify** a form of authentication.
   Test Connections to make sure the information is correct and click **Next.**
9. ***If you upgrade on the currently active node***, verify that the trace directory is the same location in which your current directory resides, and click **Next**.
   If you upgrade on a passive node, the wizard skips this step.
10. Type the appropriate credentials in the provided fields under which the IDERA services run, and then click **Next**.
    IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment, the installer grants the "Log on as a Service" right to the account that you specify.
11. Review the upgrade settings and click **Install**.
12. In Windows Services, **stop** the *SQL Compliance Manager Collection service* and **set** the Startup type to **Manual**.

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

After upgrading SQL Compliance Manager in all nodes, follow the steps below:

1. Log on to the active node and launch the Microsoft Cluster Administrator tool (Windows Server 2003) or the Microsoft Failover Cluster Management Console (Windows Server 2008 and later), right-click the *SQLComplianceCollectionService* resource, and select **Properties.**
2. Go to the **Registry Replication** tab and set the Root Registry Key to `Software\Idera\SQLCM.`
3. Close the **Properties** window, right-click the *SQLComplianceCollectionService* resource, and bring the service online.
4. Log on to the passive node, launch the Microsoft Cluster Administrator tool (Windows Server 2003) or the Microsoft Failover Cluster Management Console (Windows Server 2008 and later), and verify if the *SQLComplianceCollectionService* resource is online.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

4.1.6 Upgrade your product license key

IDERA SQL Compliance Manager version 5.0 and later use a new license key. You must update your existing product license key to complete installation of SQL Compliance Manager 5.0 or later. To request a new license, contact licensing@idera.com. Provide the host name of the server/SQL Server instance hosting SQLcompliance manager. If using the default name MSSQLSERVER for SQL, simply provide the server host name.

4.2 Installation and deployment

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

✓	**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 both the IDERA Dashboard and SQL Compliance Manager. For more information, see IDERA Dashboard requirements and 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 IDERA Dashboard and SQL Compliance Manager in your environment. For more information, see Implementation scenarios.
✓	Review the deployment considerations for implementation of best practices. For example, if you plan to audit databases that sustain a heavy workload, install the Collection Server on a dedicated computer.

	Follow these steps ...
✓	Identify the Windows account under which the SQL Compliance 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 IDERA Dashboard and SQL Compliance Manager as instructed. For more information, see How to install SQL Compliance Manager. ***If you are installing SQL Compliance Manager on a Windows* cluster**, see how to audit a virtual SQL Server instance.

⚠ It is possible to install and use IDERA SQL Compliance Manager without installing the IDERA Dashboard. The IDERA Dashboard works as a complement of SQL Compliance Manager, allowing you to monitor SQL Server instances remotely.
To learn more about this product, visit IDERA Dashboard.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

ⓘ Due to changes in the product registry with CWF, IDERA SQL Compliance Manager 5.5 installer increased in size.

4.2.1 Troubleshooting: Missing Extended Events-related DLL files

IDERA SQL Compliance Manager 5.4 and later includes support for SQL Server Extended Events. Users installing or upgrading to this version of SQL Compliance Manager may receive a message similar to the following:

> The files `Microsoft.SQLServer.XEvent.Linq.dll` and `Microsoft.SQLServer.XE.Core.dll` are missing. Please download and install the Shared Management Objects and corresponding CLR Types from the SQL Server 2016 Feature Pack. Learn more.

Also visit the following Microsoft links:

- Download the Microsoft SQL Server 2016 Feature Pack
- Installing SMO for SQL Server 2016
- CLR User-Defined Types for SQL Server 2016

4.2.2 Product components and architecture

The IDERA Dashboard and IDERA SQL Compliance Manager consist of a light, unobtrusive architecture that easily runs in your SQL Server environment with minimal configuration. All components run outside and separate from SQL Server processes.

- Learn about the IDERA Dashboard components and architecture.
- Learn about the SQL Compliance Manager components and architecture.

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

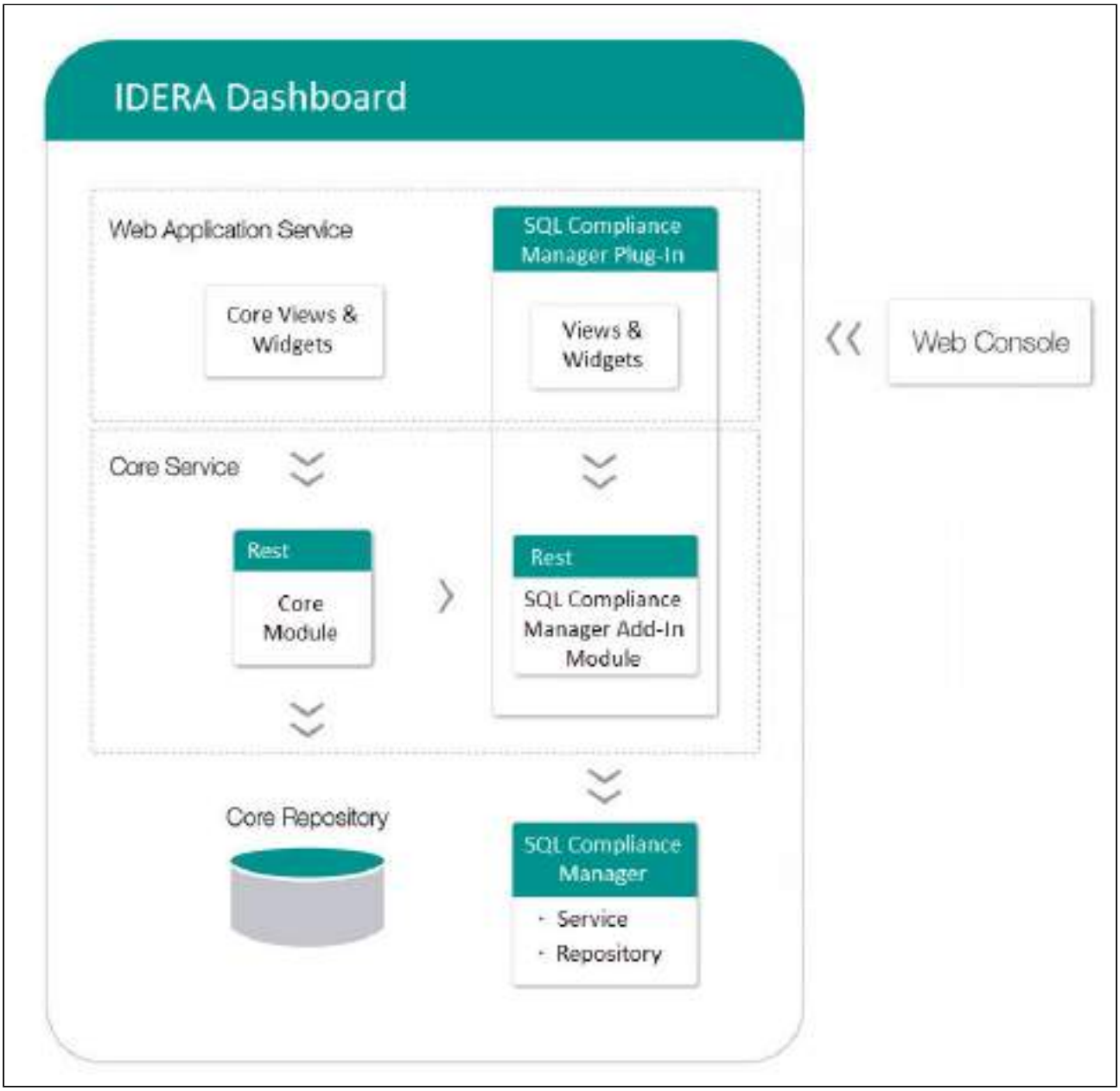
IDERA Dashboard components and architecture

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard provides web and back-end services, shared across multiple Idera products. To learn more about what the IDERA Dashboard is and how it works, see Navigate the Idera Dashboard.

The IDERA Dashboard consists of the following components:

- Web Application Service
- Core Service
- Core Repository



Web Application Service

The Web Application Service is a Windows service that wraps Apache Tomcat server. The Web Application Service serves up dashboard (IDERA Dashboard) and SQL Compliance Manager views and widgets that are displayed in the web console. The Web Application Service requires three ports:

- Standard HTTP port (by default 9290)
- Monitor port (9094)
- SSL port (9291)

Core Service

The Core Service is a C# (.NET 4.0 Framework) based Windows service that hosts dashboard and SQL Compliance Manager REST APIs that are used by the Web Application Service to configure and retrieve data. In addition, the Core Service handles product registration, security, configuration, product data, and event aggregation.

The Core Service uses two ports, one for REST API and the other for .NET remoting:

- Core Service REST API port (by default 9292)
- .NET remoting port (by default 9293)

Core Repository

The Core Repository is a database where all IDERA Dashboard's configuration and aggregated data is stored. The Core Repository database is hosted on a SQL Server instance and is accessed by the Core Service to retrieve data.

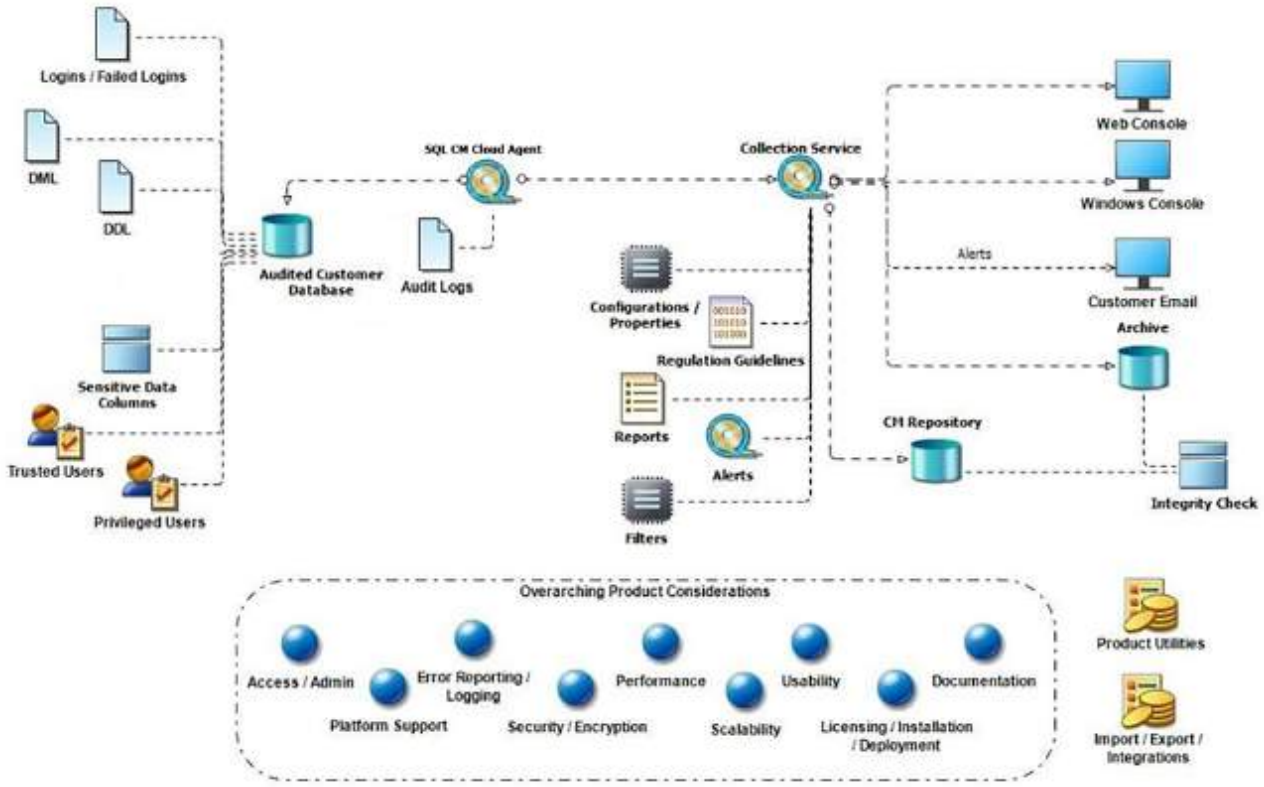
SQL Compliance Manager components and architecture

IDERA SQL Compliance Manager consists of a light, unobtrusive architecture that efficiently runs in your SQL Server environment with minimal configuration. All SQL Compliance Manager components run outside and separate from SQL Server processes. SQL Compliance Manager does not add to or modify 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 Compliance Manager offers a unique, loosely coupled architecture that is both flexible and extremely powerful. As a result, SQL Compliance Manager 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
- SQL Compliance Manager 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, SQL Compliance Manager Agent events, Activity Report Card statistics, and other SQL Compliance Manager configurations.
SQLcompliance.Processing	Stores processing event data received from the SQL Compliance Manager 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 SQL Compliance Manager Agent, stores audit data in the events and archive databases, and sends audit setting updates to the SQL Compliance Manager Agent. The Collection Server runs under the Collection Service account. By default, the Collection Server communicates with the Agents every five minutes (heartbeat) to write processed audit data to the event databases associated with the registered SQL Server instances.

SQLcompliance Agent

The SQL Compliance Manager 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 SQL Compliance Agent runs under the SQL Compliance Agent Service account. For more information, see How the SQL Compliance Manager Agent works.

SQLcompliance Cloud Agent

SQL Compliance Manager 6.0 and above support remote auditing on SQL servers on EC2, allowing users to audit instances on their Amazon EC2 Servers using the SQL CM Agent. Auditing with the Cloud Agent service, except for XEvents, Trace Files, and Before and After data, offers all the functionalities covered by the SQL CM Agent. Once the audit is complete, all data is transferred from the Cloud Agent to the Collection Service for the real-time status of your audited SQL Server instances. Users can take advantage of the improved architecture that allows registering RDS instances with the Cloud Agent Service. For more information, see How the SQL Compliance Manager Cloud Agent works

Sensitive Column auditing is supported by SQL Compliance Manager 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 SQL Compliance Manager Agent's settings 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.

CLI Operations	Description
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 SQL Compliance Manager Agent. The SQL Compliance Manager Agent stores these temporary files in a secure directory on the audited SQL Server instance. When the set directory size threshold is reached, the SQL Compliance Manager Agent stops the SQL trace until the trace files are sent to the Collection Server for processing. The trace file is cycled when the set file size threshold is met. You can configure the SQL Compliance Manager Agent trace file directory location and how the Compliance Manager Agent manages these files, such as how often the agent sends trace files to the Collection Server. For more information, see How the SQL Compliance Manager Agent works.

4.2.3 Product requirements

The IDERA Dashboard and IDERA SQL Compliance Manager consist of a light, unobtrusive architecture that easily runs in your SQL Server environment with minimal configuration.

Prior to the installation of the products, it is important for you to review the system requirements for SQL Compliance Manager and the IDERA Dashboard.

- Learn about the IDERA Dashboard requirements.
- Learn about the SQL Compliance Manager requirements:
  - Hardware requirements
  - Permissions requirements
  - Port requirements
  - Software requirements

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

IDERA Dashboard requirements

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

To successfully install the IDERA Dashboard, you need to comply with the following requirements:

Type	Requirement
Operating System	Windows XP SP2+ Windows Server 2003 SP2 Windows Server 2008 SP1+ Windows Vista SP2+ Windows 7 Windows 2008 R2 Windows 8 Windows 2012
Repository	SQL Server 2005 SP1+ SQL Server 2008 SQL Server 2008 R2 SQL Server 2012 SQL Server 2014 SQL Server 2016
Microsoft. NET Framework version	4.0 or later
Browser	Internet Explorer IE 9.x+ Google Chrome Mozilla Firefox Microsoft Edge
Web Server	Apache Tomcat 7.0

⚠ The IDERA Dashboard does not support SQL Server 2005. You can install SQL Compliance Manager on SQL Server 2005 and use a remote IDERA Dashboard installation on SQL Server 2005 SP1+ and above.
For more information, see SQL Compliance Manager Software requirements.

Port requirements

The IDERA Dashboard uses the following ports:

- IDERA Dashboard Core Services port: **9292**
- IDERA Dashboard Web Application Service port: **9290**
- IDERA Dashboard Web Application Monitor port: **9094**
- IDERA Dashboard Web Application SSL port: **9291**

The IDERA Dashboard Web Application service comes with SSL already set up. For more information on running the IDERA Dashboard over SSL, see Run the Idera Dashboard over SSL (HTTPS).

Hardware requirements

The following sections provide the hardware requirements for each IDERA 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 60-90 GB for Repository

For more information, see SQL Compliance Manager Hardware Sizing guidelines.

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

SQL Compliance Manager Hardware Sizing guidelines

The following guidelines provide an estimation of the hardware resources required to deploy SQL Compliance Manager depending on the number of servers you want to monitor with SQL Compliance Manager.

Deployments under 20 Servers

Less than 20 SQL Servers being audited and 10,000 events per hour.

SQL Compliance Manager Repository and Collection Service reside on:

Type	Requirement
Operating System	Windows Server 2012R2 or above
Memory	6 - 12 GB
CPU	2 dual core
SQLcm Repository Size	60 - 90 GB (Allocate this space ahead of time)

These hardware and configuration requirements are basic requirements and can be interpreted differently depending on each environment´s audit requirements and event activity scenarios.
The expected repository growth is approximately 1 GB per every 1 million transactions.
10K events per hour will require 7 GB of space per month.

Deployments of 20-50 Servers

20-50 SQL Servers being audited and 20,000 events per hour.

SQL Compliance Manager Repository and Collection Service reside on:

Type	Requirement
Operating System	Windows Server 2012R2 or above (64 bit)
Memory	12 - 24 GB

Type	Requirement
CPU	Dual 2 - 3 GHZ Quad Core
SQLcm Repository Size	250 GB or more (Allocate this space ahead of time)

These hardware and configuration requirements are basic requirements and can be interpreted differently depending on each environment´s audit requirements and event activity scenarios.
The expected repository growth is approximately 1 GB per every 1 million transactions.
20K events per hour will require at least 15 GB of space per month.

Deployments of 200 Servers or more

200 SQL Servers being audited and 30,000 events per hour.

SQL Compliance Manager Repository and Collection Service reside on:

Type	Requirement
Operating System	Windows Server 2012R2 or above (64 bit)
Memory	24 - 48 GB (more if monitoring Before After Data)
CPU	4 - 8 Dual Core
SQLcm Repository Size	1 TB or more (Allocate this space ahead of time)

These hardware and configuration requirements are basic requirements and can be interpreted differently depending on each environment´s audit requirements and event activity scenarios.
The expected repository growth is approximately 1 GB per every 1 million transactions.
30K events per hour will require at least 200 GB of space per month.

IDERA SQL Compliance Manager is fully supported on Virtual Machines, both HyperV and VMware.

Permissions requirements

IDERA SQL Compliance Manager requires specific permissions and rights to successfully audit events. By default, the setup program assigns the Collection Service and SQL Compliance Manager 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 SQL Compliance Manager 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

Collection service 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

SQL Compliance Manager 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 SQL Compliance Manager Agent trace directory
Manage trace directory for an audited SQL Server instance	Local Administrator permissions on the computer that hosts the registered SQL Server

Actions	Permissions Requirements
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 SQL Compliance Manager Agent trace directory

⚠ To successfully run and pass the Permissions Check, make sure you are logged in as one of the following users:

- SQL Compliance Agent Service User
- SQL Server Service User
- Current Logged-in User

Using Windows Authentication

The SQL Compliance Manager Management 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 contain the appropriate SQL privileges. However, SQL Compliance Manager does not support SQL Server authentication.

Port requirements

To ensure the SQL Compliance Manager 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 IDERA 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 Compliance Manager 5.0 and later versions require .NET 4.0 components. Previous versions of SQL Compliance Manager require at least .NET 3.5.

⚠ IDERA SQL Compliance Manager 5.5.x depends on certain Microsoft components that did not ship with SQL Server versions prior to SQL Server 2012 SP1. Before starting the installation process, please review some important installation steps.

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

SQL Compliance Manager Windows cluster support

You can install SQL Compliance Manager on a Windows cluster 2008, 2012 and later. 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. Note that .NET 4.0 or later must be installed on the audited server.

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
SQL Server 2019	Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 2019
SQL Server 2017	Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
SQL Server 2016	Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
SQL Server 2014	Windows Server 2008, Windows Server 2012
SQL Server 2012 SP1	Windows Server 2008 SP2
SQL Server 2008 R2	Windows Server 2008 R2, Windows Server 2008
SQL Server 2008	Windows Server 2008

Collection Server

The Collection Server stores SQL Compliance Manager configurations and audit data. Ensure your Collection Server resides on a version of SQL Server that is greater than or equal to the highest audited SQL Server version. For example, if the most current version of SQL Server that you are auditing is on SQL Server 2016 then your Collection Server instance could be SQL Server 2016 or 2017 but not 2012.

> ⚠ 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 2019 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 R2 • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 SP1+

Software Type	Requirement
Microsoft SQL Server	The Collection Server requires one of the following versions of Microsoft SQL Server: • SQL Server 2019 • SQL Server 2017 • SQL Server 2016 • SQL Server 2014 • SQL Server 2012 SP1 • SQL Server 2008 R2

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 2019 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 R2 • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 SP1+ 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

> SQL Compliance Manager 5.6 requires you to upgrade the SQL Compliance Manager agents to the same version.

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 2019 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 R2 • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 SP1+

Cloud

SQL Compliance Manager runs on various Cloud Virtual Machines running Microsoft Windows Server and Microsoft SQL Server.

SQL Compliance Manager can access mapped cloud drives but does not support cloud databases.

PaaS Support

Cloud relational database services are currently not supported for auditing or for deploying the software repository databases to, as SQL Compliance Manager requires an Agent Service or a Collection Management Service respectively, to be installed on the client and application/repository side.

Cloud Service Delivery Model	IaaS	PaaS (DBaaS)
Amazon EC2	Windows Server SQL Server	-
Microsoft Azure VM	Windows Server SQL Server	-
Google Cloud Platform	Windows Server SQL Server	-

Web Console

Supported web browsers for the IDERA SQL Compliance Manager Web console include:

- Internet Explorer 10.x+
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

⚠ It is important for you to review the IDERA Dashboard requirements before installing SQL Compliance Manager.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

4.2.4 Supported installation scenarios

You can install and deploy IDERA 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 Compliance Manager 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
- SQL Compliance Manager 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
- SQL Compliance Manager Agents on each cluster node hosting the virtual SQL Server you want to audit

For more information, see Deploying SQL Compliance Manager in a clustered environment.

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
- SQL Compliance Manager Agents on each SQL Server instance you want to audit in a non-trusted domain or workgroup

4.2.5 Deploy the IDERA Dashboard and SQL Compliance Manager

Use the following links to prepare for your SQL Compliance Manager and IDERA Dashboard deployment:

- Check the supported installation scenarios
- Learn about the components and architecture
- Review system requirements for the IDERA Dashboard and SQL Compliance Manager
- View the installation instructions
- Log in to the IDERA Dashboard

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

Deploying SQL Compliance Manager in a clustered environment

IDERA SQL Compliance Manager allows you to audit and report on your clustered SQL Server environment. See Deploy SQL Compliance Manager in a clustered environment using Windows Server 2008 and later for installation and configuration instructions.

The IDERA Dashboard does not provide support for clustered environments, you need to install it in a stand-alone machine first. For more information on installation and configuration instructions, see Deploy the IDERA Dashboard in clustered environments.

⚠ It is possible to install and use IDERA SQL Compliance Manager **without** installing the IDERA Dashboard. The IDERA Dashboard works as a **complement** of SQL Compliance Manager, allowing you to monitor SQL Server instances remotely.
To learn more about this product, visit IDERA Dashboard.

⚠ When a primary node of an AG becomes a secondary node, previously collected trace files fail to process and remain gathered on the Passive node. Once the node becomes Active the trace files continue to process normally.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

Deploy the IDERA Dashboard in a clustered environment and register SQL Compliance Manager

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

If you want to use the IDERA Dashboard in a clustered environment, you need to install this product in a stand-alone server first.

1. Log on with an administrator account to the stand-alone server in which you want to install the IDERA Dashboard.
2. Run `SQLCMInstall.EXE` in the root of the installation kit.
3. Review the information you need to start the installation and click **Next.**
4. Review and accept the license agreement by selecting the ***I accept the terms and conditions of the End User License Agreement*** checkbox.
   Select the **IDERA Dashboard** setup type and click **Next.**
5. Specify the location in which you want to install the IDERA Dashboard and click **Next.**
6. Specify a SQL Server Instance and a form of authentication to create the IDERA Dashboard repository, and click **Next**.
7. Type the appropriate credentials in the provided fields under which the IDERA services run, and click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
8. Review the installation settings and click **Install.**

Once the IDERA Dashboard installation is complete, you can use it to register SQL Compliance Manager.

You can install SQL Compliance Manager and register the product with an existent IDERA Dashboard. For more information, see Deploying SQL Compliance Manager in a clustered environment.

If you install the IDERA Dashboard after installing SQL Compliance Manager in your clustered environment, you can register the product through the web console.

Registering SQL Compliance Manager with IDERA Dashboard allows users to access SQL Compliance Manager using a web browser.

1. Log into the IDERA Dashboard using an administrator account.
2. Go to **Administration** and select **Manage Products.**
3. Click on **Register a Product** and specify:
    a. **Product install location:** select whether the product is installed locally or remotely.
    b. **Host (Machine or IP address):** type the cluster name where SQL Compliance Manager is located.
    c. **Host User Name and password:** type the cluster hosting SQL Compliance Manager credentials.
    d. **Product:** type SQLCM to register SQL Compliance Manager.
    e. **Display Name:** type a unique name under which the Dashboard will show SQL Compliance Manager.
    f. **Port:** specify the port number SQL Compliance Manager uses.
    g. **User Name and password:** type the credentials of a Dashboard administrator account.
4. Click **Register.**
5. Click **Yes** to confirm the registration of the product.

For more information about the IDERA Dashboard configuration, see Manage the IDERA Dashboard.

Deploy SQL Compliance Manager in a clustered environment using Windows Server 2008 and later

The following instructions guide you through the installation of IDERA SQL Compliance Manager in a Windows Server 2008 and later 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

Follow the steps described in the links below to complete the installation of SQL Compliance Manager in a Windows Server 2008 and later clustered environments

1. Install SQL Compliance Manager Collection server on cluster nodes
2. Register SQL Compliance Manager Collection server as a clustered resource

    ⚠ When auditing the **Collection Server** itself, follow steps 3 and 4 to complete the installation of SQL Compliance Manager

3. Install the IDERA Cluster Configuration Console
4. Deploy the SQLcompliance Agent to cluster nodes

Install SQL Compliance Manager 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 Compliance Manager 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 Compliance Manager 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 `SQLCMInstall.exe` in the root of the SQL Compliance Manager installation kit on the first cluster node.
3. Review the information you need to start the installation and click **Next.**
4. Select the **SQL Compliance Manager** setup type and uncheck the **IDERA Dashboard** setup type.

   ⚠ The IDERA Dashboard does not provide support for clustered environment installations. If you want to use the IDERA Dashboard, review Deploy the IDERA Dashboard in a clustered environment.

   Review and accept the license agreement by selecting the ***I accept the terms and conditions of the End User License Agreement*** checkbox.
5. Specify if you want to register SQL Compliance Manager with an existent IDERA Dashboard.
   If you select Yes, you need to provide the IDERA Dashboard location and administrator credentials.
6. Specify the location in which you want to install SQL Compliance Manager.
7. Enable the **Clustered Environment** checkbox and select whether you are installing SQL Compliance Manager in an active or a passive node.
   Specify a SQL Server Instance and a form of authentication to create the SQL Compliance Manager repository.
   Test the connections to make sure the information is correct and click **Next.**
8. ***If you install on the currently active node,*** specify a trace directory on a shared disk, and click **Next**.
   If you install on a passive node, the wizard skips this step.
9. Type the appropriate credentials in the provided fields under which the IDERA services run, and click **Next**.
   IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment, the installer grants the "Log on as a Service" right to the account that you specify.
10. Review the installation settings and click **Install**.
11. In Windows Services, stop the SQL Compliance Manager Collection service and set the Startup type to **Manual**.

Repeat the previous steps on each cluster node. Point to the SQL Compliance Manager 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.

Once the installation of SQL Compliance Manager is completed, proceed to Register the SQL Compliance Manager Collection Service as a clustered resource.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

Register the SQL Compliance Manager Collection service as a clustered resource

After installing the SQL Compliance Manager components on your cluster nodes, create the clustered service resources to allow SQL Compliance Manager to recognize the cluster nodes.

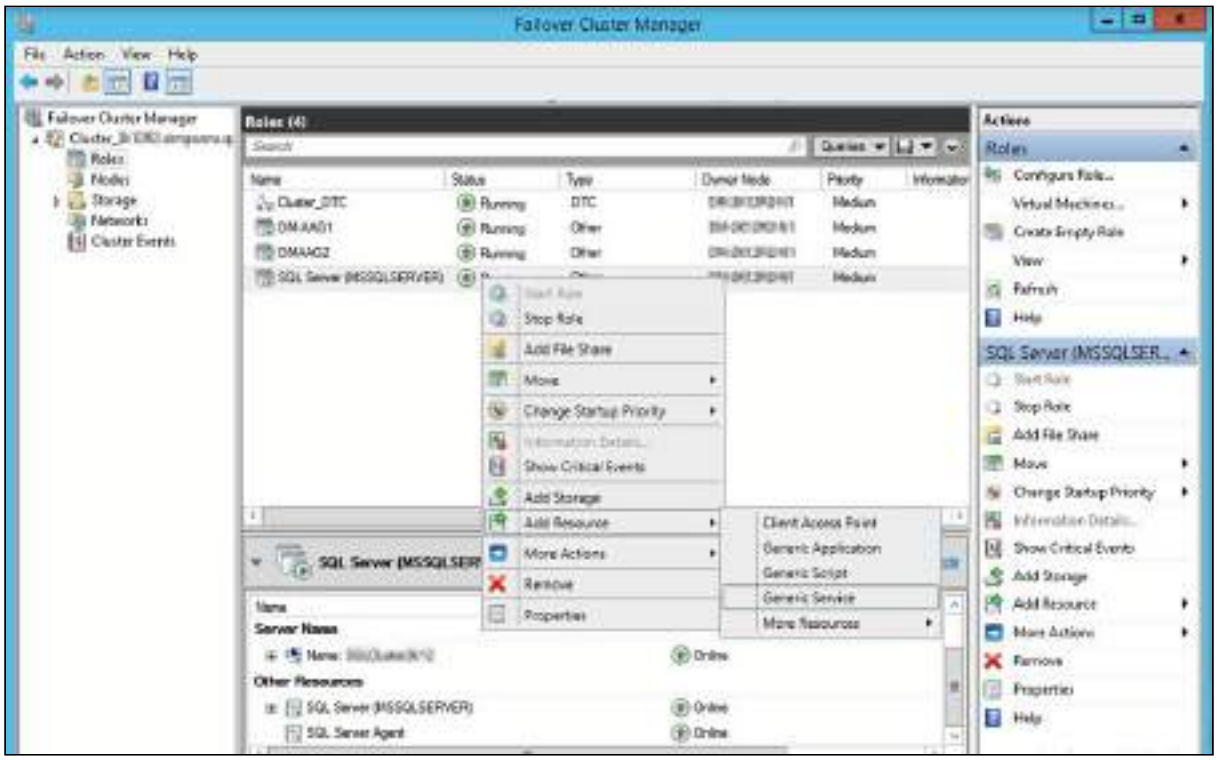
Registering SQL Compliance Manager services with Microsoft Failover Cluster Manager allows the Microsoft Cluster Service to manage the services in failover situations. The following configuration ensures the high availability of the services during a failover.

Below you can find a set of instructions to register the SQL Compliance Manager services as a clustered resource:

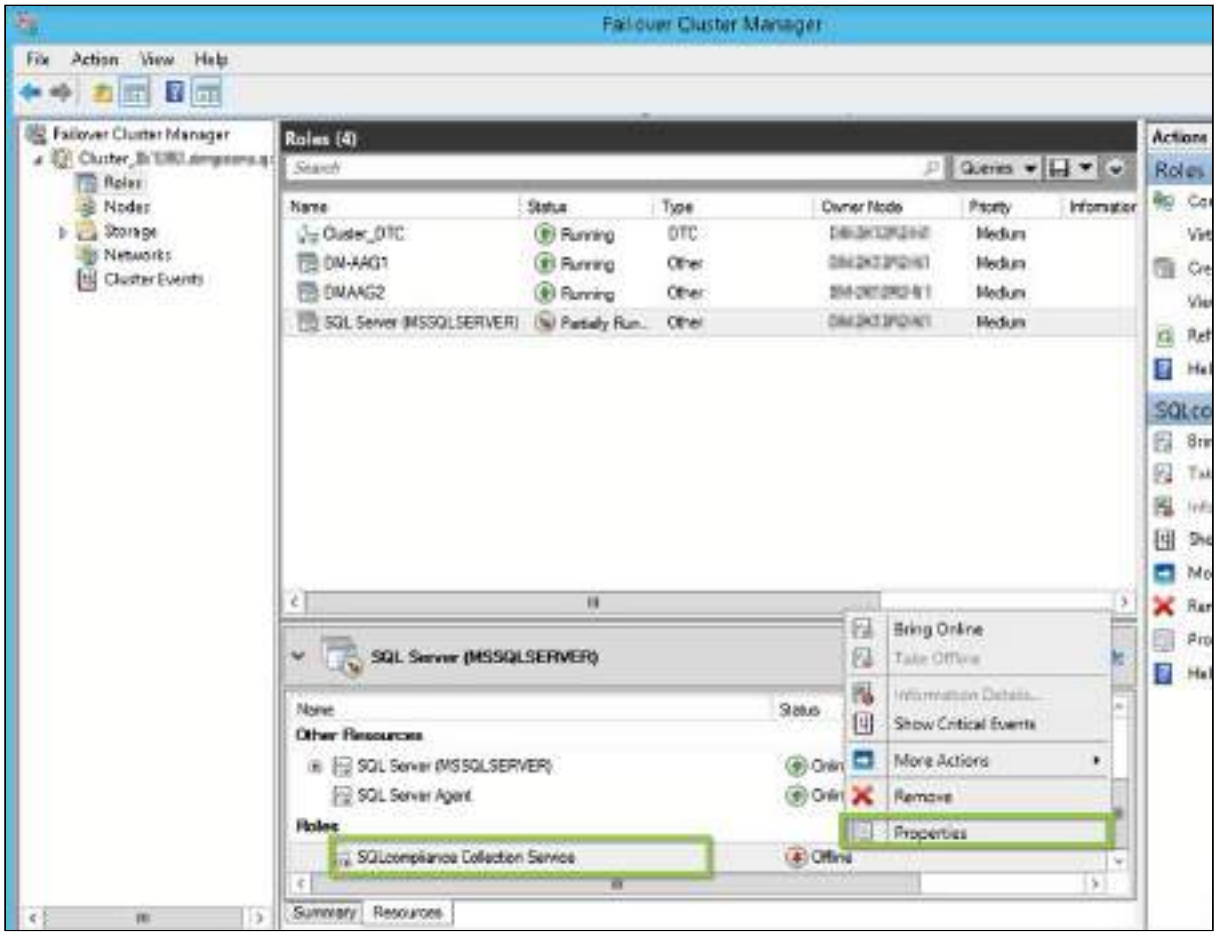
Adding SQL Compliance Manager Collection service to an existing role

After finishing the installation in all nodes, go to the active node and follow the steps below.

1. Open the Microsoft Failover Cluster Manager and select **Roles**
2. Right-click on the SQL Server role, point to **Add Resource**, and select **Generic Service**



3. Microsoft Failover Cluster Manager displays the **New Resource** Wizard
4. **Select** *SQLcompliance Collection Service*, click **Next,** review the generic service configuration summary, and click **Finish**
5. In the Roles section, right-click the *SQLcompliance Collection Service*, and select **Properties**



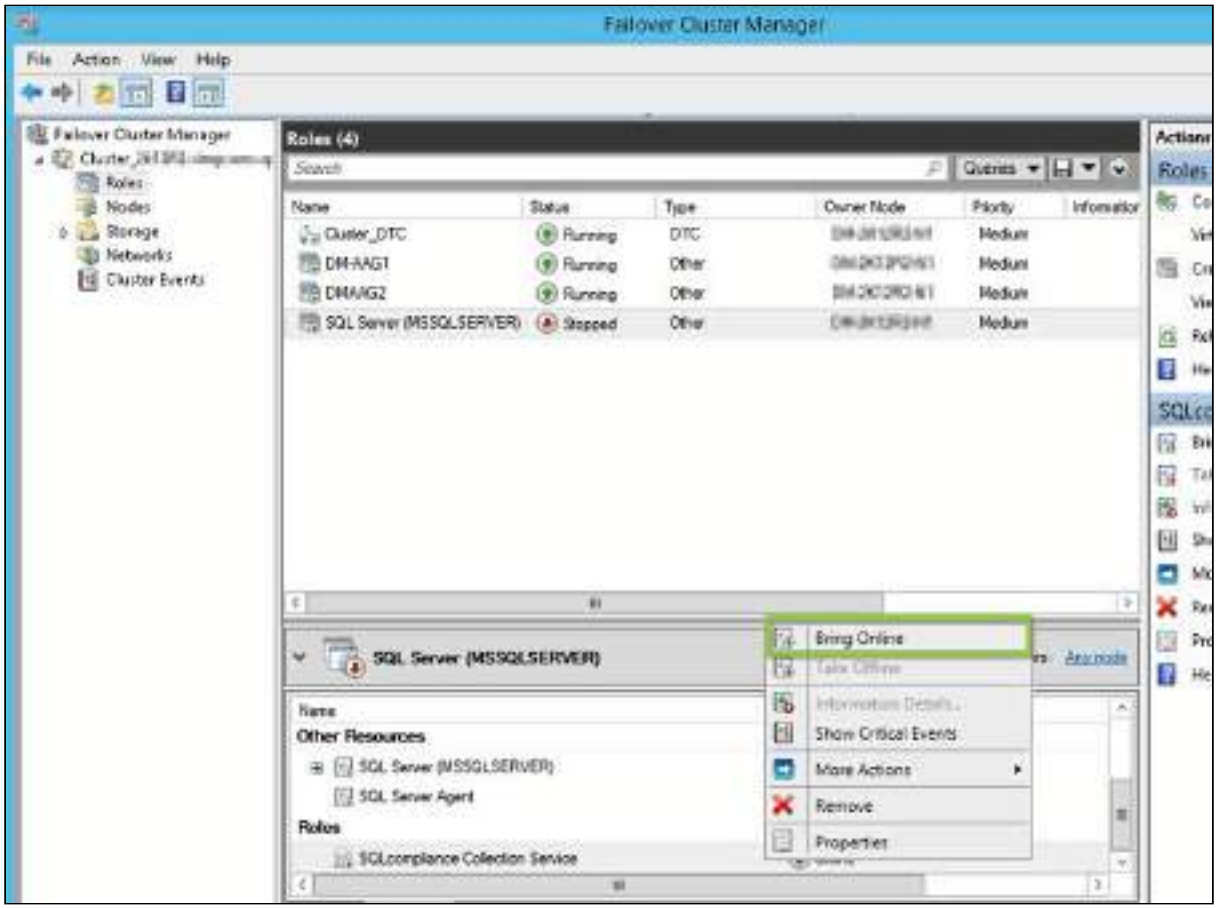
6. On the General tab, check the ***Use Network Name for computer name*** box, and click **Apply**

> If this action throws an error, try again after configuring the following information:
> Go to the **Dependencies** tab, add the following resources: *SQL Server* and *SQL Server Agent*, and click **Apply.**

7. On the Registry Replication tab, click **Add**
8. **Type** `Software\Idera\SQLCM` and click **OK**

> The **Registry Replication** tab is not available in Windows Server 2012.
> If you are using Windows Server 2012, you must use the *"Add-ClusterCheckpoint"* PowerShell cmdlet to add the necessary setting.
> For more information, see Add ClusterCheckpoint.

9. In the Roles section right-click the SQLcompliance Collection Service and **Bring** the resource **Online**.



10. Open the Microsoft Failover Cluster Manager on the other nodes and verify if the SQLcompliance Collection Service is online.

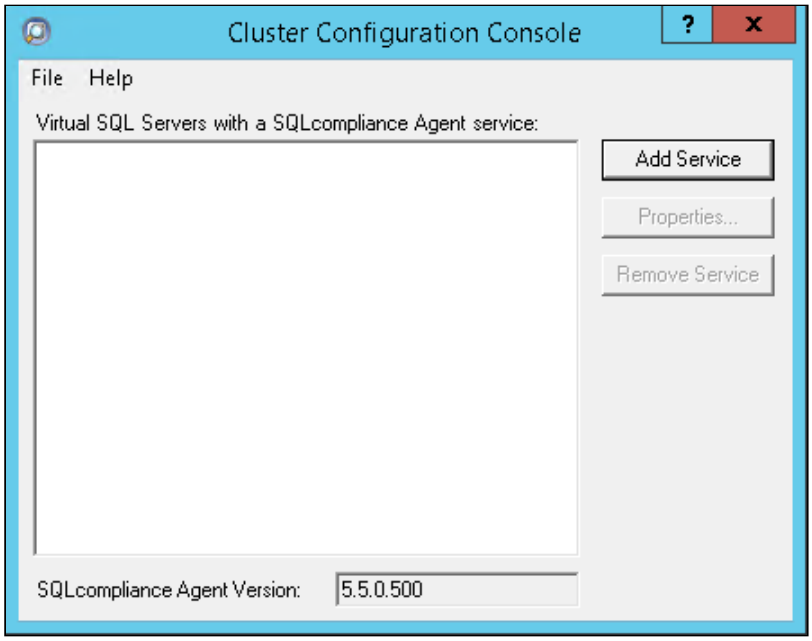
After registering the collection service as a clustered resource, proceed to install the IDERA Cluster Configuration Console to configure the SQL Compliance Manager Agent.

Install the IDERA Cluster Configuration Console

Once the installation of SQL Compliance Manager is complete, you need install the IDERA Cluster Configuration Console.

> ⓘ You must perform these steps on **all nodes** of the cluster.

1. Go to the SQL Compliance Manager install path. Unless you have specified a different path, the one by default is `C:\Program Files\IDERA\SQLCompliance`.
2. Run `SQLcomplianceClusterSetup.EXE`.
3. Once the setup wizard launches, click **Next** to proceed to the License Agreement.
4. Read the license agreement, select the option to accept the terms of the license agreement, and click **Next**.
5. Select the destination path in which you want to install the IDERA Cluster Configuration Console. Define the permissions for the software and click **Next.**
6. Click **Install** to complete the installation.



Once the Cluster Configuration Console is installed, review Deploy the SQL Compliance Manager Agent to cluster nodes.

Deploy the SQL Compliance Manager Agent to cluster nodes

Now that the IDERA Cluster Configuration Console is installed, you need to add the SQL Compliance Manager Agent to the clustered instance that is to be audited.

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 SQL Compliance Manager Agent communication.
☐	For each cluster node, identify the folder you want to use for the SQL Compliance Manager 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.

☑	**Follow these steps ...**
☐	For each cluster node, identify the account you want to use for the SQL Compliance Manager 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 SQL Compliance Manager Agent Service permission requirements.
☐	Deploy the SQL Compliance Manager Agent to each cluster node using the Cluster Configuration setup program.
☐	Add the SQL Compliance Manager Agent service on each cluster node using the Cluster Configuration Console.
☐	Register the SQL Compliance Manager Agent 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 SQL Compliance Manager 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.

1. Add the SQL Compliance Manager Agent

> ⓘ You must perform these steps on **all nodes** of the cluster.

1. Once the ***Cluster Configuration Console*** launches, click **Add Service.**
2. On the ***General*** dialog window, specify the name of the clustered instance to be audited by IDERA SQL Compliance Manager and click **Next.**
3. On the ***Collection Server*** dialog window, specify the name of the server hosting the SQLcompliance Collection Service and click **Next.**
4. On the ***SQLcompliance Agent Trace Directory*** dialog window, specify the path on which trace files will temporarily reside before being transferred to the SQLcompliance Collection Service.
   The path specified should be on a drive that is a part of the same resource group as the SQL Server instance to be audited.
5. On the ***CLR Trigger Location*** dialog window, specify the path on which trigger assembly files will reside. The path specified should be on a drive that is a part of the same resource group as the SQL Server instance to be audited.
   Click **Next**.

   > ⚠ Ensure the Agent Trace directory and the CLR Trigger location specified exist by creating the folder structure manually through Windows Explorer.

6. Review the configuration and click **Finish.**
7. The IDERA Cluster Configuration Console displays a confirmation message stating that you have successfully added the SQL Compliance Manager Agent.
   Click **OK**.

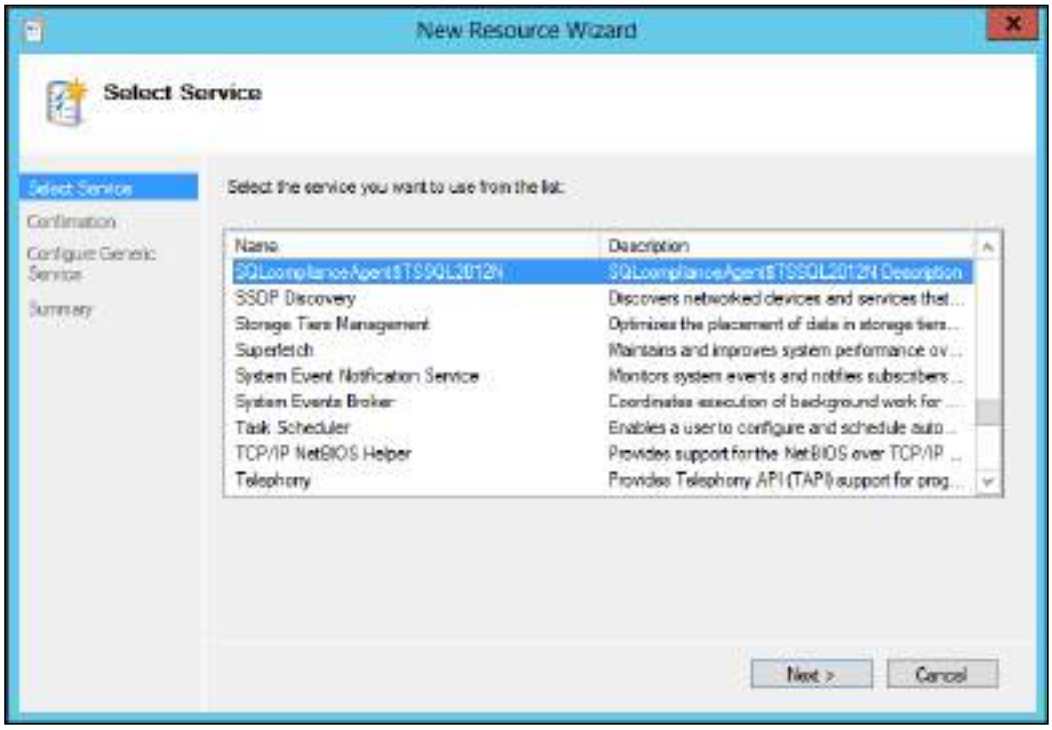
2. Register the SQL Compliance Manager Agent as a clustered service

Registering the SQL Compliance Manager Agent service with Microsoft Failover Cluster Manager allows the Microsoft Cluster Service to manage the SQL Compliance Manager Agent service in failover situations. This configuration ensures that auditing will continue during a failover and no audit data is lost.

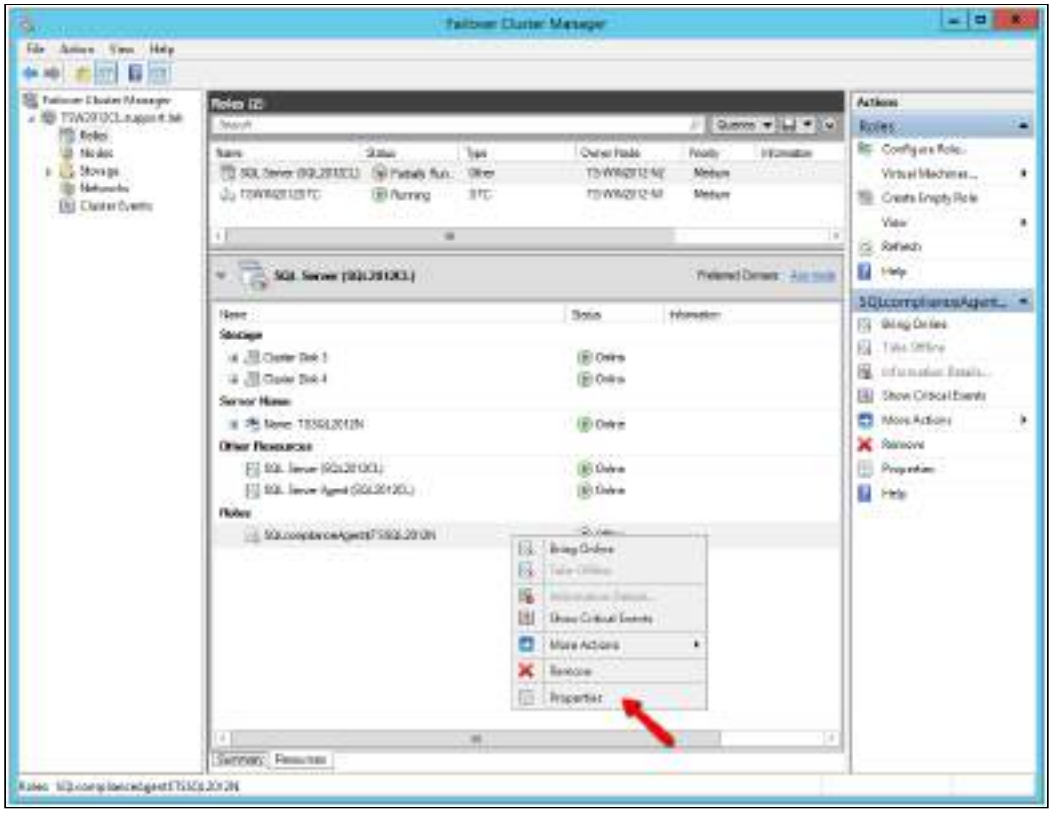
> ⓘ You must perform these steps only **once**, in the **active node**.

1. Log onto the active cluster node using an administrator account and launch the Microsoft Failover Cluster Manager.
2. Right-click the role created for the clustered instance, point to **Add a Resource,** and select **Generic Service**.

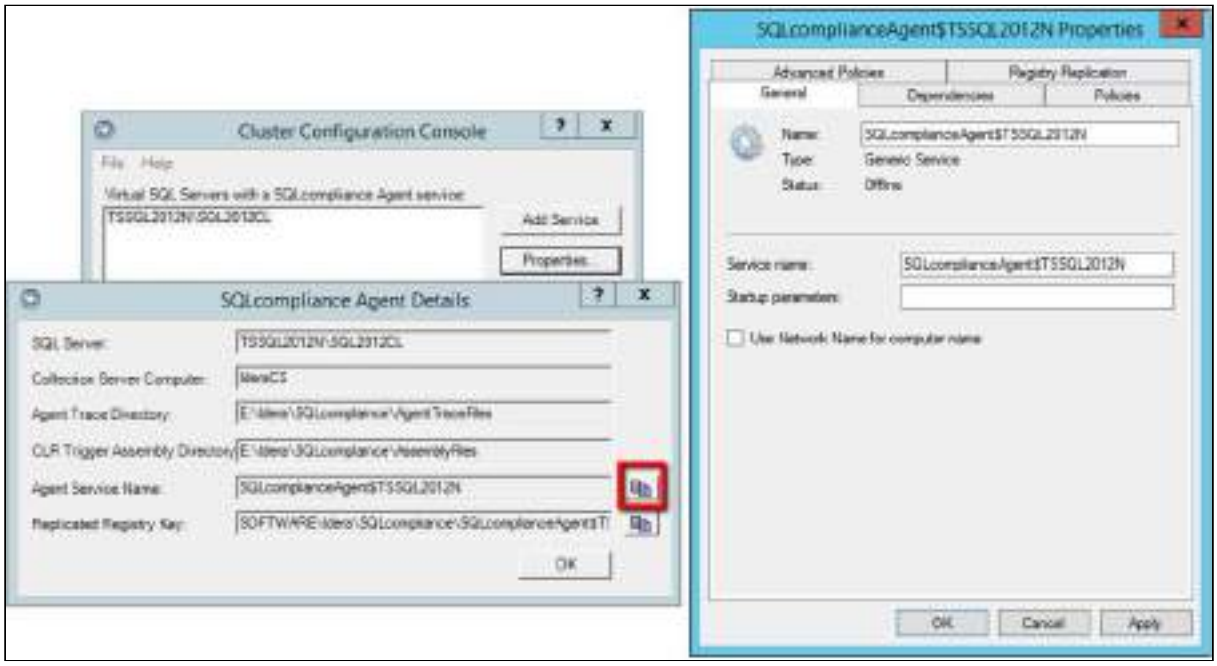
3. On the ***Select Service*** dialog window, **select** the SQL Compliance Manager Agent service created previously, continue following the wizard, and click **Finish**.



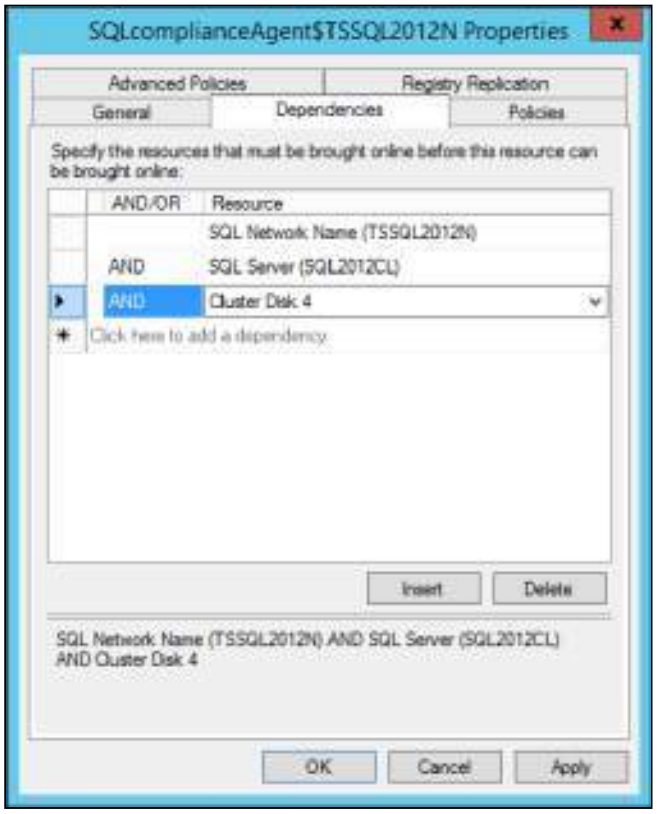
4. The Failover Cluster Manager displays the new resource in the resources tab. Right-click the new resource and select **Properties**.



5. In the ***General*** tab, specify the ***Service name*** as the Agent Service name found in the ***SQLcompliance Agent details*.**



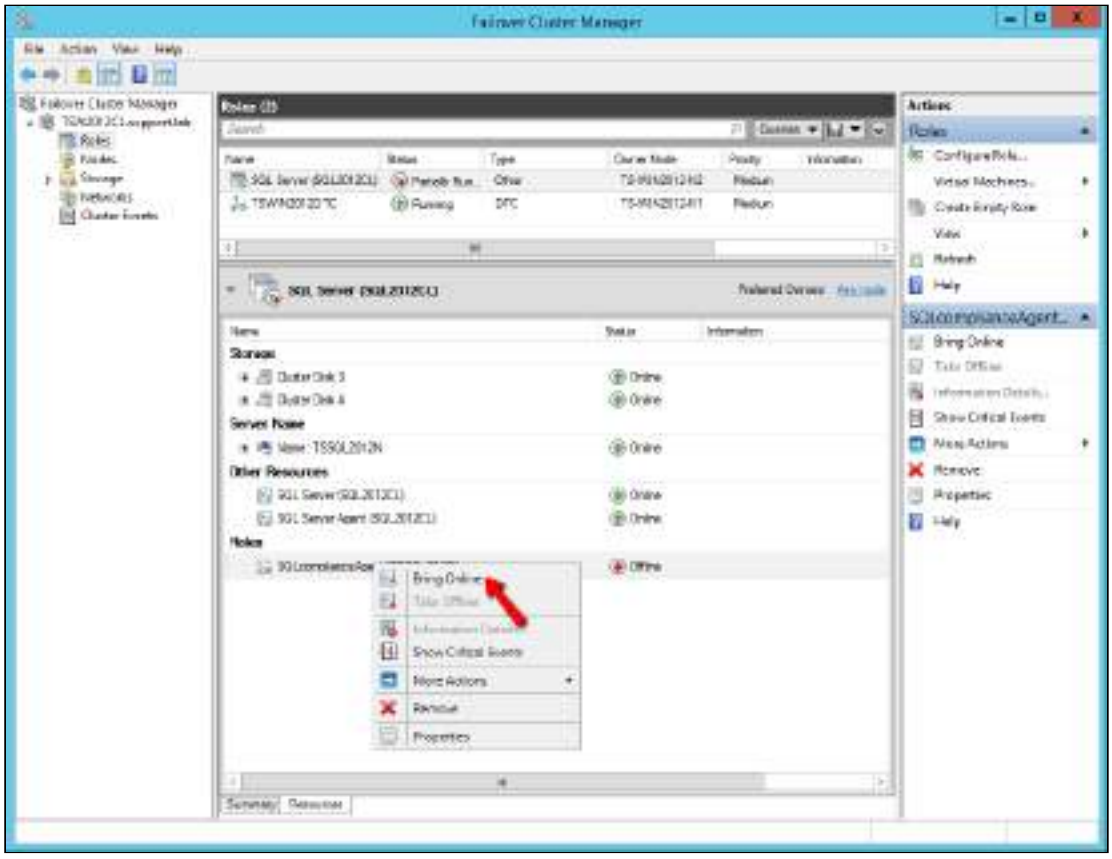
6. Clear the ***Startup parameters.***
7. Go to the ***Dependencies*** tab and add the following dependencies:
    a. *SQL Network Name:* name of the cluster hosting the SQL instance to be audited.
    b. *Cluster Disk(s):* the disk(s) on which the agent trace directory and the CLR trigger assemblies reside.
    c. *SQL Server:* the SQL Server instance to be audited by SQL Compliance Manager.



8. Once the dependencies are configured, click **Apply.**
9. Return to the ***General*** tab, check the **Use Network Name for computer name** box and click **Apply.**
10. Go to the ***Registry Replication*** tab.

    > ⚠ The Registry Replication tab is not available in Windows Server 2012.
    > If you are using Windows Server 2012, you must use the *"Add-ClusterCheckpoint"* PowerShell cmdlet to add the necessary setting.
    > For more information, see Add ClusterCheckPoint.

    Add a specific registry path. To obtain the correct path, go to the IDERA Cluster Configuration Console and copy the ***Replicated Registry Key*** from the ***SQLcompliance Agent details*.**
    Click **OK.**
11. On the **Properties** window, click **Apply** to save the changes, and click **OK** to return to the ***Resources*** *tab.*
12. Right-click the *SQLcompliance Agent* resource and click **Bring Online.**



After successfully deploy the SQL Compliance Manager Agent, you can start auditing your virtual SQL Server instances.

Deployment considerations

Before implementing IDERA 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 Compliance Manager 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 IDERA SQL Compliance Manager 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

Property Name	Benefits	Value
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 you can access for future reporting. For more information about archiving, see How archives work.

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 IDERA 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.

4.2.6 How to install SQL Compliance Manager

Pre -Installation

Before installing IDERA 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.
- A SQL Server instance to host the IDERA SQL CM and the IDERA Dashboard repository databases.
- Have valid Service Account credentials for the IDERA Services.
- ***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 or higher instance.

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

> IDERA SQL Compliance Manager versions 4.5 and older. For installations of SQL Compliance Manager 5.0 and newer, including the IDERA Dashboard, see How to install SQL Compliance Manager and the IDERA Dashboard.

Fresh Installation

Install Features

1. Select the **Fresh Installation** option.

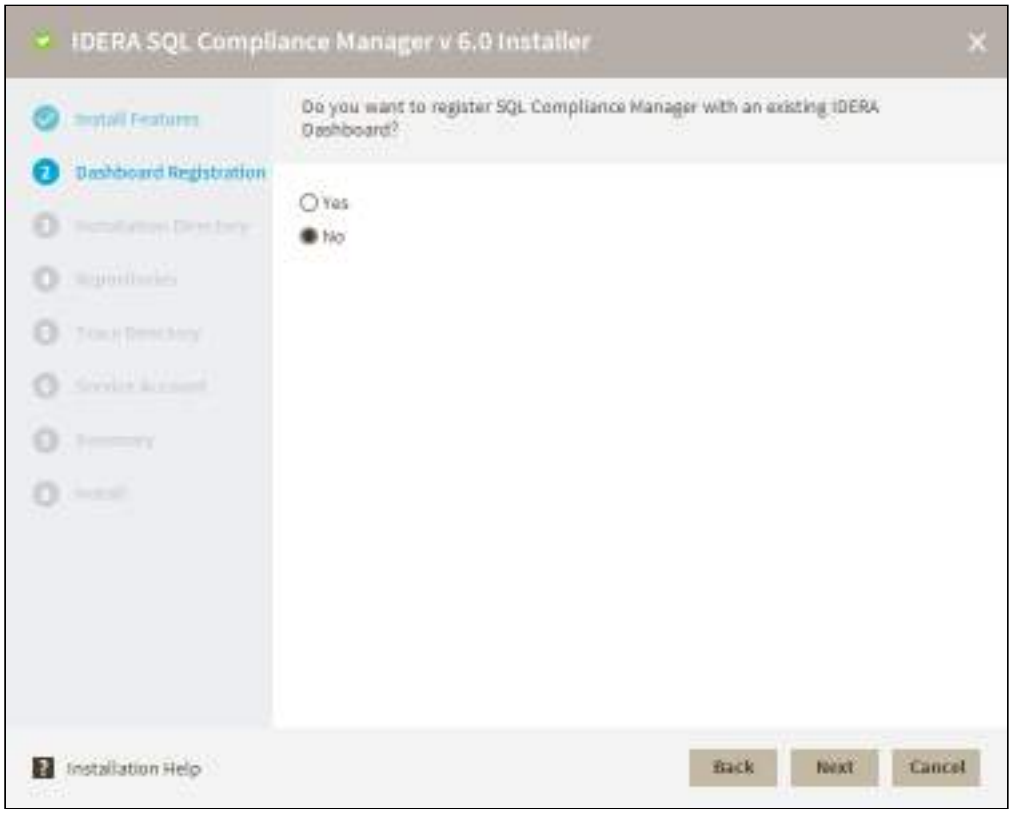
2. Accept the terms and conditions of the EULA and click **Next**.
    a. Click the link to open the EULA dialog to review it in detail.
3. Select the features you want to install and click **Next**.
    a. SQL Compliance Manager - Installs the collection service, the management console, and the agent components.
    b. SQL Compliance Manager Management Console - installs the application only.
    c. SQL Compliance Manager Agent Components - installs the agent service and its required components only.
    d. IDERA Dashboard - installs the IDERA Dashboard that can be accessed via web console to access SQL CM.

Dashboard Registration

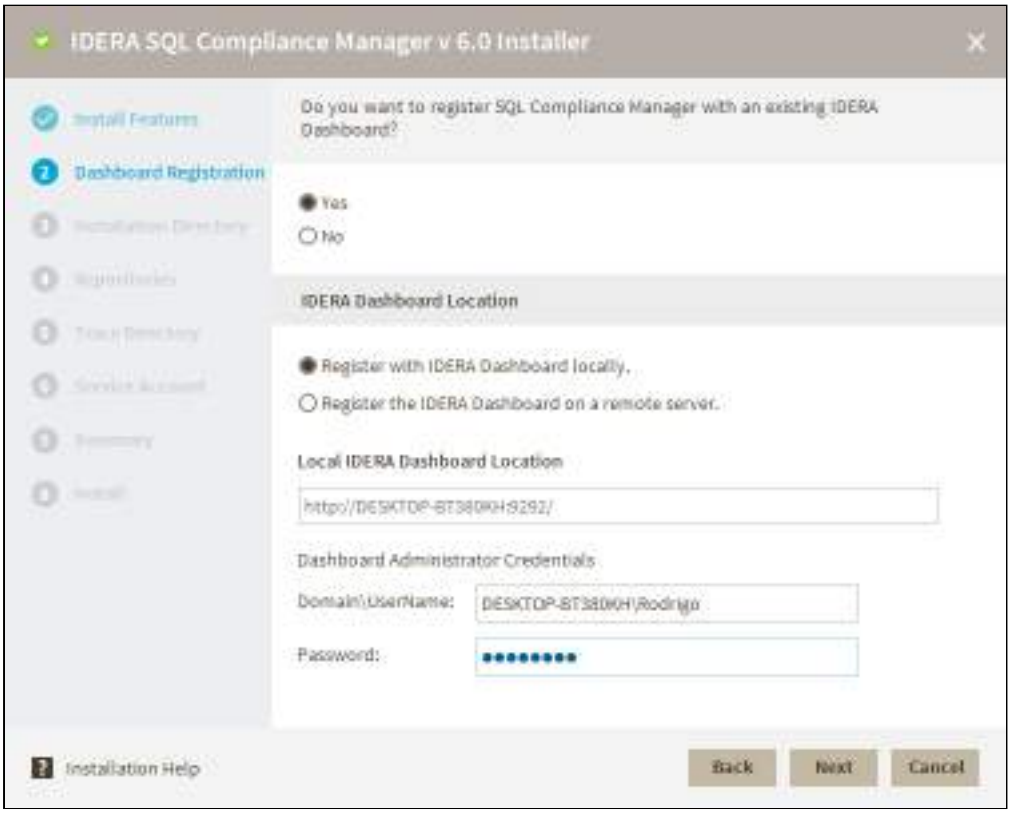
Select if you want to register SQL CM with an existing IDERA Dashboard.

Register the IDERA Dashboard locally - type in the Dashboard Location where you want to install the IDERA Dashboard and type in your Administrator Credentials.

1. Choose whether you want to register SQL CM to an existing IDERA Dashboard. If you choose **Yes**, follow the steps below. If you choose **No**, click **Next**.

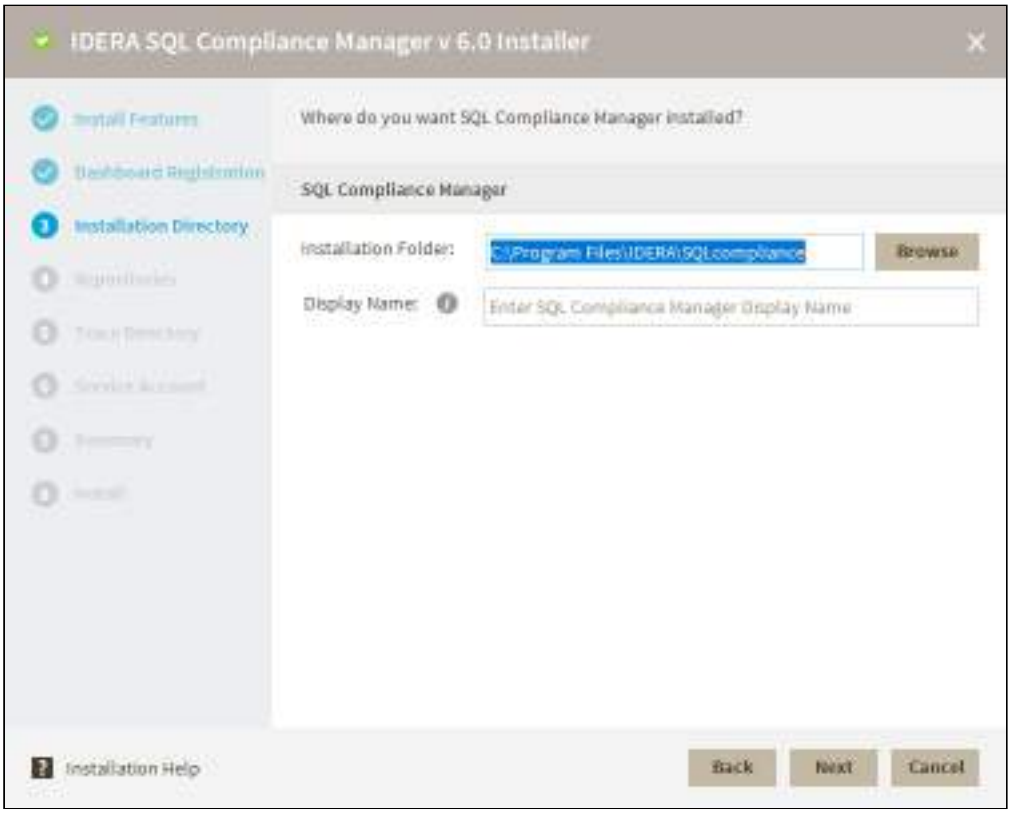


a. Select whether to register SQL CM with the IDERA Dashboard locally or on a remote server.
b. In the text field type in the Remote IDERA Dashboard Location addressed. If you selected to register locally, the address fills in automatically.
c. Fill in the text fields with your UserName and Password and click **Next**.



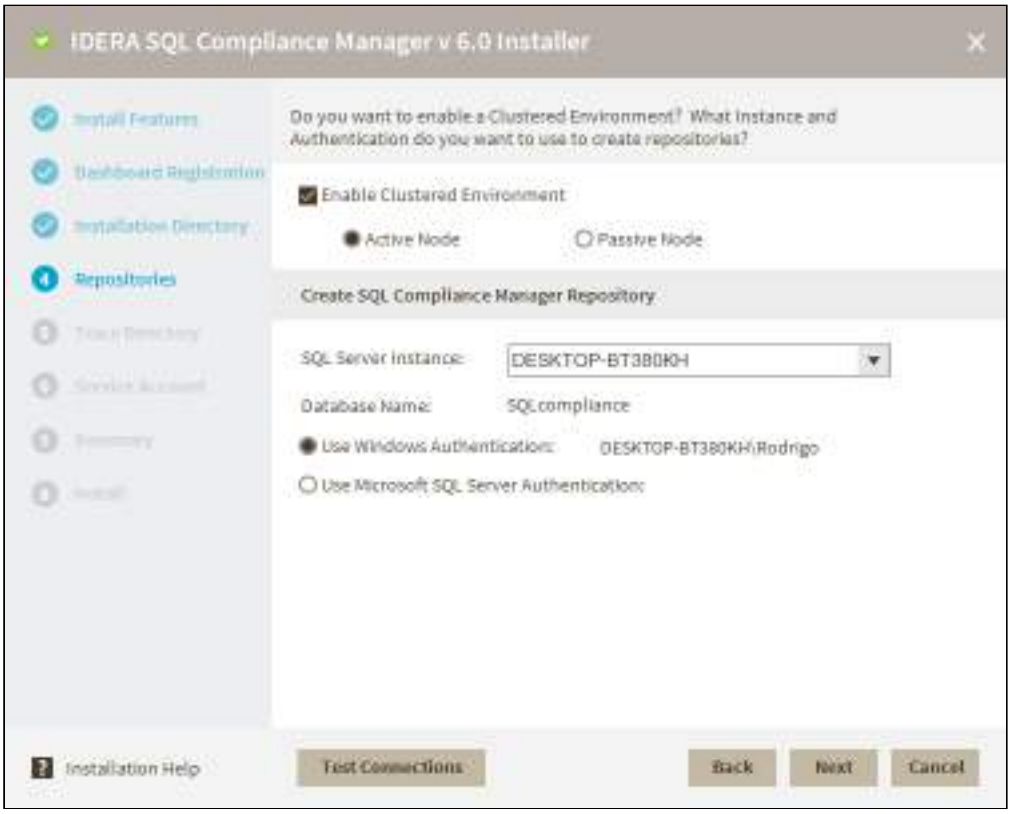
Installation Directory

1. Type in or browse the installation folder where you want to install SQL CM.
2. Type in a Display Name to be shown on the IDERA dashboard for the current installation.



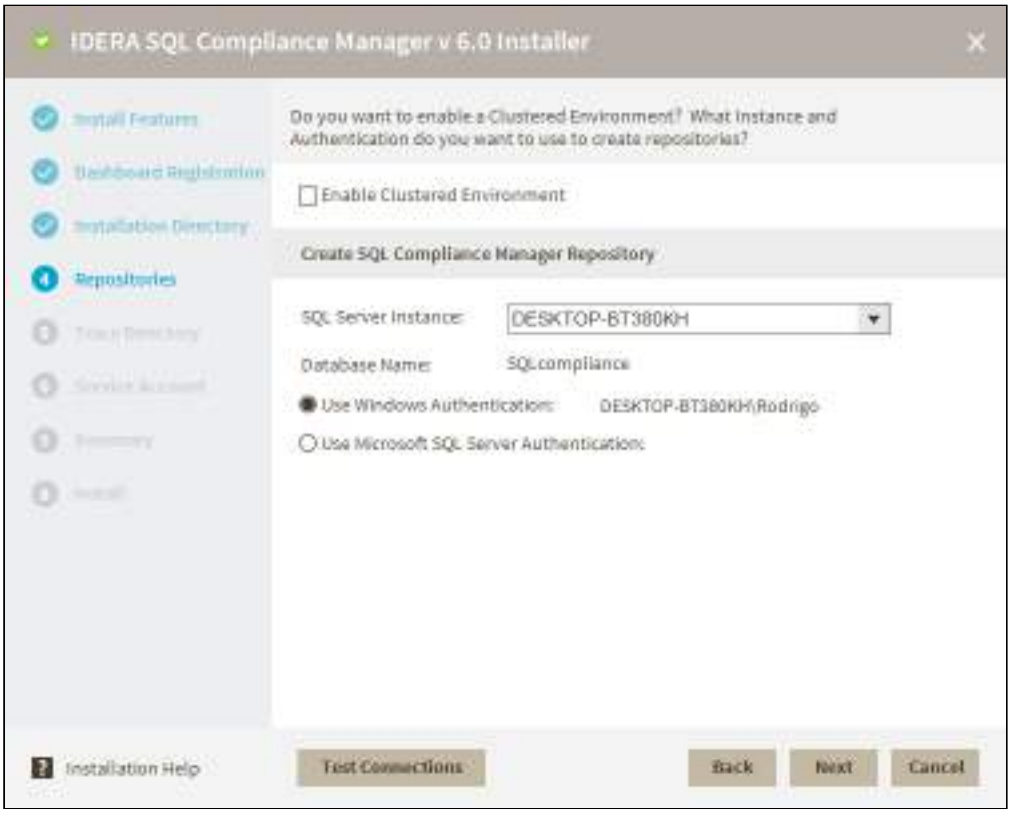
Repositories

If you want to enable a Clustered Environment. Select the checkbox and choose between an **Active Node** or a **Passive Node** to create your repositories.

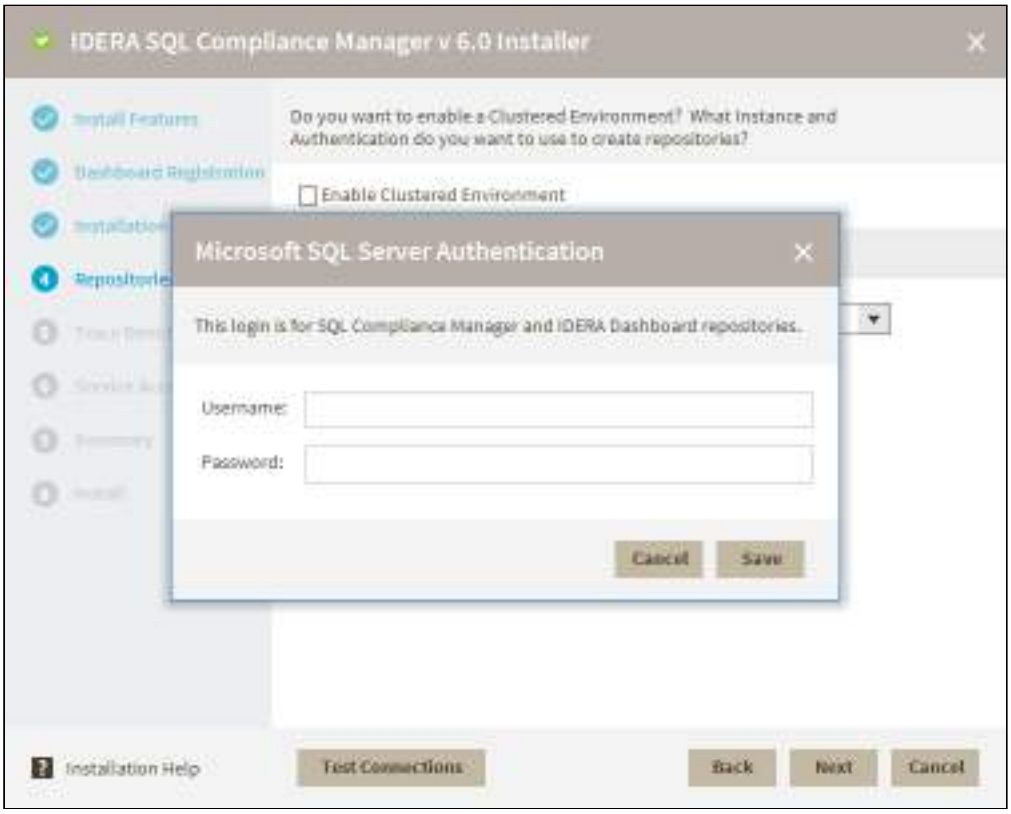


Create SQL Compliance Manager Repository

Select your SQL Server Instance from the drop-down menu.

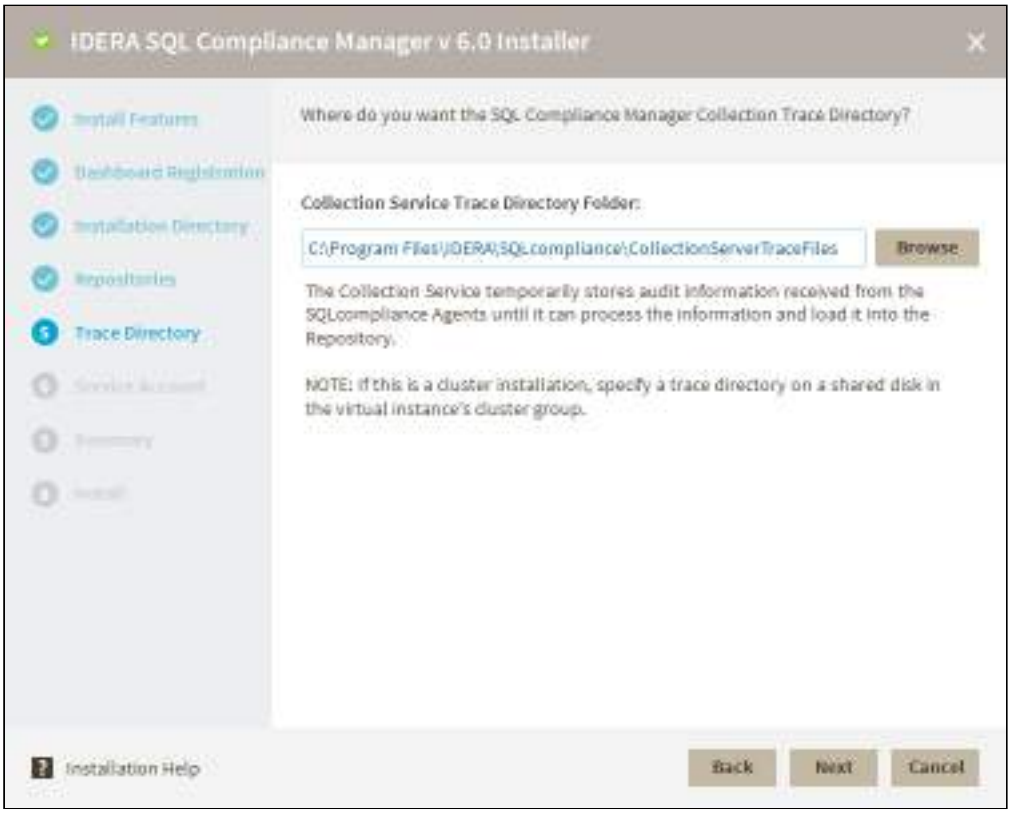


Select the authentication method. When selecting **Use Microsoft SQL Server Authentication,** a screen prompts you to add the Username and Password.



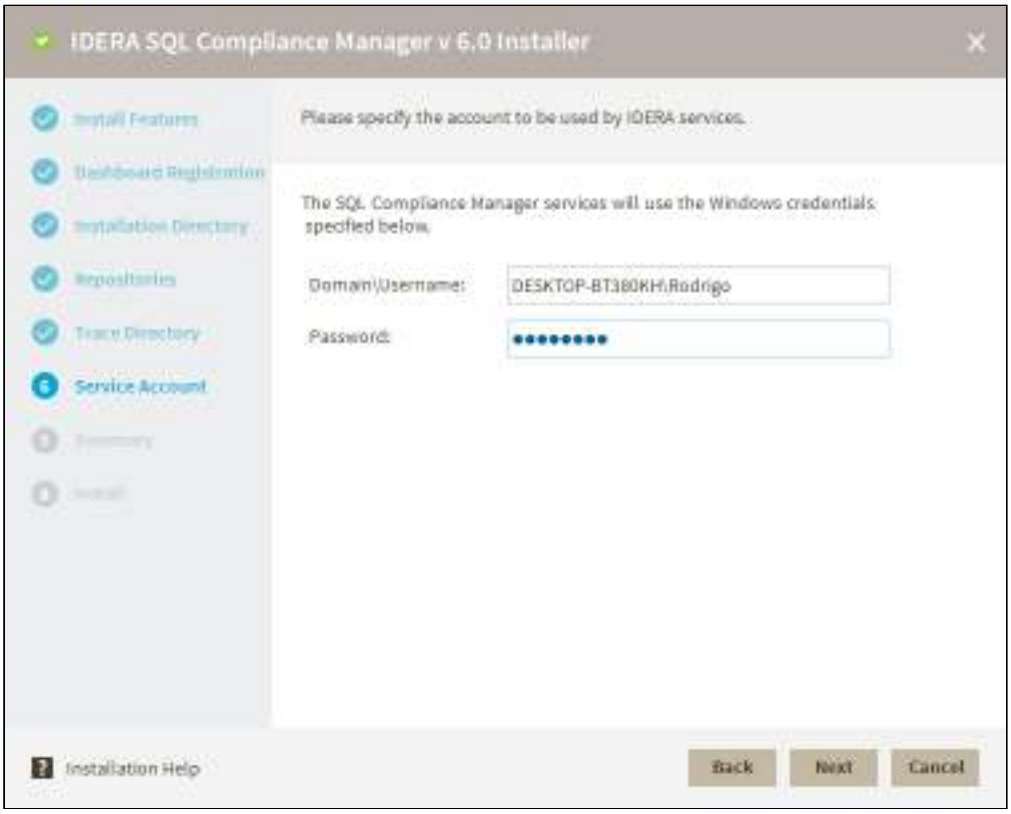
Trace Directory

Select where you want to store the audit information obtained with the **SQLCompliance Agents** before it processes the information and sends into the Repositories.



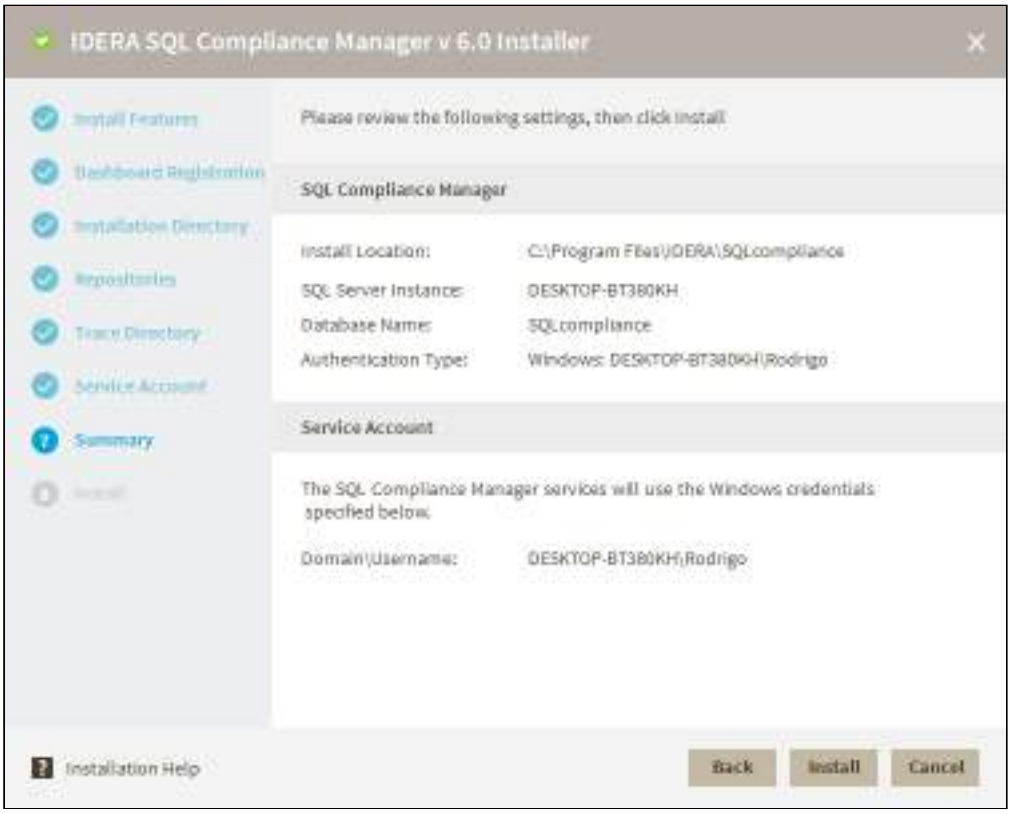
Service Account

Specify the account used for IDERA Services.



Summary

Review the stated parameters before the installation.



Press the **Install** button to start the installation.

> ⚠ The SQL Compliance Manager installer detects if the local machine has an older version of the SQL Server 2012 Native Client installed and if needed, SQL CM upgrades the Native Client to the latest version and proceeds with the installation. If no Native Client is installed on a server, then SQL CM installs the latest Native Client version and proceeds with the installation.

4.2.7 How to install SQL Compliance Manager and the IDERA Dashboard

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

> ⓘ IDERA SQL Compliance Manager versions 5.0 and newer only.

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

- Ensure you review the product 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.

This procedure guides you through the installation of SQL Compliance Manager and the IDERA Dashboard.

> ⚠ It is possible to install and use IDERA SQL Compliance Manager without installing the IDERA Dashboard. The IDERA Dashboard works as a complement of SQL Compliance Manager, allowing you to monitor SQL Server instances remotely.
> To learn more about this product, visit IDERA Dashboard.

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

Start your SQL Compliance Manager installation

You can install SQL Compliance Manager and the IDERA Dashboard on any computer that meets or exceeds the product requirements.

To install SQL Compliance Manager:

1. Log on with an administrator account to the computer on which you want to install SQL Compliance Manager.
2. Run `SQLCMInstall.EXE` in the root of the installation kit.
3. Review the information you need to start the installation and click **Next.**
4. Review and accept the license agreement by selecting the ***I accept the terms and conditions of the End User License Agreement*** checkbox.
   Select the appropriate setup type and then click **Next.**

Setup Type	Description
All SQL Compliance Manager components and IDERA Dashboard	Allows you to install all SQL Compliance Manager components and the IDERA Dashboard on this computer
SQL Compliance Manager Management console only	Allows you to install only the SQL Compliance Manager Management console
SQL Compliance Manager Agent only	Allows you to install only the SQL Compliance Manager Agent
IDERA Dashboard only	Allows you to install only the IDERA Dashboard

5. ***If you chose All SQL Compliance Manager components and IDERA Dashboard setup,*** complete the following procedure:
   a. Specify the following information and click **Next.**
      i. Location in which you want to install SQL Compliance Manager.
      ii. Display name for this installation.
      The IDERA Dashboard displays this name for the current installation. **The name can only contain letters, numbers, or hyphen - characters**.
      iii. Whether you want to install or upgrade the IDERA Dashboard locally or use a remote installation.
      If you chose to use a remote installation, you need to provide an existing IDERA Dashboard URL and Dashboard administrator credentials.
   b. Specify a SQL Server Instance and a form of authentication to create the SQL Compliance Manager and the IDERA Dashboard repositories.
   At this point, you can enable the **Clustered Environment** checkbox. If you select this option, you have to select whether you are working on an active or passive node and specify the same information mentioned above for the environment. For more information, see Deploying SQL

Compliance Manager in a Clustered Environment.
Test the connections to make sure the information is correct and click **Next.**

c. Specify where the SQL Compliance Manager Agent should store collected audit data, and click **Next**. The specified folder will be the trace file directory on the audited SQL Server instance.
d. Type the appropriate credentials in the provided fields under which IDERA services run, and click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
e. Review the installation settings and click **Install.**

6. ***If you chose the SQL Compliance Manager Console* setup**, complete the following procedure:
   a. Specify the location in which you want to install the console and click **Next.**
   b. Review the installation settings and click **Install.**
7. ***If you chose the SQL Compliance Manager Agent setup,*** complete the following procedure:
   a. Specify the location in which you want to install the console and click **Next.**
   b. Select a SQL Server instance to audit and the appropriate credentials. Click **Next.**
   c. Specify where the SQL Compliance Manager Agent should store collected audit data, and click **Next**. The specified folder will be the trace file directory on the audited SQL Server instance.
   d. Specify the SQL Server hosting the SQL Compliance Manager collection service and click **Next**.
   e. Review the installation settings and click **Install.**
8. ***If you chose the IDERA Dashboard setup***, complete the following procedure:
   a. Specify the location in which you want to install the IDERA Dashboard and click **Next.**
   b. Specify a SQL Server Instance and a form of authentication to create the IDERA Dashboard repository and click **Next.**
   c. Type the appropriate credentials in the provided fields under which IDERA services run, and then click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
   d. Review the installation settings and click **Install.**
9. ***If you chose the SQL Compliance Manager Agent and the IDERA Dashboard setup***, complete the following procedure:
   a. Specify the location in which you want to install the SQL Compliance Manager Agent and the IDERA Dashboard, then click **Next.**
   b. Specify a SQL Server Instance and a form of authentication to create the IDERA Dashboard repository and click **Next**.
   c. Type the appropriate credentials in the provided fields under which the IDERA services run, and then click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
   d. Specify where the SQL Compliance Manager 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.
   e. Specify the SQL Server hosting the SQL Compliance Manager collection service and click **Next.**
   f. Review the installation settings and click **Install.**
10. ***If you chose the SQL Compliance Manager Management Console and the IDERA Dashboard setup***, complete the following procedure:
    a. Specify the location in which you want to install the SQL Compliance Manager Console and the IDERA Dashboard, then click **Next.**
    b. Specify a SQL Server Instance and a form of authentication to create the IDERA Dashboard repository and click **Next**.
    c. Type the appropriate credentials in the provided fields under which IDERA services run, and then click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
    d. Review the installation settings and click **Install.**

> If you are installing SQL Compliance Manager's collection service on a repository running on SQL Server 2012 or below, the wizard will automatically install the necessary Microsoft components to finish the SQL Compliance Manager installation.
> For more information, see these important installation steps.

11. To launch SQL Compliance Manager**,** you can select the ***Launch the SQL Compliance Manager Windows Console*** checkbox.
    To access the IDERA Dashboard, open the URL provided in the completed installation window. Ensure to review Log in to IDERA Dashboard.

> If you want to install the SQL Compliance Manager Management Console and the SQL Compliance Manager Agent, you must install them together; otherwise, you will need to install the console with the installation wizard first, and then use the *SilentInstaller* to install the agent.
> For more information, see Perform a silent installation of the SQLCM Agent.

> The SQL Compliance Manager installer detects if the local machine has an older version of the SQL Server 2012 Native Client installed and if needed SQL CM upgrades the Native Client to the latest version and proceeds with the installation. If no Native Client is installed on the server, then SQL CM installs the latest Native Client version and proceeds with the installation.

> If you wish to uninstall the IDERA Dashboard, make sure to un-register all products by clicking the **Manage Products** link of the Products widget in the Administration view. For additional information, see Managing product registry in the IDERA Dashboard.

4.2.8 Perform a silent installation of the SQLCM Agent

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **versions 5.5.1 and later**.

For a fresh installation:

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" /qb+
```

Minor/Maintenance Upgrade (from 5.x to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Major upgrade (from 4.5 to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" AllUsers=1 /qb+
```

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **version 5.5**.

For a fresh installation:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" /qb+
```

For an upgrade:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Associated parameters include:

Parameter	Description
COLLECT_SERVER	The machine where the Collection server is installed and where you want to collect audited data.
INSTANCE	The SQL Server instance name where you want to install the Agent.
TRACE_DIRECTORY	The Agent trace file directory where you want to generate the trace files on the Agent server.
SERVICEUSERNAME	The Windows service account used to run the Agent service. This account must be local admin and have sa rights to the monitored SQL Server.
PASSWORD	The password for the service account.
STARTSERVICE	Denotes whether to start the service.

Parameter	Description
SILENT	Indicates to the installer that it is installed silently.
REINSTALL MODE	**Vamus,** indicates the type of reinstall to perform.
REINSTALL	**All,** instructs the installer to reinstall all pre-installed features.

The login and password must be encrypted strings. On IDERA SQL Compliance Manager 3.0 and later, you can encrypt the login and password using the encrypt command on the command line to get an encrypted version of the string that can then be used:

```
sqlcmcmd encrypt THESTRING
```

Note

Should the password contain the ¨^¨ special character, please consider enclosing the password string in between quotation marks, as shown below.
sqlcmcmd encrypt "THESTRING"
Also, note that this option would work if the password string does not contain double-quotes.

4.2.9 Log in to IDERA Dashboard

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

Once you have installed and configured your IDERA Dashboard and IDERA SQL Compliance Manager deployments, you can login to the IDERA Dashboard by doing the following:

1. Open your selected Browser and make sure it is compatible with the IDERA Dashboard console requirements.
2. Type the IDERA Dashboard product URL: **http://<machinename>:<port>** where **<machinename>** is the name of your host or machine, and **<port>** is the port specified during installation. The default URL is **http://<localhost>:9290** or **http://<machinename>:9290**.
3. When the IDERA Dashboard launches on your browser, use your Windows user account **<domain\user>** with the respective password to log into the product.

The IDERA Dashboard Web Application service comes with SSL already set up. For more information on running the IDERA Dashboard over SSL, see Run the Idera Dashboard over SSL (HTTPS)

4.3 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

4.3.1 Check the product version

You can check the IDERA SQL Compliance Manager version at any time. The product version consists of the release 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**.

4.3.2 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.

4.3.3 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. Close that window when done viewing.
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**.

4.3.4 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 consistently audited 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 consistently audited 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 are 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.

4.3.5 Manage the SQLcompliance Agent

The SQL Compliance Manager 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 SQL Compliance Manager Agent to each SQL Server computer that hosts the instances and databases you want to audit.

- How the SQL Compliance Manager Agent works
- SQL Compliance Manager Agent version compatibility
- Deploy the SQL Compliance Manager Agent manually
- Deploy the SQL Compliance Manager Agent remotely
- Upgrade the SQL Compliance Manager Agent locally
- Upgrade the SQL Compliance Manager Agent remotely
- Ensure the SQL Compliance Manager Agent has current audit settings
- Check trace file integrity
- Check the SQL Compliance Manager Agent status
- Check the SQL Compliance Manager Agent version
- Configure how the SQL Compliance Manager Agent manages trace files
- How the SQL Compliance Manager Cloud Agent works

How the SQL Compliance Manager Agent works

The SQL Compliance Manager Agent runs under the SQL Compliance Manager Agent Service account on each registered SQL Server computer that hosts the audited instances and databases. To audit events, the SQL Compliance Manager Agent starts SQL Server traces that run on the target SQL Server. Once a trace starts, SQL Compliance Manager 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 SQL Compliance Manager Agent compresses the trace files and sends them to the Collection Server. After a trace file is successfully sent, the SQL Compliance Manager Agent deletes the file.

You can configure how the SQL Compliance Manager 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 SQL Compliance Manager Agent stops the SQL trace until the existing trace files can be sent to the Collection Server.

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

> **Note**
>
> During the heartbeat, the Collection Service requests a list of the Database Names and ID´s in order to update the table stored in the event database.

If the SQL Compliance Manager Agent continues to run without a heartbeat, IDERA 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 SQL Compliance Manager Agent is not responding or is deleted.

When you deploy the SQL Compliance Manager Agent, SQLcompliance installs the SQL Compliance Manager 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.

SQL Compliance Manager Agent version compatibility

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

Deploy the SQL Compliance Manager Agent manually

To deploy the SQL Compliance Manager Agent manually, run an 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 SQL Compliance Manager 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 SQL Compliance Manager Agent on each cluster node hosting the server. For more information about installing and configuring the SQL Compliance Manager Agent for a virtual SQL Server, see Deploy the SQL Compliance Manager Agent to cluster nodes.

Perform a silent installation

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **versions 5.5.1 and later**.

For a fresh installation:

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
```

```
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" /qb+
```

Minor/Maintenance Upgrade (from 5.x to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Major upgrade (from 4.5 to this version):

```
msiexec /i "\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" AllUsers=1 /qb+
```

Use the following commands to perform a silent installation or upgrade the IDERA SQL Compliance Manager Agent for **version 5.5**.

For a fresh installation:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" /qb+
```

For an upgrade:

```
msiexec /i "<Path_to_Agent_MSI>\SQLcomplianceAgent-x64.msi" /l*v InstallAgent.log
COLLECT_SERVER="IderaCollectionServerName" INSTANCE="AgentSQLServerInstanceName"
TRACE_DIRECTORY="C:\Program Files\Idera\SQLcompliance\AgentTraceFiles"
SERVICEUSERNAME="Domain\Username" PASSWORD="!mySec@tP@55w0rD" STARTSERVICE="TRUE"
SILENT="1" REINSTALLMODE=vamus REINSTALL=All AllUsers=1 /qb+
```

Associated parameters include:

Parameter	Description
COLLECT_SERVER	The machine where the Collection server is installed and where you want to collect audited data.
INSTANCE	The SQL Server instance name where you want to install the Agent.

Parameter	Description
TRACE_DIRECTORY	The Agent trace file directory where you want to generate the trace files on the Agent server.
SERVICEUSERNAME	The Windows service account used to run the Agent service. This account must be local admin and have sa rights to the monitored SQL Server.
PASSWORD	The password for the service account.
STARTSERVICE	Denotes whether to start the service.
SILENT	Indicates to the installer that it is installed silently.
REINSTALL MODE	**Vamus,** indicates the type of reinstall to perform.
REINSTALL	**All,** instructs the installer to reinstall all pre-installed features.

The login and password must be encrypted strings. On IDERA SQL Compliance Manager 3.0 and later, you can encrypt the login and password using the encrypt command on the command line to get an encrypted version of the string that can then be used:

```
sqlcmcmd encrypt THESTRING
```

Note

Should the password contain the ¨^¨ special character, please consider enclosing the password string in between quotation marks, as shown below.
sqlcmcmd encrypt "THESTRING"
Also, note that this option would work if the password string does not contain double-quotes.

Deploy the SQL Compliance Manager Agent remotely

You can deploy the SQL Compliance Manager 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 SQL Compliance Manager Agent for a virtual SQL Server, see Deploy the SQL Compliance Manager Agent to cluster nodes.

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 SQL Compliance Manager Agent to the host computer using the IDERA SQL Compliance Manager setup program.

To deploy the SQL Compliance Manager 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 SQL Compliance Manager Agent.
3. Select **Deploy Agent** from the context menu.
4. Type and confirm the account name and password. You want the SQL Compliance Manager 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 SQL Compliance Manager Agent.

Upgrade the SQL Compliance Manager Agent locally

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

Upgrade the SQL Compliance Manager Agent remotely

You can upgrade the SQL Compliance Manager 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 SQL Compliance Manager Agent, use the IDERA SQL Compliance Manager setup program to manually upgrade the agent. For more information, see Upgrade the SQL Compliance Manager Agent locally.

To upgrade the SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent has current audit settings

You can ensure the SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent manages the SQL trace that collects audit data. ***If the SQL trace is stopped, modified, paused, or deleted by another application***, the SQL Compliance Manager 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 SQL Compliance Manager Agent Properties window. For more information, see Configure how the SQL Compliance Manager 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 SQL Compliance Manager Agent started a new trace.
Trace altered	A SQL trace setting was altered.

Check the SQL Compliance Manager Agent status

You can quickly check the status of a SQL Compliance Manager 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 SQL Compliance Manager Agent status:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQL Compliance Manager Agent you want to check.
3. Click **Check Agent Status** 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 SQL Compliance Manager Agent version

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

To check the SQL Compliance Manager Agent status:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQL Compliance Manager Agent you want to check.
3. On the Agent menu, click **Agent Properties**.
4. On the General tab, review the SQL Compliance Manager 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 SQL Compliance Manager Agent manages trace files

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

If you specify a different location for the trace directory, ensure the SQL Compliance Manager Agent Service account has read and write privileges on that folder. IDERA 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 Compliance Manager applies this change to the active node in the cluster hosting the virtual SQL Server. SQL Compliance Manager Agent properties are later replicated from the active node to the passive nodes.

To configure how the SQL Compliance Manager Agent manages trace files:

1. Navigate to **Registered SQL Servers** in the **Administration** tree.
2. Select the SQL Server instance that hosts the SQL Compliance Manager 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 is stopped, modified, paused, or deleted	Trace Options
Verify agent service account	Deployment

4. ***If you want to designate a different folder for the SQL Compliance Manager 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**.

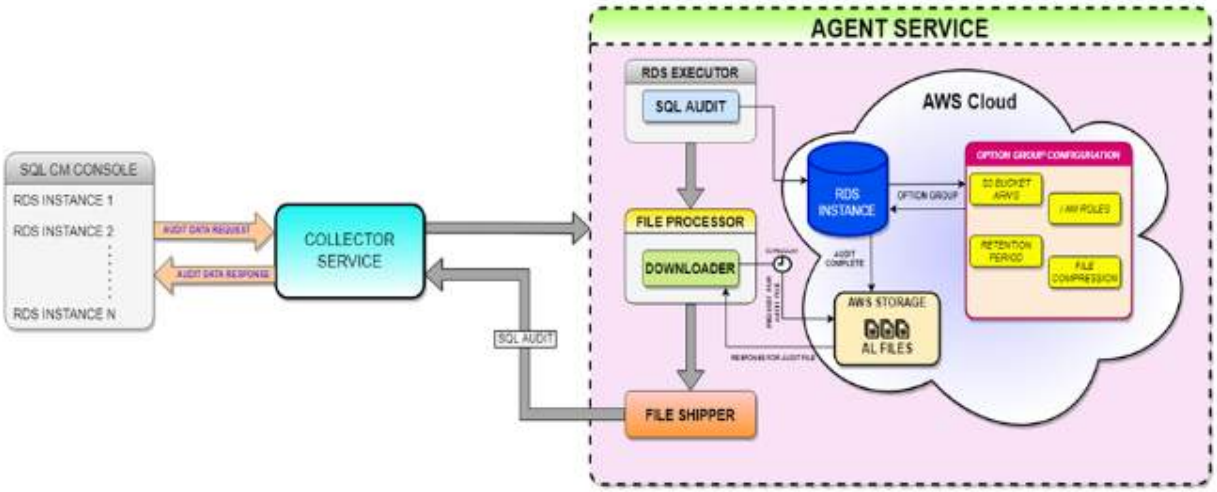
How the SQL Compliance Manager Cloud Agent works

SQL Compliance Manager offers an improved architecture that allows registering cloud instances with its new Cloud Agent Service. The SQL Compliance Manager Cloud Agent runs under the SQL Compliance Manager Agent Service account on each registered SQL Server computer that hosts the audited instances and databases inside the AWS Cloud. The Cloud Agent gathers SQL events logs from audited SQL Server on cloud instances and databases and then sends the raw data to the Collection Server.

Architecture

Once a cloud instance is registered to audit events, the Collector service receives the audit data request from your registered cloud instance and invokes the Cloud Agent Service to start auditing your cloud instance.

The audited cloud instance is based on the Option Group and S3 bucket Configuration, and after audit completion, the cloud instance transmits the audit file to the AWS S3 bucket. Then, the File processor downloads the new **.sqlaudit* file from the AWS S3 bucket parses the file and transfers it to the File Shipper. Finally, the SQL Audited files are transferred to the Collector Service, where the files are processed, and the data is updated in the SQL Compliance repository.



Pre-Requisites

The following access and permissions are required on AWS RDS in the AWS console before registering an RDS instance through the SQL CM Console.

- Access to an AWS Account
- Permission to create a directory service for RDS (if RDS is registered using windows auth).
- Permission to create Microsoft AD Windows authentication (if RDS is registered using windows auth).
- Permission to configure and add permissions to the IAM role in RDS.
- Permission to create Option Group and lists of S3 buckets.

Create an Option Group

An *Option Group* specifies features called options that are available in your registered Amazon RDS DB instance. Options can have settings that specify how the option works. When you associate a DB instance with an Option Group, the specified options, and option settings are enabled for that DB instance.

Configure your Option Group by using the SQLcm Configuration Wizard for the Agent RDS configuration, or create an option group by using the AWS Management Console.

Create an Option Group from the AWS console

Login to your AWS account and follow the steps below:

1. In the main navigation pane, select the **Options groups** from the sidebar menu.
2. In the Create option group window, fill out the Option group details and click **Create**.
   - **Name** - the name of the option group.
   - **Description** - a brief description of the option group.

   - **Engine type** - choose the DB engine that you want.
   - **Major engine version** - choose the major version of the DB engine that you want.
3. Next, select the created Option Group and select **Add option**.
4. In the S3 destination section, fill out the required S3 Bucket information.
5. Next, choose the **Create a New Role** option, and provide a name for the IAM role.
   a. Make sure to check the permissions policies for the IAM role.
6. In the Additional configuration section, make sure to enable the **compression** and **retention** options.
7. Select the **Database** option from the sidebar menu, and in the Database options section, select the recently created option group from the Option group dropdown menu.
8. Finally, in the Manage IAM roles section, select the role for the instance.

Important notes on RDS auditing

- RDS does not support the Middle East (Bahrain) region and works only with SQL Server versions 2012 and above.
- The Max File Size for SQL Audit on the RDS instance limit is 50 MB.
- Before and After Data is not supported on the RDS instance due to the limitation of creating trusted assemblies using sql script. BAD operations are removed from the properties, reports, alerts, and summary tabs.

4.3.6 Licensing

IDERA 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 Compliance Manager architecture.

How licensing works

By default, IDERA 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 Compliance Manager 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 Compliance Manager associates the instance with an available license. ***If the attempted registration exceeds your licensed limit***, SQL Compliance Manager 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 Compliance Manager 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 IDERA SQL Compliance Manager 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**.

4.3.7 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 SQL Compliance Manager Agent to begin auditing SQL events on this instance.

Use the Console to register your SQL Servers

To register your SQL Server instance:

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 Compliance Manager 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 SQL Compliance Manager Agent now or later, and then click **Next**. You can also choose to deploy the SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 Compliance Manager 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 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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 SQL Compliance Manager 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"`.

> If there are any backlogged audit trace files that you need to process for the instance you are considering to decommission, make sure to disable auditing and decommissioning your server only after processing these backlogged audit trace files. For additional information on how to process backlogged trace files, please contact Idera Support.

4.3.8 Manage the registry key

IDERA 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 SQL Compliance Manager 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 SQL Compliance Manager 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.

4.4 Index rebuild operation

The online index rebuild operation is an application that upgrades indexes in the background and converts them from a none compression state into a page level compression type. This operation updates indexes on the Events table in the databases on each of the monitored instance to become a page compressed type. This index upgrade shows considerable performance advantages and optimizes performance when viewing and managing event data.

The following 7 Indexes are included in the Events table of a monitored instance being audited:

- IX_Events_eventId
- IX_Events_eventCategory
- IX_Events_eventType
- IX_Events_databaseId
- IX_Events_appNameId
- IX_Events_hostId
- IX_Events_loginId

The operation is performed as an ONLINE operation (only for supported SQL Server versions) keeping the database table(s) available for users. The application checks the SQL Server version and then checks if the index compression type is set to page or none. based on the compression type, it performs the Index upgrade query which is set to be an ONLINE operation for any compression type to page compression type. The operation then runs and converts the 7 indexes of the event databases (for each instance added for auditing) to be page compressed. For environments with large repositories, the index rebuilds can take a significant amount of time. If you need to defer the rebuild, the SQL Compliance Manager update process will proceed without rebuilding the indexes and you can choose to do so at a later. For new instances, the page compressed type indexes is created by default.

> The index upgrade operation is skipped if the compression type is already set to page compression type.

4.4.1 Running the Index rebuild operation manually

Several SQL Servers editions (such as the STANDARD edition), do not support the index rebuild operation to be performed in an ONLINE state. Therefore the operation results in a failure message displayed to the user instructing them to run the application manually without the ONLINE property.

Before updating the indexes, please ensure that the selected database has sufficient free space to accommodate these changes. For example, if the current size of your database is 1MB, the updated database may grow to 2MB. In this case, the update process would require 1MB of free space.

Users are able to run the utility manually with additional parameters in order to rebuild the indexes without the ONLINE option as follows:

<installdir>\SQLcomplianceIndexUpgrade.exe "server=serverName; database=SQLcompliance; integrated security=SSPI; Connect Timeout=30;" "ONLINE=OFF"

The second parameter "**ONLINE=OFF**" is an optional parameter and is meant to be used only when the index update operation cannot be performed with the ONLINE option.

⚠ This operation should only be done during a downtime, since the index creation will acquire a lock on the Events table and the auditing will not work in that duration.

⚠ When the utility is running manually the Index rebuild operation does not occur as an ONLINE operation.

5 Navigate the IDERA Dashboard Web Console

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard is a common technology framework designed to support the entire IDERA product suite. The IDERA Dashboard allows users to get an overview of the status of their SQL Server instances and hosted databases all in a consolidated view, while providing users the means to drill in to individual product overviews for details. The IDERA Dashboard supports multiple copies of each product installation.

5.1 IDERA Dashboard menu bar

In the IDERA Dashboard menu bar, you can perform the following actions:

- Select the product content you want to view through the **Product** menu.
- Access administration tasks through the **Admin** menu.
- Access to a number of assistance topics through the **Help** menu.

5.1.1 Product menu

The Product menu allows you to quickly toggle between all of your installed IDERA products. You can customize the default order of your products in the Product menu by selecting the **Customize** option from the drop-down list and then clicking, holding, and dragging the product labels to the desired order. After selecting the order, click **Save** to save the changes.

If the product list is long, the IDERA Dashboard displays the option **More** at the bottom of the menu. Click **More** to expand the next products in the list.

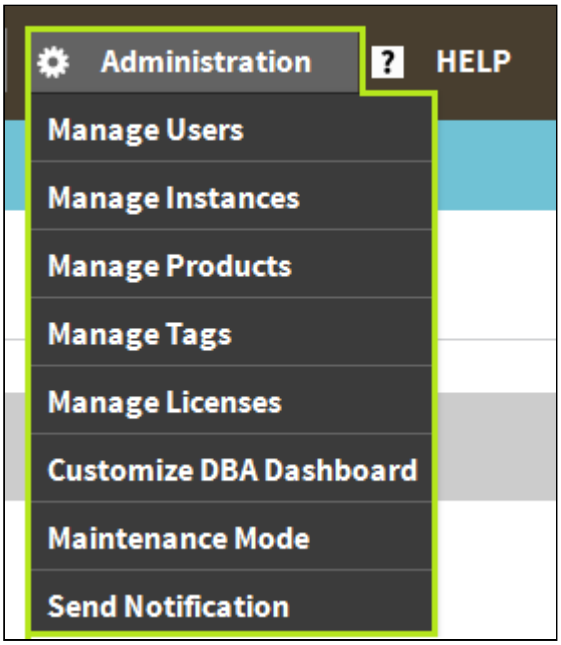
5.1.2 Welcome user

The user menu, which displays **<domain\username>**, allows you to manage the user account (if the user has the Product Administrator role) and log out of the IDERA Dashboard session. Click **Manage Accounts** to display the Manage Users view with the current user account selected and the details displayed in the User/Group Details pane.

5.1.3 Administration menu

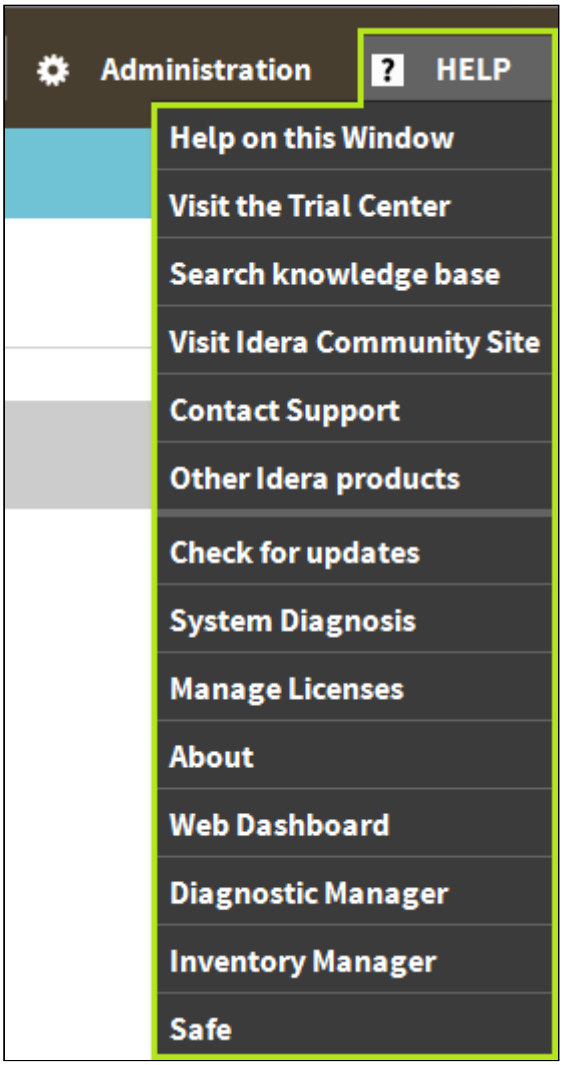
The **Administration** menu provides a list of shortcuts to the views available on the Administration tab.

If a menu item is displayed but disabled, the current user account **does not have** the permission necessary to perform the associated function.



5.1.4 Help menu

The Help menu provides links to helpful areas such as the IDERA Knowledge Base or the IDERA Customer Support.



5.2 IDERA Dashboard Tabs

The IDERA Dashboard is comprised of the following tabs:

- Overview
- Details View
- Alerts
- Administration

5.3 Overview tab

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard Overview provides an area for users to quickly view top metrics regarding their monitored SQL Server instances.

By default, the following IDERA SQL Compliance Manager widget appears on the IDERA Dashboard Overview:

- SQL Compliance Manager Environment Alerts
- SQL Compliance Manager Enterprise Activity Report Card
- SQL Compliance Manager Audited Instances

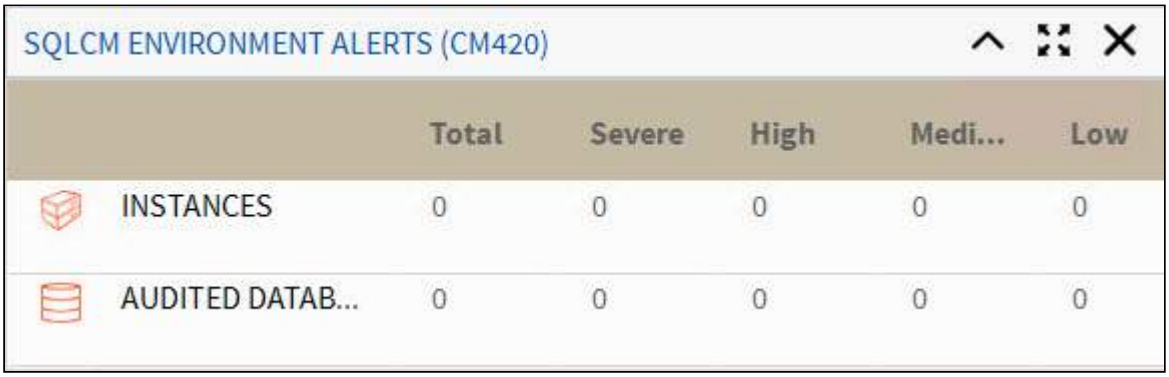
In the Overview tab, you can perform the following actions:

- Expand or collapse a widget .
- View a widget in full size .
- Remove a widget .
- Filter widget information by Products and by Tags.

5.3.1 SQL Compliance Manager Environment Alerts widget

The SQL Compliance Manager Environment Alerts widget displays the number of active alerts for the entire environment with Severe, High, Medium, or Low status along with the:

- Total number of audited *instances* in your environment. Click **Instances** to access the Audited Instances view within SQL Compliance Manager.
- Total number of audited *databases* in your environment. Click **Audited Databases** icon to access the Audited Databases view within SQL Compliance Manager.



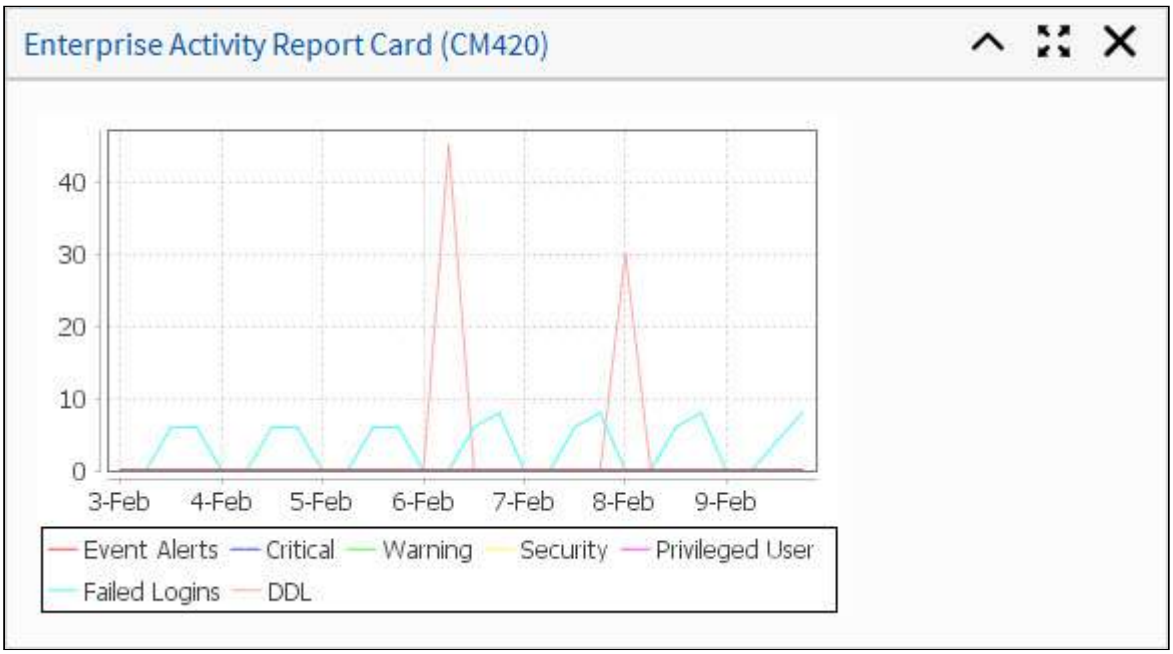
5.3.2 SQL Compliance Manager Enterprise Activity Report Card

The SQL Compliance Manager Enterprise Activity Report Card widget displays your SQL Compliance Manager enterprise activity in a line graph based on the Overall Activity graph on the SQL Compliance Manager Enterprise Activity report Card. This graph displays activity for the past seven days and includes:

- Critical Alerts
- DDL
- Event Alerts
- Failed Logins

- Privileged User
- Security
- Warning Alerts

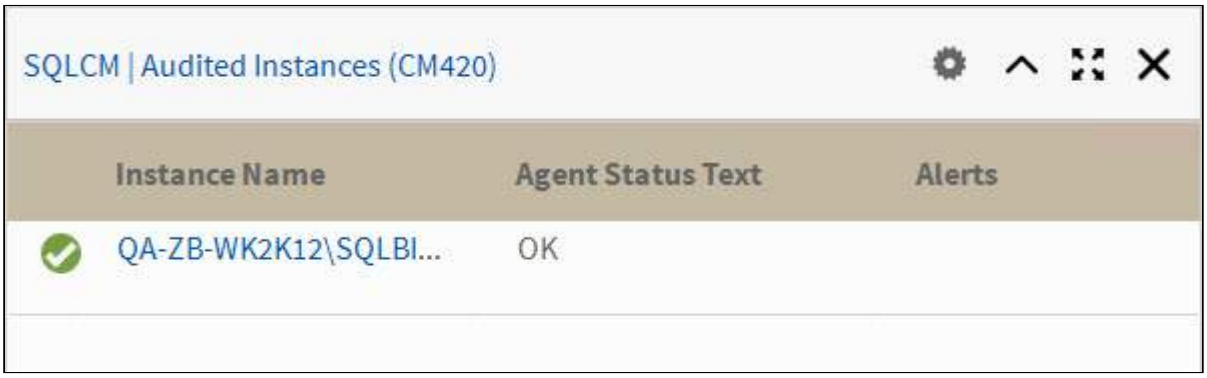
For more information about the Enterprise Activity report Card, see Explore Activity - Audited SQL Servers Summary tab.



5.3.3 SQL Compliance Manager Audited Instances

The SQL Compliance Manager Audited Instances widget displays a list of audited SQL Server instances. This widget includes:

- Status icon: green check for okay (successful connection and the SQL Server Agent is running) or red x for error (instance connection failed or the SQL server Agent is not running)
- Instance name
- Agent Status text
- Any available alerts
- Number of audited databases per instance (scroll right if not available)



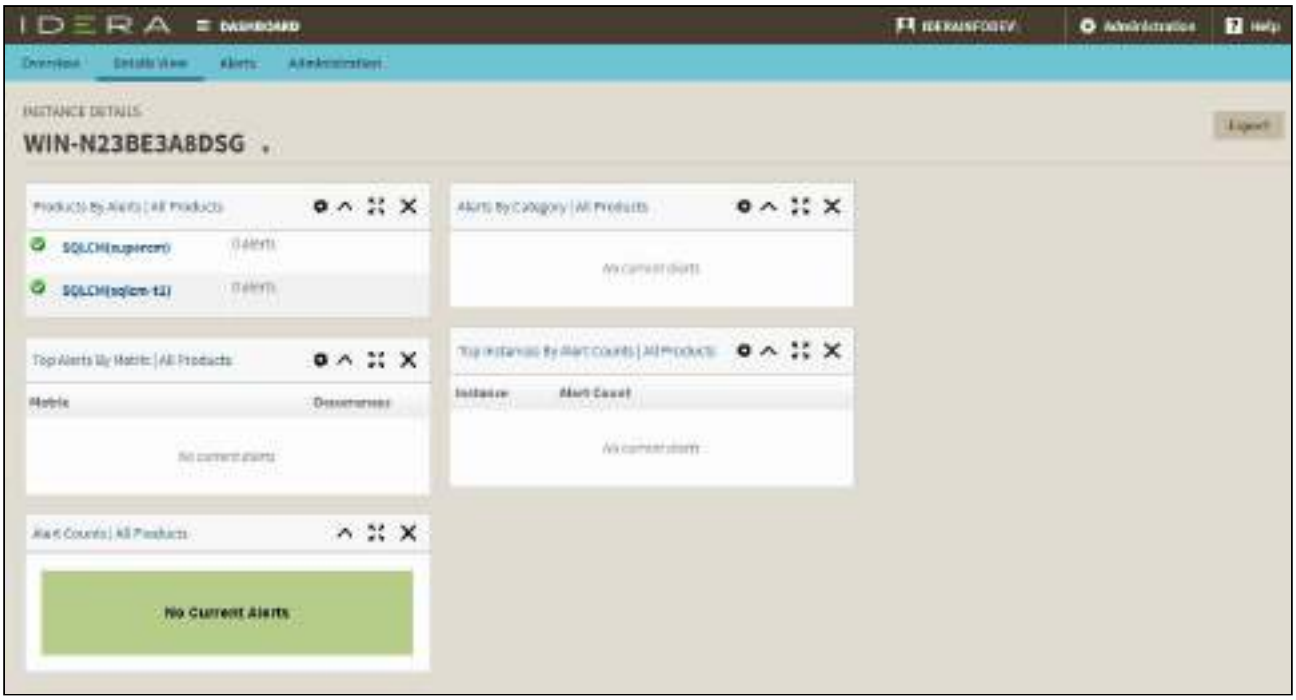
5.4 Details View tab

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

In the IDERA Dashboard Details view tab, users can select specific metrics to display. This tab contains product widgets of all the products registered with the IDERA Dashboard.

By default, the Details view tab contains the following widgets:

- Products by Alerts (All Products).
- Alerts by Category (All Products).
- Top Alerts by Metric (All Products).
- Alerts by Counts (All Products).
- Top Instances by Alert Count.
- Top Instances by CPU Usage.
- Top Databases by Alert Counts.
- Alert Counts by Category.



In the Details tab, you can perform the following actions:

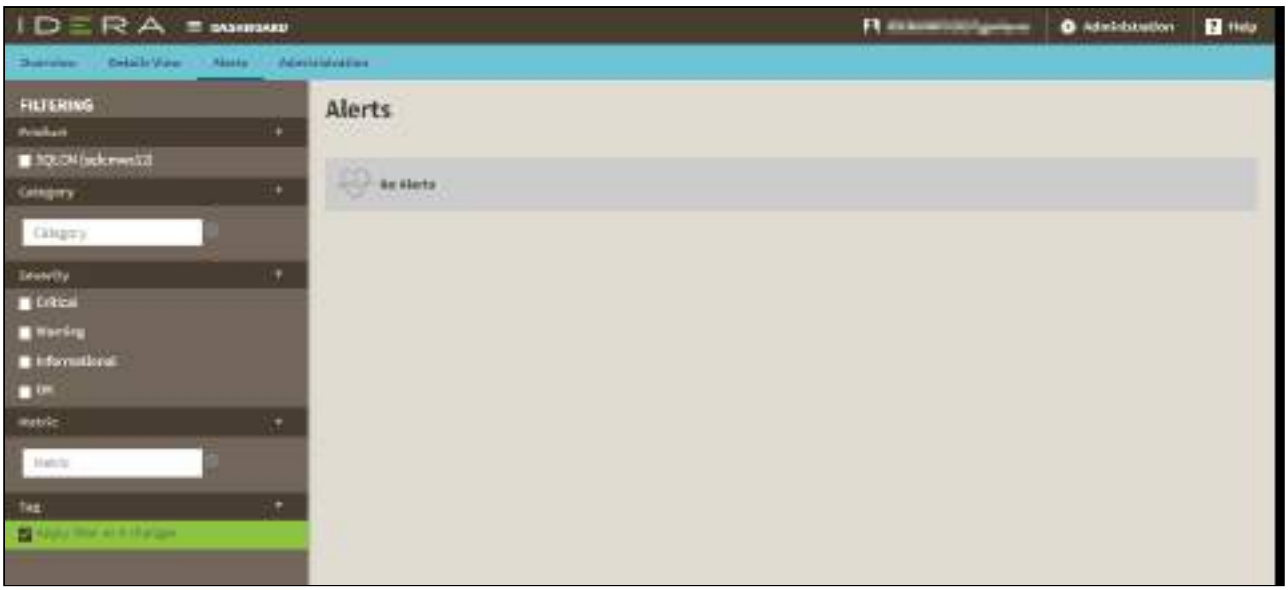
- Expand or collapse a widget ^ .
- View a widget in full size ⛶ .
- Remove a widget ✕ .
- Filter widget information.

5.5 Alerts tab

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard Alerts view displays any alerts generated by the monitored SQL Server instances in your environment. You can filter by:

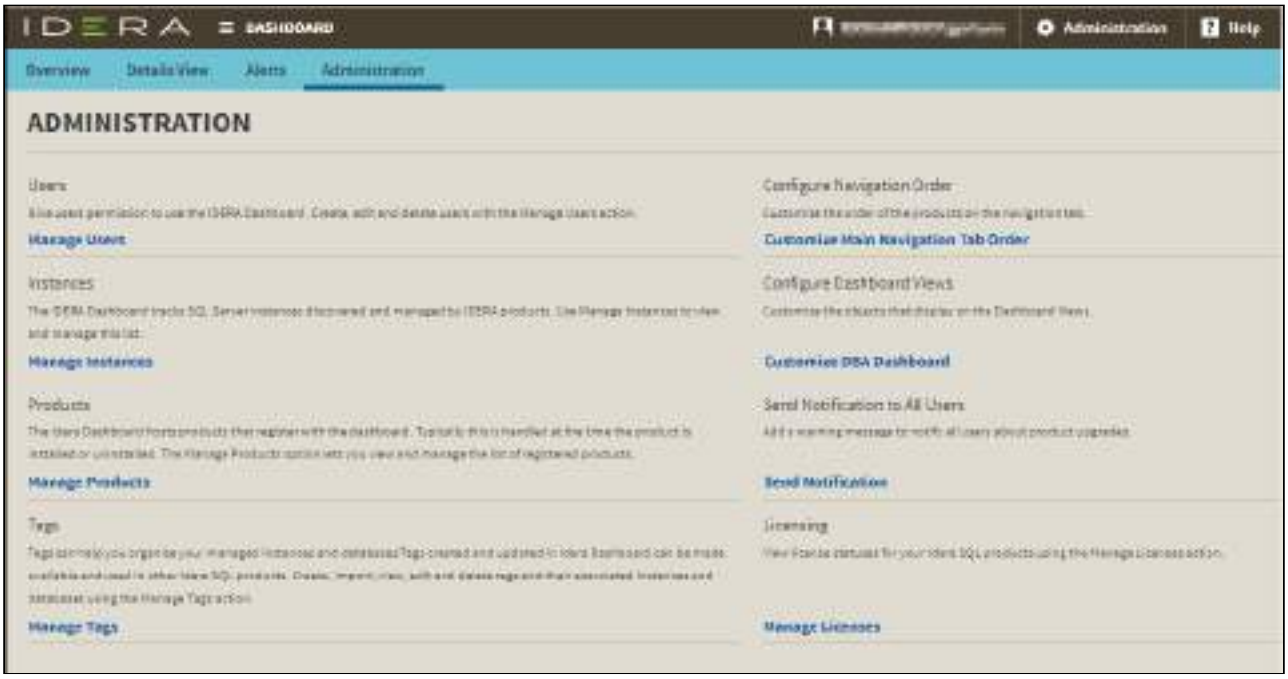
- **Product**. Select one or more of your installed IDERA products to view generated alerts.
- **Category**. Add category filters to view alerts associated with a specific type.
- **Severity**. Select one or more severities to view alerts corresponding to those levels. Options include Critical, Warning, Info, and OK.
- **Metric**. Add metric filters to view alerts associated with a specific metric.
- **Tag**. Filter alerts based on your created tags.



5.6 Administration tab

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

In the IDERA Dashboard, all products show a common Administration tab, granted the logged-in user has administrator privileges. Selecting this tab displays the Administration view which hosts a range of options for performing administration-related actions.



5.6.1 Available actions in the Administration view of the IDERA Dashboard

The Administration view of the IDERA Dashboard provides a central set of services related to specific actions such as:

- User management
- Instance management
- Product registry
- Manage Tags
- Configure navigation order
- Configure Dashboard Views
- Product notification management
- Manage Licenses

For more information on each service and what configuration settings are available, visit each respective section.

5.6.2 Managing users in the IDERA Dashboard

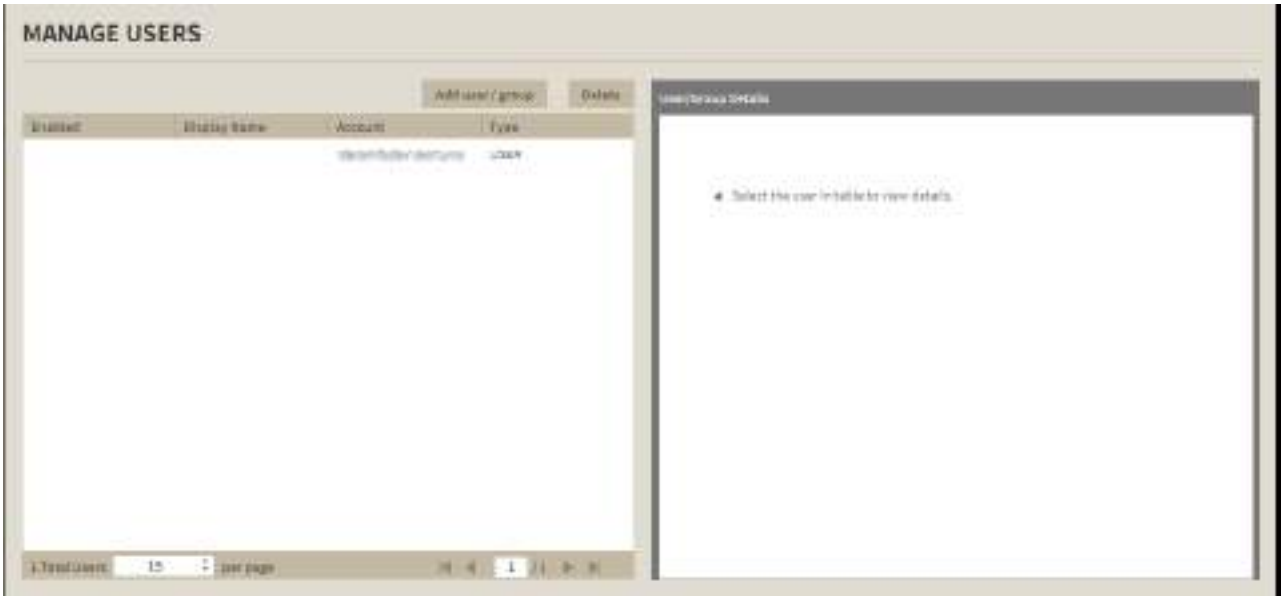
⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The Users section of the IDERA Dashboard Administration view allows users to grant access to other team members or groups, and manage their roles. For more information about user roles, see Understanding user roles . Users with administrative privileges are divided into two groups:

- The IDERA Dashboard Roles
  - **Dashboard Administrator:** Allows the user to manage access over Dashboard functions as well as individual product functions.
  - **Dashboard Guest:** Grants the user read-only access to the Dashboard and all installed products.
- Product Roles
  - **Product Administrator:** Allows the user to grant access to individual products for which they have administrative rights.
  - **Product Guest:** Grants the user read-only access to the installed products. This role has no administrative functions.
  - **Product User:** Allows the user to read and modify access to the installed products and limited administrative functions.

Users must be existing **Active Directory users**. Newly-added users should use their Windows user account with their respective passwords to log in to the SQL Compliance Manager.

To add new users, edit their details (name, subscription, or email address), or remove them, select **Manage Users** in the Administration view, and the Manage Users window displays:

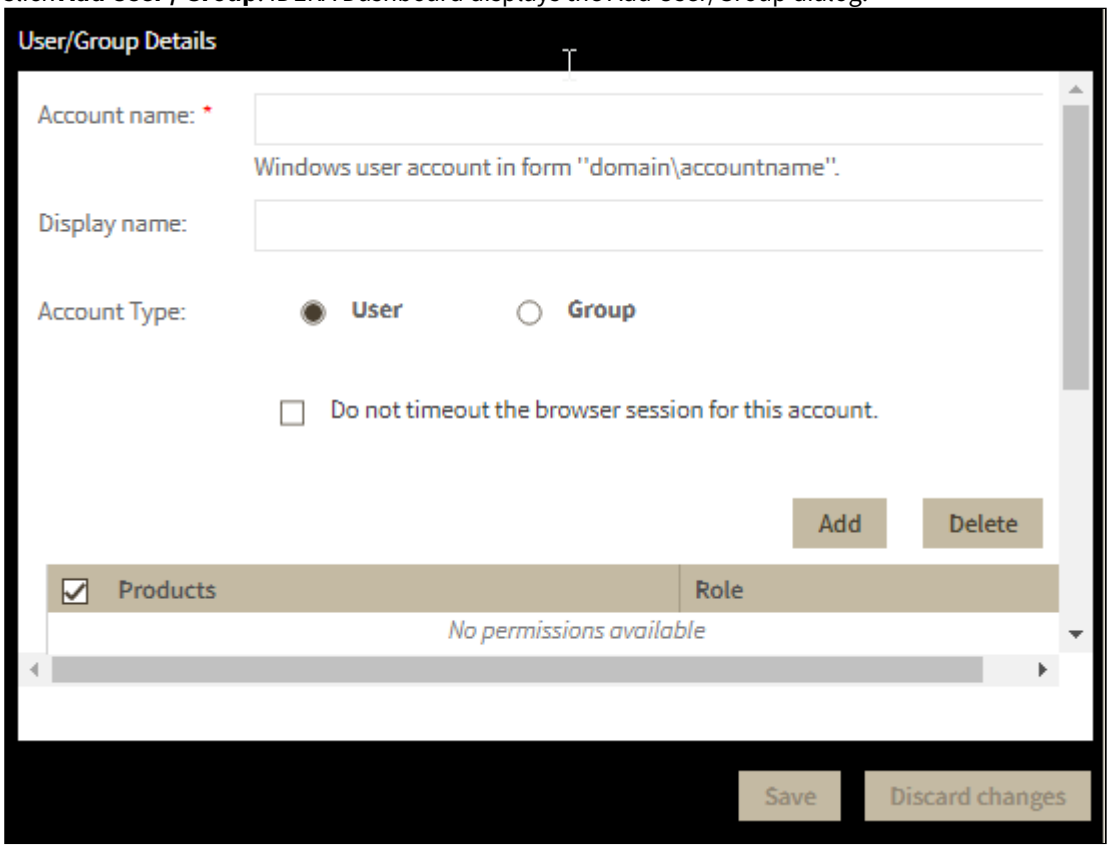


Adding a user in the IDERA Dashboard

In the IDERA Dashboard, access is granted to Windows users or groups.

To add a user account:

1. Click **Add User / Group**. IDERA Dashboard displays the Add User/Group dialog.



2. Type the name of the user to which you want to grant access. Enter a Windows user name in the format <*domain\accountname*>.
3. *Optional*. In **Display name**, type a name for the user account that you want SQL Compliance Manager to display within the product.
4. In the **Account Type** field, select **User** or **Group**.
5. *Optional*. Check **Do not timeout the browser session for this account** if you want the user to be able to remain logged in to SQL Compliance Manager after a period of inactivity.
6. Click **Add.** The IDERA Dashboard displays the *Add Permission* window.
7. In the **Product** field, select the product name to which you want to add this new user account.
   If you select IDERA Dashboard in the Product field , the **Role** field allows you to select from the Dashboard Administrator and Dashboard Guest roles.
   If you select SQL Compliance Manager in the Product field , the **Role** field allows you to select from the Product Administrator, Product User, and Product Guest roles.
8. In the **Role** field, select the role you want to assign to this new user account.
9. Click **Save**.

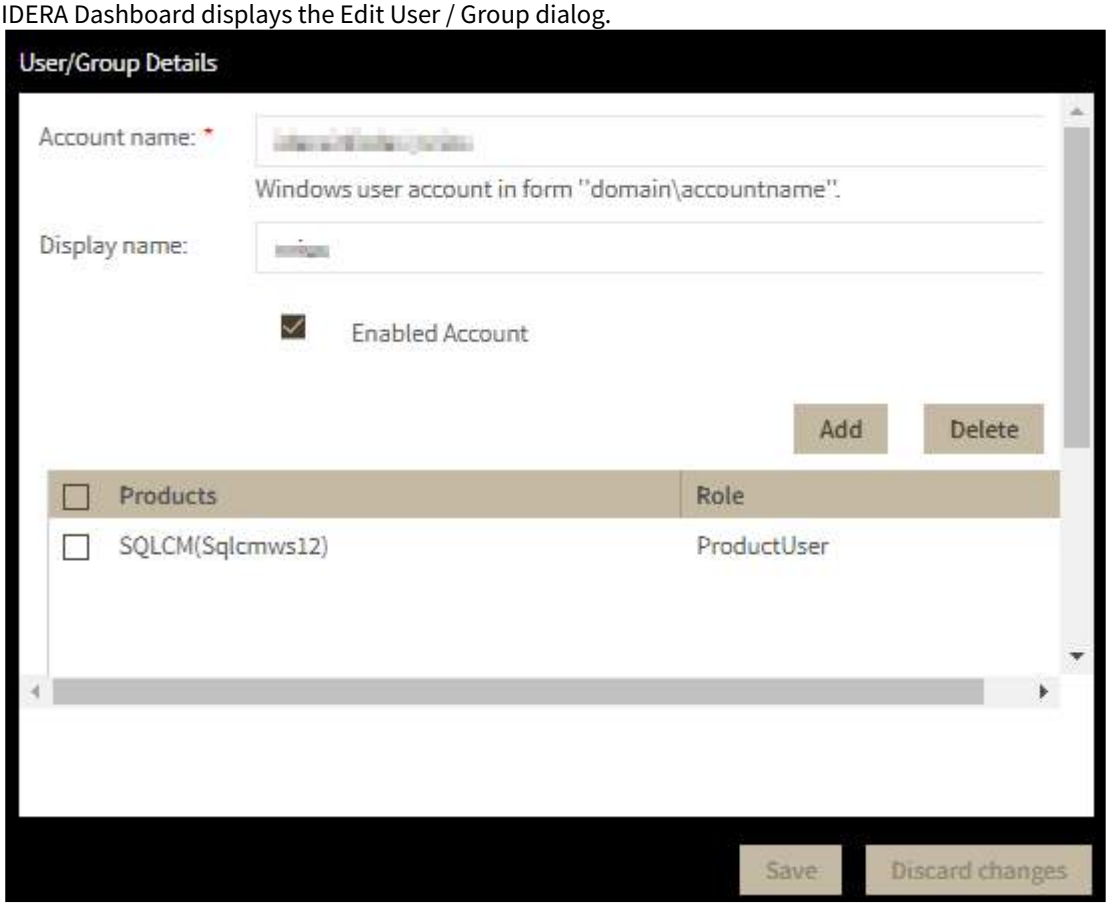
Editing a user in the IDERA Dashboard

Clicking the Edit icon for an existing user account allows you to edit the account name, enable or disable the user account, and add new permissions.

To edit a user or group:

1. Click the user account to edit it.

IDERA Dashboard displays the Edit User / Group dialog.



2. Make the necessary changes.
3. ***If you want to disable a user account*** , clear the **Account Enabled** checkbox. To enable the account, simply check the box.
4. ***If you want to add more roles to this user account or group*** , click **Add**. IDERA Dashboard displays additional **Product** and **Role** fields for you to add another role.
5. Click **Save**.

You **cannot** edit the logged in user credentials.

Removing a user from the IDERA Dashboard

Clicking the Delete icon for an existing user account or group allows you to remove that account from access to the IDERA Dashboard.

To delete a user or group.

1. In the list of users, click the **Delete** button for the user account or group that you want to delete. IDERA Dashboard displays a warning message that requires a confirmation whether you want to delete that

selection.

2. Click **Yes**. IDERA Dashboard removes the user account or group and they can no longer access the IDERA Dashboard using the account. ***If you did not mean to delete the selected* account**, click **No**.

Understanding user roles

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

IDERA common framework provides the functionality to add, edit, and delete users and groups while also managing their roles. IDERA SQL Compliance Manager leverages this user role functionality to allow you to easily manage the instance permissions associated with your accounts. For more information about managing users, see Managing users in the IDERA Dashboard.

There are three roles available:

- **Product Administrator**. Full access and control of SQL Compliance Manager.
- **Product User**. Cannot access the Dashboard Administration page, but can perform all job management and instance management actions.
- **Product Guest (Read-Only)**. Cannot access the Dashboard Administration page, but can access all other pages in read-only mode. This user cannot perform any job management or instance management actions.

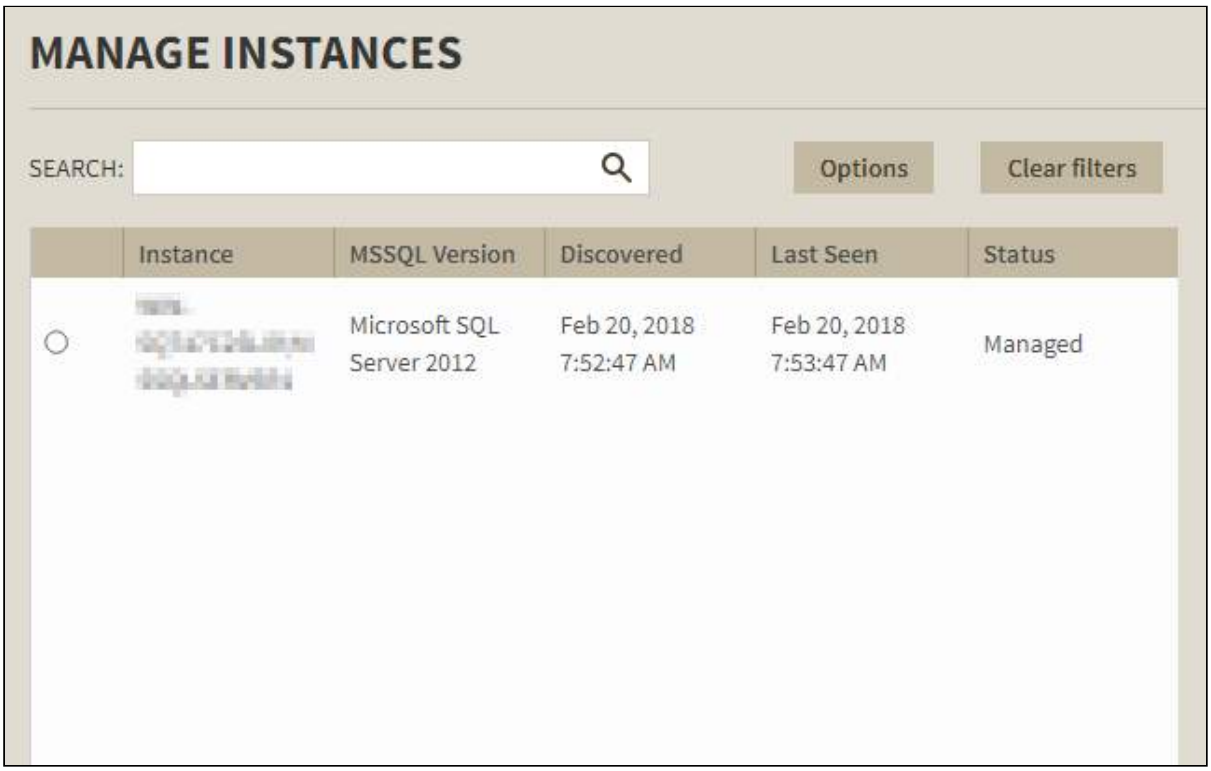
5.6.3 Managing instances in the IDERA Dashboard

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard tracks SQL Server instances, discovered and managed by different IDERA products. The Instances widget of the Administration view allows users to view and delete registered instances.

To view coverage or remove registered instances that no longer exist in your SQL Server environment, select **Manage Instances** in the Administration view, and the Managed Instances window displays. The View filter allows you to select from:

- **All**. Lists all instances discovered in your SQL Server environment and network.
- **Managed**. Lists only those managed instances in various IDERA products.
- **Unmanaged**. Lists instances discovered on the network but not registered.



5.6.4 Managing product registry in the IDERA Dashboard

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard hosts IDERA products that register with the Dashboard. To access product management in the IDERA Dashboard, either select **Manage Products** from the Administration menu or click **Manage Products** on the Administration view of the IDERA Dashboard. In the **Manage Products** window you can perform the following actions:

Registering a product in the IDERA Dashboard

Follow the instructions below to manually register a product.

1. In the **Manage Products** view, click **Register a Product**. The IDERA Dashboard displays the **Register a Product to IDERA Dashboard** dialog.

2. Select the location of the product you want to register, **Local** or **Remote**.

Local Installation:

1. Select the product you want to register from the available list or type in the name of the product.
2. Type a unique display name to help distinguish this instance from another instance if you have multiple installations of the same product. IDERA recommends a display name using the location or function, such as "DiagnosticManagerWest" or "DiagnosticManagerProd."
3. Type the name of the host instance where this product resides and the default port for the product. See the table below for information on the default ports for each product.

Idera Product Name	Product	Default Port	
SQL Business Intelligence	SQLBI	9277	
SQL Inventory Manager	SQLInventory Manager	9275	
SQL Diagnostic Manager	SQLdm	5170	
SQL Safe	SQLSafeRest Service	9998	
SQL Compliance Manager	SQLCM	5200, 5201	Can register manually as of version 5.4
SQL Workload Analysis	SQLWA	20700	Cannot register manually
SQL Enterprise Job Manager	SQLEJM	9271	Cannot register manually

> **Note**
>
> When you manually register the product it will use port 9292.

4. In the **Product Administrator** section, type the user name and password for the administrator account using the *domain\username* format.
5. Click **Register**. A confirmation message appears warning you that the system logs out your session upon continuing.
6. Click **Yes**. Log in to begin using the newly-registered product.

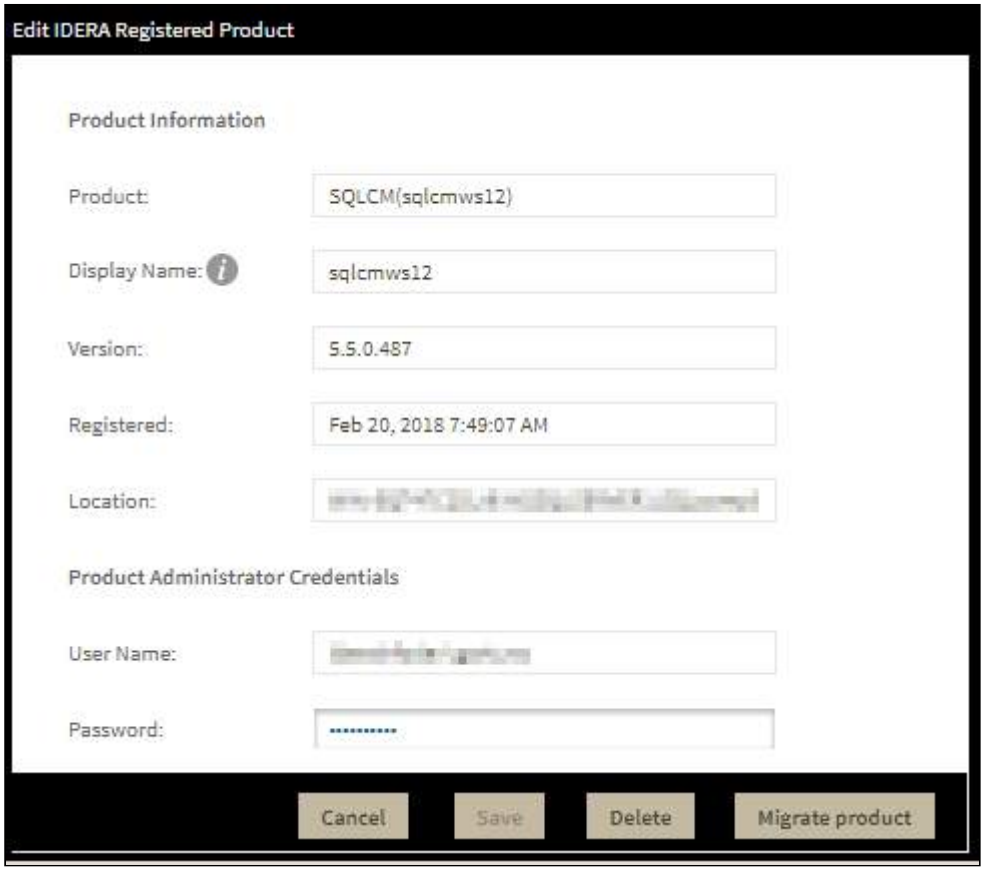
Remote Installation:

1. Enter the Host Name or IP Address of the server where your product is installed.
2. Provide the corresponding **Host User Name** and **Host Password**.
3. In the **Product Information** section, type the product information provided on the above table.
4. Under Product Administrator Credentials section enter the server credentials.
5. Click **Register**. A confirmation message appears warning you that the system logs out your session upon continuing.

Editing a product in the IDERA Dashboard

Clicking the **Edit** icon for an IDERA product allows you to edit the associated instance name, install location, user name and password for the account used to connect to the product, and the short or common name of the product. To edit a product, follow these steps:

1. Click one product in the list to edit it. IDERA Dashboard displays the the Edit IDERA Registered Product window.



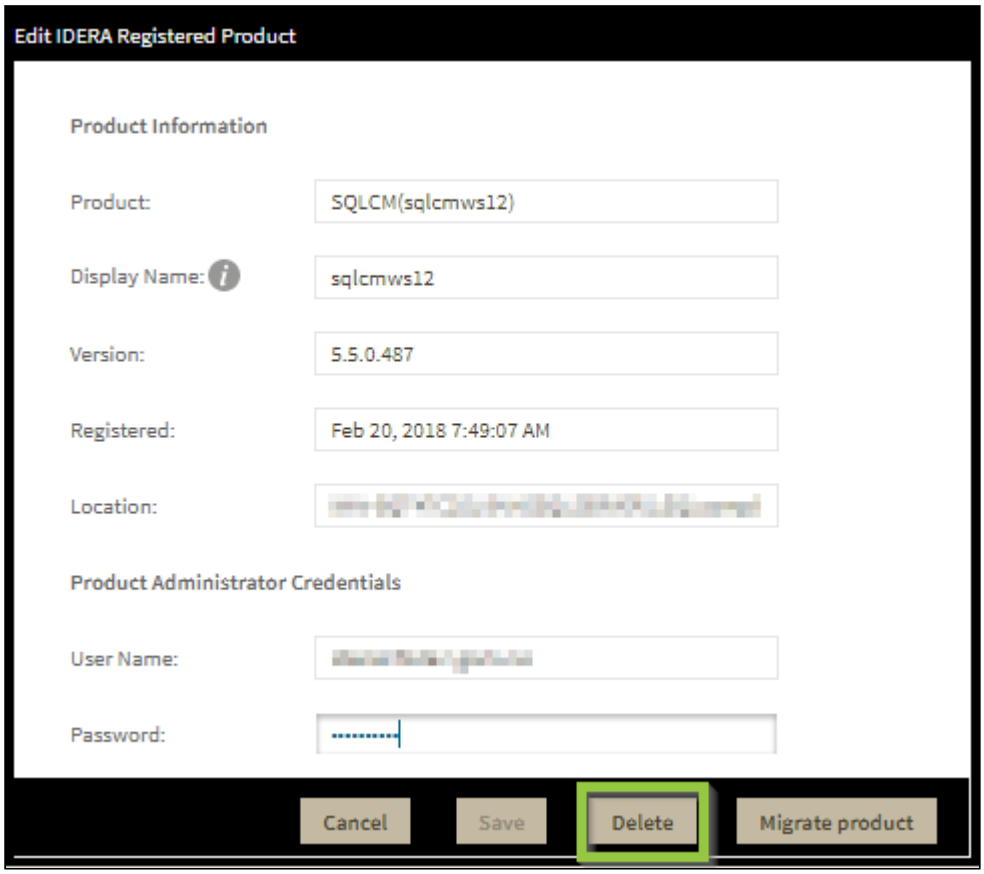
2. Make the necessary changes.
3. Click **SAVE**.

> **Note**
>
> Only user roles with administrative privileges can edit the products.

Removing a product from the IDERA Dashboard

Clicking the **Delete** icon for an IDERA product allows you to unregister that product. Use the following steps to delete a product.

1. Click one product in the list to delete it. IDERA Dashboard displays the Edit IDERA Registered Product window.



2. Click **Delete**. IDERA Dashboard displays the displays a warning message that requires a confirmation whether you want to delete that selection.
3. Click **Yes**. IDERA Dashboard unregisters and deletes the product and users can no longer access that product. ***If you did not mean to delete the selected account***, click **No**.

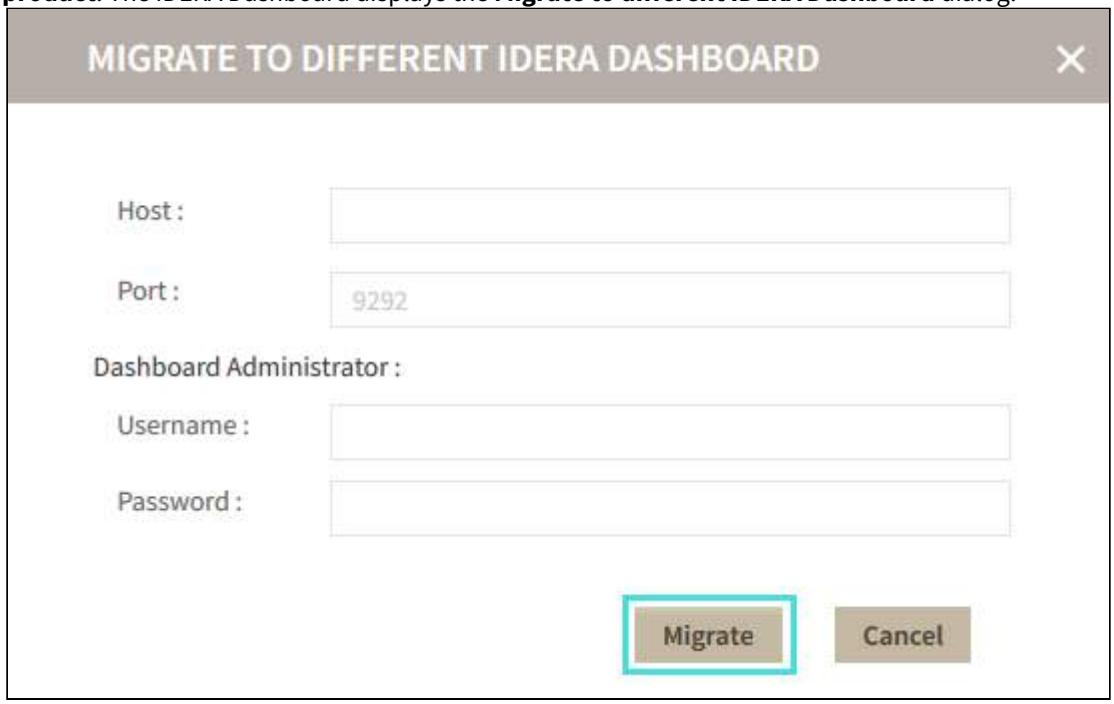
Migrating a product to another IDERA Dashboard installation

Users who have multiple IDERA products also may have more than one version or installation of the IDERA Dashboard. To take advantage of all of the features of the latest version of the IDERA Dashboard, you can migrate your products from one version of the IDERA Dashboard to another. This process migrates data to the target installation of the IDERA Dashboard and un-registers the product from the previous IDERA Dashboard.

Use the following steps to migrate an IDERA product from one installation or version of the IDERA Dashboard to another.

1. In the **Manage Products** view, select the product you want to migrate from one installation of the IDERA Dashboard to another.

2. Verify that the **Edit Product** dialog displays the information for the correct product, and then click **Migrate product**. The IDERA Dashboard displays the **Migrate to different IDERA Dashboard** dialog.



3. Type the name of the host machine on which the target IDERA Dashboard is installed and the port number.
4. In the **Dashboard Administrator** section, type the user name and password for the target IDERA Dashboard administrator account using the *domain\username* format.
5. Click **Migrate**. The IDERA Dashboard migrates the product to the target IDERA Dashboard.

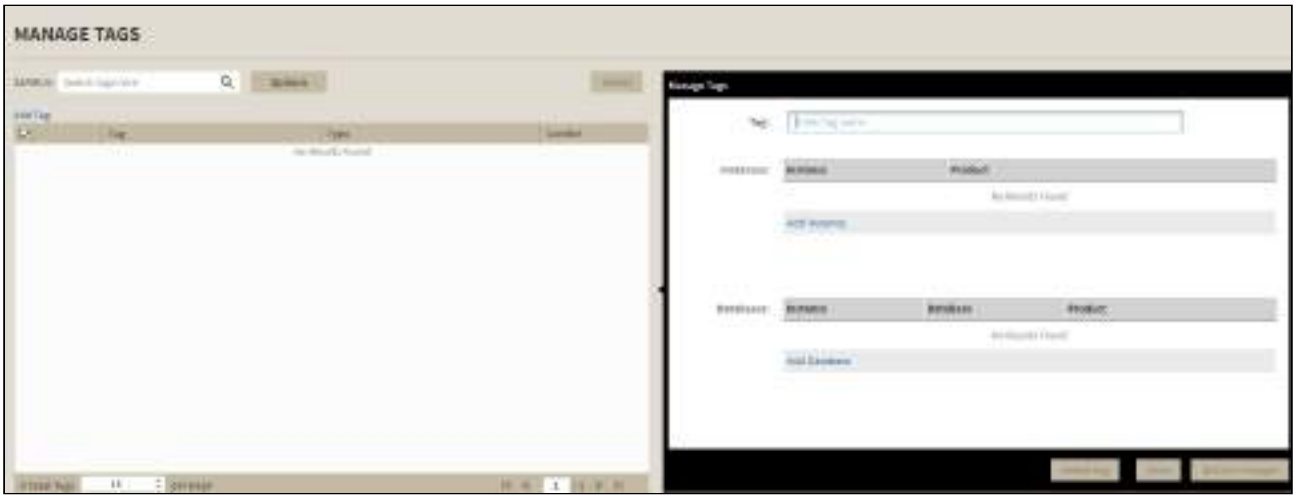
5.6.5 Managing tags in the IDERA Dashboard

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

IDERA Dashboard tags help you organize and manage instances and databases within your environment. Created and updated are available to use with the IDERA SQL products.

You can add, view, edit, and delete tags and their associated instances and databases.

Click **Manage Tags** in the **Administration** tab to display the configuration window.



⚠ Global tags are managed only through the IDERA Dashboard.

Adding, editing, and removing a tag

To add a tag and assign it to a specific instance and/or database, click **Add Tag,** type all required information, and click **Save.**

To edit an existing tag, select one from the list, make all necessary changes, and click **Save**.

To remove a tag, select one from the list, and click **Delete tag.** The IDERA Dashboard displays a confirmation dialog, click **Yes** to delete the tag.

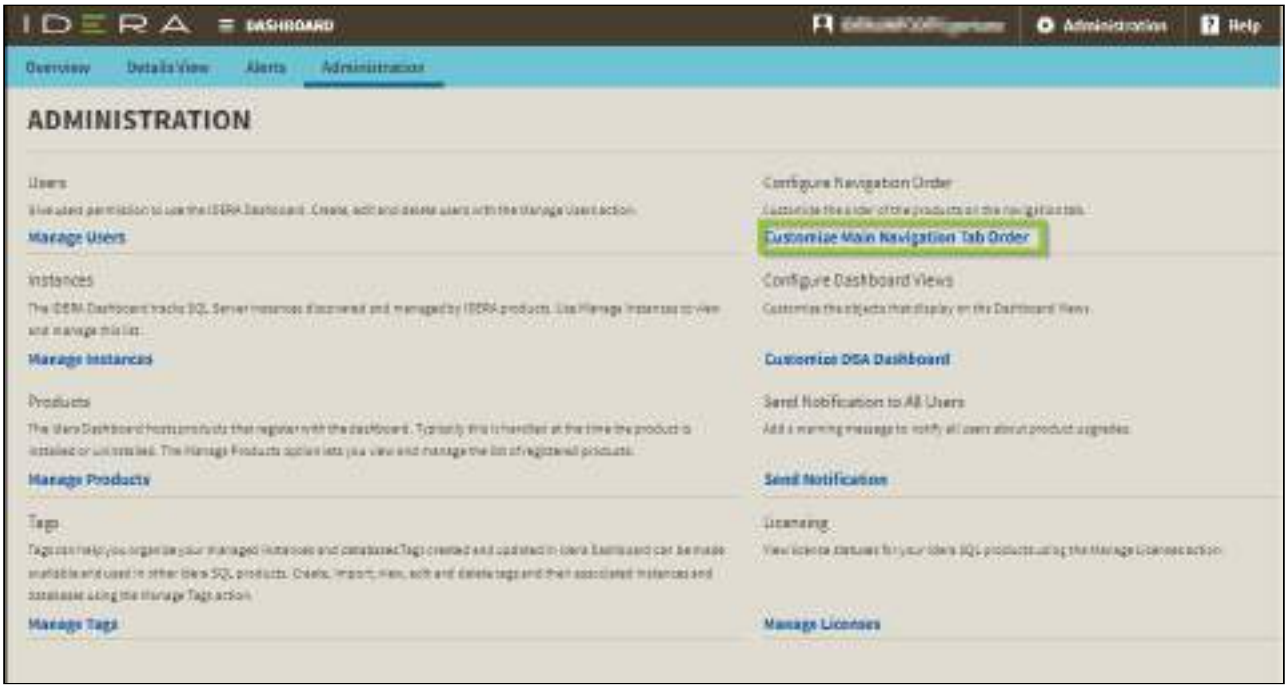
You can search tags using filters by clicking on **Options** next to the **Search** box**.** Available filters are:

- Product
- Instance
- Database

5.6.6 Configure navigation order in the IDERA Dashboard

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The Configure Navigation Order widget of the Administration view, allows users to customize the order of the different IDERA products on the navigation tab.



To rearrange product tabs:

1. Click the **Customize Main Navigation Tab Order** link and a dialog displays.

2. Move tabs using a drag-and-drop operation.
3. Click **Save** when done.

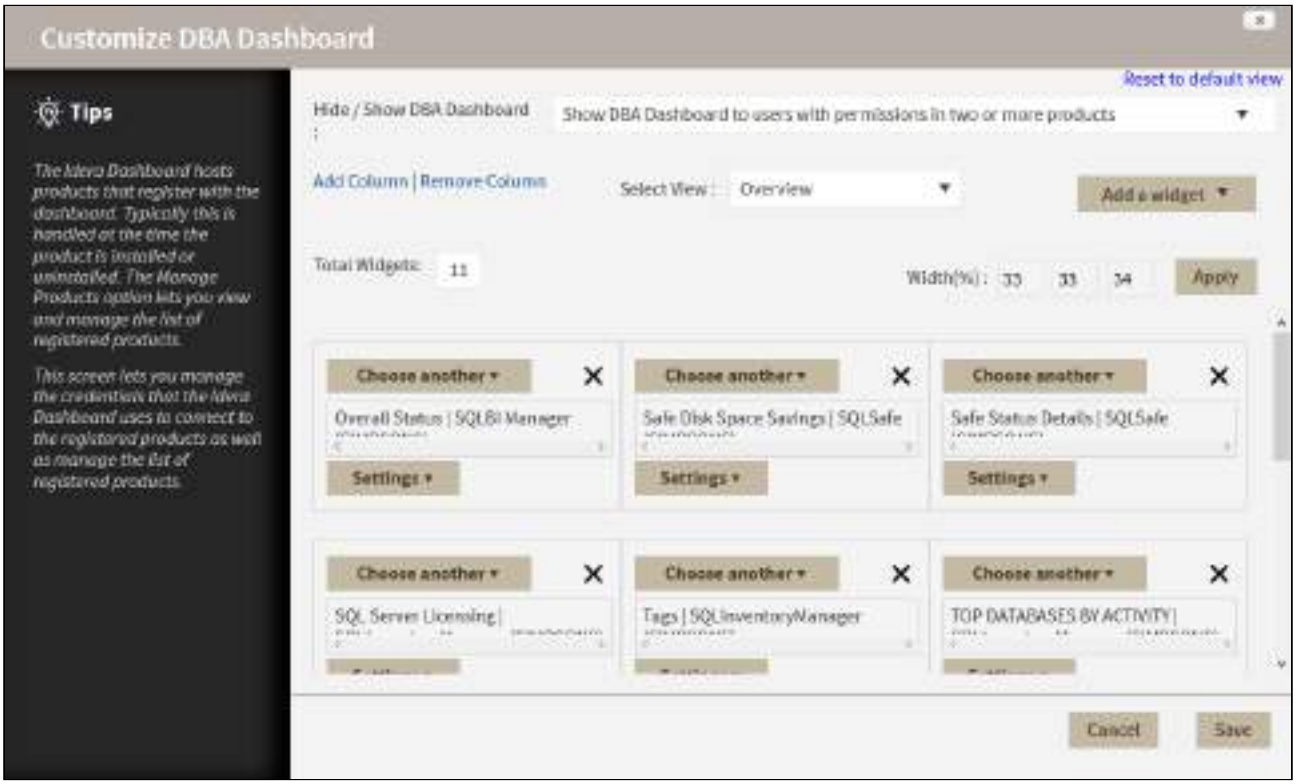
5.6.7 Configure Dashboard Views

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The purpose of the IDERA Dashboard is to host other IDERA products. These products must register with the IDERA Dashboard, which is typically done at the time the product is installed or uninstalled. The Manage Products option lets you view and manage the list of registered products.

The **Configure Dashboard Views** option allows users to customize which product widgets are shown in the Overview and Details view tabs of the IDERA Dashboard.

Click the **Customize DBA Dashboard** option in the **Administration** tab to display the Customize DBA Dashboard configuration panel.

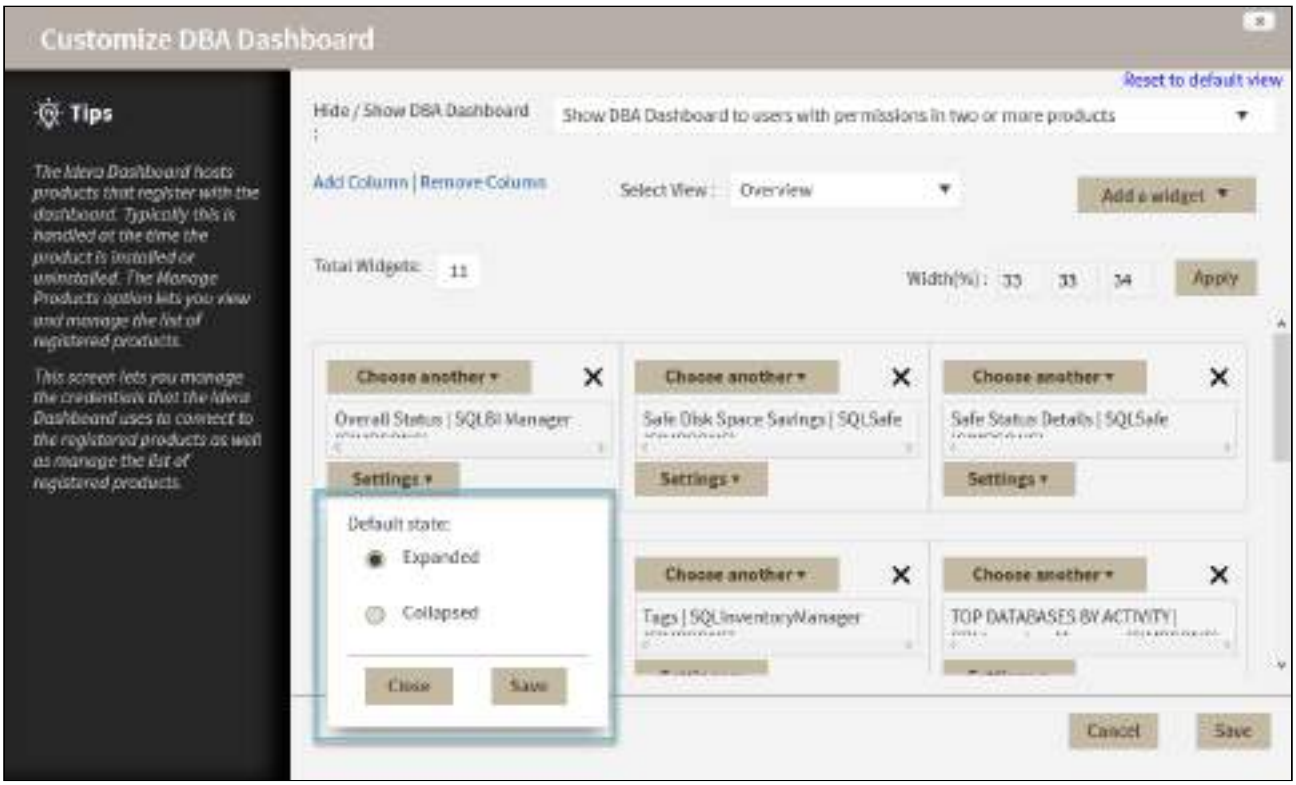


In the Customize DBA Dashboard dialog you can try the following:

- Choose to hide or show the DBA Dashboard to all users or to users with permissions in two or more products.
- Select the View you want to modify (Overview or Details View).
- Add or remove columns from the selected View.
- Specify the column widths.
- Add product widgets.
- Remove widgets.
- Re-arrange widgets (drag and drop).

Additionally, you can:

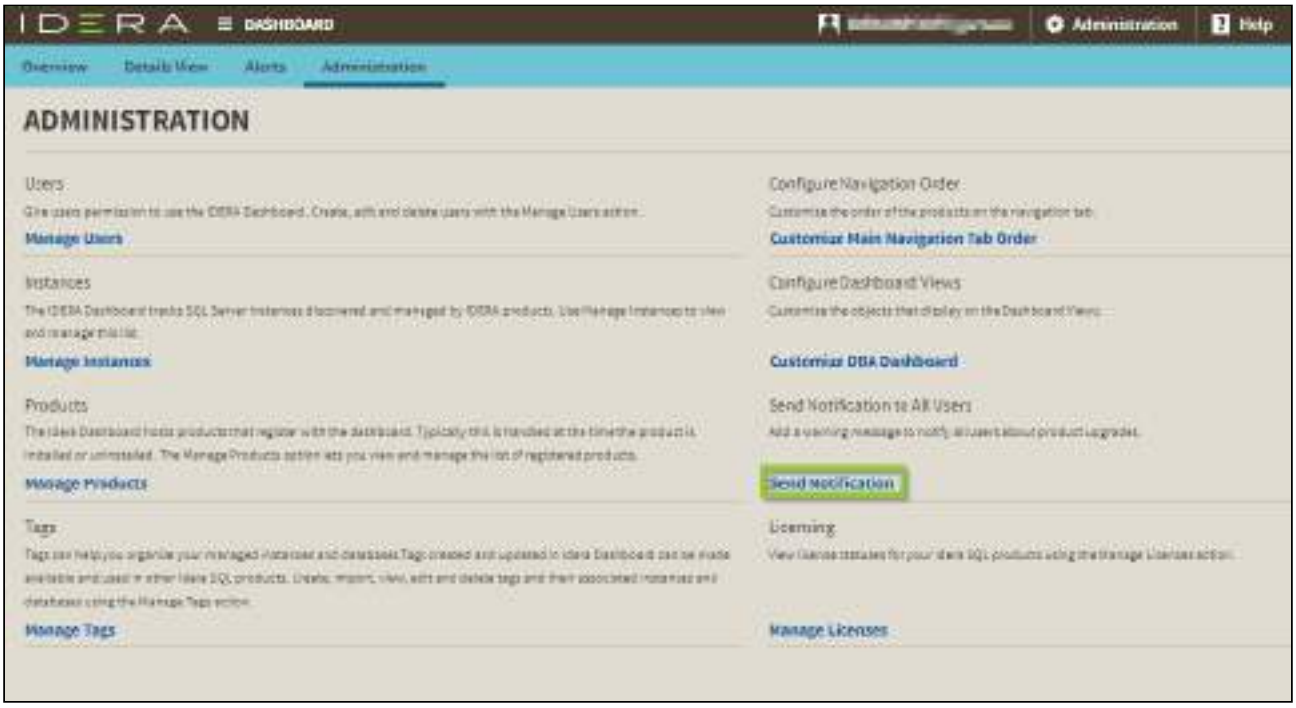
- Modify specific settings for each widget, such as its default state (Expanded or Collapsed).
- Assign another widget to a previously placed widget.



5.6.8 Notifying users about product upgrades in the IDERA Dashboard

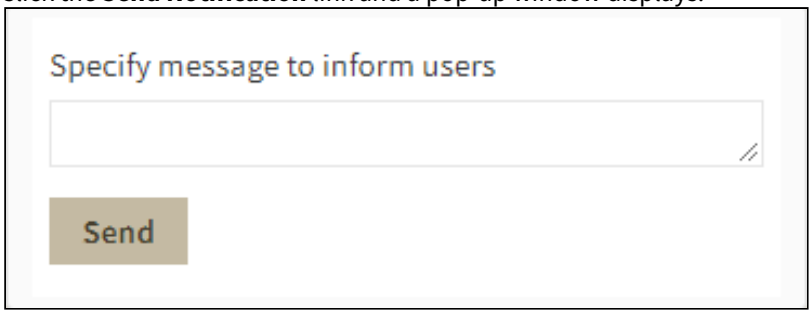
⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The Send Notification to All Users widget of the Administration view lets you send a notification to all user accounts added to IDERA Dashboard. Use this feature to notify users about product upgrades and other issues affecting product use.



To send notification to all users:

1. Click the **Send Notification** link and a pop-up window displays.



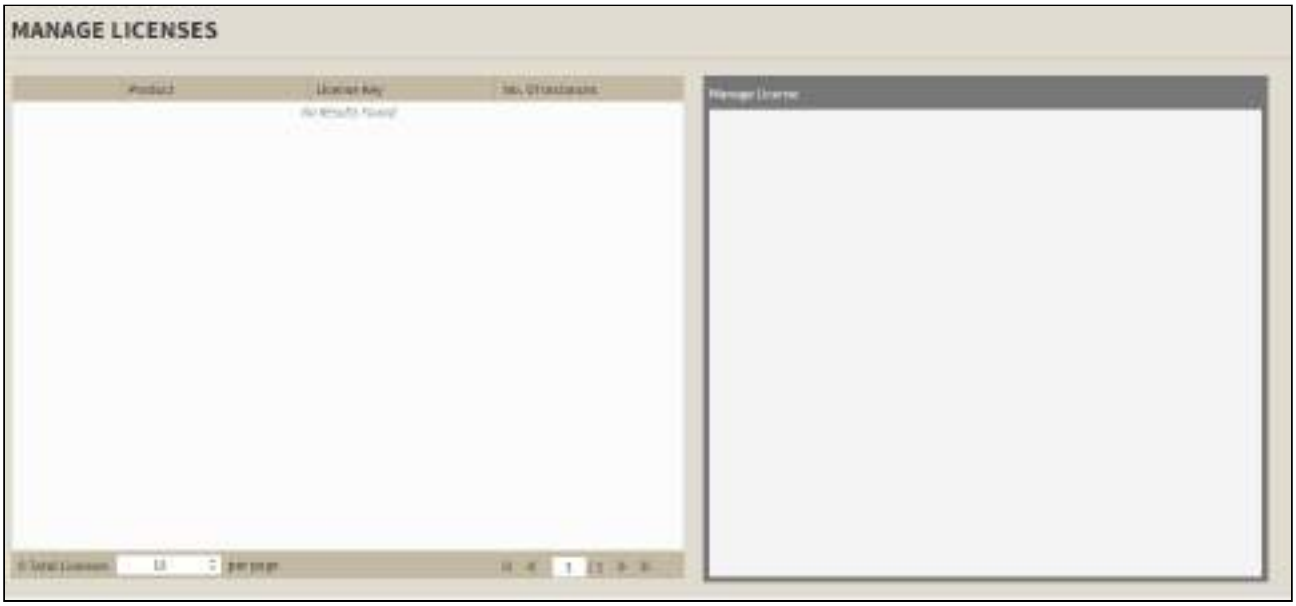
2. Type the message you want to send, and click **Send**.

5.6.9 Managing licenses in the IDERA Dashboard

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA Dashboard allows you to manage licenses for the different IDERA SQL products.

To view and manage licenses, click **Manage Licenses** in the **Administration** tab.



In the **Manage Licenses** view, you can see the following information:

- Product
- License key
- No. Of Instances

To **Add, Edit,** and/or **Delete** a license, click on a license from the list and fill the required information or make the necessary changes.

6 Navigate the SQL Compliance Manager Web Console

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

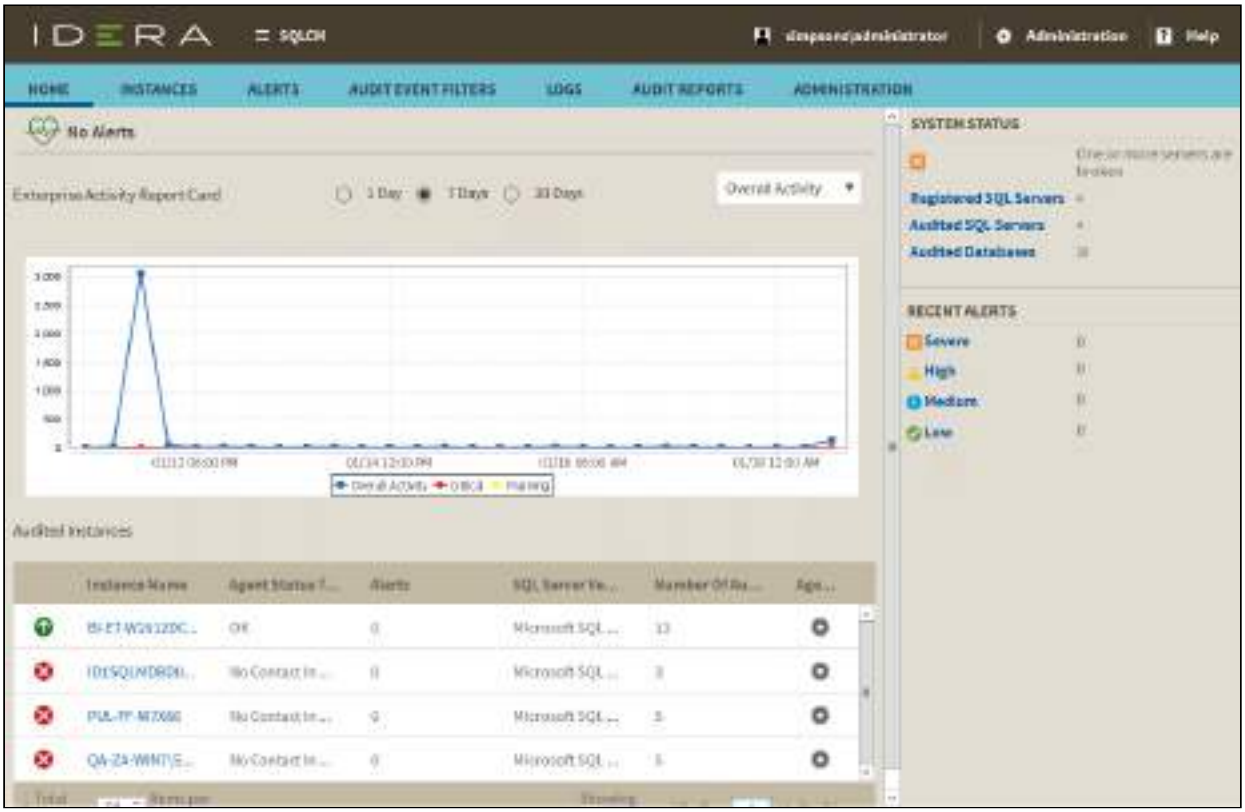
The IDERA Dashboard SQL Compliance Manager Web Console provides a browser-based interface for many of the features within the SQL Compliance Manager Management (Windows) Console. the following topics help you explore what features are available to you:

- View the Home tab
- Manage audited instances
- View alerts and alert rules
- Manage audit event filters
- View logs
- Generate audit reports
- Administer SQL Compliance Manager
- Sensitive Column Search window

6.1 View the Home tab

> ⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The Home tab is the default overview page of the product. This tab provides a high-level status of your audited instances and enterprise activity occurring within your environment.



6.1.1 Alerts

IDERA SQL Compliance Manager performs health checks on your registered instances to help you monitor the most important issues across your environment. On this section of the Overview tab, SQL Compliance Manager shows you the active alerts for your environment, grouped by alert type, and ordered by level of criticality, where:

- Level 4 = Severe
- Level 3 = Critical
- Level 2 = Warning
- Level 1 = Informational

> If you have no active alerts, you will see the message: **No alerts.**

You can click the options available for each alert to:

- **Show Details** of instances or databases affected by the respective alert.
- Individually **Acknowledge** the alert.
- Individually **Dismiss** the alert.
- Individually **Clear** the alert.

If you do not want to see these details, click **Hide Details.**

You can also get the most updated information for your alerts by clicking **Refresh**.

6.1.2 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 for 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. Use Activity Report Cards to identify problems that might require more in-depth analysis based on:

- Overall Activity.
- Event Alerts.
- Failed Logins.
- Security.
- DDL.
- Privileged User.

For more information about the Enterprise Activity Report Card, see Explore Activity - Audited SQL Servers Summary tab.

6.1.3 Audited Instances

All audited SQL Server instances in your environment appear in the Audited Instances section of the Home tab. The default sort order displays the first five instances based on instance name. If you have more than five registered instances, SQL Compliance Manager allows you to page through the results. This table includes:

- **Instance Name**. Displays the name of the audited SQL Server instance.
- **Agent Status Text**. Displays the current status of the SQL Compliance Manager Agent. Options include OK, Informational, Warning, and Critical.
- **Alerts**. Displays the number of alerts associated with that instance.
- **SQL Server Version**. Displays the SQL Server version installed on that instance.
- **Number of Audited DBs**. Displays the number of databases audited by SQL Compliance Manager on that instance.

- **Agent Actions**. Displays a list of actions you can perform on the Agent associated with the instance. Options include Enable Auditing, Disable Auditing, and Upgrade Agent.

Click the name of a SQL Server instance, and SQL Compliance Manager opens the Instance Details view for that instance.

6.1.4 System Status and Recent Alerts area

On the right side of the IDERA Dashboard SQL Compliance Manager Home page, you can view the number of SQL Server instances and databases needing your immediate attention in addition to a count of recent alerts by severity.

System Status

Indicates whether IDERA SQL Compliance Manager encountered any issues while auditing your SQL Server environment. Click the status link to open the more detailed Audited Instances view. Use view to see the status of the audited databases on this instance, validate audit settings, and check the SQL Compliance Manager Agent status.

Registered SQL Servers

Displays the number of SQL Server instances that are registered with SQL Compliance Manager.

Audited SQL Servers

Displays the number of instances currently audited. This number does not include instances where auditing is not yet configured or is disabled.

Audited Databases

Displays the number of databases currently audited. These databases are hosted by SQL Server instances that are registered with SQL Compliance Manager. This number does not include databases where auditing is not yet configured or is disabled.

For more information about the System Status area, see Explore Activity - Audited SQL Servers Summary tab.

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.

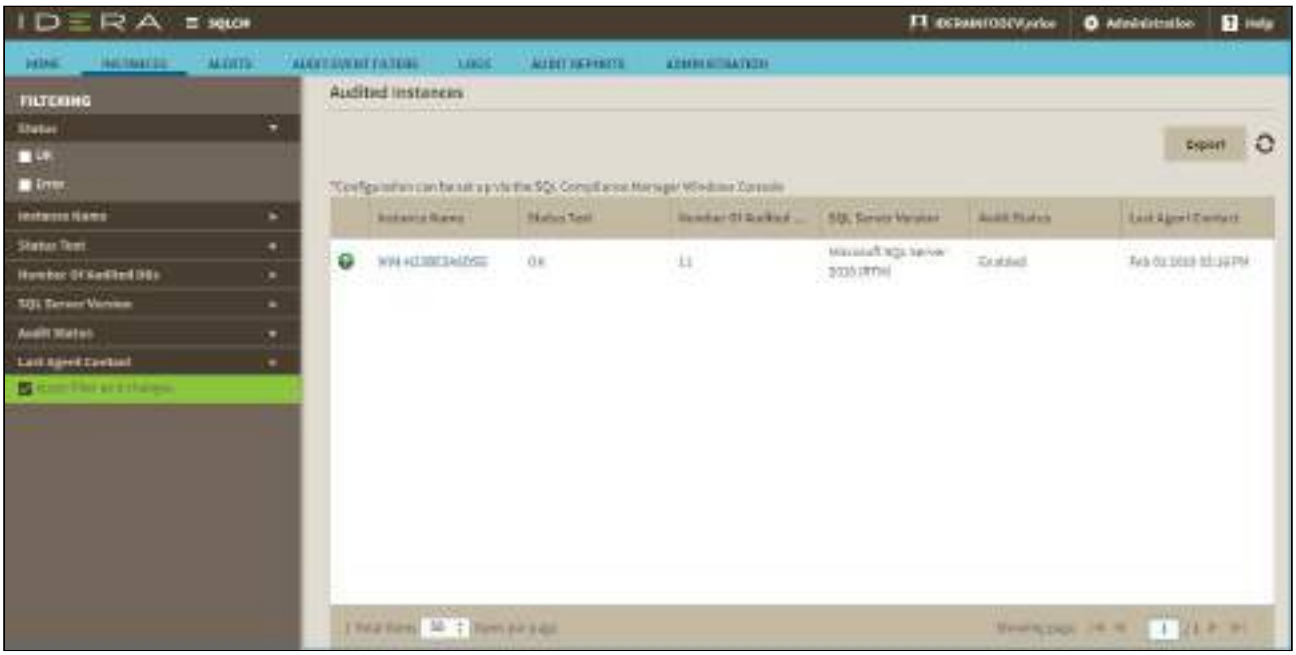
For more information about specific alerts, see View alerts and alert rules. You can view which alerts are generated from multiple instances across your environment or from a particular instance.

6.2 Manage audited instances

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA SQL Compliance Manager Instances view displays the status of audit activity across your SQL Server environment. Use the statistics and graphs on this view to quickly and easily identify issues so you can continue to ensure the correct level of compliance. Be sure to review the associated topics about managing properties for the registered SQL Server instance and the Agent:

- Viewing instance details



Configuration can be set up via the SQL Compliance Manager Windows Console.

6.2.1 Available actions

Filtering

Allows you to filter the listed instances by status, instance name, status text, number of audited databases, SQL Server version, audit status, and timestamp for the last time the agent was contacted.

Export

Allows you to export the list of audited SQL Server instances in PDF, XLS, or XML format.

Refresh

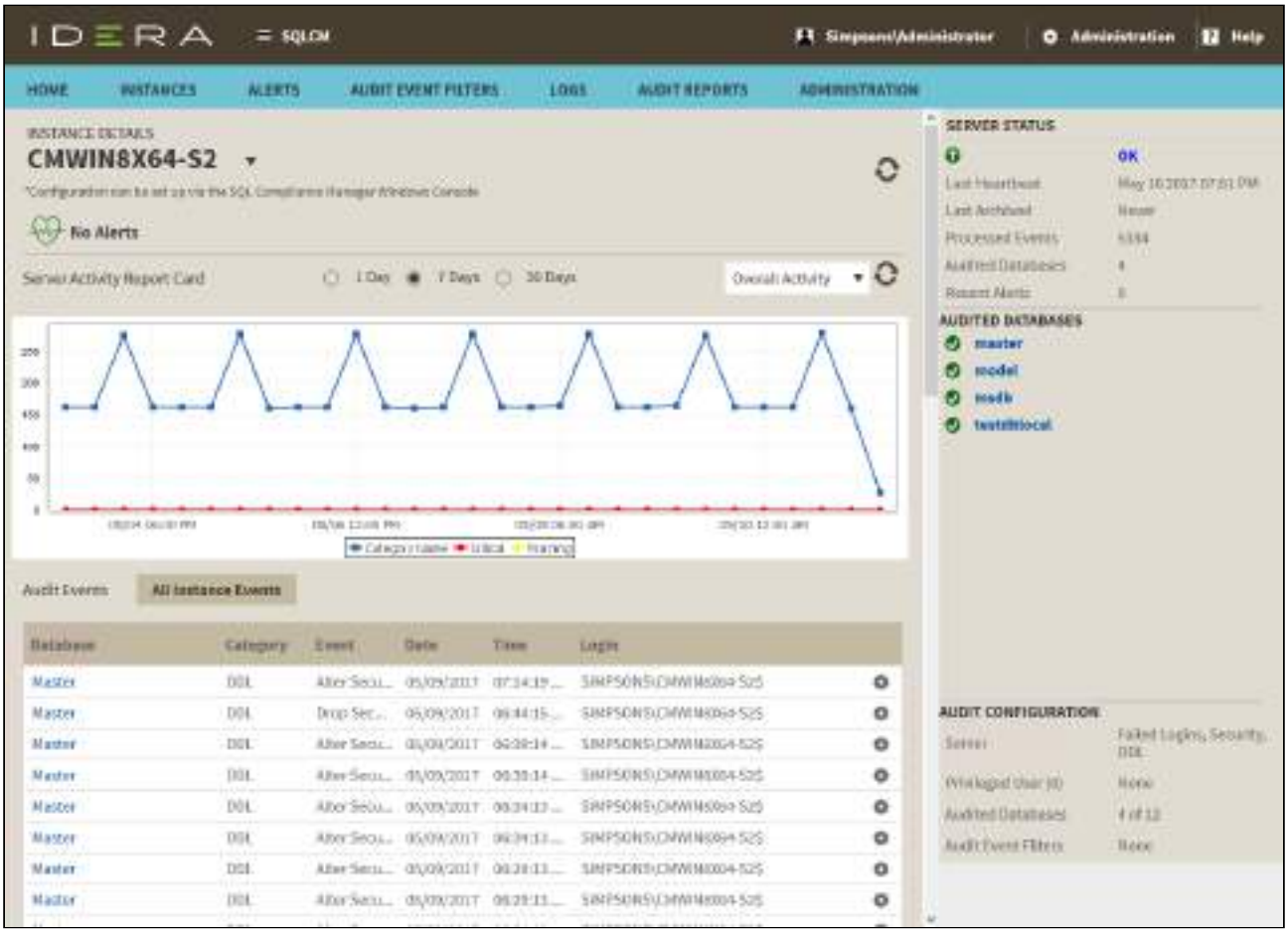
Allows you to update the Audited Instances list with current data.

Click the name of a SQL Sever Instance to open the Instance Details view for the selected instance.

6.2.2 Viewing instance details

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

After you register an instance in IDERA SQL Compliance Manager, you can access the Instance Details view by clicking an instance name.



The Instance Details view allows you to view a list of audit events occurring on the databases for that instance, information about its databases, bar graphs, other relevant information, and also get access to audit configuration details.

The instance Details view provides a high-level status of the audited events and the activity occurring in the selected instance.

Alerts

On this SQL Compliance Manager shows you the active alerts for the selected instance, grouped by alert type, and ordered by level of criticality, where:

- Level 4 = Severe
- Level 3 = Critical
- Level 2 = Warning
- Level 1 = Informational

If you have no active alerts, you will see the message: **No alerts.**

Server Activity Report Card

The Server Activity Report Card allows you to review the status of the selected instance and the recent activity on it for up to 30 days. Use Server Activity Report Cards to identify problems that might require more in-depth analysis based on:

- Overall Activity.
- Event Alerts.
- Failed Logins.
- Security
- DDL
- Privileged User.

Audit Events

All audited events for the selected instance appear in the Audited Events section of the Instance Details page. This table includes:

- Database Name
- Event
- Date
- Time
- Login

Users can also view the Event Properties by clicking the gear icon and selecting the Event Properties option.

Server Status

On the right side of the Instance Details page, users can check the Server Status. This section displays.

Audited Databases

Displays the number of databases currently audited. These databases are hosted by SQL Server instances that are registered with SQL Compliance Manager. This number does not include databases where auditing is not yet configured or is disabled.

Audit Configuration

Displays the audit configurations set for the selected instance.

6.3 View alerts and alert rules

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA SQL Compliance Manager Alerts view allows you to view the current alerts and alert rules throughout your environment. 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.

6.3.1 Available actions include:

Page through alerts and alert rules

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

Filtering

Allows you to filter the listed alerts and rules by rule, rule type, server name, alert level, user email address, event log, and SNMP traps. Filtering includes a **Save View** feature that lets you select all of your filtering options, and then save the settings for future use. Click **Load View** to select a previously-saved view for use.

View By

Allows you to select whether Alerts or Alert Rules appear in this view.

Filtered By

Allows you to select the type of Alerts displayed in this view. You can view all Alerts, only your Event Alerts, only Data Alerts, or only Status Alerts based on this selection.

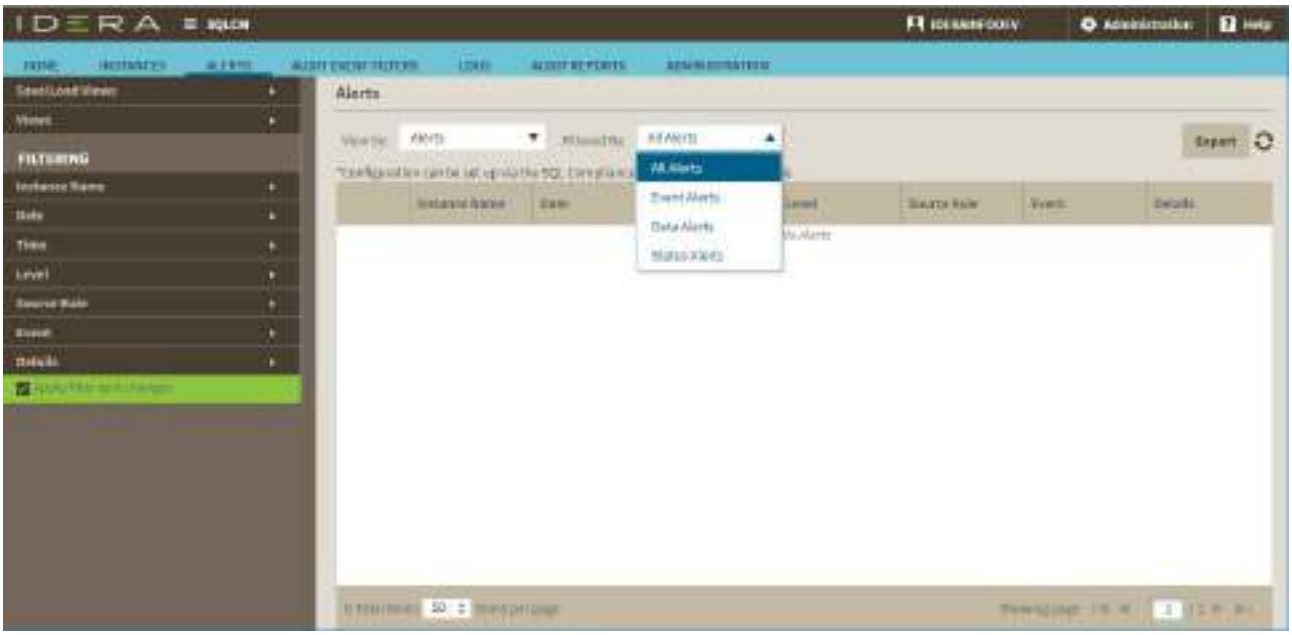
Export

Allows you to export the Activity Log and Change Log information to a CSV, PDF, or XML file.

Refresh

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

6.3.2 Alerts view



Configurations can be set up via the SQL Compliance Manager Windows Console.

Default columns

Instance name

Provides the name of the audited SQL Server instance where this event occurred.

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.

Detail

Provides additional information about the alert.

Event Alerts view

The Event Alerts view, available from the **Filtered By** selection, 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.

Data Alerts view

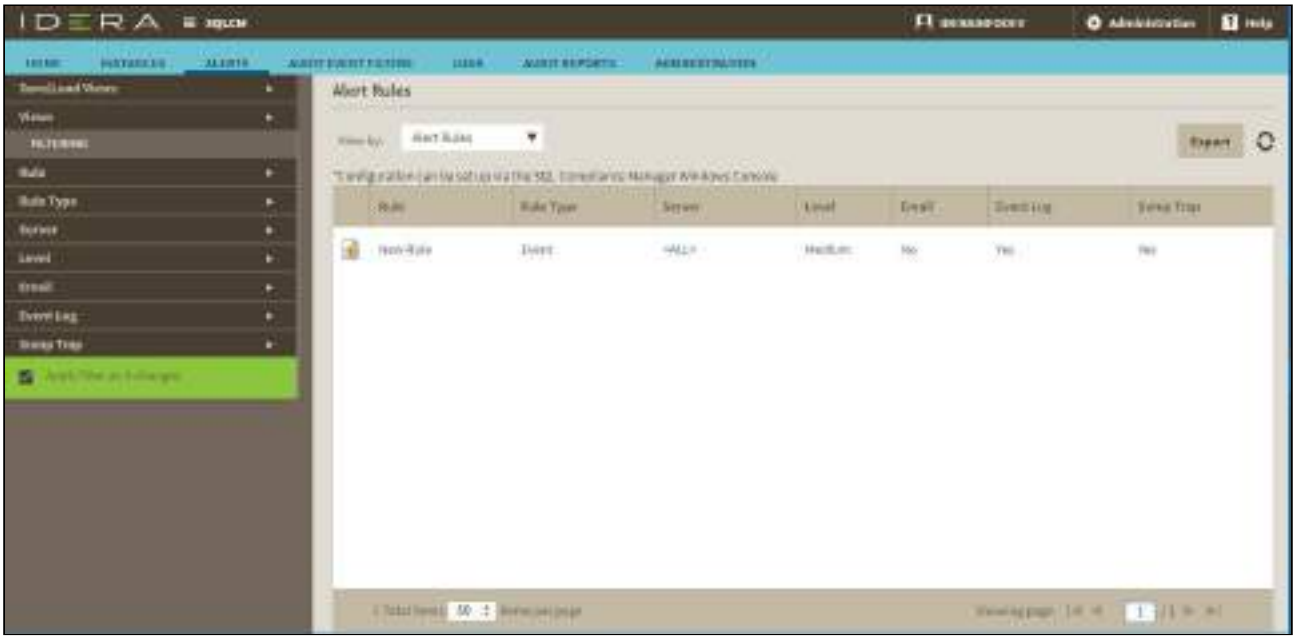
The Data Alerts view, available from the **Filtered By** selection, allows you to view previously generated Data Alerts. A Data Alert is generated when the Collection Server processes a SQL Server event that matches the alert rule criteria. Use Data Alerts to identify and investigate data manipulation 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.

Status Alerts view

The Status Alerts view, available from the **Filtered By** selection, 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 IDERA SQL Compliance Manager operations, such as deployed agents that may have stopped running.

6.3.3 Alert Rules view



Configurations can be set up via the SQL Compliance Manager Windows Console.

Default columns

Rule

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

Rule Type

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

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 Compliance Manager 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 Compliance Manager 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.

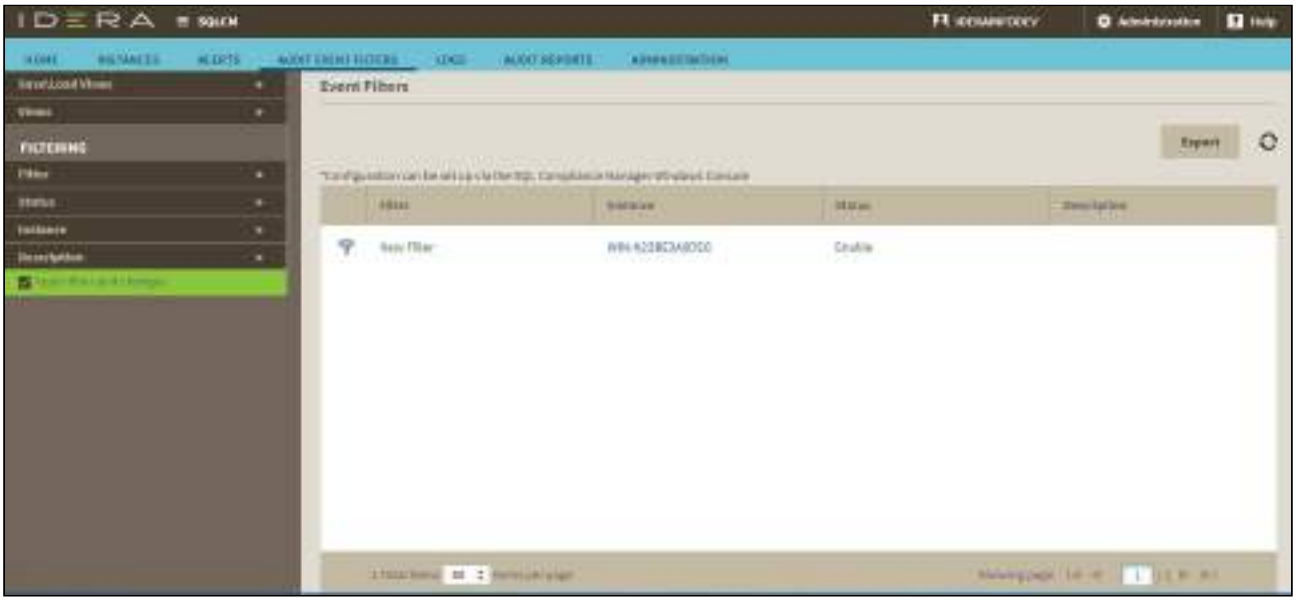
SNMP Trap

Indicates whether the alert rule criteria includes sending SNMP Trap messages to a specified network management console. When SNMP Trap is configured, SQL Compliance Manager sends an alert message to the specified network management console. Depending on the rule type, you can set up SNMP Trap notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

6.4 Manage audit event filters

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA SQL Compliance Manager Audit Event Filters view 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.



ⓘ Configurations can be set up via the SQL Compliance Manager Windows Console.

6.4.1 Available actions

Filtering

Allows you to filter the listed event filters by status, instance name, and description. Filtering includes a **Save View** feature that lets you select all of your filtering options, and then save the settings for future use. Click **Load View** to select a previously-saved view for use.

Refresh

Allows you to update the Audit Event Filters list with current data.

Export

Allows you to export Event Filters created for the associated 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.

6.5 View logs

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA SQL Compliance Manager Logs view lists events and alerts initiated by SQL Compliance Manager components, allowing you to monitor operations and diagnose issues within your environment. The Logs view consists of the Activity Log and Change Log areas, toggled by the option at the top of the page.

Available actions include:

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.

Filtering

Allows you to filter the listed activities by date, time, instance name, event, user name, and description. Filtering includes a **Save View** feature that lets you select all of your filtering options, and then save the settings for future use. Click **Load View** to select a previously-saved view for use.

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.

Export

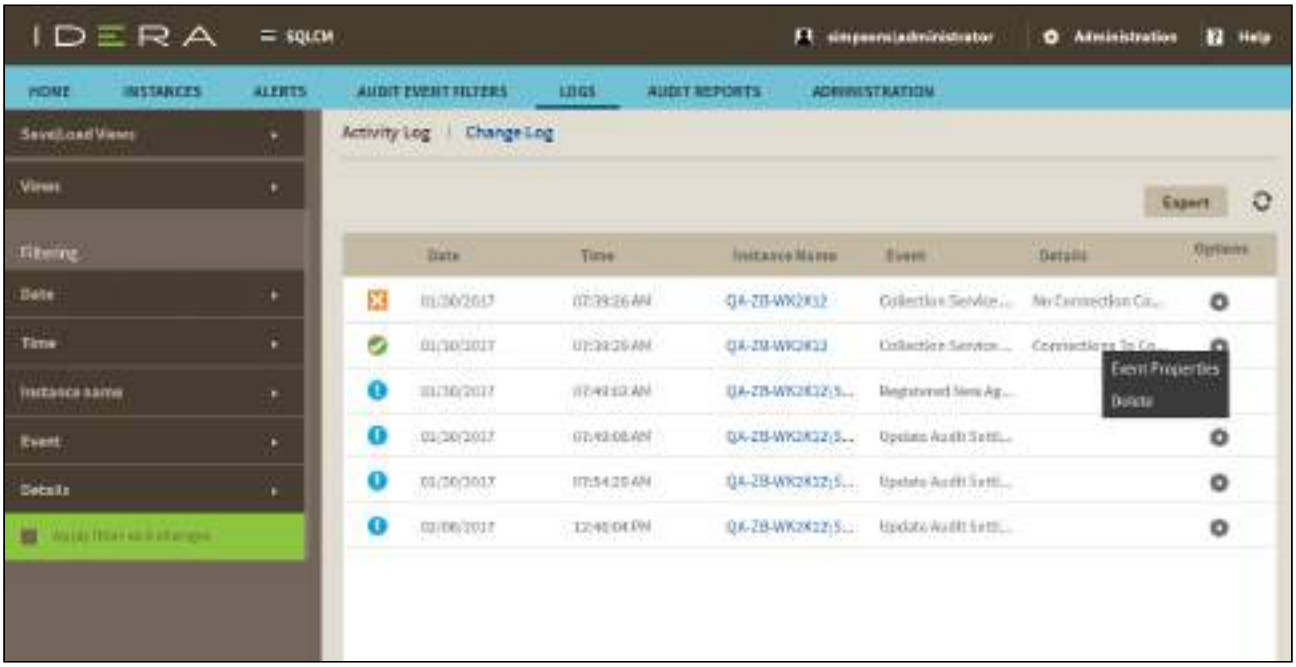
Allows you to export the Activity Log and Change Log information to a CSV, PDF, or XML file.

Refresh

Allows you to update the activity list with current data.

For more information about the Activity Log and Change Log tabs in the SQL Compliance Manager Monitoring Console, see Activity Log tab and Change Log tab.

6.5.1 Activity Log view



The Activity Log view displays a list of activity and system alerts across all registered instances. SQL Compliance Manager generates the following types of system alerts:

System Alert	Caused by ...	Resolves when ...
Agent Configuration Error	Error saving the SQL Compliance Manager Agent configuration file (.bin) Error loading the new configuration	File is successfully saved SQL Compliance Manager 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	SQL Compliance Manager Agent configuration update or health check is successful
Server Connection Error	Error when connecting to the audited instances, due to invalid permissions or the offline SQL Server instance	Connection is established
SQL Trace Error	Error when starting or stopping the audit traces	Audit traces are started or stopped

System Alert	Caused by ...	Resolves when ...
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

Available columns include:

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Instance Name

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

Event

Provides the type of event that occurred.

Detail

Displays the first line of the event details.

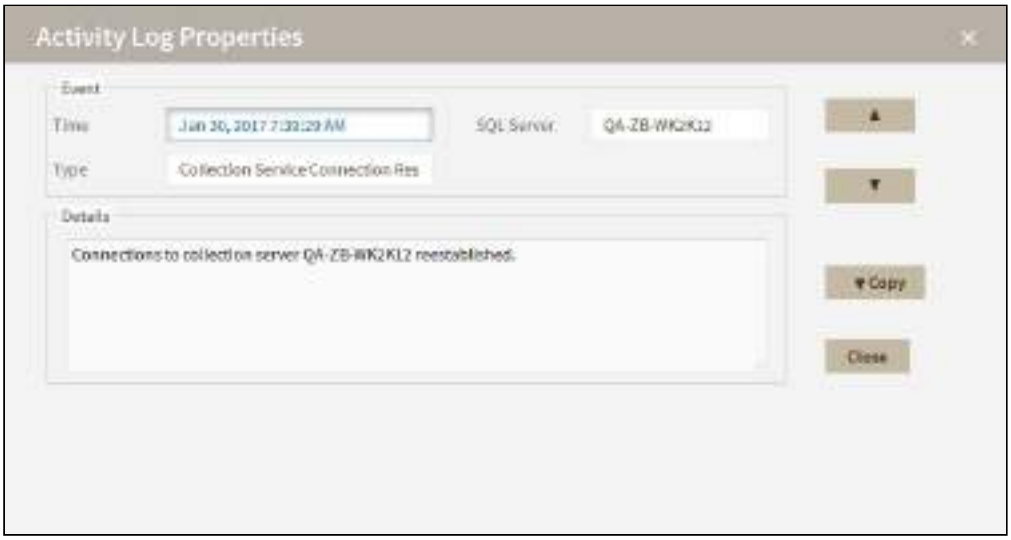
Activity Log Properties

For each event, you can view properties by clicking **Event Properties** under the gear icon for the associated event. The Activity Log Properties window allows you to view details about an individual event in the Activity Log. You can view the following information:

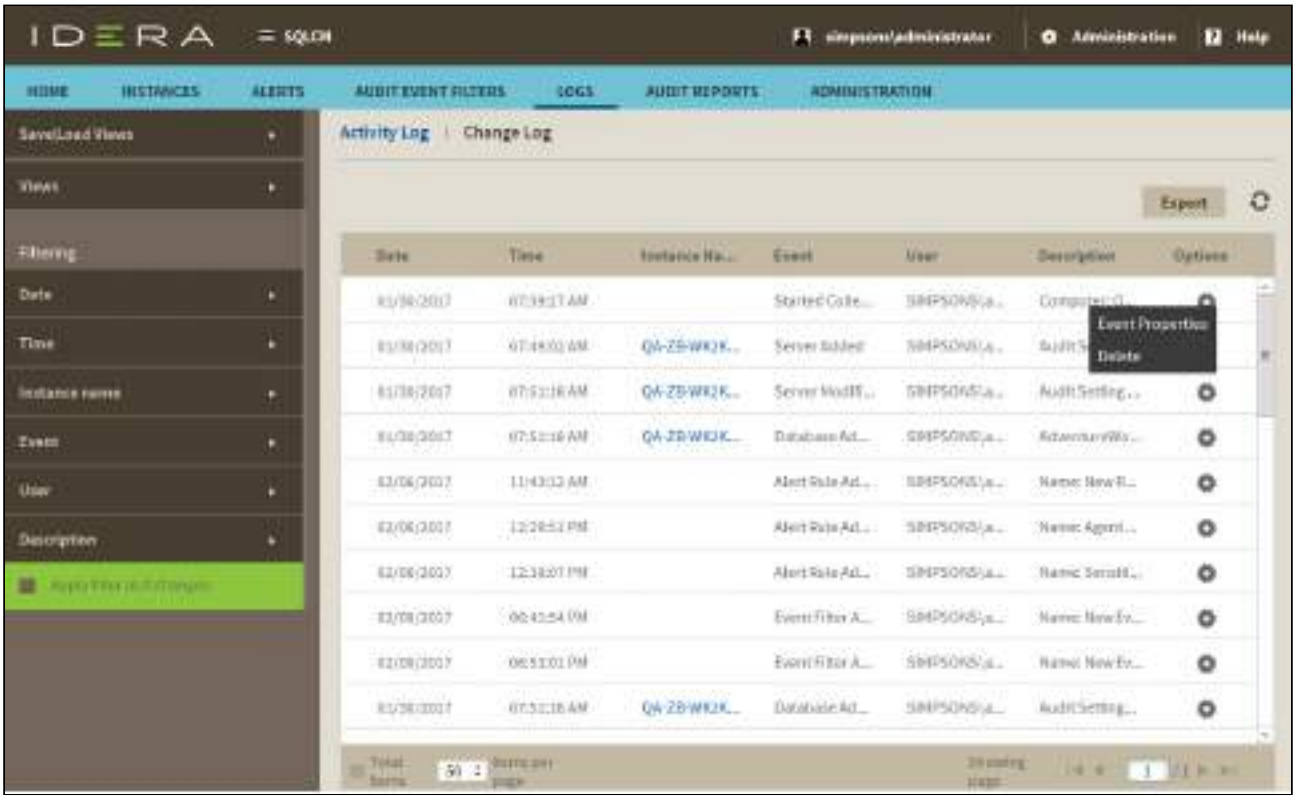
- Date and time the event occurred
- Type of event
- SQL Server instance on which the event occurred

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

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



6.5.2 Change Log view



The Change Log view lists changes and events initiated through the Management Console and the Collection Server, allowing you to monitor IDERA SQL Compliance Manager operations and diagnose issues.

Available columns include:

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Instance Name

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

Event

Provides the type of event that occurred.

User

Provides the name of the user account associated with the event.

Description

Displays the first line of the event details.

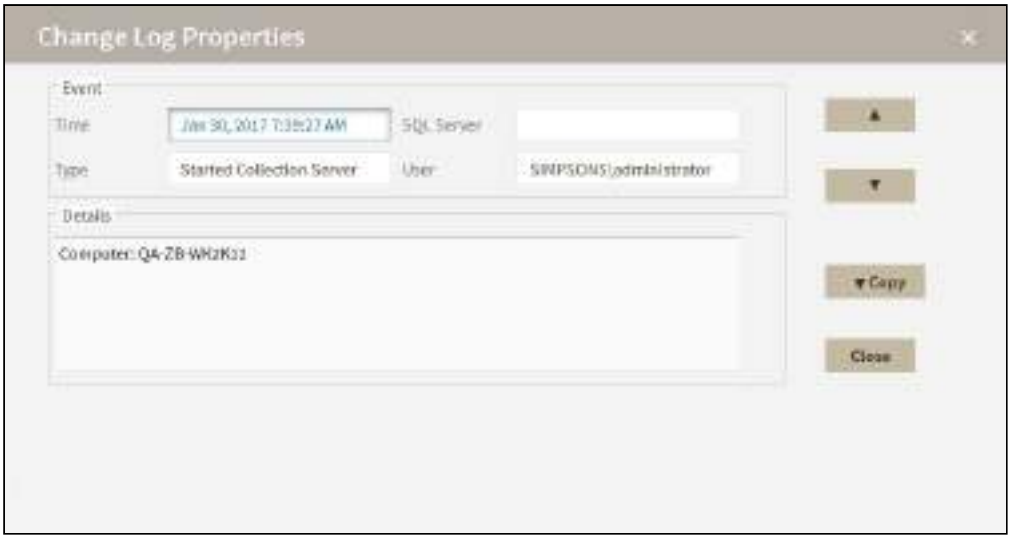
Change Log Properties

The Change Log Properties 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.



6.6 Generate audit reports

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The IDERA SQL Compliance Manager Audit Reports view contains a simple 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.

For additional information about SQL Compliance Manager reporting, see Report on Audit Data.

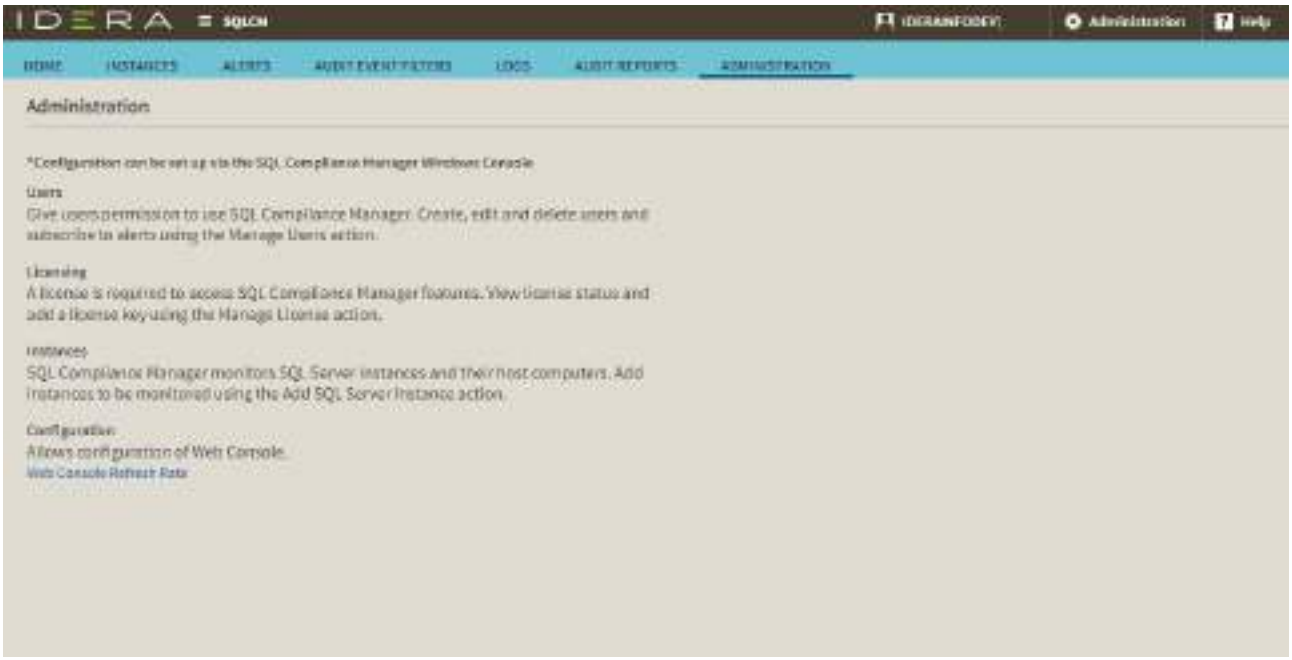
Available reports include:

- **Application Activity**. The Application Activity 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.
- **Configuration Check**. The Configuration Check report displays a list of all the configurations that are set up for your servers and databases.
- **DML Activity (Before-After)**. 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.
- **Login Creation History**. The Login Creation History report lists a history of login creation activities performed on a specific SQL Server instance. Use this report to audit user behavior and login management.
- **Login Deletion Histor**y. The Login Deletion History report lists a history of login deletion activities performed on a specific SQL Server instance. Use this report to audit user behavior and login management.
- **Object Activity**. The Object Activity report lists activities performed on a specific SQL Server instance. Use this report to audit object behavior and settings.
- **Permission Denied Activity**. The Permission Denied Activity report lists unauthorized attempts to execute activities. Use this report to audit your SQL Server security settings and identify misconduct.
- **Regulatory Compliance Check**. The Regulation Compliance Check report displays which servers or databases continue to be in compliance with the selected Regulation Guidelines.
- **Table/Data Access by Row Count.** The Row Count reports on the frequency data is accessed. Use this report to audit sensitive data access and identify suspicious behavior.
- **User Activity Histor**y. The User Activity History report lists activities performed by user account. Use this report to audit your user account settings and identify misconduct.

6.7 Administer SQL Compliance Manager

SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

The **Administration** tab gives you easy access to manage IDERA SQL Compliance Manager options such as users, licenses, and instances, which all must be added to SQL Compliance Manager if they are not already added.



The Administration tab allows users to Configure the Web Console refresh rate.

Users who want control of the Web Console refresh rate can manage the configuration using the Web Console Refresh Rate page. By default, the console refreshes every 30 seconds. The available range is between 30 and 3600 seconds.

To change the refresh rate, go to the **Administration** tab, and in the **Configuration** section, click **Web Console Refresh Rate**. Make the necessary change, and then click **Save**.

7 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.

7.1 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

	Task	Description	For more information ...
✓	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

5. 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

6. 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 Compliance Manager 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

7. 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

8. Archive events.

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

7.2 How auditing works

IDERA 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.

7.2.1 Complying with regulations

If you are subject to comply with regulations such as PCI DSS or HIPAA, you can use SQL Compliance Manager to configure your audit settings according to the specific guidelines of the regulation. SQL Compliance Manager 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 Compliance Manager. You can apply the regulation guideline audit settings to one or more databases on a registered SQL Server instance. For more information, see Comply with specific regulations.

7.2.2 Understanding traces

On each registered SQL Server instance, the SQL Compliance Manager 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 SQL Compliance Manager 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 Compliance Manager collects each event as separate audit data according to the SQL trace.

7.2.3 Using SQL Server Extended Events

IDERA SQL Compliance Manager 5.5 and later include 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.

7.2.4 Using SQL Server Audit Logs

IDERA SQL Compliance Manager 5.5 and later include support for event handling with SQL Server Audit Logs. This optional feature is available for use in auditing as an alternative to using SQL Server Extended Events or SQL Trace.

Auditing via Audit Logs offers the ability to track your alerts for Agents running SQL Server 2017 and later. For more information about using the Audit Logs option, see Using SQL Server Audit Logs.

7.2.5 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 SQL Compliance Manager Agent manage the trace files.

7.2.6 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.

7.2.7 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 or an entire server. As these users are trusted, the events generated by accounts are removed by the SQL Compliance Manager 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. Keep in mind that Server-level Trusted Users apply across all databases for that server, where the Database-level only applies to a particular database. For more information, see the Configuration wizard - Trusted Users window and the Registered SQL Server Properties window - Trusted User tab.

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 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.

7.2.8 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.

7.2.9 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, 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.

7.2.10 SQL Server events you can audit

IDERA 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 • Logouts • 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

Data Type	Events Audited	Description
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.

Database-level audit settings

You can specify which SQL events you want to audit at the database level. IDERA 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 Compliance Manager 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

Event class	SQL Server version	Description
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

Event class	SQL Server version	Description
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

Event class	SQL Server version	Description
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. IDERA 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.

⚠ Configurations applied at Server-level automatically apply across all databases for that server, showing items as checked and unavailable for deselection at the Database-level.

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

Event class	SQL Server version	Description
Audit Login	SQL Server 2000 and later	Records all successful logins on the registered SQL Server instance
Audit Logouts	SQL Server 2000 and later	Records all logouts 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

Event class	SQL Server version	Description
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

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.

7.2.11 Using SQL Server Extended Events

IDERA SQL Compliance Manager 5.4 and later allows you to take advantage of the SQL Server Extended Events (XEvents) feature to track and archive specific events occurring in your monitored environment. SQL Server Extended Events is an event handling system that offers lower overhead and delivers performance gains over the default SQL trace method. In SQL Compliance Manager 5.4 and later, only SELECT and DML events for SQL Server 2012 and later versions are supported by this feature. All functionality that works on top of these events, such as DML/Select filtering, Before-After data, sensitive column auditing, and more, work with this new method of capturing event data.

When Extended Events mode is enabled, events generate XEL files instead of trace files (.xel rather than .trc) but the files still are located in the Agent trace directory.

There are two ways to enable Extended Event capture:

- Through stored procedures.

- Through the Registered SQL Server Properties window - Audited Activities tab in the Windows Management Console.

> **Extended Events captures extra Execute events**
>
> **Due to differences in how Microsoft has implemented Extended Events compared to other auditing methods, when auditing via Extended Events the user will see extra Execute events as compared to the same data captured by other auditing methods.**

> **Extended Events does not Support Auditing a specific table/object**
>
> Due to technical limitations, Extended Events does not support auditing for a specific table/object. To audit a specific table/object please audit using SQL Trace or SQL Server Audit Logs.

Prerequisites and conditions for enabling auditing using Extended Events

IDERA SQL Compliance Manager supports Extended Events based auditing for SQL Server 2012 or above. The following prerequisites and conditions are required to switch auditing based on Extended Events.

- During installation
  - SQL Compliance Manager checks to make sure that Microsoft.SqlServer.XEvent.Linq.dll is available. If not, installation aborts.
- While enabling Extended Events from the web console
  - SQL Compliance Manager checks for the following conditions, which all must be met to successfully enable Extended Events:
    - Agent is reachable
    - SQL Server 2012 or above
    - SQL Compliance Manager Agent 5.4 or above
    - Microsoft.SqlServer.XEvent.Linq.dll is available (along with Microsoft.SqlServer.XE.Core.dll if Linq.dll is obtained from SQL Server SMO 2014 or 2016)

    Note that these conditions must be checked and confirmed manually if Extended Events is being enabled using a SQL stored procedure.

Enable Extended Event mode using stored procedures

To enable Extended Event mode using stored procedures, go to the location where the IDERA SQL Compliance Manager Console application is installed, and then execute the stored procedure `[dbo].[sp_enable_ExtendedEvents]`. For example:

```
EXEC [dbo].[sp_enable_ExtendedEvents] <SERVER_NAME>,<YES/NO>
```

Enable Extended Event mode using the Windows Management Console

Users wanting to take advantage of SQL Server Extended Events auditing capabilities can do so by completing the following steps:

1. Right-click the instance you want to audit and select **Properties**.
2. In the **Registered SQL Server Properties** window, select the **Audited Activities** tab.
3. Under the **Capture DML and Select activities** options, select the **Via Extended Events** option.
4. Click **OK**.

For more information about enabling this feature using the Windows Management Console, see Registered SQL Server Properties window - Audited Activities tab.

7.2.12 Using SQL Server Audit Logs

Starting IDERA SQL Compliance Manager 6.0 and above, the SQL Compliance Manager default Event Collection method is SQL Server Audit Specifications. Use the SQL Server Audit Logs feature to track specific events occurring in your monitored environment. SQL Server Audit Logs is an event-handling system that helps you reduce the size of data gathered and deliver performance gains over the default SQL trace method. In SQL Compliance Manager 5.5 and later, only SELECT and DML events for SQL Server 2017 and later versions are supported by this feature.

⚠ Upon version upgrade or new installation, the SQL Compliance Manager Event Collection method setting changes to "SQL Server Audit Specifications" by default. Users can manually change the collection method.

⚠ Before and After Data is not supported on the RDS instance due to the limitation of creating trusted assemblies using SQL script. BAD operations are removed from the properties, reports, alerts, and summary tabs.

To manually change the capturing events method, go to:

- The Registered SQL Server Properties window - Audited Activities tab in the Windows Management Console.

Prerequisites and conditions for enabling auditing using Audit Logs

IDERA SQL Compliance Manager supports Audit Logs based auditing for SQL Server 2017 and above. The following prerequisites and conditions are required to switch auditing based on Audit Logs.

- While enabling Audit Logs from Web or Windows Management console.
    - SQL Compliance Manager checks for the following conditions, which all must be met to successfully enable Audit Logs:
        - The Agent is reachable.
        - SQL Server 2017 or above.
        - SQL Compliance Agent 5.5 or above.

Enable Audit Logs mode using the Windows Management Console

Users wanting to take advantage of SQL Server Audit Logs auditing capabilities can do so by completing the following steps:

1. Right-click the instance you want to audit and select **Properties**.
2. In the **Registered SQL Server Properties** window, select the **Audited Activities** tab.
3. Under the **Capture DML and Select activities** options, select the **Via SQL Server Audit Specifications** option.
4. Click **OK**.

For more information about enabling this feature using the Windows Management Console, see Registered SQL Server Properties window - Audited Activities tab.

7.2.13 Comply with specific regulations

IDERA SQL Compliance Manager audits and identifies events that affect SQL Server objects and data. By selecting a specific regulation guideline set, SQL Compliance Manager applies audit settings to your selected databases according to the corresponding data security rules. This audited data is collected and securely stored for forensic

analysis and reporting. SQL Compliance Manager 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 through the Console or CLI. The following tables list each section of a regulation and the associated SQL Server events that SQL Compliance Manager 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 ensure 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.

All Regulation Guidelines are available at both, the server level and the database level, except for the CIS Regulation Guideline.
The CIS Regulation Guideline can be applied only at the server level.

CIS Compliance

Section	Summary	Associated Audit Events and Features
5.4	Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'. SQL Server Audit is capable of capturing both failed and successful logins and writing them to one of three places: the application event log, the security event log, or the file system. We will use it to capture any login attempt to SQL Server, as well as any attempts to change audit policy. This will also serve as a second source to record failed login attempts.	Server Events: • Logins • Logouts • Failed Logins Database Events: • None

When selecting CIS regulation, default database level settings automatically apply. Logins and Failed Logins get captured to comply with this regulation and continue auditing the server.

DISA/STIG Compliance

Section	Summary	Associated Audit Events and Features
DISA 2016 Database **DISA 2016 Instance** SQL6-D0-004300, SQL6-D0-004500, SQL6-D0-004700, SQL6-D0-004800, SQL6-D0-005500, SQL6-D0-005900, SQL6-D0-006000, SQL6-D0-006100, SQL6-D0-006200, SQL6-D0-006300, SQL6-D0-006400, SQL6-D0-010700, SQL6-D0-010800, SQL6-D0-011100, SQL6-D0-011200	SQL Server must be configured to generate audit records for DoD-defined auditable events within all DBSM/database components. SQL Server must generate audit records when privileged/ permissions are retrieved. SQL Server must initiate session auditing upon startup. SQL Server must be configured to allow authorized users to capture, record, and log all content related to a user session. SQL Server must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject. The audit information produced by SQL Server must be protected from unauthorized read access. The audit information produced by SQL Server must be protected from unauthorized modification. The audit information produced by SQL Server must be protected from unauthorized deletion. SQL Server must protect its audit features from unauthorized access. SQL Server must protect its audit configuration from unauthorized modification. SQL Server must protect its audit features from unauthorized removal. SQL Server must utilize centralized management of the content captured in audit records generated by all components of SQL Server. SQL Server must provide an immediate real-time alert to appropriate support staff of all audit failure events requiring real-time alerts. SQL Server must record time stamps in audit records and application data that can be mapped to Coordinate Universal Time (UTC, formerly GMT).	Server Events: • Successful and Failed Logins • Security Changes • Privileged User Activity • User Defined Event Tracking Database Events: • Security changes • SELECT statements • Privileged User Activity • Sensitive Column Monitoring • Before-After Data Auditing

Section	Summary	Associated Audit Events and Features
DISA 2012 Database SQL2-00-011200 **DISA 2014 Database** SQL4-00-011200	SQL Server must generate Trace or audit records for organization-defined auditable events. Audit records can be generated from various components within the information system.	Server Events: • None Database Events: • Security • DDL • DML • Privileged Users Events • Privileged Users • Sensitive Columns • Before-After Data auditing

Section	Summary	Associated Audit Events and Features
DISA 2012 Instance SQL2-00-012400, SQL2-00-009700, SQL2-00-011800, SQL2-00-011900, SQL2-00-011400, SQL2-00-012000, SQL2-00-012100, SQL2-00-012200, SQL2-00-012300, SQL2-00-014700, SQL2-00-002300 **DISA 2014 Instance** SQL4-00-011900, SQL4-00-012000, SQL4-00-012100, SQL4-00-012200, SQL4-00-012300, SQL4-00-037600, SQL4-00-037900, SQL4-00-037500, SQL4-00-037600, SQL4-00-037900, SQL4-00-038000, SQL4-00-011200, SQL4-00-036200, SQL4-00-036300, SQL4-00-038100, SQL4-00-034000	SQL Server must include organization-defined additional, more detailed information in the audit records for audit events identified by type, location or subject. Audit record content which may be necessary to satisfy the requirement of this control includes: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, file names involved, and access control or flow control rules revoked. All use of privileged accounts must be audited. SQL Server must produce audit records containing sufficient information to establish what type of events occurred. SQL Server must produce audit records containing sufficient information to establish when (date and time) the events occurred. SQL Server must generate audit records for the DoD-selected list of auditable events. SQL Server must produce audit records containing sufficient information to establish where the events occurred. SQL Server must produce audit records containing sufficient information to establish the sources (origins) of events. SQL Server must produce audit records containing sufficient information to establish the outcome (success or failure) of events. SQL Server must produce audit records containing sufficient information to establish the identity of any user/subject associated with the event. SQL Server must support the employment of automated mechanisms supporting the auditing of the enforcement actions. SQL Server must enforce access control policies to restrict Alter server state permissions to only authorized roles. SQL Server must generate Trace or audit records when unsuccessful logins or connection attempts occur. SQL Server must generate Trace or audit records when logoffs or disconnections occur. SQL Server must generate Trace or audit records when successful logons or connections occur. SQL Server must generate Trace or audit records when concurrent logins/connections by the same user from different workstations occur.	Server Events: • Logins • Logouts • Failed Logins • Security changes • Privileged Users activity • User defined events • Privileged Users Database Events: • None

Section	Summary	Associated Audit Events and Features
	SQL Server must produce Trace or audit records containing sufficient information to establish when the events occurred. SQL Server must produce Trace or audit records of its enforcement of access restrictions associated with changes to the configuration of the DBMS or database.	
DISA 2014 0	If SQL Server authentication, using passwords, is employed, SQL Server must enforce the DoD standards for password lifetime.	Server Events: • Security changes Database Events: • Security

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

Section	Summary	Associated Audit Events and Features
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

Section	Summary	Associated Audit Events and Features
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

Section	Summary	Associated Audit Events and Features
99.35 (a)(1)(2), (b)(1)	**What conditions apply to disclosure of information for Federal or State program purposes?** Authorized representatives of the officials or agencies headed by officials listed in 99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. Authority for an agency or officially listed in § 99.31(a)(3) to conduct an audit, evaluation, or compliance or enforcement activity is not conferred by the Act or this part and must be established under other Federal, State, or local authority. Information that is collected under paragraph (a) of this section must: • Be protected in a manner that does not permit personal identification of individuals by anyone other than the officials or agencies headed by officials referred to in paragraph (a) of this section, except that those officials and agencies may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of 99.33(b).	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • DDL • Sensitive Columns • SELECT statements

GDPR Compliance

Section	Summary	Associated Audit Events and Features
Article 5	**Principles relating to processing of personal data** 1. Personal data shall be: a. processed lawfully, fairly and in a transparent manner in relation to the data subject (´lawfulness, fairness and transparency´); b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (´purpose limitation´); c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (´data minimisation´); d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (´accuracy´); e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (´storage limitation´); f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (´integrity and confidentiality´). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (´accountability´).	Server Events: • Privileged User - DDL • Privileged User - DML Database Events: • Privileged User - DDL • Privileged User - DML
Article 13 (1, e)	**Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: e. the recipients or categories of recipients of the personal data, if any;	Server Events: • None Database Events: • Sensitive Column Auditing • Before-After Data

Section	Summary	Associated Audit Events and Features
Article 24	**Responsibility of the controller** 1. [1]Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [2]Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.	Server Events: • Logins • Failed Logins Database Events: • None
Article 25(2)	**Data protection by design and by default** 2. [1]The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2]That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual´s intervention to an indefinite number of natural persons.	Server Events: • Logins Database Events: • Sensitive Column Auditing • Before-After Data • Privileged Logins

Section	Summary	Associated Audit Events and Features
Article 30 (1)	**Records of processing activities** 1. [1]Each controller and, where applicable, the controller´s representative, shall maintain a record of processing activities under its responsibility. [2]That record shall contain all of the following information: a. the name and contact details of the controller and, where applicable, the joint controller, the controller´s representative and the data protection officer; b. the purposes of the processing; c. a description of the categories of data subjects and of the categories of personal data; d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; f. where possible, the envisaged time limits for erasure of the different categories of data; g. where possible, a general description of the technical and organisational security measures referred to in Article 32 (1).	Server Events: • None Database Events: • Sensitive Columns • Before-After Data Change

Section	Summary	Associated Audit Events and Features
32(2)	**Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a. the pseudonymisation and encryption of personal data; b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Server Events: • None Database Events: • Sensitive Column Auditing • Before-After Data

Section	Summary	Associated Audit Events and Features
Article 33	**Notification of a personal data breach to the supervisory authority** 1. [1]In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c. describe the likely consequences of the personal data breach; d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5. [1]The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [2]That documentation shall enable the supervisory authority to verify compliance with this Article.	Server Events: • Logins • Failed Logins Database Events: • Privileged Users
Article 35(7)	**Data protection impact assessment** 7. The assessment shall contain at least: a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Server Events: • None Database Events: • Sensitive Column Auditing

Section	Summary	Associated Audit Events and Features
Recital 39	**Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; d. to cooperate with the supervisory authority; e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. 2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing,	Server Events: • None Database Events: • Sensitive Column Auditing • Before-After Data

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

Section	Summary	Associated Audit Events and Features
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

Section	Summary	Associated Audit Events and Features
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: • 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

Section	Summary	Associated Audit Events and Features
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

Section	Summary	Associated Audit Events and Features
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

NERC-CIP Compliance

Section	Summary	Associated Audit events and Features
CIP-007-6 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: detected successful login attempts, detected failed access attempts and failed login attempts; and detected malicious code.	Server Events: • Logins • Logouts • Failed Logins • Security changes • User Defined Events • Privileged Users • Privileged Users events Database Events: • Security changes • DDL • DML • Sensitive Columns • Before-After Data change • Privileged Users

PCI DSS Compliance

Section	Summary	Associated Audit Events and Features
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Server Events: • Failed Logins • Security Changes • DDL • Administrative activities • Privileged Users • User defined events Database Events: • Security • DDL • Administrative activities • DML • SQL statements • Sensitive columns • Before-After data change • Privileged users
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures.	
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	

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

Section	Summary	Associated Audit Events and Features
10.1	Implement audit trails to link all access to system components 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, stopping, or pausing of the 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 Compliance Manager 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 the 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: • Logins • Logouts • Failed Logins • Security Changes • 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
404 CDC	Implement change data capture.	Server Events: • None Database Events: • Sensitive columns • Before-After data change

7.2.14 Control data access using Row Count

> ⚠ In SQL Compliance Manager version 5.6.1 the Row count functionality may show as “Not Applicable”. The issue occurs when you execute large query and during execution the start and the end of the SQL Statement get captured in different trace files. Since both events are located in different trace files, SQL CM is not able to map these events and therefore displays that Row count is “Not Applicable”.
> Users can increase the time of collection (default is set to 60 seconds) to capture Row count correctly

> ⚠ This feature is only **available** for SQL Server 2008 and above.

> ⚠ To capture row count information, **update** the SQL Compliance Manager Agent to version **5.5** or above.

IDERA SQL Compliance Manager audits and reports on the frequency that users access sensitive data, alerting about suspicious behavior.

The row count feature allows users to:

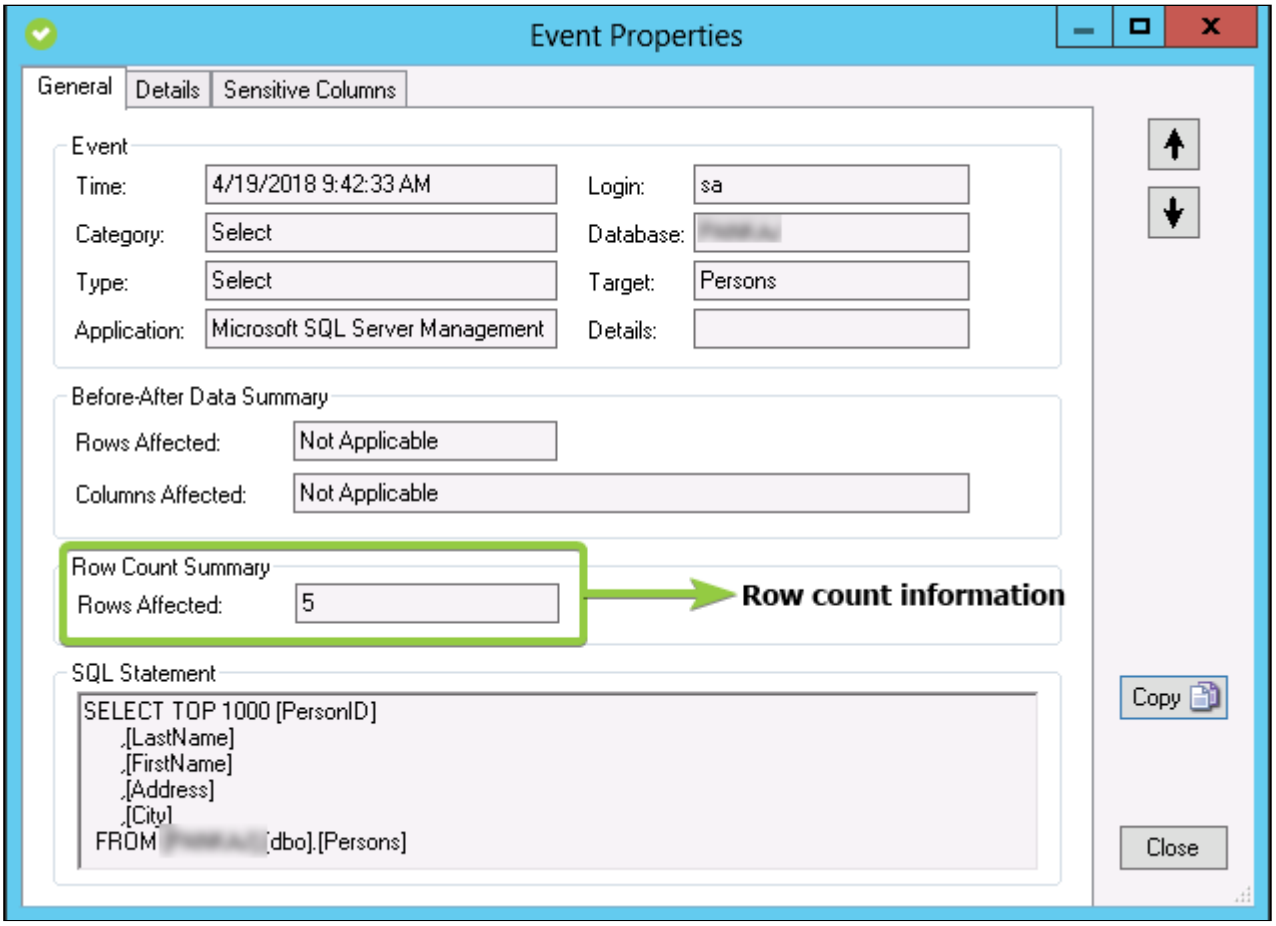
- Audit and capture row count for all event types and SQL statements.
- Audit and capture row count for joined query statements.
- Report on row count and access sensitive data.
- Set alerts based on thresholds for row counts, users, sensitive data, and specific queries.

Row count information is captured as part of an audit event and gathers information from both, traces and extended events.

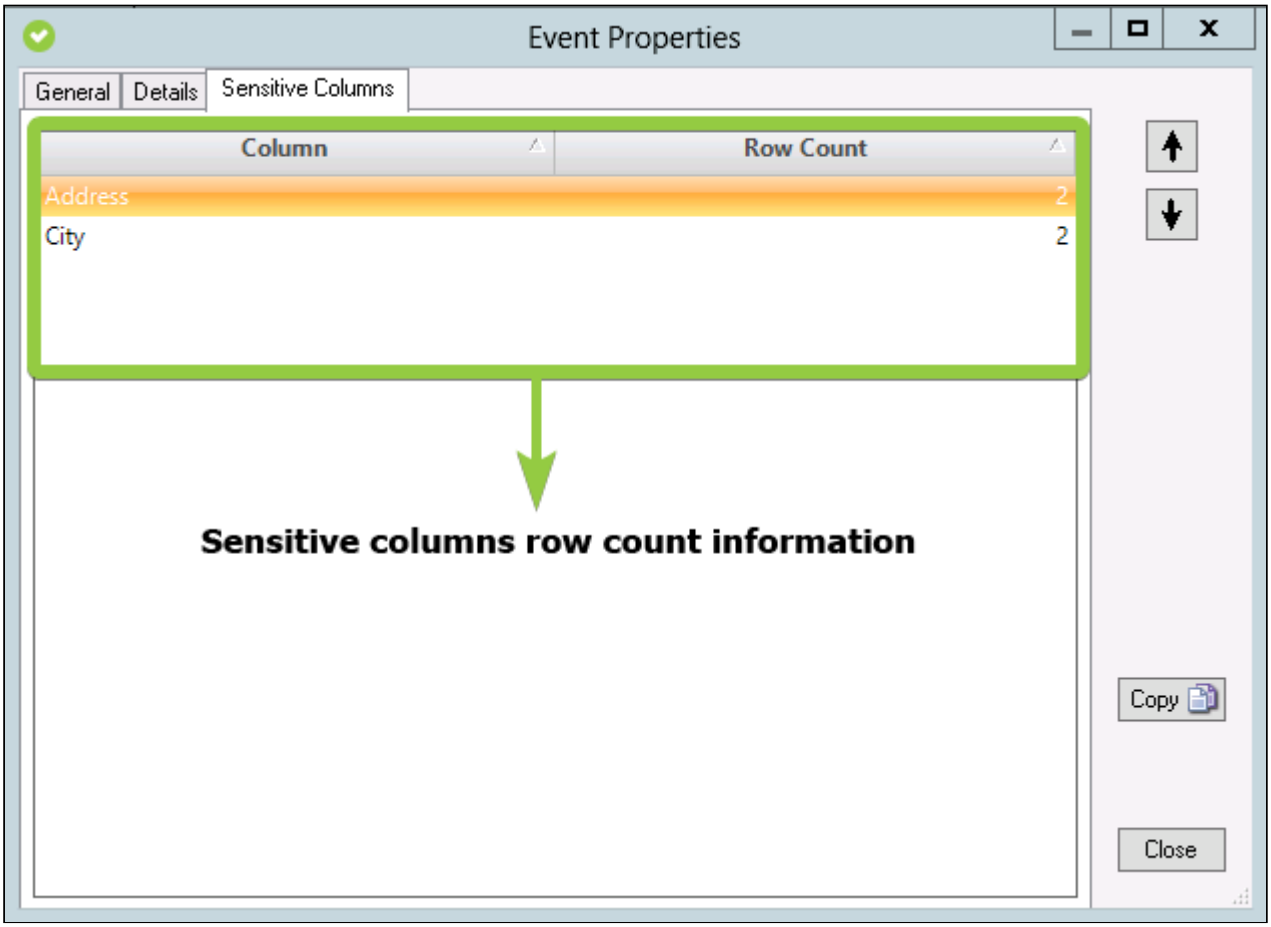
> ⚠ Row count information does not show when capturing DML and SELECT activities using SQL Server audit specifications.

See row count information

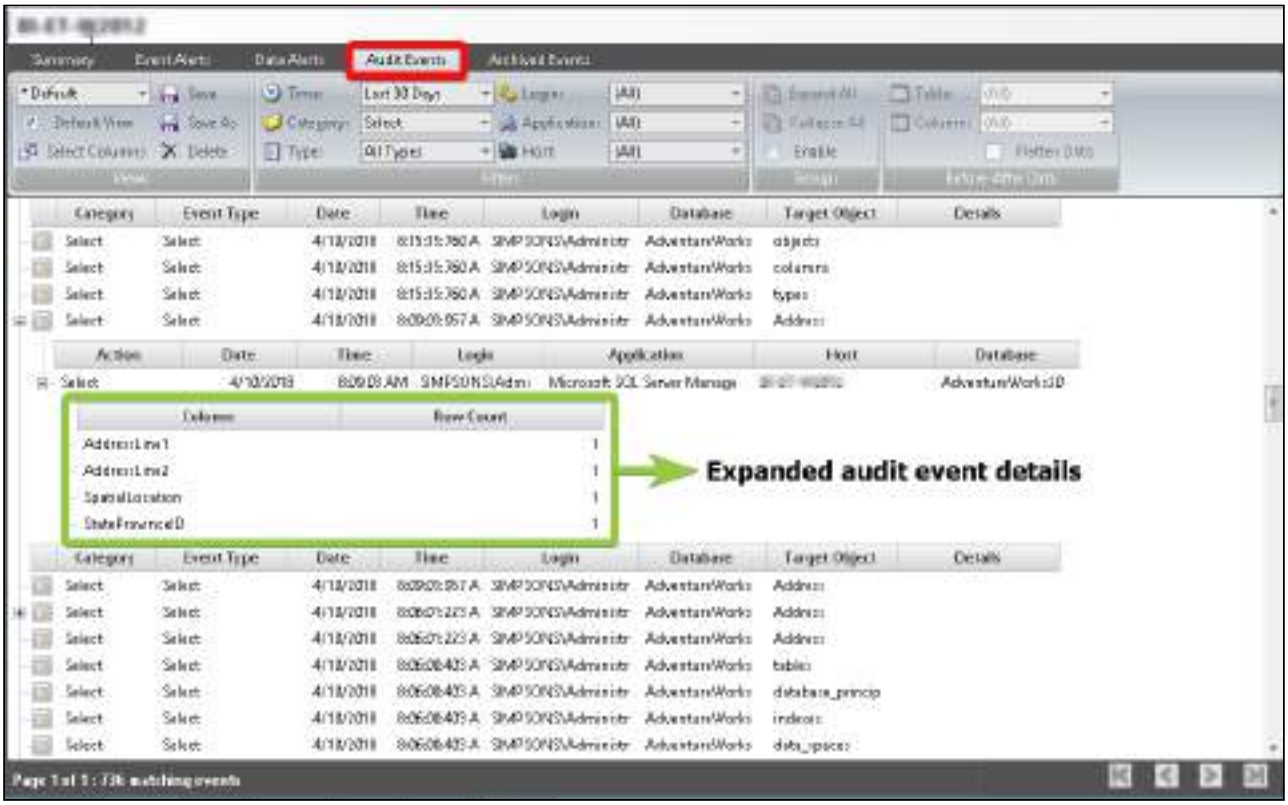
The row count information is available in the General tab of any event properties, as well as the Audit Events tab in the Explore Activity View.



For select statements with sensitive columns, event properties contain a Sensitive Columns tab which shows the row count value for each audited sensitive column.



When you expand the audit events, the Audit Events tab shows the row count information in the event details.

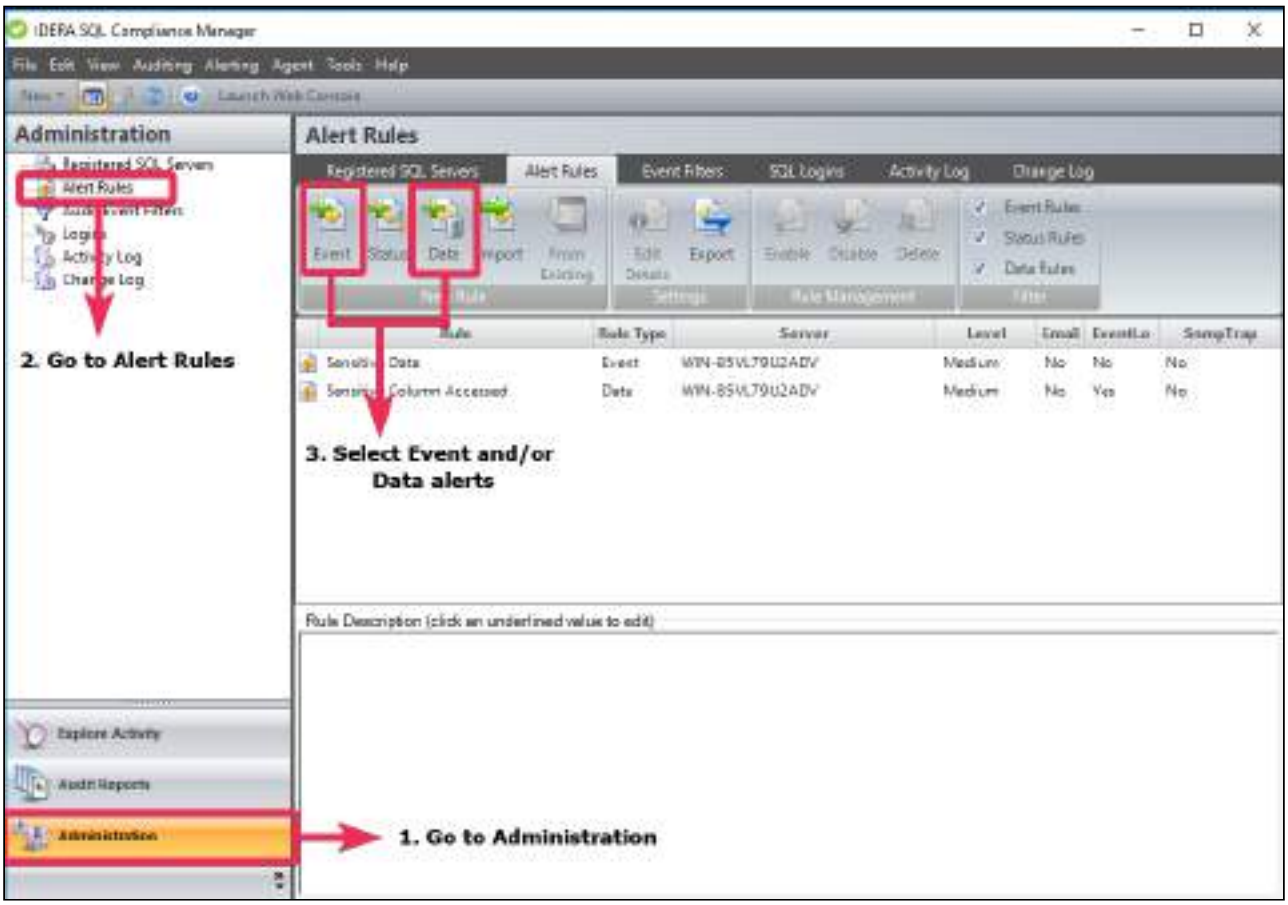


If you use SQL statements with joined queries, SQL Compliance Manager displays multiple (equivalent to the number of distinct queries joined) events, however, row count information is available only with the primary statement and not applicable with other statements.

Row count Alerts

IDERA SQL Compliance Manager allows you to set alerts on row count and data access. Alerts can be set by row count alone or adding a specific time interval.

For more information, see Alert on Audit Data and Status.

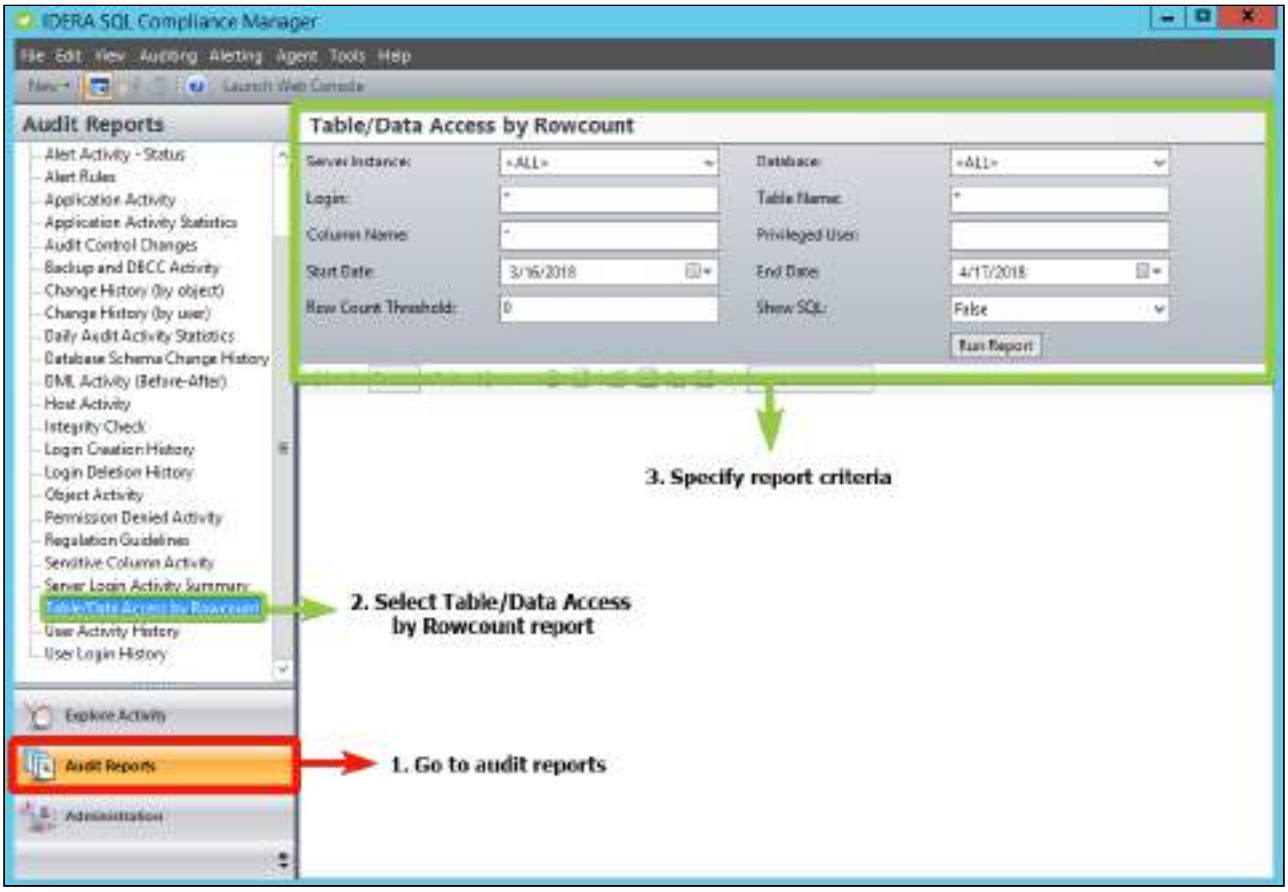


If you use SQL statements with joined queries, only the primary statement triggers any alert set for row count.

Row count Reports

IDERA SQL Compliance Manager allows you to generate reports on data access, including the new row count feature. You can generate reports with the SQL Compliance Manager console and with Reporting Services.

For more information, see Report on Audit Data.



7.2.15 Event Auditing Matrix

IDERA SQL Compliance Manager offers different auditing options, each option allows you to audit specific types of SQL Server event data.

> If you choose to audit via Extended Events or Audit Logs, the unavailable information will be gathered from the Trace Events.

Depending on your auditing selection SQL Compliance Manager allows you to capture the following types of event data.

Event	Trace Events (.trc)	Extended Events (.xel)	Audit Logs (.audit)
ApplicationName	Available	Available	Unavailable
ColumnPermissions	Available	Unavailable	Available
BeforeAfter	Available	Available	Unavailable

Event	Trace Events (.trc)	Extended Events (.xel)	Audit Logs (.audit)
DatabaseID	Available	Available	Available
DatabaseName	Available	Available	Available
DBUserName	Available	Unavailable	Available
EventClass	Available	Available	Available
EventSequence	Available	-	Available
EventSubClass	Available	Available	Available
FileName	Available	Unavailable	Available
HostName	Available	Available	Unavailable
IsSystem	Available	Available	Unavailable
LinkedServerName	Available	Unavailable	Unavailable
LoginName	Available	Available	Available
NestLevel	Available	Available	Available
ObjectID	Available	Unavailable	Available
ObjectName	Available	Unavailable	Available
ObjectType	Available	Unavailable	Available
OwnerName	Available	Unavailable	Unavailable
ParentName	Available	Unavailable	Unavailable
Permissions	Available	Unavailable	Available
ProviderName	Available	Unavailable	Unavailable

Event	Trace Events (.trc)	Extended Events (.xel)	Audit Logs (.audit)
RoleName	Available	Unavailable	Unavailable
RowCounts	Available	Available	Unavailable
ServerName	Available	Available	Available
SessionLoginName	Available	Available	Available
SPID	Available	Available	Available
StartTime	Available	Available	Available
Success	Available	Unavailable	Available
TargetLoginName	Available	Unavailable	Available
TargetUserName	Available	Unavailable	Available
TextData	Available	Available	Available

Extended Events captures extra Execute events

Due to differences in how Microsoft has implemented Extended Events compared to other auditing methods, when auditing via Extended Events the user will see extra Execute events as compared to the same data captured by other auditing methods.

NOTE

- The Extended Events auditing feature is only available with SQL Server 2012 and newer.
- The Audit Logs auditing feature is only available with SQL Server 2017 and newer.

SQL Compliance Manager Calculated Columns

Depending on your auditing selection SQL Compliance Manager allows you to capture the following calculated columns event data type.

Event	Trace Events (.trc)	Extended Events (.xel)	Audit Logs (.audit)
alertLevel	Available	Available	Available

Event	Trace Events (.trc)	Extended Events (.xel)	Audit Logs (.audit)
appNameId	Available	Available	Unavailable
details	Available	Unavailable	Available
endSequence	Available	Available	Available
endTime	Available	Available	Available
eventCategory	Available	Available	Available
hash	Available	Available	Available
hostId	Available	Available	Unavailable
loginId	Available	Available	Available
privilegedUser	Available	Available	Available
startSequence	Available	Available	Available
targetObject	Available	Unavailable	Available

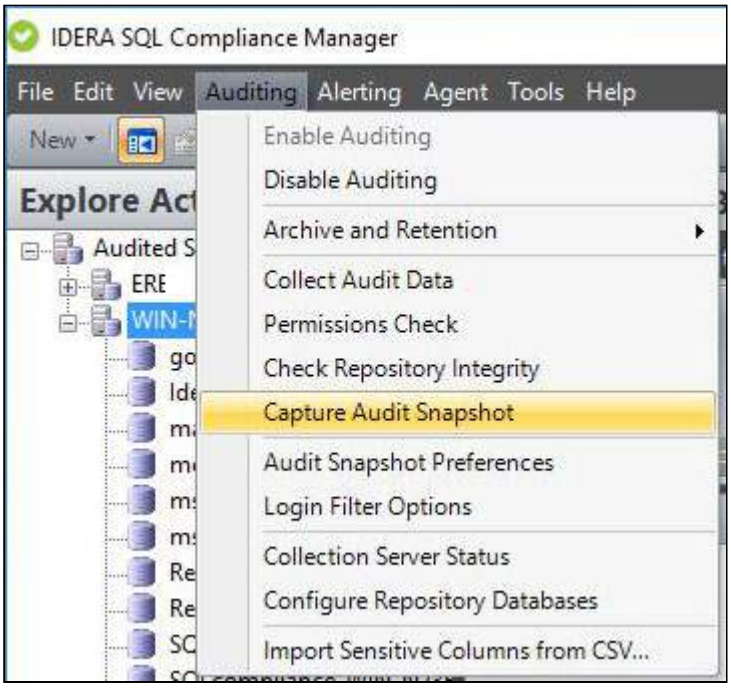
7.3 Audit snapshots

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.

7.3.1 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:

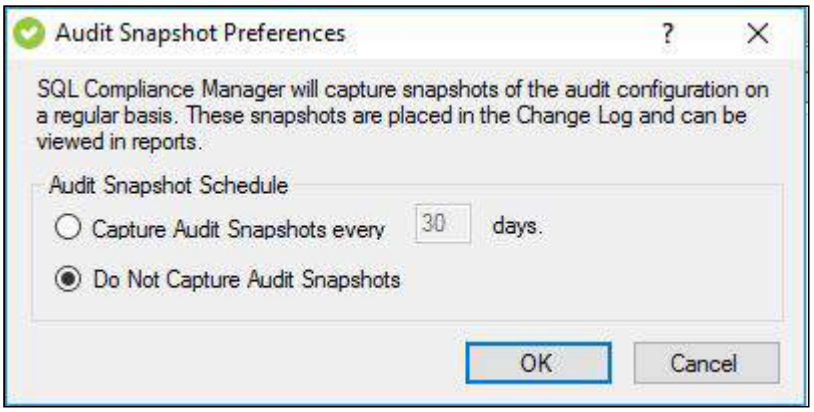
1. Click **Auditing** on the menu bar, and then select **Capture Audit Snapshot**.
2. Specify whether you want a snapshot of audit settings for all registered SQL Server instances or for a specific instance, and then click **OK**.
3. Review the newly captured snapshot.

7.3.2 Schedule an audit snapshot

You can schedule IDERA SQL Compliance Manager to take a snapshot of your audit settings at a routine interval (in days), or you can configure SQL Compliance Manager 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**.



7.3.3 View the audit snapshot

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

To view the audit snapshot:

1. Select the **Change Log** option 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**.

7.4 Control access to audit data

You can control who can access audit data by granting the appropriate IDERA 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.

7.5 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.

7.5.1 Use the SQL Compliance Manager 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 Compliance Manager 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 Compliance Manager 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 Compliance Manager 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 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.
8. Click **Finish**.

7.5.2 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.

7.5.3 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 SQL Compliance Manager 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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"`.

7.5.4 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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 Compliance Manager setup program to manually deploy the SQL Compliance Manager 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"`.

7.6 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**.

7.7 Enable automatic failover using AlwaysOn Availability Groups

The AlwaysOn Availability Groups feature uses the availability of a set of databases within your enterprise to improve your failover options and general availability. This feature makes the database highly available using the Windows Failover Cluster Service for Windows Server 2008 and above. As a result, this feature requires Windows Failover Cluster as well as SQL Server on all cluster nodes.

When an availability group is configured using multiple SQL Servers, one of the servers is designated as the PRIMARY node and others are considered SECONDARY nodes. If the primary node SQL Server stops or shuts down, the failover automatically switches to the synchronized secondary node with no data loss. You also can manually perform a failover on the SQL Server.

SQL Compliance Manager provides auditing of the AlwaysOn-configured database and audits the events on the AlwaysOn database along with the failovers.

> The AlwaysOn Availability Groups feature is available for SQL Server 2012 and above only.

7.7.1 How AlwaysOn integrates with SQL Compliance Manager

There are two scenarios of how SQL Compliance Manager can work with AlwaysOn availability group databases:

- Listener. Use this scenario when you want to audit a listener (virtual SQL server instance) that works only with a node in the PRIMARY role.
- Nodes. Use this scenario when you want to audit every node that can be in PRIMARY or SECONDARY roles. Note that the secondary role is read-only.

> You can use only one scenario at a time, it is not possible to use both of them at the same time on a cluster.

> Each node of the SQL Server instance used in the AlwaysOn Availability Group must have a license.

Review the following links to configure AlwaysOn Availability Groups:

Configuring Listener scenario:

1. Install cluster agent services on all Listener nodes using the SQL Compliance Manager Cluster Configuration Console
2. Install cluster agent services on all Listener nodes using the Failover Cluster Manager
3. Add the Listener to SQL Compliance Manager

Configuring Nodes scenario:

- Manually deploy the SQL Compliance Manager Agent

Ensure to review additional information to start working with AlwaysOn Availability Groups:

- Removing a Listener from SQL Compliance Manager
- Exporting/importing audit settings for all AlwaysOn nodes
- Removing an AlwaysOn node from SQL Compliance Manager

7.7.2 Configuring Listener scenario

The Listener scenario is recommended for users who want to audit only AlwaysOn databases on the Primary node of the Availability Group by registering the Availability Group Listener for auditing in SQL Compliance Manager. ***If you want to audit read-only Secondary nodes***, use the Nodes scenario instead.

Review the following steps to successfully configure your Availability Group Listener for auditing:

1. Install the clustered Agent service on all Availability Group nodes using the SQL Compliance Manager Cluster Configuration Console.
2. Create a clustered resource for the newly installed Agent service in Failover Cluster Manager.
3. Register the Availability Group Listener in SQL Compliance Manager.

1. Install the cluster Agent service on all Availability Group nodes using the SQL Compliance Manager Cluster Configuration Console

Use the following steps on each node involved in the AlwaysOn group before adding the listener to SQL Compliance Manager for auditing.

> ⚠ Before stepping through the following instructions, ensure that the SQL CM Collection Server, the Management Console, and the Repository Databases are already installed.
>
> - Please review step 10 in How to install SQL Compliance Manager to install these components in a standalone server.
> - Please review the steps to Install SQL Compliance Manager Collection Service on Cluster nodes to install these components in a clustered environment.

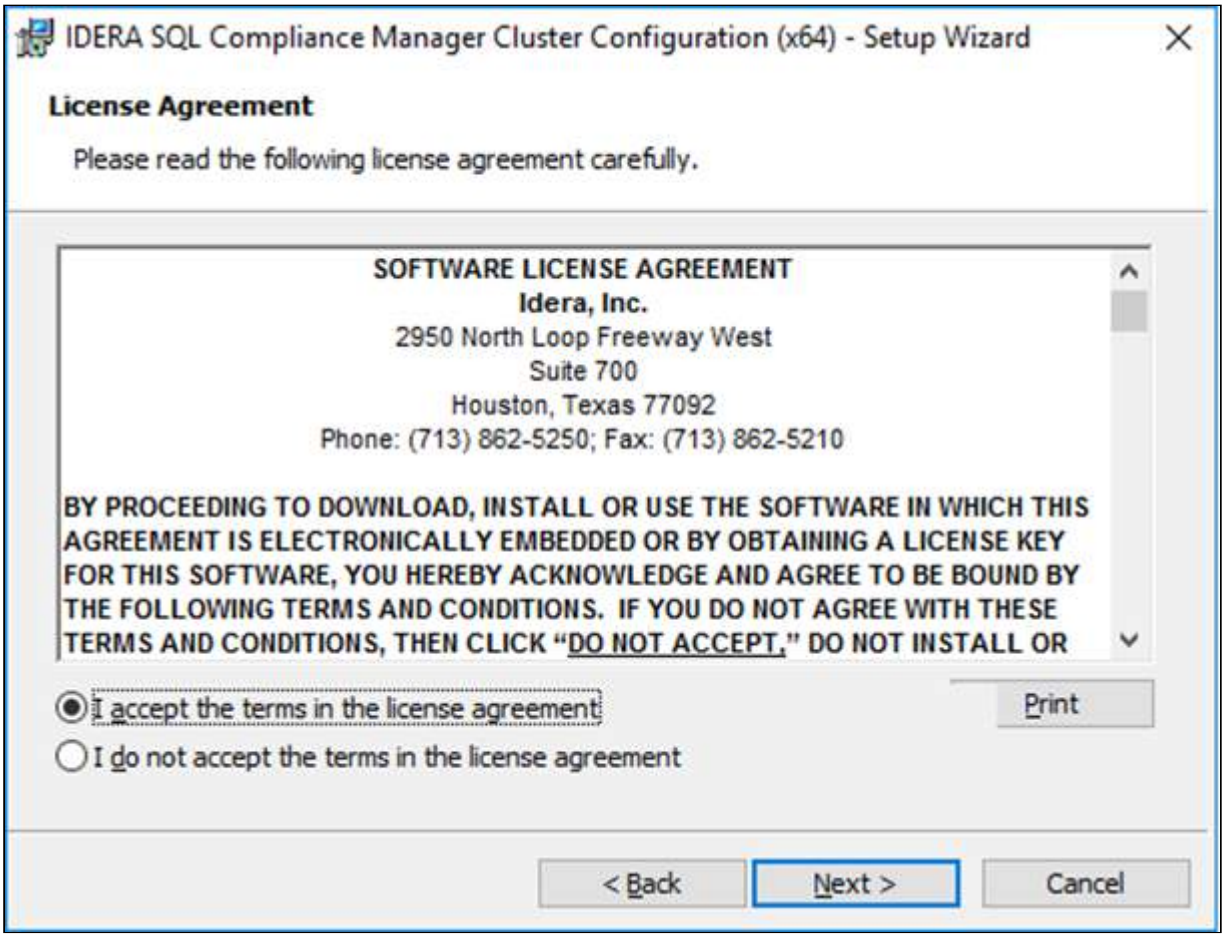
1. From the installation folder of the SQL Compliance Manager Collection Service on the Collection and Repository database server, copy the *SQLComplianceClusterSetup.exe* file onto the nodes of the Availability Group. To install the Cluster Configuration Console on the nodes of the Availability Group, you are going to be auditing. This is located by default at the following path:

   C:\Program Files\Idera\SQLcompliance

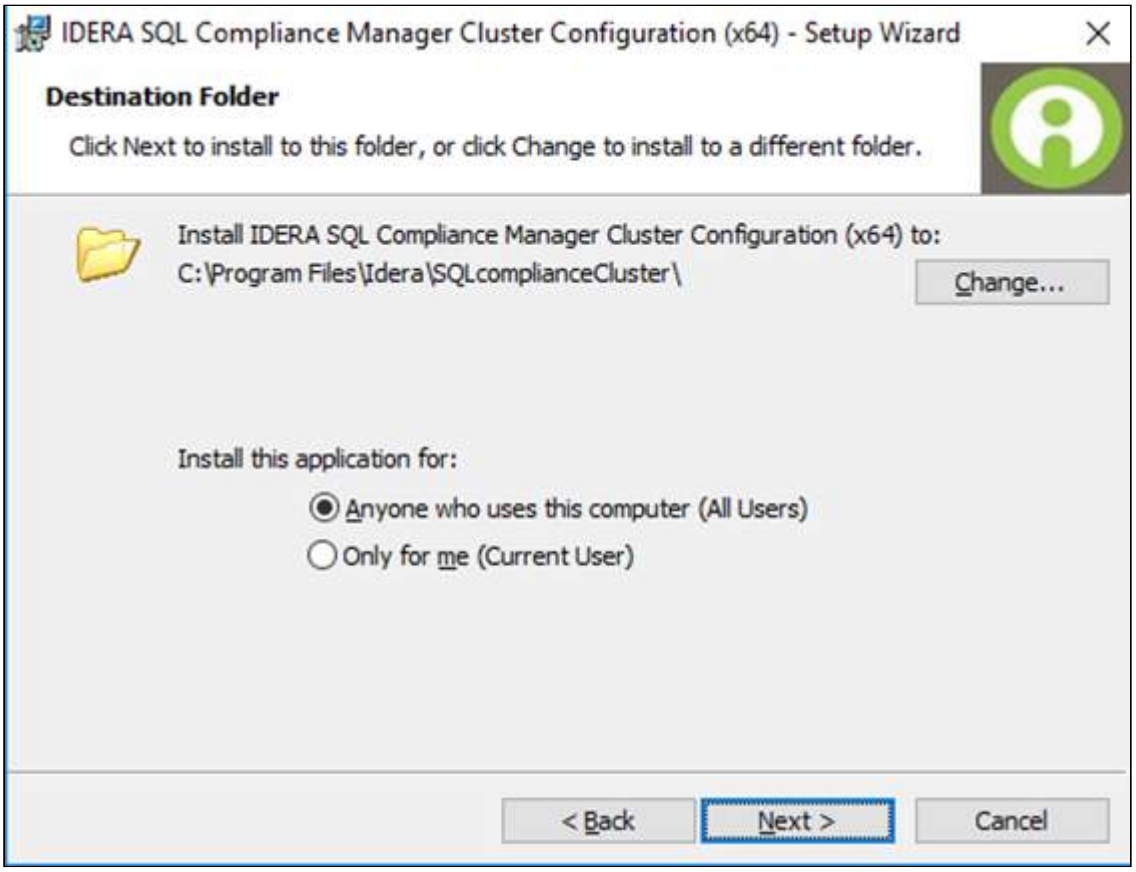
2. Beginning with the primary node of the Availability Group. Run the *SQLcomplianceClusterSetup.exe* to launch the installation wizard.

3. Once the setup wizard launches, click the **Next** button to proceed to the License Agreement.

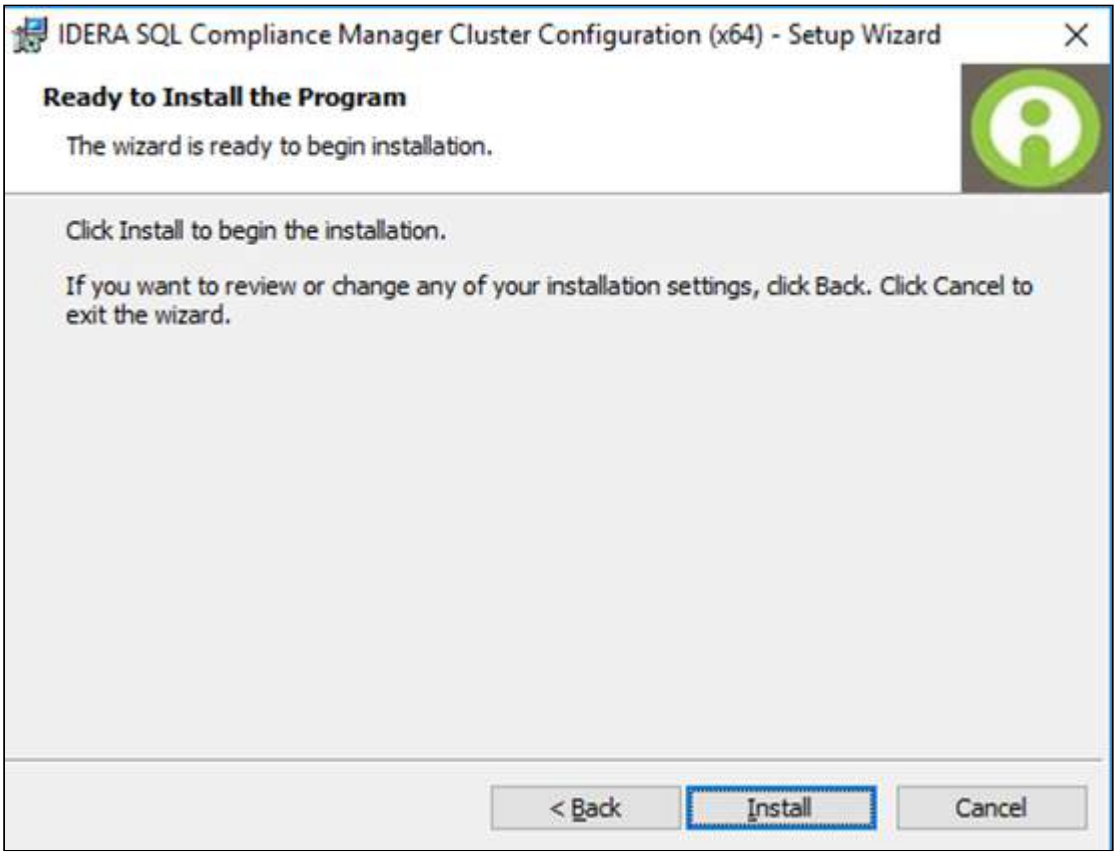
4. Read the license agreement, select the option to accept the license agreement terms, and click **Next**.



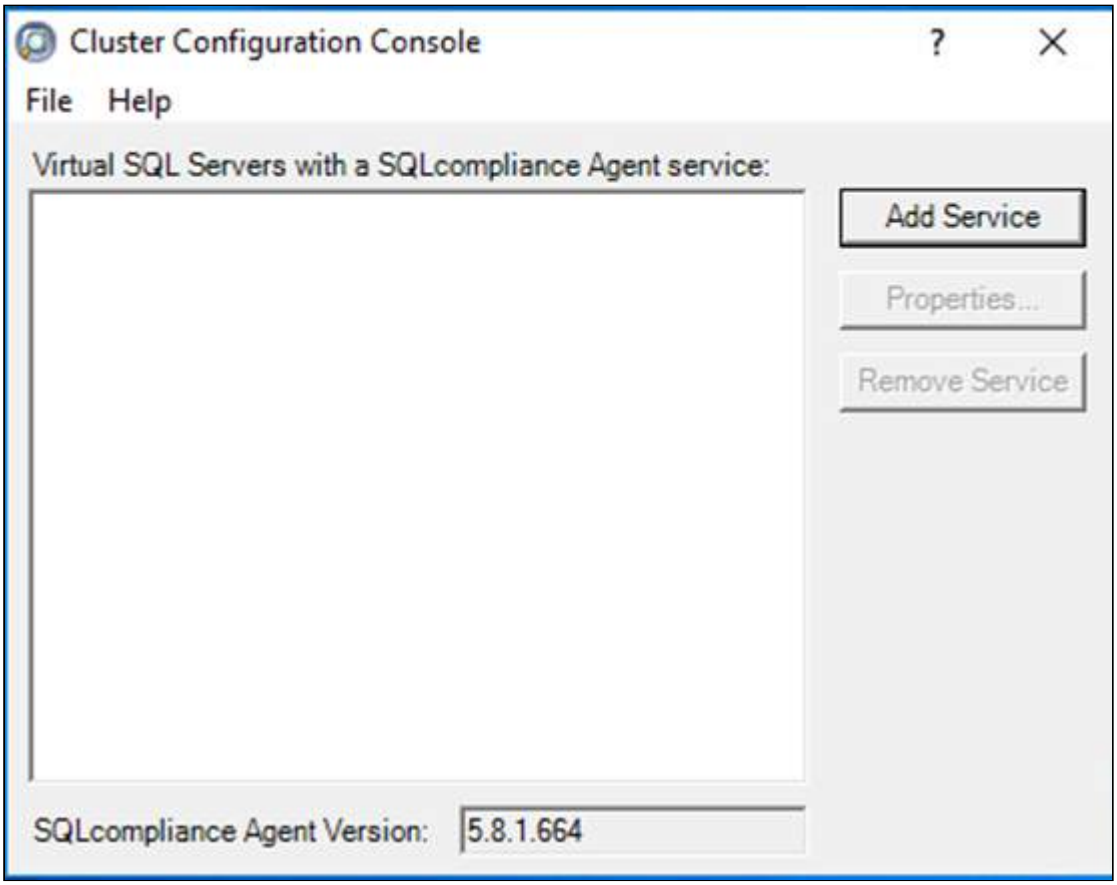
5. Select the destination path in which you want to install the IDERA Cluster Configuration Console.



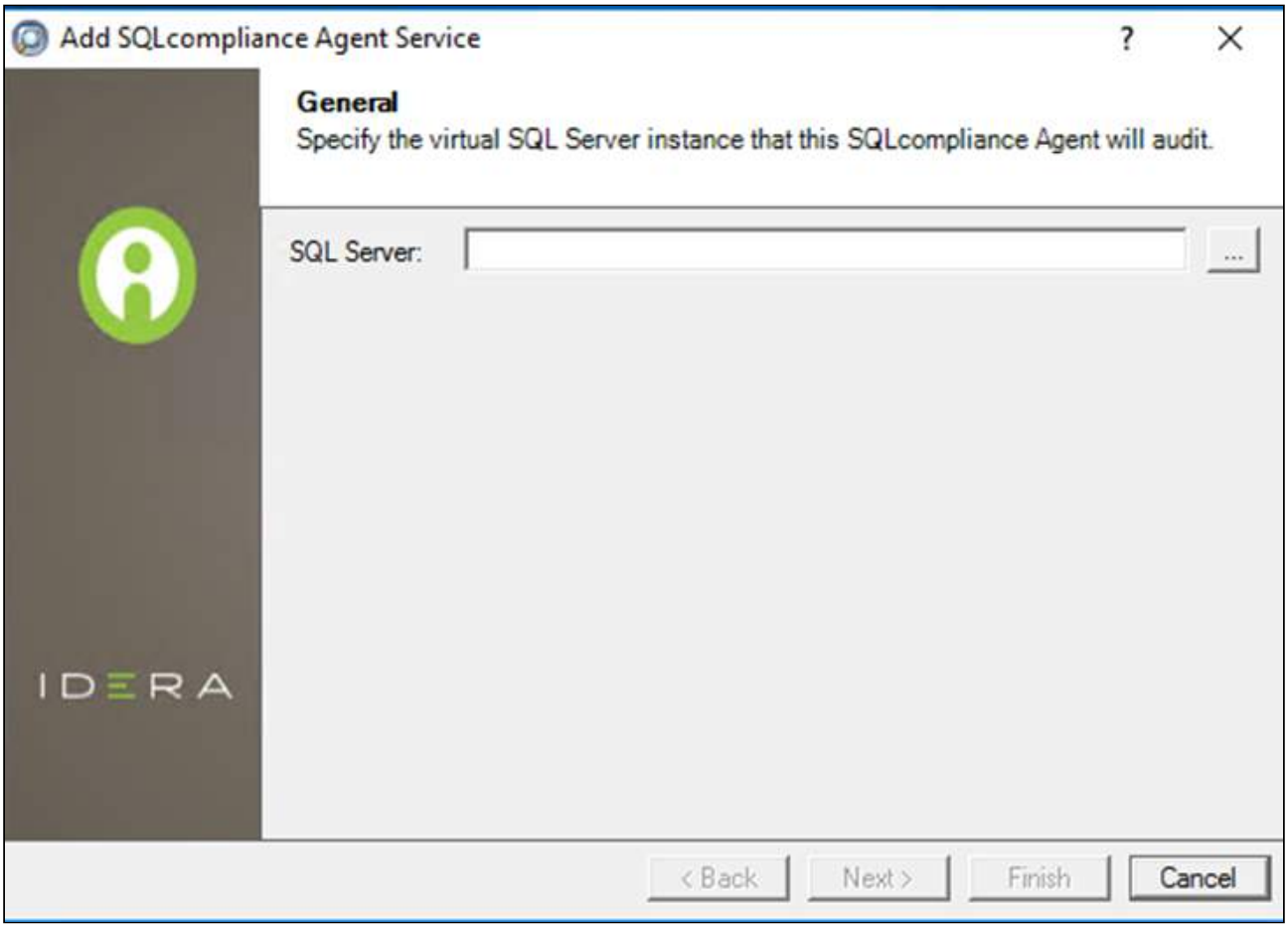
6. Click **Install** to begin the installation.



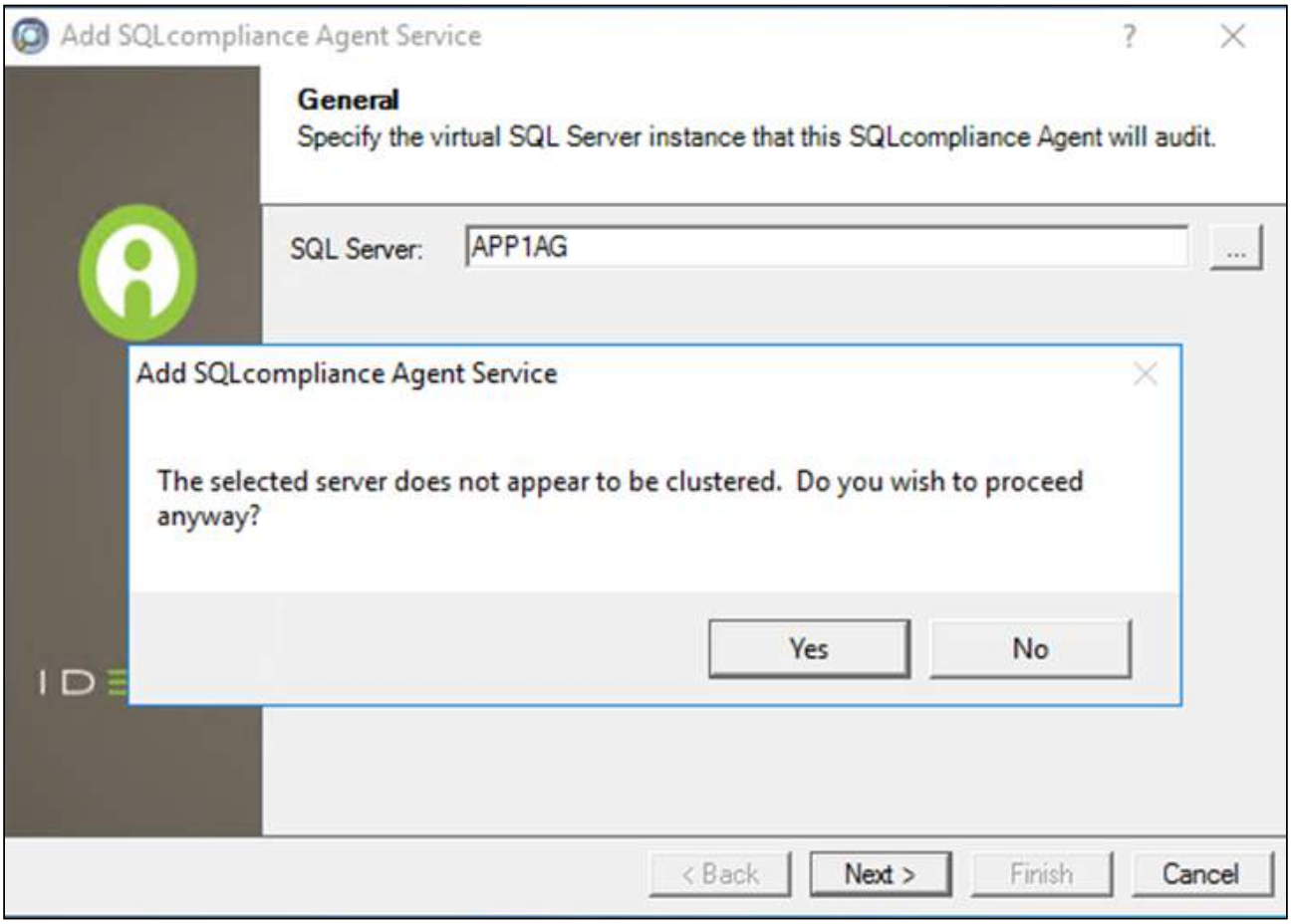
7. The Cluster Configuration Console launches automatically after installation.



8. Click **Add Service** to register the Availability Group Listener. SQL Compliance Manager displays the **Add SQLcompliance Agent Service - General** window, where the name of the Availability Group Listener to audit will need to be entered into the SQL Server textbox.

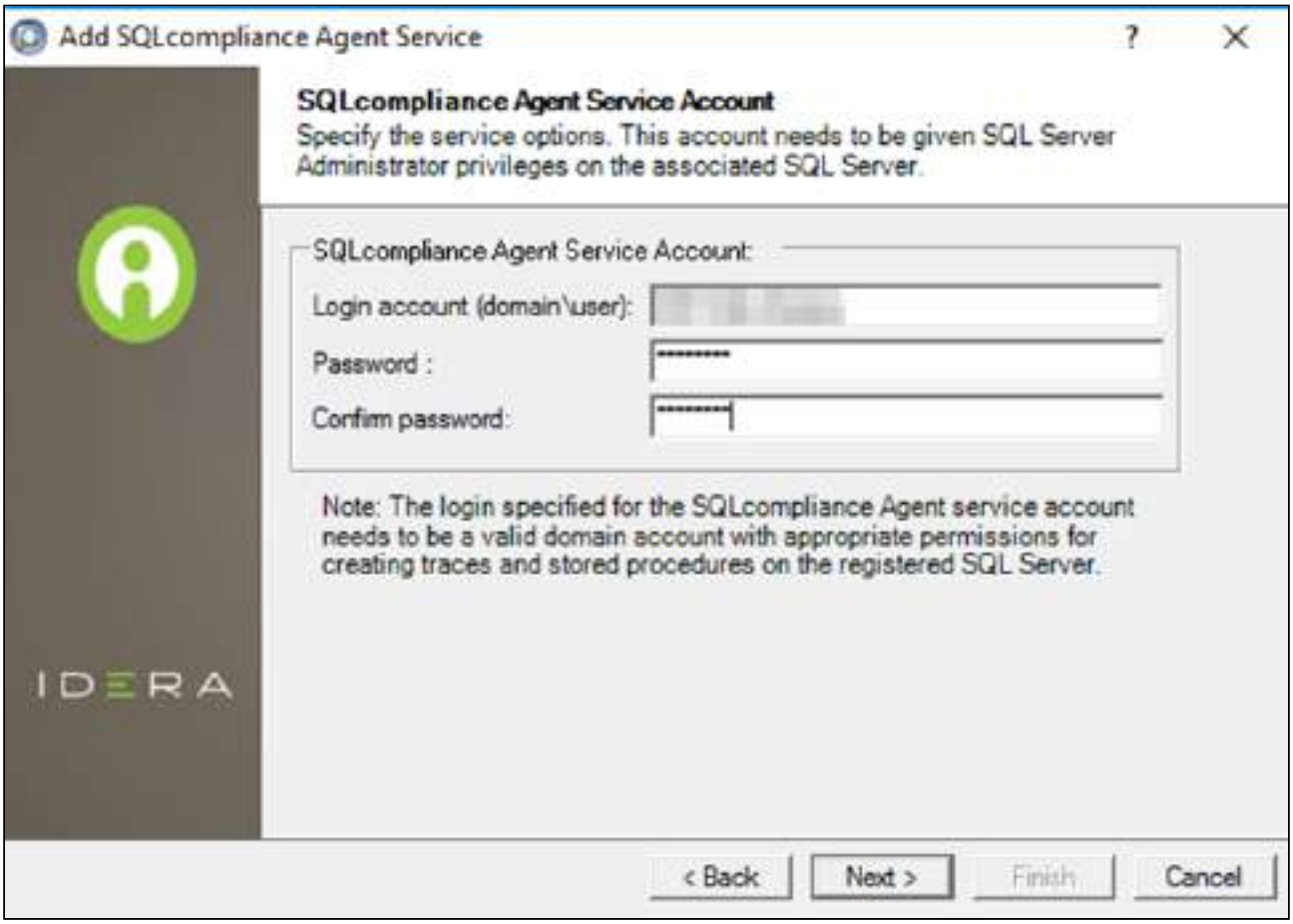


9. Once the name of the Availability Group Listener to audit has been entered, click **Next**. If you receive a message stating that the selected SQL Server instance is not clustered, click **Yes** to confirm. When configuring a Listener scenario, this is the correct behavior and ensures that the selected SQL Server instance is hosted on a Windows Failover Cluster.



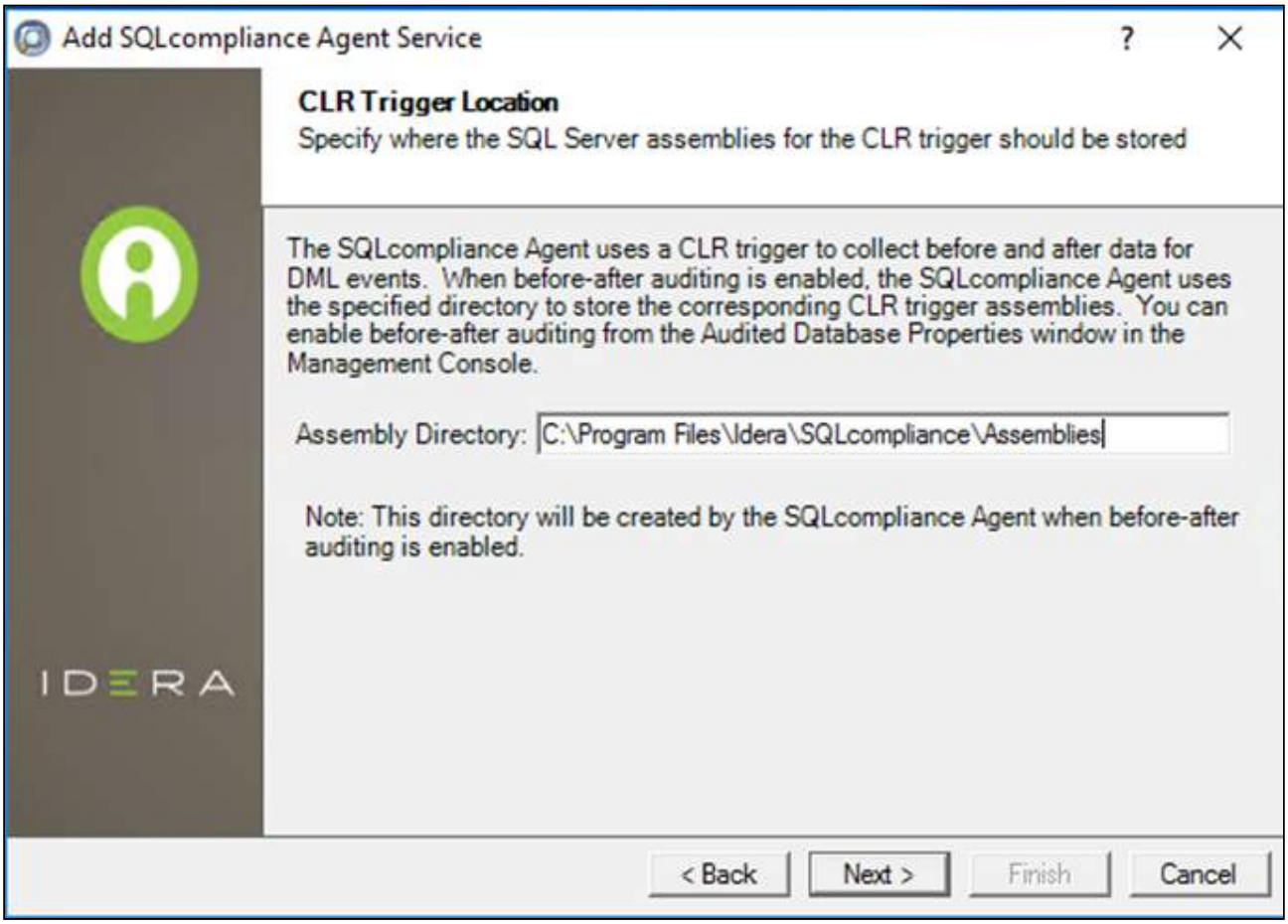
10. On the ***Collection Server*** dialog window, specify the server's name where the SQL Compliance Manager Collection Service is installed and click **Next.**

11. On the ***SQLcompliance Agent Service Account*** dialog window, specify the login credentials for the Agent service account and click **Next**. This account must have local administrator privileges, and sysadmin permissions on the SQL Server nodes of the Availability Group set up for auditing.



12. On the ***SQLcompliance Agent Trace Directory*** dialog window, specify the path where audit trace files will be created for the audit process and click **Next**. Note that the service account specified to run the Agent service must have read and write permissions on this trace directory folder.

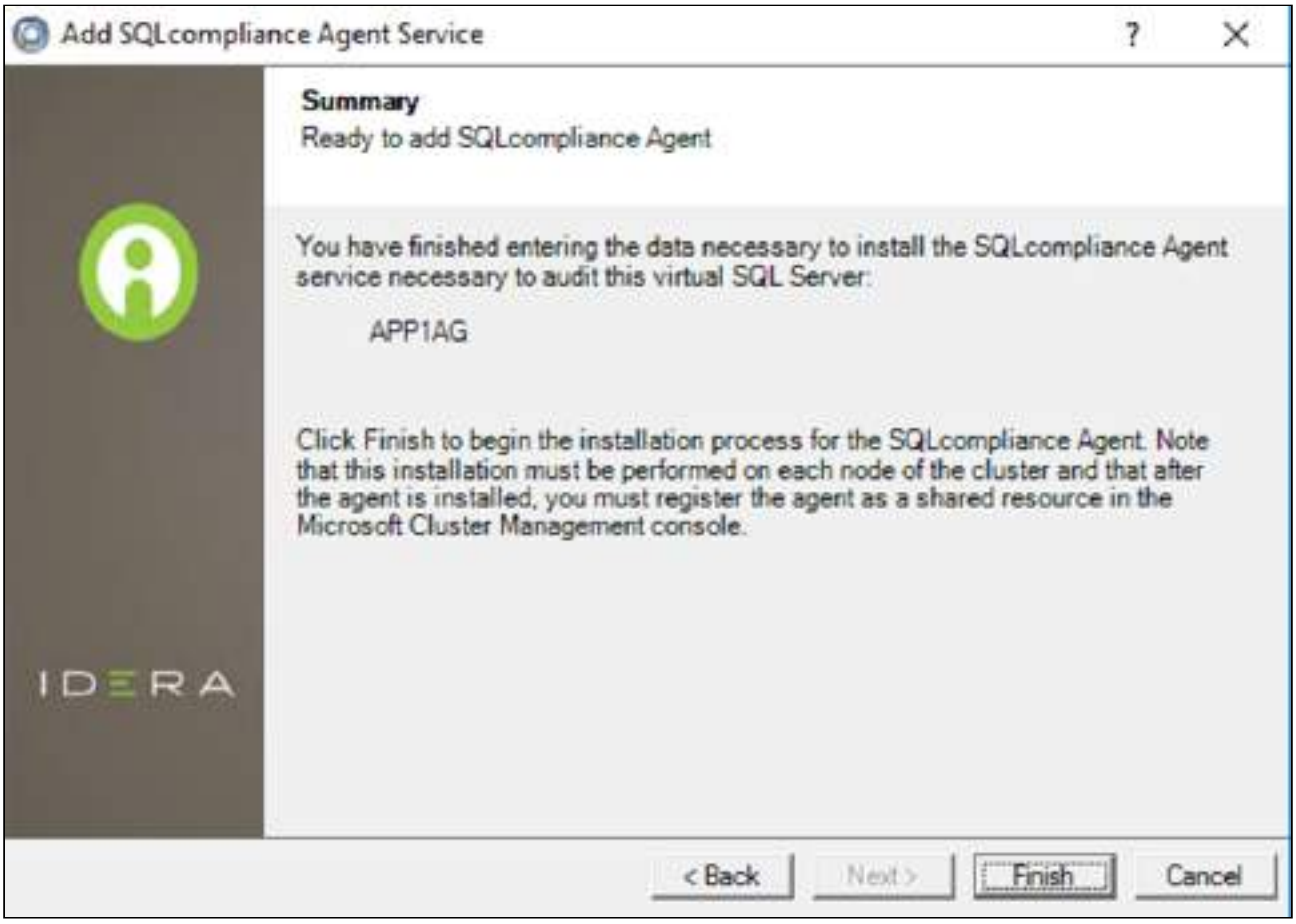
13. On the ***CLR Trigger Location*** dialog window, specify the location where you want the SQL Compliance Manager Agent to store the corresponding CLR trigger assemblies, and click **Next**. Note that the service account specified to run the Agent service must have read and write permissions on this trace directory folder.



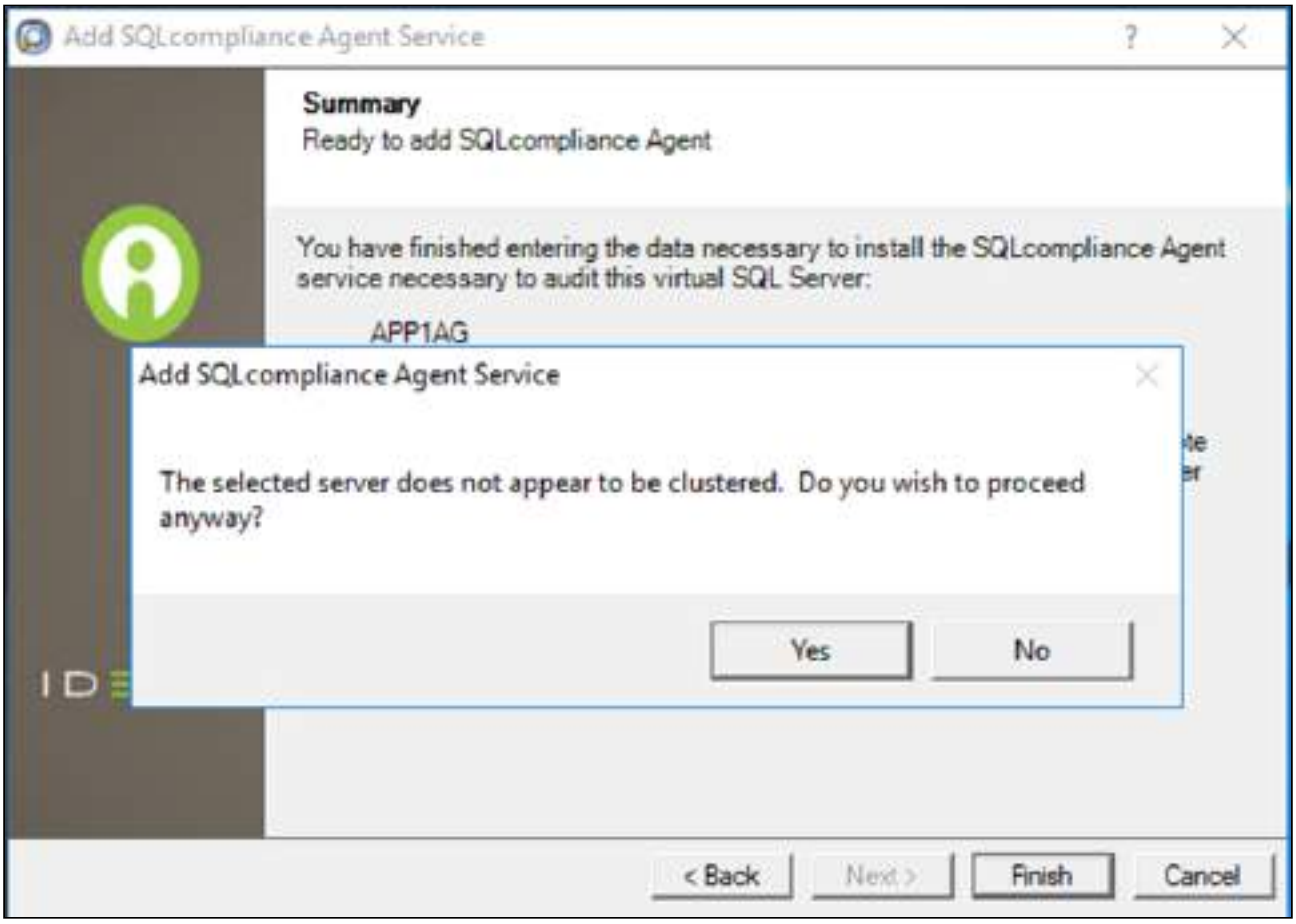
Note

Ensure the Agent Trace directory and the CLR Trigger location specified exist by creating the folder structure manually through Windows Explorer.

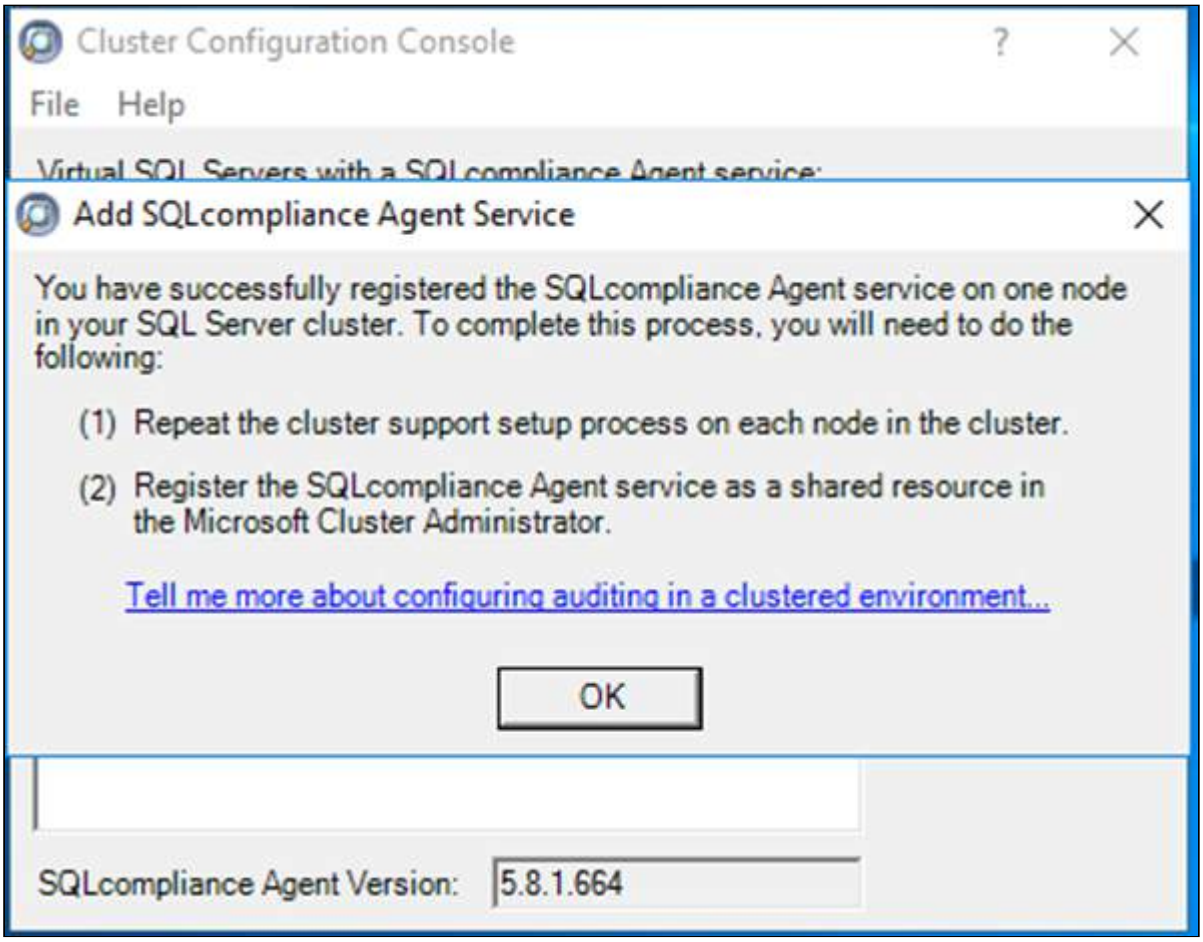
14. Review the configuration ***Summary*** and click **Finish**.



15. The wizard asks for another confirmation to proceed with the registration of the Availability Group Listener as a virtual cluster server registration, click



16. The IDERA Cluster Configuration Console displays a confirmation message stating that you have successfully added the SQL Compliance Manager Agent. Click **OK**.



Note

Repeat these steps on each remaining node in your AlwaysOn Availability Group. Consider using the same folder structure for the *Agent Trace directory* and the *CLR Trigger location* when setting the Agent up on the secondary nodes. When you are finished configuring all the nodes, proceed with the steps below.

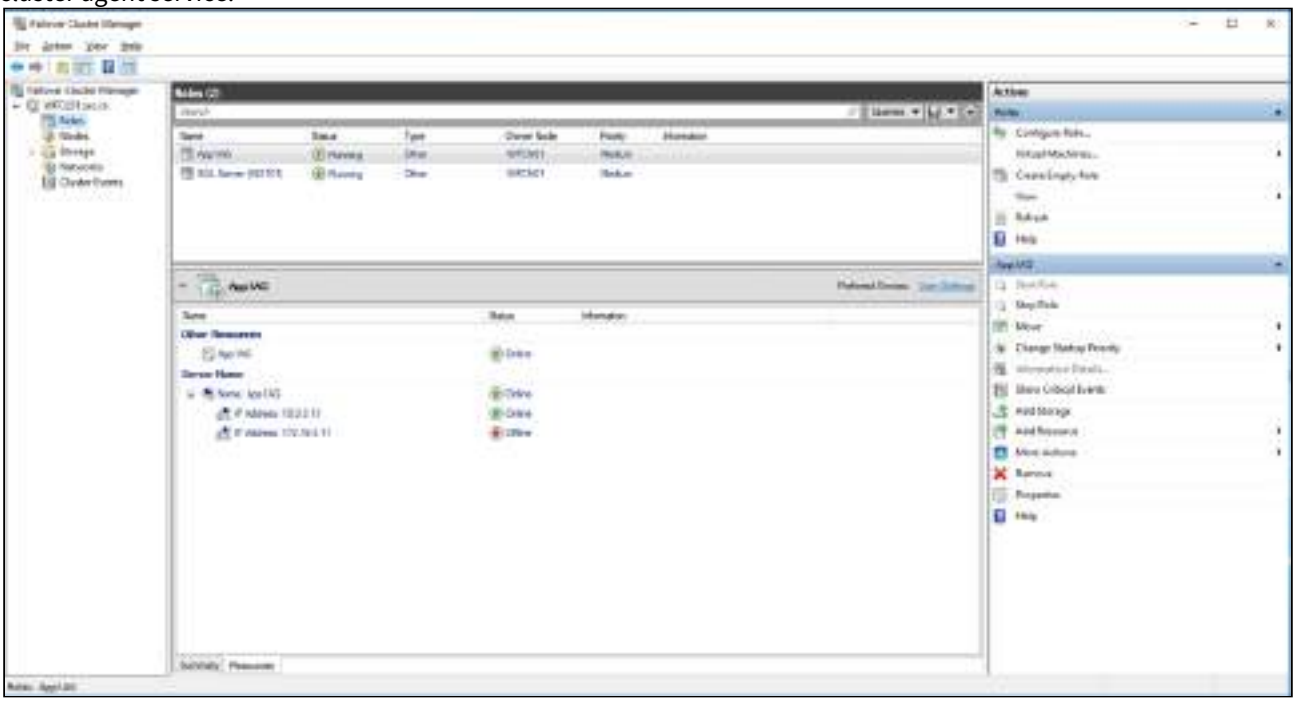
2. **Create a clustered resource for the newly installed Agent service in Failover Cluster Manager**

The Registry Replication tab is not available in Windows Server 2012.
If you are using Windows Server 2012, you must use the *"Add-ClusterCheckpoint"* PowerShell cmdlet to add the necessary setting.
For more information, see Add ClusterCheckpoint.

Use the following steps only on the Primary node of the AlwaysOn Availability Group before finally registering the Availability Group Listener for auditing into the SQL Compliance Manager console.

1. Launch the **Failover Cluster Manager**

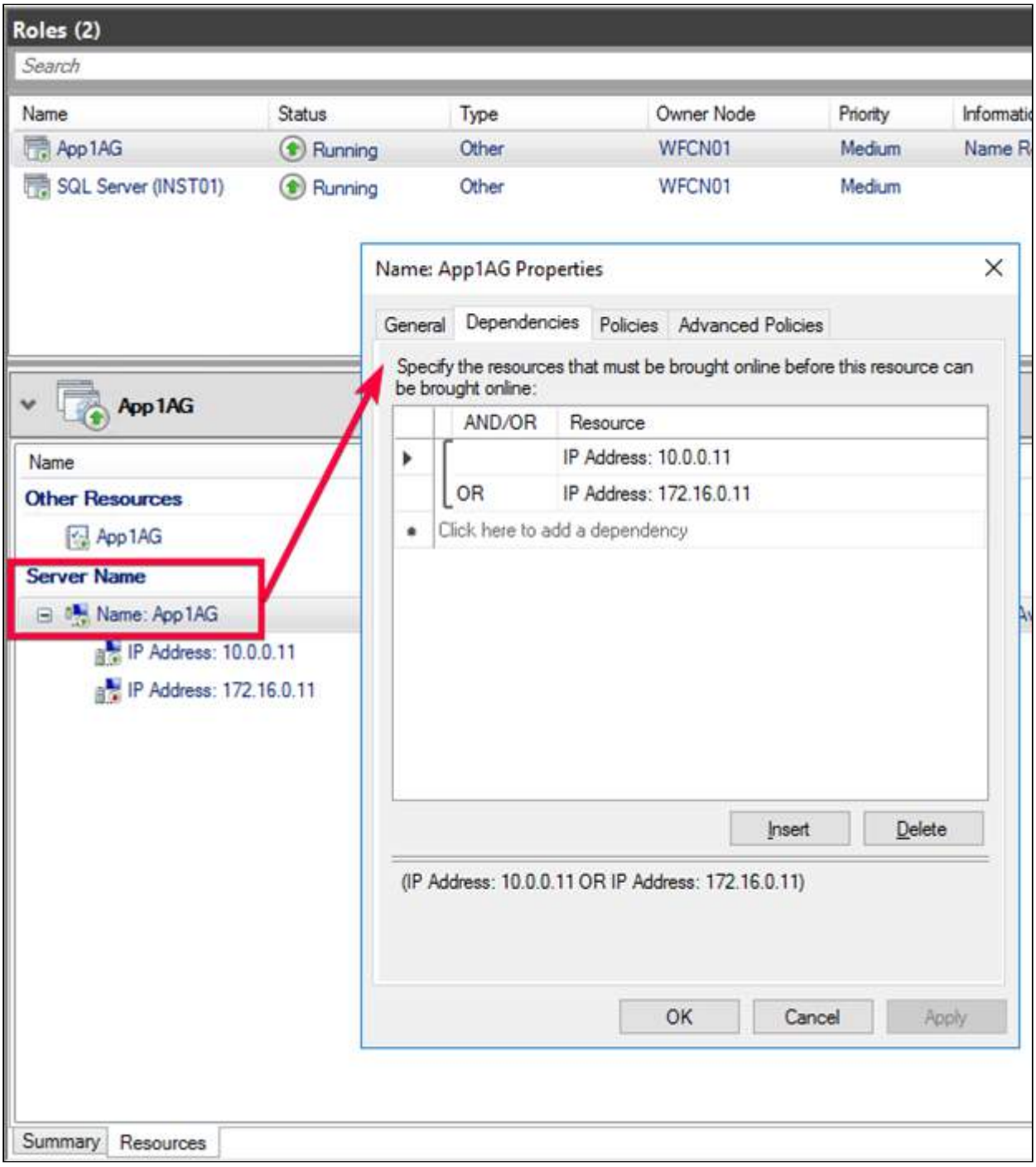
2. Select the clusters' ***ServiceGroup*** (Windows Server 2008) or ***Role*** (Windows Server 2012 and later) created for the cluster agent service.



3. On the ***Server Name*** area, right-click the resource name and click Failover Cluster Manager displays the ***Properties*** window.

4. Click the ***Dependencies.***

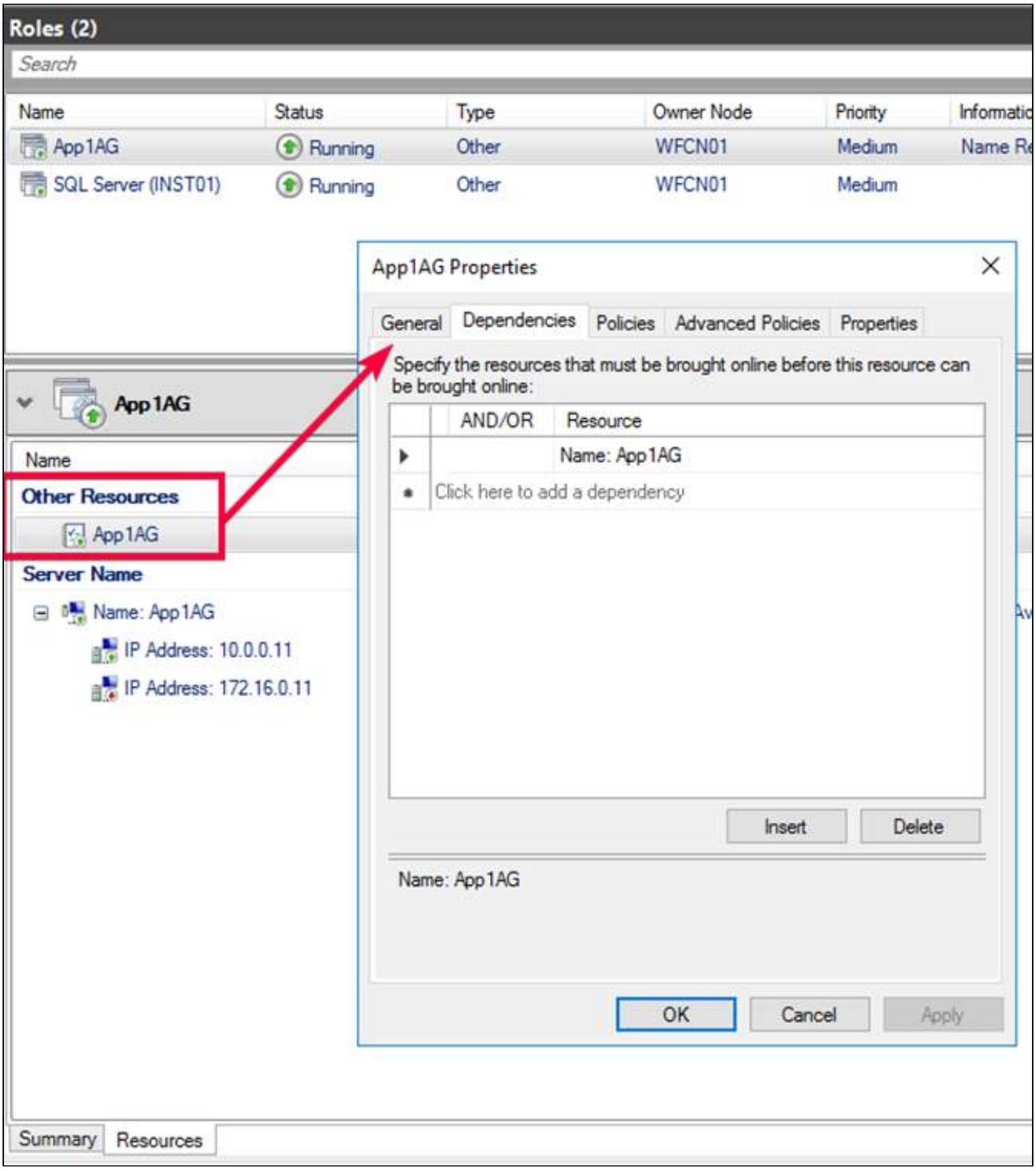
5. Verify that the **Resource** field displays the listener's IP address.



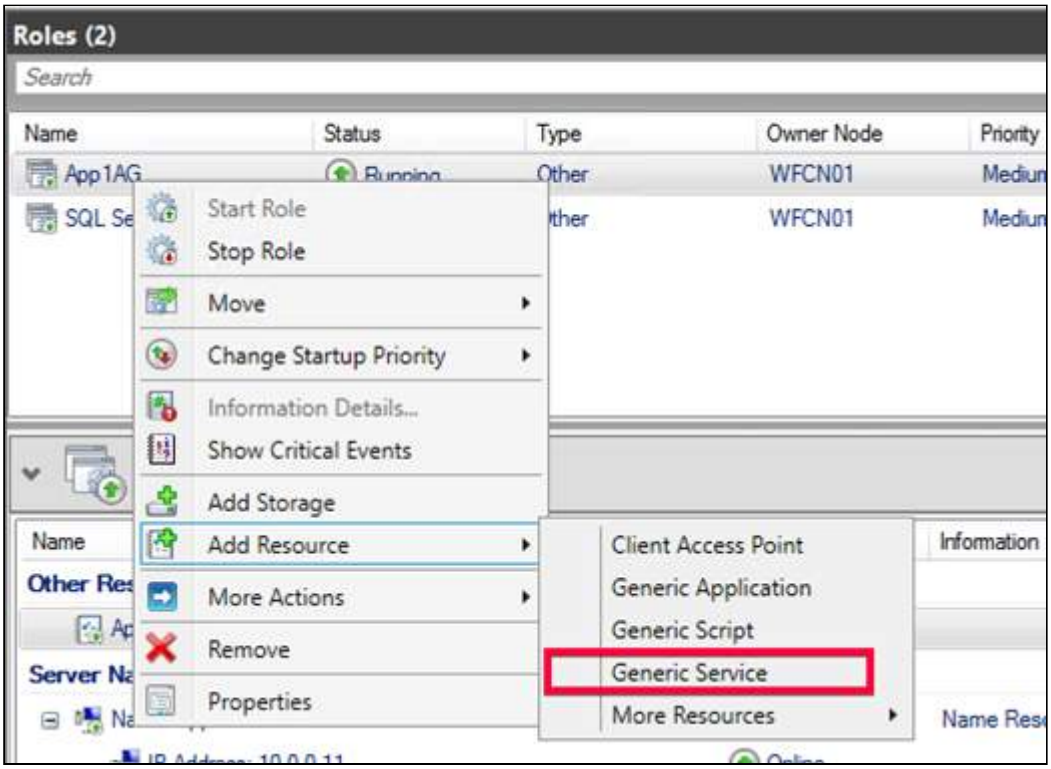
6. On the ***Other Resources*** area of the ***Failover Cluster Manager*** window, right-click the resource within the role and select **Properties**. Failover Cluster Manager displays the ***Properties*** window.

7. Click the ***Dependencies***

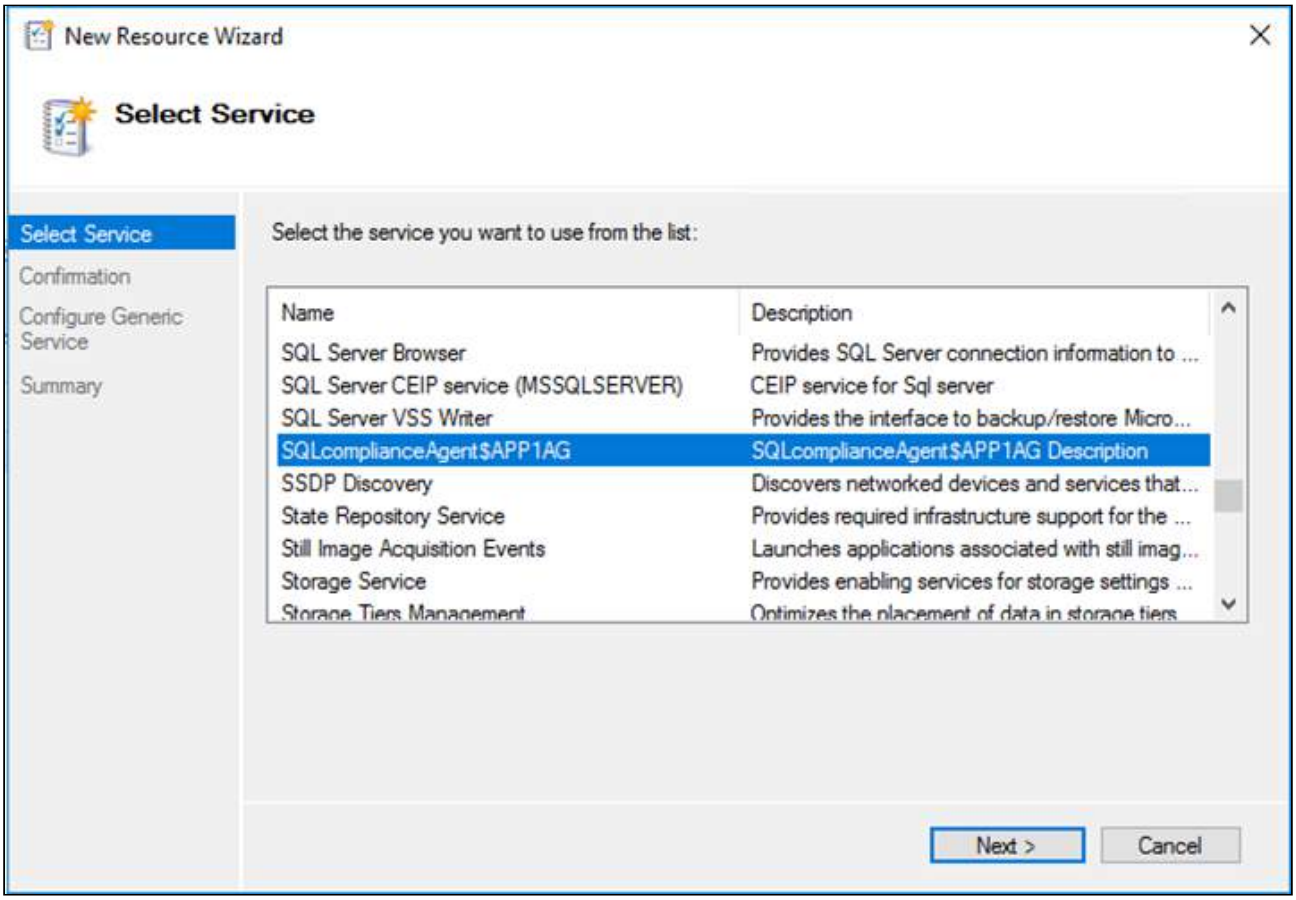
8. Verify that the **Resource** field displays the listener name. Click **Cancel** to close this window.



9. After verifying the resource information, right-click the ***Service Group*** or ***Role*** and point to **Add a resource**. Click on **Generic Service**. Failover Cluster Manager displays the ***New Resource Wizard***.

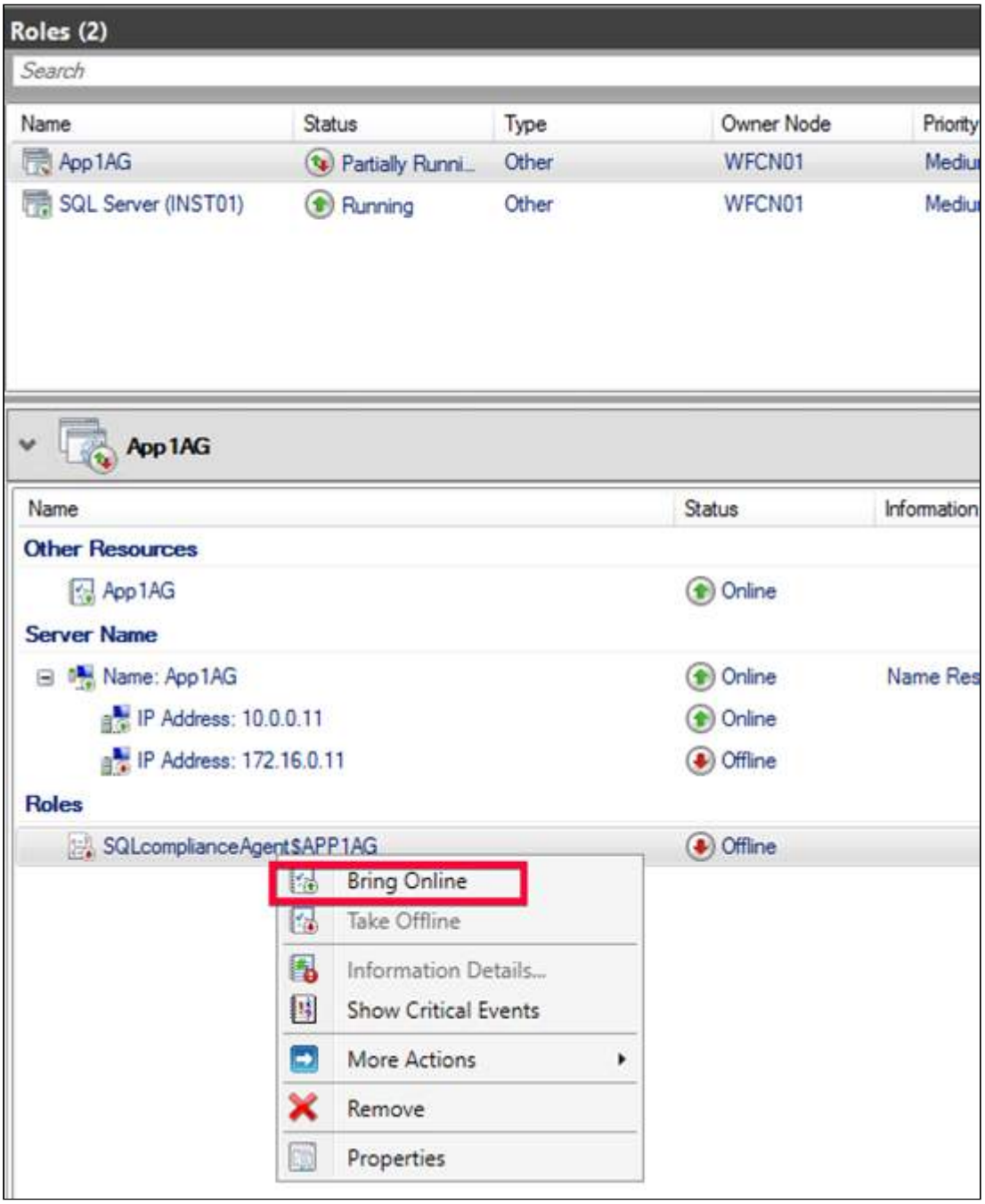


10. On the ***Select Service*** page, select the SQLcompliance Agent service from the available list. The service name is displayed in the format ***SQLcomplianceAgent$[listener name],*** where **[*listener name*]** is the SQL Server Availability Group Listener name previously registered into the SQLcompliance Cluster Configuration Console**.**



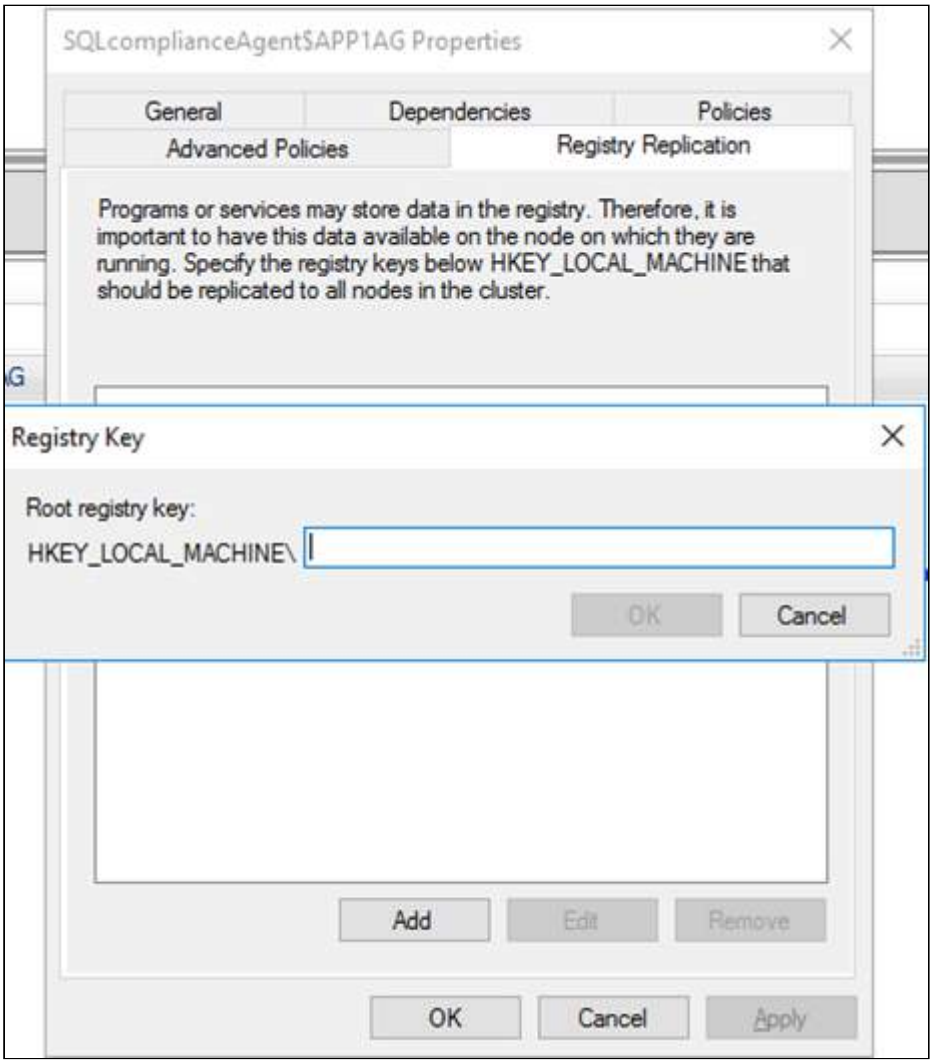
11. Click **Next**, continue following the wizard, and click **Finish**.

12. On the ***Other Resources*** area of the Failover Cluster Manager window, right-click the ***SQLcomplianceAgent$ [listener name]*** and select **Bring Online** the **resource**.



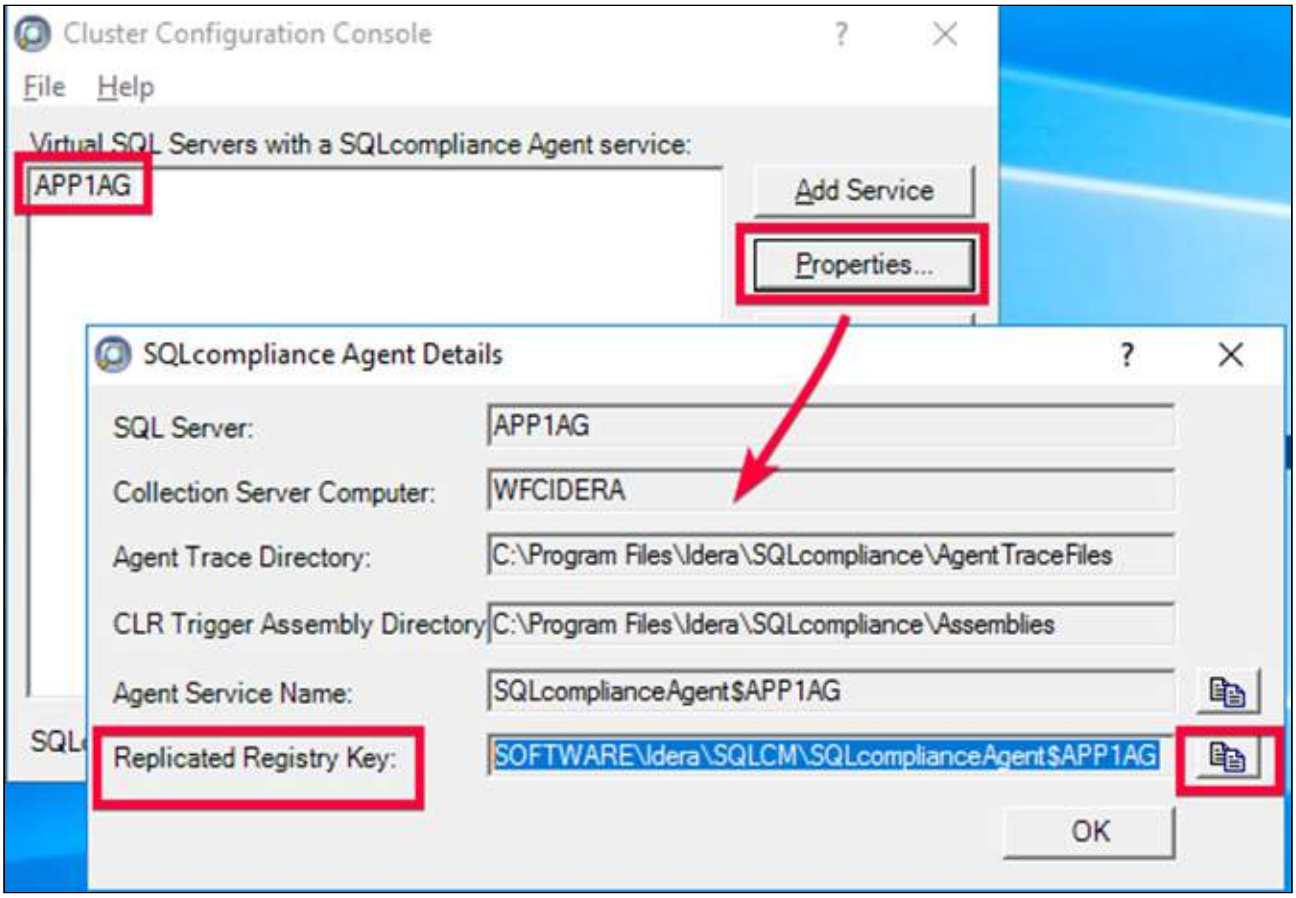
13. While the cluster service is online, right-click the ***SQLcomplianceAgent$[listener name]*** cluster service and click **Properties**.

14. On the ***Registry Replication*** tab, click **Add.** Failover Cluster Manager displays the ***Registry Key*** window.

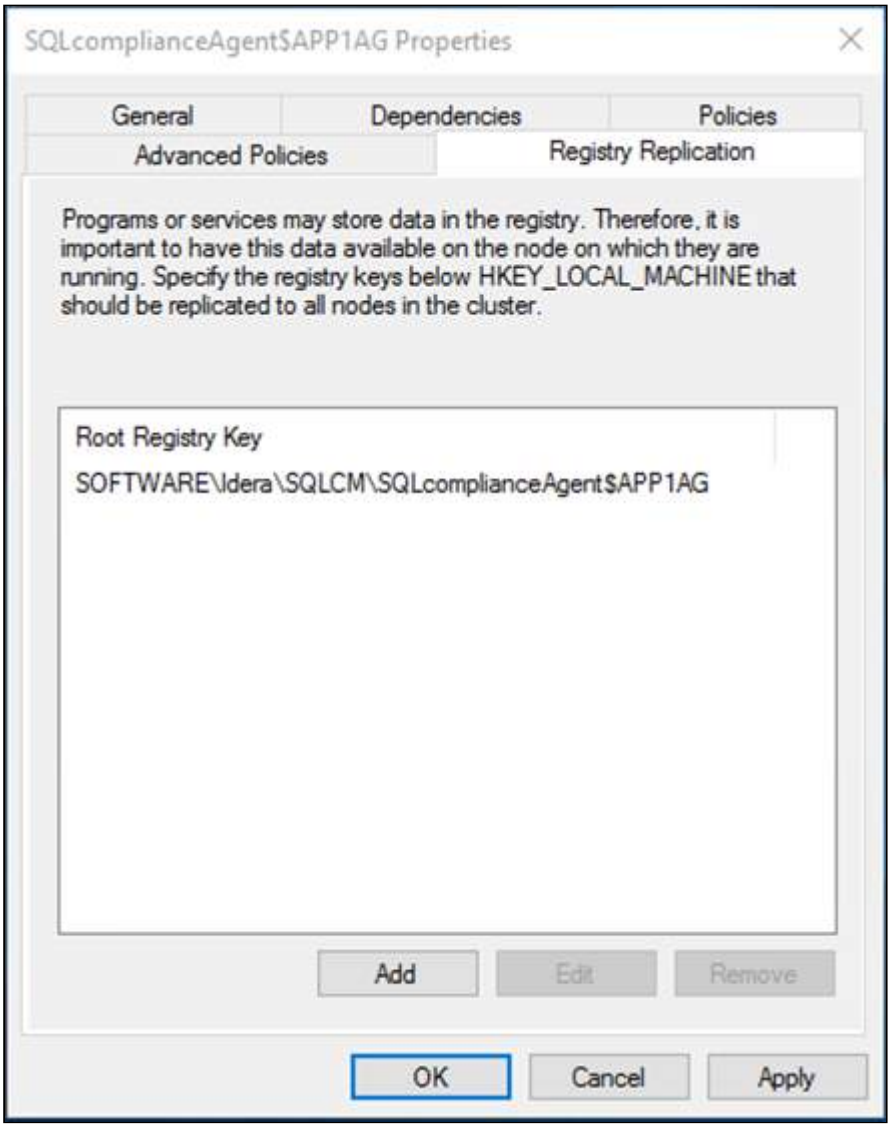


> The Registry Replication tab is not available in Windows Server 2012.
> If you are using Windows Server 2012, you must use the *"Add-ClusterCheckpoint"* PowerShell cmdlet to add the necessary setting.
> For more information, see Add ClusterCheckpoint.

15. To obtain the correct path, go to the **IDERA Cluster Configuration Console** and copy the Replicated Registry Key from the ***SQLcompliance Agent details*.**



16. Click **OK** and copy the registry key path back into the service properties window**.** The new root registry key appears in the ***Registry Replication*** tab of the Properties window. Click **Apply** and then **OK** to save changes.



3. **Register the Availability Group Listener in SQL Compliance Manager**

Use the following steps to add the listener to SQL Compliance Manager for auditing.

1. Start the IDERA SQL Compliance Manager Management Console and click **New > Registered SQL Server**. SQL Compliance Manager displays the ***SQLcm Configuration Wizard - Add Server.***
2. On the ***SQL Server*** window, specify or browse the Availability Group Listener you want to register with SQL Compliance Manager, and click **Next**.
3. On the ***SQL Server Cluster*** page, check ***This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server*** box, and click **Next**. This step registers the AG Listener as a virtual cluster SQL Server name.
4. On the ***SQLcompliance Agent Deployment*** page, verify that the **Manually Deploy** is selected, and click **Next**. This option is required for all virtual SQL Servers.
5. On the ***Select Databases*** page, check the AlwaysOn database that you want to audit, and click **Next**.
6. SQL Compliance Manager displays the ***AlwaysOn Availability Group Details*** page, including a list of all nodes where the AlwaysOn database is replicated.

> This step is valid only if the database selected for auditing is AlwaysOn. The wizard skips this page for regular databases.

7. ***If the AlwaysOn Availability Group Details window is displayed,*** click **Next** to continue.
8. On the ***Audit Collection Level*** page, select the desired audit collection level for the database and click **Next**.
9. SQL Compliance Manager verifies that all the required permissions are in place on the SQL Server instance you want to audit on the Permissions Check page.
10. After all the operations are complete and all permissions checks pass, click **Next**. The ***Summary*** page displays the audit settings for the SQL Server instance.
11. Click **Finish** to close the wizard. Finally, SQL Compliance Manager displays the newly-added AlwaysOn Availability Group Listener in the ***Explore Activity*** tree.
12. Make all necessary audit settings for the listener and AlwaysOn databases, and then update the configuration and begin collecting data. It is recommended to update the configuration before collecting data because users are unaware of which node is PRIMARY. After updating the configuration, click **Refresh** in the node context menu to apply the settings to the displayed information.

After configuration, review some Additional information on SQL Compliance Manager and AlwaysOn Availability Groups.

7.7.3 Configuring Nodes scenario

The Nodes scenario is recommended for users who want to audit regular databases and AlwaysOn databases on nodes that can be in PRIMARY or READ-ONLY SECONDARY nodes.

The SQL Compliance Manager administrator adds each node or instance of SQL Server involved in the availability group individually, which is the same process as with any regular SQL Server instance. You can then add any database that you want to audit. While you can automatically deploy the agent through the console, it is recommended that you manually deploy in case the automatic deployment fails. Note that the permissions requirements are the same as for the Listener scenario. For more information about permissions, see Permissions requirements.

AlwaysOn databases running as the secondary replica do not appear in the Add Database wizard unless the replica is marked as read-only. Note that the default status is non-readable.

Review the following steps to manually deploy the agent service to all AlwaysOn node.

1. Start the SQL Compliance Manager Management Console.
2. Select the SQL Server instance to which you want to manually deploy the agent, and click **Add Server**. SQL Compliance Manager displays the ***SQL Compliance Manager Configuration Wizard - Add Server***.
3. On the ***Specify SQL Server*** page, specify or browse the node, and click **Next.**
4. On the ***Existing Audit Data*** page, select the option to retain all of the previously-collected audit data and use the existing database, and click **Next**.
5. On the ***SQL Server Cluster*** page, check this option if the instance is a virtual SQL Server, and click **Next**.
6. On the ***SQLcompliance Agent Deployment*** page, verify that the **Manually Deploy** option is selected, and click **Next**.
7. On the ***Select Databases*** page, select the AlwaysOn database, and click **Next**.
8. SQL Compliance Manager displays the ***AlwaysOn Availability Group Details*** page. This page displays information about all nodes where the AlwaysOn database will be replicated. ***Note that this page does not appear if the database is not AlwaysOn***.
9. Review the available information, and click **Next**.
10. On the ***Audit Collection Level*** page, select the **Default** audit level, and click **Next**.
11. On the ***Permissions Check*** page, verify that all permissions pass, and click **Next**.
12. SQL Compliance Manager displays the ***Summary*** page. Click **Finish**.

After adding all nodes, the SQL Compliance Manager displays the primary node, as shown in the following image. You also now can audit any AlwaysOn databases in the added nodes if they are in PRIMARY or READ-ONLY SECONDARY roles.

7.7.4 Additional information on SQL Compliance Manager and AlwaysOn Availability Groups

After configuring the AlwaysOn Availability Groups on SQL Compliance Manager, review the following information to start auditing and modify your AlwaysOn databases.

- Removing a Listener from SQL Compliance Manager
- Exporting/importing audit settings for all AlwaysOn nodes
- Removing an AlwaysOn node from SQL Compliance Manager

Removing a Listener from SQL Compliance manager

Use the following steps to remove the listener from SQL Compliance Manager auditing.

1. Open Server Manager.
2. In the Server Manager tree, click **Server Manager > Features > Failover Cluster Manager**. The system displays Failover Cluster Manager.
3. On the ***Other Resources*** area, right-click the *SQLcomplianceAgent$[listener name],* and select **Bring Offline**.
4. Verify in the confirmation message that you want to take the resource offline.
5. Keep Failover Cluster Manager open as you will return to this view after removing the listener from SQL Compliance Manager.
6. Open the SQL Compliance Manager Management Console.
7. Click the listener name on the ***Explore Activity*** panel, and click **Remove**. SQL Compliance Manager displays an error message concerning the inability to contact the agent when removing the listener.
8. Click **Yes** to confirm that you want to continue with the removal of the instance.

9. ***If you want to re-add this listener for auditing at a later time,* do not** continue with the next steps.
   ***If you no longer want to use this listener,* continue** with the following steps for all nodes included in the AlwaysOn Availability Group.
10. Return to Failover Cluster Manager.
11. On the ***Other Resources*** area, right-click the *SQLcomplianceAgent$[listener name],* and select **Delete**
12. Verify in the confirmation message that you want to delete the resource.
13. Open the Cluster Configuration Console by clicking **Start > IDERA > Cluster Configuration Console**.
14. Select the virtual SQL Server listener, and click **Remove Service**.
15. Click **Yes** in the confirmation message. The cluster service agent is removed.
16. ***If you no longer need to add listeners,*** uninstall the Cluster Configuration console.

Exporting/importing audit settings for all AlwaysOn nodes

Users can select all of the appropriate audit settings for each AlwaysOn database and export these settings as XML files. You then can import the files into the remaining instances or nodes in the group.

To import the audit settings to each node, click **Import** on the Summary tab. Choose the exported XML file, the information you want to import, and the servers to which you want to apply the settings. Select all the other servers in the availability group as the target for audit settings. After users apply the settings from the file, each member of their availability group is set to audit in exactly the same way as noted in the exported file. This process also allows you to add additional databases that are the part of an availability group on these servers.

Removing an AlwaysOn node from SQL Compliance Manager

To remove an AlwaysOn node from SQL Compliance Manager, first stop the agent service using the Failover Cluster Manager before attempting to remove a node instance from SQL Compliance Manager. This step must be performed if you may want to add back to SQL Compliance Manager the removed node using the Manual Deployment option without any agent deployment. In this case, ignore the error message that appears after you remove the node.

7.8 Disable auditing on a database

You can disable auditing on any database associated with a registered SQL Server instance. When you disable auditing, IDERA 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.

7.9 Disable auditing on a SQL Server

You can disable auditing on any registered SQL Server instance and the associated databases. When you disable auditing, IDERA 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.

7.10 Fine tune your audit settings

IDERA SQL Compliance Manager provides 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 possibly are resource-intensive and can cause significant growth in the Repository databases, thereby decreasing SQL Compliance Manager performance. For more information about avoiding performance issues, see Reduce audit data to optimize performance.

7.10.1 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 can collect a significant number of events initiated by benign applications simply because they are 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.

7.10.2 Auditing the system databases for DML or SELECT activity

Gathering events directly from the system databases is useful only under very specific circumstances in an audited environment. Accidental collection of SQL Server internal operations can occur when you audit DML or SELECT events, resulting in the storage of unnecessary data. ***If you want to continue auditing system databases***, consider routinely archiving or grooming your event databases.

7.10.3 Auditing login events at the server level

Some third-party applications perform a login to the SQL Server instance before initiating any individual operation. This action can cause the collection of a large number of login events 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.

> ⚠ Auditing the Login Failed event category does not result in the collection of the same level of data. You can leave this action enabled.

7.11 Monitor SQL Compliance Manager Agent activities

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

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

7.11.1 To monitor SQL Compliance Manager 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.

7.12 Reduce audit data to optimize performance

Use the following checklist to help you optimize IDERA 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 collection and storage of unwanted events. 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.

7.13 Enable self-auditing and monitoring

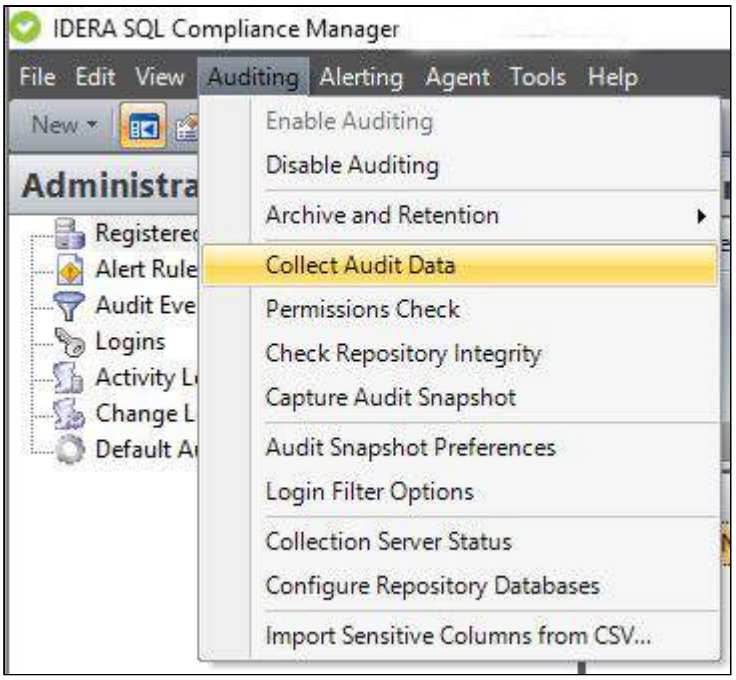
Auditing your IDERA SQL Compliance Manager implementation is called self-auditing. Self-auditing consists of regularly checking the integrity of the Repository databases. You can also audit the Repository databases. For example, you can audit specific events, such as logins, on the Repository. For more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

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

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

7.14 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.



7.14.1 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 SQL Compliance Manager 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.

7.15 Verify audit data integrity

IDERA 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 is 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 is not 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 about integrity checks, see Use the CLI to verify audit data integrity.

7.15.1 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 inserted, modified, deleted) and changes the event category to Integrity Check. For more information about integrity checks, see the help topic for the corresponding window.

7.16 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.

7.16.1 Use custom views

IDERA 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

- **Data 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**.

7.16.2 View your activity summary

IDERA 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.

8 Manage Audit Data

You can optimize auditing performance and preserve your compliance history through IDERA 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.

8.1 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. IDERA 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 they are 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 about archiving 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.

8.2 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.

8.3 Archive collected events

When you archive your registered SQL Server instances, IDERA 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 was allocated due to the previous growth.

8.3.1 Use the Management Console to archive events

When you archive events using the Management Console, IDERA 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. ***If you want 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**.

8.3.2 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 uses the settings you selected in your archive preferences. An integrity check is performed unless you use the `-nointegrity` parameter in your command.

8.4 Attach existing archives

Attaching an archive allows you to view audited events that 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, IDERA SQL Compliance Manager automatically attaches an archive when creating the corresponding database. ***If you do not report 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.

8.4.1 To attach archives:

1. In the **Explore Activity Tree**, select the SQL Server instance to which you want to attach an archive.
2. On the menu bar, click **File** > **Attach Archive Database**.
3. Specify the appropriate settings, and then click **OK**.

8.5 Automate audit data management

IDERA 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.

8.6 Groom alerts from Repository

You can groom alerts from the Repository. When you groom alerts, IDERA 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.

8.6.1 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**.

8.7 Groom audit data

You can groom audited SQL events from the event databases in the Repository. When you groom audit data, IDERA 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 was allocated due to the previous growth.

8.7.1 Use the Console to groom events

When you groom events using the Management Console, IDERA 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**.

8.7.2 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
```

8.8 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

Repository Database	Supported Recovery Model
`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 SQL Safe allow you to schedule fast, secure backups using optimized compression and encryption settings.

8.8.1 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 SQL Safe 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.
3. Use SQL Server Enterprise Manager or Management Studio to bring the SQLcompliance database online.

8.8.2 Back up and restore archive databases

To ensure optimal audit performance while minimizing storage requirements, consider implementing a maintenance plan to back up your archive databases on a routine basis using IDERA SQL Compliance Manager. Each archive database is independent, and you can maintain each on a different schedule.

Once you back up the archive, you can drop the archive 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 the database using the Management Console. For more information about attaching archives, see Attach existing archives.

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

8.8.3 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 IDERA 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.

8.8.4 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 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 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.

8.9 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, IDERA 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).

8.9.1 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**.

8.9.2 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
```

8.10 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
```

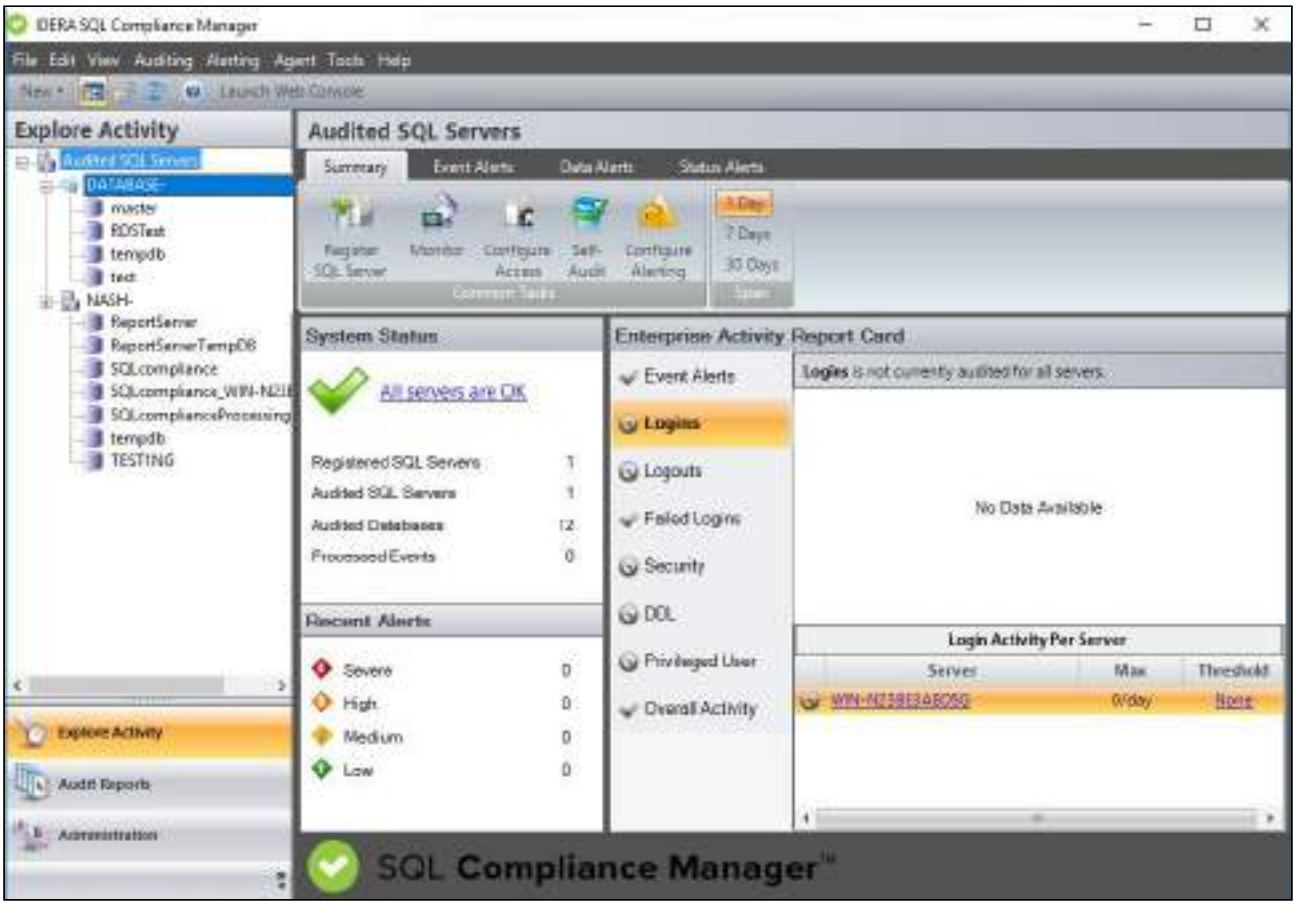
9 Management Console User Interface

The IDERA SQL Compliance Manager 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

9.1 Explore Activity View

The SQL Compliance Manager Explore Activity view is the windows console main display screen which allows you to get an overview of the status of your SQL Server instances and hosted databases all in a consolidated view, while providing the means to drill into individual SQL Server or database configuration settings for more details. Select the Audited SQL Servers option from the expansion tree to display an overview of your registered servers, or select a registered instance to view the captured events and to set your desired configurations. In addition, you can also select a database to view detailed information or to set your configuration settings for that specific database.



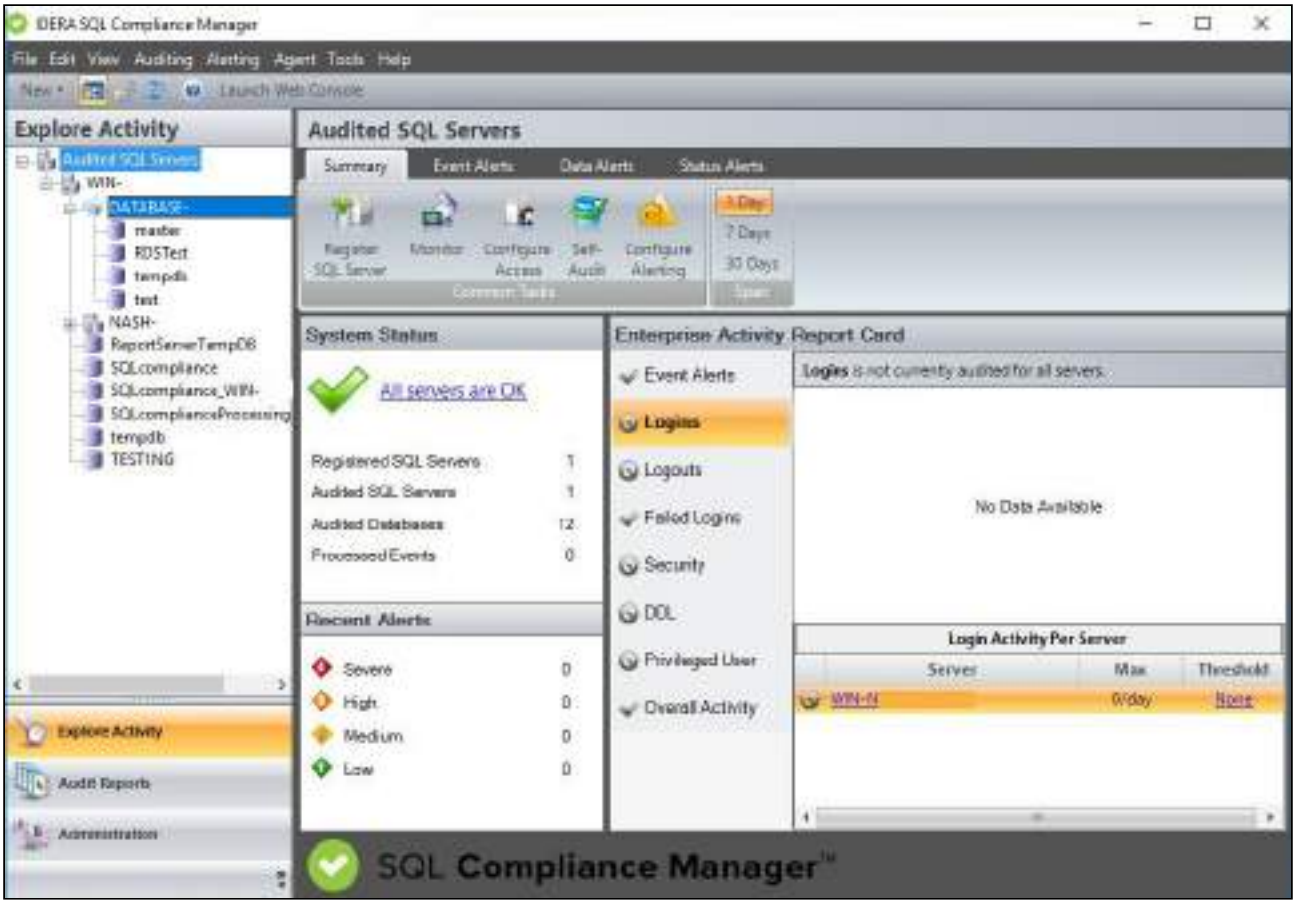
9.1.1 Use the links below to learn more about the different level Explore Activity views:

- Explore Activity - Audited SQL Servers View

- Explore Activity - Instance View
- Explore Activity - Database View

9.1.2 Explore Activity - Audited SQL Servers View

The Explore Activity Audited SQL Servers view displays the status of audit activity across your SQL Server environment. Use Summary tab to view the statistics and graphs to quickly identify issues so you can continue to ensure the correct level of compliance in your environment. View in detail your previously generated alerts by selecting the respective alert tab.

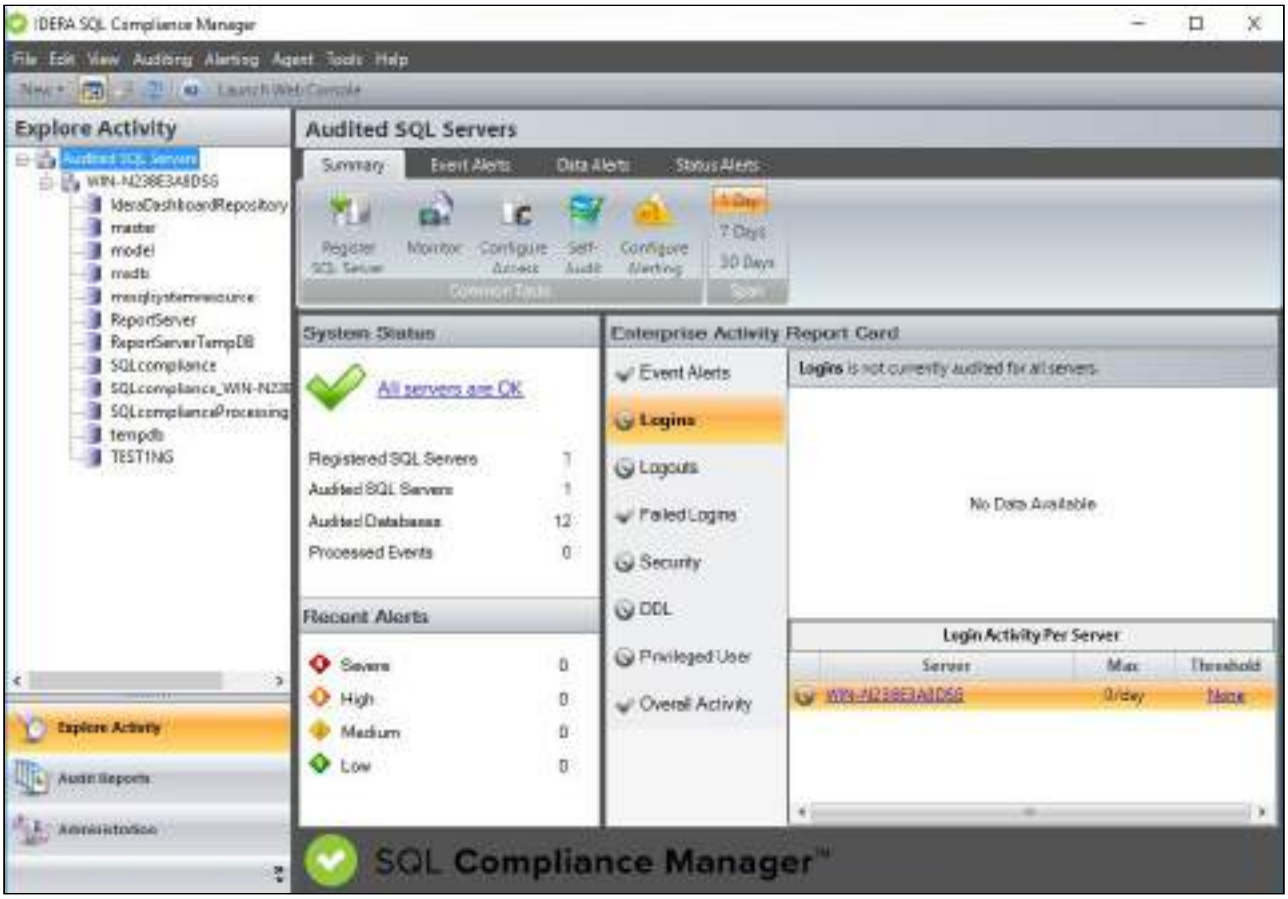


For more information, visit the different tabs for the Explore Activity Audited SQL Servers view below:

- Event Alerts tab
- Status Alerts tab
- Data Alerts Tab
- Explore Activity - Audited SQL Servers Summary tab

Explore Activity - Audited SQL Servers Summary tab

The Audited SQL Servers Summary tab (Management Console) 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 IDERA SQL Compliance Manager 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 view the status of audited databases on this instance, validate audit settings, and check the SQL Compliance Manager Agent status.

Status Type	Possible Causes
Alert/Error	• **The Repository is installed on a SQL Server 2005 instance but a SQL Compliance Manager Agent is deployed to a SQL Server 2012 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 SQL Compliance Manager Agent is 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 SQL Compliance Manager Agent missed every heartbeat over the last 24 hours.** This issue occurs when the SQL Compliance Manager Agent service is stopped, the Collection Server is offline, the computer hosting the agent is offline, or network availability is lost. • **The SQL Compliance Manager Agent service is no longer running.** The SQL Compliance Manager Agent service is stopped by a SQL Server login or a third-party application. • **A system alert is 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 are registered with SQL Compliance Manager.** SQL Compliance Manager cannot begin auditing your environment until instances are registered, SQL Compliance Manager Agents are deployed, and audit settings are configured. • **The SQL Compliance Manager Agent is not yet deployed to an instance that is registered with SQL Compliance Manager.** SQL Compliance Manager cannot audit this instance until an agent is deployed and audit settings are configured. • **A deployed SQL Compliance Manager Agent has not yet contacted SQL Compliance Manager.** This issue occurs when the SQL Compliance Manager Agent service is stopped, the computer hosting the agent is offline, or network availability is lost. • **A deployed SQL Compliance Manager Agent missed two sequential heart beats.** This issue occurs when the SQL Compliance Manager 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 Compliance Manager.

Audited SQL Servers

Displays the number of instances currently audited. This number does not include instances where auditing is not yet configured or is disabled.

Audited Databases

Displays the number of databases currently audited. These databases are hosted by SQL Server instances that are registered with SQL Compliance Manager. 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 previously archived or groomed events.

Understanding the Enterprise Activity Report Card status

Each tab of the Enterprise Activity Report Card provides an auditing status for the corresponding event category. Use this status to help 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 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 flagged event category. You can view the detailed properties of an event by double-clicking the listed event.
OK	green check	This event category is audited on instances in your environment and auditing thresholds are set for this event category.
Not audited	red icon	This event category is not 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.

Status Type	Indication	Meaning
Not audited and no thresholds set	gray circle	This event category is not 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 are 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 are 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.

Register a SQL Server

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 SQL Compliance Manager Agent to begin auditing SQL events on this instance.

Before registering your SQL Server instance:

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**.

To Register your SQL Server instance follow the steps from the New Registered SQL Server wizard below:

- Configuration wizard - Add Server window
- Configuration wizard - License Limit Reached window
- Configuration wizard - Existing Audit Data window
- Configuration wizard - Existing Incompatible Database window
- Configuration wizard - SQL Server Cluster window
- Configuration wizard - SQL Compliance Manager Agent Deployment window
- Configuration wizard - Add Databases window
- Configuration wizard - Audit Collection Level window
- Configuration wizard - Permissions Check window
- Configuration wizard - Summary window
- Configuration wizard - Specify Connection Credentials window

Configuration wizard - Add Server window

The Add Server window of the Configuration wizard allows you to specify the SQL Server instance you want to register with IDERA SQL Compliance Manager. Once you register an instance, you can begin auditing database activity on that server.

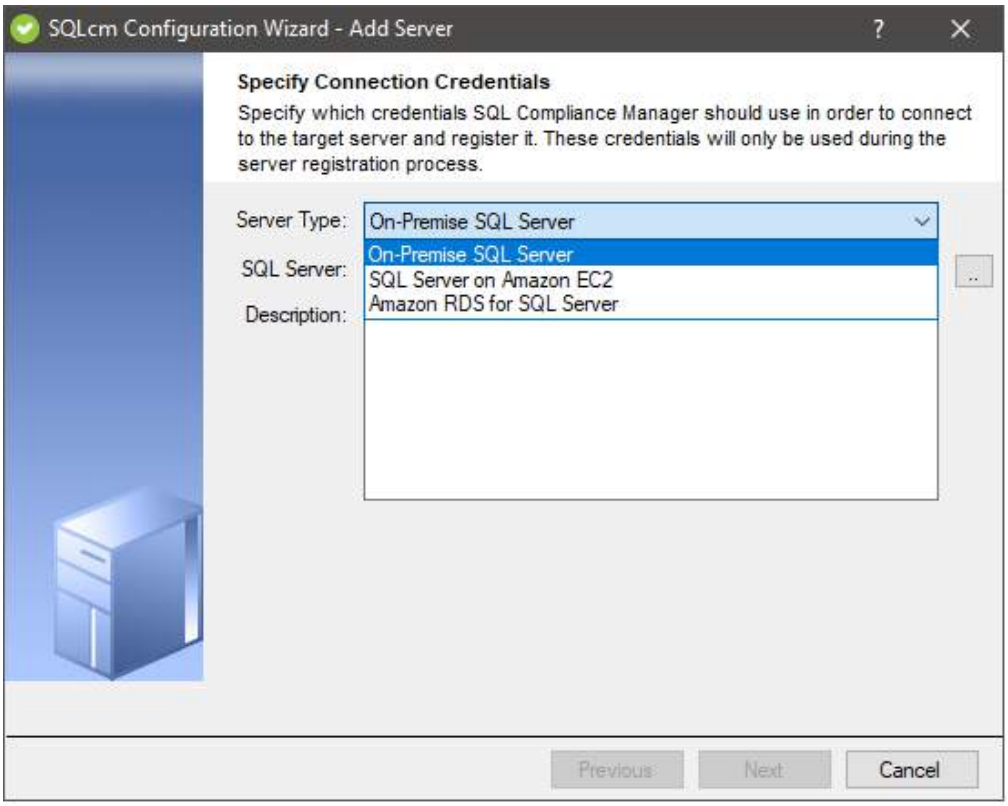
Select the SQL Server instance you want to register, and then click **Next**.

Available fields

Server Type

Allows you to select from a drop-down selection the Server Type you want to Add with the following available options:

- **On-Premise SQL Server**. Allows you to register an on-premise SQL Server. This is set as the default selected option.
- **SQL Server on Amazon EC2**. Allows you to register a server connected to an AWS Account.
- **Amazon RDS for SQL Server**. Allows you to register a database connected to an AWS Account.

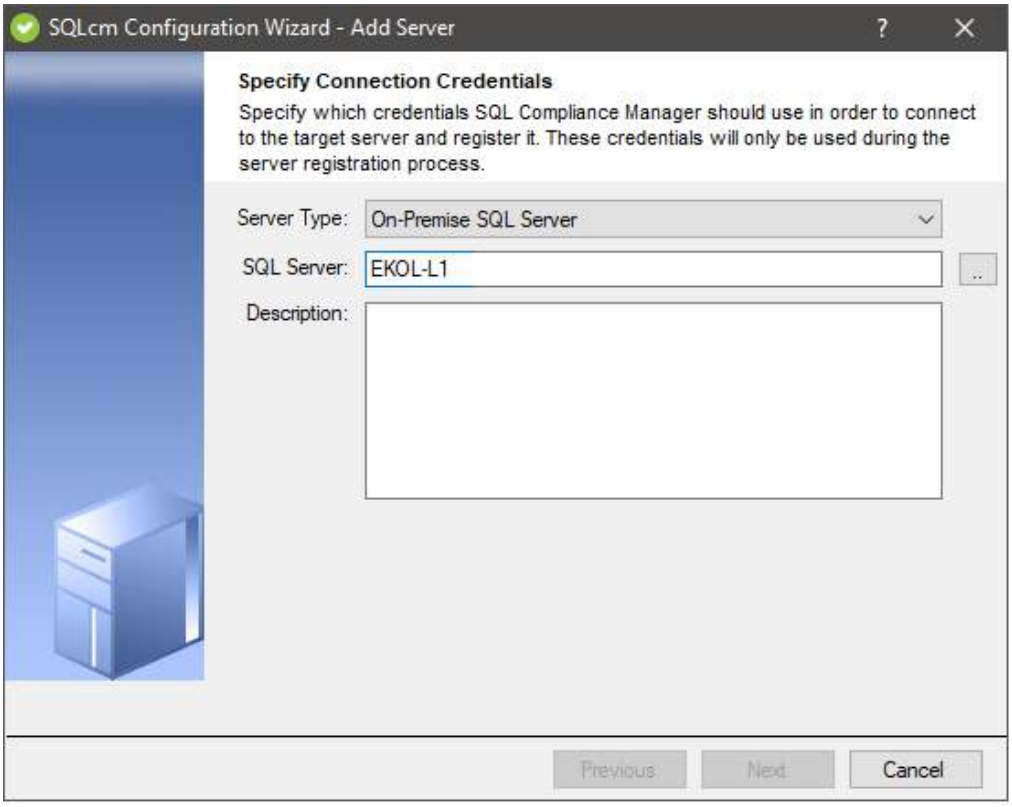


SQL Server

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

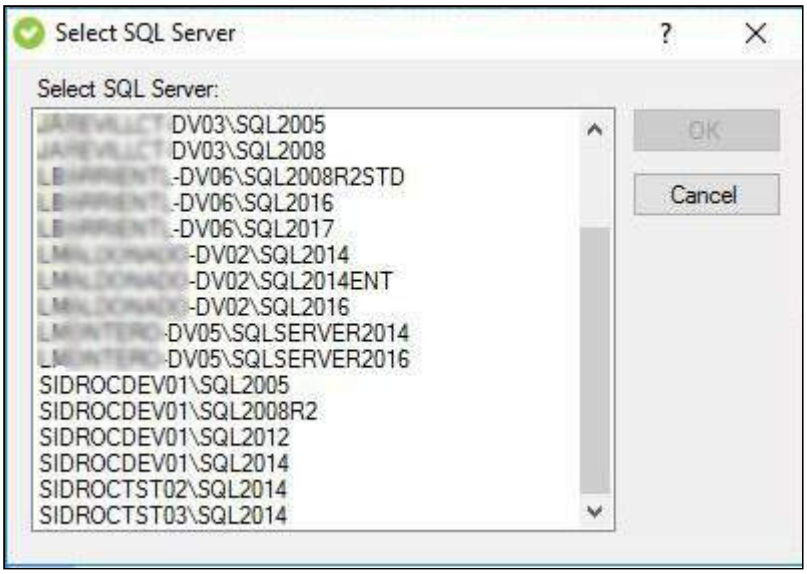
Allows you to specify a description for this instance. The Management Console uses this description when you view SQL Server properties or report on audit data. Consider including information about the databases hosted on this instance, or the organization to which this instance belongs.



Select SQL Server window

The Select SQL Server window allows you to select the SQL Server instance you want to register with IDERA 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.



Configuration wizard - License Limit Reached window

The License Limit Reached window of the Configuration wizard indicates that you have registered the maximum number of SQL Server instances allowed by your IDERA 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 Compliance Manager. For more information, contact IDERA Support.

Configuration wizard - Existing Audit Data window

The Existing Audit Data window of the Configuration wizard indicates that an event database already exists for this SQL Server instance in IDERA 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**.

Configuration wizard - Existing Incompatible Database window

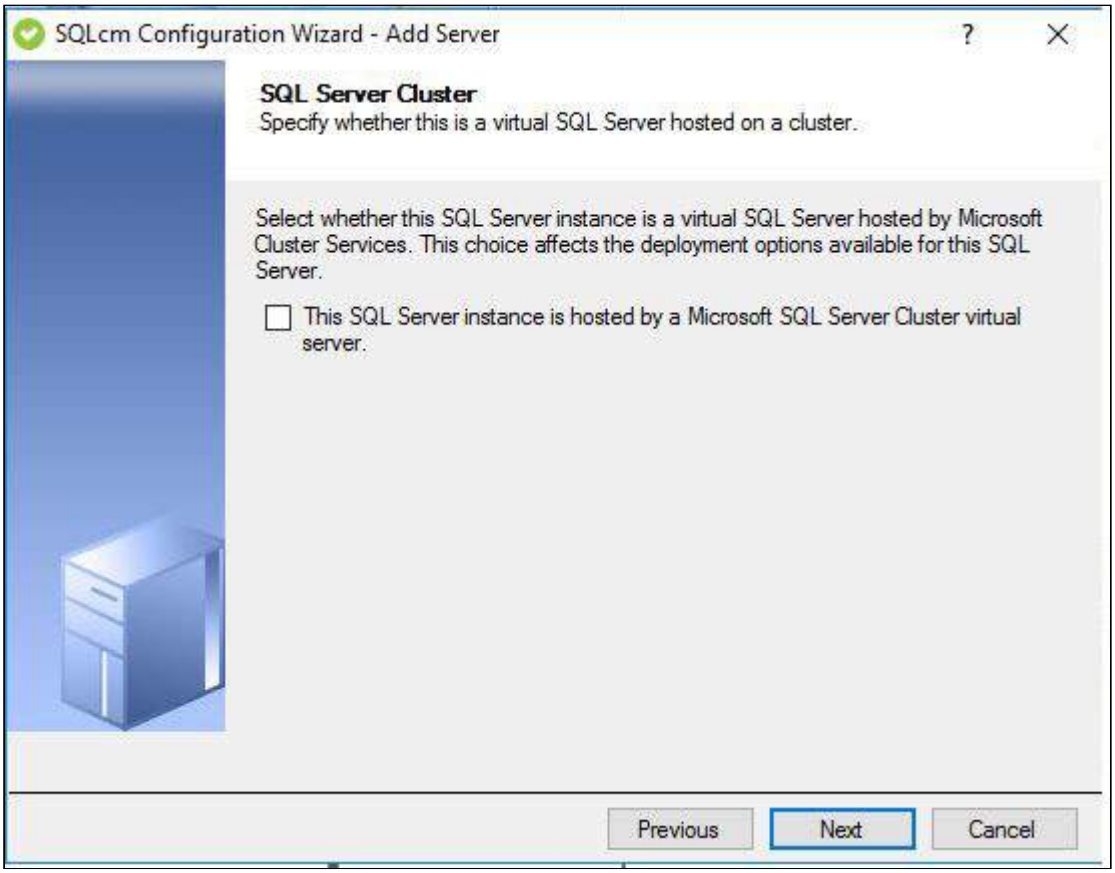
The Existing Incompatible Database window of the Configuration wizard allows you specify how you want to resolve this situation in IDERA SQL Compliance Manager.

Configuration wizard - SQL Server Cluster window

The SQL Server Cluster window of the Configuration wizard allows you to confirm whether the SQL Server instance you want to audit through IDERA 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 SQL Compliance Manager 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 SQL Compliance Manager Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.



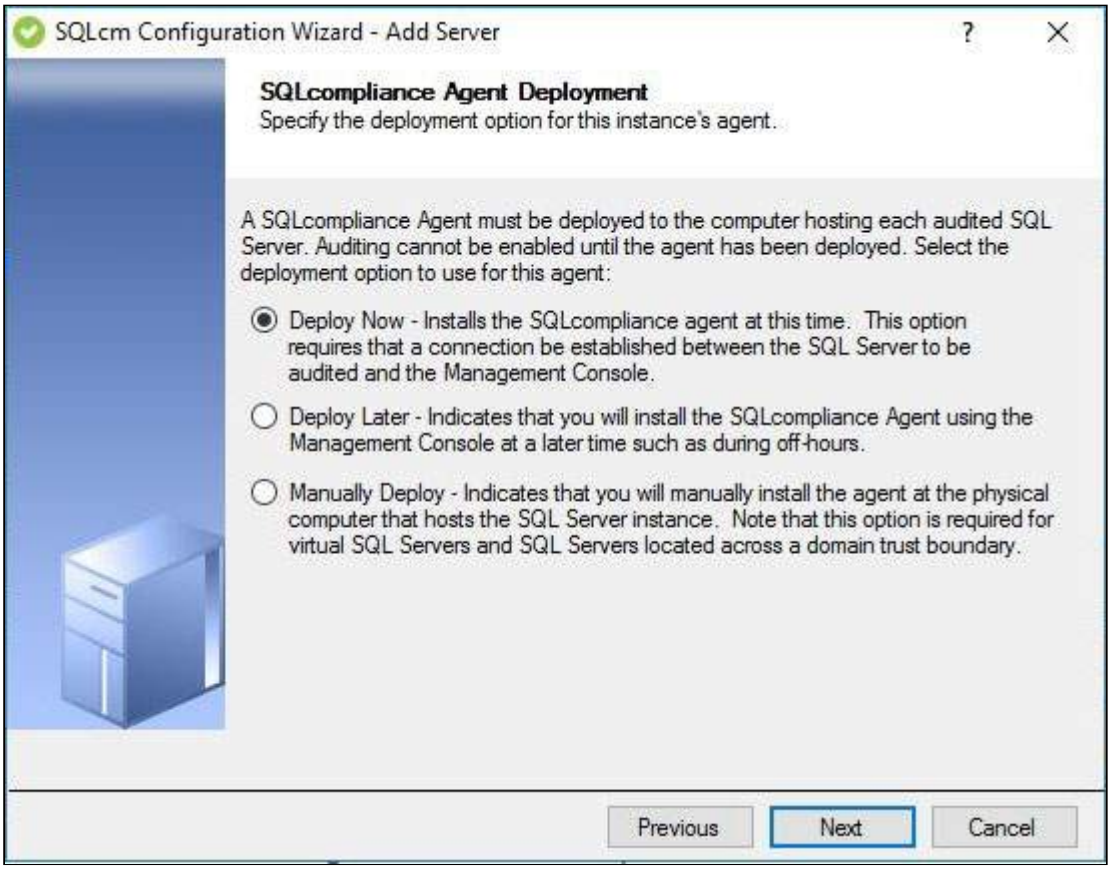
Configuration wizard - SQL Compliance Manager Agent Deployment window

The SQL Compliance Manager Agent Deployment window of the Configuration wizard allows you to choose when and how you want to deploy the SQL Compliance Manager Agent to the target SQL Server instance. You can deploy the SQL Compliance Manager Agent now or later using the IDERA SQL Compliance Manager Management Console, or manually using the setup program.

If you are auditing a virtual SQL Server, you must manually deploy the SQL Compliance Manager Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent. For more information about installing and configuring the SQL Compliance Manager Agent for a virtual SQL Server, see Deploy the SQL Compliance Agent to cluster nodes.

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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent. Select this option when you plan to install the SQL Compliance Manager Agent later using only the Management Console, such as installing during off-hours.

Manually Deploy

Does not install the SQL Compliance Manager 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.

⚠ To manually deploy the SQL Compliance Manager Agent, you need to install the agent using the SQL Compliance Manager installer or the silent command before starting the instance registration process.

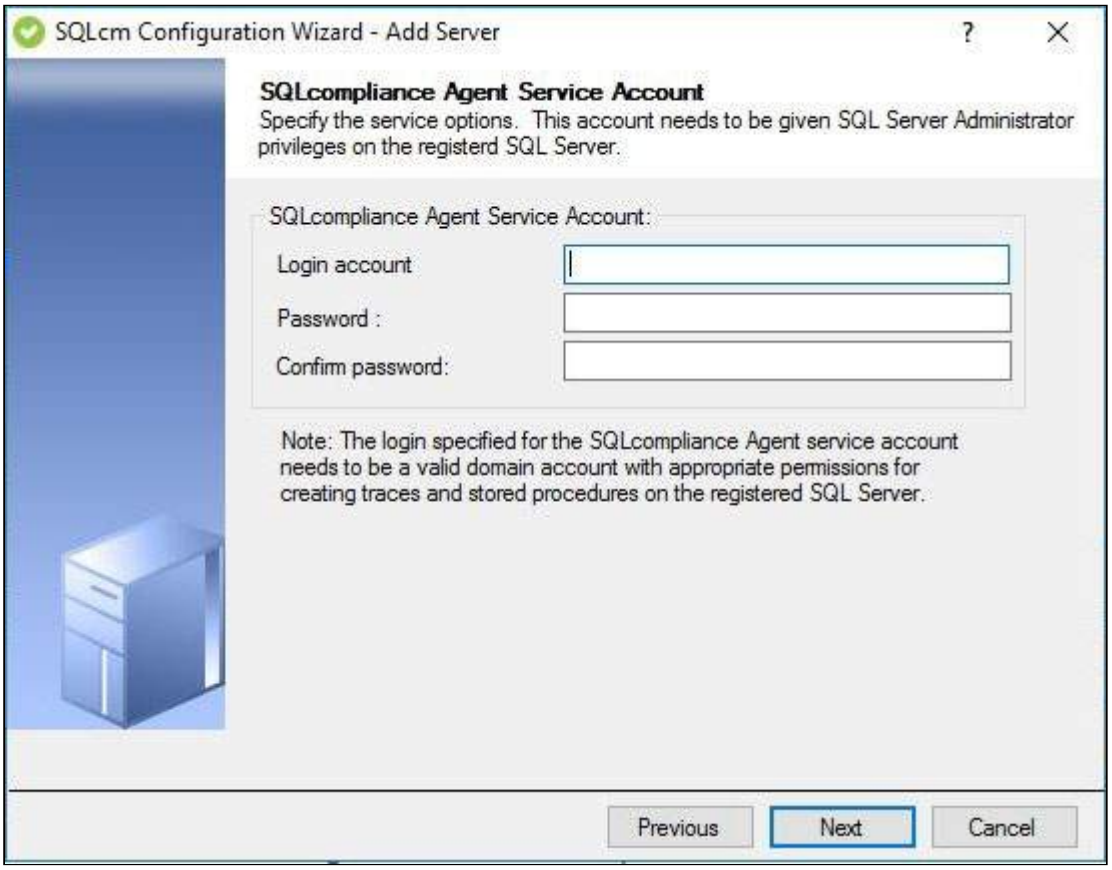
Already Deployed

Display only. Informs you that the SQL Compliance Manager Agent is already deployed on the computer hosting this SQL Server instance.

Configuration wizard - SQLcompliance Agent Service Account window

The SQL Compliance Manager Agent Service Account window of the Configuration wizard is available when you choose to deploy the SQL Compliance Manager Agent now, and allows you to specify the credentials of the account under which the SQL Compliance Manager Agent Service runs. The SQL Compliance Manager 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**.



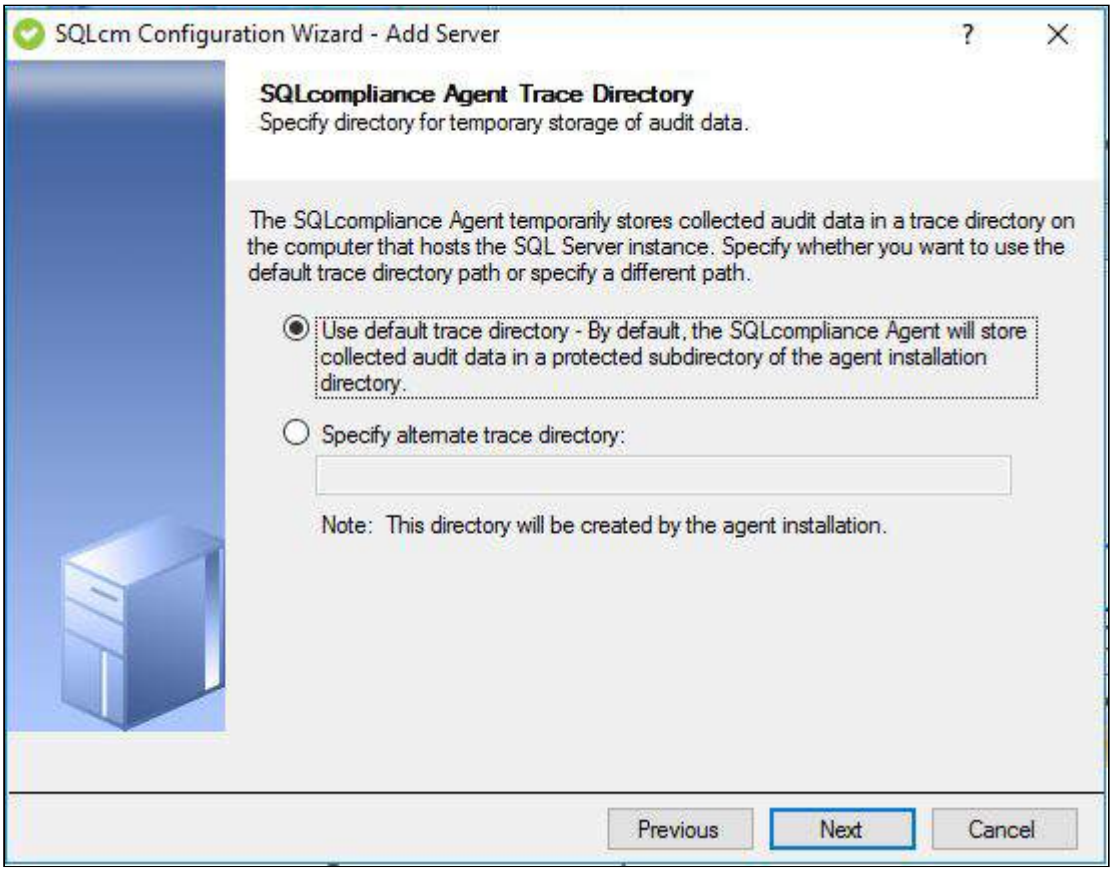
Configuration wizard - SQL Compliance Manager Agent Trace Directory window

The SQL Compliance Manager Agent Trace Directory window of the configuration wizard is available when you choose to deploy the SQL Compliance Manager 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 SQL Compliance Manager Agent stores SQL Server trace files in this directory until the files are sent to the Collection Server.

When SQL Compliance Manager creates the default trace directory, the directory is secured using ACL settings. Only local administrators have read and write access to this folder.

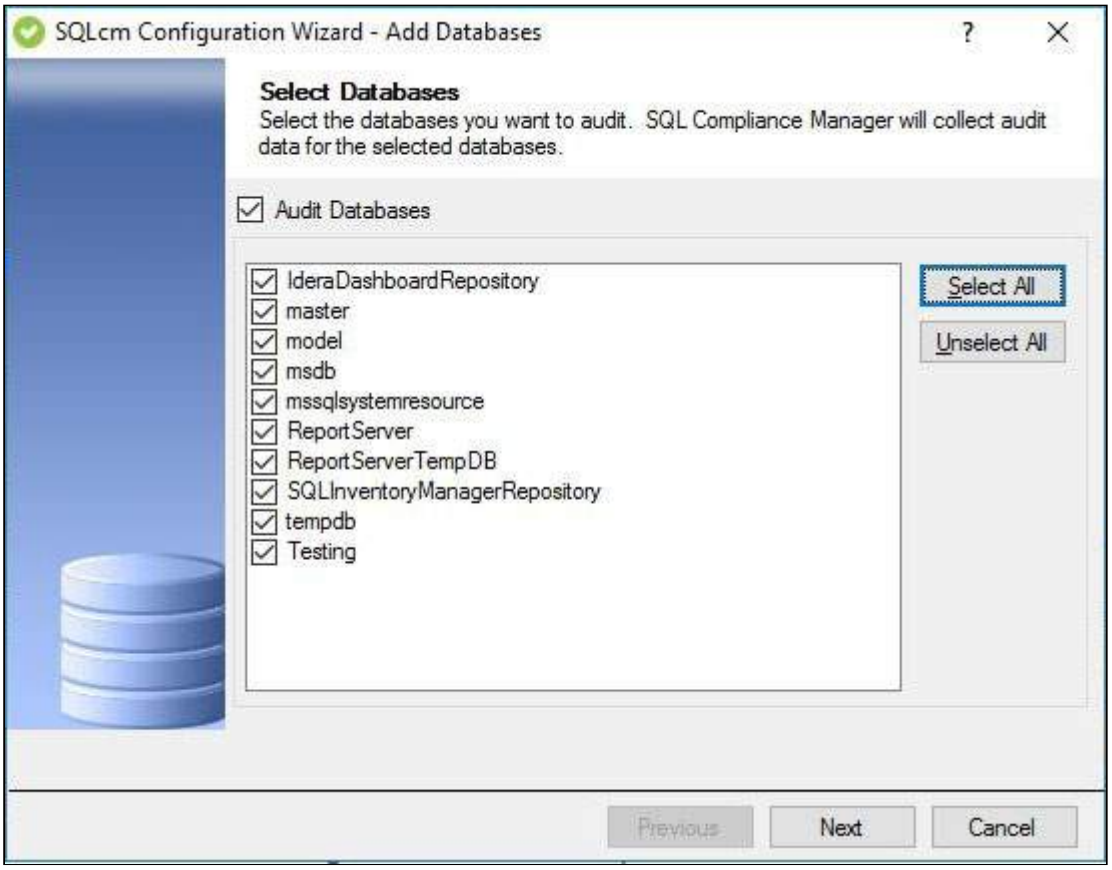
If you specify a different directory path, ensure the SQL Compliance Manager Agent Service account has read and write privileges on that folder. SQL Compliance Manager does not change the security settings on existing folders.

Choose whether you want to use the default path for the agent trace directory, and then click **Next**.



Configuration wizard - Add Databases window

The Add Databases window of the Configuration wizard allows you to select one or more user databases to audit. When you choose to audit a database, IDERA 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

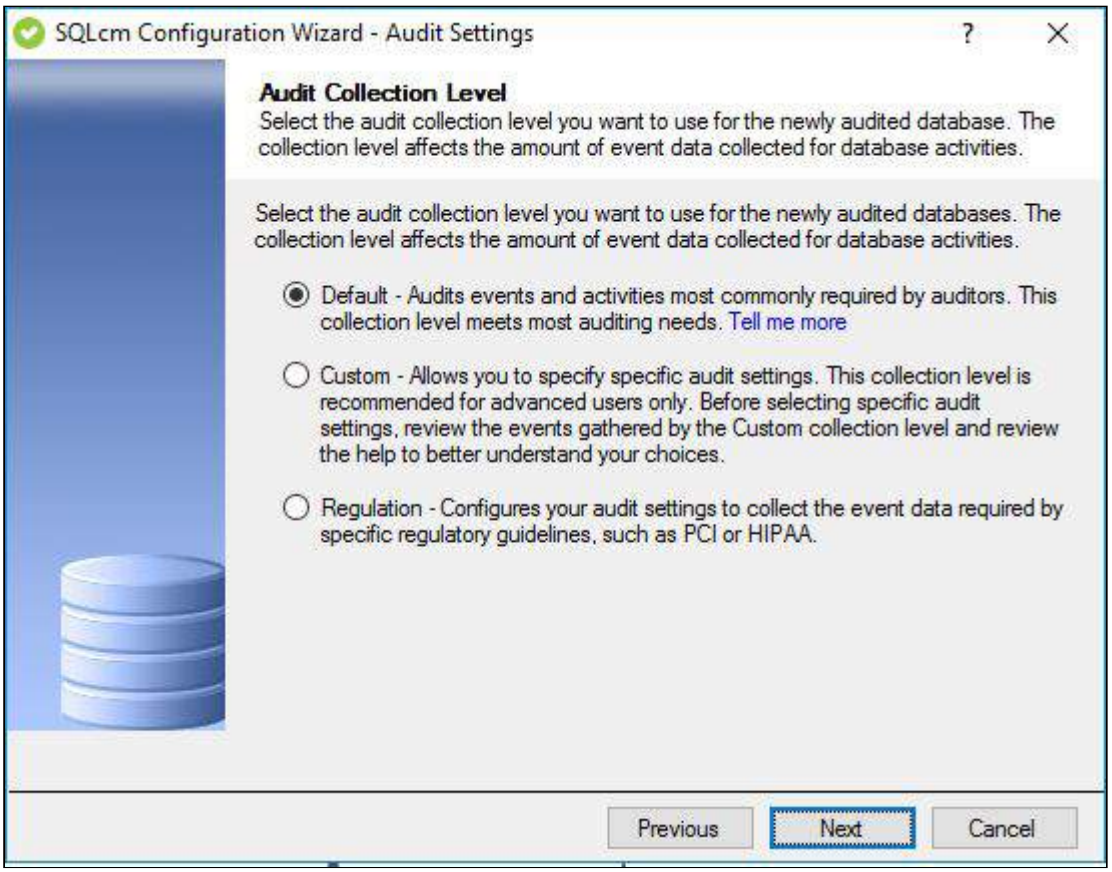
User Databases

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 - Audit Collection Level window

The Audit Collection Level window of the Configuration wizard 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 IDERA 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

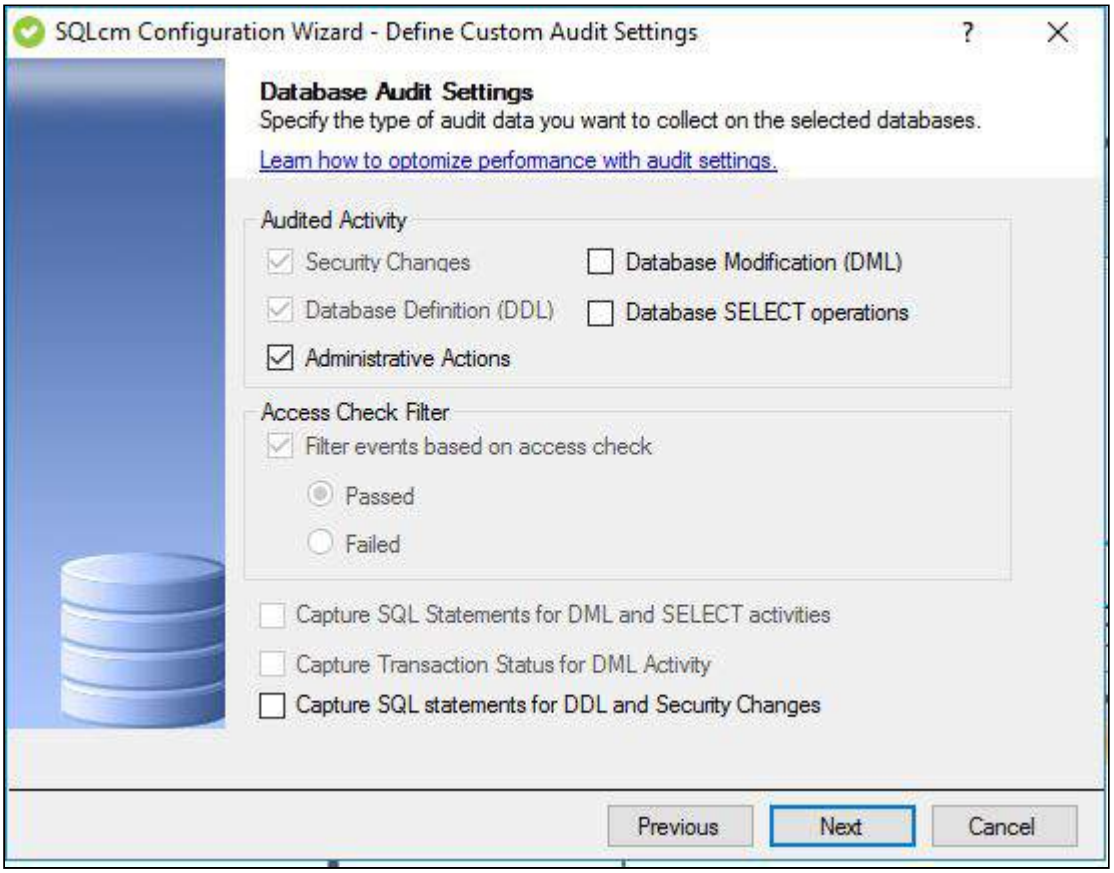
Choosing the **Custom** audit collection level allows you to specify the activities and SQL events you want to audit on these databases. You can also audit system tables. The **Custom** collection level is recommended for advanced users, or for cases in which only one type of data is required for compliance. 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

The Database Audit Settings window of the Configuration wizard allows you to specify which types of SQL Server events you want to audit on the selected databases in IDERA 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 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 Compliance Manager 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 - DML and SELECT Audit Filters window

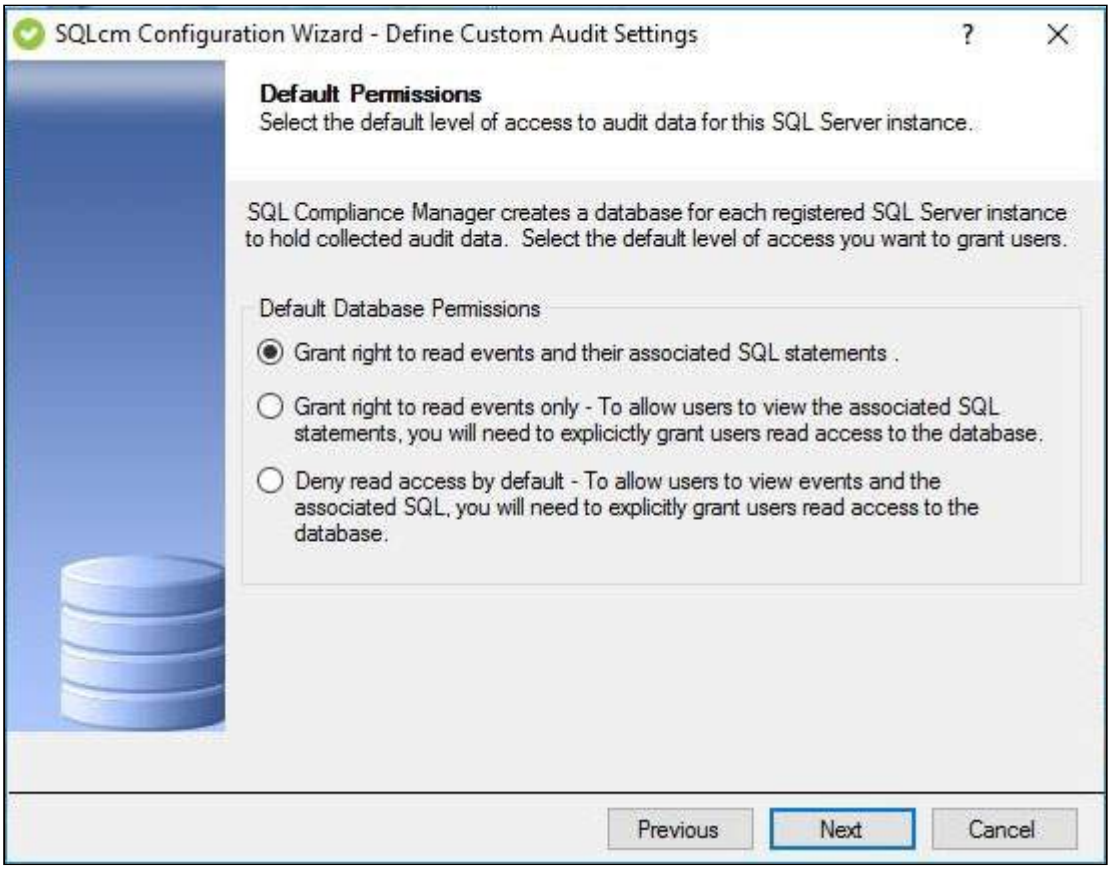
The DML and SELECT Audit Filters window of the Configuration window allows you to specify which database objects you want to audit for DML and SELECT statements in IDERA SQL Compliance Manager. These settings are available when you choose to audit DML or SELECT statements on the selected databases, and 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 - Default Permissions window

The Default Permissions window of the Configuration wizard lets you specify the default permission settings on the Repository databases that contain audit data for this SQL Server instance in IDERA 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 Compliance Manager 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.

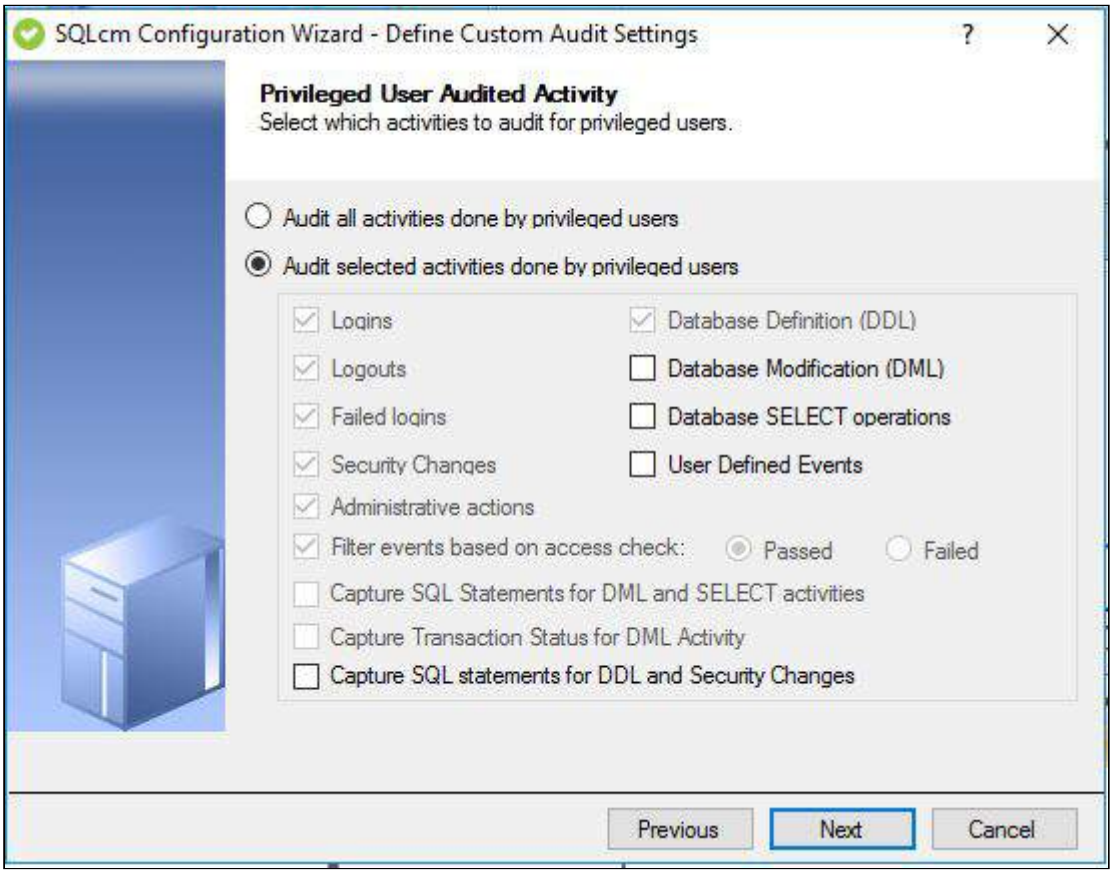
Configuration wizard - Privileged Users Audited Activity window

The Privileged Users Audited Activity window of the Configuration wizard 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 IDERA 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. Available options include:

- Logins
- Logouts
- Failed logins
- Security changes

- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User defined events
- Filter events based on access check.

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.

Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

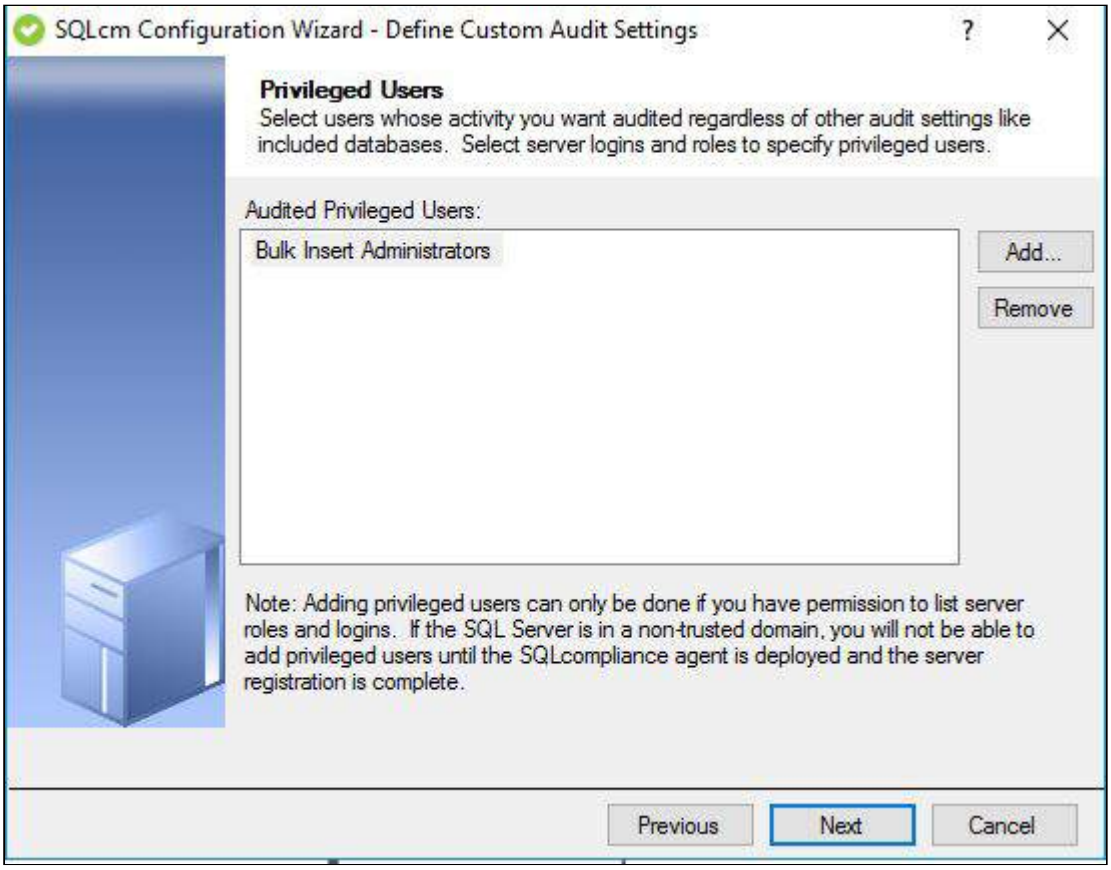
Configuration wizard - Privileged Users window

The Privileged Users window of the Configuration wizard allows you to select which privileged users you want to audit using IDERA 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 SQL Compliance Manager Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent. For more information about installing and configuring the SQL Compliance Manager 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 SQL Compliance Manager 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.

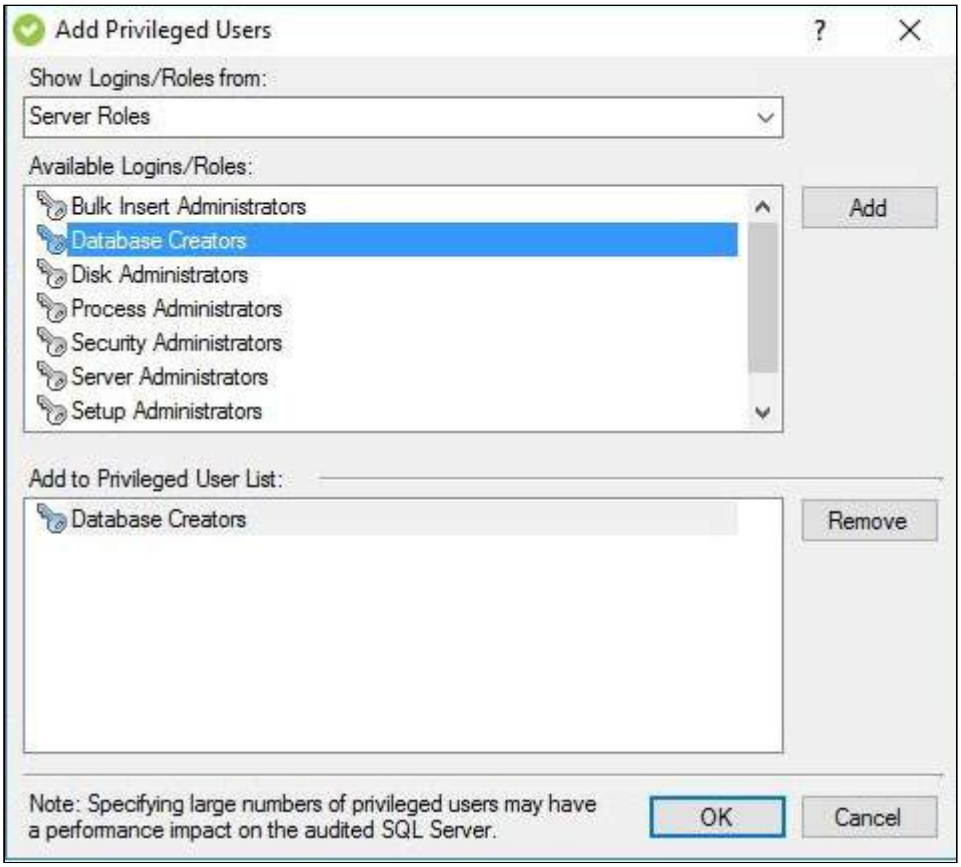
Remove

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 SQL Compliance Manager 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.

Add Privileged Users window

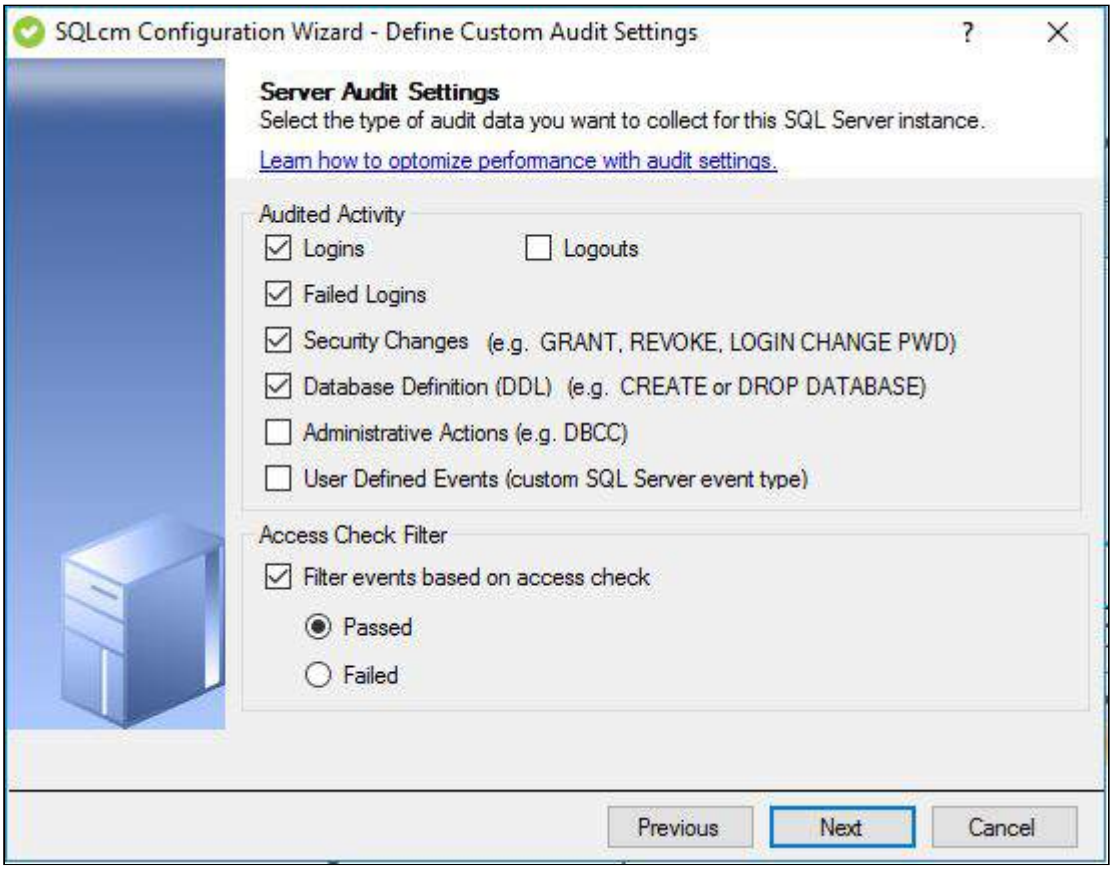
The Add Privileged Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager Agent collects events generated by any login who 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.



Configuration wizard - Server Audit Settings window

The Server Audit Settings window of the Configuration wizard allows you to specify which types of SQL Server events you want to audit on the selected instance. IDERA 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 Compliance Manager 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 Compliance Manager 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

Type of Event Filter	Description
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

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 IDERA 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.

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.

> ⚠ 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.

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 SQL Compliance Manager Agent omits all database-level activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

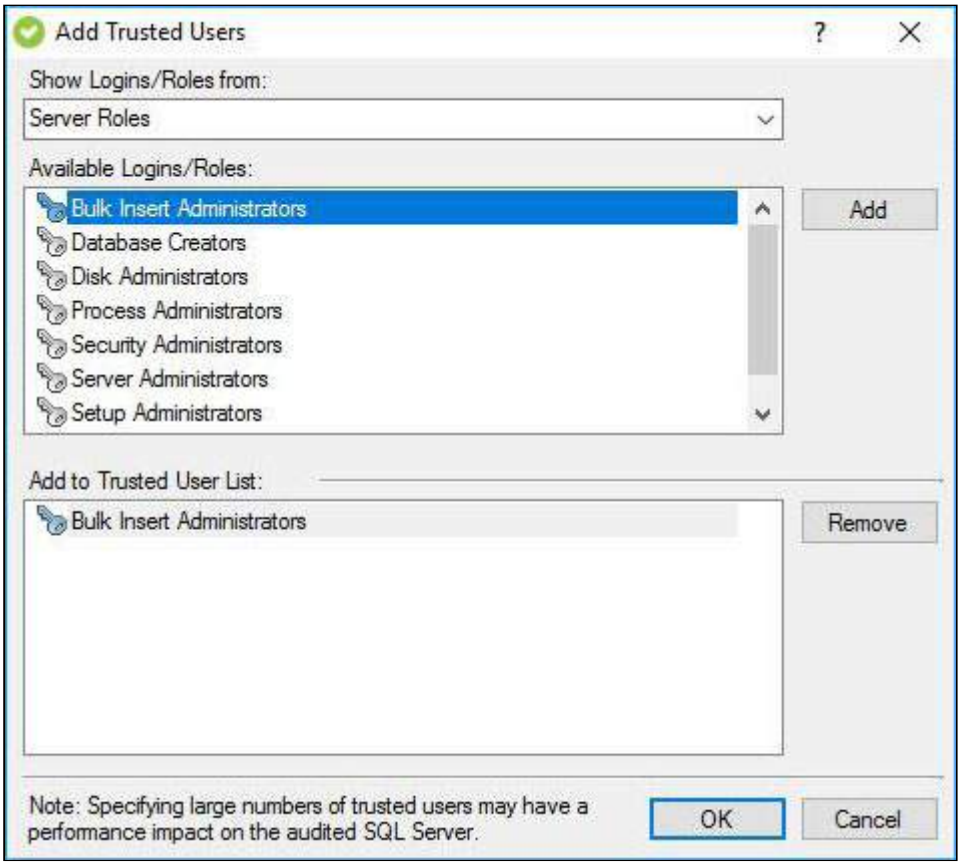
Allows you to designate a previously trusted SQL Server login or role as non-trusted. When a login or role becomes non-trusted, SQL Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

Add Trusted Users window

The Add Trusted Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager Agent collects events generated by any login who is a member of that role.

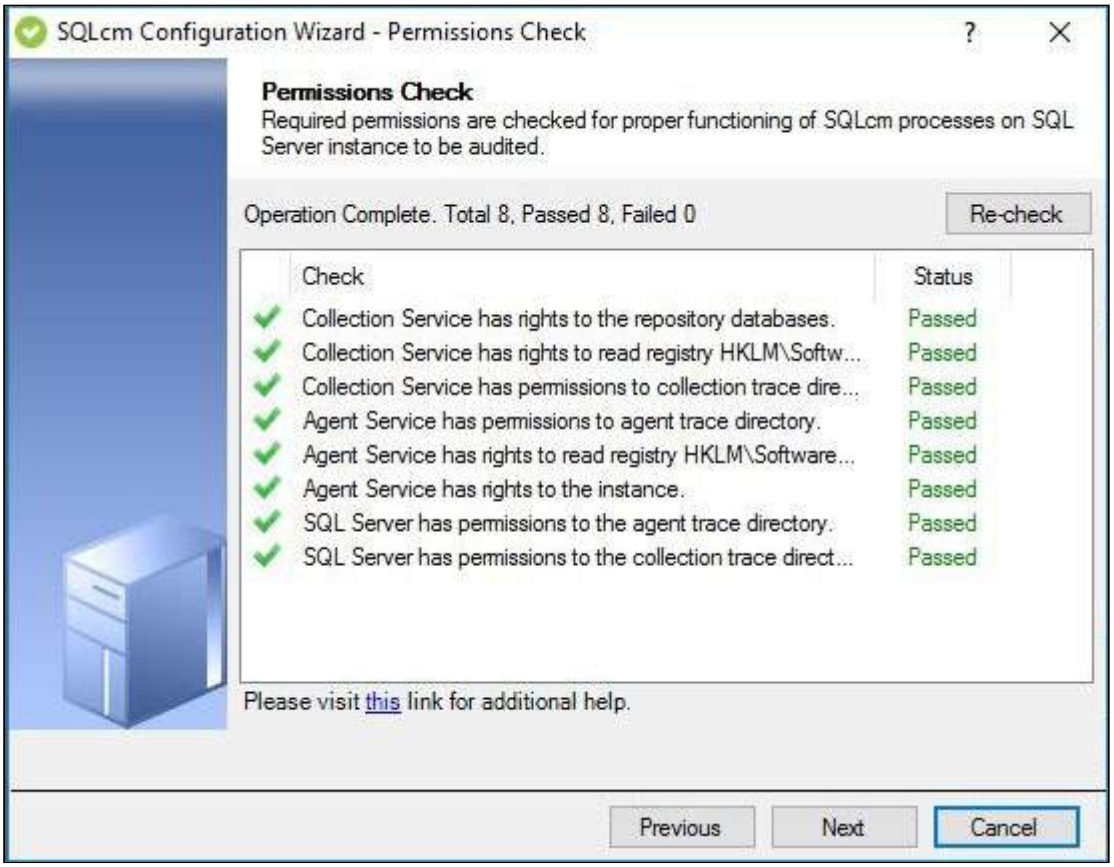
> ⚠ When you designate trusted users, consider limiting your list to a few specific logins. This approach optimizes event processing performance and ensures you filter the intended accounts.

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



Configuration wizard - Permissions Check window

The Permissions Check window of the Configuration wizard displays the results of a check of the permissions required by IDERA 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 is 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.

To successfully run and pass the Permissions Check, make sure you are logged in as one of the following users while registering an instance:

- SQL Compliance Agent Service User

- SQL Server Service User
- Current Logged-in User

For more information, see SQL Compliance Manager Permissions Requirements.

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

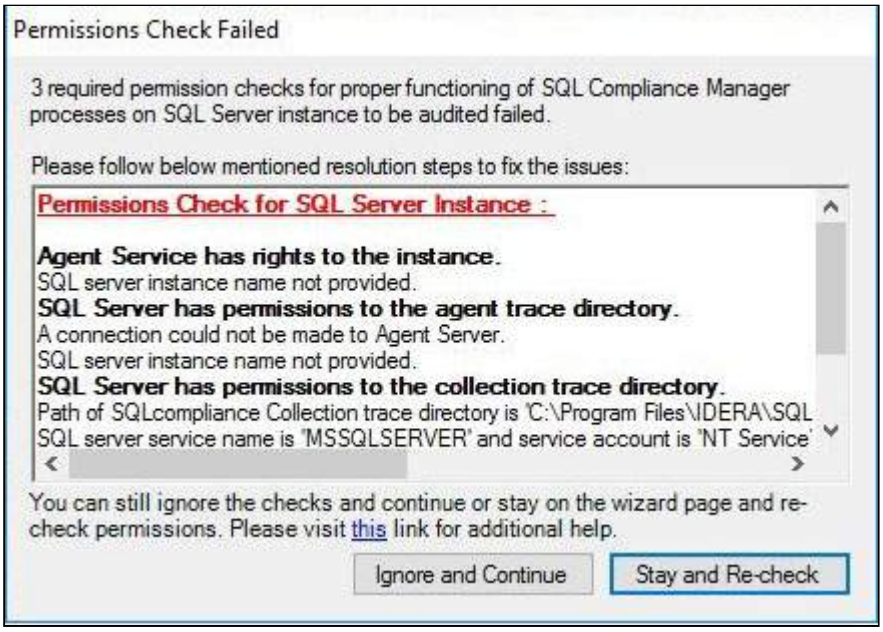
Displays the current status of the associated check. All checks display **Waiting** until run.

Configuration wizard - Permissions Check Failed window

The Permissions Check Failed window of the Configuration wizard 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. SQL Compliance Manager 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 SQL Compliance Manager 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 - Summary window

Use the Summary window of the IDERA SQL Compliance Manager Configuration wizard to review the provided summary, and then click **Finish**. When you complete 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 - Specify Connection Credentials window

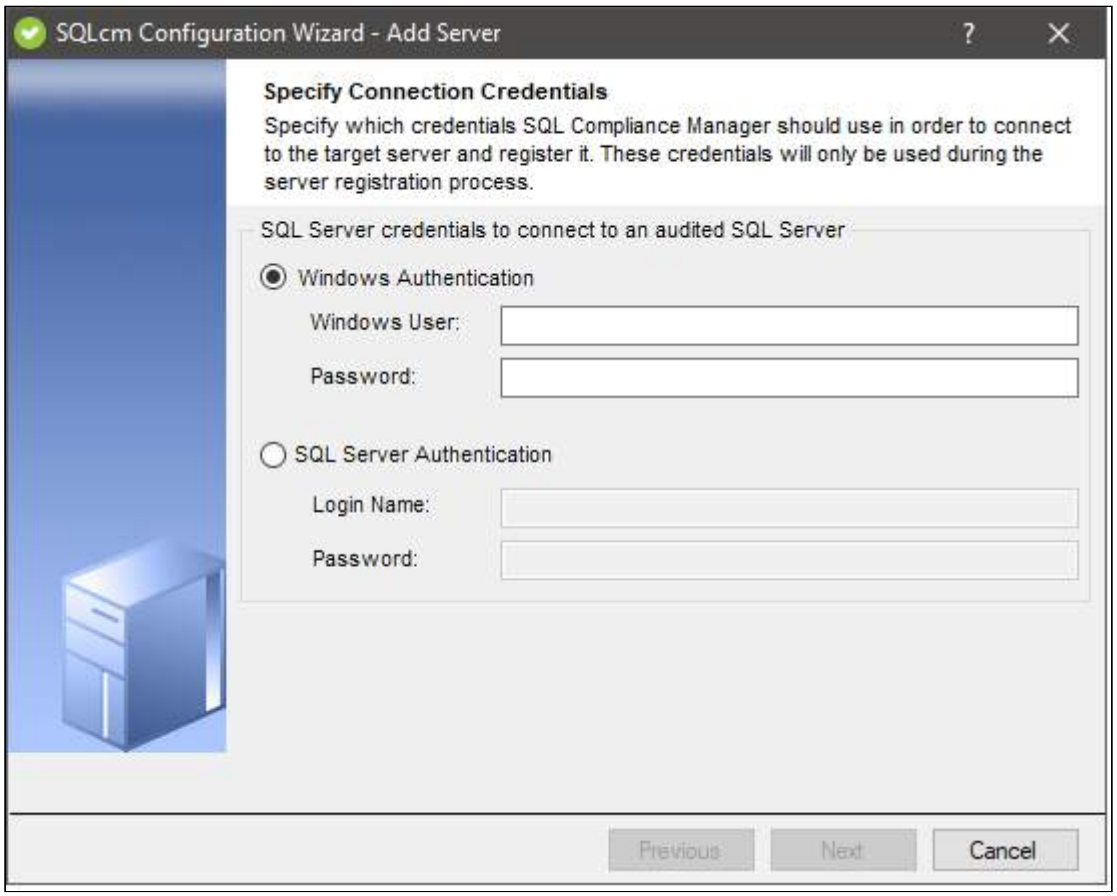
The Specify Connection Credentials window allows you to configure the credentials you want to use to connect to the target server and register it. These credentials will only be used during the server registration.

Specify Connection Credentials

The following options are available for the connection:

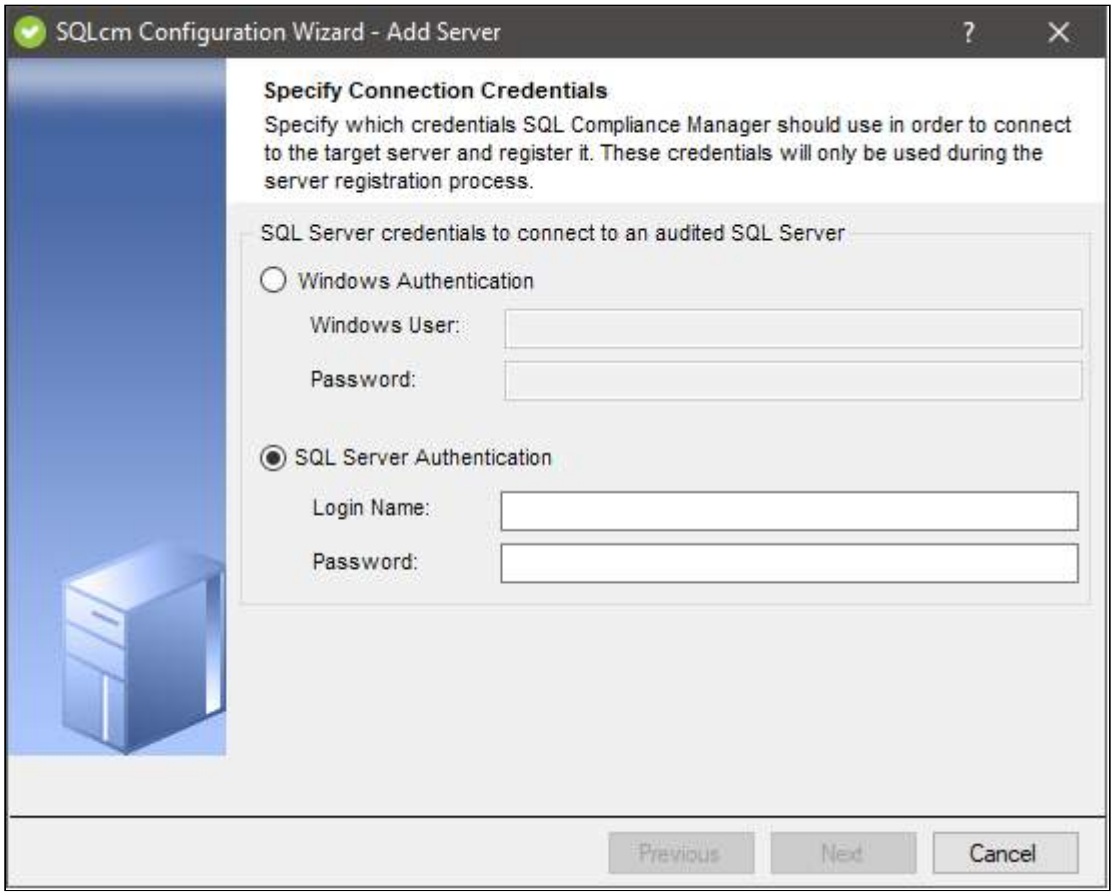
Windows Authentication

Allows you to set a *domain\username* format with Windows Username and Password credentials. This option is set as default for the connection credentials.



SQL Server Authentication

Allows you to register your **SQL Server Agent** credentials for the connection of the registered SQL Server.

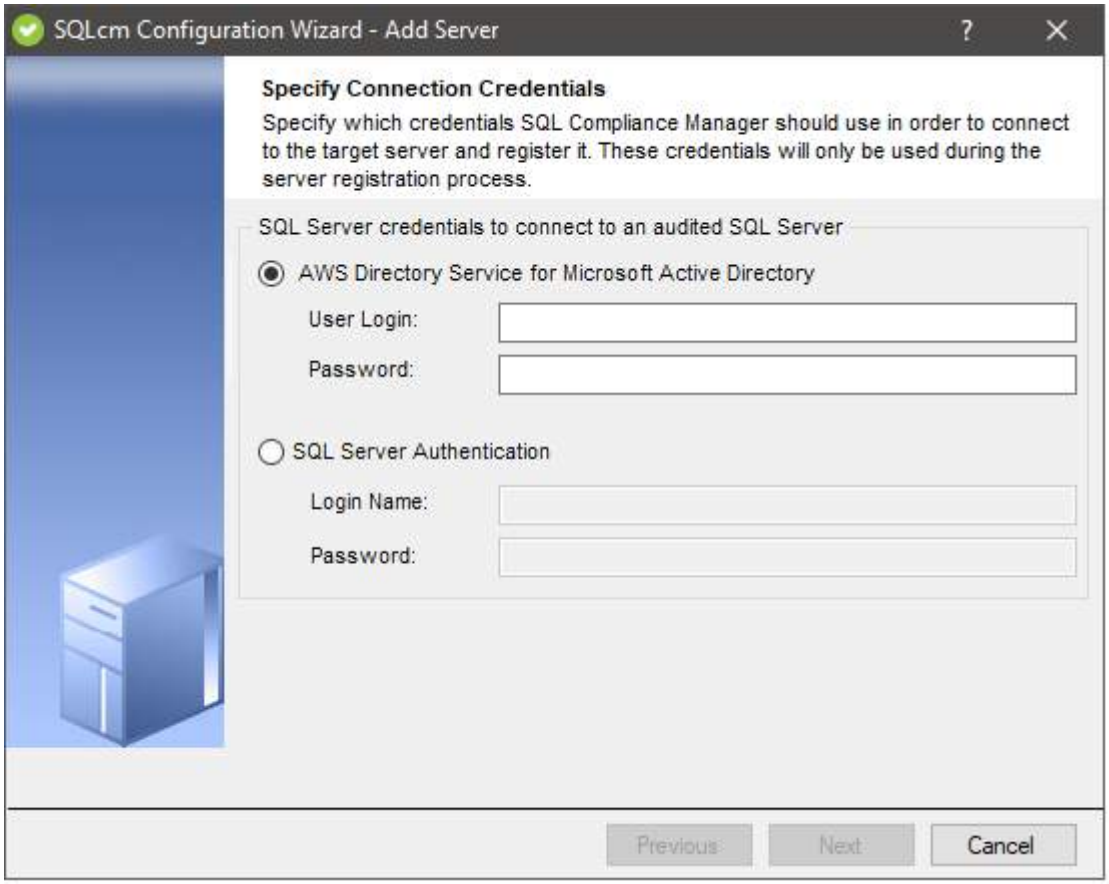


If you want to apply the **Windows Authentication** option, the **SQL Server Authentication** fields gray out and are unusable. The same happens when selecting the **SQL Server Authentication** option.

Amazon RDS for SQL Server

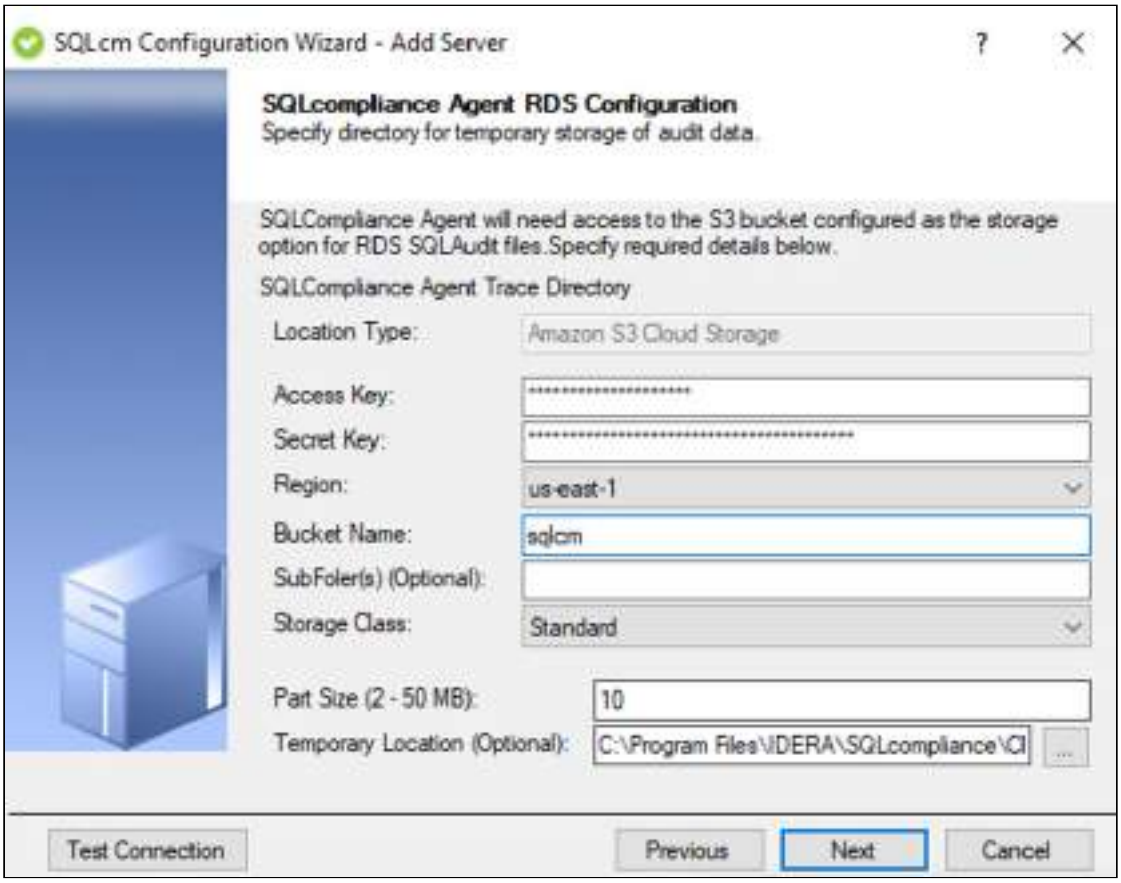
Specify Connection Credentials

Suppose you selected the **Amazon RDS for SQL Server** option in the **Server Type** when adding a server. In that case, the Windows Authentication is replaced with the **AWS Directory Service for Microsoft Active Directory** credentials for the authentication.



SQLcompliance Agent RDS Configuration

Enter the Acces and Secret keys to grant the SQLcompliance Agent access to the S3 Bucket. Next, select a region, type in your Bucket name, and select your desired Storage Class.



Available Fields

Location Type

This field displays the location type.

Access Key

Enter your Access key.

Secret Key

Enter your Secret Key.

Region

Select your region.

> **Note**
>
> RDS does not support the Middle East (Bahrain) region.

Bucket Name

Choose a name for your Bucket. Valid access to the S3 Bucket services is needed.

SubFolders (Optional)

Choose names for any optional subfolders.

Storage Class

Select the Storage class type.

Part Size

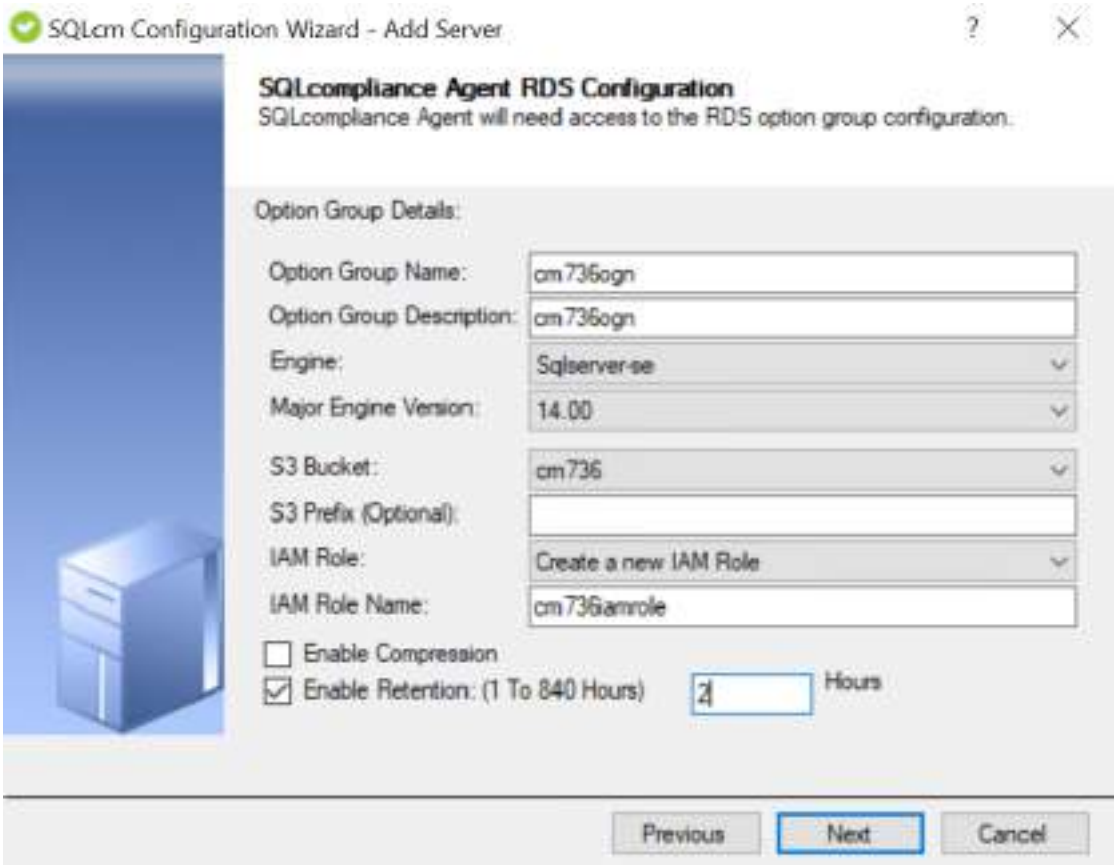
Choose the part size you desire; the part size must be between 2 and 50 MB.

Temporary Location (Option)

Choose a temporary location path.

Agent RDS Configuration - Option Group

Once connected, add the Option Group details by completing the SQLcompliance Agent RDS Configuration settings.



Available Fields

Option Group Name

Choose a unique name for your Option Group within your AWS account. The name can contain only letters, digits, and hyphens.

Option Group Description

Type a brief description of the Option Group.

Engine

Choose your desired DB Engine.

Major Engine Version

Choose the major version of the DB engine of your preference.

S3 Bucket

Select your S3 Bucket from the dropdown list.

S3 Prefix (Optional)

Optionally choose a prefix for your S3 bucket.

IAM Role

Select your IAM role from the dropdown list or create a new IAM Role.

Users can choose an existing or create a new IAM Role and map it to the option group and RDS instance registered.

> **Note**
>
> In case of any incompatibilities on AWS, remain on the screen, select the newly created IAM Role, and map it to the option group and registered RDS instance.

IAM Role Name

Choose a unique name for the new IAM Role.

> **IAM Role**
>
> Newly created IAM roles can be utilized across different SQL server versions.

Enable Compression

Select this checkbox to enable compression.

Enable Retention

Select this checkbox to enable retention.

Retention Window

Input the number of hours for the retention window. The minimum is 1 hour, and the maximum is 840 hours.

Event Alerts tab

The Event Alerts 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 IDERA 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.

Data Alerts Tab

The Data Alerts 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. For more information, see Event Properties.

Alert Message

Allows you to view the message IDERA 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.

Status Alerts tab

The Status Alerts 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 IDERA 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 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.

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 SQL Compliance Manager Agent rule.

Computer Name

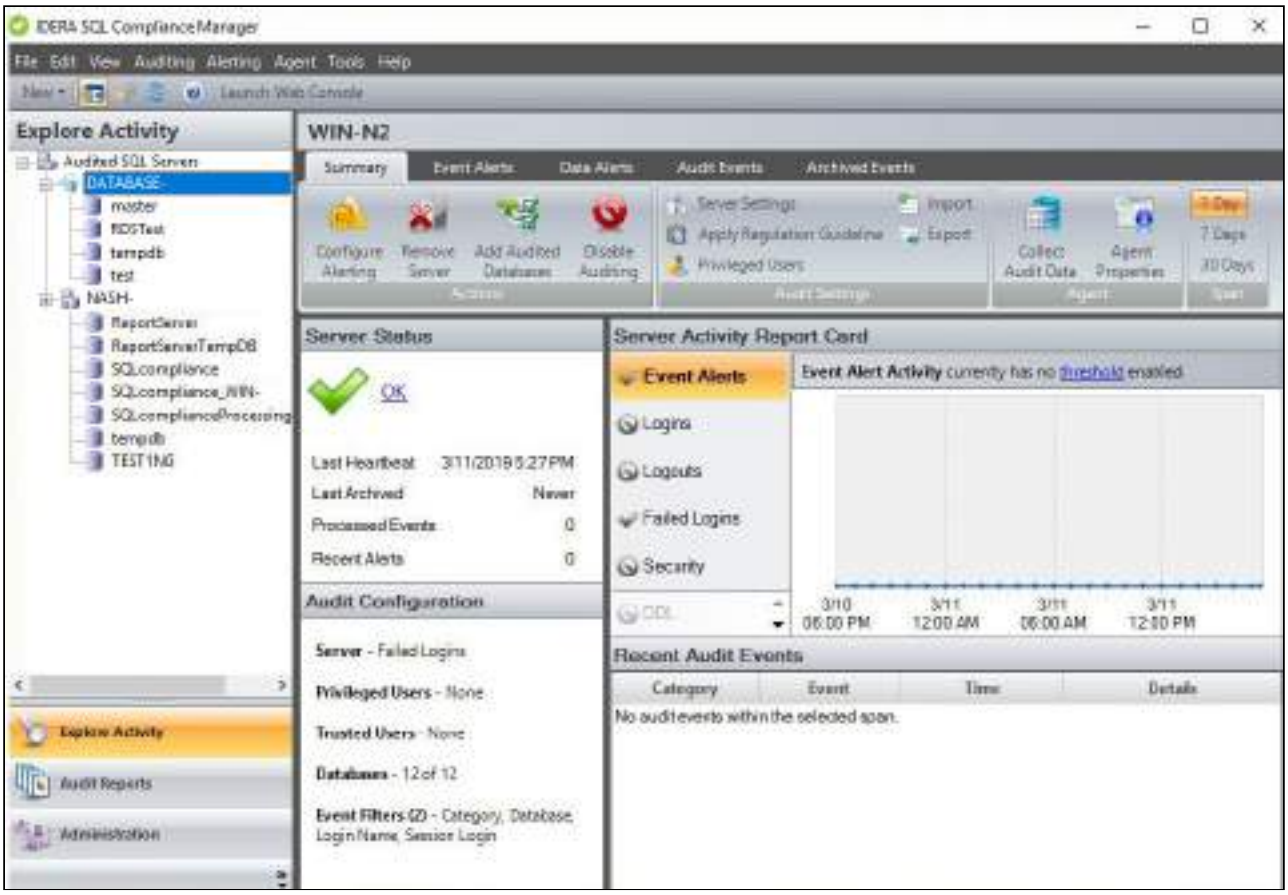
Provides the name of the SQL Server computer hosting the affected instance. For example, if the SQL Compliance Manager Agent or Collection Server trace directory has reached its size limit, this column displays the name of the computer on which the trace directory folder resides.

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 SQL Compliance Manager Agent, this column displays the name of the registered instance to which the agent was deployed.

9.1.3 Explore Activity - Instance View

The Explore Activity Instance view displays the status of audit activity for a particular SQL Server instance in your environment. Use the statistics and graphs from the Summary tab to identify server-level issues, or to configure your desired server-level settings. Use the Event Alerts and Data Alerts tabs to drill on your on specific details of your previously generated Event and Data Alerts. In addition, you can also visit the Audit Events tab to analyze the collected database events, or the Archived Events tab to view your archived databases.

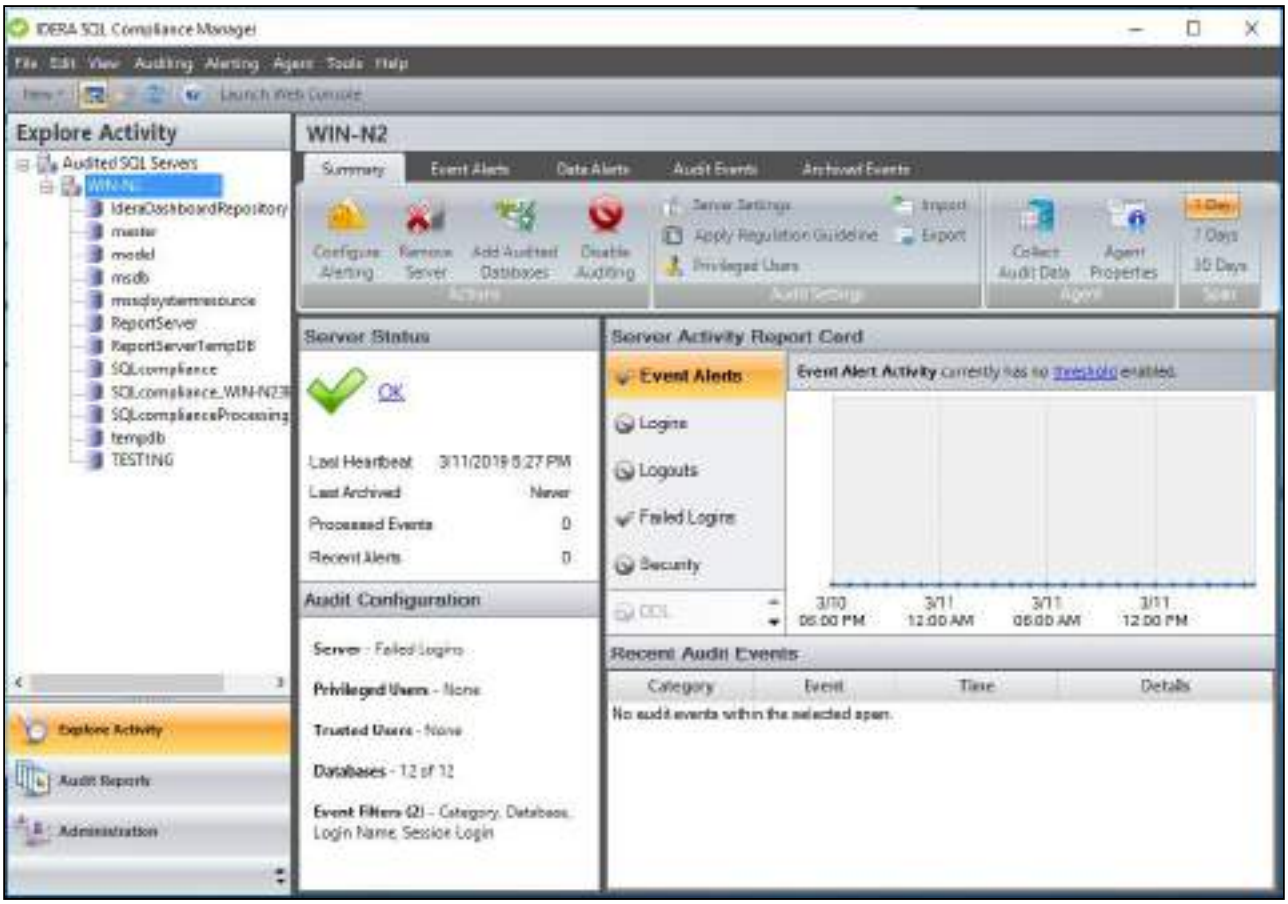


For more information, visit the different tabs for the Explore Activity Instance view below:

- Explore Activity Instance view - Summary tab
- Explore Activity Instance view - Event Alerts tab
- Explore Activity Instance view - Data Alerts tab
- Explore Activity Instance view - Audit Events tab
- Explore Activity Instance view - Archived Events tab

Explore Activity - Instance Summary tab

The IDERA 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 Compliance Manager 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 Compliance Manager deployment may be compromised. For more information, see the Activity Log tab.

Last Heartbeat

Provides the most recent date and time that the SQL Compliance Manager 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 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 audited on instances in your environment and auditing thresholds are set for this event category.
Not audited	red icon	This event category is not 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 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.

Status Type	Indication	Meaning
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 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 audited.

Event Filters

Displays the number of Event Filters created to streamline audit data collected from this SQL Server instance, and the event properties 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 Compliance Manager also uninstalls the SQL Compliance Manager Agent. ***If you manually deployed the SQL Compliance Manager Agent,*** you must manually uninstall it from the SQL Server computer.

⚠ If there are any backlogged audit trace files that you need to process for the instance you are considering to decommission, make sure to disable auditing and decommissioning your server only after processing these backlogged audit trace files. For additional information on how to process backlogged trace files, please contact Idera Support.

Add Audited Databases

Starts the New Audited Database wizard, allowing you to enable auditing on additional databases hosted by this SQL Server instance. For more information, see Add Audited Databases.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQL Compliance Manager 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. For more information. see Disable auditing on a SQL Server.

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. For more information, see Registered SQL Server Properties.

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. For more information, see Apply Regulation Guideline.

Privileged Users

Allows you to change how privileged user activity is audited on the selected SQL Server instance. For more information, see Privileged User Auditing tab.

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 SQL Compliance Manager Agent to send trace files to the Collection Server for processing. Typically, the SQL Compliance Manager 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

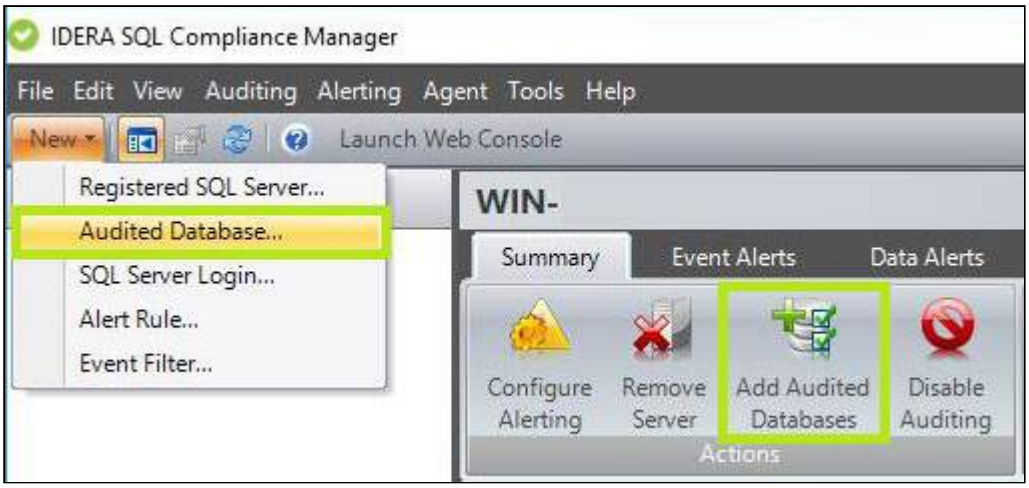
Allows you to view or change the properties, such as the heartbeat interval and the collection interval, of the SQL Compliance Manager Agent deployed to the selected SQL Server instance. For more information, see SQL Compliance Manager Agent Properties.

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.

Add Audited Databases

The Add Audited Databases wizard allows you to enable auditing on additional databases hosted by this SQL Server instance. When you choose to audit a database, IDERA SQL Compliance Manager collects and processes SQL Server events on the database according to your audit settings.

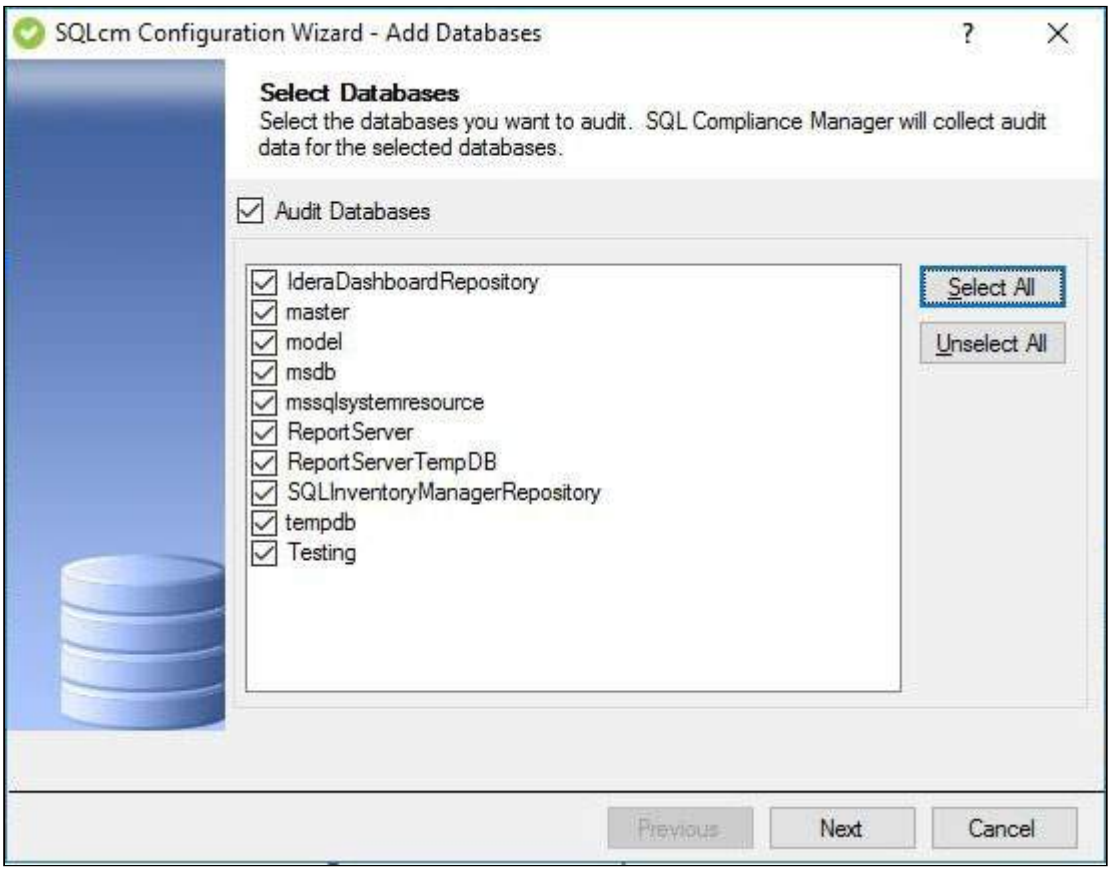


To register databases follow the steps from the Add Audited Databases wizard below:

- Configuration wizard Add Audited Database - Add Databases window
- Configuration wizard Add Audited Database - Audit Collection Level window

Configuration wizard Add Audited Database - Add Databases window

The Add Databases window of the Configuration wizard allows you to select one or more user databases to audit. When you choose to audit a database, IDERA 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

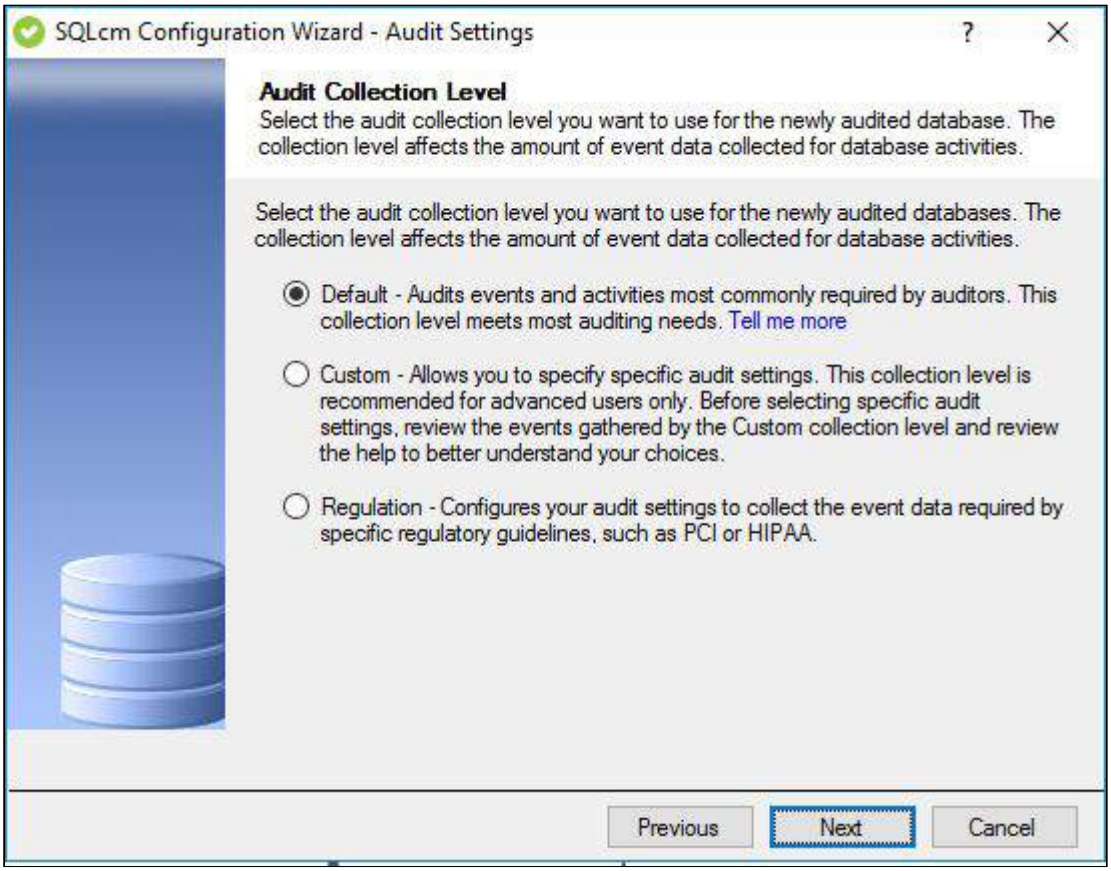
User Databases

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 Audited Database - Audit Collection Level window

The Audit Collection Level window of the Configuration wizard 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 IDERA 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.

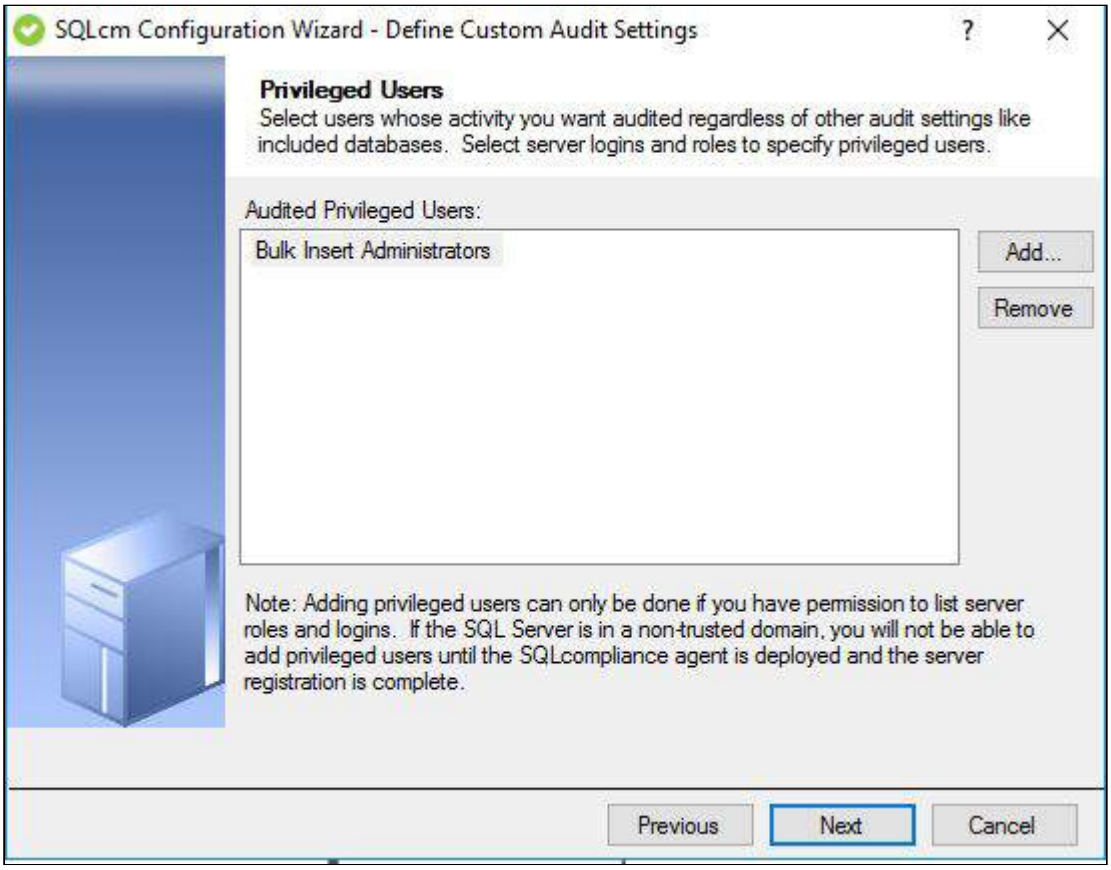
Configuration wizard Add Audited Database - Privileged Users window

The Privileged Users window of the Configuration wizard allows you to select which privileged users you want to audit using IDERA 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 SQL Compliance Manager Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent. For more information about installing and configuring the SQL Compliance Manager 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 SQL Compliance Manager 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.

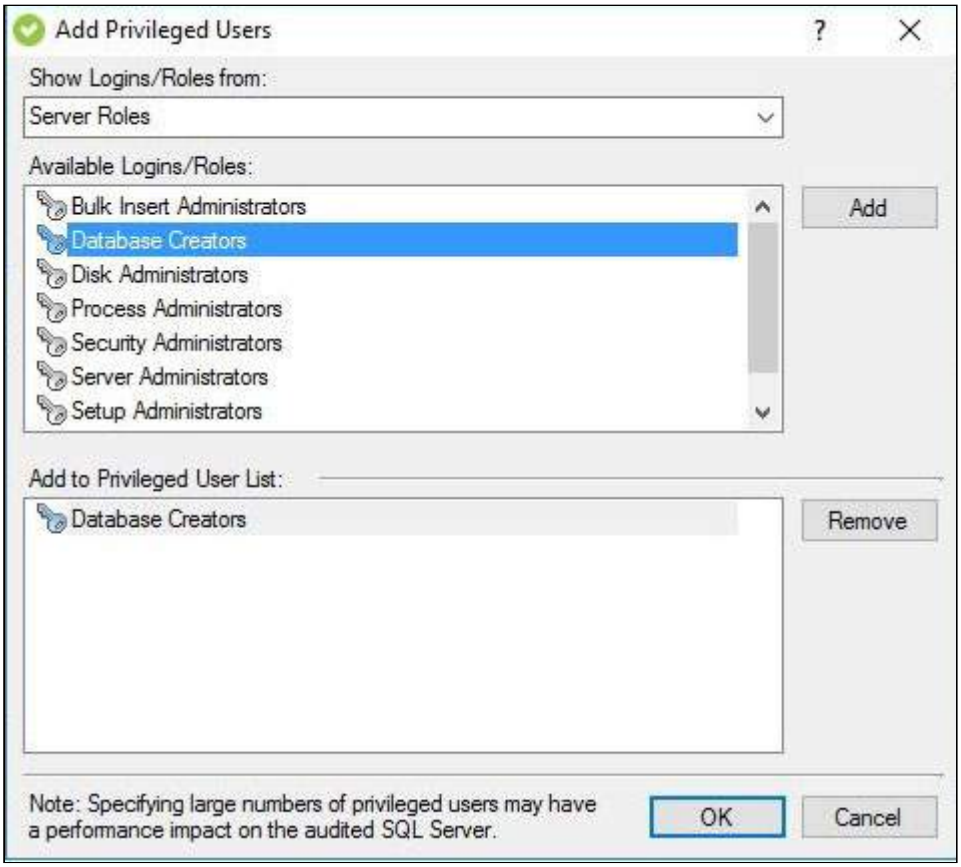
Remove

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 SQL Compliance Manager 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 Add Audited Database - Add Privileged Users window

The Add Privileged Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager 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.



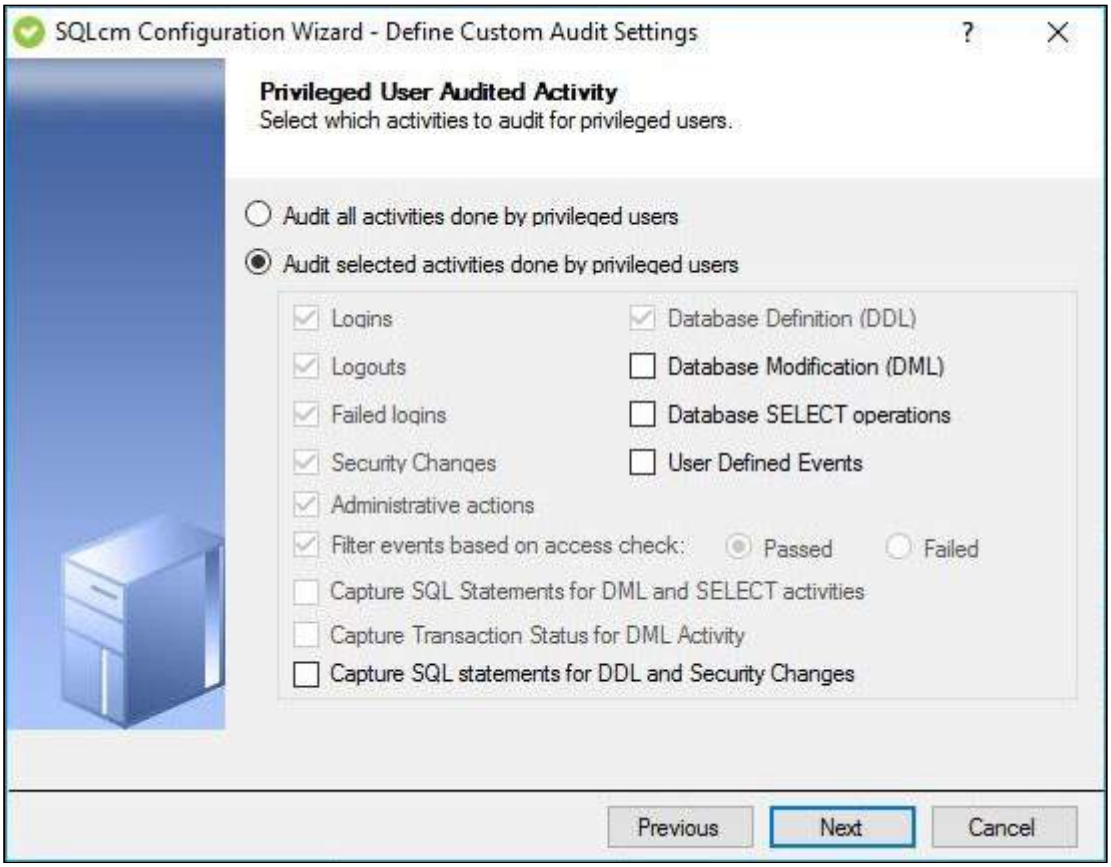
Configuration wizard Add Audited Database - Privileged Users Audited Activity window

The Privileged Users Audited Activity window of the Configuration wizard 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 IDERA 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. Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User defined events
- Filter events based on access check.

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.

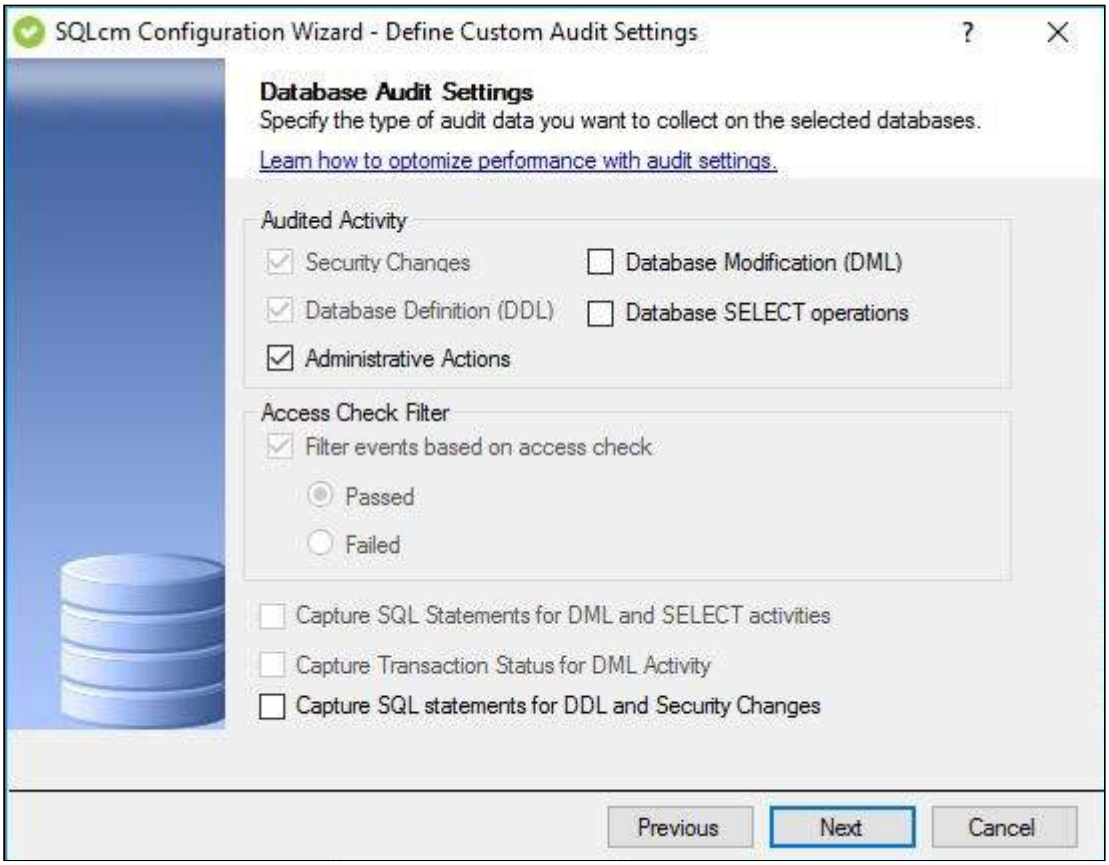
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

Configuration Wizard Add Audited Database - Database Audit Settings window

The Database Audit Settings window of the Configuration wizard allows you to specify which types of SQL Server events you want to audit on the selected databases in IDERA 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 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 Compliance Manager 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

Type of Event Filter	Description
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 Add Audited Database - 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 IDERA 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.

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.

⚠ 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.

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

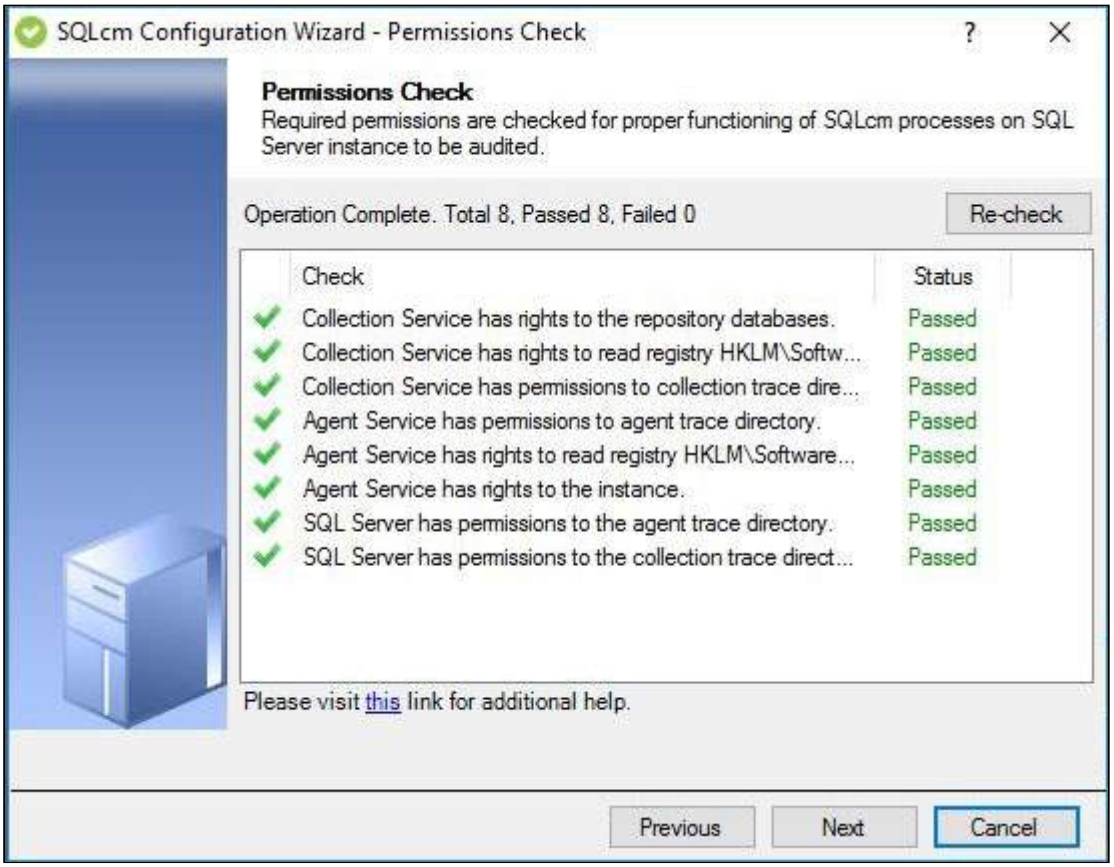
Allows you to select which SQL Server logins or roles you want to trust on this database. When a login or role is designated as trusted, the SQL Compliance Manager Agent omits all database-level activity generated by these logins from the audit data trail.

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 Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

Configuration wizard Add Audited Database - Permissions Check window

The Permissions Check window of the Configuration wizard displays the results of a check of the permissions required by IDERA 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 is 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.

To successfully run and pass the Permissions Check, make sure you are logged in as one of the following users while registering an instance:

- SQL Compliance Agent Service User

- SQL Server Service User
- Current Logged-in User

For more information, see SQL Compliance Manager Permissions Requirements.

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

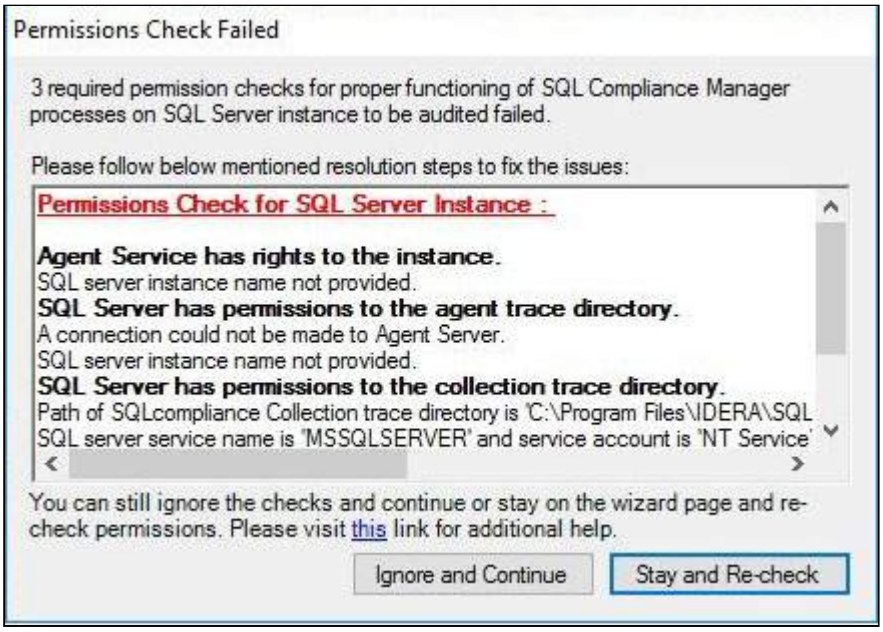
Displays the current status of the associated check. All checks display **Waiting** until run.

Configuration wizard Add Audited Database - Permissions Check Failed window

The Permissions Check Failed window of the Configuration wizard 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. SQL Compliance Manager 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 SQL Compliance Manager 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 Add Audited Database - Summary window

Use the Summary window of the IDERA SQL Compliance Manager Configuration wizard to review the provided summary, and then click **Finish**. When you complete 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.

Registered SQL Server Properties

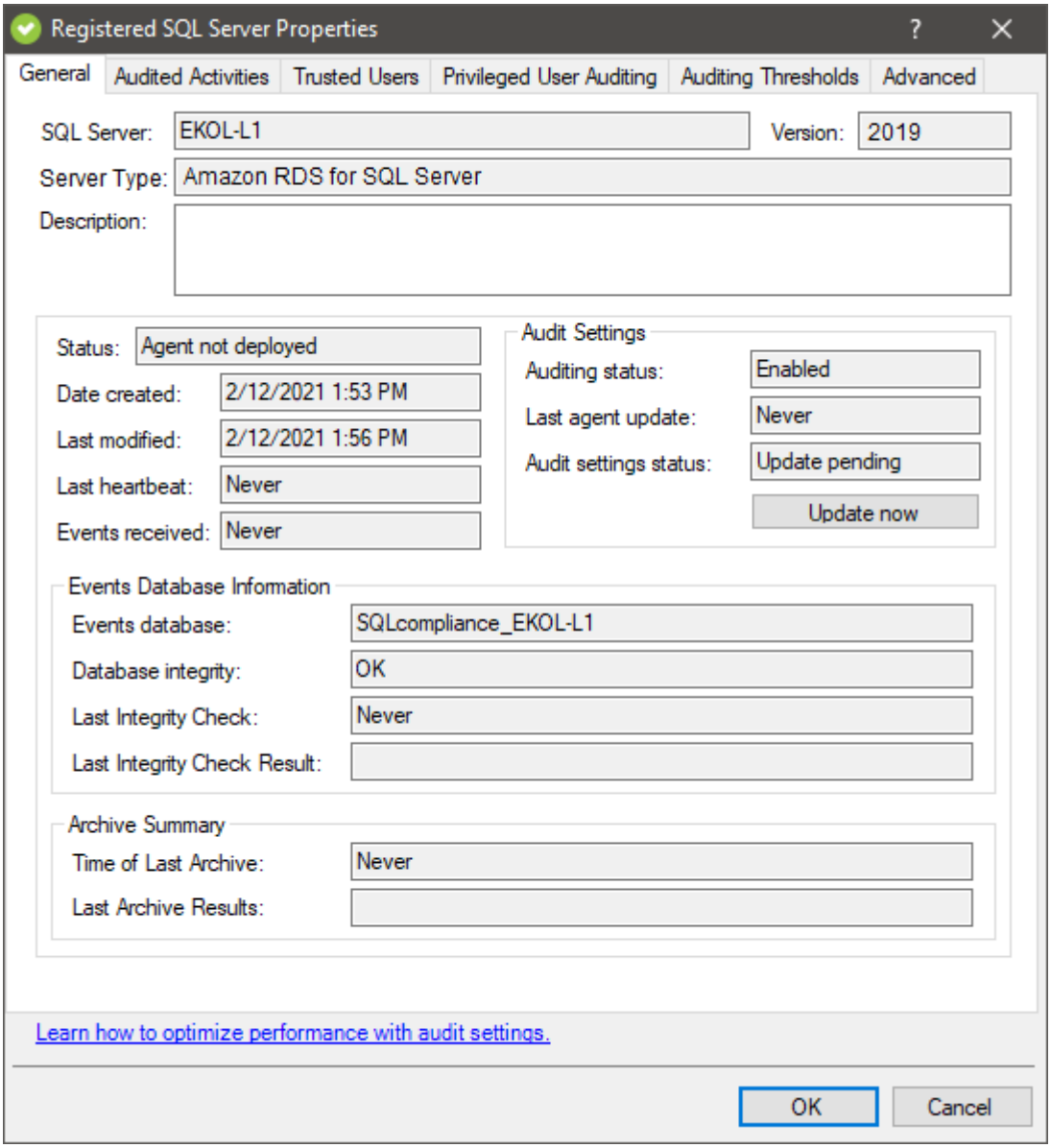
Use the different properties tabs to configure your desired Server audit settings for the selected SQL Server and it´s audited databases.

Use the different tabs to set your Registered SQL Server Properties:

- Registered SQL Server Properties window - General tab
- Registered SQL Server Properties window - Audited Activities tab
- Registered SQL Server Properties window - Trusted Users tab
- Registered SQL Server Properties window - Privileged User Auditing tab
- Registered SQL Server Properties window - Auditing Thresholds tab
- Registered SQL Server Properties window - Advanced tab

Registered SQL Server Properties window - General tab

The General tab of the Registered SQL Server Properties window 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 SQL Compliance Manager 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 SQL Compliance Manager Agent.

To diagnose SQL Compliance Manager Agent issues, check the SQL Compliance Manager Agent status and review the SQL Compliance Manager Agent properties.

Available fields

SQL Server

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.

Server Type

Provides the type of server running on this registered 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 SQL Compliance Manager 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 SQL Compliance Manager Agent auditing this instance contacted the Collect Server. This communication is called a heartbeat. Typically, the SQL Compliance Manager 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 SQL Compliance Manager Agent.

Audit Settings

Provides the following information about the status of your audit settings:

- Whether auditing is enabled on this instance
- When the SQL Compliance Manager 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 SQL Compliance Manager 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.

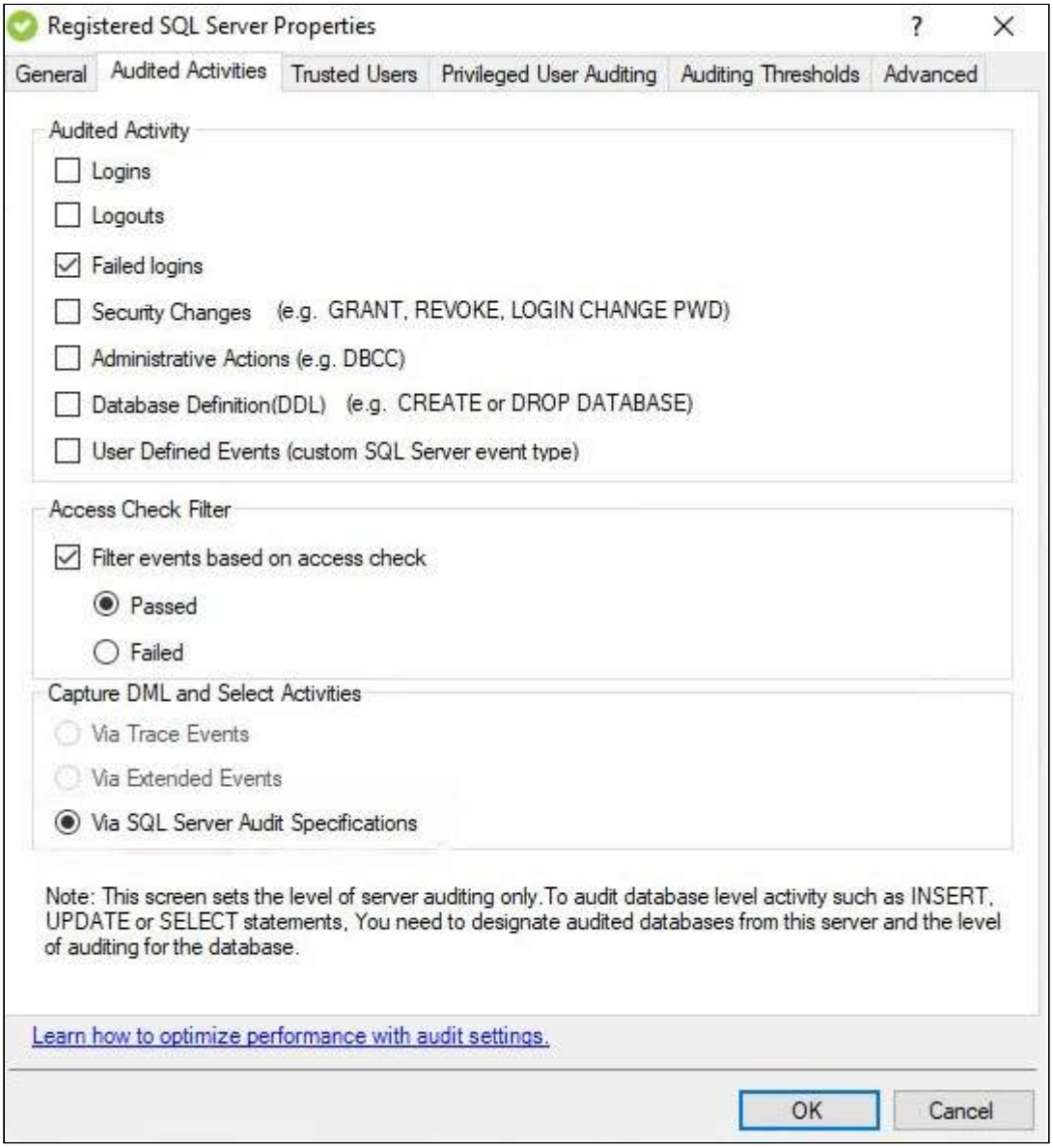
Last Archive Results

Provides the results of the data integrity check. SQL Compliance Manager automatically performs a data integrity check each time you archive audited events from the Repository databases.

Registered SQL Server Properties window - Audited Activities tab

> If you want to use SQL Extended Events as the event handling system for DML and SELECT events occurring on your SQL Server 2012 and later instances, you must enable/disable this feature in the SQL Compliance Manager Web Console. For more information about this feature, see Using SQL Server Extended Events.

The Audited Activities tab allows you to change which types of SQL Server events you want to audit on the selected instance. IDERA SQL Compliance Manager audits these events at the server level only.



Available fields

Audited Activity

Allows you to select the type of activity you want to audit. SQL Compliance Manager collects and processes the corresponding SQL Server events based on your selections.

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.

Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- User-defined events

⚠ Audited Activities selected at Server-level are automatically pre-selected and disabled for selection for Privileged Users added at the Server-level Privileged User Auditing.

ⓘ **Note**

Audited Activities selected at Server-level are no longer pre-selected at the audited activities for the Database auditing level.

Capture DML and Select Activities

For each instance registered, the option of Extended Events is selected by default to capture DML and Select activities. During the upgrade process, SQL Compliance Manager checks for the current saved value for the Capture DML and Select Activities options.

Via Trace Events - Allows you to select Trace Events as your event handling system for DML and SELECT activities. For more information about this feature, see Understanding Traces.

Via Extended Events - Allows you to select SQL Server Extended Events as your event handling system for DML and SELECT events for SQL Server 2012 and later versions. For more information about this feature, see Using SQL Server Extended Events.

⚠ SQL Compliance Manager does not support Extended Events functionality on SQL Server releases earlier than SQL Server 2012, therefore, for the registration of SQL Server instances with versions lower than SQL Server 2012, the Capture DML and Select Activities option is set to Via Trace Events.

Via SQL Server Audit Specifications - Allows you to select SQL Server Audit Logs as your event handling system for DML and SELECT events for SQL Server 2017 and later versions. For more information about this feature, see Using SQL Server Audit Logs.

⚠ SQL Server Audit Specifications is the default Event Collection Method.

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 Compliance Manager collects access check events at the server level.

Select this filter to help identify logins with 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

Registered SQL Server 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 an entire server´s databases. 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. This exclusion occurs for all auditing, including DML and SELECT events related to sensitive columns.

By designating trusted users at server level, you can more efficiently audit servers 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.

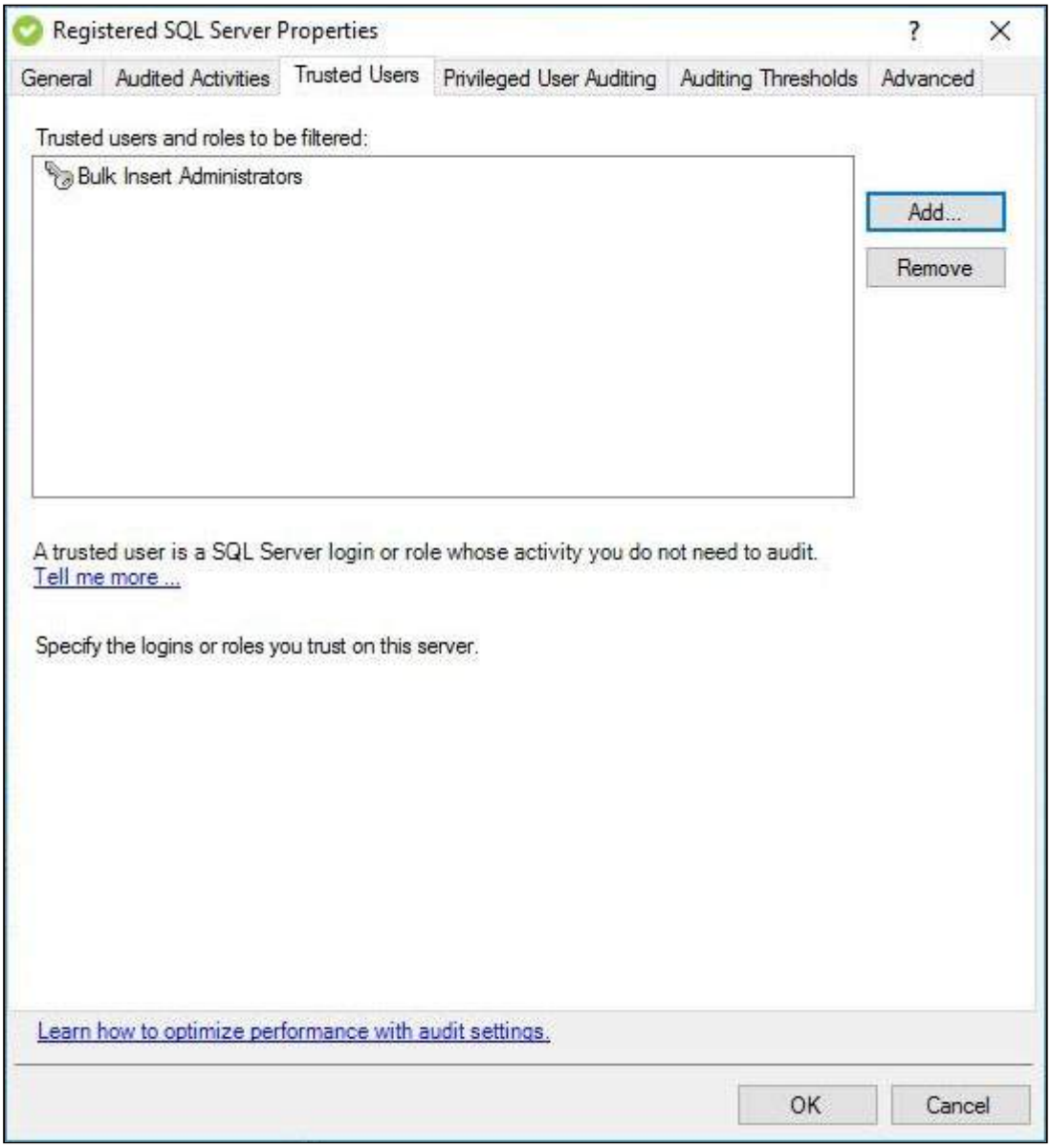
If you are auditing privileged user activity and the trusted user is also a privileged user, IDERA SQL Compliance Manager will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited 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.

⚠ Trusted Users applied at Server level will automatically be applied to all databases under the selected Server.

⚠ 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.

ⓘ 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 for this server. When a login or role is designated as trusted, the SQL Compliance Manager Agent omits all activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

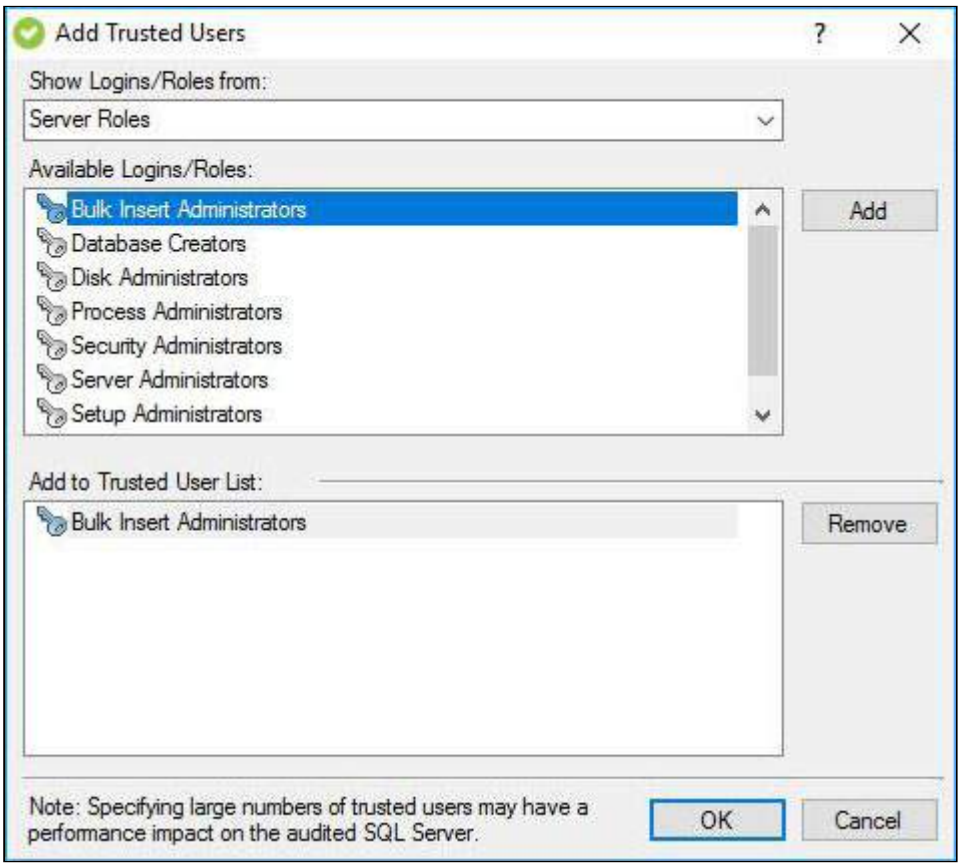
Allows you to designate a previously trusted user or SQL Server role as non-trusted. When a login or role becomes non-trusted, SQL Compliance Manager begins auditing the activity generated by this login or role, based on your current audit settings.

Registered SQL Server Properties - Add Trusted Users window

The Add Trusted Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager Agent collects events generated by any login who is a member of that role.

> ⚠ 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.

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

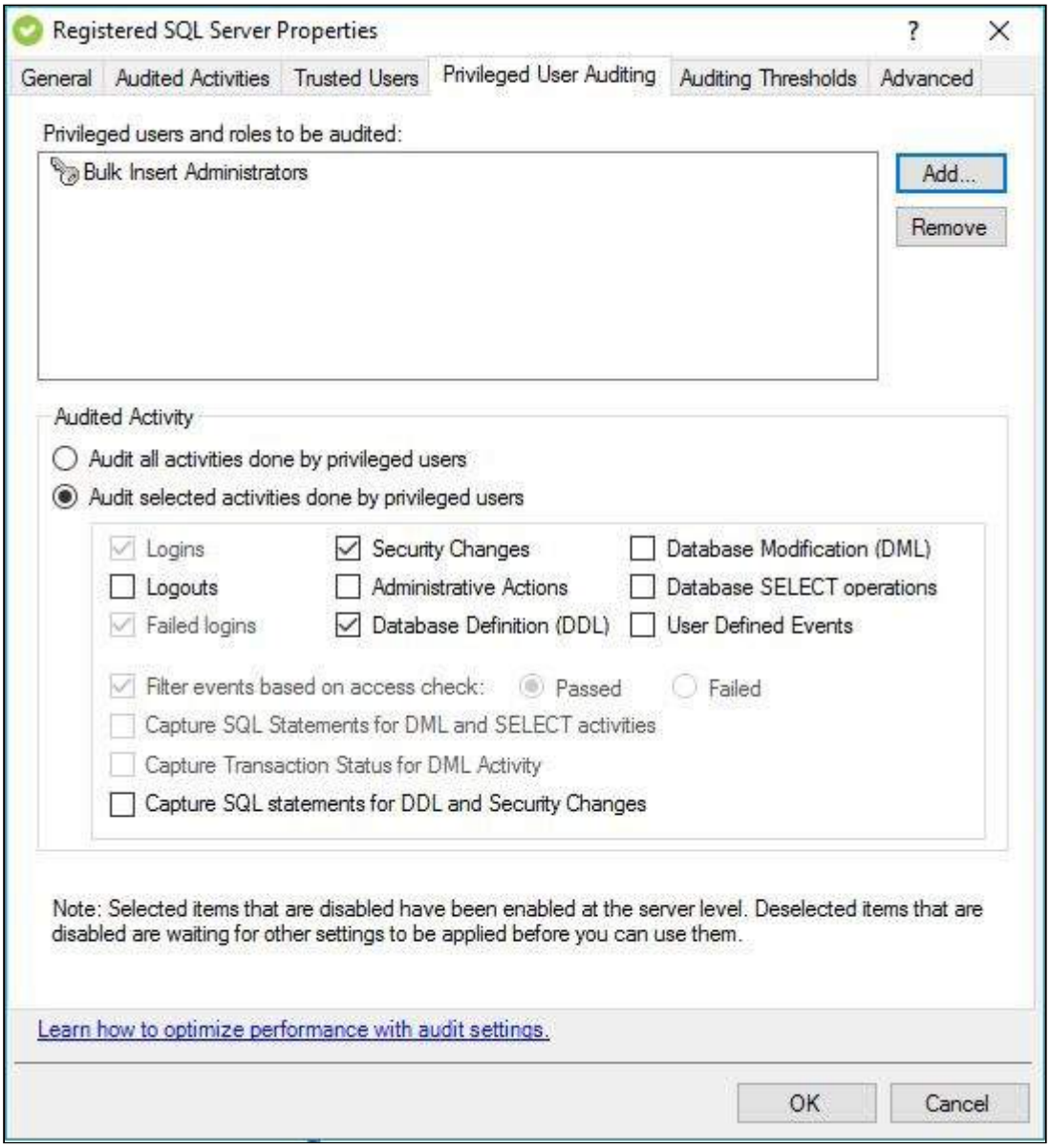


Registered SQL Server Properties window - Privileged User Auditing tab

The Privileged User Auditing tab of the Registered SQL Server Properties window 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 SQL Compliance Manager 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 the 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 SQL Compliance Manager Agent no longer collects events recorded for that login or the role members.

Note

Any Privileged Users added at Server-level are automatically inherited and therefore disabled for selection at the Database Privileged User's settings.

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 SQL Compliance Manager 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. Select **Audit all activities done by privileged users** to include everything or select **Audit selected activities done by privileged users** followed by additional preferences for selective auditing. Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User-defined events
- Filter events based on access check.

Note

Audited Activities configured at Server-level auditing are automatically pre-selected and disabled for selection for Privileged Users added at Server-level auditing. Users must edit changes at the Server-level audited activities tab to disable these settings.

Capture SQL statements for DML and SELECT activities

Allows you to specify whether you want to collect SQL statements associated with audited database modification (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.

Capture SQL statements for DDL and Security Changes

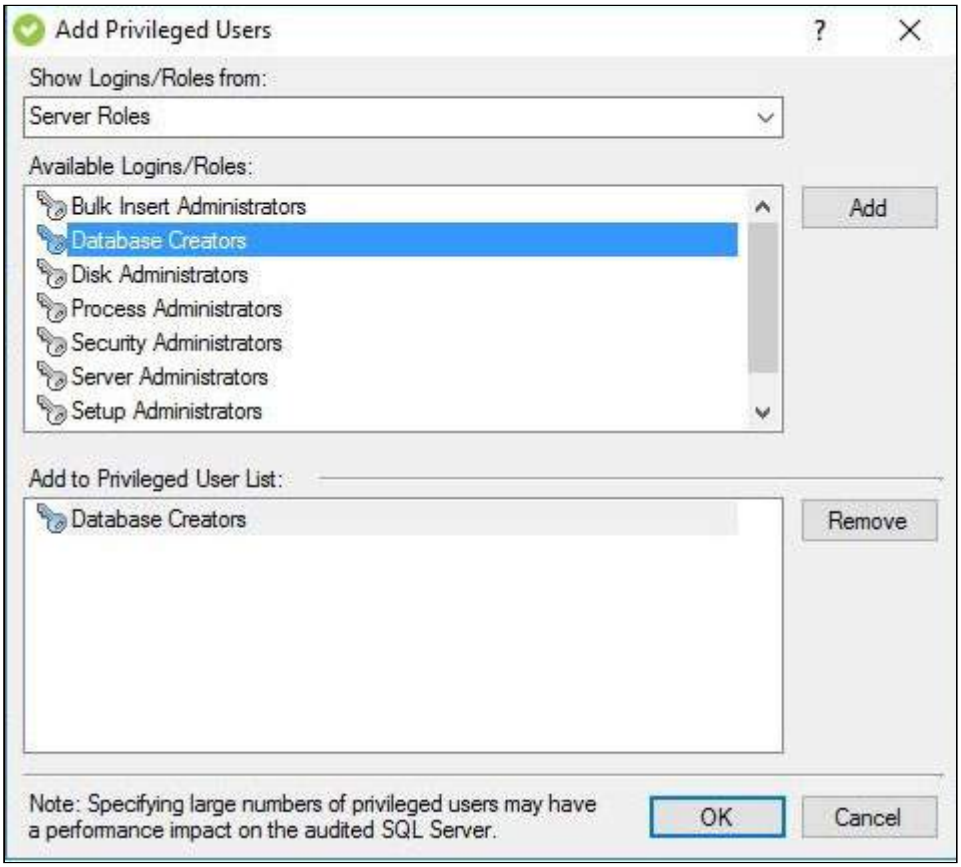
Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

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.

Registered SQL Server Properties - Add Privileged Users window

The Add Privileged Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager Agent collects events generated by any login who is a member of that role.

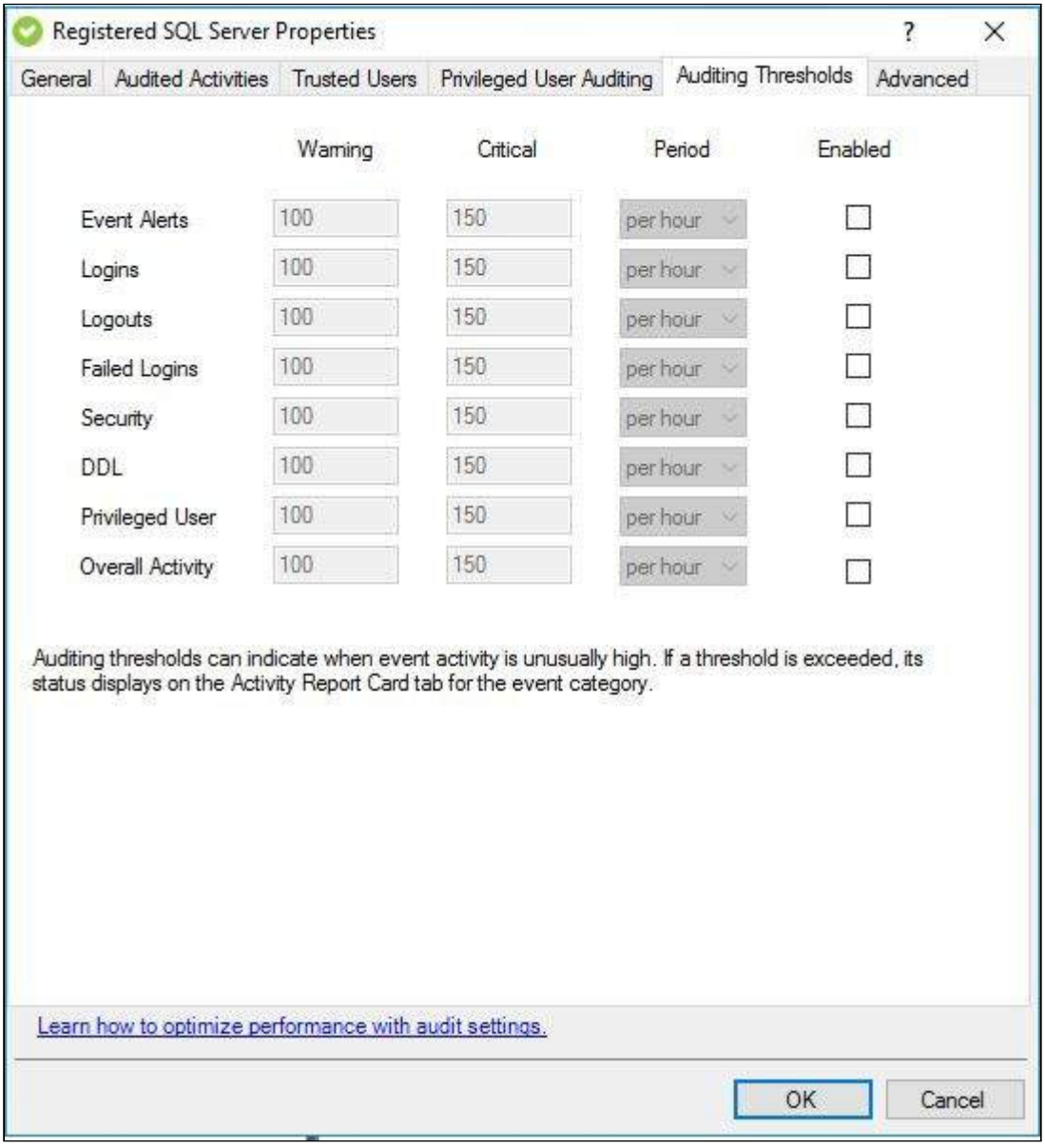
Select the logins or fixed server roles you want to audit, and then click **Add**. You can specify both individual logins and roles.



Registered SQL Server Properties window - Auditing Thresholds tab

The Auditing Thresholds tab of the Registered SQL Server Properties window allows you to set auditing thresholds to identify unusual activity on the selected SQL Server instance. IDERA 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.

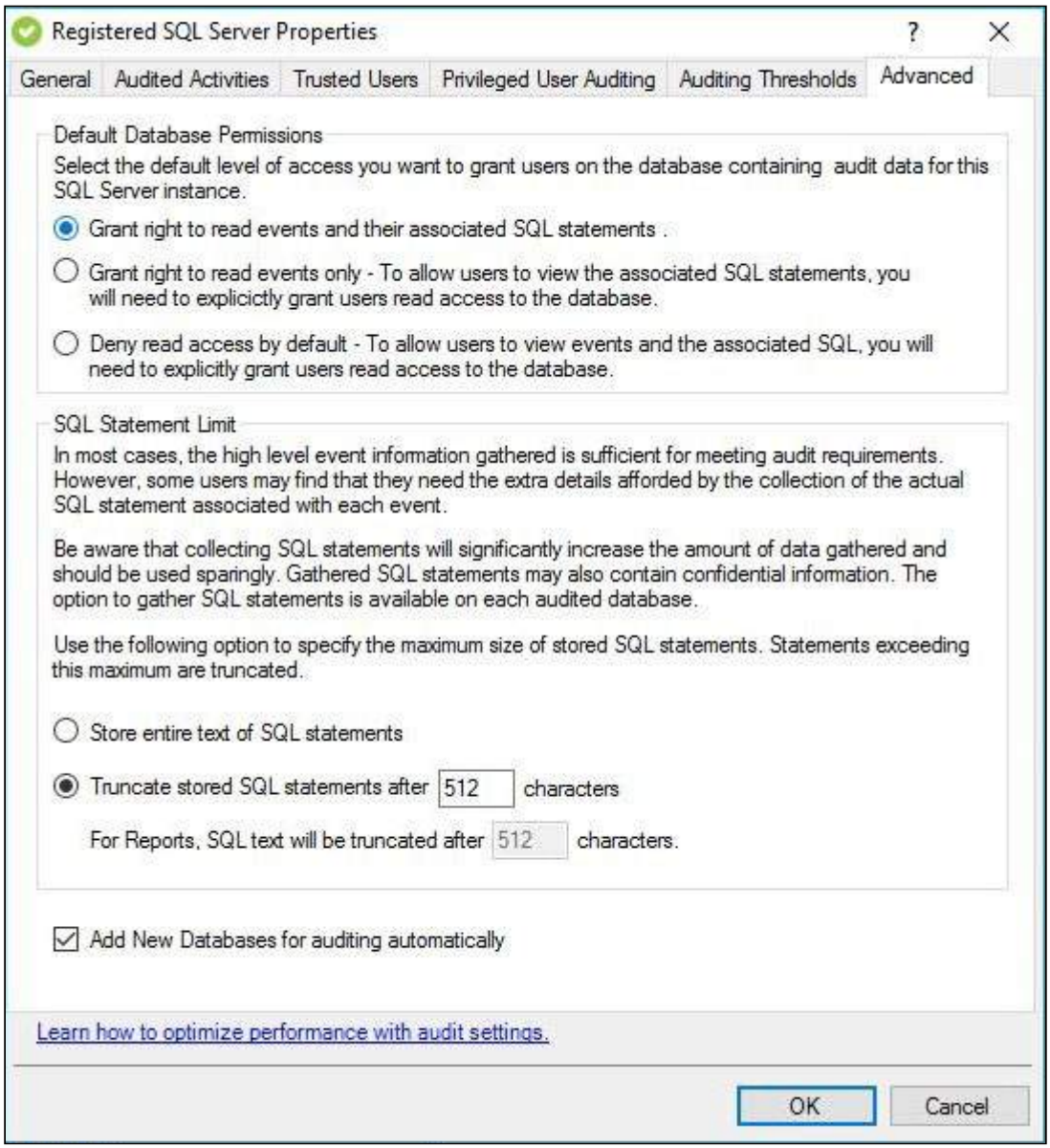
Enabled

Allows you to enable (select) or disable (clear) auditing thresholds for a particular event category.

Registered SQL Server Properties window - Advanced tab

The Advanced tab of the Registered SQL Server Properties window 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 right to read events and their associated SQL statements.
- Grant right to read events only - To allow users to view the associated SQL statements, you will need to explicitly grant users read access to the database.
- Deny read access by default - To allow users to view events and the associated SQL statements, you will need to explicitly grant users read access to the database.

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.

Add New Databases Automatically

Selecting this checkbox will automatically add newly created databases to your list of audited databases for the selected server. Database Default Audit Settings will be apply to the newly created databases, you can update the Database Default Audit Settings at any time.

Apply Regulation Guideline

The Apply Regulation window of the Configuration wizard allows you to apply regulation guidelines to the selected, audited databases. IDERA 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.

Follow apply Regulation Guidelines follow the wizard below:

- Configuration wizard - Enforce Regulation Guidelines window
- Configuration wizard - Apply Regulation window
- Configuration wizard - Server event settings window
- Configuration wizard Apply Regulation - Privileged Users window
- Configuration Wizard - Database event settings window
- Configuration wizard - Privileged Users at Database level window
- Configuration wizard - Database level Privileged Users Audited Activity window
- Configuration wizard - Sensitive Column window
- Configuration wizard - Before-After Data window
- Configuration wizard Apply Regulation - Permissions Check window
- Configuration wizard Apply Regulation - Summary window
- Configuration wizard - Regulation Details window

Configuration wizard - Enforce Regulation Guidelines window

The enforce Regulation Guidelines window of the Configuration wizard displays additional information regarding the regulation guideline selections for the audited databases on your SQL Server instance. IDERA 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

- Before After data change

After reviewing this information, click **Next**.

Configuration wizard - Apply Regulation window

The Apply Regulation window of the Configuration wizard allows you to apply regulation guidelines to the selected, audited databases. IDERA 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.

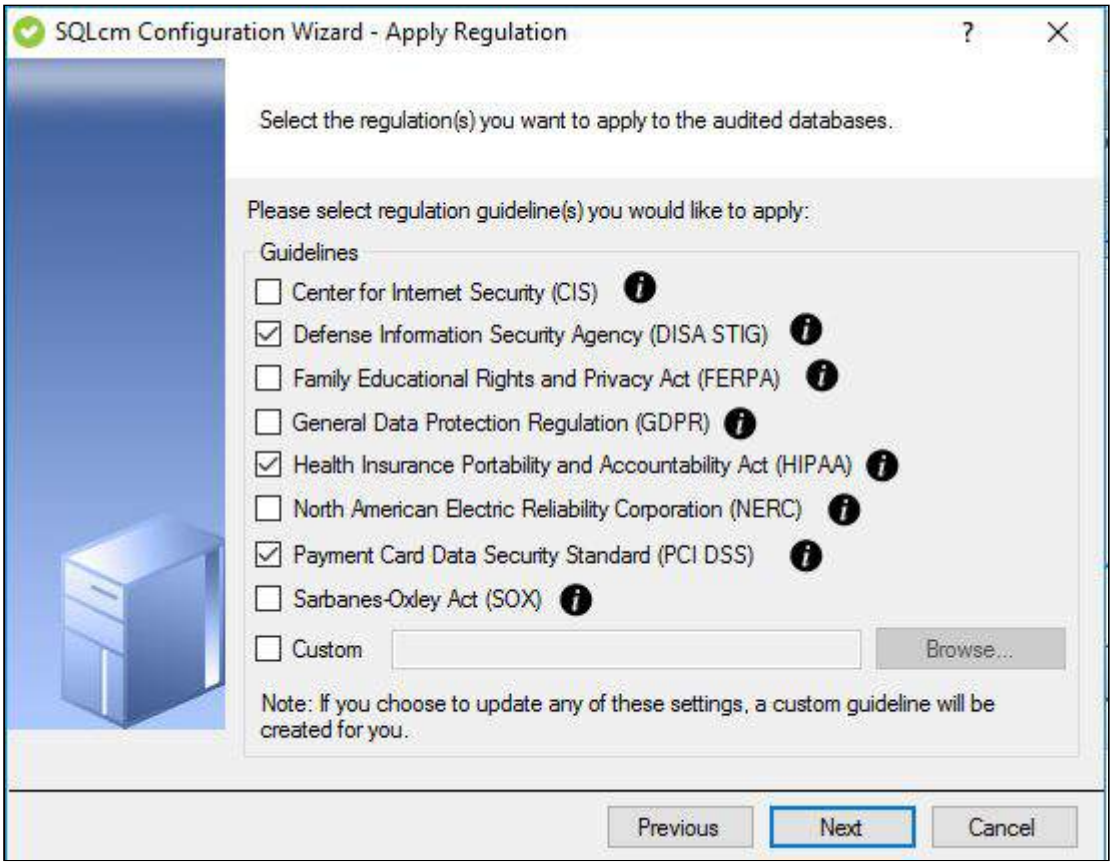
After selecting your regulation guidelines and completing the wizard, you must then configure the following audit settings, if not already set:

- Privileged users
- Privileged user audited activity
- Sensitive columns
- Permissions to list server roles and logins

Check the box for the regulation guidelines you want to enforce, and SQL Compliance Manager displays a description of that guideline and what it can do for your organization.

> If you choose a regulation guideline(s) and update it, you can save the changes as a custom template at the end of the wizard.

Select the regulation guideline(s) you want to apply, and click **Next**.



Available fields

CIS

Allows you to apply regulation guidelines for the Center for Internet Security (CIS).

⚠ The CIS Regulation Guideline is only available at the server level.

DISA STIG

Allows you to apply regulation guidelines for the Defense Information Security Agency (DISA STIG).

FERPA

Allows you to apply regulation guidelines for the Family Educational Rights and Privacy Act (FERPA).

GDPR

Allows you to apply regulation guidelines for the General Data Protection Regulation (GDPR).

HIPAA

Allows you to apply regulation guidelines for the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

NERC

Allows you to apply regulation guidelines for the North American Electric Reliability Corporation (NERC).

PCI DSS

Allows you to apply regulation guidelines for the Payment Card Industry Data Security Standard (PCI DSS).

SOX

Allows you to apply regulation guidelines for the Sarbanes-Oxley Act (SOX).

Custom

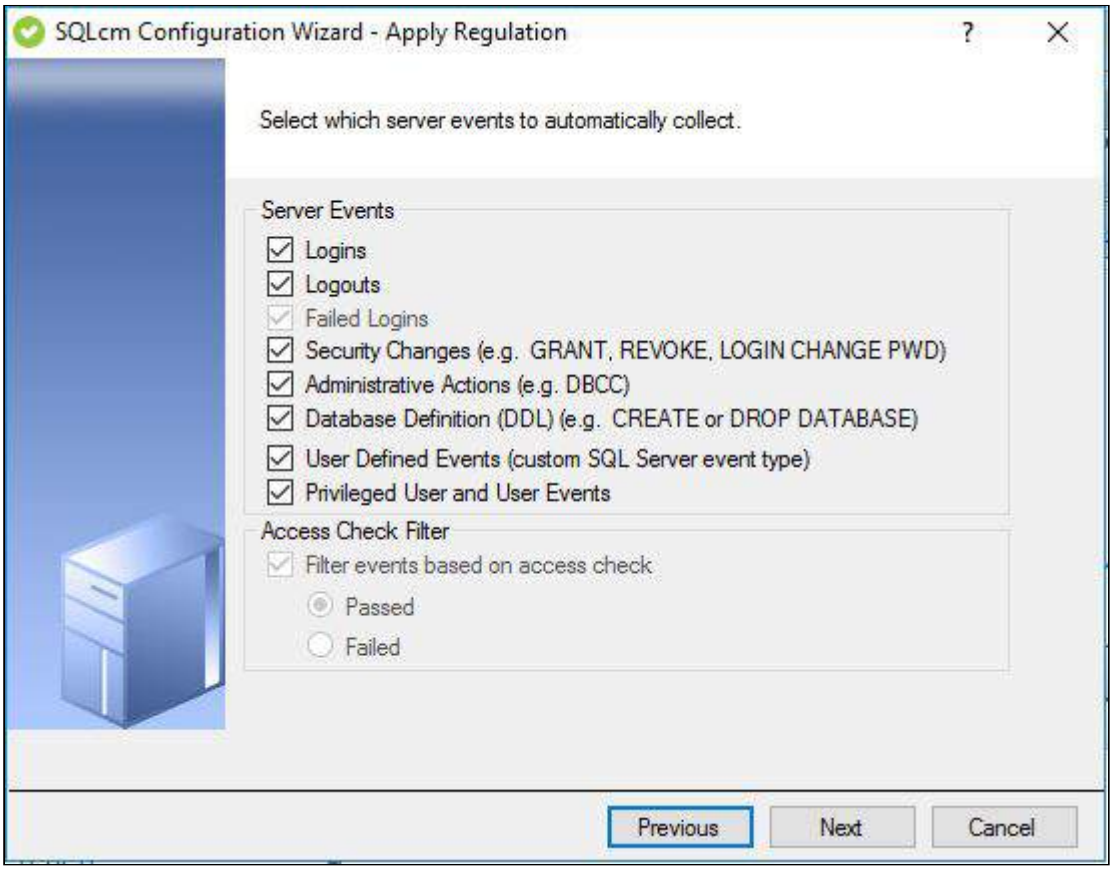
Allows you to upload and apply a custom audit settings regulation.

⚠ When uploading a custom regulation, the file needs to be in XML format to proceed successfully with the wizard.

ⓘ Sensitive columns and Before-After data settings are not included when uploading a custom regulation. Before-After and sensitive columns need to be configured with each server/database.

Configuration wizard - Server event settings window

The Server Audit Settings window of the Configuration wizard allows you to specify which types of SQL Server events you want to automatically collect for the selected instance.



> This step of the configuration wizard is only necessary when Applying Regulation Guidelines at the database level.

Available fields

Audited Activity

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. 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 Compliance Manager 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

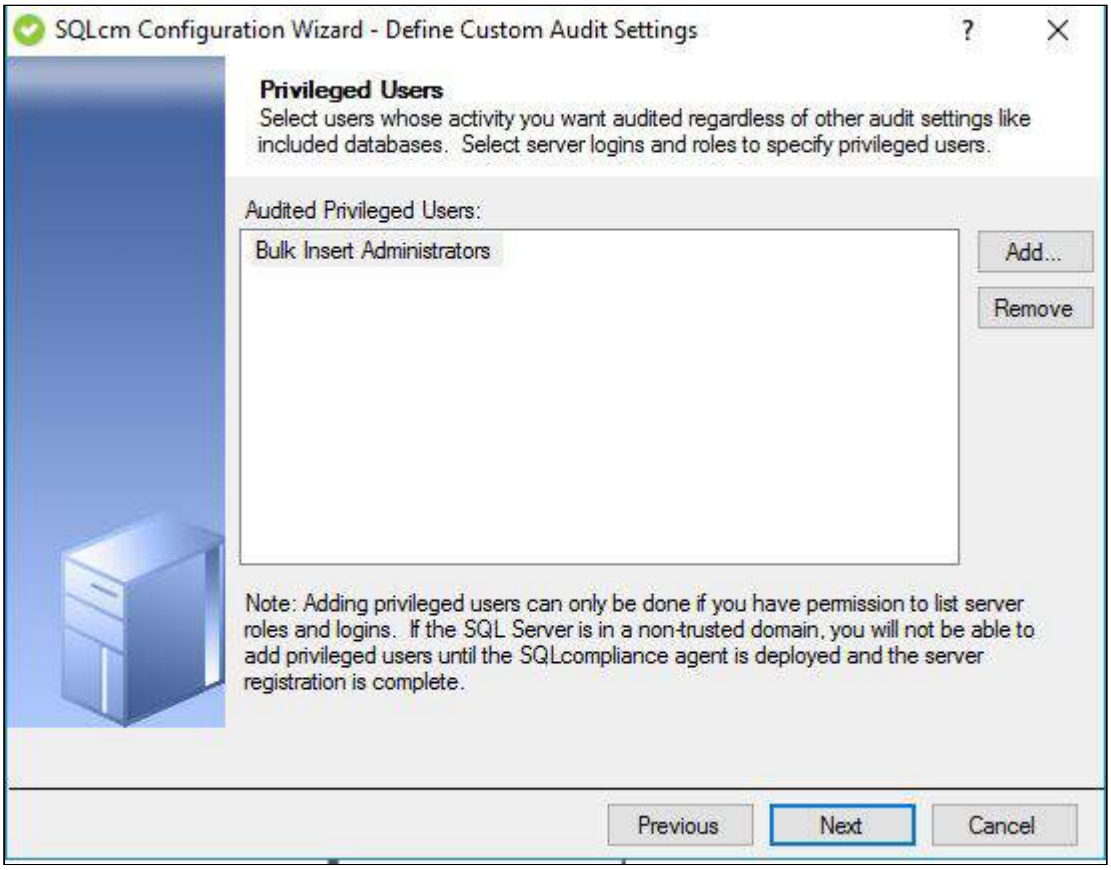
Configuration wizard Apply Regulation - Privileged Users window

The Privileged Users window of the Configuration wizard allows you to select which privileged users you want to audit using IDERA 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 SQL Compliance Manager Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent. For more information about installing and configuring the SQL Compliance Manager 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 SQL Compliance Manager 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.

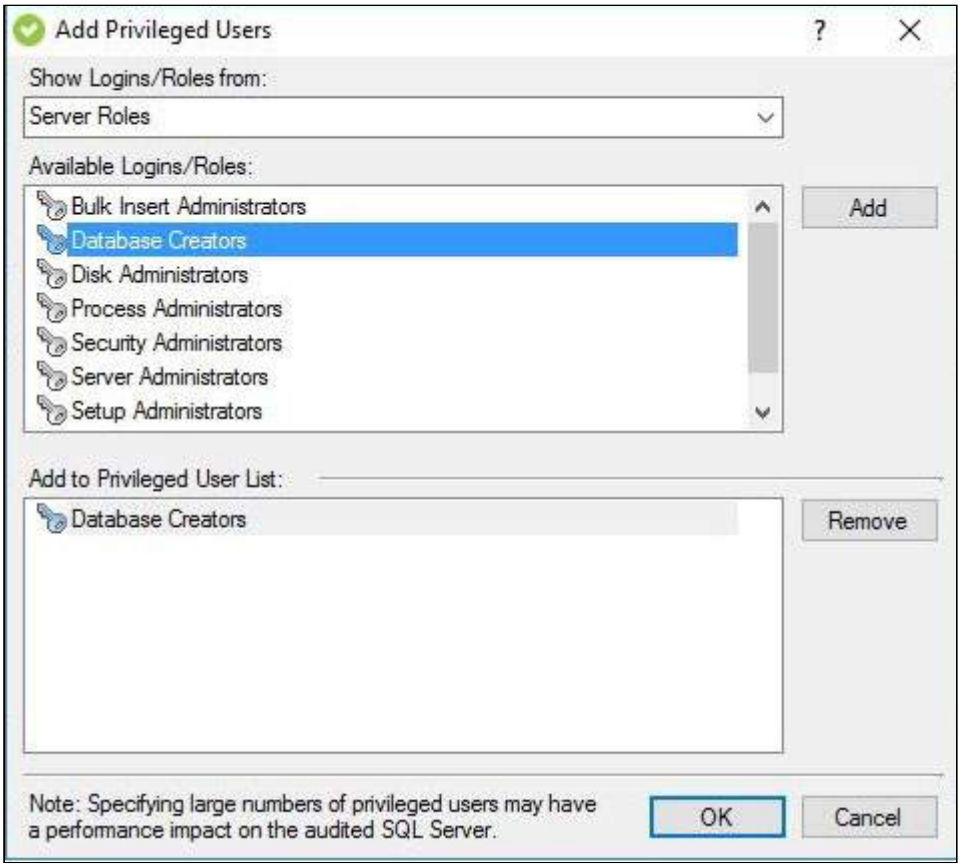
Remove

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 SQL Compliance Manager 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 Apply Regulation - Add Privileged Users window

The Add Privileged Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager 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.



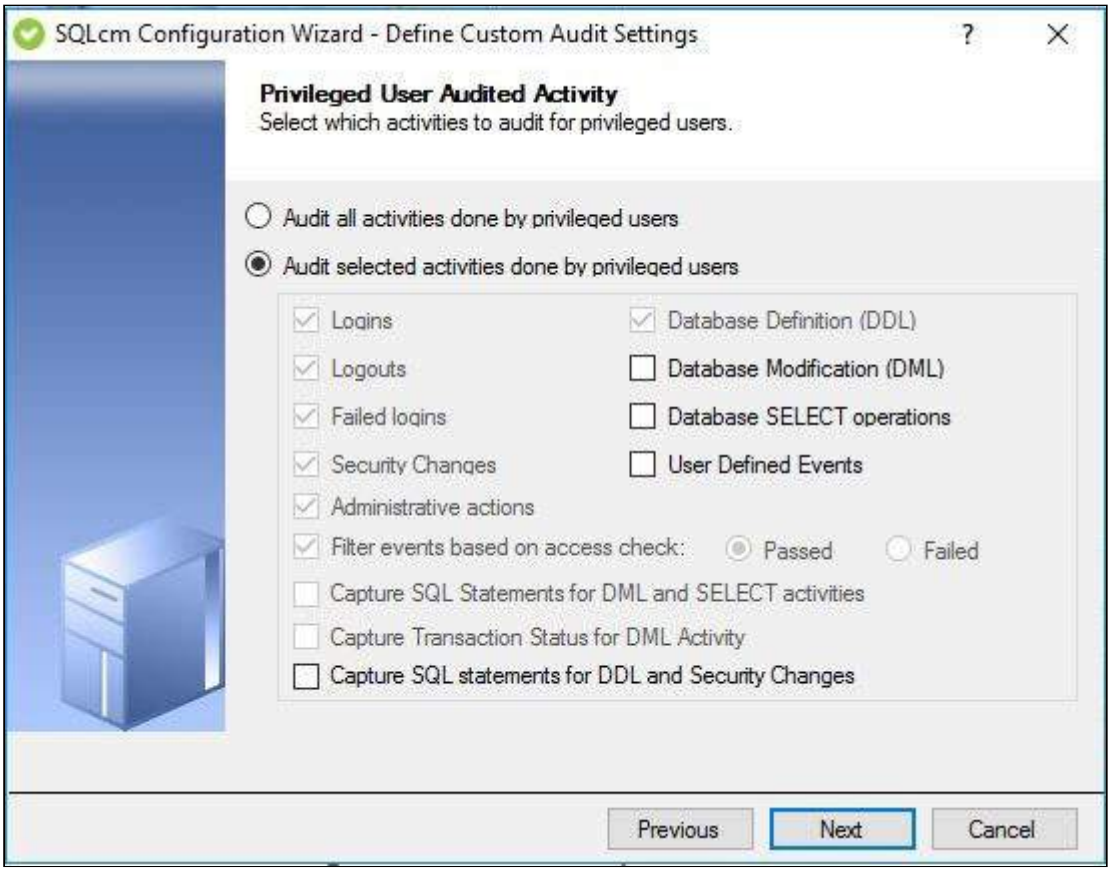
Configuration wizard Apply Regulation - Privileged Users Audited Activity window

The Privileged Users Audited Activity window of the Configuration wizard 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 IDERA 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. Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User defined events
- Filter events based on access check.

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.

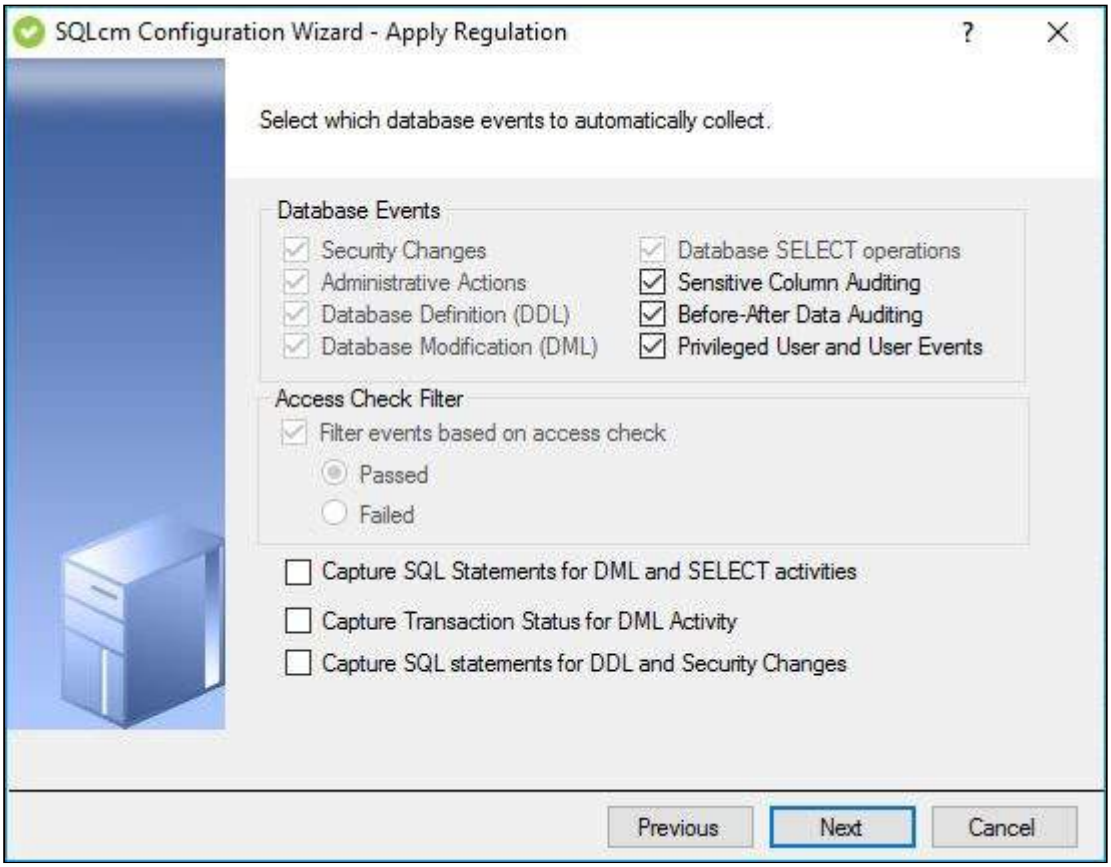
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

Configuration Wizard - Database event settings window

The Database event settings window of the Configuration wizard allows you to specify which types database events you want to audit on the selected databases in IDERA SQL Compliance Manager.



Available fields

Database Events

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 Compliance Manager 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

Type of Event Filter	Description
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.

Capture SQL statements for DDL and Security Changes

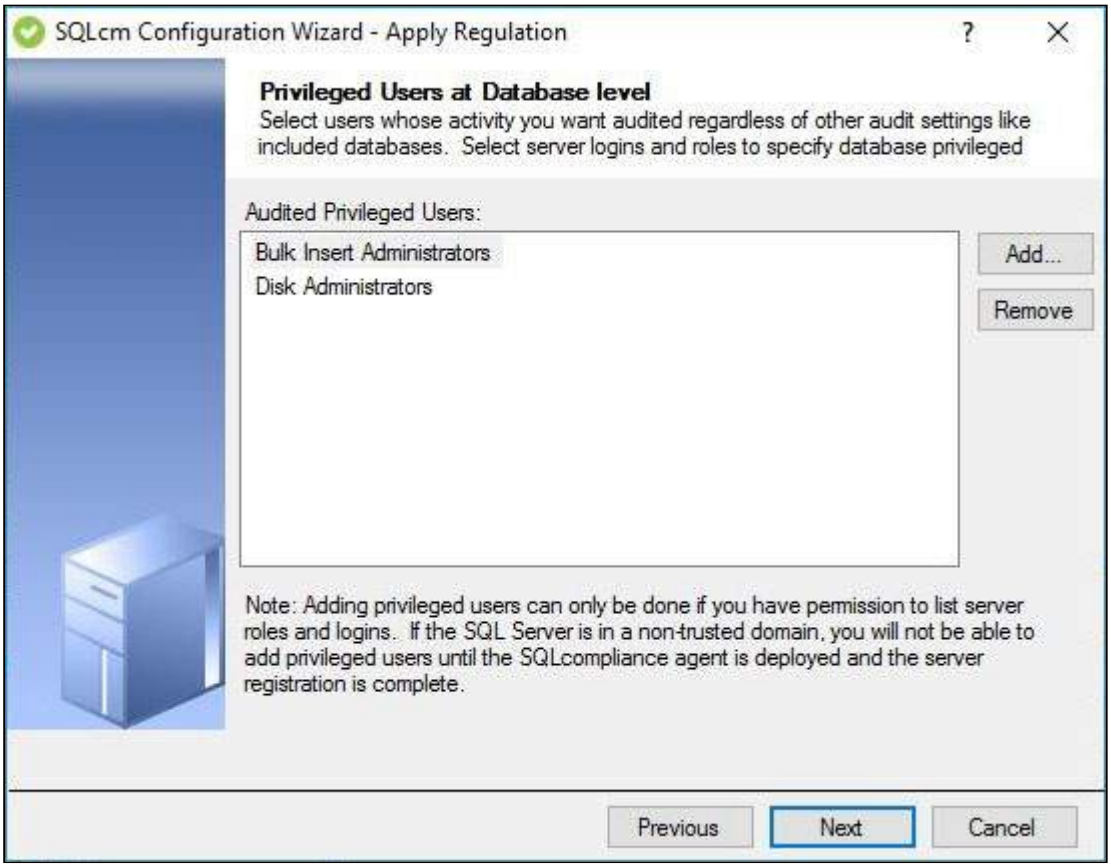
Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

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.

Configuration wizard - Privileged Users at Database level window

The Privileged Users at Database window of the Configuration wizard allows you to select which privileged users you want to audit using IDERA SQL Compliance Manager at the Database level. 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.



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.

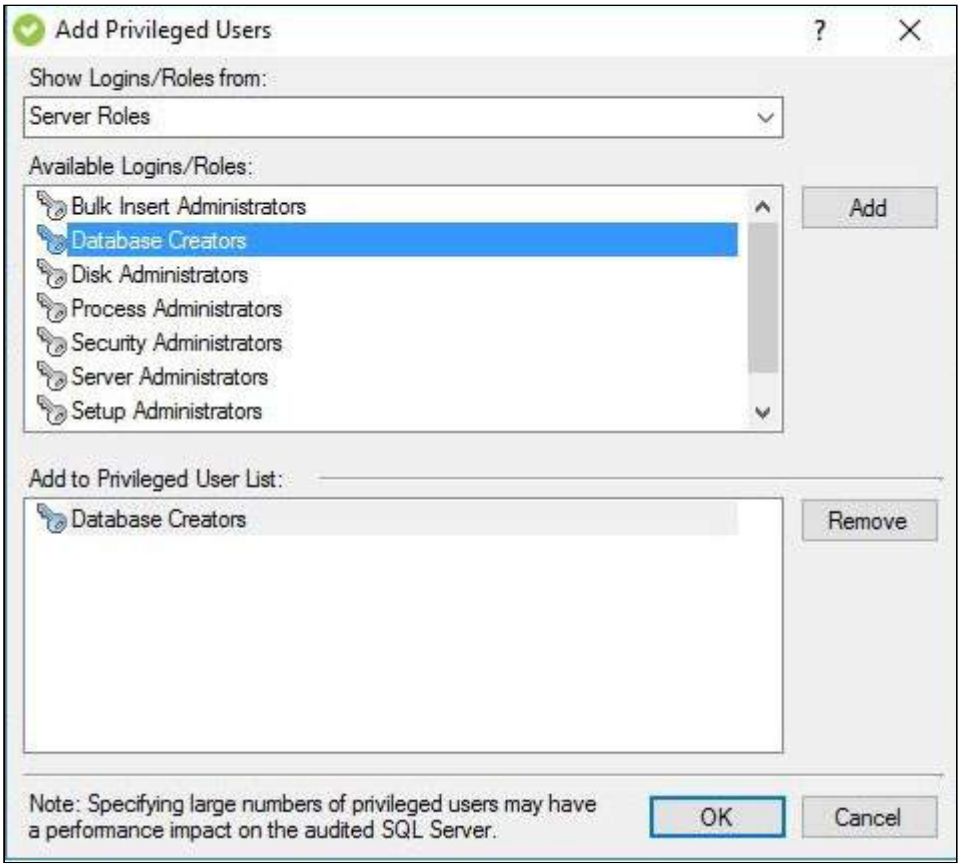
Remove

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 SQL Compliance Manager 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 Apply Regulation - Add Privileged Users at Database level window

The Add Privileged Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager 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.



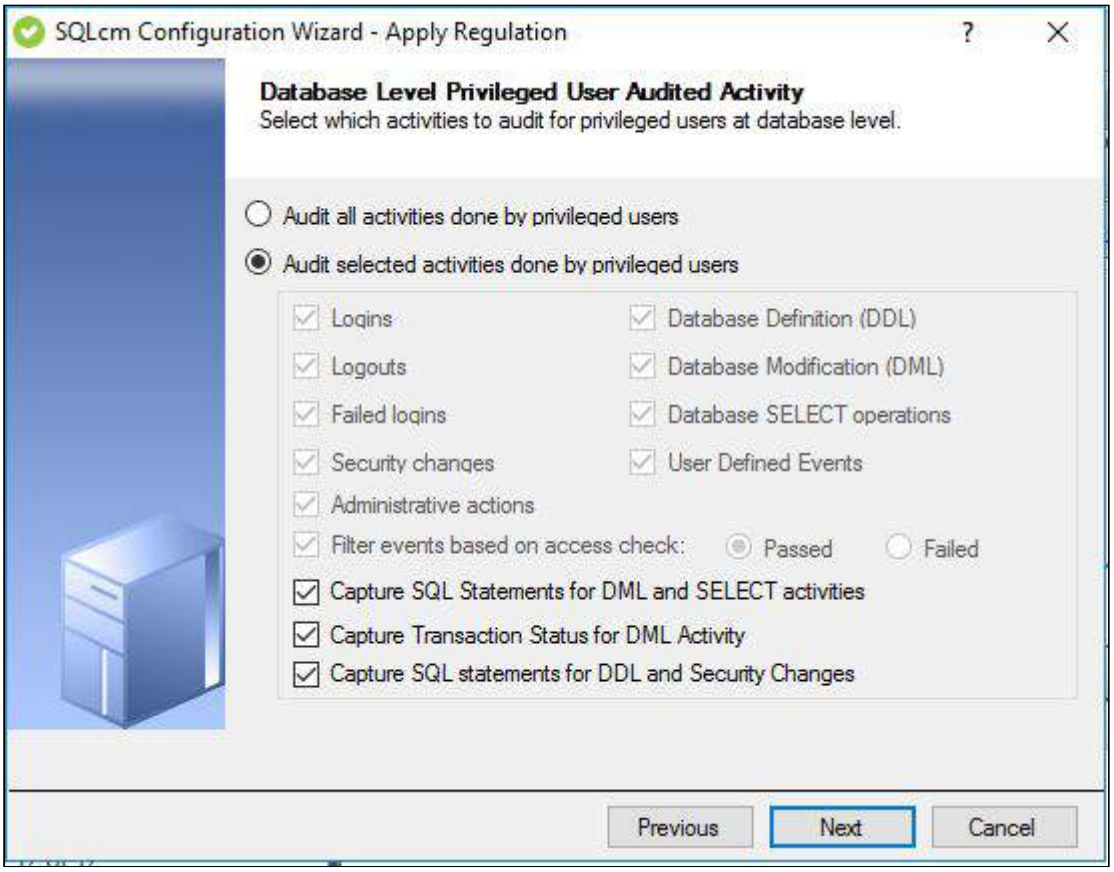
Configuration wizard - Database level Privileged Users Audited Activity window

The Database Level Privileged Users Audited Activity window of the Configuration wizard allows you to specify which activities (events) you want to audit when the selected privileged users perform certain actions. You can choose to audit user defined events using IDERA SQL Compliance Manager. 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.

Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

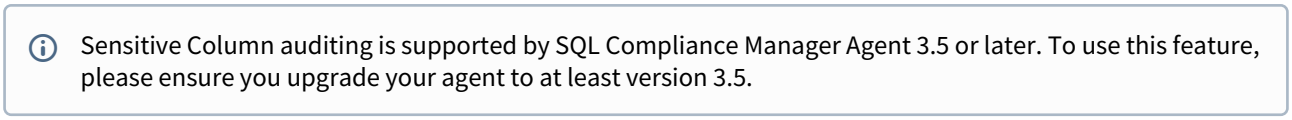
Configuration wizard - Sensitive Column window

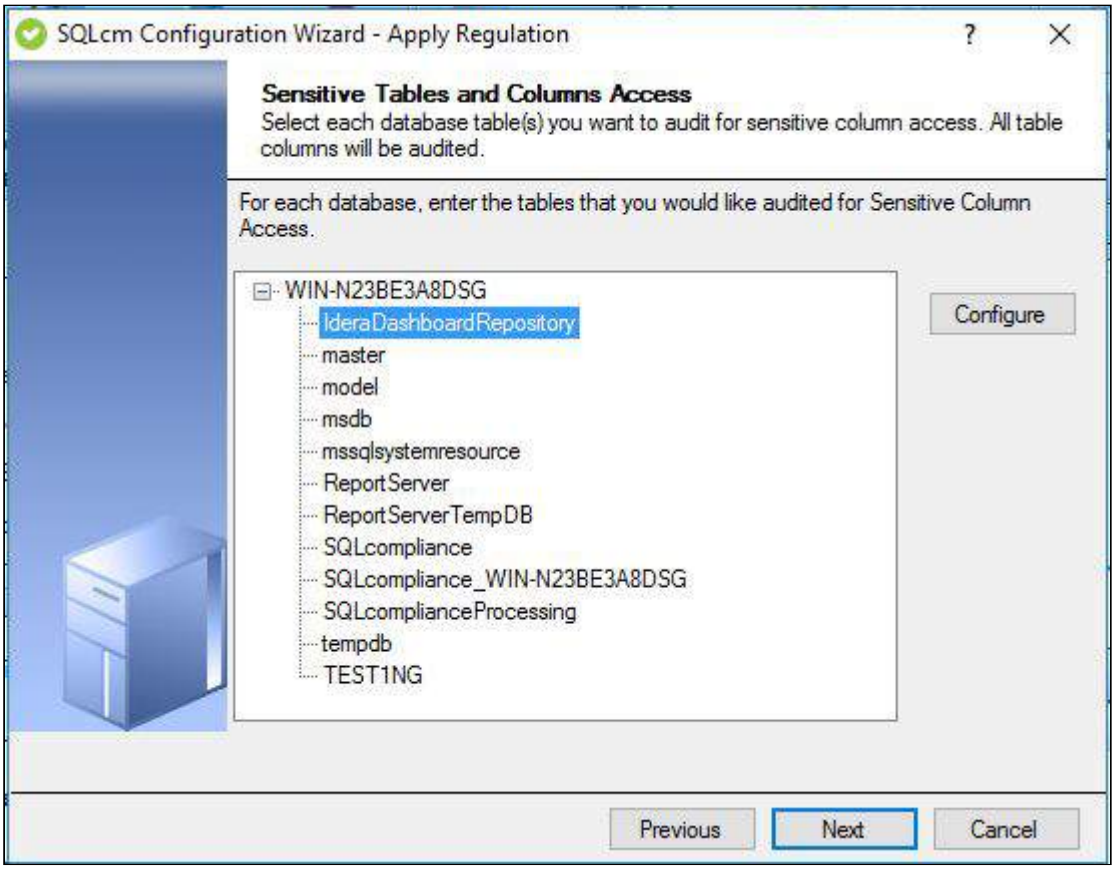
The Sensitive Column window of the Configuration wizard allows you to select the individual table columns or datasets you want IDERA SQL Compliance Manager to audit for sensitive column access. Configure the type of activity you want to collect data for, choose between Selects, Selects and DML or All Activity. This information is important to track whether a third-party application or database user read data in a specific table column.

This feature can affect the performance of your Collection Server and Management Console. Auditing sensitive columns can result in a significant amount of data being collected, consider auditing SELECT commands at the column level only when those columns contain highly sensitive data that should not be widely accessed or read.

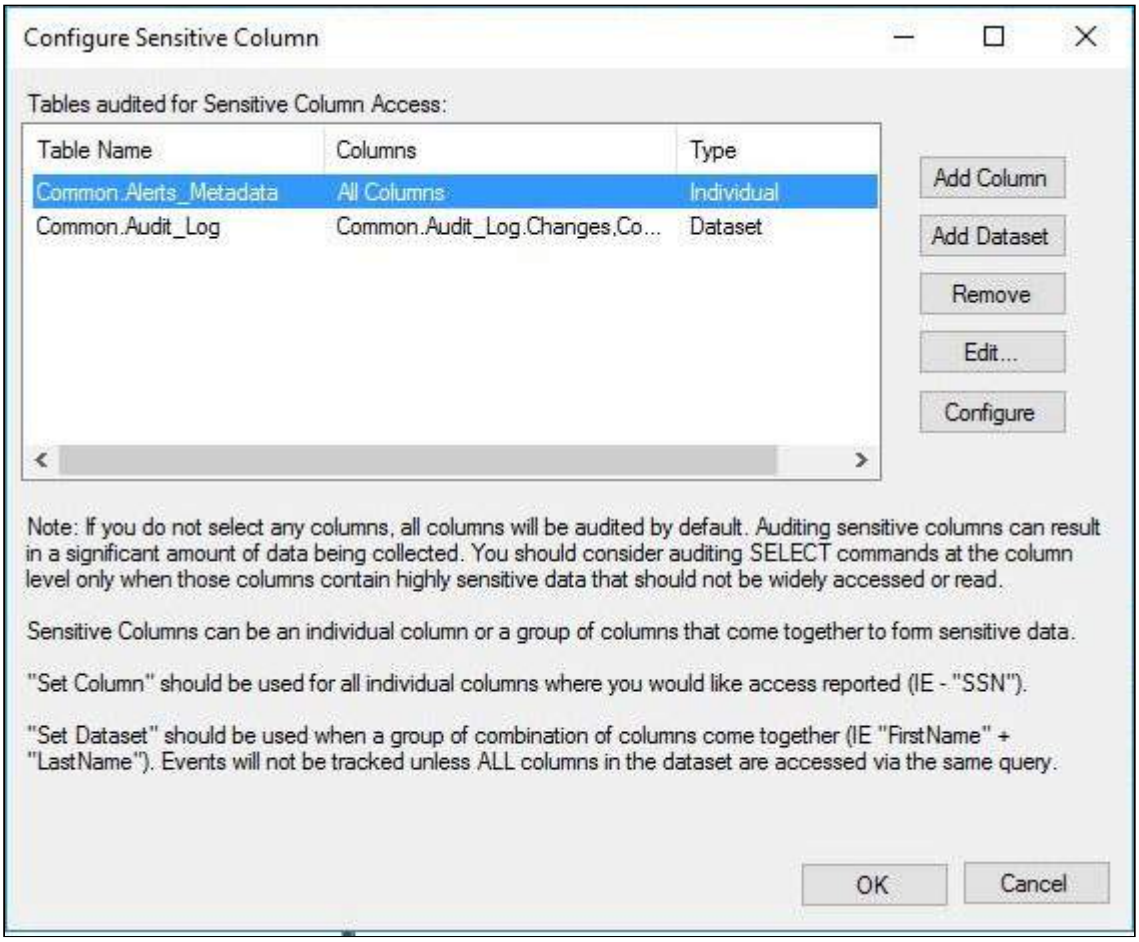
Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data. If no individual columns are selected, by default all columns from the selected table will be audited.

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 SQL Compliance Manager Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.



Select a Database from the list and click **Configure**.



Available actions

Add Column

Allows you to select one or more database tables to audit for sensitive columns.

Add Dataset

Allows you to specify a group of columns to audit as a set of sensitive information.

Remove

Allows you to remove the selected database table from the list of audited tables.

Edit

Allows you to select individual columns to be audited within the selected table.

Configure

Allows you to choose which type of activity you want Sensitive Columns to collect data for. You can choose one of the following types of activity to collect data for your Sensitive Columns:

- Select Only - captures all Select queries only.
- All Activity - captures all Select, DDL and DML activities on tables configured for Sensitive Column.
  - Captures Select, Insert, Update and Delete on the Sensitive Columns.
  - Captures Alter and Drop queries on tables where Sensitive Columns are present.

    - Captures Select, Insert, Update and Delete on the Sensitive Columns if the sensitive columns are accessed through views or Stored Procedures.
- SELECT and DML - captures Select queries and DML activity such as; Select, Insert, Update and Delete.

Configuration wizard - Before-After Data window

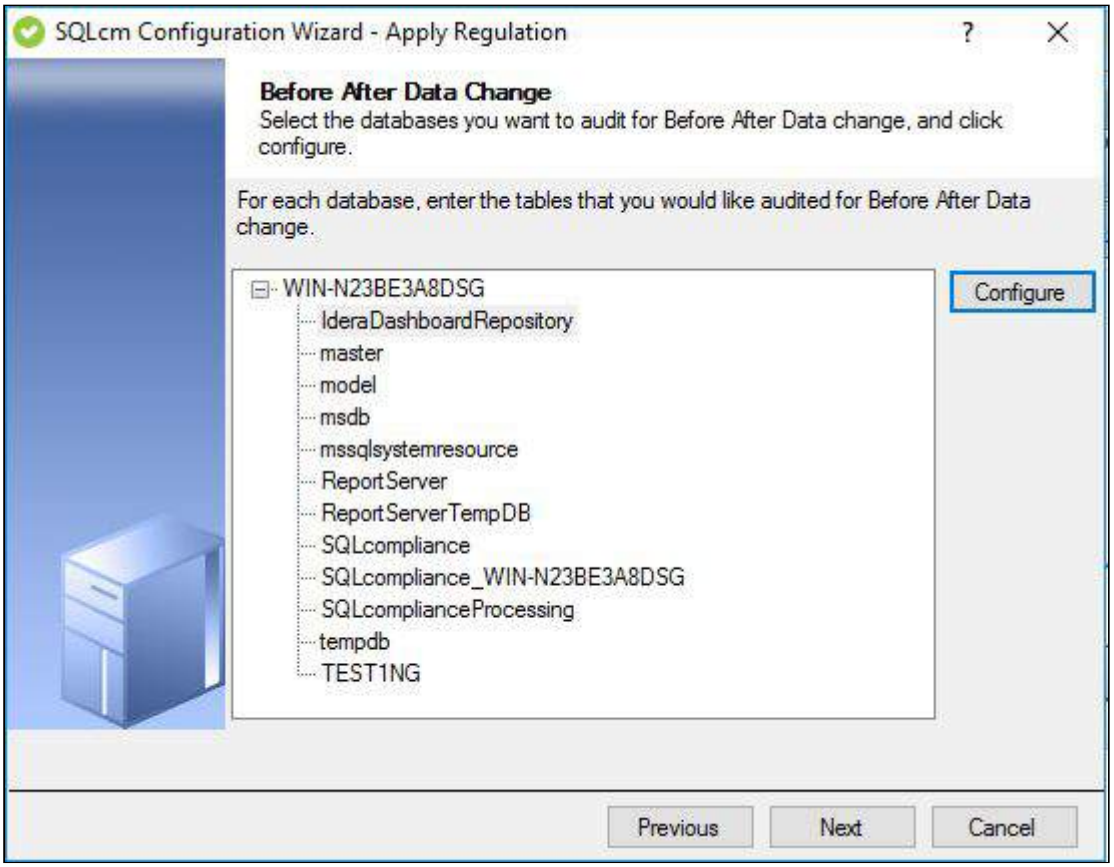
The Before-After Data window of the Apply Regulation Guidelines configuration wizard allows you to select the tables for which you want to collect before and after data. You can collect before and after data for DML events generated by DELETE, INSERT, and UPDATE commands.

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.

IDERA provides limited support for before-after data auditing of the publisher database in SQL Servers with replication. However, this scenario is supported only when the publisher database with transaction replication is set to replicate data ONLY. ***If the target database uses SQL Server replication set to replicate more than data***, do not enable before-after auditing. Before and after data collection does not support SQL Server replication in that situation. For more information, see Microsoft Books Online for the version of SQL Server you are using.

To successfully audit specific columns on a table, ensure the table name does not contain the following special characters: \ / : * ? "



Available actions

Configure

Select a database from the list and click **Configure** to open the Configure Before After Data Change window where you can add, edit or remove your specific user tables for Before-After Data auditing.

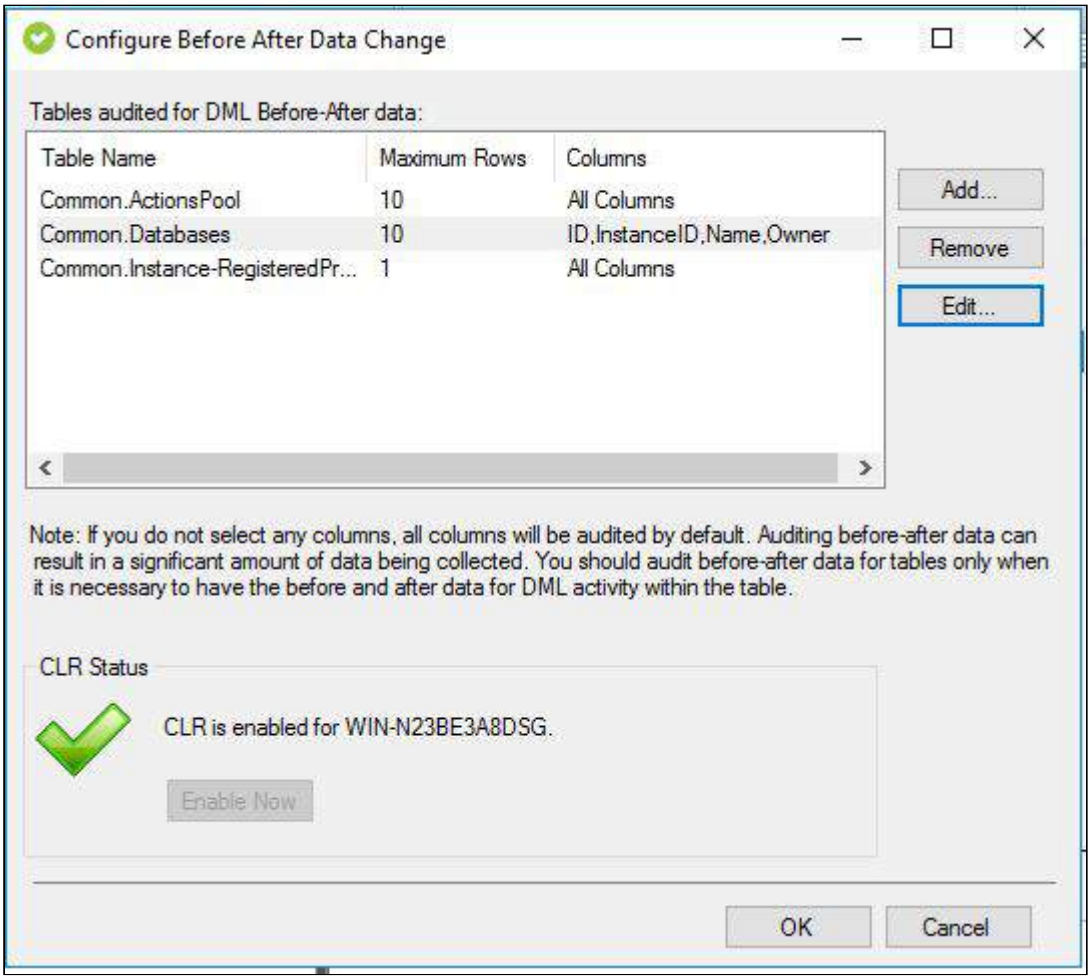
Configure Before-After Data Change window

The Configure Before-After Data Change window allows you to add, edit or remove 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.

ⓘ 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 SQL Compliance Manager 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 SQL Compliance Manager Agent will capture of each DML transaction.

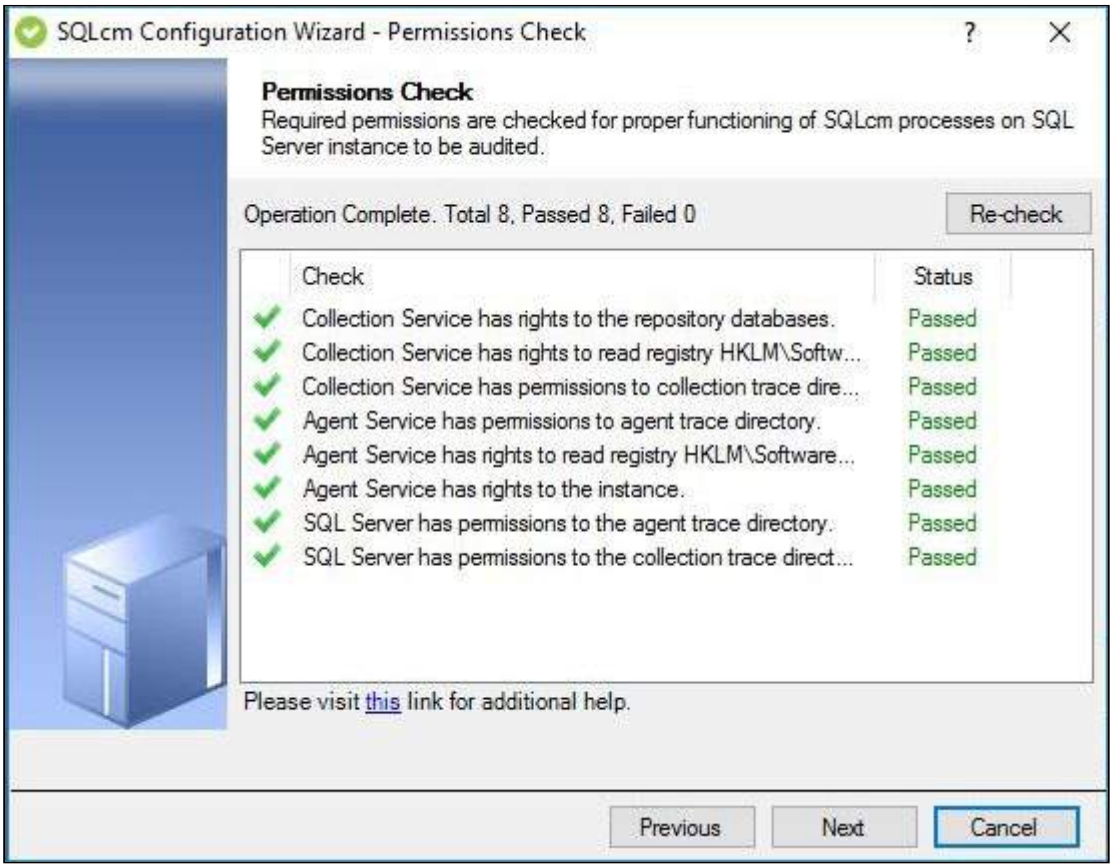
Columns

Indicates the status of the columns associated with the audited tables. Typically, this field displays **All Columns** or lists the individual columns that are audited for before-and-after data.

If the audited table contains BLOB data and individual columns that are not 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.

Configuration wizard Apply Regulation - Permissions Check window

The Permissions Check window of the Configuration wizard displays the results of a check of the permissions required by IDERA 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 is 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.

To successfully run and pass the Permissions Check, make sure you are logged in as one of the following users while registering an instance:

- SQL Compliance Agent Service User
- SQL Server Service User
- Current Logged-in User

For more information, see SQL Compliance Manager Permissions Requirements.

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

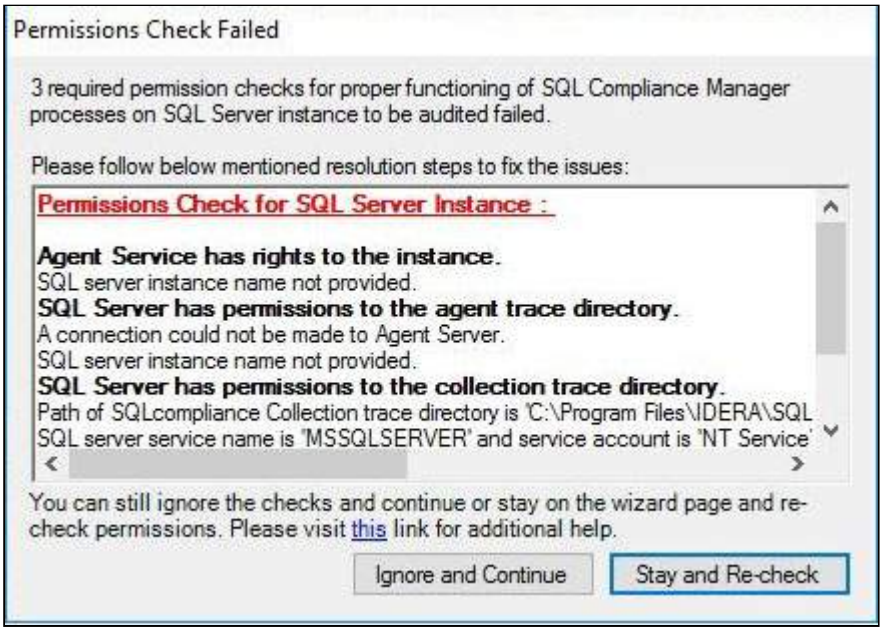
Displays the current status of the associated check. All checks display **Waiting** until run.

Configuration wizard Apply Regulation - Permissions Check Failed window

The Permissions Check Failed window of the Configuration wizard 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. SQL Compliance Manager 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 SQL Compliance Manager 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 Apply Regulation - Summary window

Use the Summary window of the IDERA SQL Compliance Manager Configuration wizard to review the provided summary, and then click **Finish**. When you complete 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.

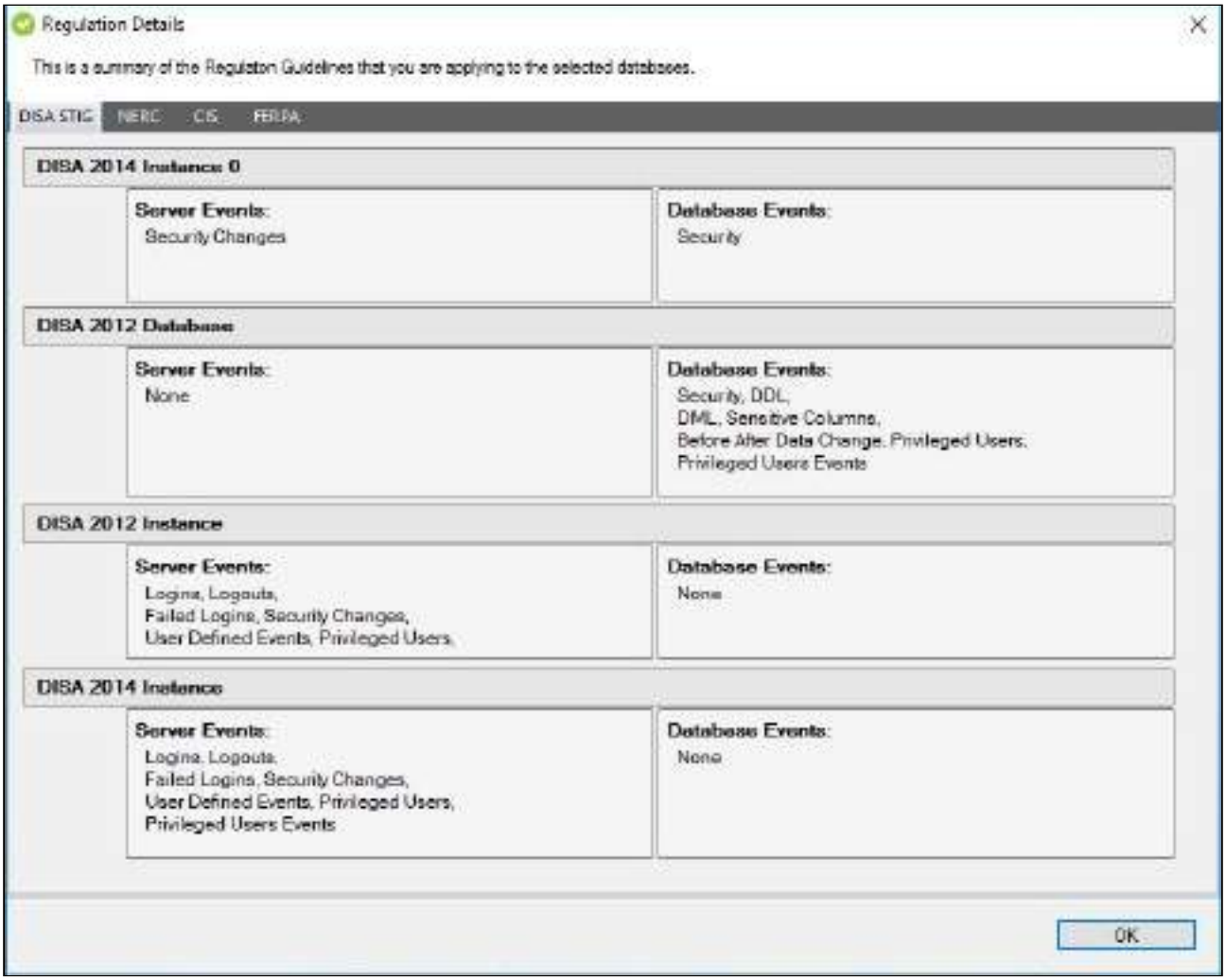
If you want to change a setting now, click **Previous** to return to the appropriate window. You can also change audit settings later using the Audited Database Properties window.

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 - Regulation Details window

The Regulation Details window of the Configuration wizard 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, IDERA 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 Compliance Manager Configuration wizard Summary window.



Import your audit settings wizard

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 consistently audited 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.

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.

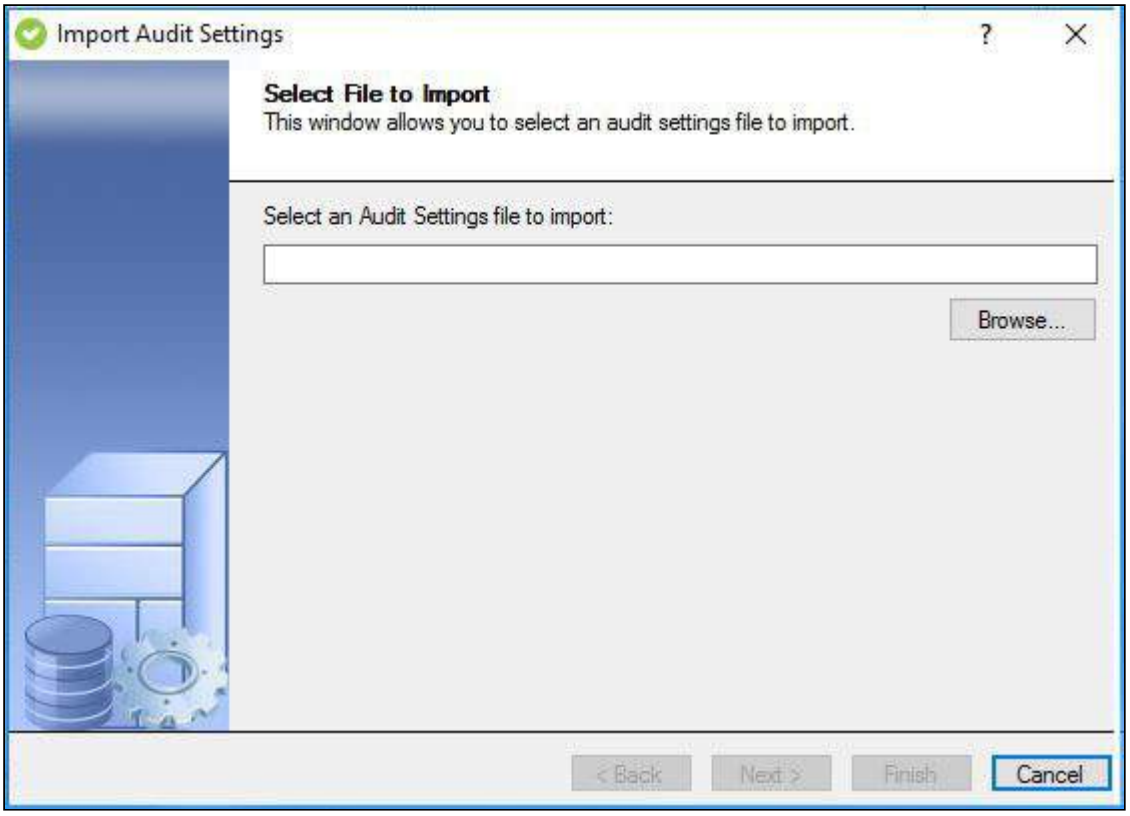
To audit the same events across multiple instances or databases follow the wizard steps below:

- Import Audit Settings wizard - Select File to Import window
- Import Audit Settings wizard - Import Audit Settings window
- Import Audit Settings wizard - Target Servers window
- Import Audit Settings wizard - Target Databases window
- Import Audit Settings wizard - Summary window

Import Audit Settings wizard - Select File to Import window

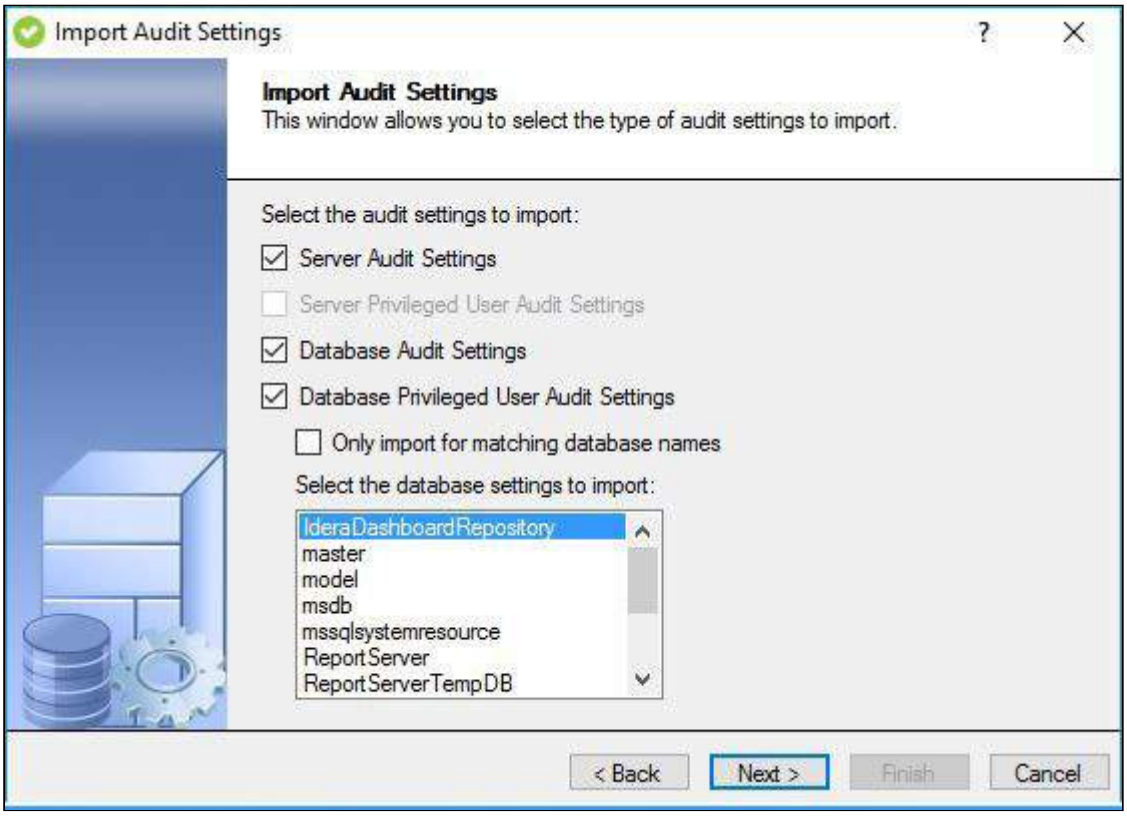
The Select File to Import window of the Import Audit Settings wizard allows you to specify which audit settings you would like import by selecting the corresponding XML file.

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 - Import Audit Settings window

The Import Audit Settings window of the Import Audit Settings wizard 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

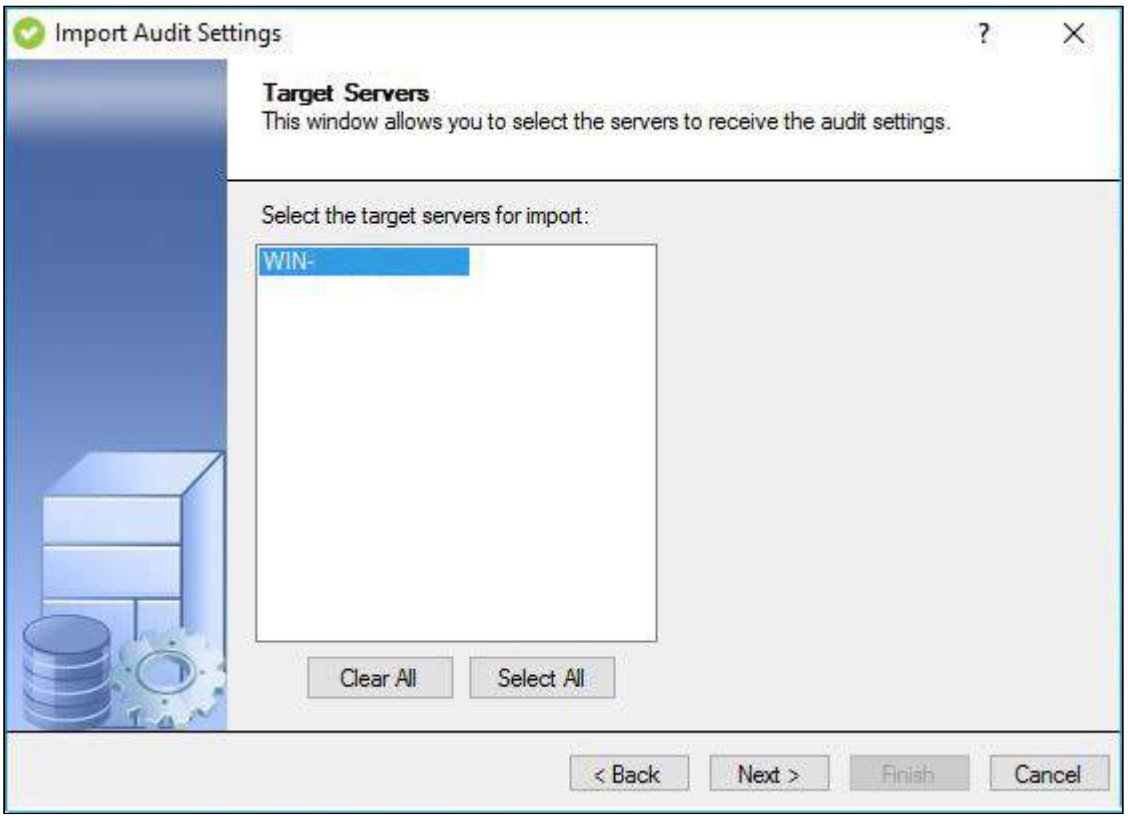
Allows you to import database-level audit settings previously configured for a specific database, using the selected database as a baseline or template. You can import these settings to multiple databases or limit your import to target databases whose names match the baseline database.

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 - Target Servers window

The Target Servers window of the Import Audit Settings wizard 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

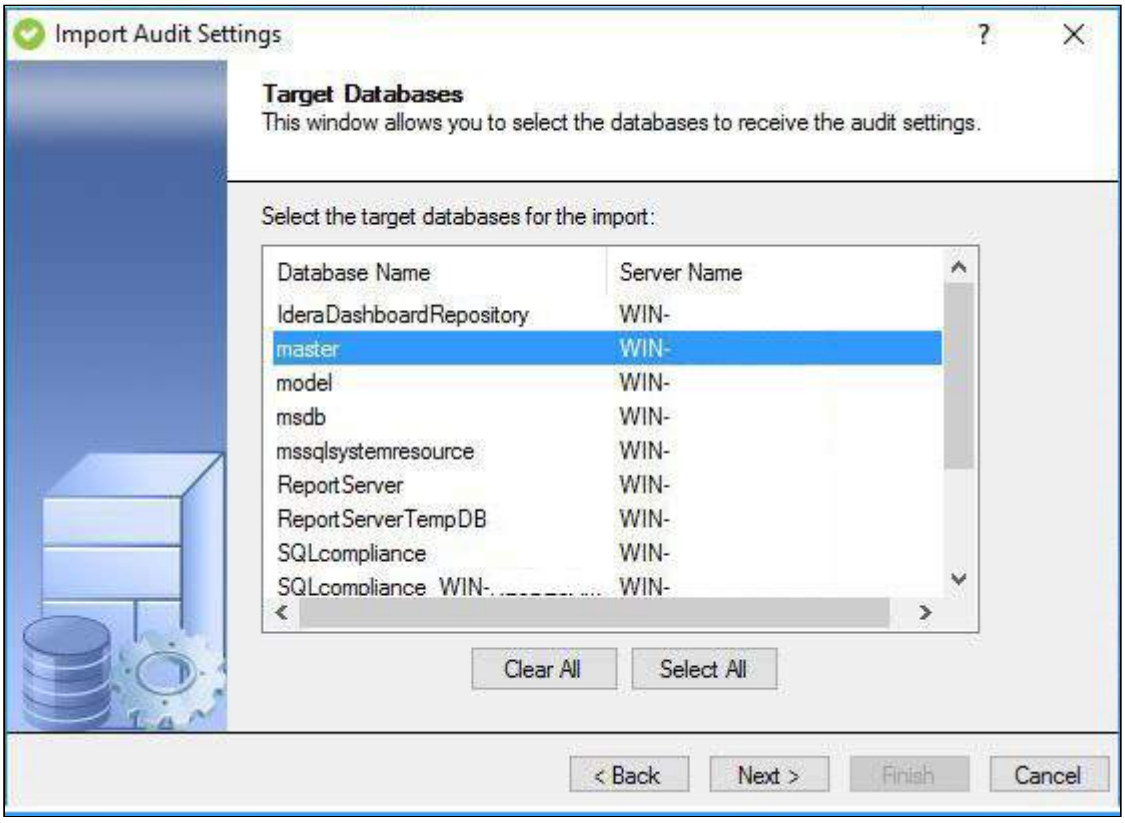
Selects all registered SQL Server instances.

Import Audit Settings wizard - Target Databases window

The Target Databases window of the Import Audit Settings wizard 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.

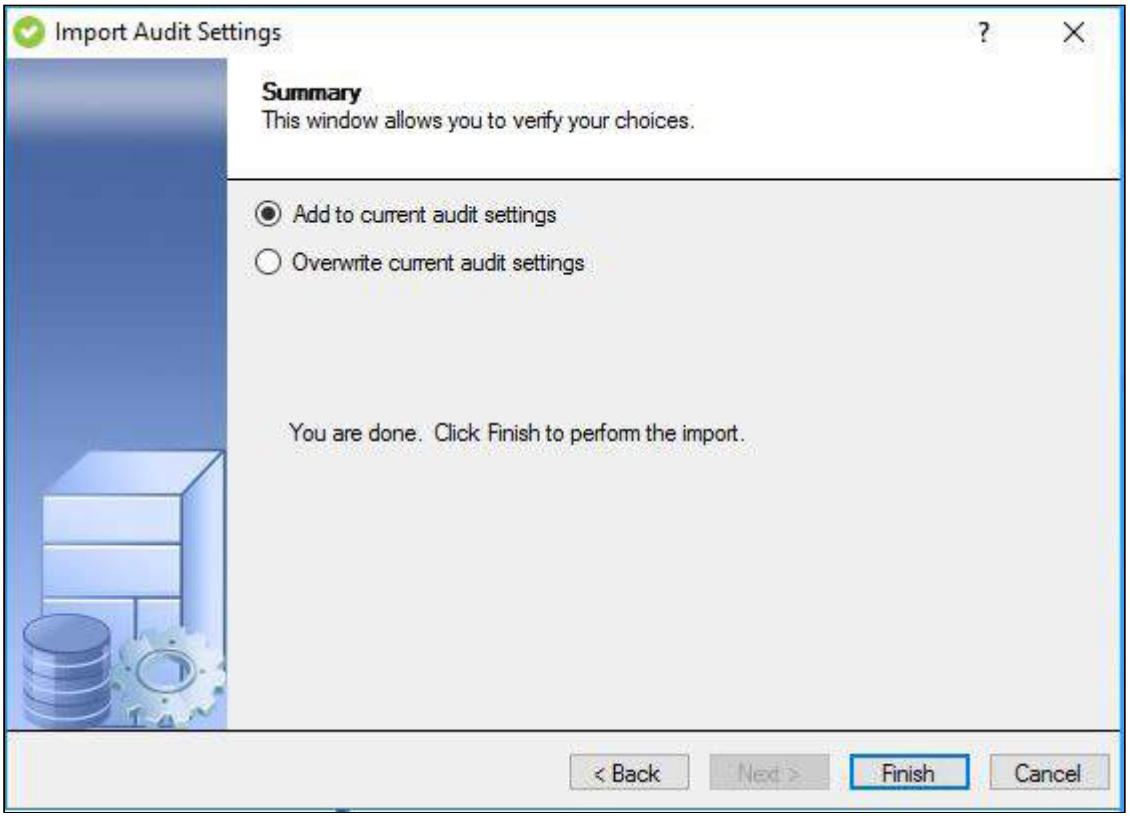
Select All

Selects all audited databases.

Import Audit Settings wizard - Summary window

The Summary window of the Import Audit Settings wizard 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 SQL Compliance Manager Agent at the next heartbeat.



Available actions

Add to current audit settings

Appends the existing audit settings the SQL Compliance Manager Agent is using to audit the target SQL Server instance or database with the settings you have chosen to import. The SQL Compliance Manager 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 SQL Compliance Manager Agent is using to audit the target SQL Server instance or database with the settings you have chosen to import. The SQL Compliance Manager Agent will use only the imported settings to collect events from this instance or database.

SQL Compliance Manager Agent Properties

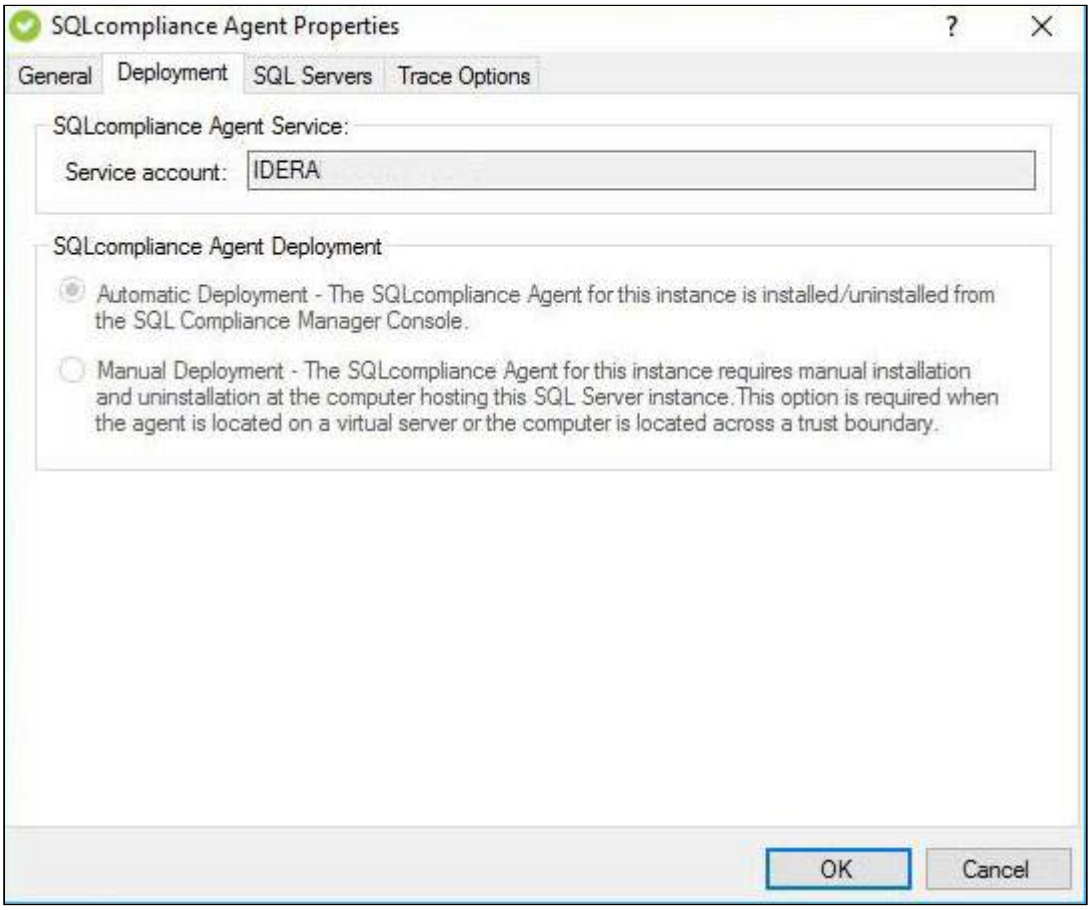
The SQL Compliance Manager Agent gathers SQL Server events written to the SQL trace, caching these audited events in trace files. By default, the SQLcompliance Agent calls the Collection Server every five minutes (heartbeat) to receive audit setting updates, and sends trace files for processing every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

Use the links below to set your desired SQL Compliance Manager Agent Properties:

- SQL Compliance Manager Agent Properties window - Deployment tab
- SQL Compliance Manager Agent Properties window - General tab
- SQL Compliance Manager Agent Properties window - SQL Servers tab
- SQL Compliance Manager Agent Properties window - Trace Options tab

SQL Compliance Manager Agent Properties window - Deployment tab

The Deployment tab of the SQL Compliance Manager Agent Properties window allows you to verify how the SQL Compliance Manager Agent was deployed on the selected SQL Server instance. You can view the account used by the SQL Compliance Manager Agent Service as well as the deployment method used.



Available fields

SQL Compliance Manager Agent Service

Provides the name of the user account under which the SQL Compliance Manager Agent is running on this SQL Server instance. The displayed account name uses the format *DomainName\LogonName*.

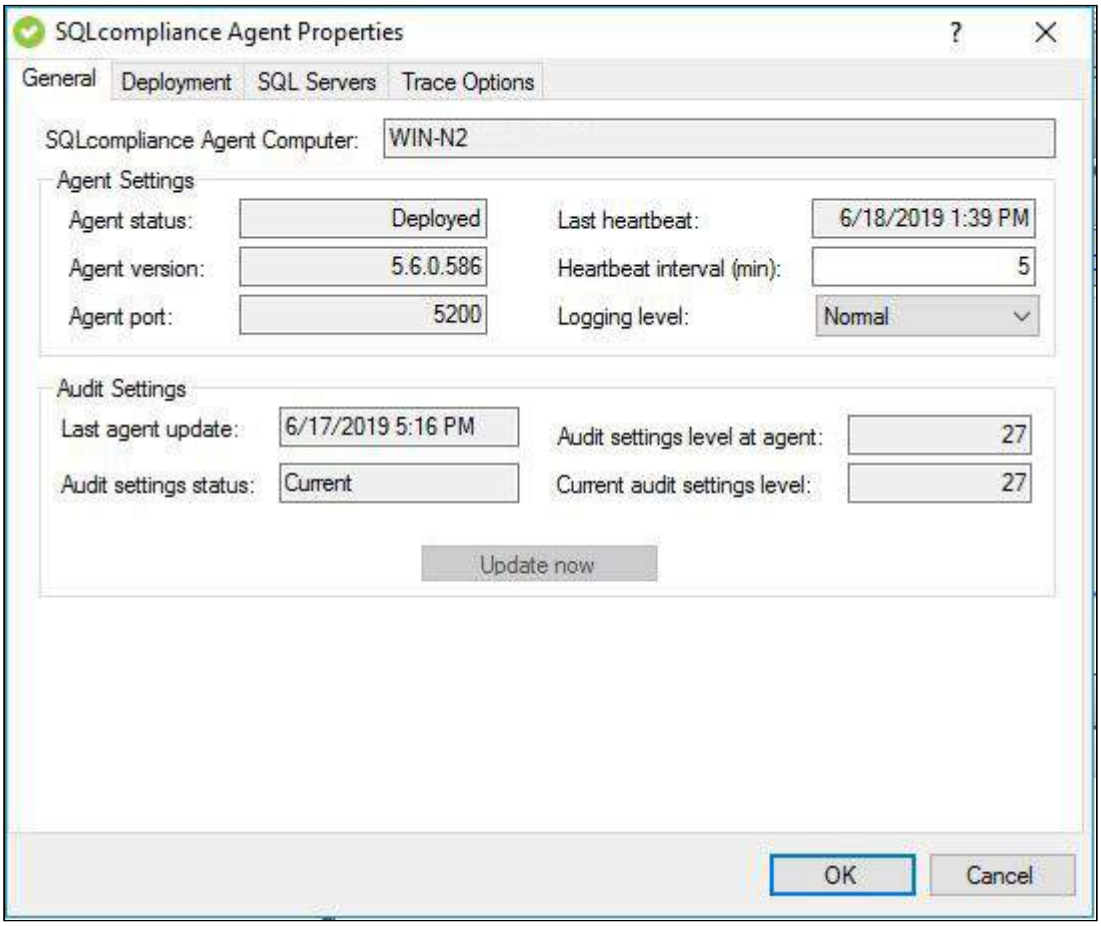
SQL Compliance Manager Agent Deployment

Indicates which deployment method (automatic or manual) was used to install the SQL Compliance Manager Agent on this SQL Server instance.

SQL Compliance Manager Agent Properties window - General tab

The General tab of the SQL Compliance Manager Agent Properties window allows you to monitor the health of the SQL Compliance Manager Agent that is auditing the selected SQL Server instance.

If you modifying properties for a SQL Compliance Manager Agent that is auditing a virtual SQL Server, IDERA SQL Compliance Manager applies your changes to the active node in the cluster hosting the virtual SQL Server. SQL Compliance Manager 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 SQL Compliance Manager Agent. The SQL Compliance Manager Agent service applies your updates immediately.

Available fields

SQL Compliance Manager Agent Computer

Provides the name of the computer on which the SQL Compliance Manager 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 SQL Compliance Manager Agent calls the Collection service and receives audit setting updates. By default, the heartbeat interval is five minutes.

Logging level

Allows you to select the logging level at which the SQL Compliance Manager 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

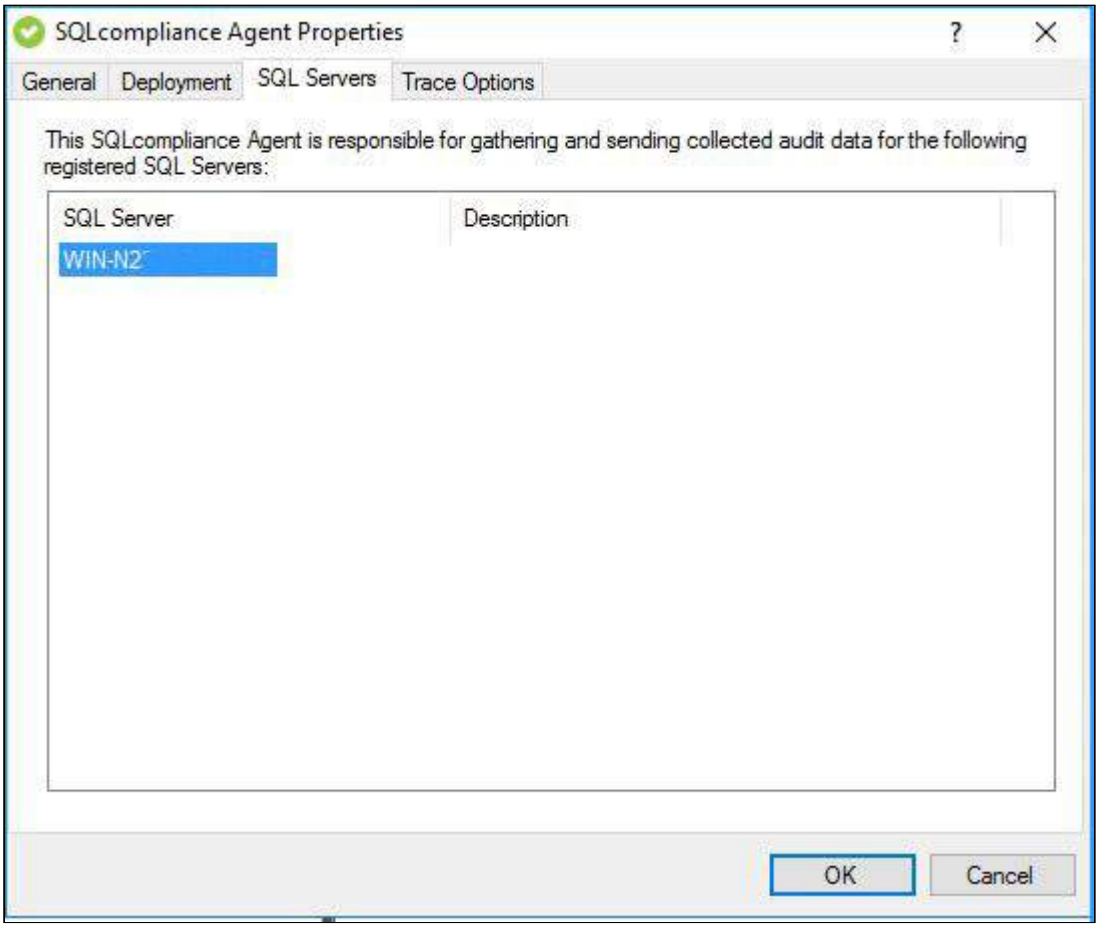
Provides the version of the audit settings applied at the agent. ***If the agent audit settings level does not match the current audit settings level***, consider performing an immediate update.

Current audit settings level

Provides the version of the audit settings available at the Collection Server.

SQL Compliance Manager Agent Properties window - SQL Servers tab

The SQL Servers tab of the SQL Compliance Manager Agent Properties window allows you to verify which SQL Server instances are currently audited by the SQL Compliance Manager 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*.

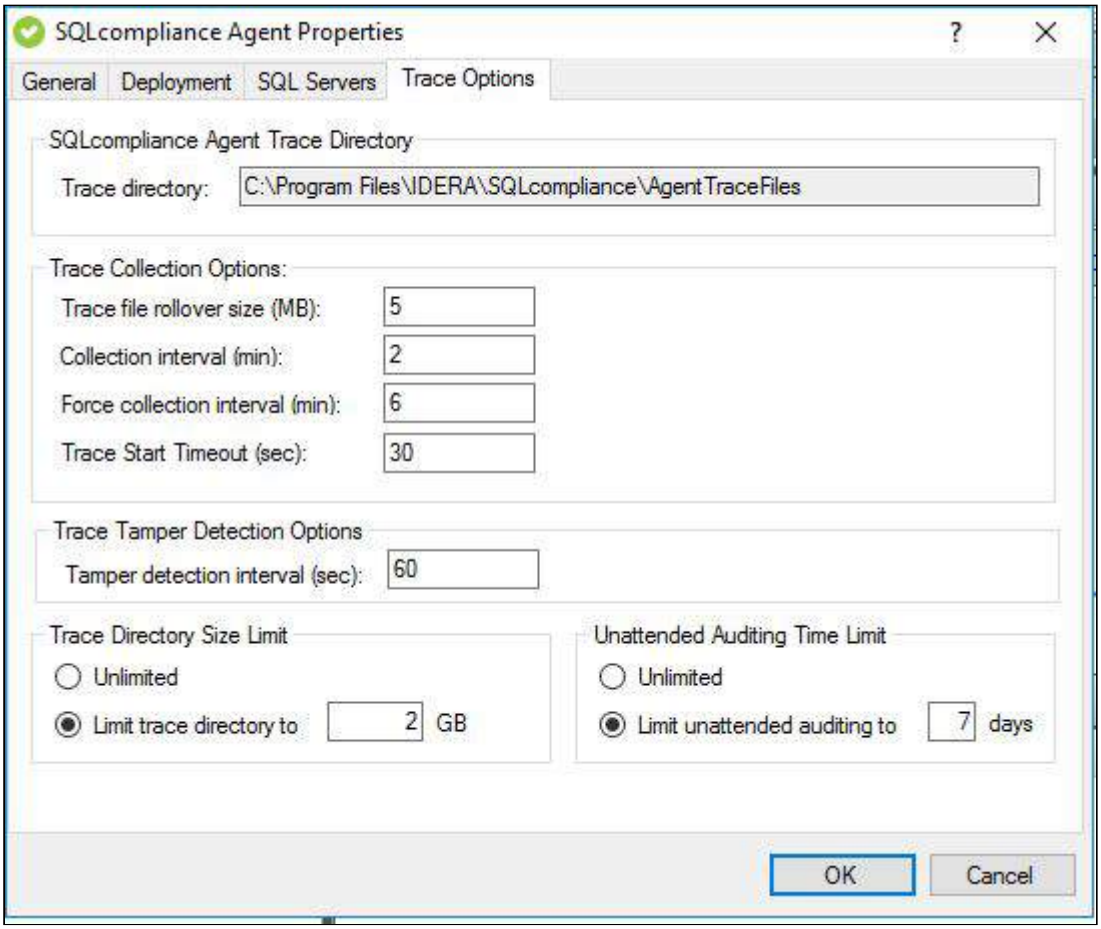
Description

Provides the description you specified when you registered the selected SQL Server instance.

SQL Compliance Manager Agent Properties window - Trace Options tab

The Trace Options tab of the SQL Compliance Manager Agent Properties window allows you to configure how the SQL Compliance Manager Agent manages the trace files that contain collected events for auditing.

If you are modifying properties for a SQL Compliance Manager 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. SQL Compliance Manager Agent properties are later replicated from the active node to the passive nodes.



Available fields

SQL Compliance Manager Agent Trace Directory

Provides the directory path under which the SQL Compliance Manager Agent stores trace files.

Trace Collection Options

Allows you to specify the following settings:

- The rollover size (MB) at which the SQL Compliance Manager 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 SQL Compliance Manager Agent should send full trace files to the Collection Server
- Maximum time (minutes) that should elapse before the SQL Compliance Manager Agent sends existing trace files to the Collection Server (if no trace files are received during the normal collection interval)
- Maximum time (seconds) that should elapse before the SQL Compliance Manager 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 SQL Compliance Manager Agent automatically restarts the SQL trace. The SQL Compliance Manager Agent detects whether the trace is stopped, modified, paused, or deleted by another application. After the specified tamper

detection interval, the SQL Compliance Manager Agent restarts the trace and records the trace status to the application event log.

Trace Directory Size Limit

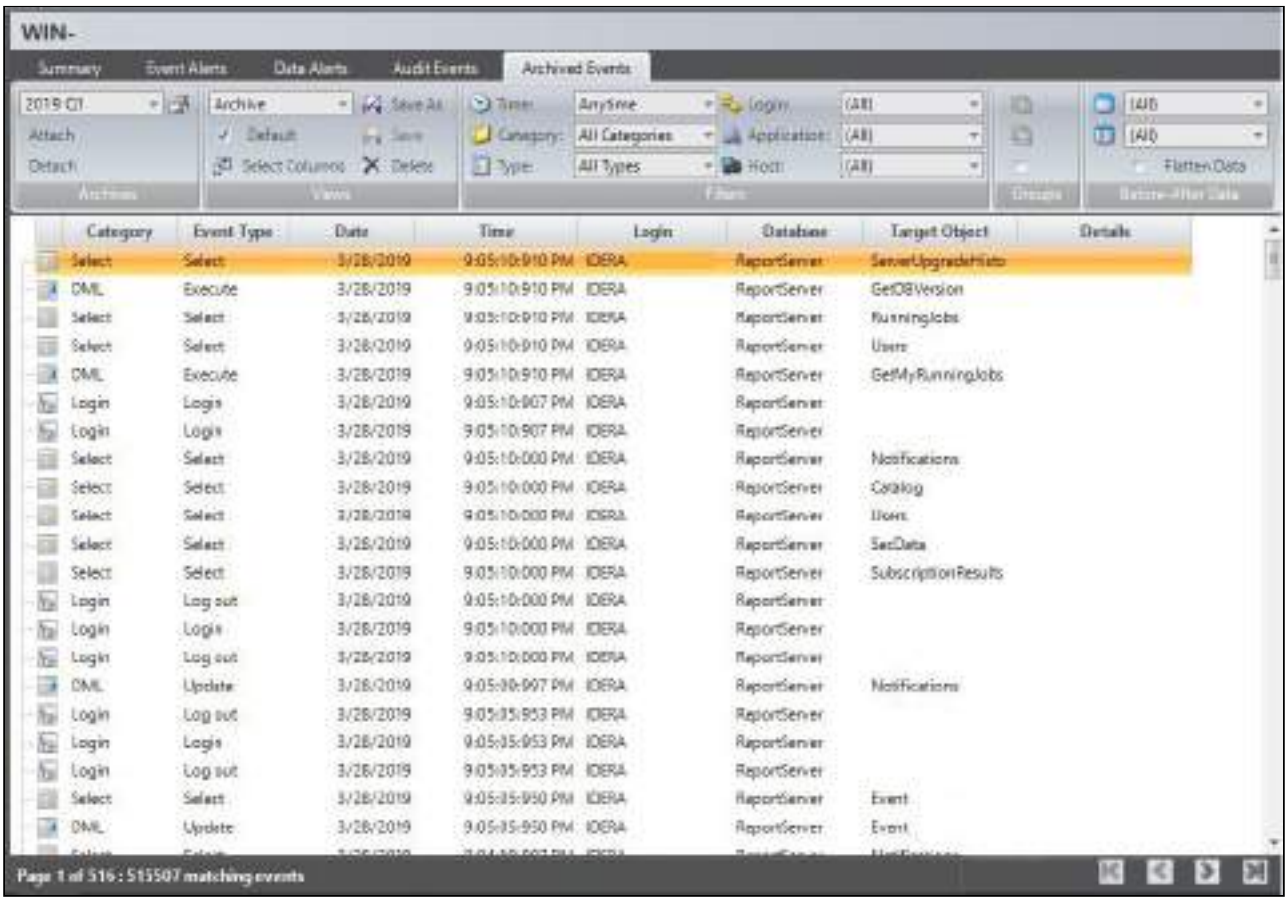
Allows you to specify the maximum size threshold (GB) for the directory where you are storing the trace files. The directory size is checked at each heartbeat. To effectively manage the directory size, ensure you allow ample room to accommodate your auditing needs and set the SQL Compliance Manager Agent heartbeat interval at a low frequency.

Unattended Auditing Time Limit

Allows you to specify the maximum time threshold (days) for allowing the SQL Compliance Manager Agent to run without receiving a heartbeat.

Archived Events tab

The Archived Events 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 IDERA 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

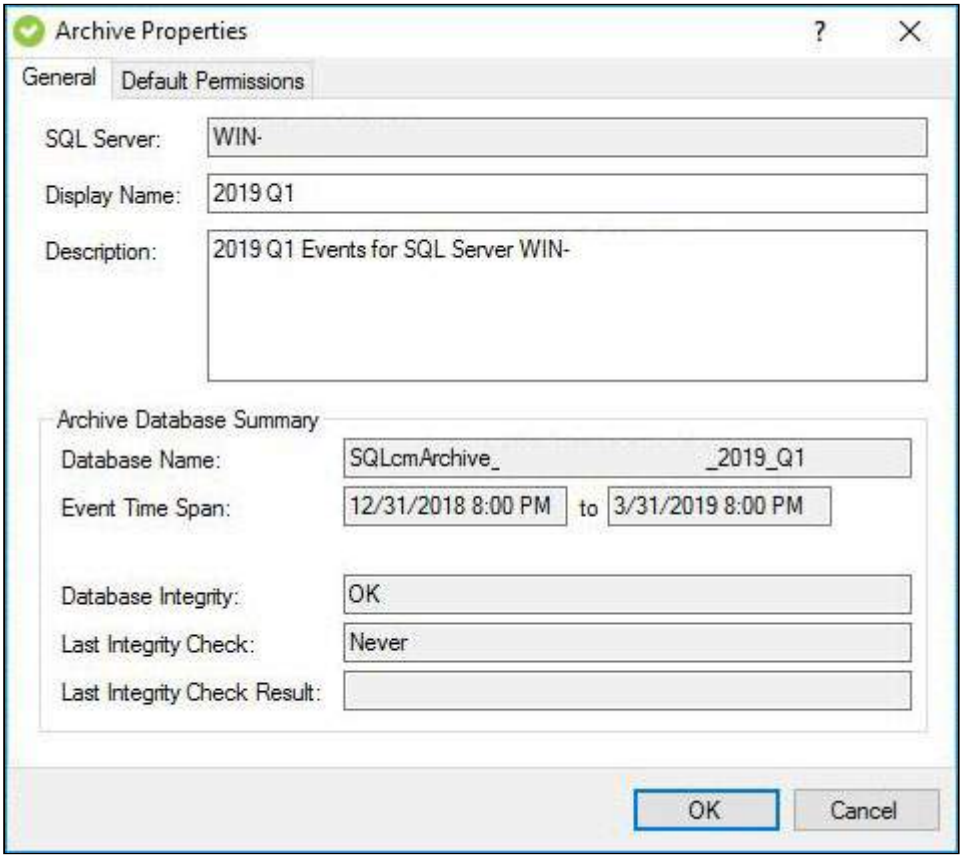
Provides the name of the SQL Server login targeted by the T-SQL statement associated with this event.

Target User

Provides the name of the database user targeted by the T-SQL statement associated with this event.

Archive Properties Window - General tab

The General tab of the Archive Properties window 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 2017 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 2017 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

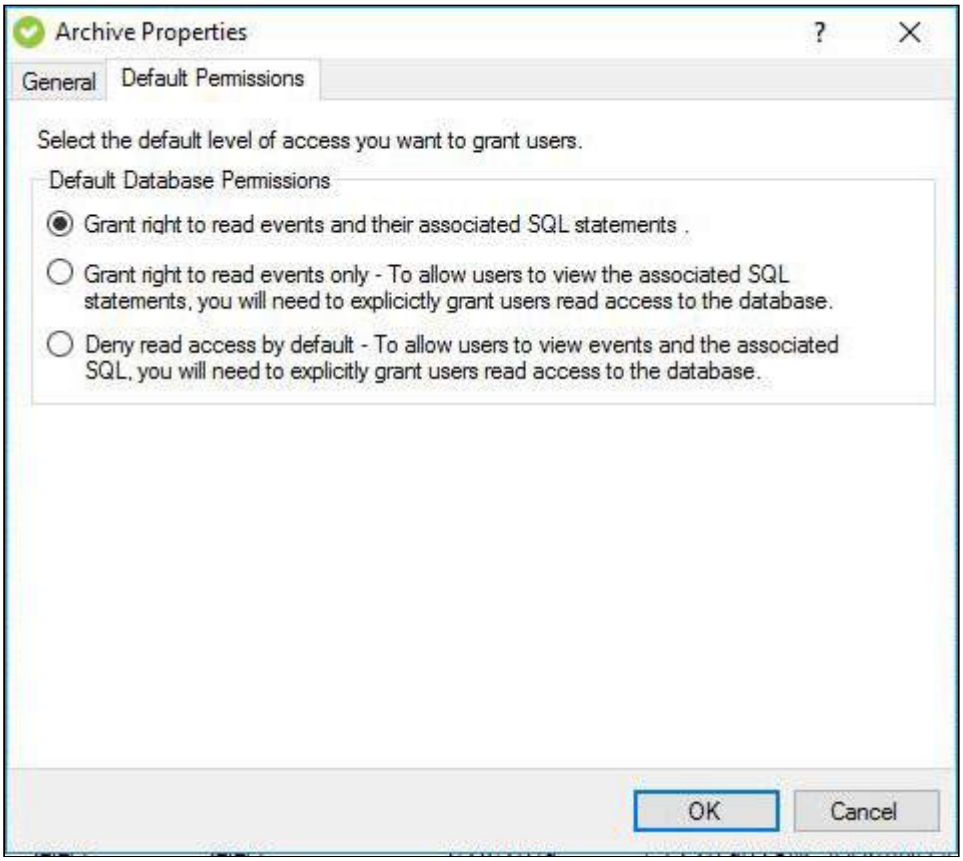
Provides the date and time an integrity check was last performed on this archive database.

Last Integrity Check Result

Summarizes the results of the last integrity check, such as **Passed** or **Problems found and marked in audit data.**

Archive Properties Window - Default Permissions tab

The Default Permissions tab of the Archive Properties window lets you control the default permission settings at the archive database.



Available fields

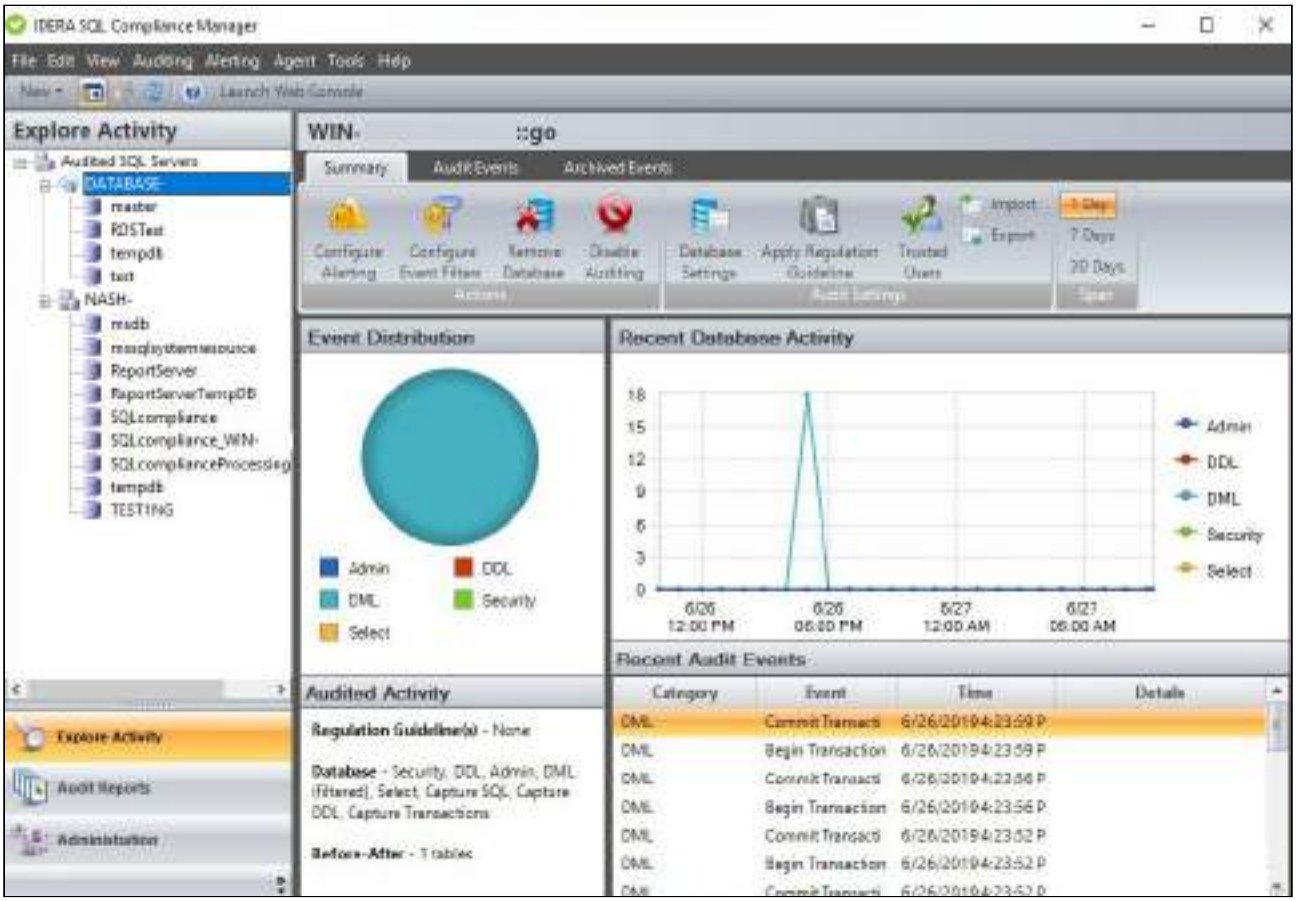
Default Database Permissions

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

9.1.4 Explore Activity - Database View

The Explore Activity Database view allows you to view the status of audit activity for a particular database hosted by the selected SQL Server instance. View the Summary tab for an overview of the recent activity performed on the selected database, or use the Audit Events tab to analyze the collected database events. You can also visit the Archived Events tab to view your archived databases.

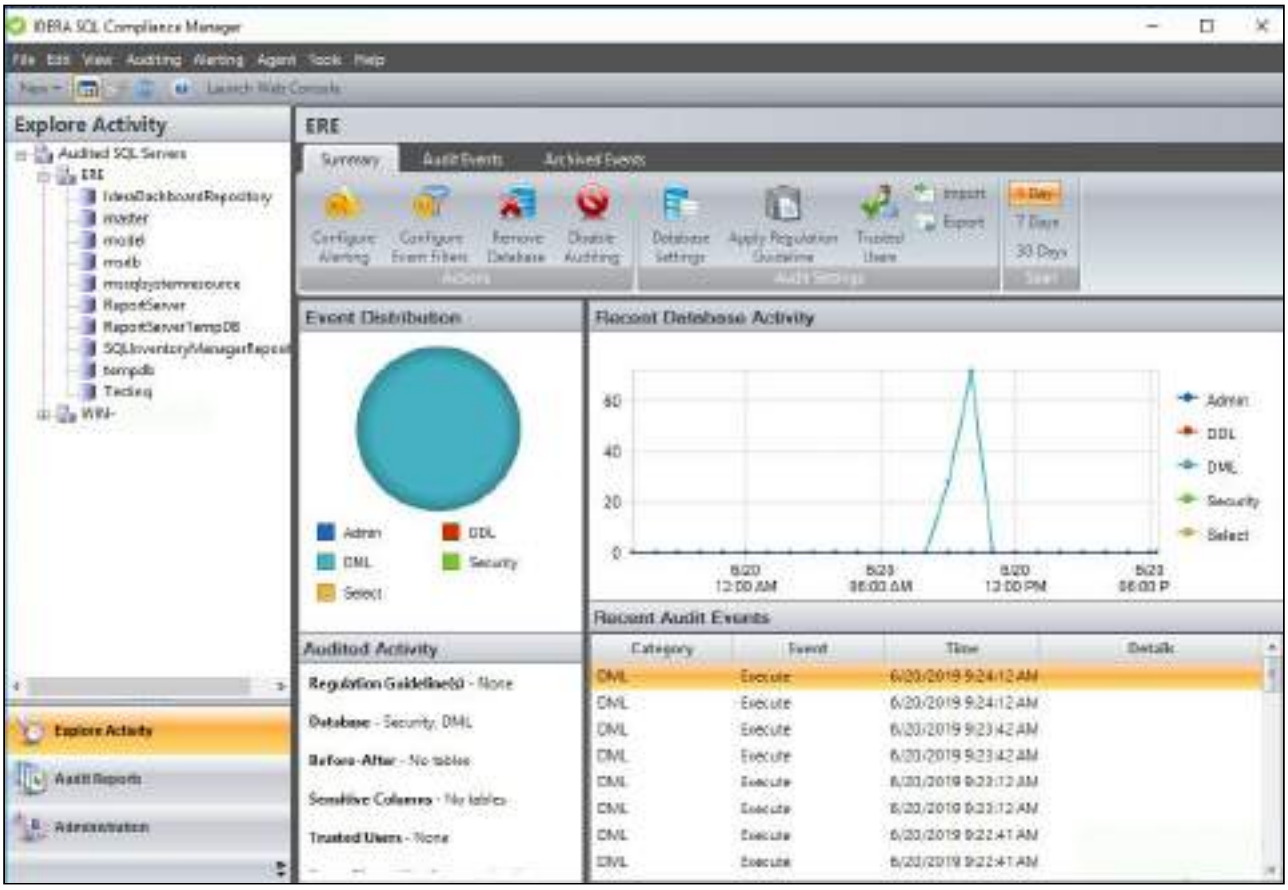


For more information visit the different tabs of the Explore Activity Database view below:

- Explore Activity Database view - Summary tab
- Explore Activity Database view - Audit Events tab
- Explore Activity Database view - Archived Events tab

Explore Activity - Database Summary tab

The IDERA 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 audited for before and after data.

Sensitive Columns

Lists which tables are audited at the column level for SELECT events.

Trusted Users

Displays the number of trusted users that are excluded from the audit trail.

Event Filters

Displays the number of Event Filters that are created to streamline audit data collected from this database, and the event properties 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 SQL Compliance Manager 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. For more information, see Disabling auditing on a database.

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. For more information, see Audited Database Properties.

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. For more information, see Apply Regulation Guideline.

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. For more information, see Audited Database Properties window - Trusted Users tab.

Import

Allows you to import audit settings previously exported from another audited instance or database. For more information, see Import your audit settings wizard.

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.

Audited Database Properties

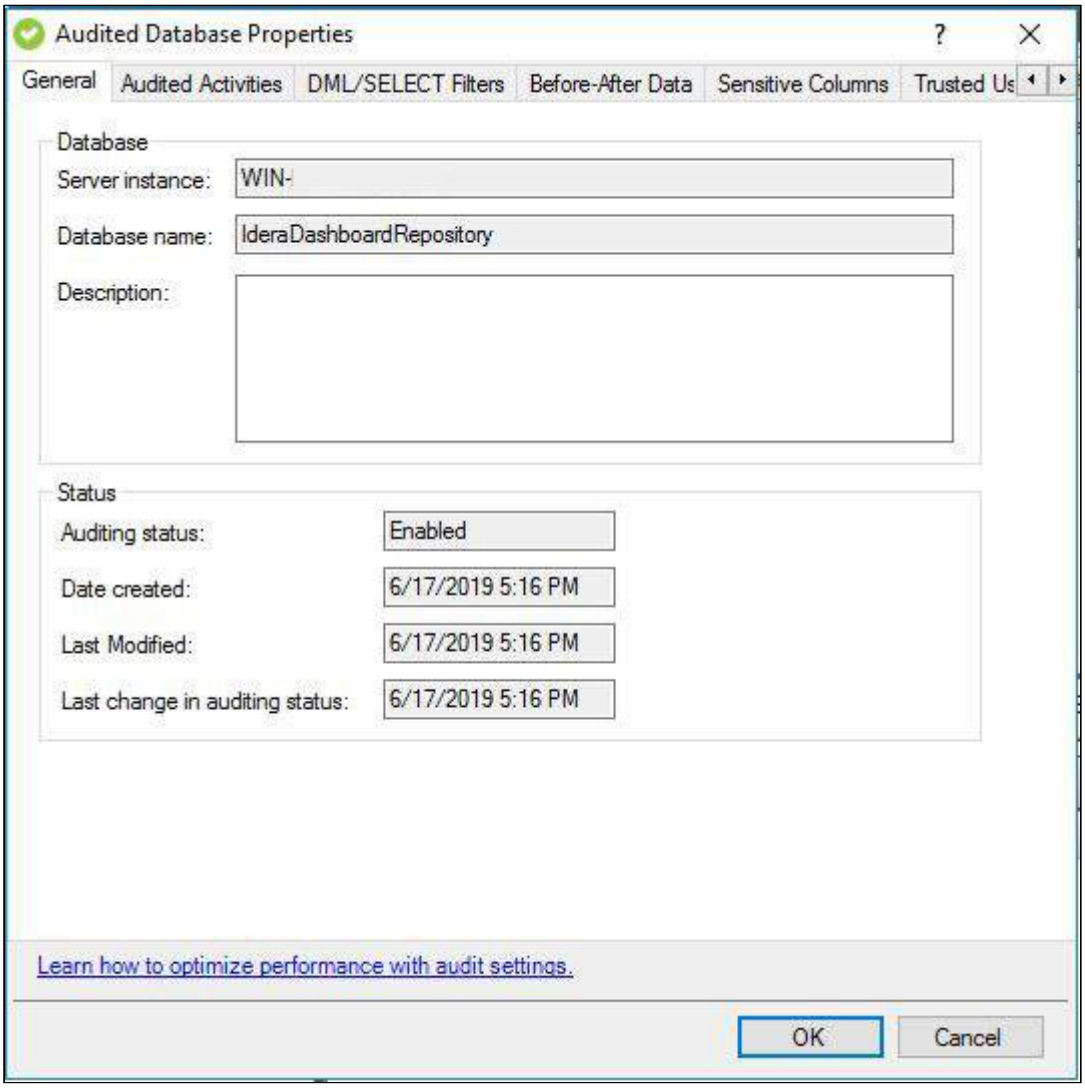
Use the different Audited Database Properties windows to configure your desired audit settings. When you choose to audit a database, IDERA SQL Compliance Manager collects and processes SQL Server events on the database according to your audit settings.

Use the different tabs to set your Audited Database Properties:

- Audited Database Properties window - General tab
- Audited Database Properties window - Audited Activities tab
- Audited Database Properties window - DML/SELECT Filters tab
- Audited Database Properties window - Before-After Data tab
- Audited Database Properties window - Sensitive Columns tab
- Audited Database Properties window - Trusted Users tab
- Audited Database Properties window - Privileged User Auditing tab

Audited Database Properties window - General tab

The General tab of the Audited Database Properties window 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

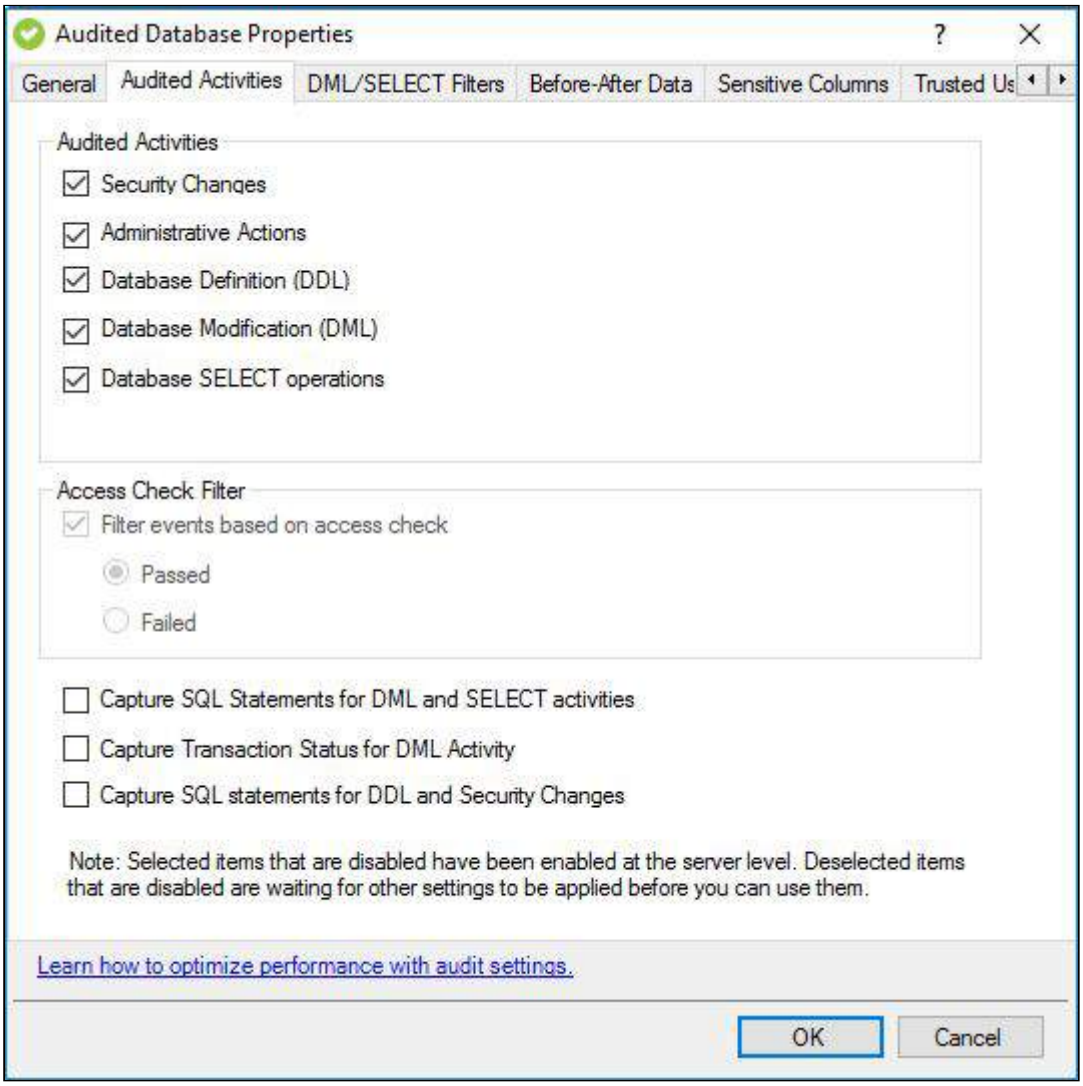
Provides the date and time when audit settings were last modified for this database.

Last change in auditing status

Provides the date and time when the auditing status of this database changed.

Audited Database Properties window - Audited Activities tab

The Audited Activities tab of the Audited Database Properties 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 to select the type of activity you want to audit. IDERA SQL Compliance Manager collects and processes the corresponding SQL Server events based on your selections.

The following are the activities you can audit:

- Security changes
- Administrative Actions
- Database Definition (DDL)
- Database Modification (DML)
- Database SELECT operations

> **Note**
>
> Audited Activities selected at Database-level are automatically pre-selected and disabled for selection when adding new Privileged Users at the Database Privileged User auditing configurations.

> **Note**
>
> When deselecting an audited activity, choose between deselecting at Database-level auditing only or Database-level and Privileged Users auditing.

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 Compliance Manager 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.

Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

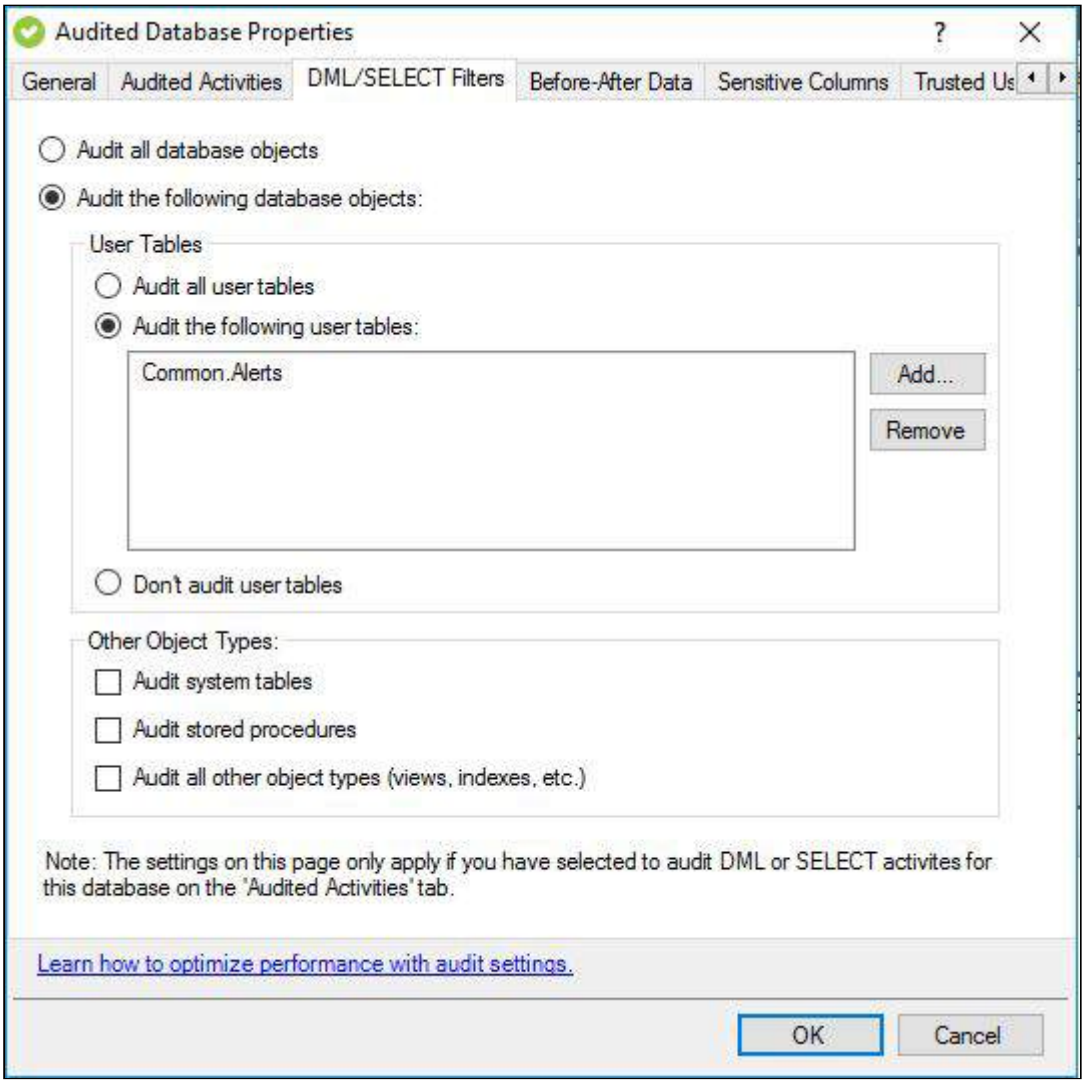
Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Audited Database Properties window - DML/SELECT Filters tab

The DML/Select Filters tab of the Audited Database Properties window 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.

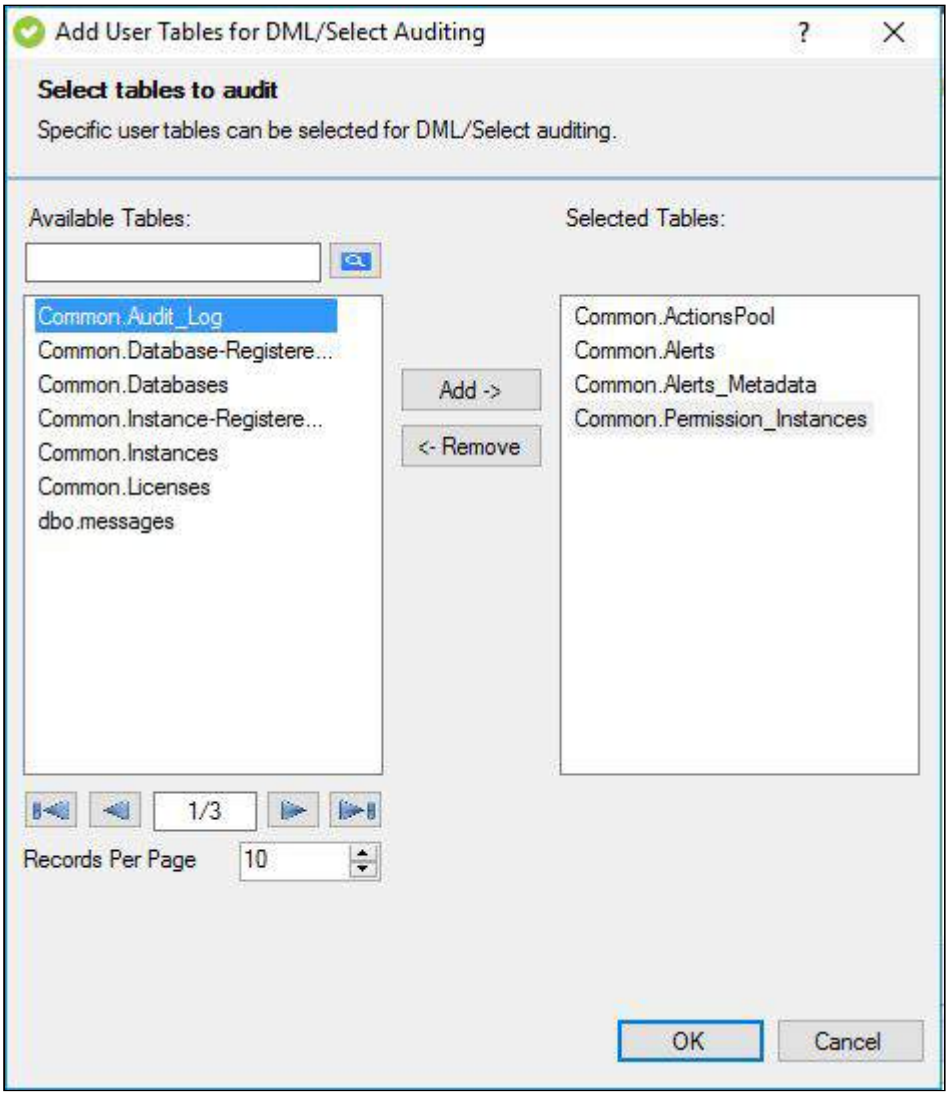
Remove

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.

Add User Tables window - DML and SELECT statements

The Add User Tables 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**.



Audited Database Properties window - Before-After Data tab

The Before-After Data tab of the Audited Database Properties window 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.

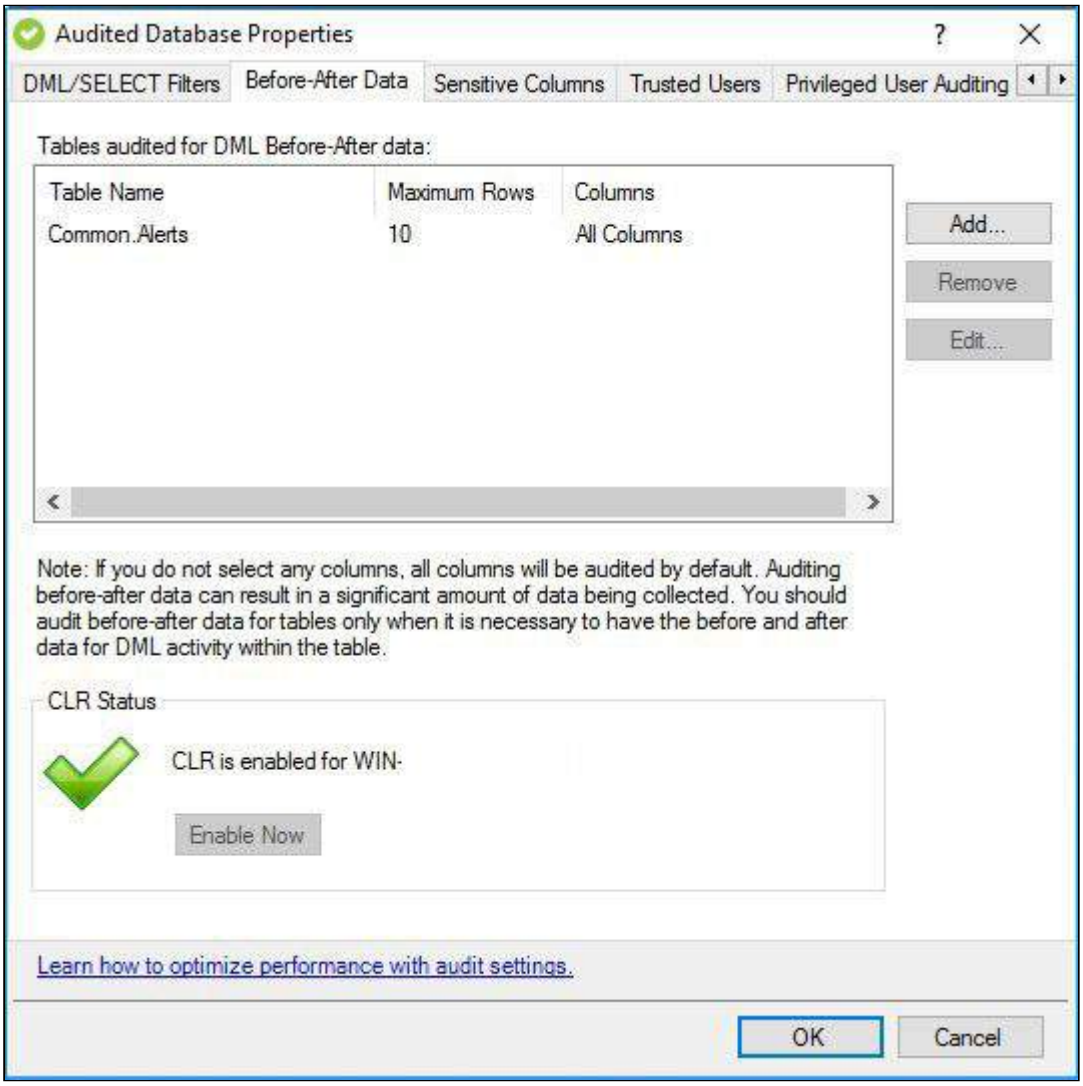
Collect before and after data when it is critical to capture the exact data change in a table column. When this feature is enabled, you can evaluate the before value and after value for each change in the Audit Events view. Enabling this feature can impact your Collection Server and Management Console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

IDERA provides limited support for before-after data auditing of the publisher database in SQL Servers with replication. However, this scenario is supported only when the publisher database with transaction replication is set to replicate data ONLY. ***If the target database uses SQL Server replication set to***

replicate more than data, do not enable before-after auditing. Before and after data collection does not support SQL Server replication in that situation. For more information, see Microsoft Books Online for the version of SQL Server you are using.

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 SQL Compliance Manager 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 SQL Compliance Manager Agent will capture of each DML transaction.

Columns

Indicates the status of the columns associated with the audited tables. Typically, this field displays **All Columns** or lists the individual columns that are audited for before-and-after data.

If the audited table contains BLOB data and individual columns that are not 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

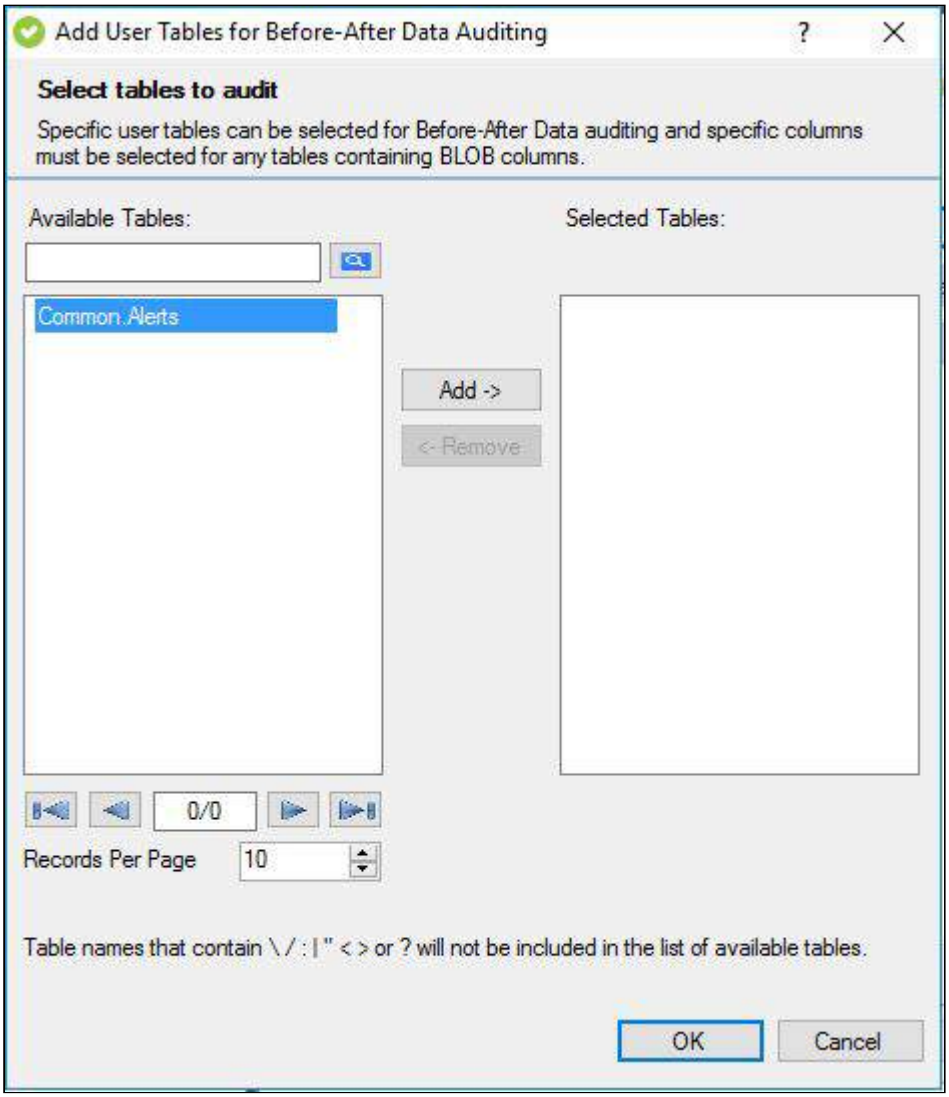
Auditing before and after data is an extension of DML event auditing at the table column level.

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**.

Add User Tables window - Before and after data

The Add Users Tables 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 IDERA SQL Compliance Manager does not support auditing BLOB data types. BLOB data includes:

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

Audited Database Properties window - Sensitive Columns tab

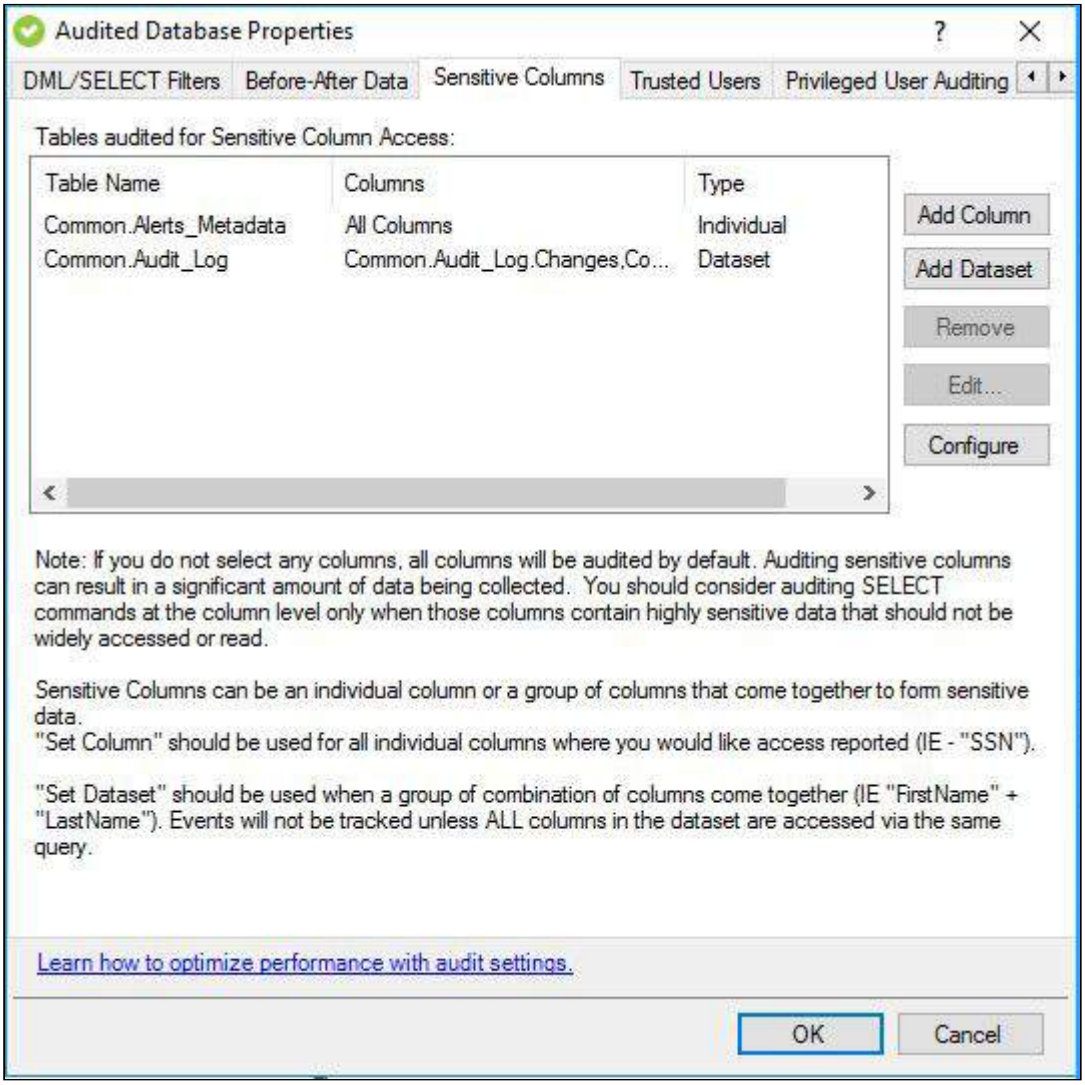
The Sensitive Columns tab of the Audited Database Properties window allows you to select the individual table columns or datasets you want IDERA SQL Compliance Manager to audit for sensitive column access. Configure the type of activity you want to collect data for, choose between Selects, Selects and DML or All Activity. This data tells you which third-party application or database user accessed and read the specified columns. Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data. If no individual columns are selected, by default all columns from the selected table will be audited.

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.

IDERA SQL Compliance Manager does not capture sensitive column data for trusted user accounts. For more information about trusted users, see Audited Database Properties window - Trusted Users tab.

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 SQL Compliance Manager 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.

Specify which columns to audit as a group

Use **AddDataSet** to specify a group of columns to audit as a set of sensitive information.

Configure

Allows you to choose which type of activity you want Sensitive Columns to collect data for. You can choose one of the following types of activity to collect data for your Sensitive Columns:

- Select Only - captures all Select queries only.
- All Activity - captures all Select, DDL and DML activities on tables configured for Sensitive Column.
  - Captures Select, Insert, Update and Delete on the Sensitive Columns.
  - Captures Alter and Drop queries on tables where Sensitive Columns are present.
  - Captures Select, Insert, Update and Delete on the Sensitive Columns if the sensitive columns are accessed through views or Stored Procedures.
- SELECT and DML - captures Select queries and DML activity such as; Select, Insert, Update and Delete.

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 audited for SELECT events.

Type

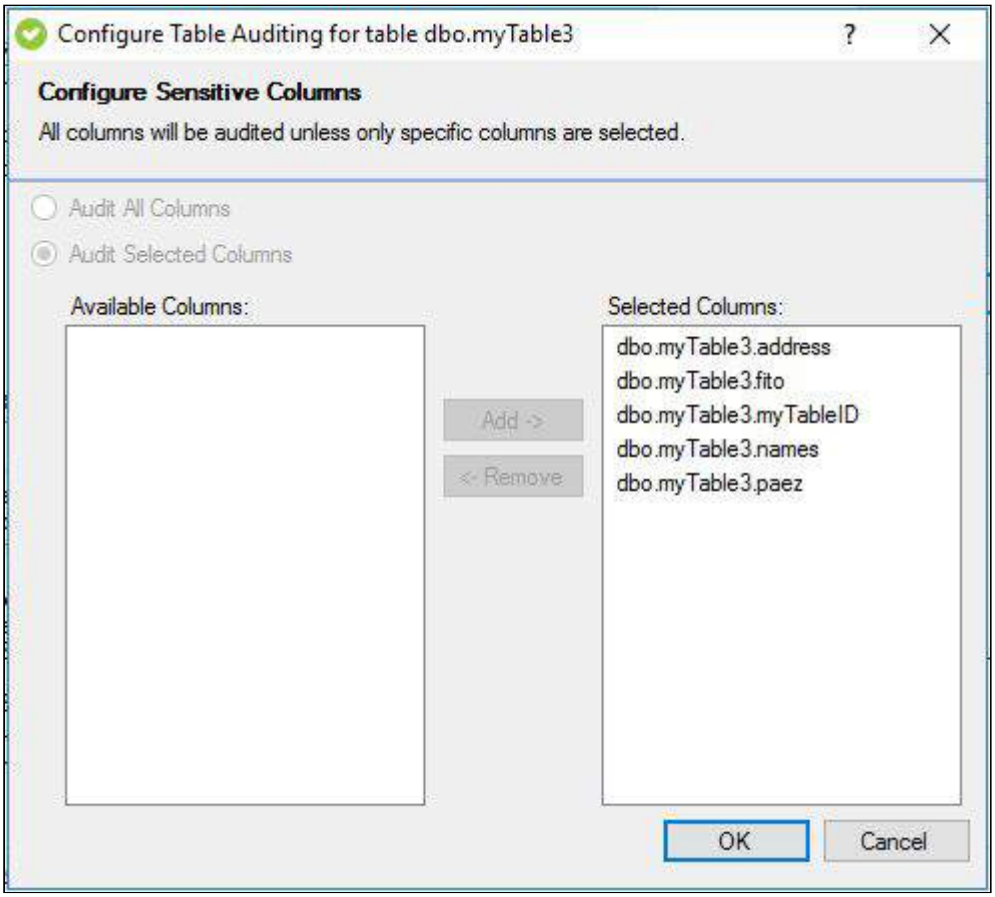
Indicates whether the column is being audited as an 'Individual' or as part of a 'Dataset'.

Set up auditing sensitive columns

Sensitive column auditing occurs independently from your other database-level audit settings.

To set up auditing sensitive columns:

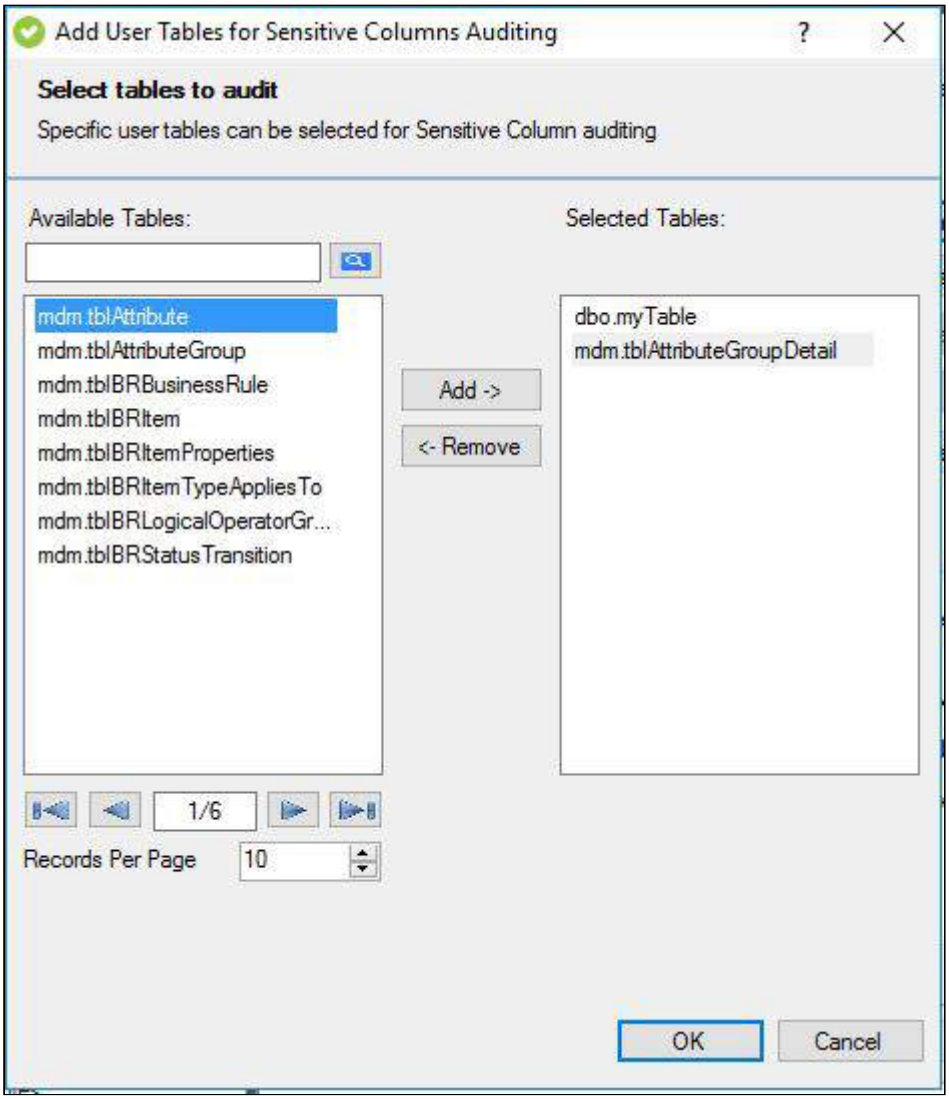
1. On the Sensitive Columns tab, click **Add** to choose which audited tables should also be audited at the column level when a user attempts to access this column.
2. Choose the appropriate tables, and then click **OK**. By default, all columns are audited.
3. ***If you want to audit specific columns***, select the table, and then click **Edit**.
4. ***if you want to audit a group of columns***, click **AddDataSet.**



Add User Tables window - Sensitive columns

The Add User Tables window allows you to specify which user tables you want to audit for sensitive columns. You can add specific columns as well as entire datasets. This setting is available when you choose to audit sensitive columns at the database level.

From the Available Tables pane, select the user tables you want to audit, and then click **Add**.



Configure Table Auditing window

The Configure Table Auditing 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.

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 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. 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.

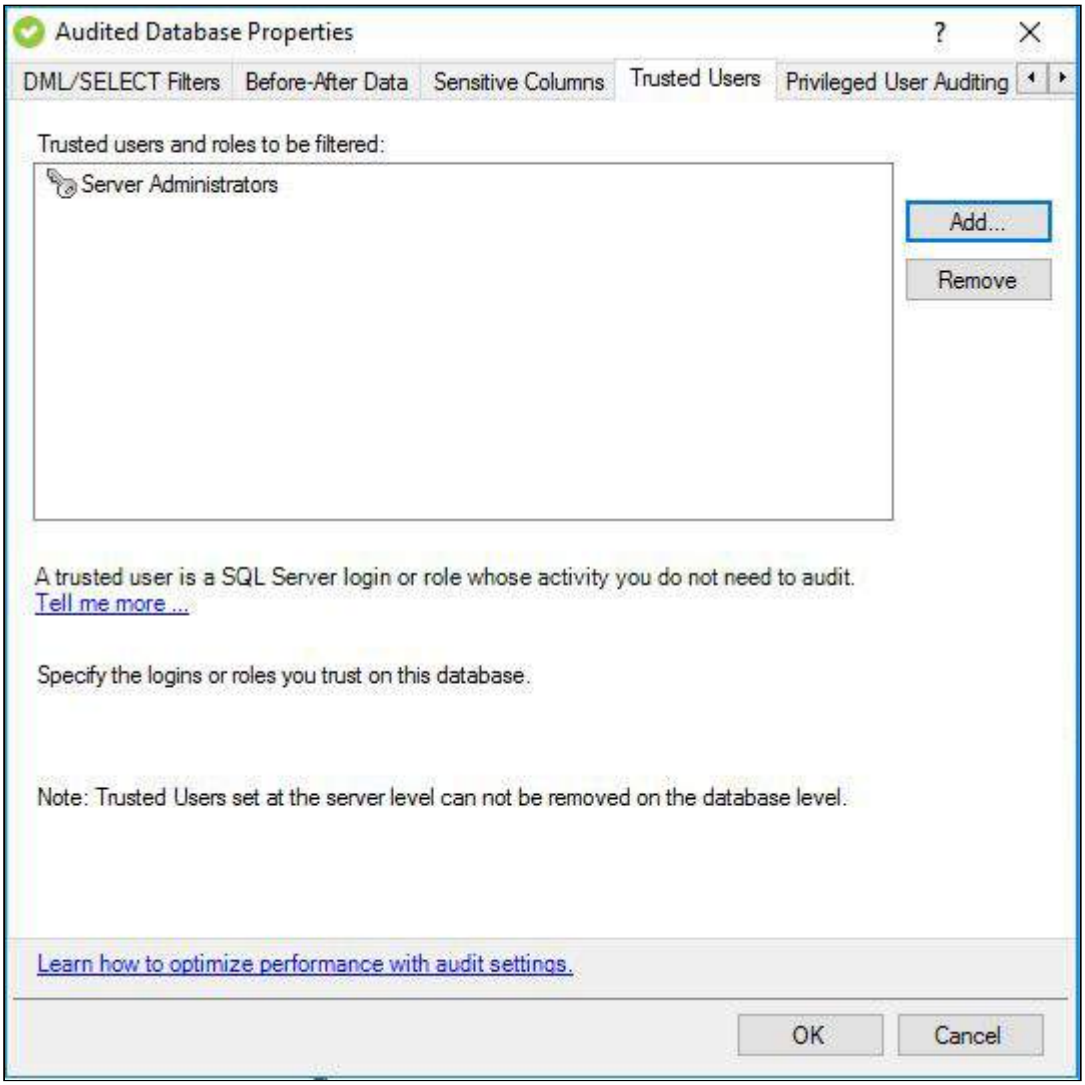
If you are auditing privileged user activity and the trusted user is also a privileged user, IDERA SQL Compliance Manager will continue to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited 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.

⚠ Trusted Users set at Server level will automatically be enabled for all databases under that server. To remove Trusted Users, you must do so at Server Level Properties.

⚠ 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.

ⓘ 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 SQL Compliance Manager Agent omits all database-level activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

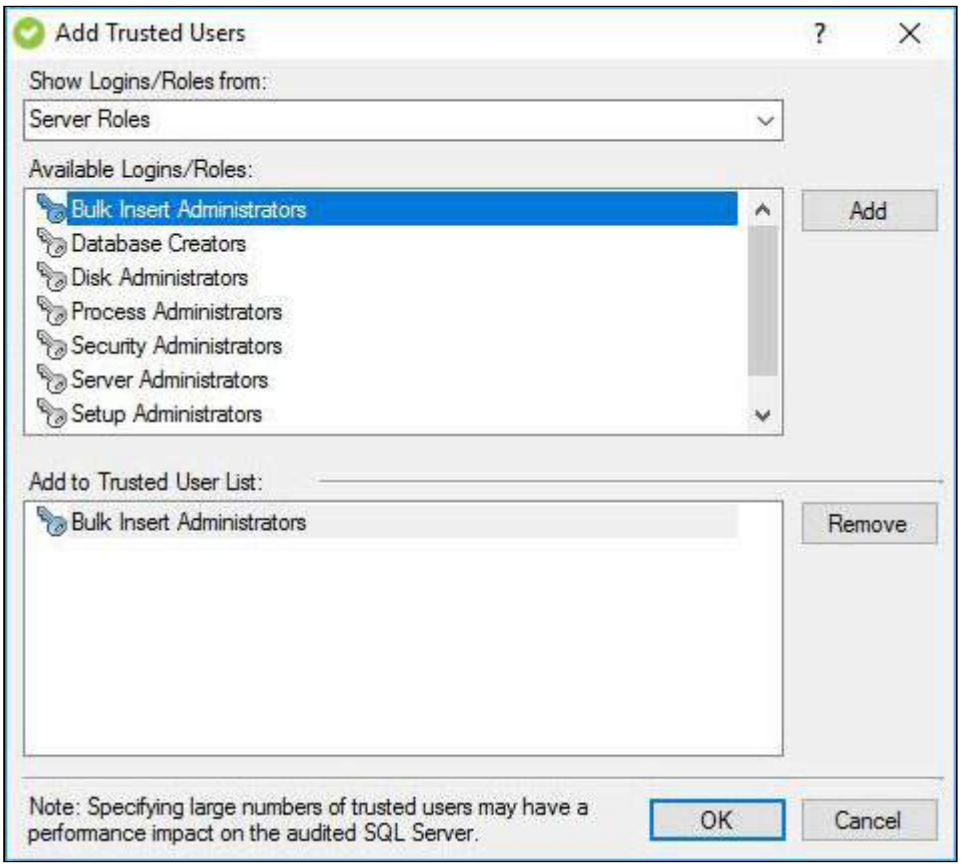
Allows you to designate a previously trusted user or SQL Server role as non-trusted. When a login or role becomes non-trusted, SQL Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

Database Properties - Add Trusted Users window

The Add Trusted Users window allows you to specify which trusted users you want to audit. You can specify trusted users by individual SQL Server login names or by the fixed server role. When you specify a fixed server role, the SQL Compliance Manager Agent collects events generated by any login who is a member of that role.

> ⚠ 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.

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

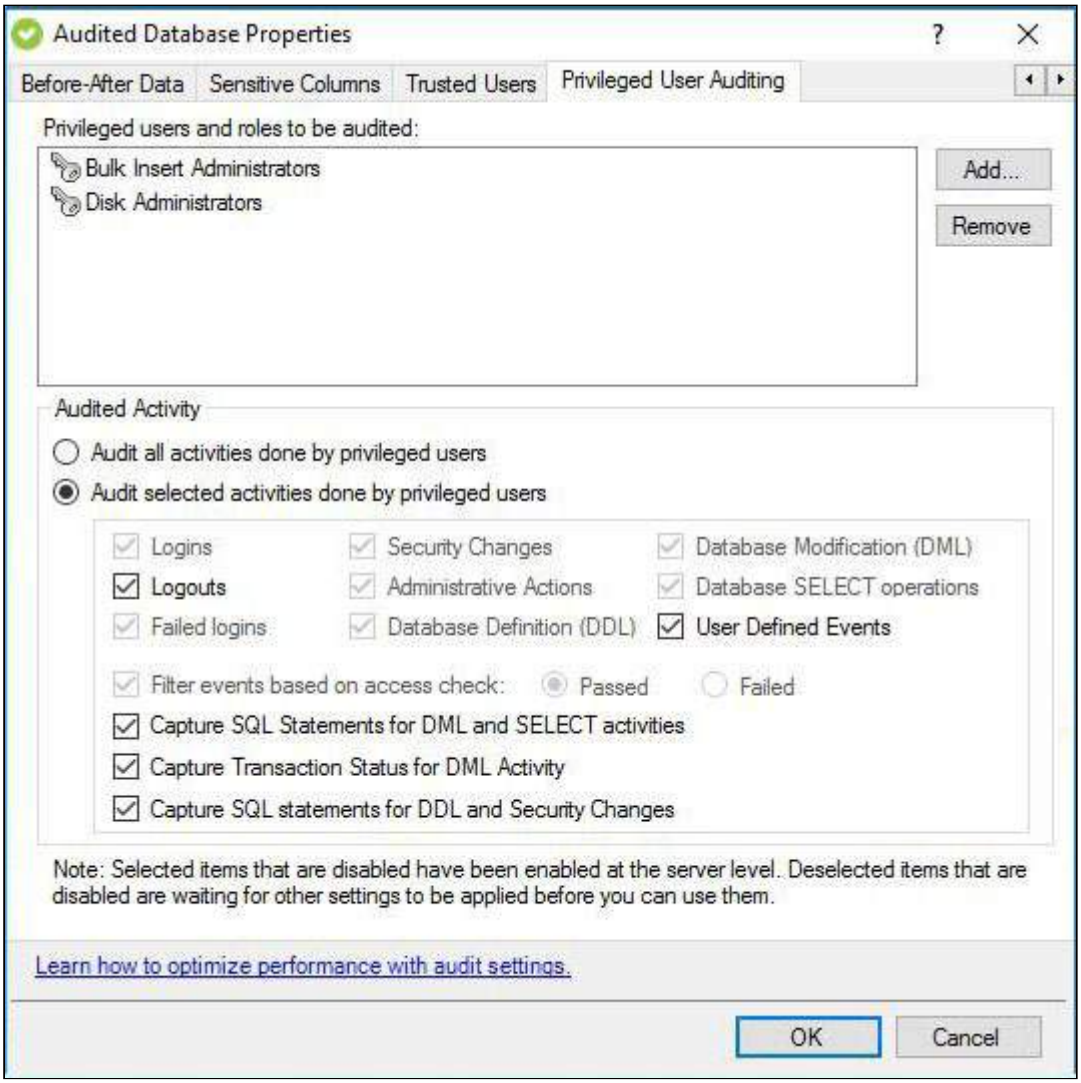


Audited Database Properties window - Privileged User Auditing tab

The Privileged User Auditing tab of the Audited Database Properties window allows you to change the audit settings currently applied to privileged users for the selected Database. 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.

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 SQL Compliance Manager 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 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 SQL Compliance Manager Agent no longer collects events recorded for that login or the role members.

> **Note**
>
> Privileged Users selected at Server-level auditing are pre-selected and disabled for selection. These Privileged Users can be removed only at Server-level Privileged Users auditing.

Available fields

Server-Level Privileged Users

Lists the audited privileged users configured at Server-level. These users can only be edited at Server-level Privileged Users.

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 SQL Compliance Manager 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. Select **Audit all activities done by privileged users** to include everything or select **Audit selected activities done by privileged users** followed by additional preferences for selective auditing. Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- Database modification (DML)
- Database SELECT operations
- User-defined events
- Filter events based on the access check

> **Note**
>
> Audited activities configured at Database-level auditing are automatically pre-selected and disabled for selection for Privileged Users added at Database level auditing. Users must edit changes at the Database level Auditing Activities tab to disable these settings.

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.

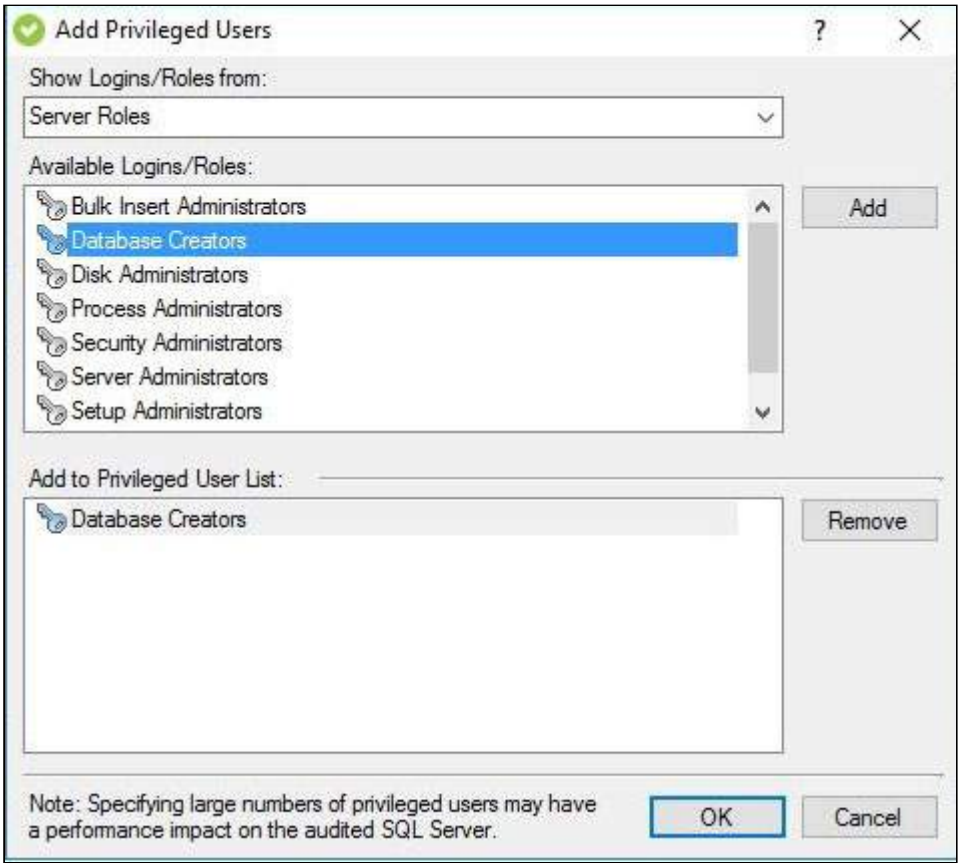
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

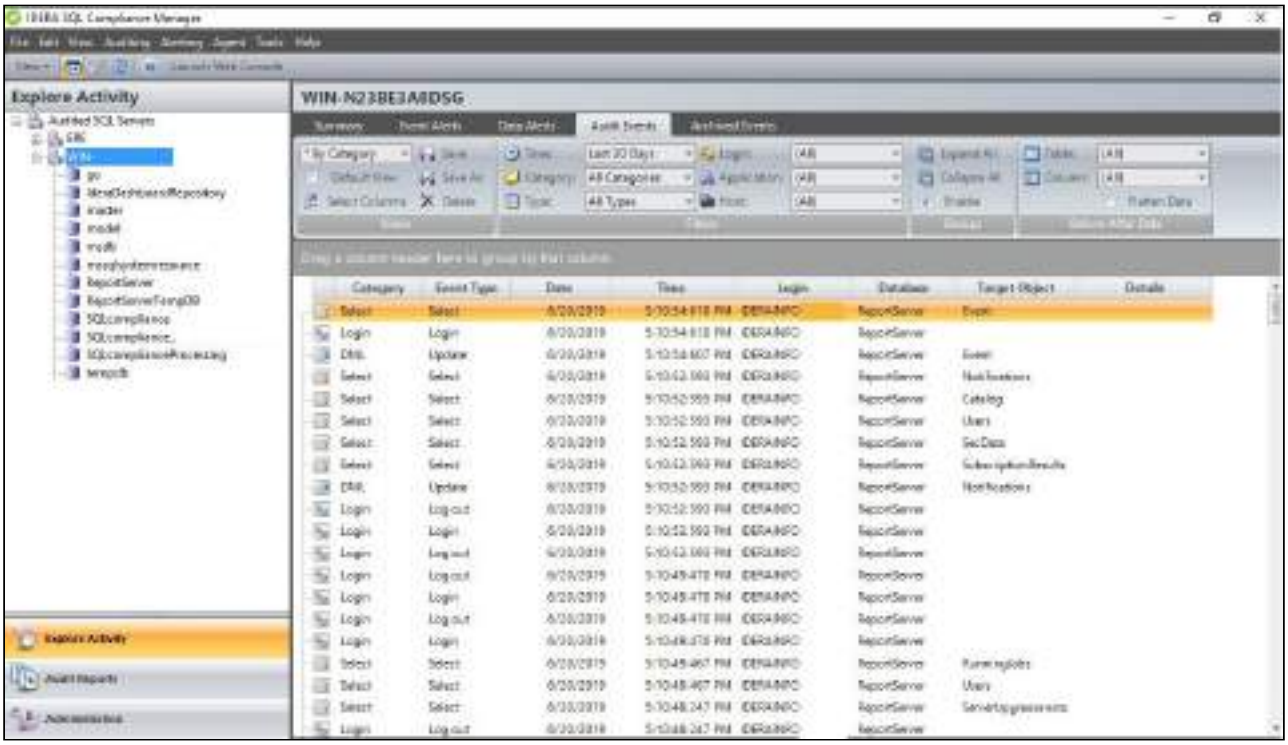
Add Privileged Users window

The Add Users window is accessed by clicking **Add** on the Privileged User Auditing tab while viewing Registered SQL Server Properties. Use this window to include selected login accounts and roles as privileged. Added logins/roles may be removed by selecting the item in the Privileged User Auditing tab and clicking **Remove**.



Audit Events tab

The Audit Events 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.

Row Count

Provides the frequency of data access.

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.

Row Count

Provides the frequency of data access.

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.

Event Properties window - General tab

The General tab of the Event Properties window allows you to view high-level information about an individual event.

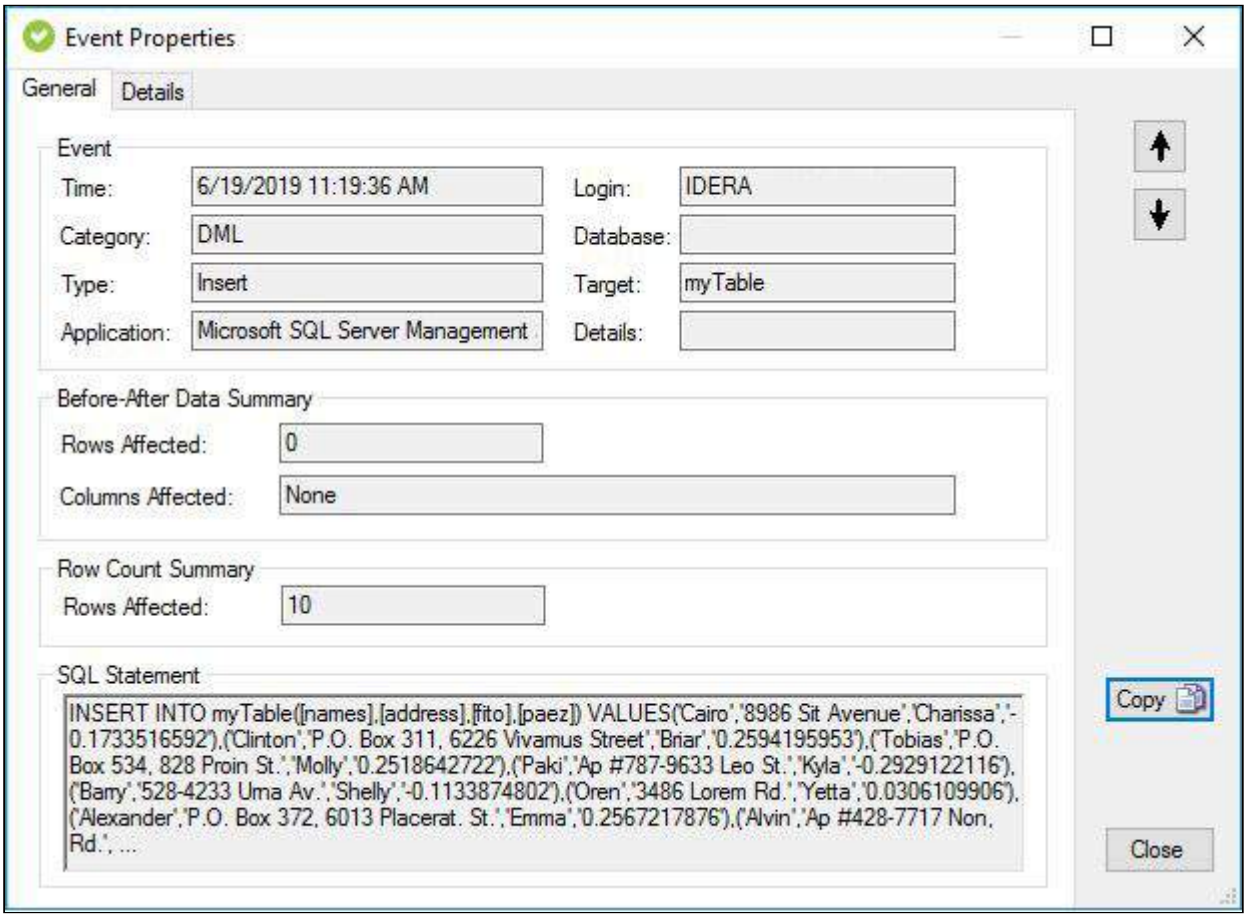
You can view the following information:

- 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)
- Row count information (if available)
- 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.

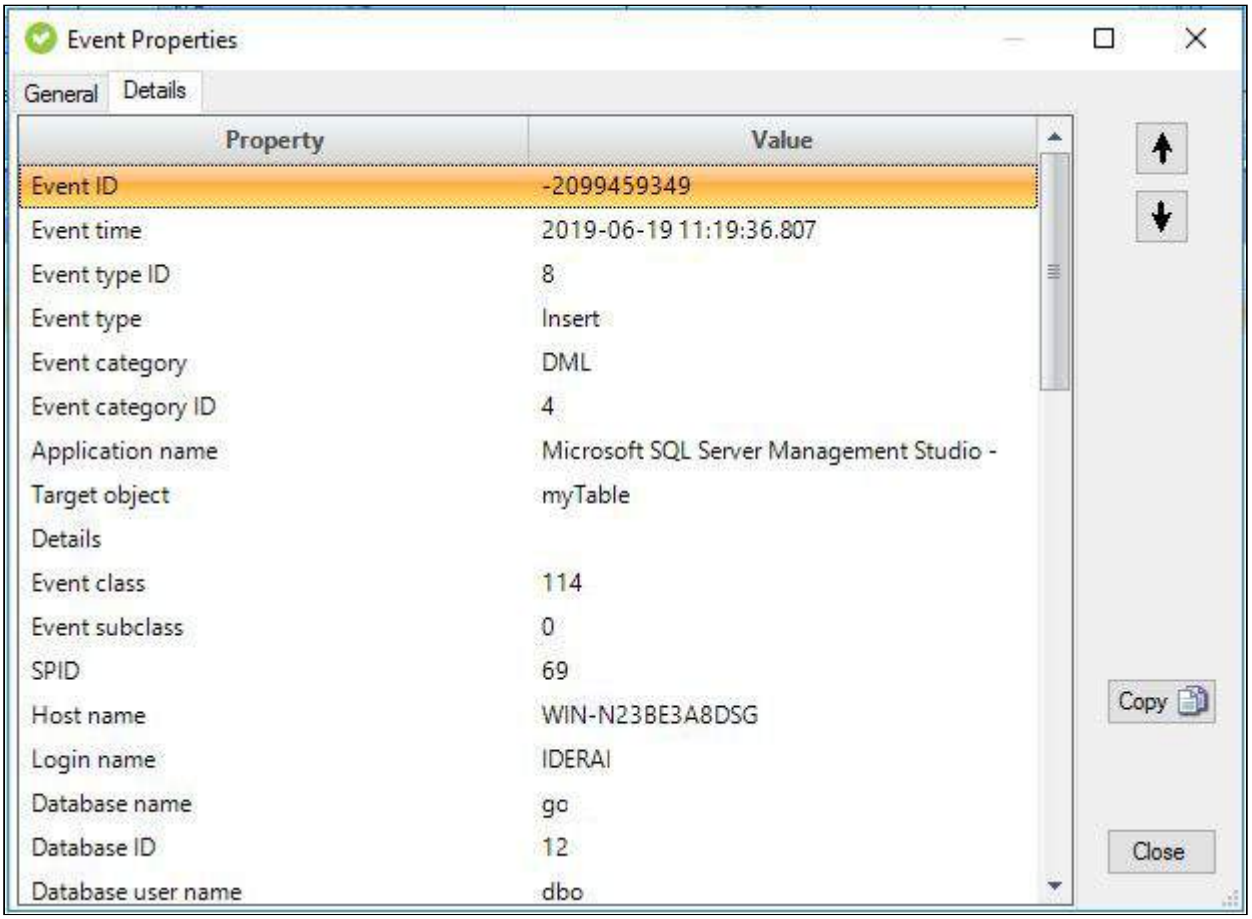


Event Properties window - Details tab

The Details tab of the Event Properties window 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.



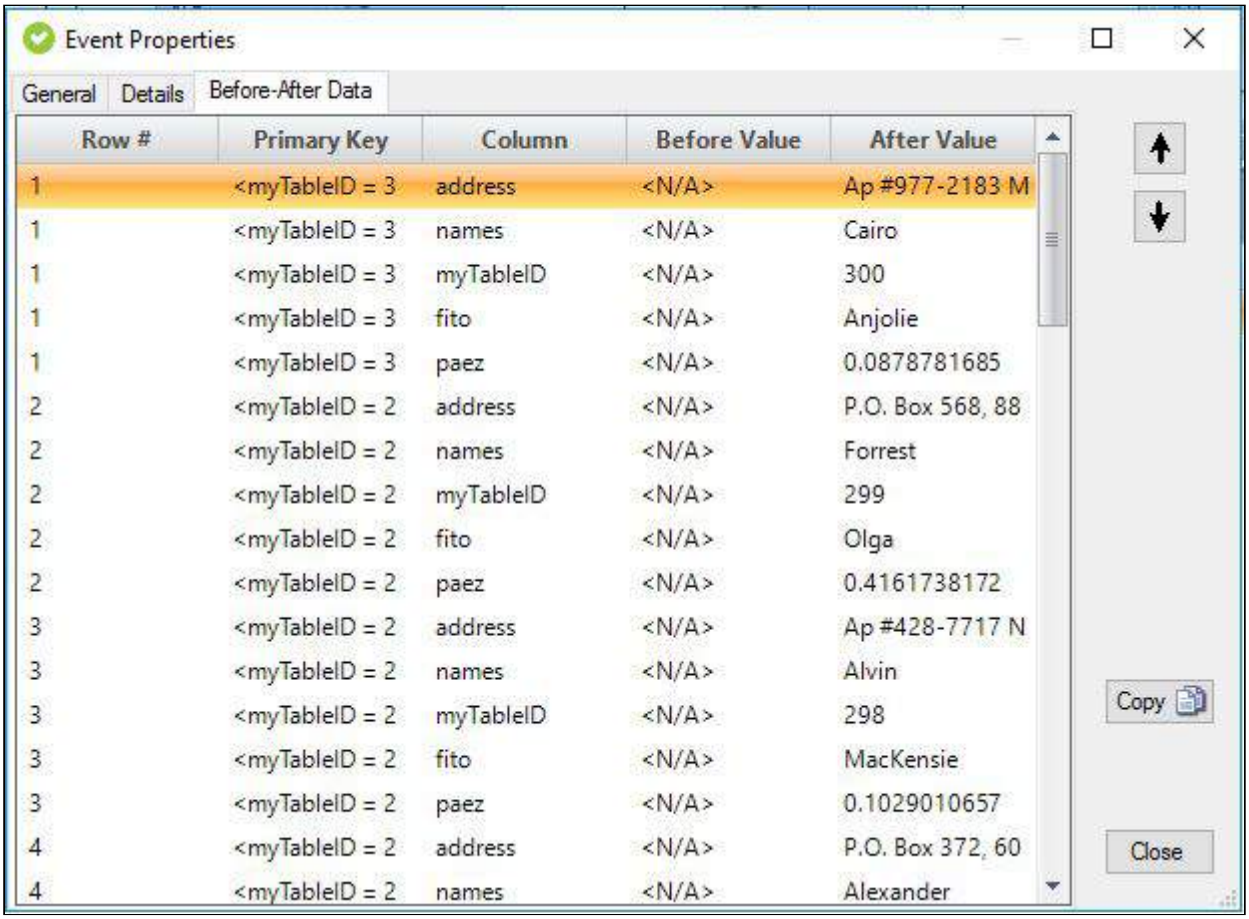
Event Properties window - Data Change tab

The Data Change tab of the Event Properties window 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 - Sensitive Columns tab

The Sensitive Column tab of the Event Properties window allows you to review the frequency on which sensitive data has been accessed.

This tab is available only if you audit SELECT statements with sensitive columns.

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

Column Name

Provides the name of the column affected by the event.

Row count

Provides the row count value for the selected column.

9.2 Report on Audit Data

IDERA 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.

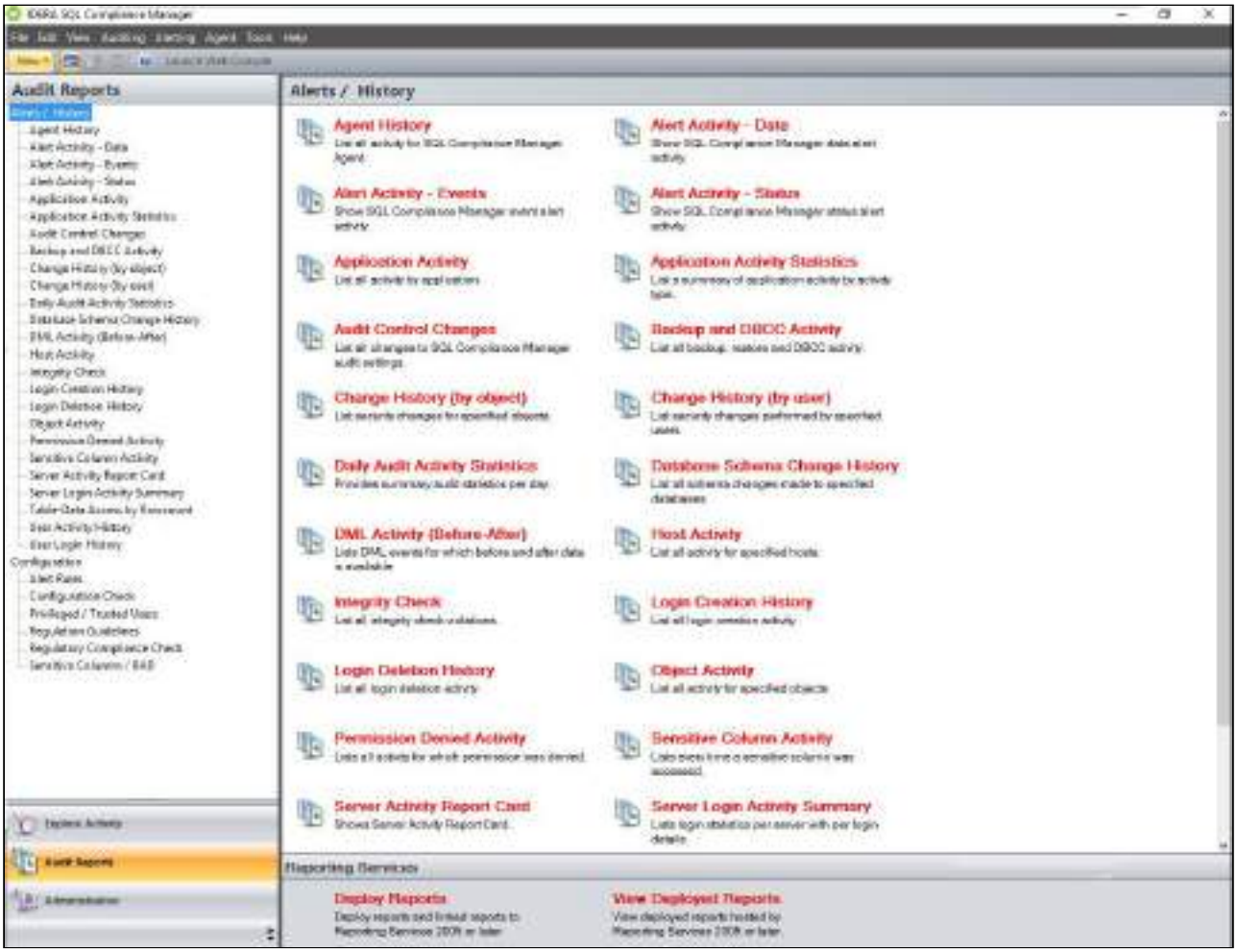
9.2.1 How reports work

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

9.2.2 Audit reports view

The Audit reports 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 IDERA 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 Compliance Manager 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 - Data
- 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

Configuration Check Report

The configuration check report lists all the configurations selected on a Server or Database. Use these reports to reconcile the differences in regards to the configurations across different servers and databases.

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 Report

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.

Privileged / Trusted Users Report

The Privileged User/Trusted User report lists trusted and privileged users of a specified server instance or database. Use this report to view the list of trusted/privileged users on specific servers and databases.

Policy Audit Reports

These reports list changes and updates applied to the SQL Compliance Manager 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 SQL Compliance Manager Agent service restarts.

- Agent History
- Alert Rules

- Audit Control Changes
- Integrity Check

Regulation Audit Reports

These reports list all the regulations and their individual guidelines applied to your servers and databases. Use the Regulation Guideline report to audit the regulatory guidelines applied to your SQL Server instance, or use the Regulation Compliance Check report to ensure that your servers and databases continue to be in compliance with the selected regulatory guidelines.

- Regulation Guideline Report
- Regulation Compliance Check Report

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
- Table/Data Access by Row count

Server Activity Report Card Report

The Server Activity Report Card report allows you to review the activity status and recent audit event history on your SQL Server instance. Use this report to display a particular server´s activity status.

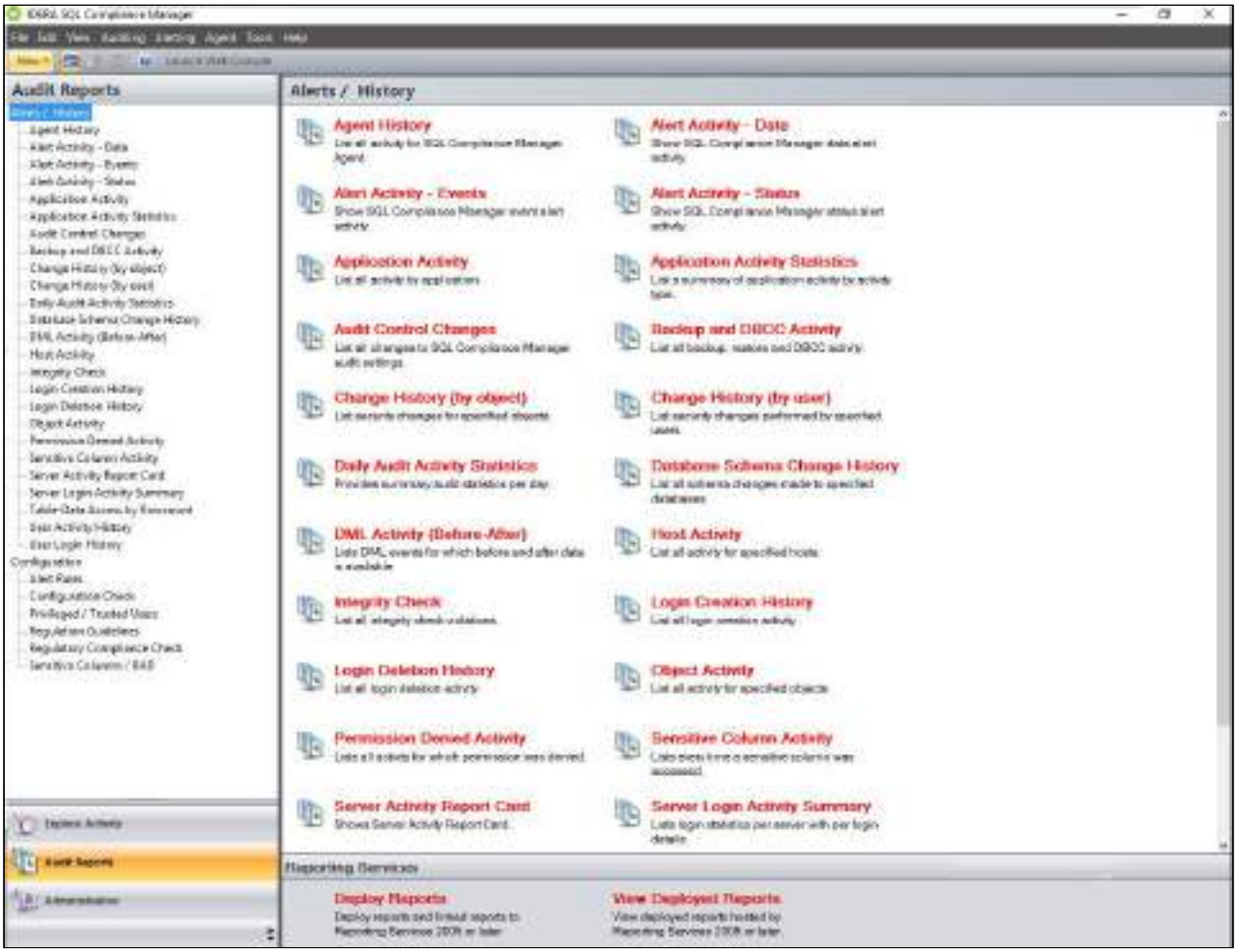
User Audit Reports

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

9.2.3 Available reports

The following report categories are included with IDERA 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.



Alerts/History Reports

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.

- Daily Audit Activity Statistics

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.

- Alert Activity - Data
- Alert Activity - Events
- Alert Activity - Status

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.

- Backup and DBCC Activity
- 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.

- Database Schema Change History

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.

- DML Activity (Before-After)

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.

- Host Activity

Policy Audit Reports

These reports list changes and updates applied to the SQL Compliance Manager 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 SQL Compliance Manager Agent service restarts.

- Agent History
- Audit Control Changes
- Integrity Check

Row Count Reports

The Row Count reports lists all information about data access. Use this report to audit the frequency in which data is accessed, identifying suspicious behavior.

- Table-Data Access by Rowcount

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

Server Activity Reports

The Server Activity Report Card report allows you to review the activity status and recent audit event history on your SQL Server instance. Use this report to display a particular server´s activity status.

- Server Activity Report Card

SELECT Audit Reports

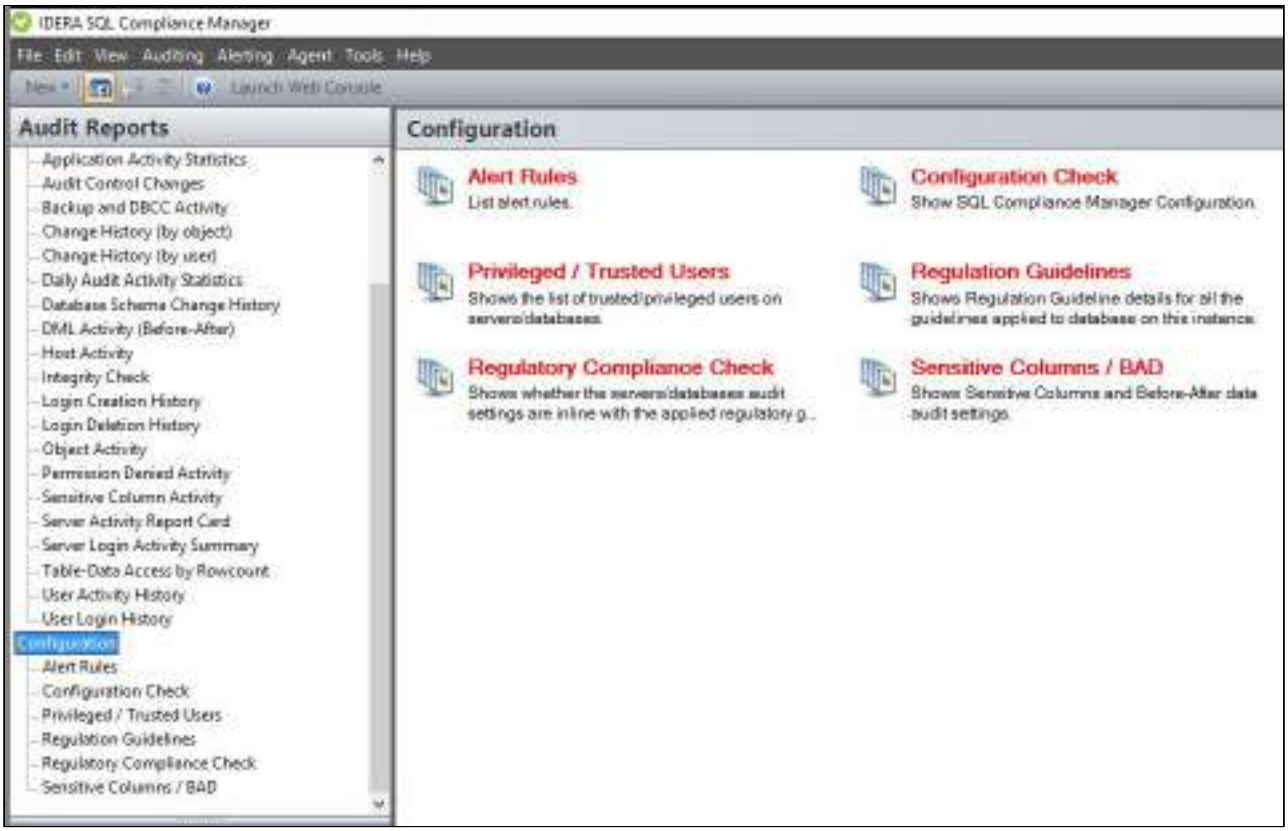
The Sensitive Column report lists all SELECT events that were initiated by applications to read specific columns that contain sensitive data. This report also includes the T-SQL statements that executed the corresponding commands. Use this report to audit columns that require high security, such as employee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

- Sensitive Column Activity

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



Configuration Reports

Alert Rules

The Alert Rules report lists the existing alert rules for your servers and databases. Use these reports to diagnose audit data integrity issues.

- Alert Rules

Configuration Check Reports

The configuration check report lists all the configurations selected on a Server or Database. Use these reports to reconcile the differences in regards to the configurations across different servers and databases.

- Configuration Check Report

Privileged/Trusted User Reports

The Privileged/Trusted Users report lists all trusted and privileged users set in each server instance and database. Use this report to monitor which Trusted and Privileged Users were set to during a snapshot in time.

- Privileged/Trusted Users

Regulation Audit Reports

These reports list all the regulations and their individual guidelines applied to your servers and databases. Use the Regulation Guideline report to audit the regulatory guidelines applied to your SQL Server instance, or use the Regulation Compliance Check report to ensure that your servers and databases continue to be in compliance with the selected regulatory guidelines.

- Regulation Guideline Report
- Regulation Compliance Check Report

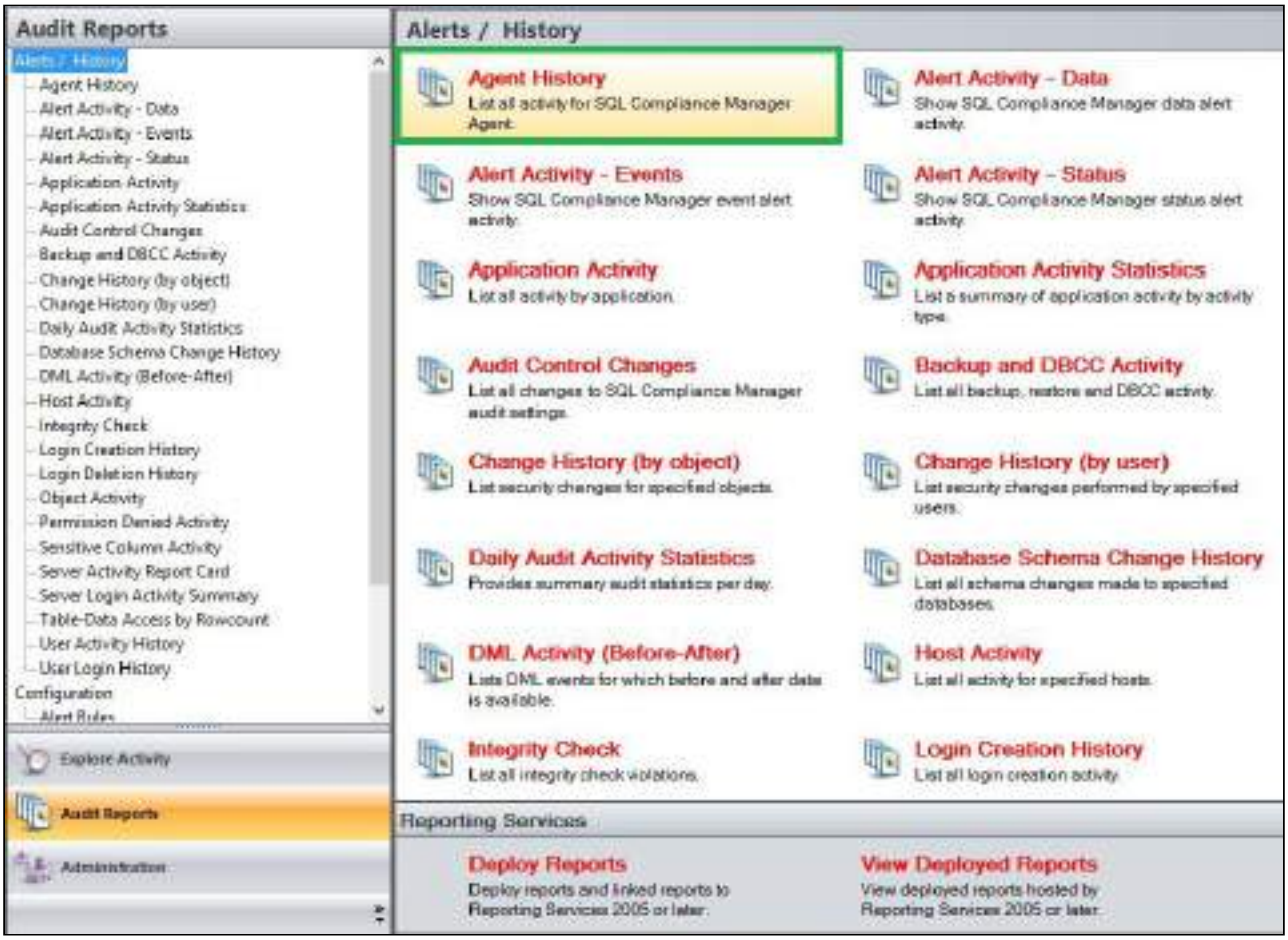
Sensitive Column/BAD Reports

The Sensitive Column/BAD report lists Sensitive Column and Before-After data audit settings applied to your servers and databases. Use this report to monitor what Sensitive Columns and Before-After data auditing were set to during a snapshot in time.

- Sensitive Column/BAD

Agent History Report

The Agent History Report lists the changes and updates applied to the SQL Compliance Manager Agent deployed on a specific SQL Server. Use this report to track agent configuration changes as well as agent activities, such as SQL Compliance Manager Agent service restarts.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Agent

Allows you to type the name of one or more agents on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Time

The Time column displays the date and time when the event was captured.

Agent

The Agent column displays the name of the SQL Server Agent.

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Event

The Event column displays a description of the event captured.

Alert Activity - Data Report

The Alert Activity - Data Report shows SQL Compliance Manager data alert activity in your monitored environment. Use this report to identify and investigate data manipulation on specific databases, tables, or columns.

A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Table Name

Allows you to select or type the name of one or more table names on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Alert Level

Choose to filter alerts by their different levels; Severe, High, Medium, or Low.

Run Report

Click this button to Run the report.

Default columns

Time

The Time column displays the date and time when the event was captured.

Alert Level

The Alert Level column displays the level the alert is configured to.

Event

The Event column provides the name of the audited event that triggered this alert.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Table Name

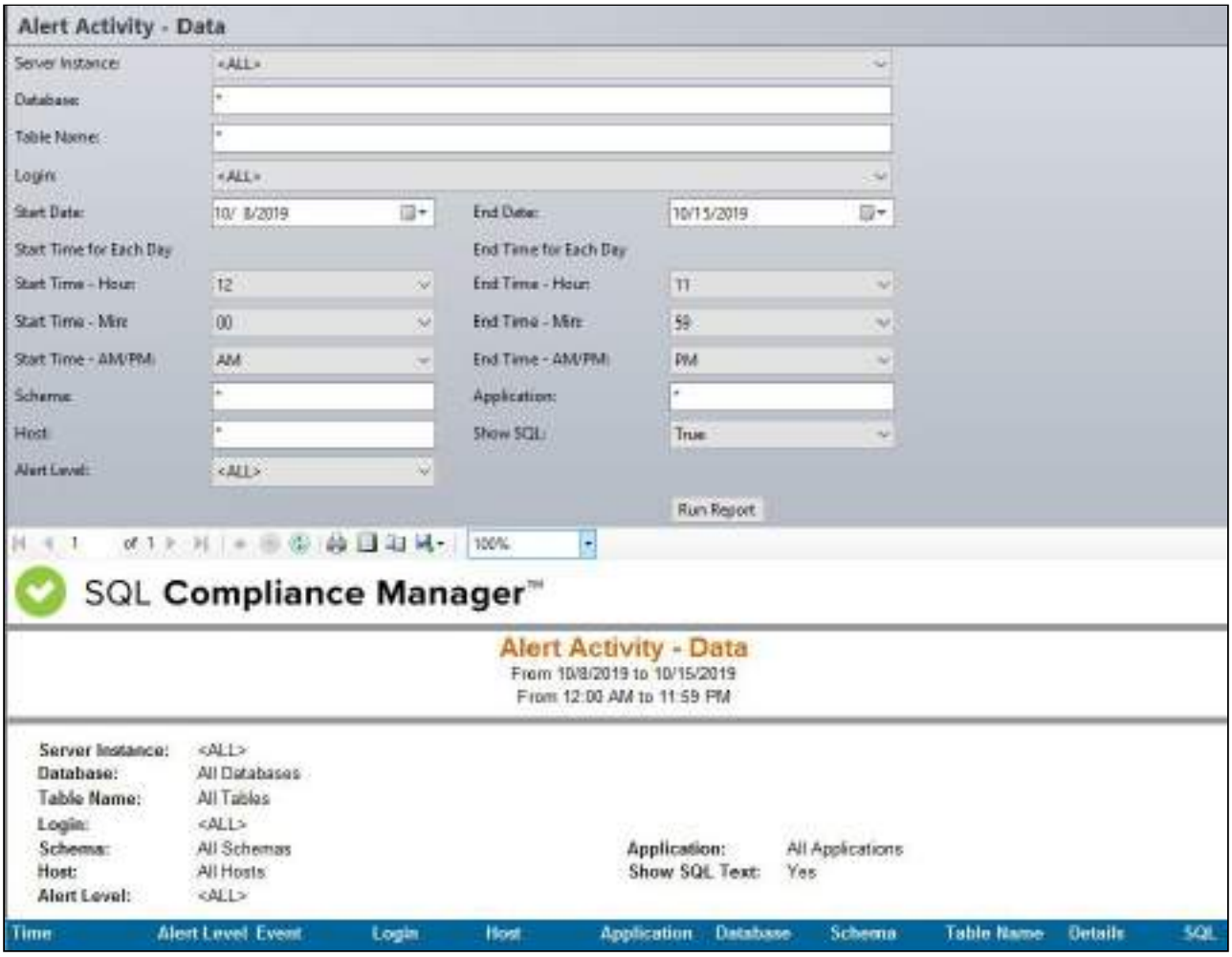
The Table Name column displays the name of the table were the event was captured.

Details

The Details column provides the first line of the alert message associated with this alert.

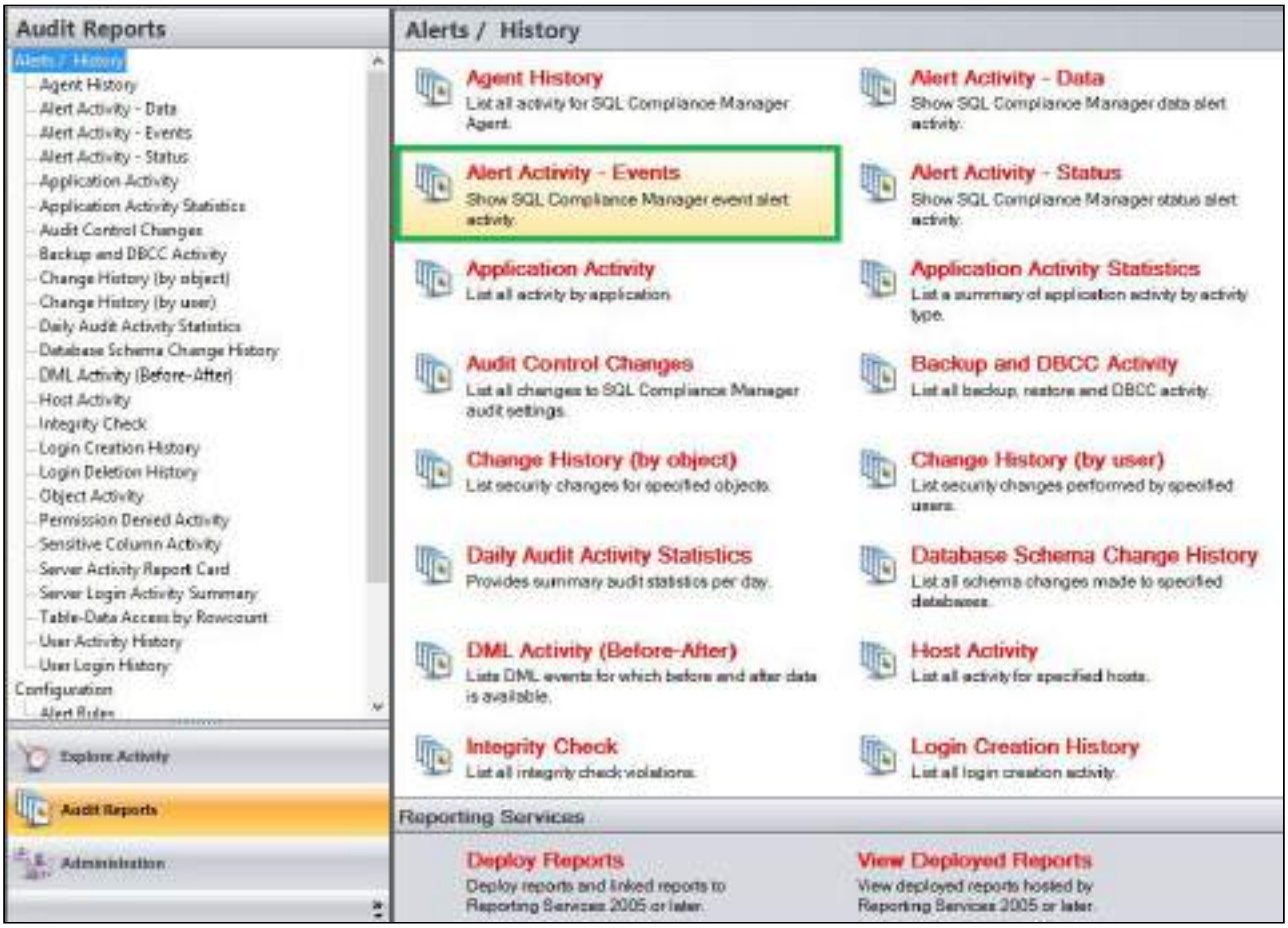
SQL

The SQL column when set to True, provides the SQL Statement for the captured event.



Alert Activity - Events Report

The Alert Activity - Events Report shows the SQL Compliance Manager event alert activity in your monitored environment. Use this report to identify and investigate suspicious activity on specific databases, users, or instances.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Alert Level

Choose to filter alerts by their different levels; Severe, High, Medium, or Low.

Run Report

Click this button to Run the report.

Default columns

Time

The Time column displays the date and time when the event was captured.

Alert Level

The Alert Level column displays the level the alert is configured to.

Event

The Event column provides the name of the audited event that triggered this alert.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

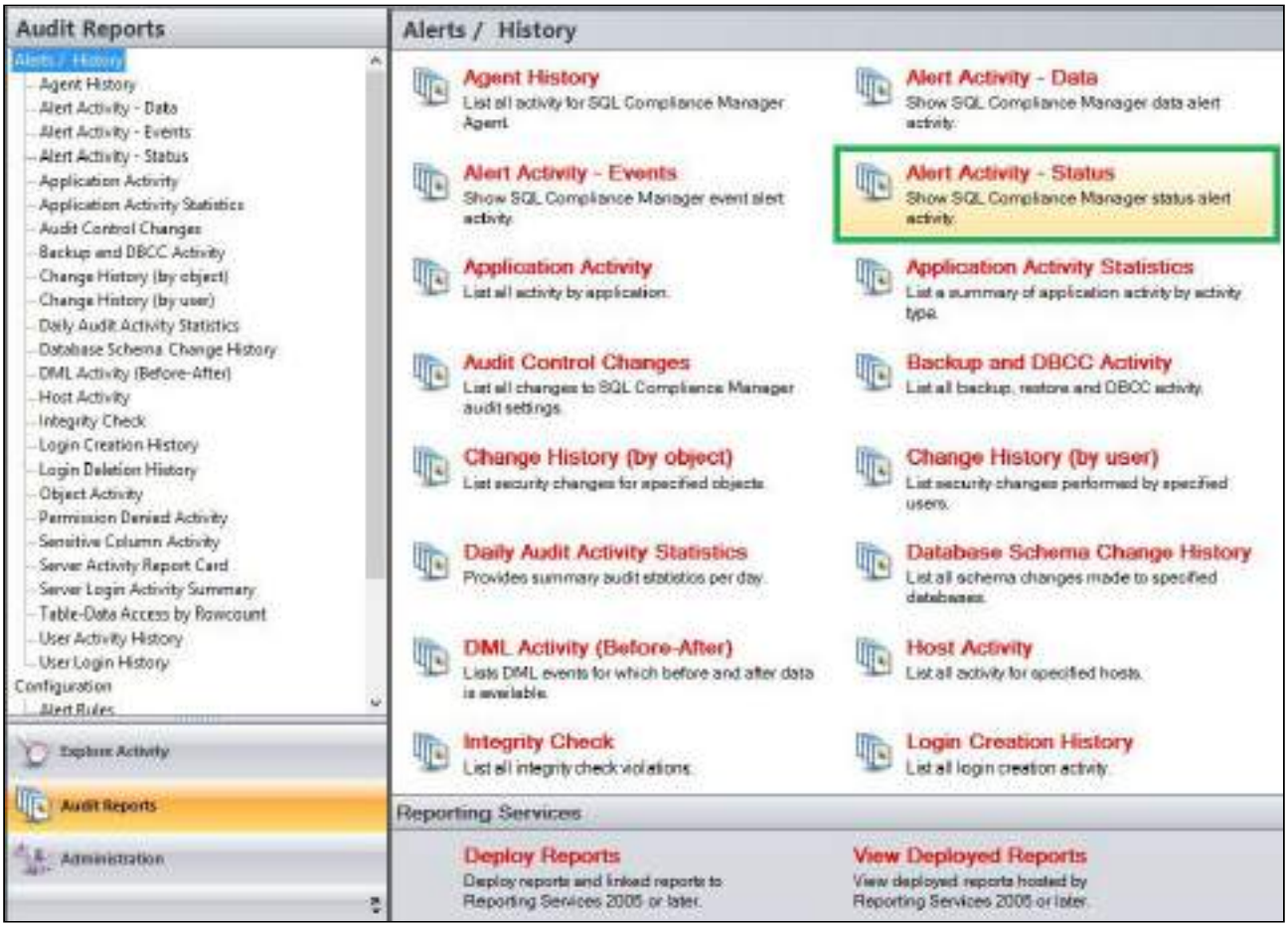
The Details column provides the first line of the alert message associated with this alert.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Alert Activity - Status Report

The Alert Activity - Status Report shows SQL Compliance Manager status alert activity in your monitored environment. Use this report to identify and investigate possible issues with IDERA SQL Compliance Manager operations, such as deployed agents that may have stopped running.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Alert Level

Choose to filter alerts by their different levels; Severe, High, Medium, or Low.

Run Report

Click this button to Run the report.

Default columns

Time

The Time column displays the date and time when the event was captured.

Alert Level

The Alert Level column displays the level the alert is configured to.

Source Rule

The Source Rule column provides the name of the alert rule that generated this alert.

Rule Name

The Rule Name column displays the name of the alert rule.

Computer Name

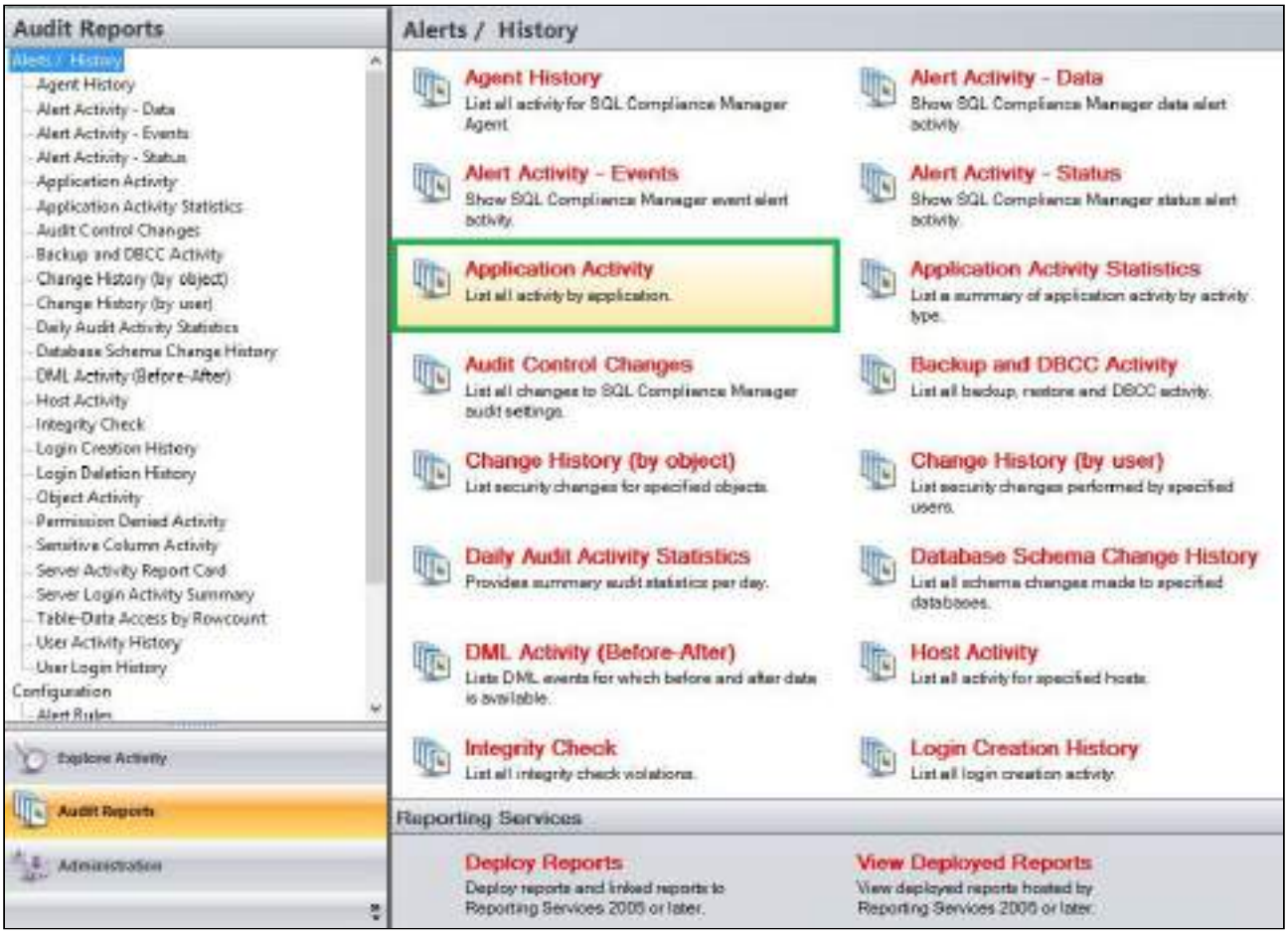
The Computer Name column displays the name of the local computer.

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Application Activity Report

The Application Activity Report lists all activity details, such as login, event, and time of activity, performed per application and database. Use this report to audit activity across multiple applications and databases.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select a category type from the drop down menu to filter the report on.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default Columns

Application

The Application column displays the name of the application used to capture the event.

Host

The Host column displays the name of the host.

Login

The Login column displays the login name of the user who performed the event.

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column provides the name of the audited event that triggered this alert.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Time

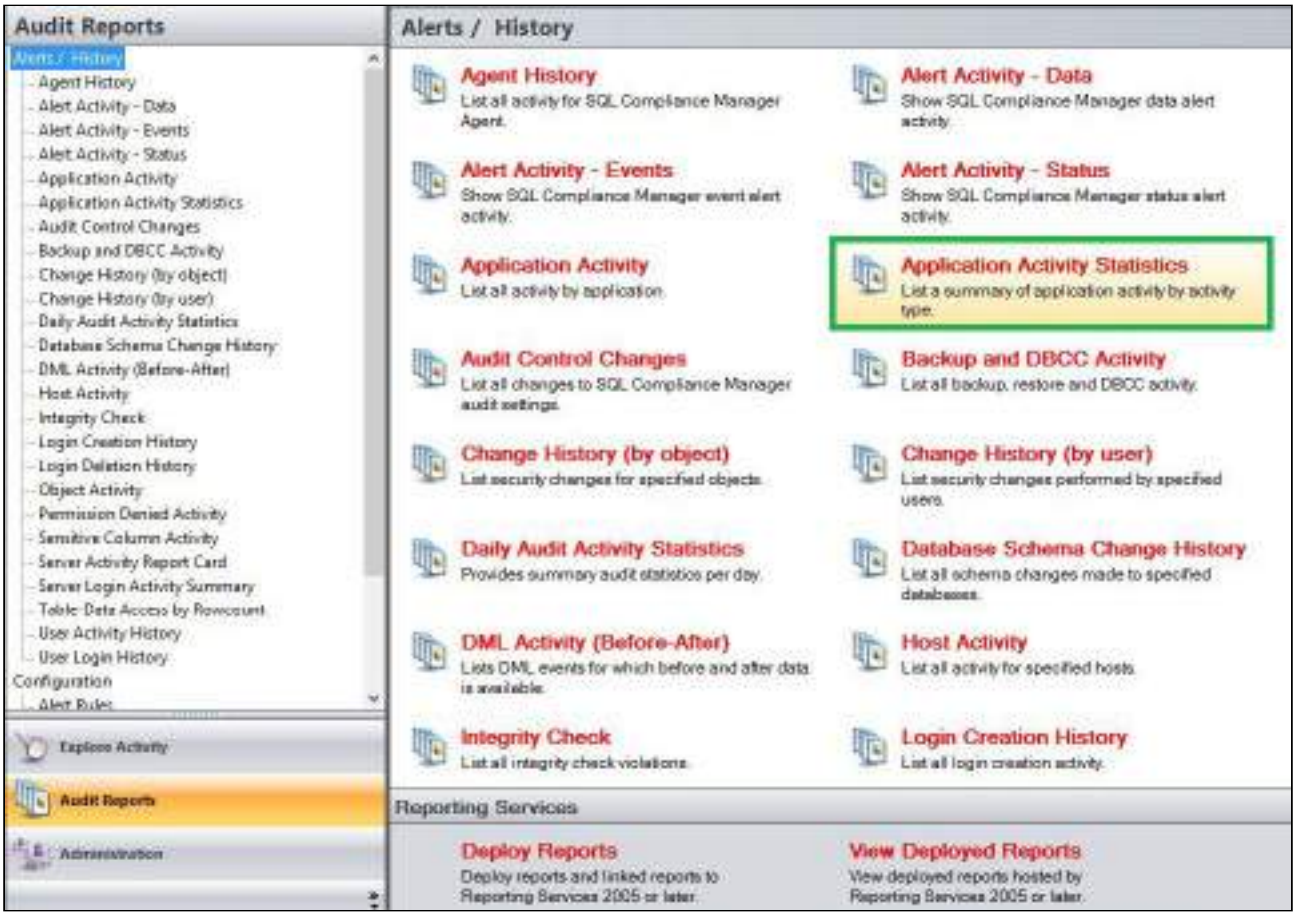
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Application Activity Statistics Report

The Application Activity Statistics Report lists a summary of application activity by activity type. Use this report to audit activity across multiple applications and databases.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Category

Allows you to select the category type on which you want to report.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

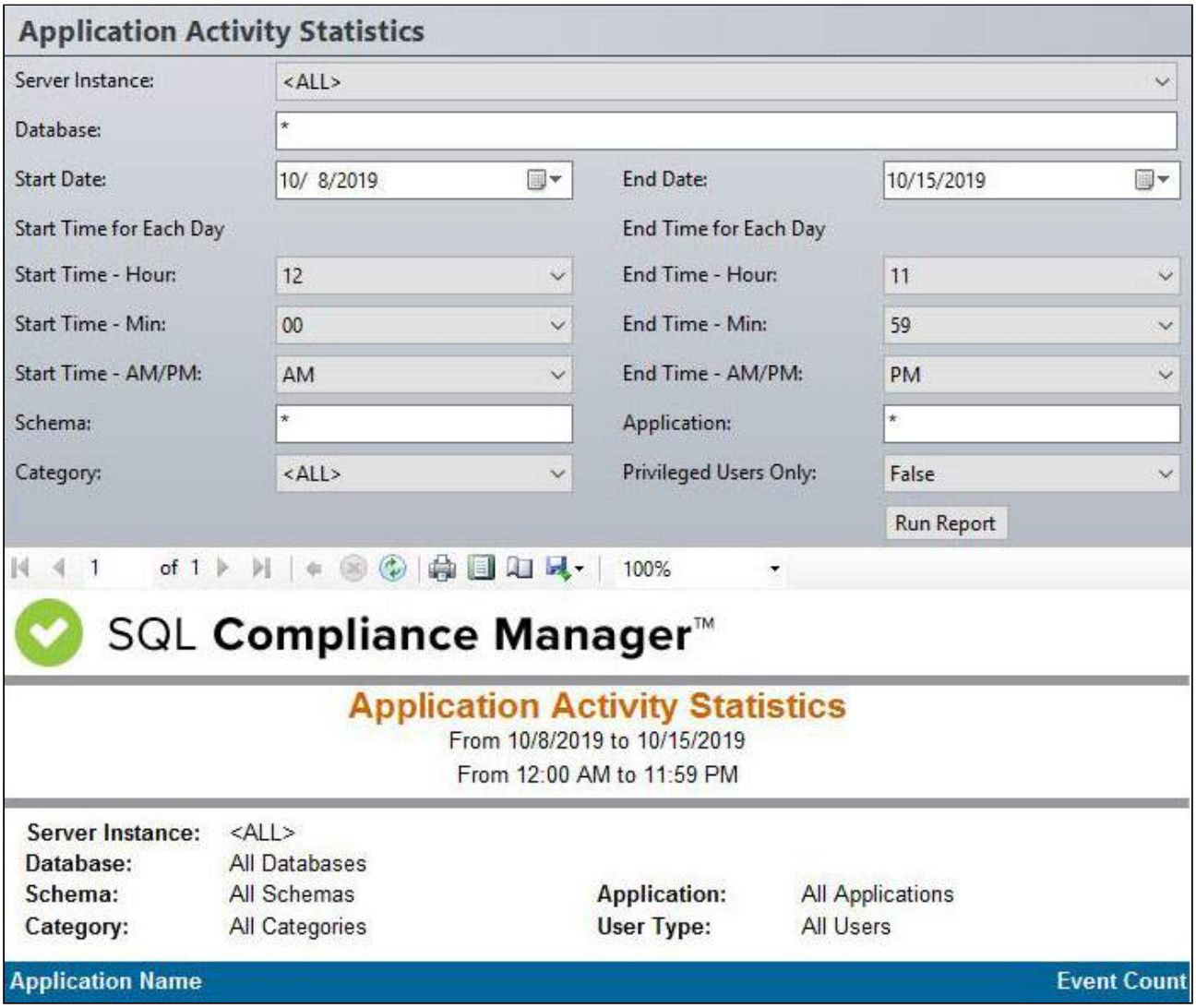
Default columns

Application Name

The Application Name column provides the name of the application where events were captured.

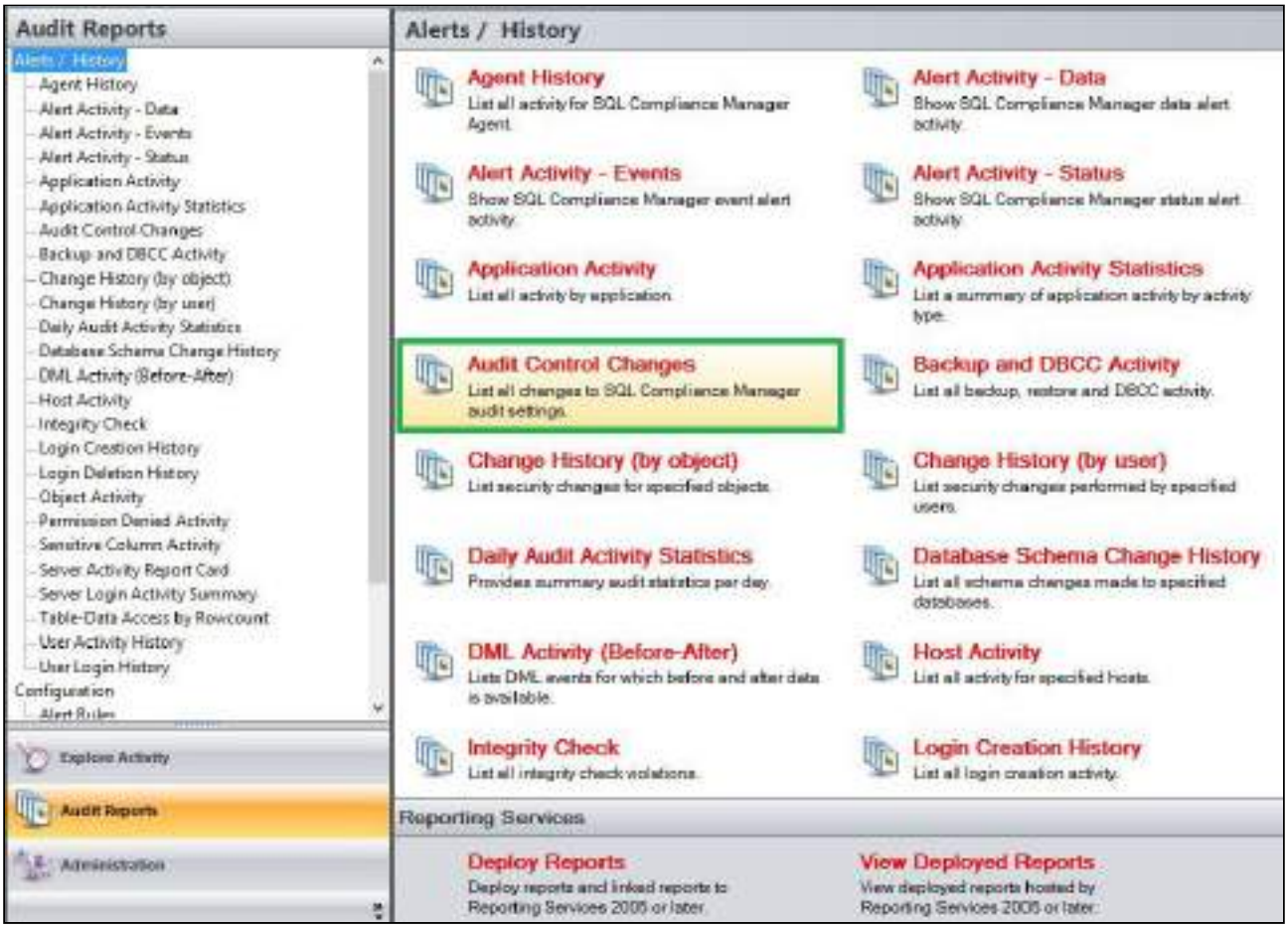
Event Count

The Event Count column show the number of events captured by each application.



Audit Control Changes Report

The Audit Control Changes Report lists all changes and updates to SQL Compliance Manager audit settings. Use this report to diagnose audit data integrity issues and control all changes to the audit settings in your environment.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Time

The Time column displays the date and time when the event was captured.

Event

The Event column indicates the type of event captured.

Login

The Login column displays the login name of the user who performed the event.

Server Instance

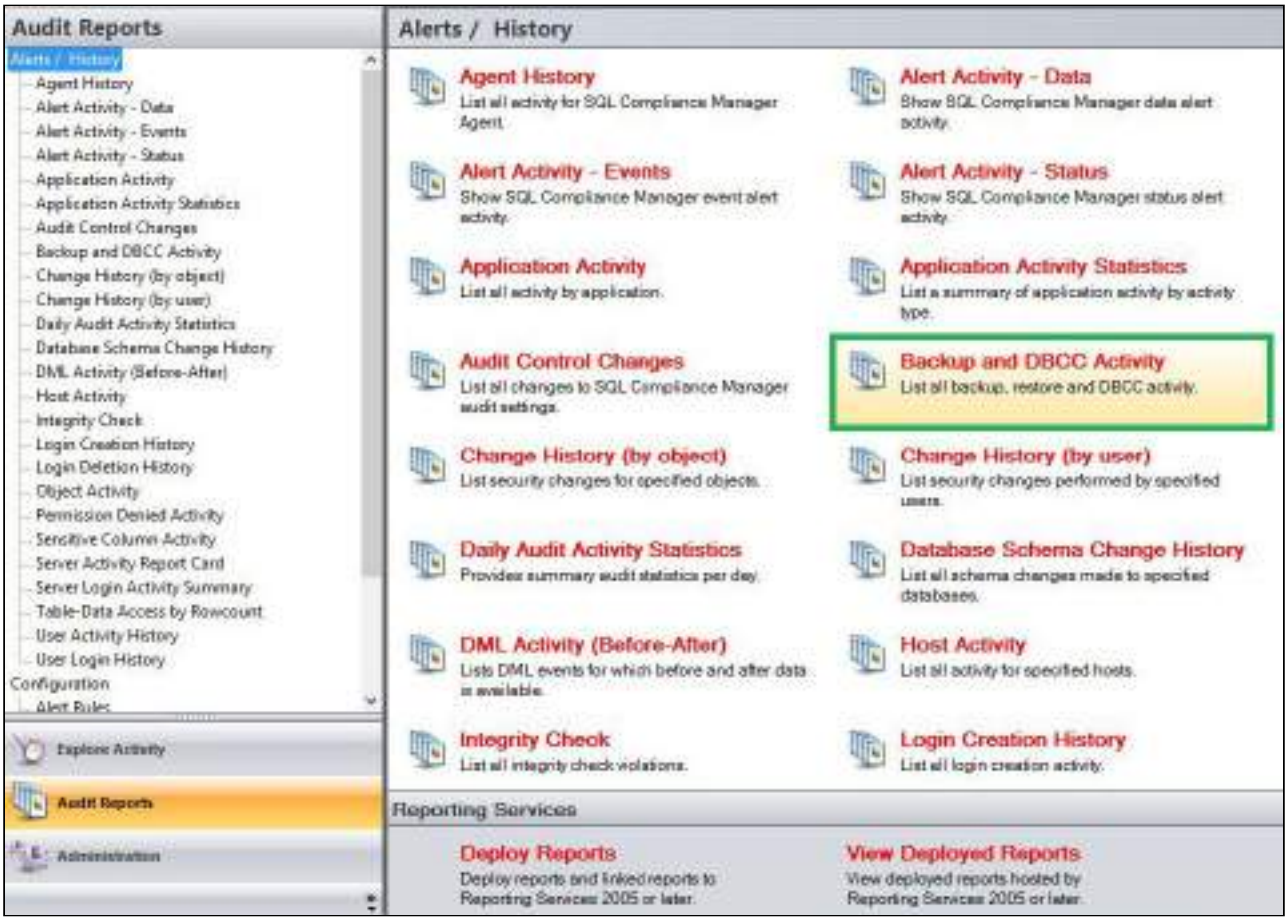
The Server Instance column displays the name of the Instance Server where the event was captured.

Description

The Description column displays a description of the event captured.

Backup and DBCC Activity Report

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



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types

Run Report

Click this button to Run the report.

Default columns

Event

The Event column displays a description of the event captured.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object for the event captured.

Time

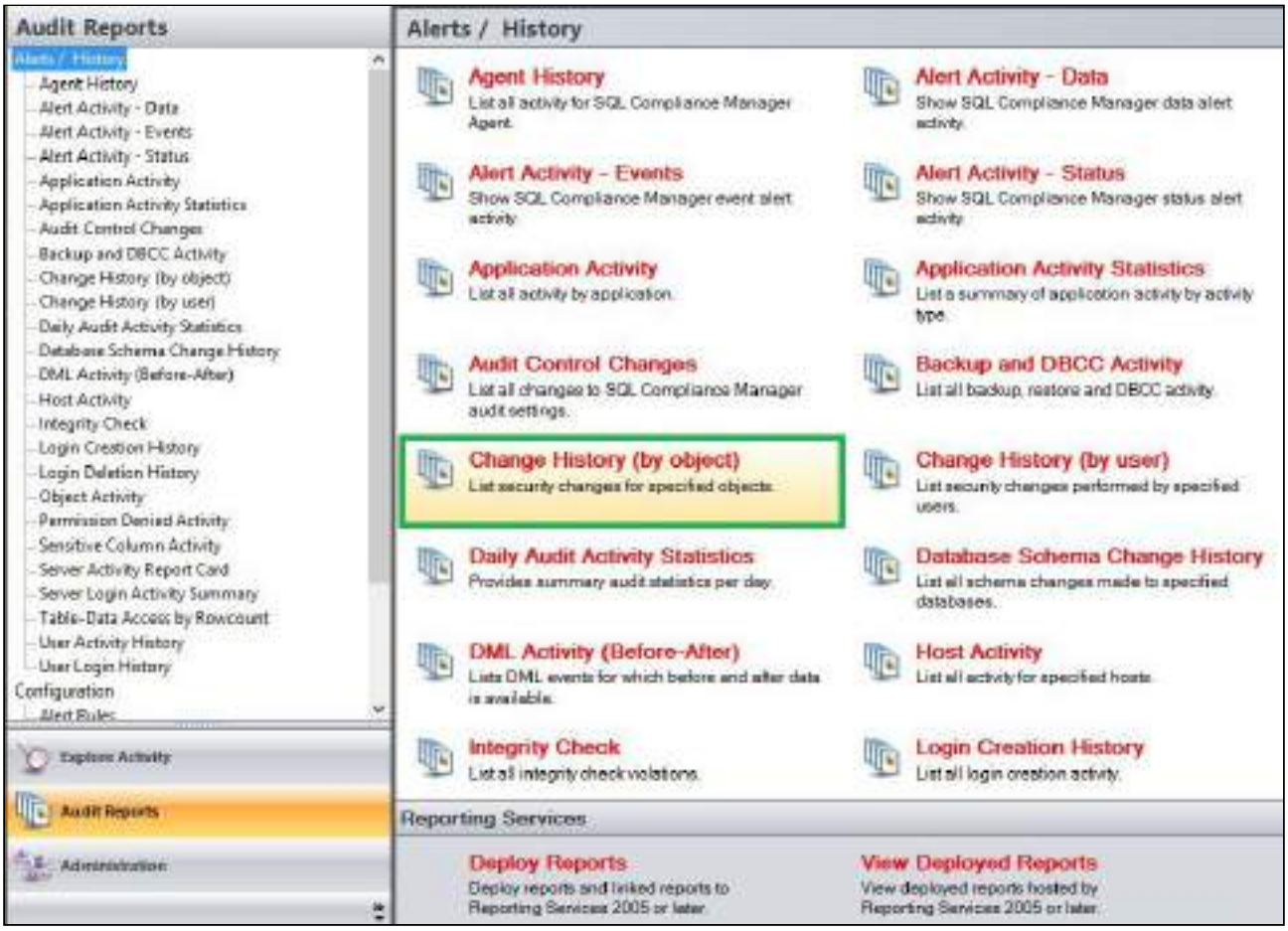
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Change History (by Object) Report

The Change History by Object Report lists all security changes for specified objects. Use this report to audit your SQL Server security settings and identify any misconduct.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column provides a description of the event captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object for the event captured.

Details

The Details column provides details of the captured event.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

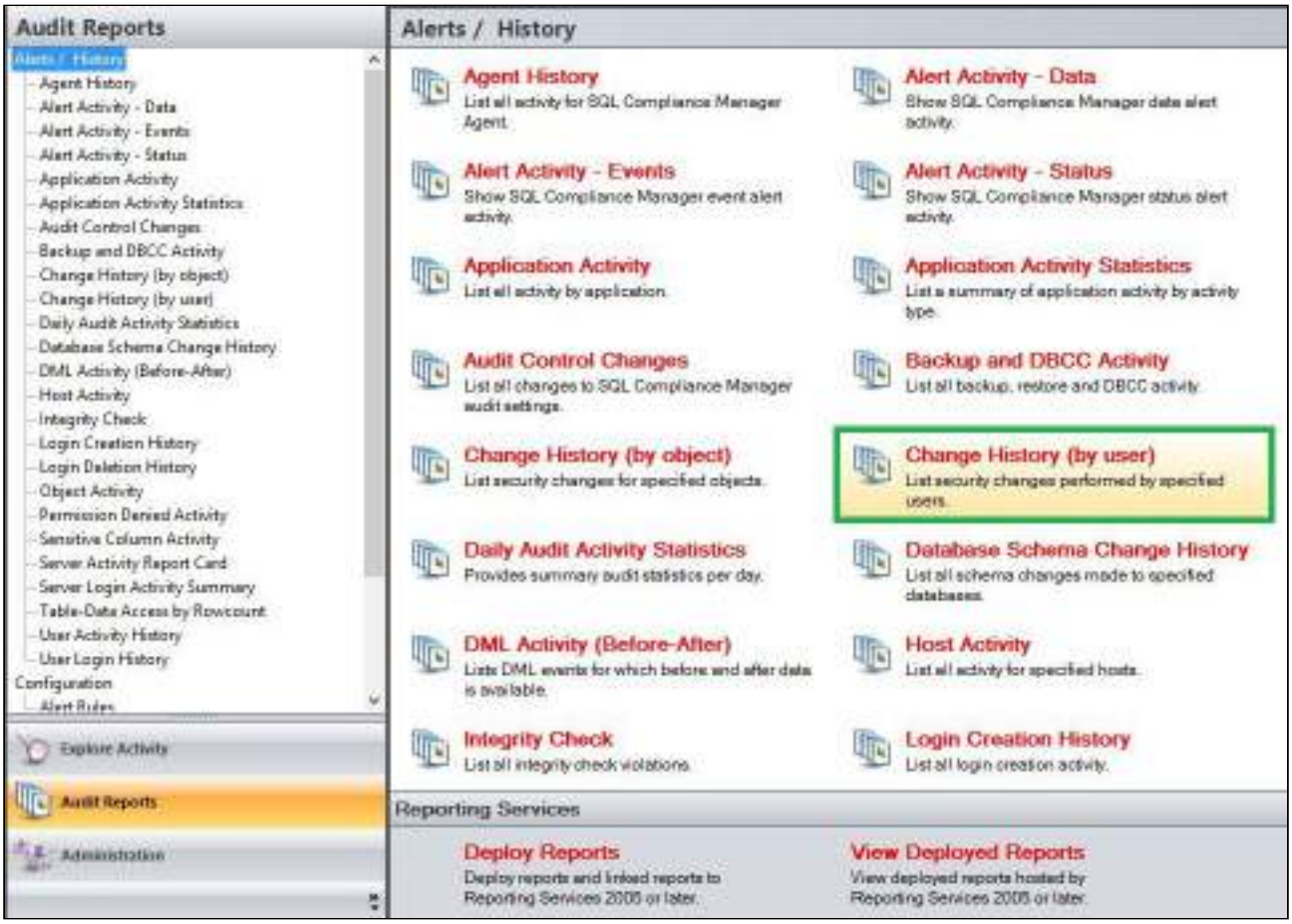
The Application column displays the name of the application used to capture the event.

Time

The Time column displays the date and time when the event was captured.

Change History (by User) Report

The Change History by User Report lists all security changes performed by specified users. Use this report to audit your SQL Server security settings and identify any misconduct.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column displays a description of the event captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object for the event captured.

Details

The Details column provides details of the captured event.

Login

The Login column displays the login name of the user who performed the event.

Host

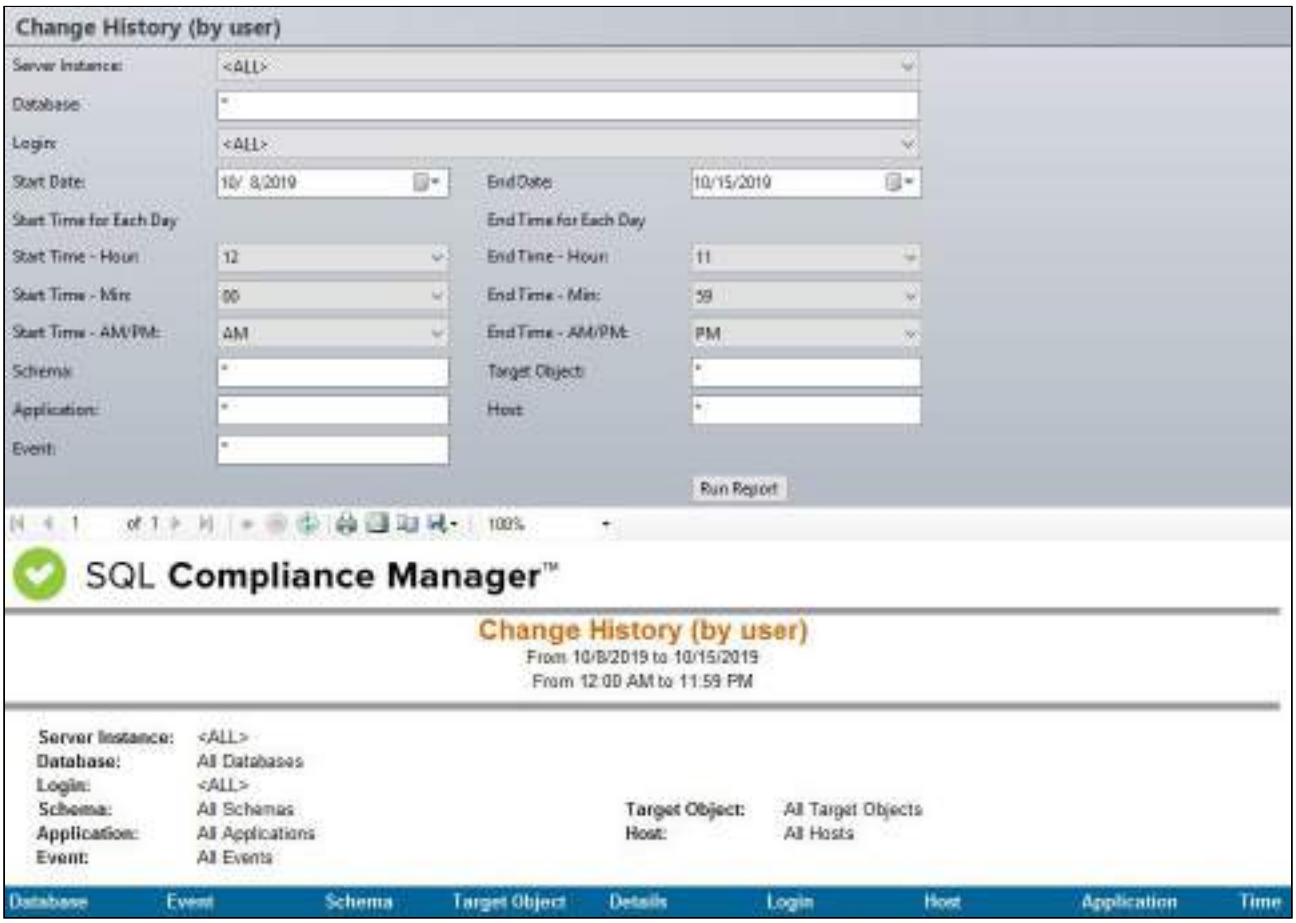
The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

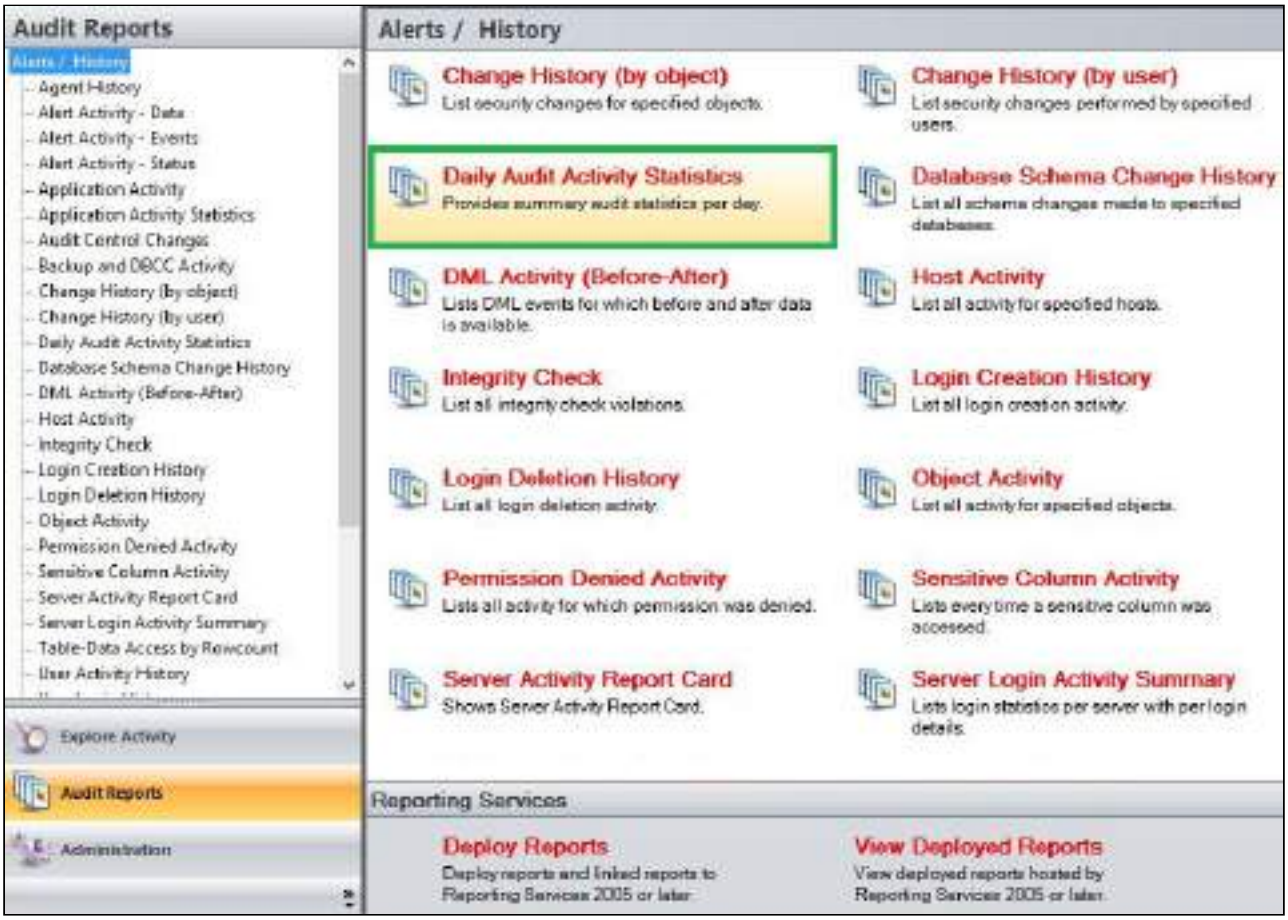
Time

The Time column displays the date and time when the event was captured.



Daily Audit Activity Statistics Report

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.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

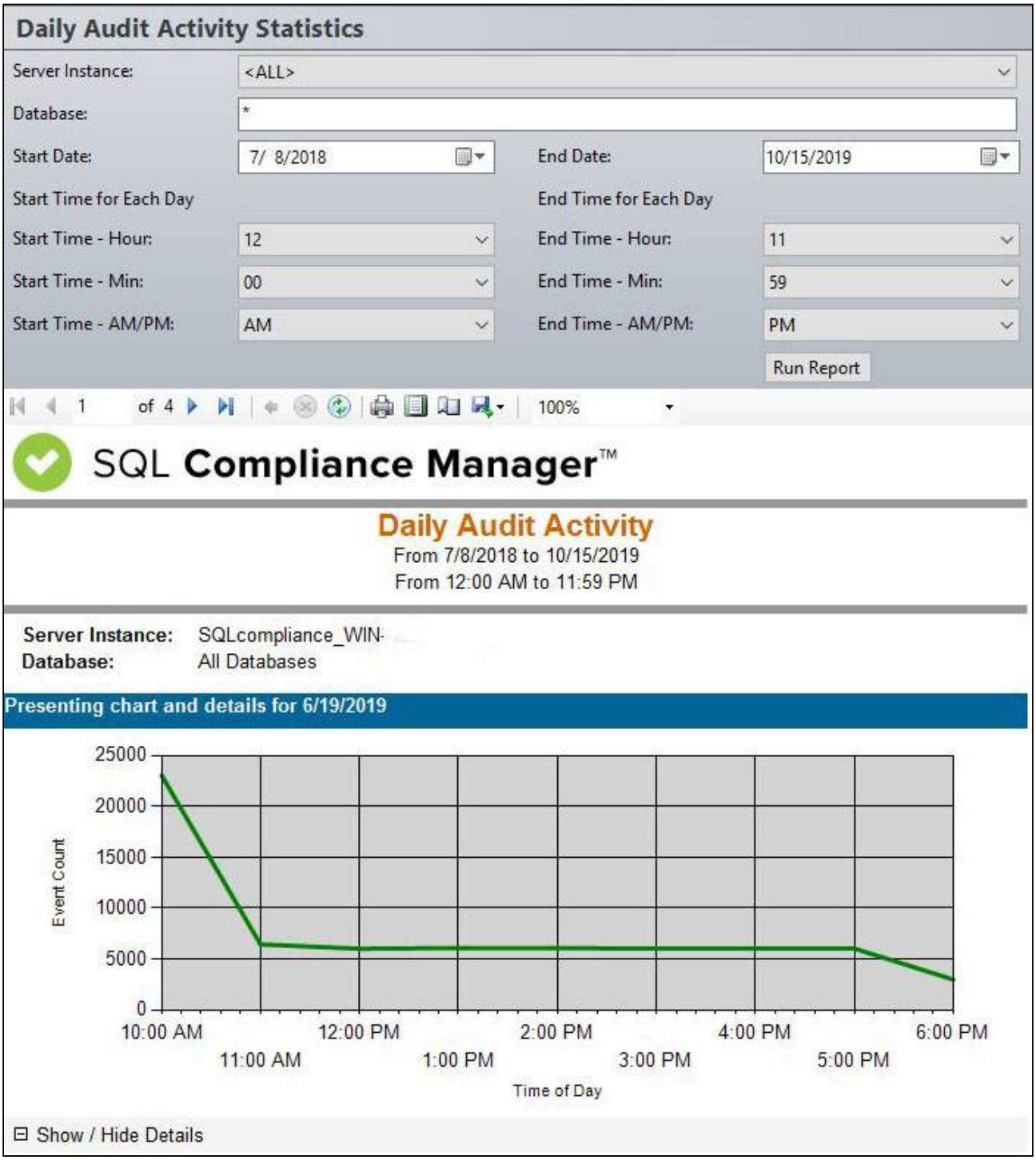
Run Report

Click this button to Run the report.

Default columns

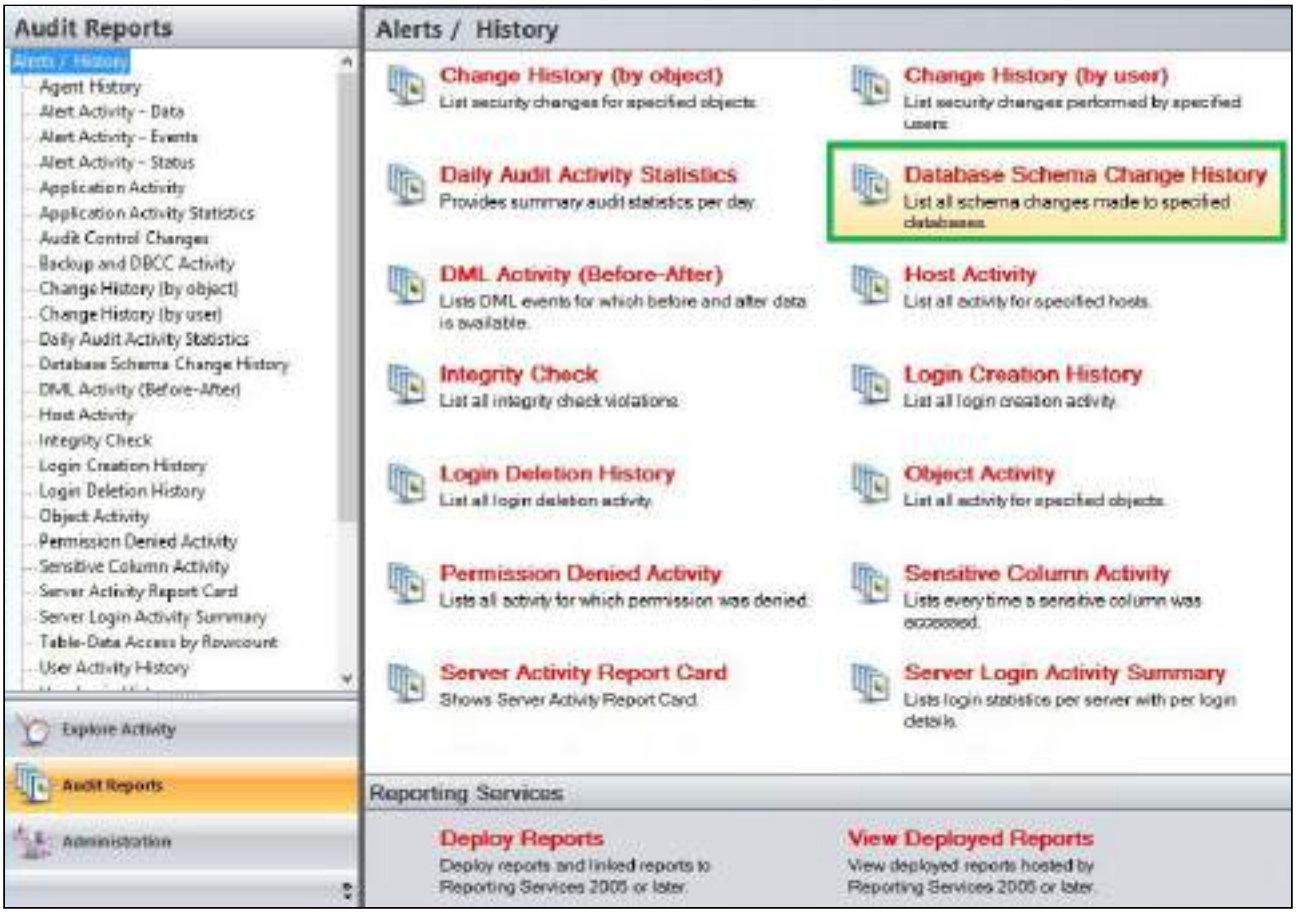
Chart and details

Presents the daily audit activity statistics data in a graph along with details.



Database Schema Change History Report

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



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column displays a description of the event captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Time

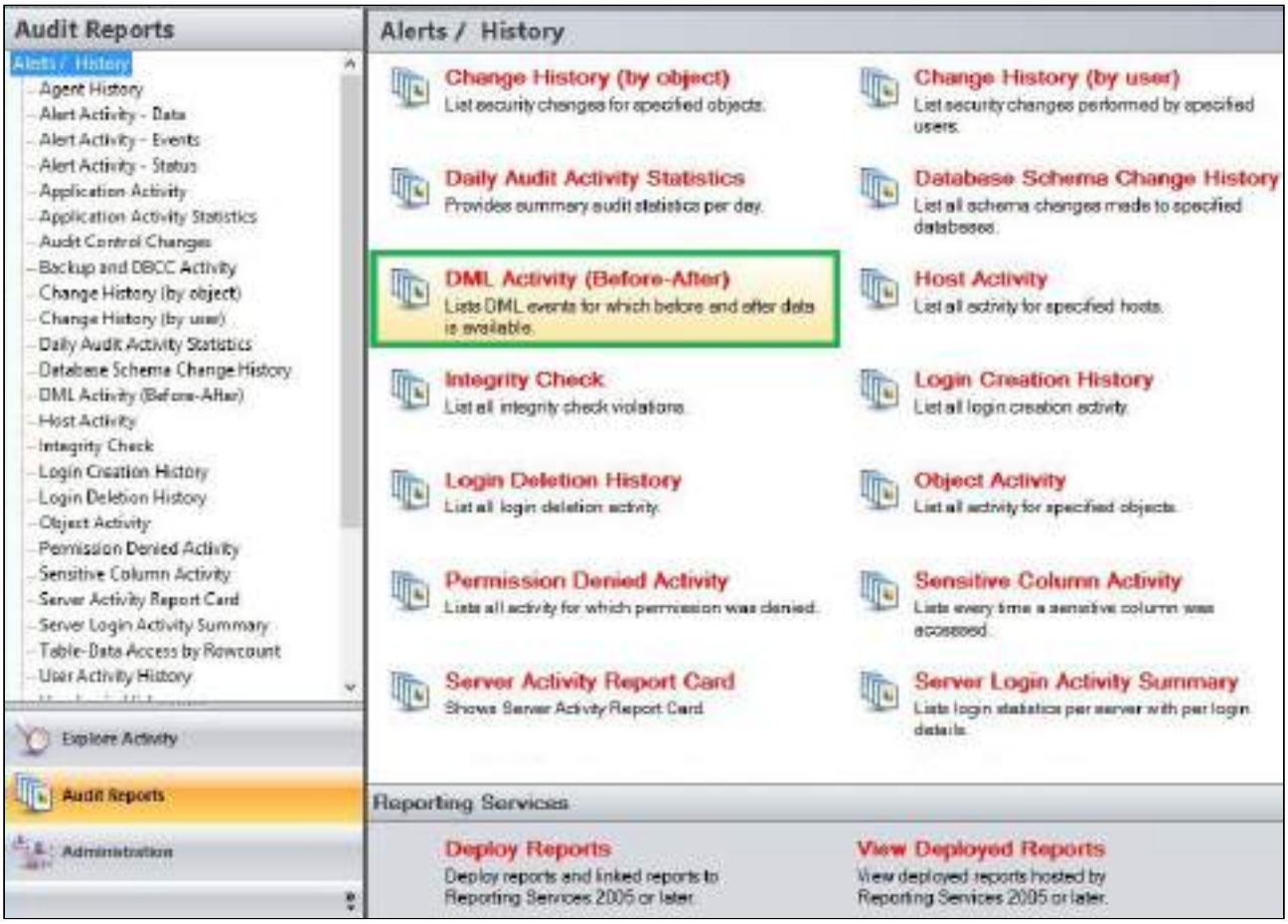
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

DML Activity (Before-After) Report

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.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Table Name

Allows you to select or type the name of one or more table names on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Column Name

Allows you to type the column names of one or more columns on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Primary Key

Allows you to type the name of one or more primary keys on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Event

The Event column displays a description of the event captured.

Time

The Time column displays the date and time when the event was captured.

Login

The Login column displays the login name of the user who performed the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Table

The Table column displays the name of the table where the event was captured.

Column

The Column column displays the name of the column where the event was captured.

Before

The Before column displays the value stored before change.

After

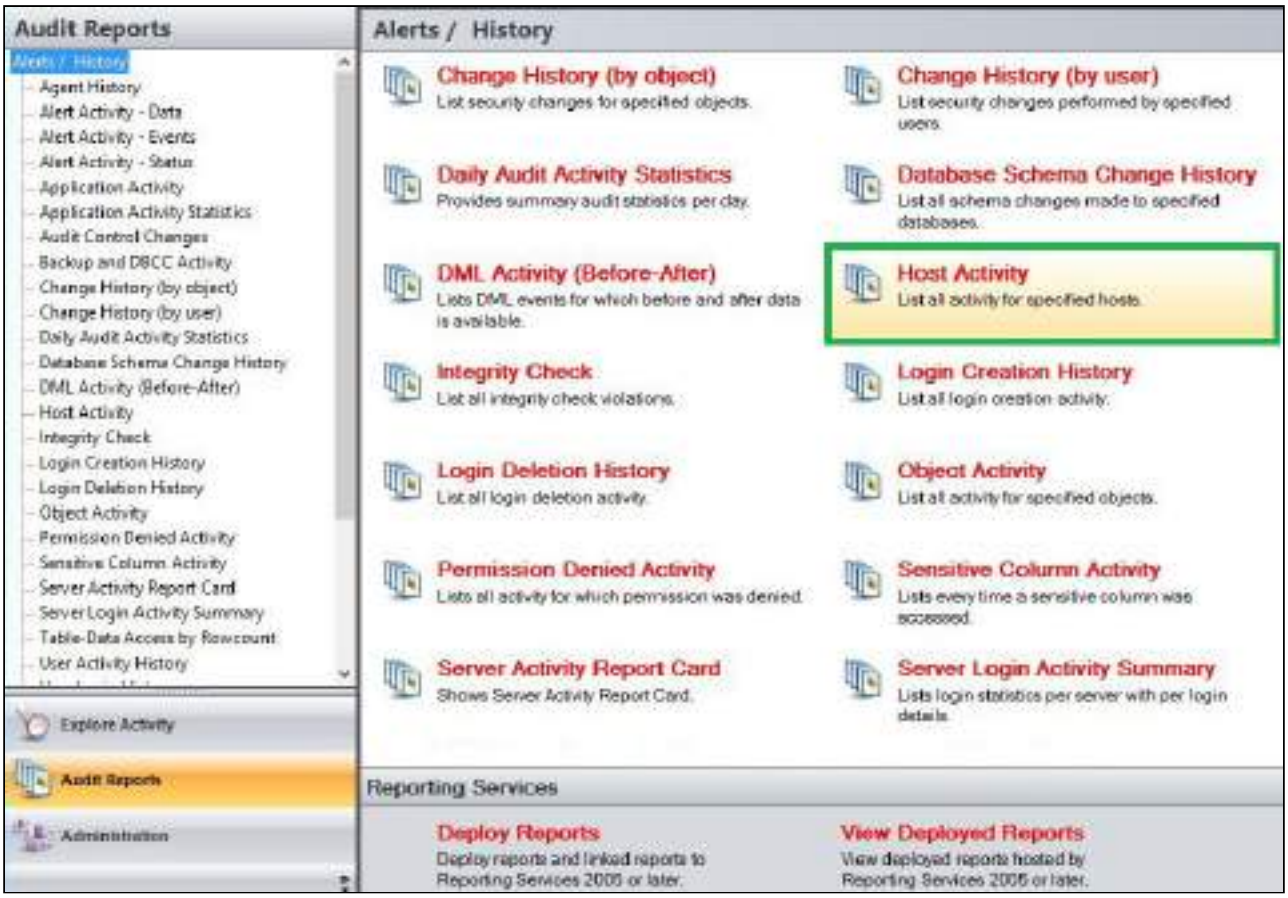
The After column displays the value stored after change.

Key

The Key column displays the primary key description.

Host Activity Report

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.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select from a category type to filter on from the drop down menu.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Host

The Host column displays the name of the host.

Login

The Login column displays the login name of the user who performed the event.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column indicates the type of event captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Time

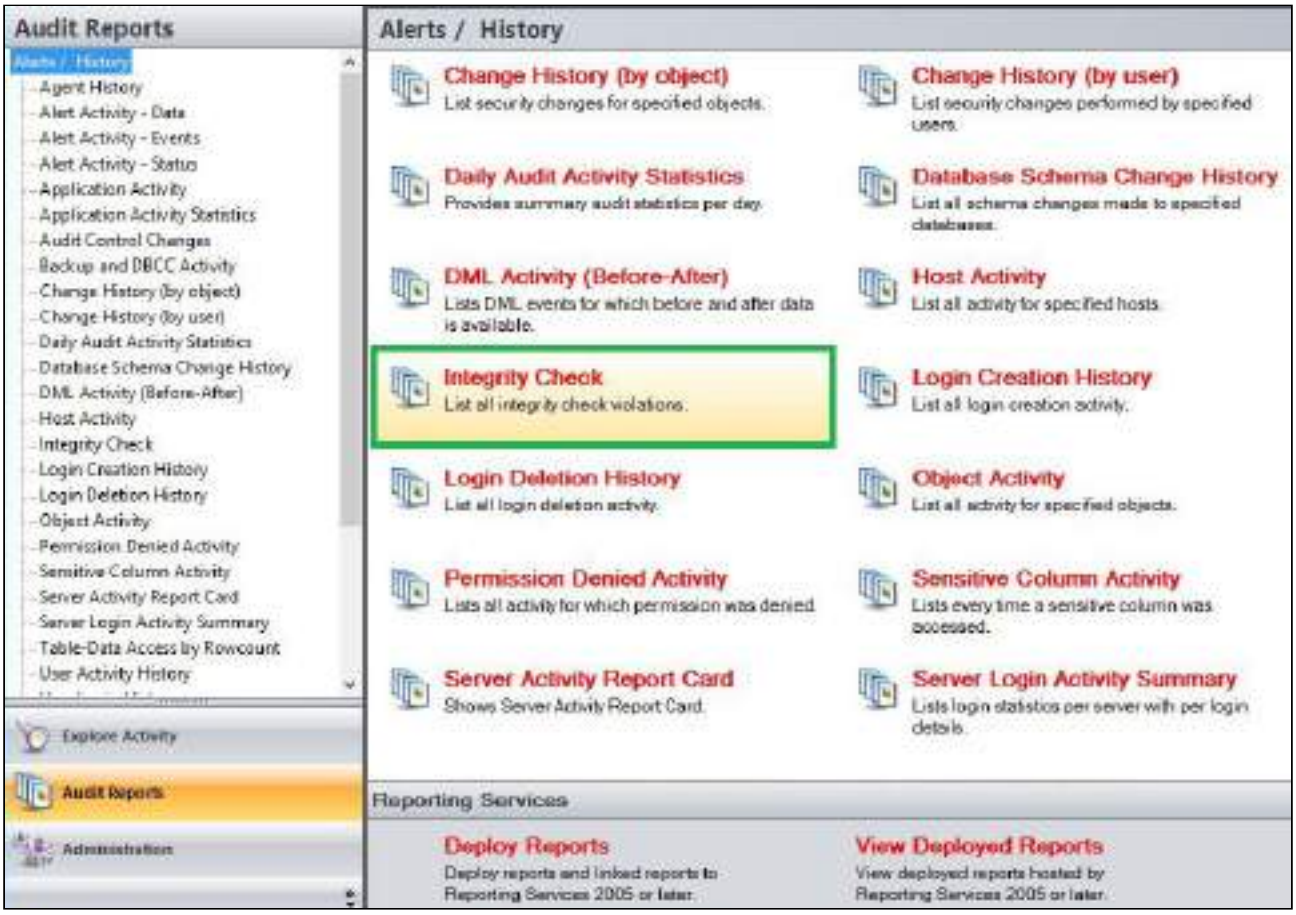
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Integrity Check Report

The Integrity Check Report lists changes and updates applied to the SQL Compliance Manager Agent deployed on a specific SQL Server, and any integrity violations in your audit data. Use this report to diagnose audit data integrity issues.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Run Report

Click this button to Run the report.

Default columns

Event

The Event column indicates the type of event captured.

Host

The Host column displays the name of the host.

Login

The Login column displays the login name of the user who performed the event.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Time

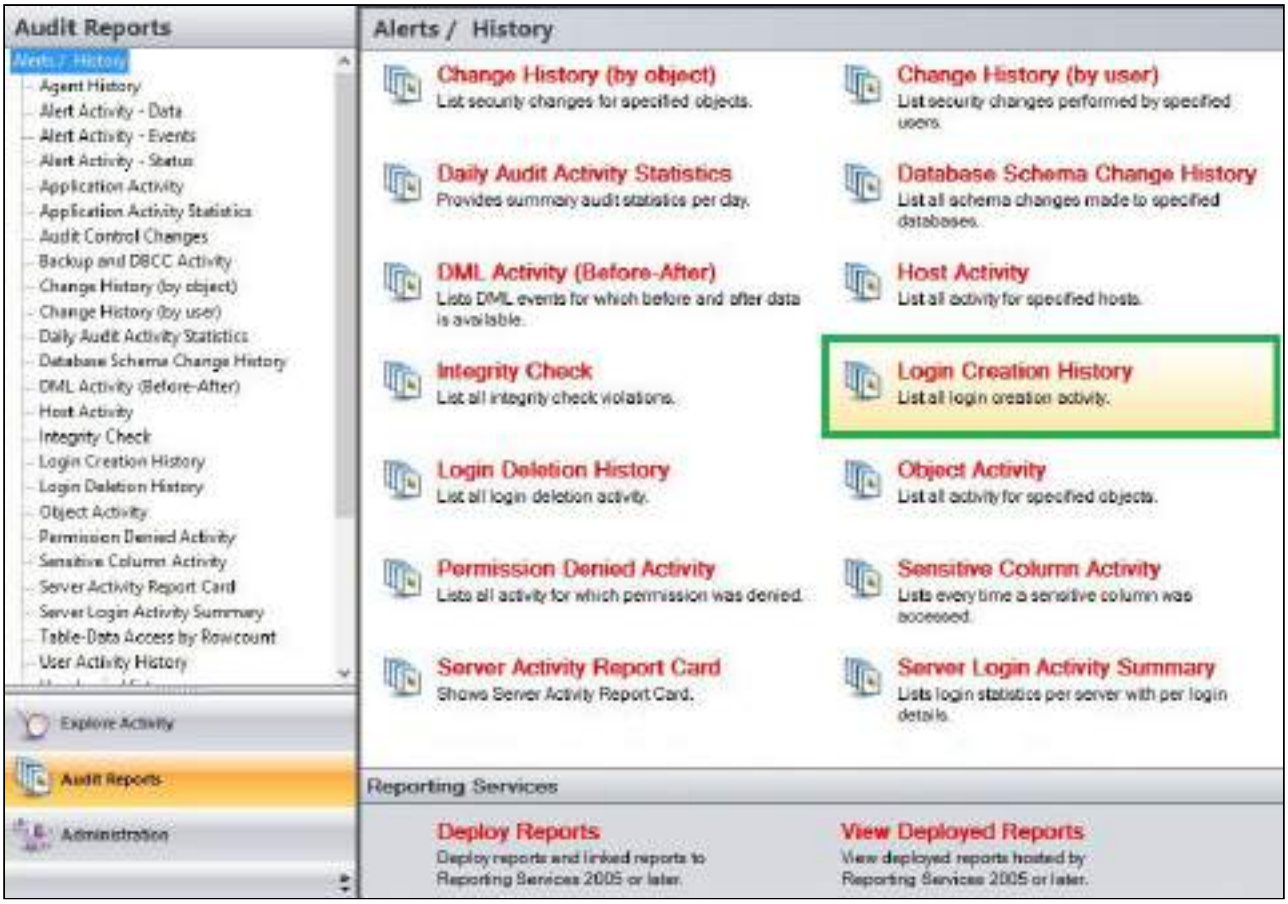
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Login Creation History Report

The Login Creation History Report provides the history of login creation activity. Use this report to audit user behavior and login management.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Created Login

The Created Login column displays the name of the login created.

Login

The Login column displays the login name of the user who performed the event.

Host

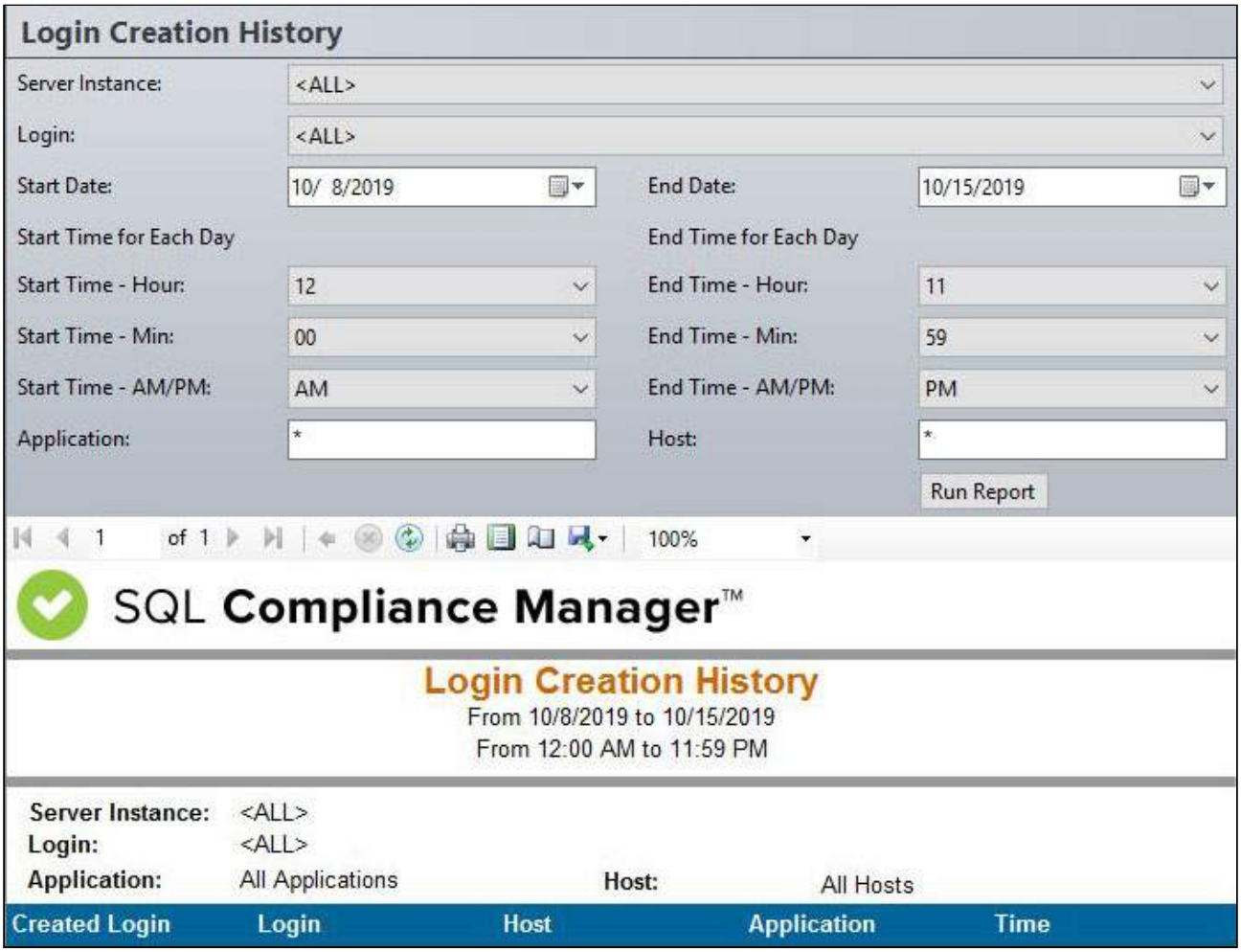
The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

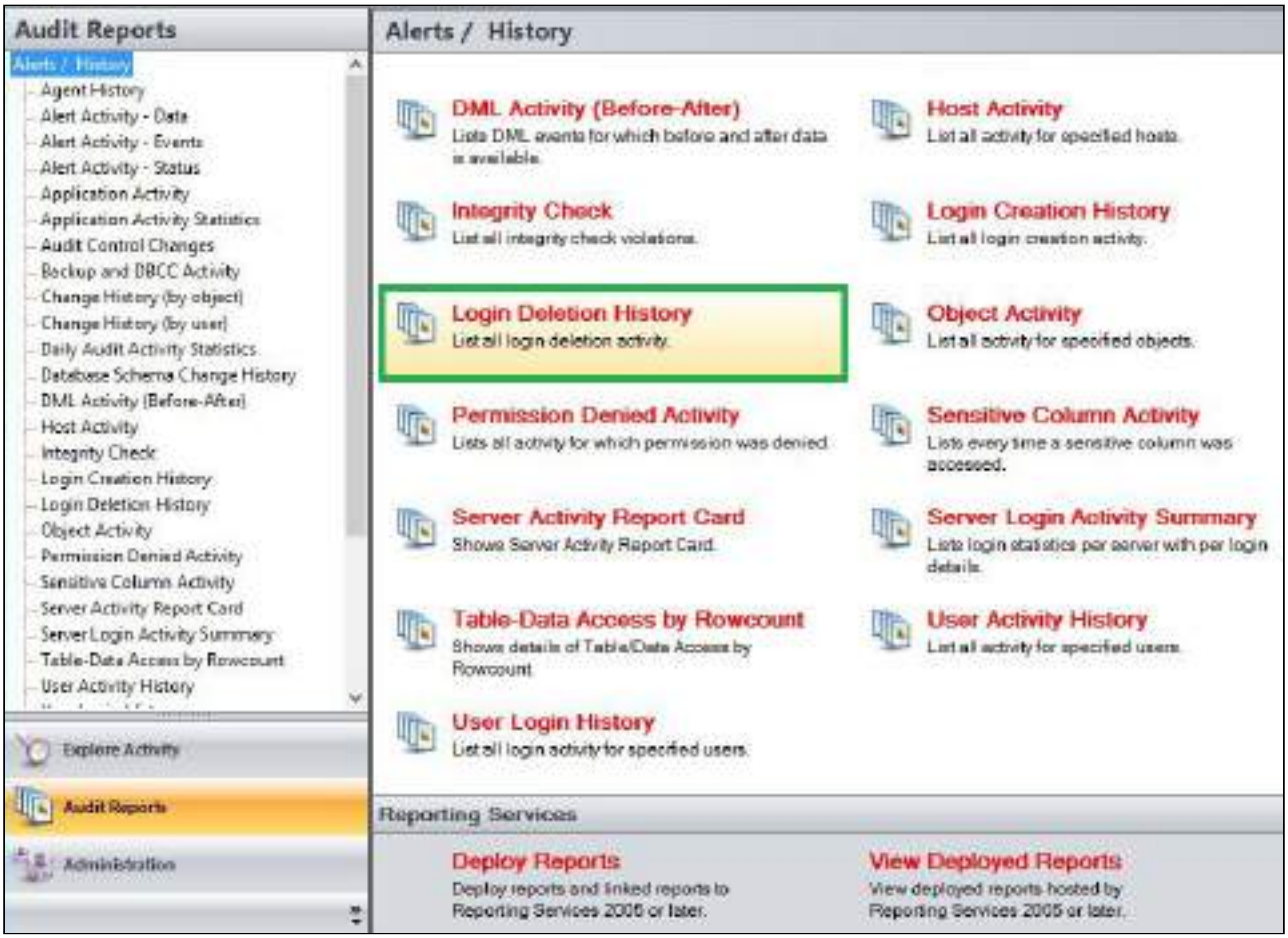
Time

The Time column displays the date and time when the event was captured.



Login Deletion History Report

The Login Deletion History Report provides the history of login deletion activity. Use this report to audit user behavior and login management.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Deleted Login

The Deleted Login column displays the name of the login deleted.

Login

The Login column displays the login name of the user who performed the event.

Host

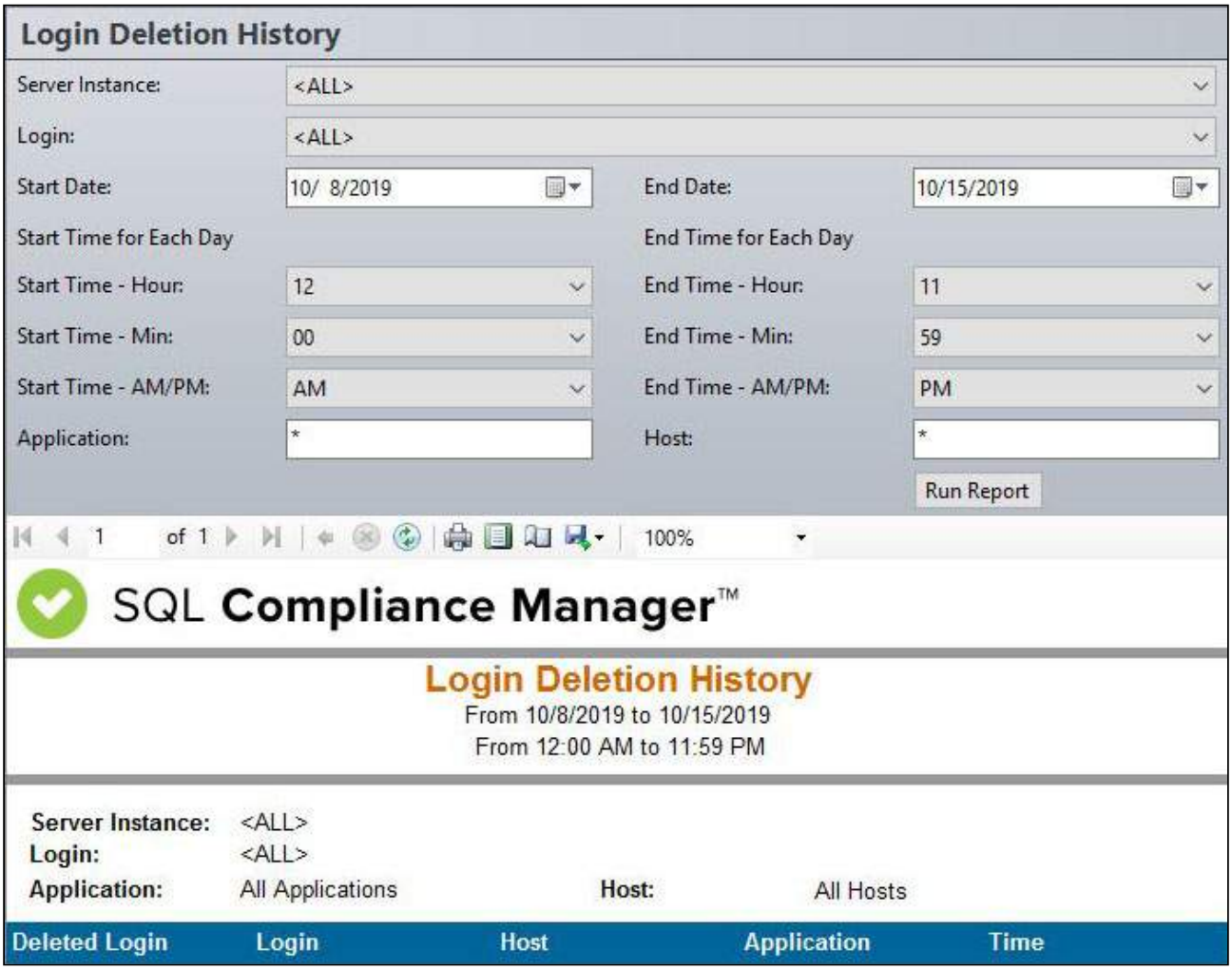
The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

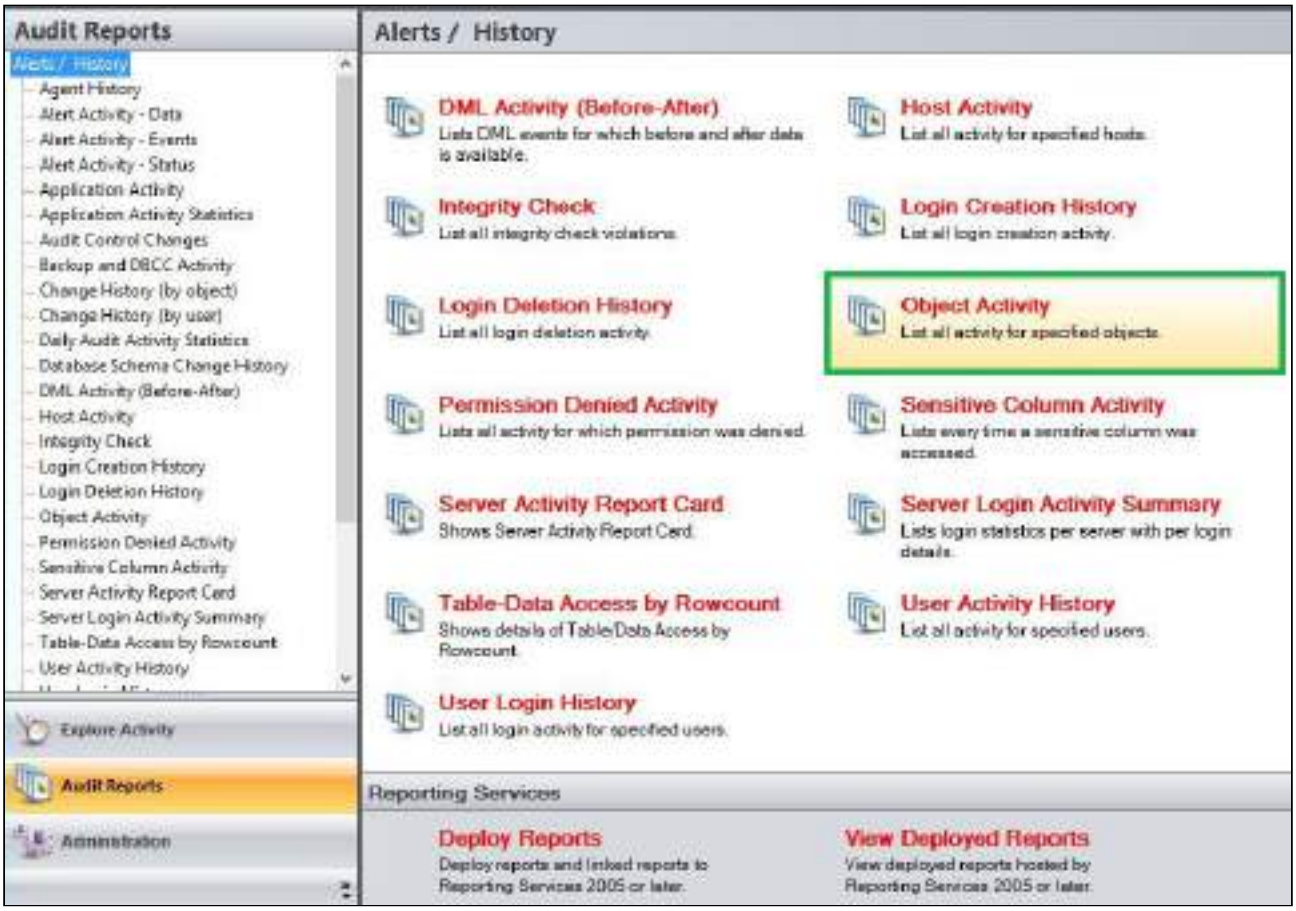
Time

The Time column displays the date and time when the event was captured.



Object Activity Report

The Object Activity Report lists all activity for specified objects performed on specific databases. Use this report to audit mass data movement or database object activity, such as SELECT or UPDATE, across multiple databases.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of one or more schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select from a category type to filter on from the drop down menu.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Event

The Event column displays a description of the event captured.

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Time

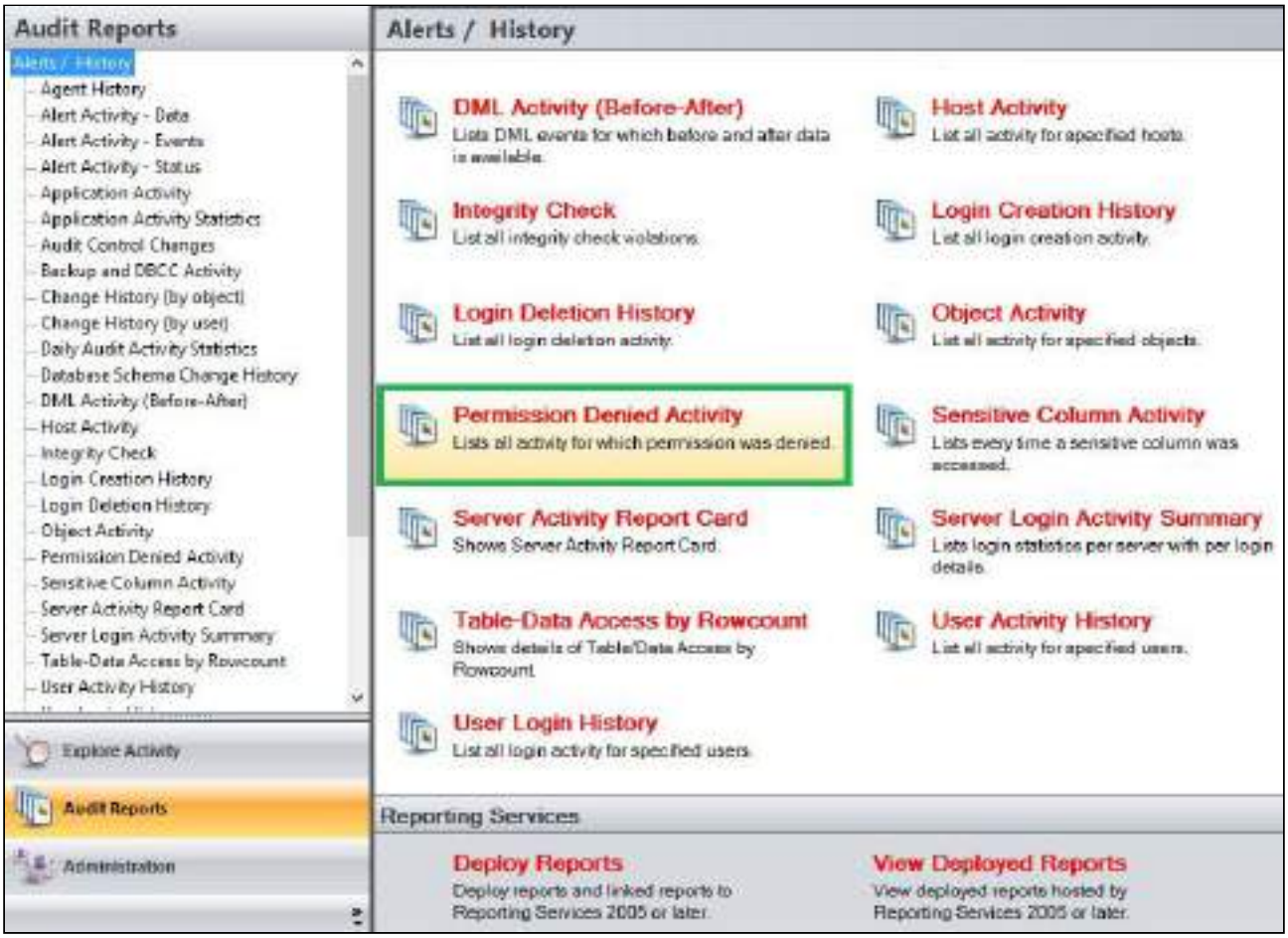
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Permission Denied Activity Report

The Permission Denied Activity Report lists all unauthorized attempts to execute activities. Use this report to audit your SQL Server security settings and identify misconduct.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select a category type from the drop down menu to filter the report on.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Host

The Host column displays the name of the host.

Login

The Login column displays the login name of the user who performed the event.

Application

The Application column displays the name of the application used to capture the event.

Database

he Database column displays the name of the database where the event was captured.

Event

The Event column indicates the type of event captured.

Schema

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Time

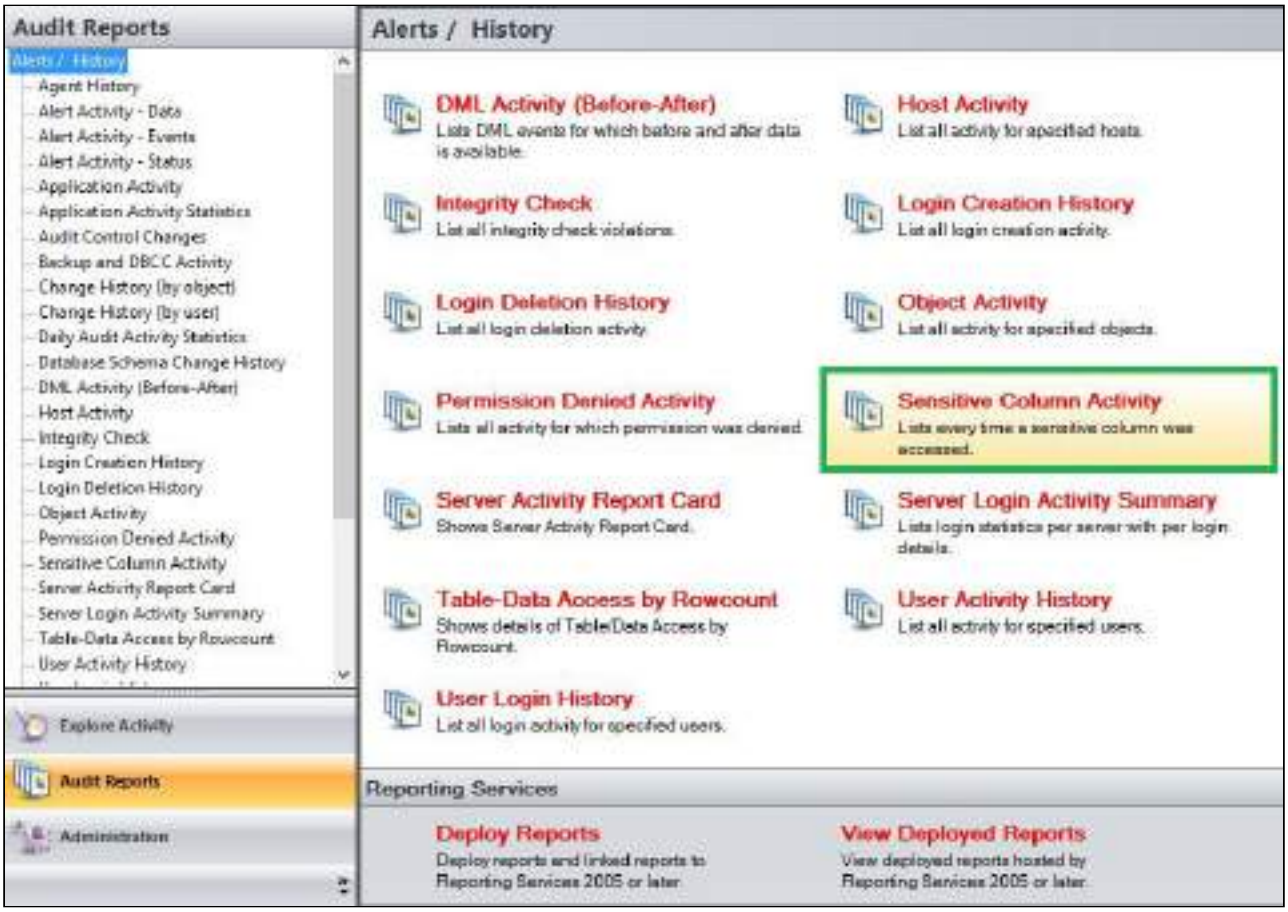
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

Sensitive Column Activity Report

The Sensitive Column Activity Report lists every time a sensitive column is accessed. The report lists all SELECT events that were initiated by applications to read specific columns that contain sensitive data. Use this report to audit columns that require high security or contain sensitive data.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Table Name

Allows you to select or type the name of one or more table names on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Column Name

Allows you to type the column names of one or more columns on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Run Report

Click this button to Run the report.

Default columns

Event

The Event column indicates the type of event captured.

Time

The Time column displays the date and time when the event was captured.

Login

The Login column displays the login name of the user who performed the event.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Table Name

The Table Name column displays the name of the table where the event was captured.

Column Name

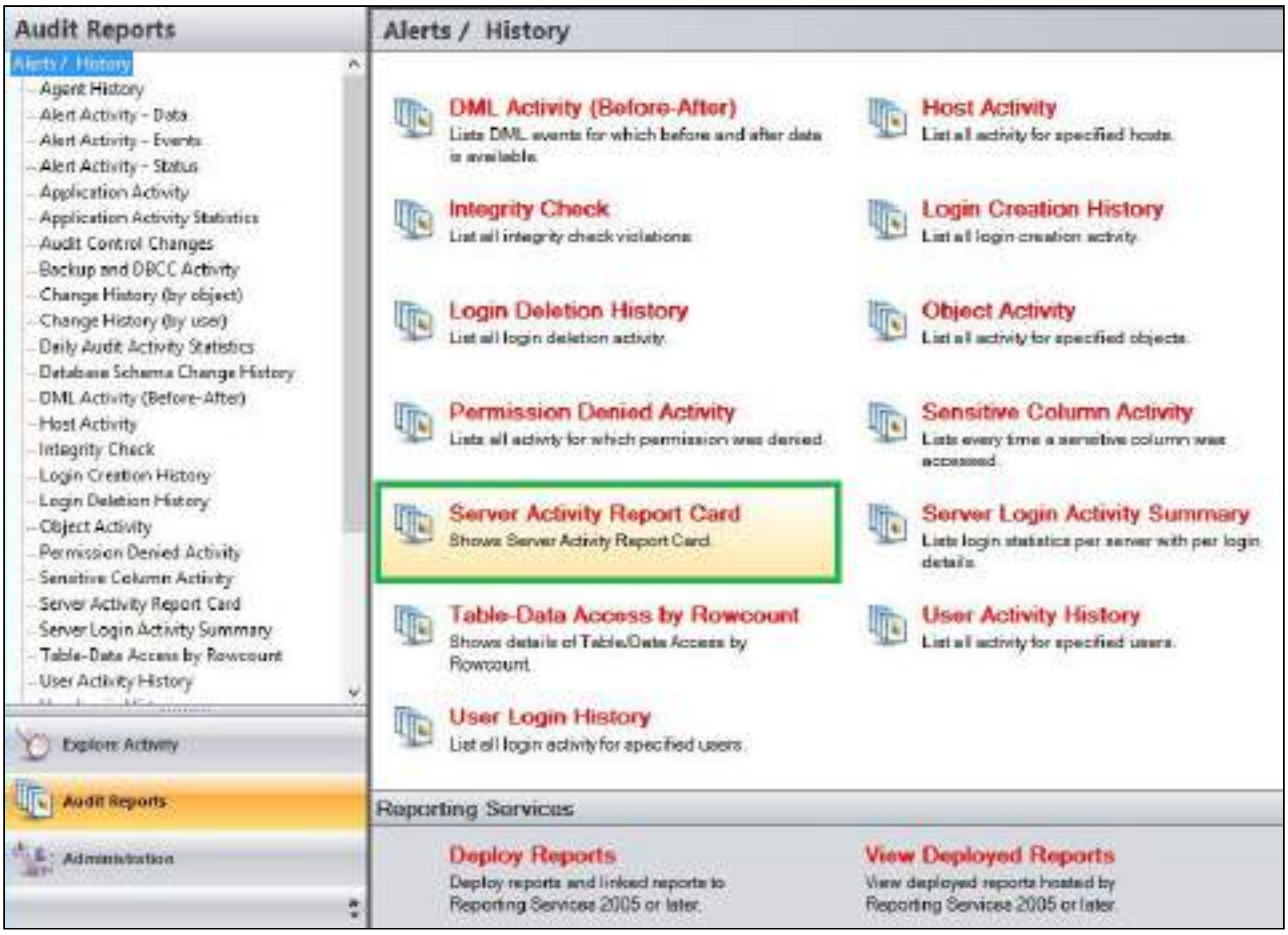
The Column Name column displays the name of the column where event was captured.

Application

The Application column displays the name of the application used to capture the event.

Server Activity Report Card Report

The Server Activity Report Card report allows you to review the activity status and recent audit event history on your SQL Server instance. Use this report to display a particular server´s activity status to help determine whether you are effectively auditing events in your environment.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Server Activity

Allows you to filter the report by a specific server activity. Select a server activity from the drop down menu to filter the report on.

Category

Allows you to select the category type on which you want to report. Select a category type from the drop down menu to filter the report on.

Event

Allows you to type the name of one or more events on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Database

The Database column displays the name of the database where the event was captured.

Category

The Category column indicates the category type of the event captured.

Event

The Event column indicates the type of event captured.

Time

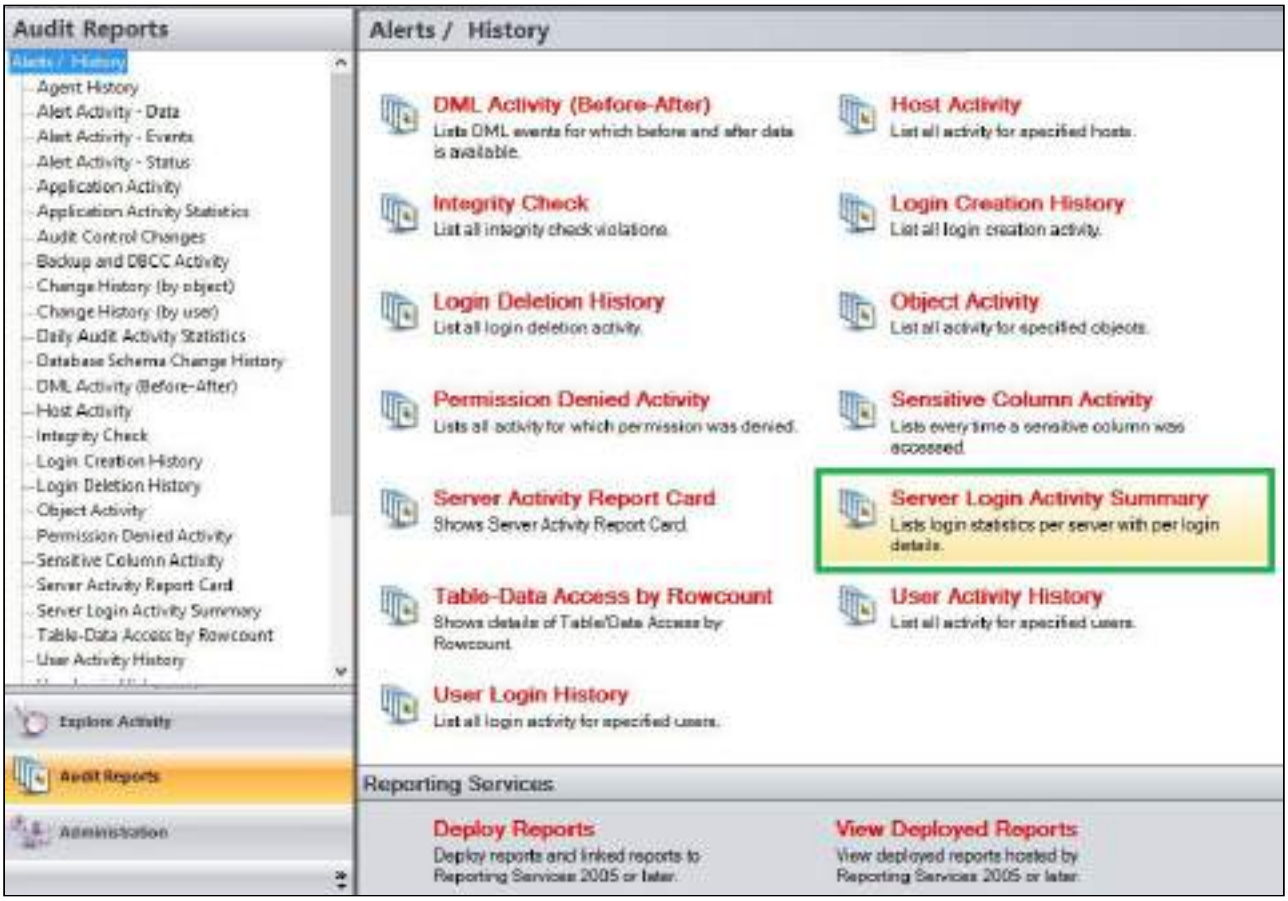
The Time column displays the date and time when the event was captured.

Details

The Details column provides details of the captured event.

Server Login Activity Summary Report

The Server Login Activity Summary Report lists user activities performed on a specific SQL Server instance with details per login. Use this report to audit user behavior and login management.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Login Status

Allows you to define the login status you want this report to filter on. Select between the following options; Both, Login or Login Failed.

Run Report

Click this button to Run the report.

Default columns

Login

The Login column displays the login name of the user who performed the event.

Application

The Application column displays the name of the application used to capture the event.

Count

The Count column displays count value.

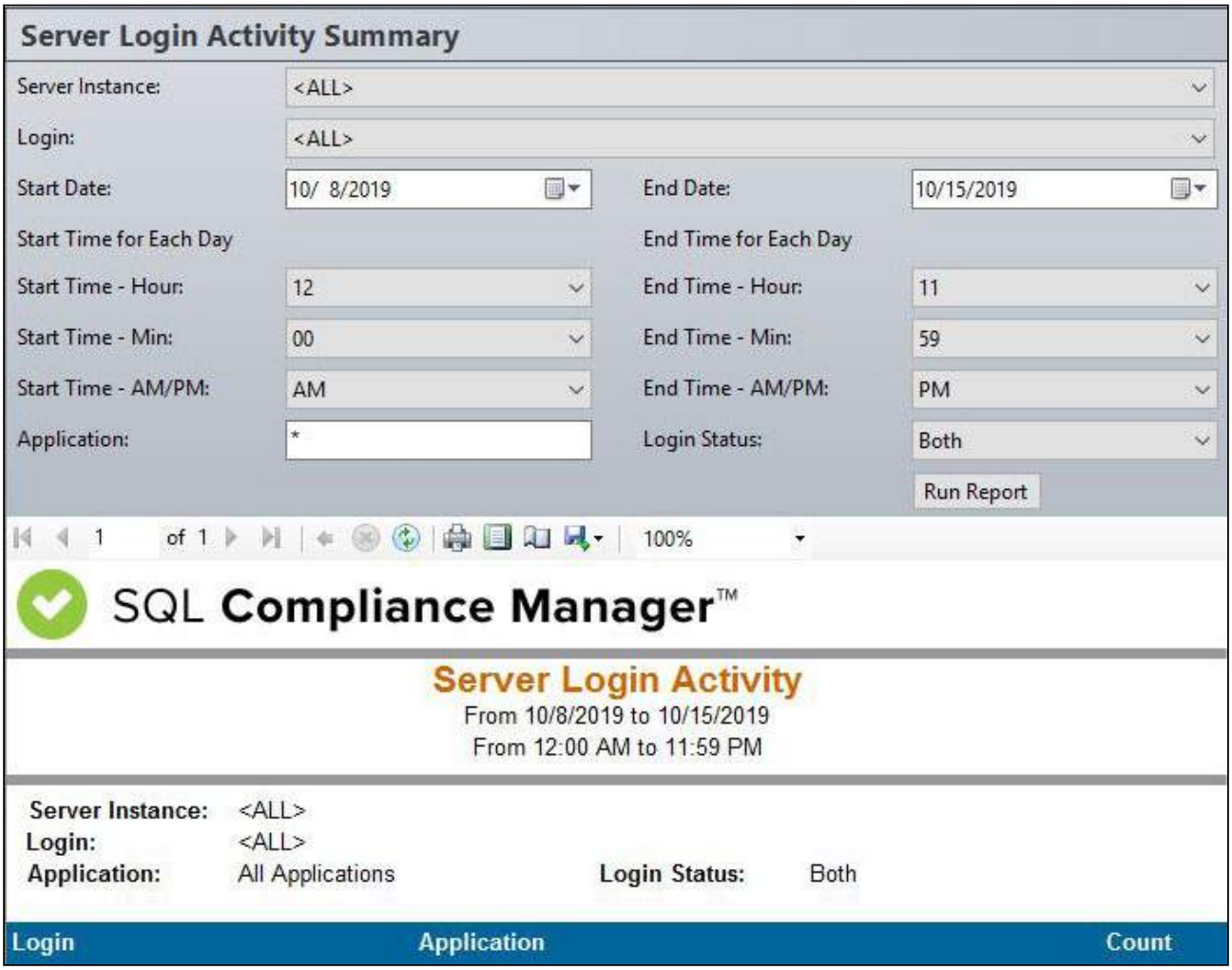
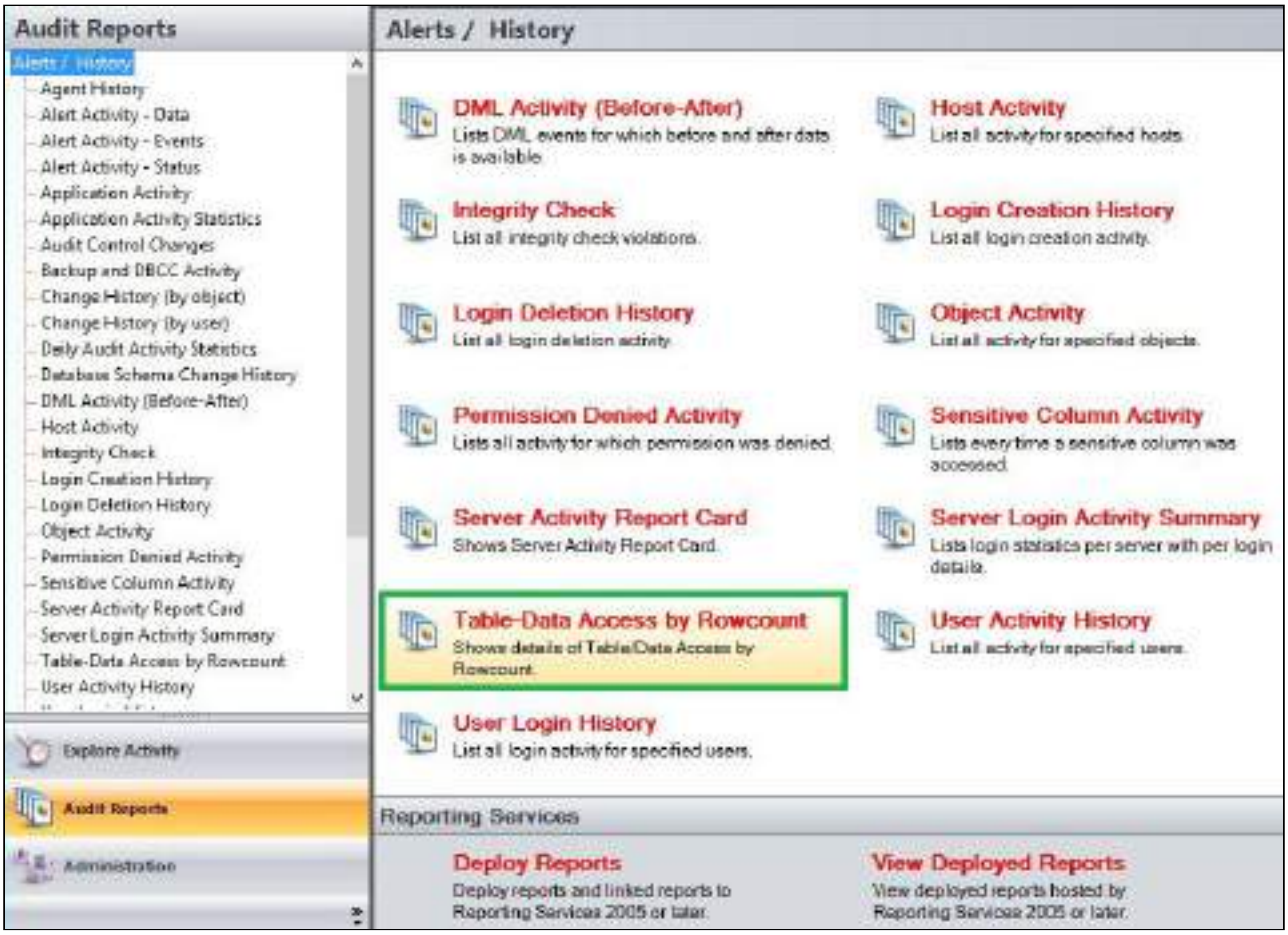


Table-Data Access by Rowcount Report

The Table-Data Access by Row count lists all information about table/data accessed by Rowcount. Use this report to audit the frequency in which data is accessed, identifying suspicious behavior.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Table Name

Allows you to select or type the name of one or more table names on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Column Name

Allows you to type the column names of one or more columns on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged User

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Default Status

Allows you to define the default status you want this report to filter on. Select between the following options; All, Same or Different.

Row Count Threshold

Allows you to type the number of Row count Threshold on which you want to report.

Run Report

Click this button to Run the report.

Default columns

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Database

The Database column displays the name of the database where the event was captured.

Schema

The Schema column displays the name of the event´s schema.

Table Name

The Table Name column displays the name of the table where the event was captured.

Column Name

The Column Name column displays the name of the column where event was captured.

Login

The Login column displays the login name of the user who performed the event.

Role

The Role column displays whether the users login role is a Privileged or a Trusted user.

Number of Rows

The Number of Rows column displays the number of rows affected.

Application

The Application column displays the name of the application used to capture the event.

Event

The Event column displays a description of the event captured.

Date/Time

The Date/Time column displays the date and time the event was captured.

SPID

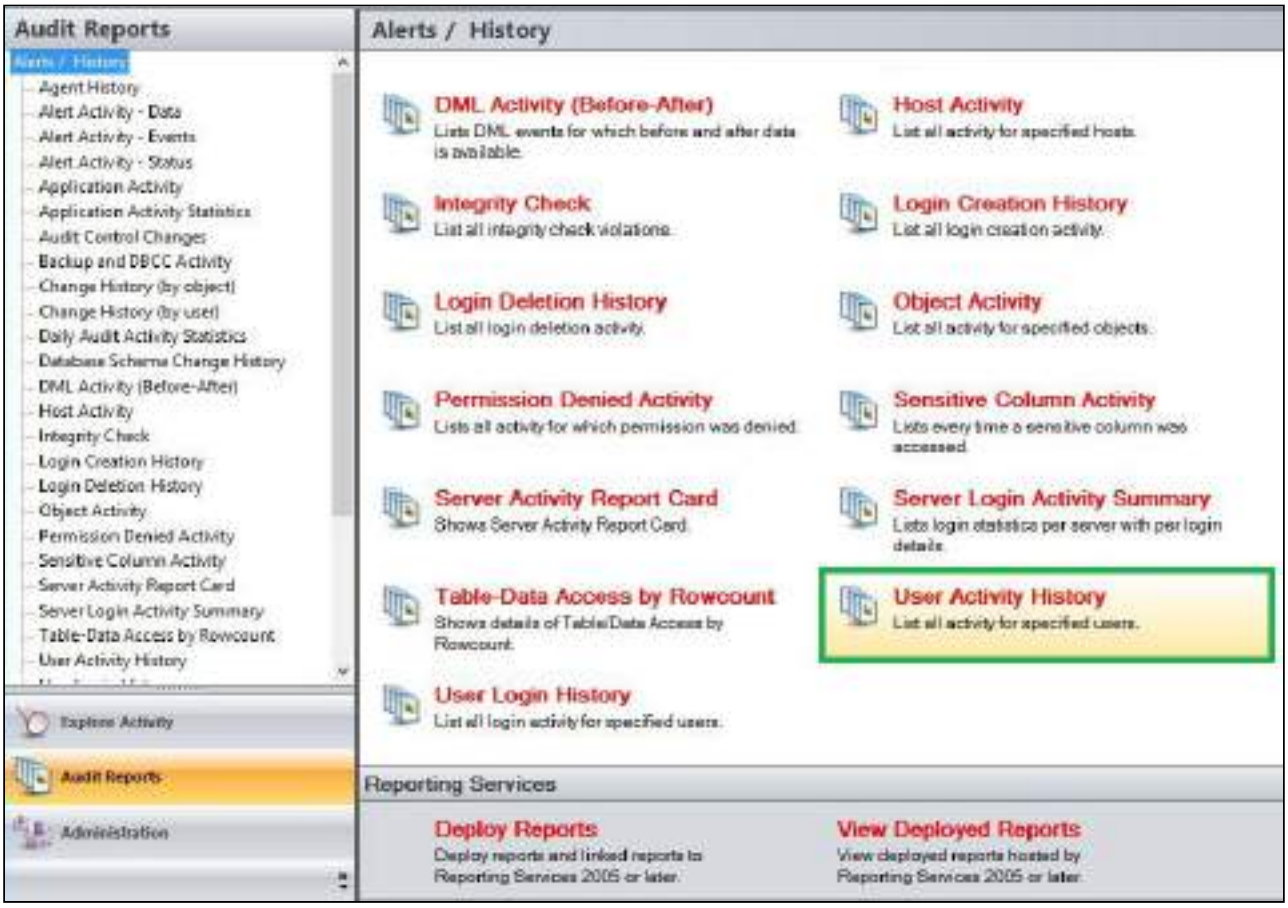
The SPID column displays the server process ID.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

User Activity History Report

The User Activity History Report lists user activities performed on a specific SQL Server instance, and provides a history of user activity for specified users.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select a category type from the drop down menu to filter the report on.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Host

The Host column displays the name of the host.

Login

The Login column displays the login name of the user who performed the event.

Application

The Application column displays the name of the application used to capture the event.

Database

The Database column displays the name of the database where the event was captured.

Event

The Event column displays a description of the event captured.

Schema Name

The Schema column displays the name of the event´s schema.

Target Object

The Target Object column displays the name of the target object.

Details

The Details column provides details of the captured event.

Time

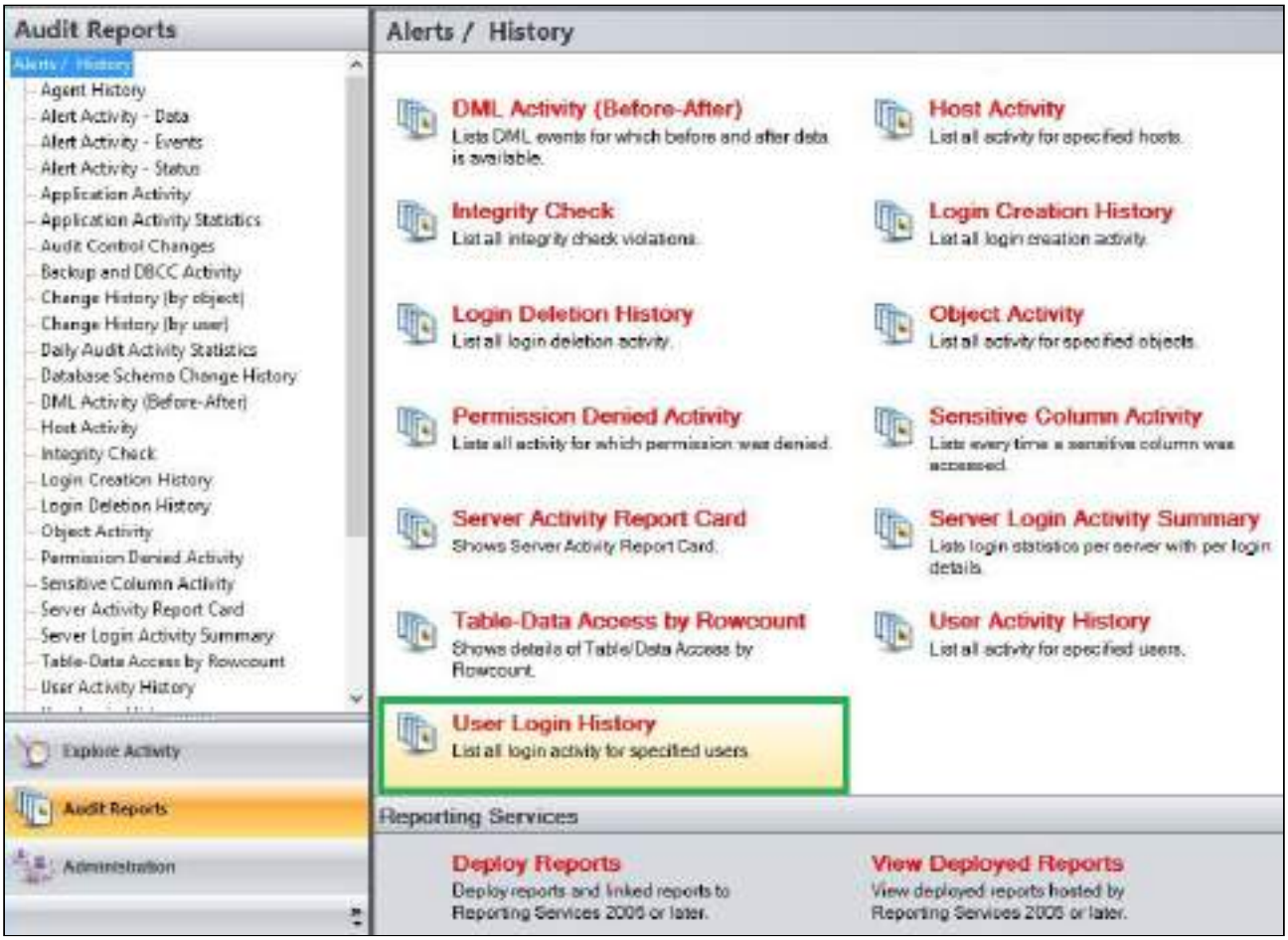
The Time column displays the date and time when the event was captured.

SQL

The SQL column when set to True, provides the SQL Statement for the captured event.

User Login History Report

The User Login History Report lists all login activity for specified users. Use this report to audit your SQL Server security settings and identify misconduct.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Start Date

Allows you to select the start date for the range from which you want to report.

End Date

Allows you to select the end date for the range from which you want to report.

Start Time - Hour

Allows you to select the exact starting hour of the day for the range from which you want to report.

Start Time - Min

Allows you to select the exact starting minute of the day for the range from which you want to report.

Start Time - AM/PM

Select between AM or PM from the drop down list to configure the Start Time for Each Day range from which you want to report.

End Time - Hour

Allows you to select the exact ending hour of the day for the range from which you want to report.

End Time - Min

Allows you to select the exact ending minute of the day for the range from which you want to report.

End Time - AM/PM

Select between AM or PM from the drop down list to configure the End Time for Each Day range from which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Target Object

Allows you to type the name of one or more target objects on which you want to report.

Application

Allows you to type the name of one or more applications on which you want to report.

Host

Allows you to type the name of one or more hosts on which you want to report.

Category

Allows you to select the category type on which you want to report. Select a category type from the drop down menu to filter the report on.

Event

Allows you to type the name of one or more events on which you want to report.

Show SQL

Select between True or False from the drop down menu to filter the report by SQL Text.

Privileged Users Only

Select between True or False from the drop down list to report on Privileged Users only or to report on All User types.

Run Report

Click this button to Run the report.

Default columns

Login

The Login column displays the login name of the user who performed the event.

Host

The Host column displays the name of the host.

Application

The Application column displays the name of the application used to capture the event.

Time

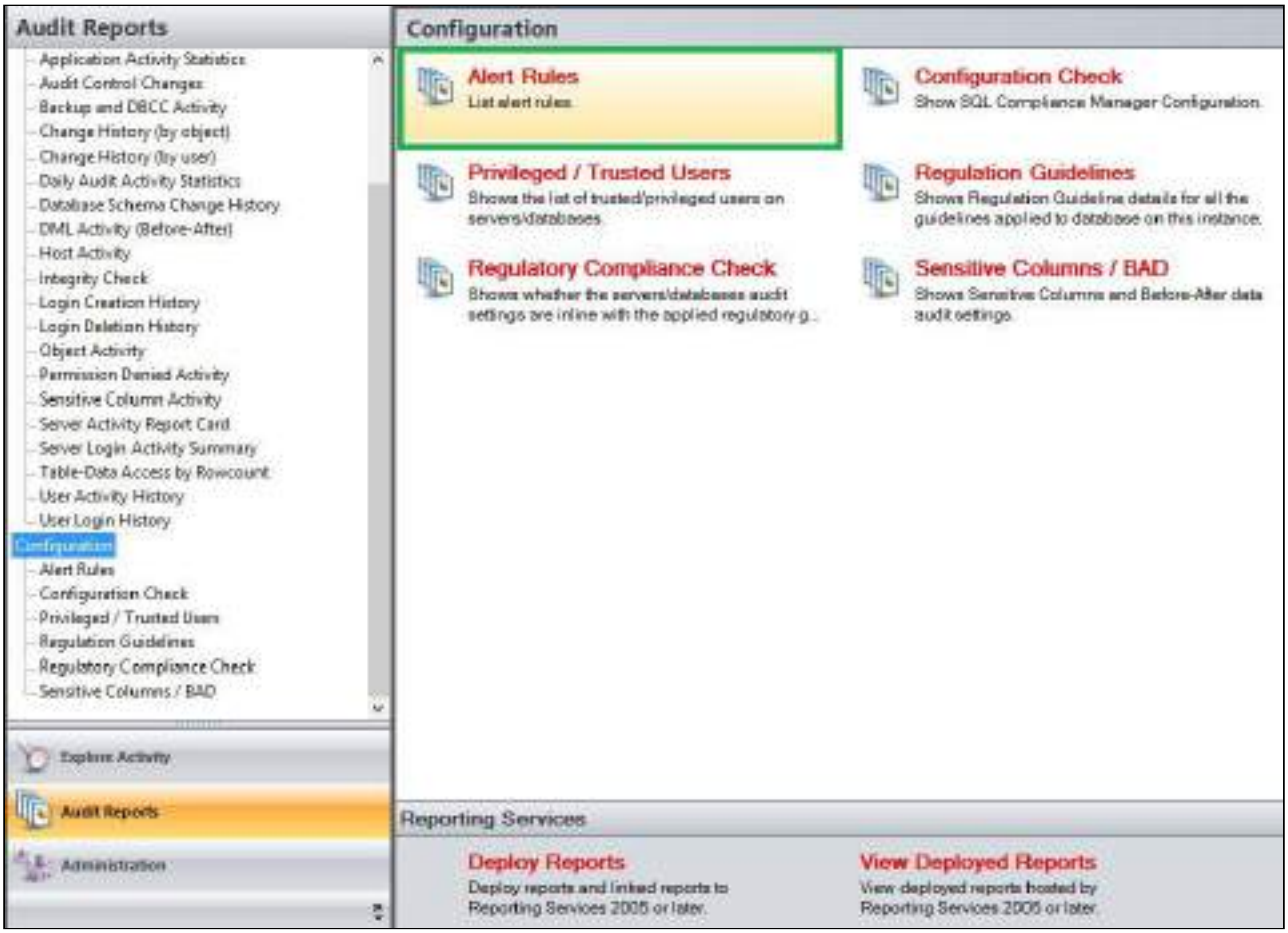
The Time column displays the date and time when the event was captured.

Event

The Event column displays a description of the event captured.

Alert Rules Report

The Alert Rules report shows a lists of all the existing alert rules in your environment, you can filter the alerts by the rule name, by the alert level or by selecting the rule type. Use this report to monitor all types of alert rules in your environment.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Rule

Allows you to type the name of one or more rules on which you want to report.

Rule Type

Allows you to select the rule type on which you want to report. Select between the following rule types; All, Event Rules, Status Rules or Data Rules.

Event Log

Choose to filter alert rules based on alerts which log events or do not log events. Select **ALL** to report on all alert rules.

Alert Level

Choose to filter alerts by their different levels; Severe, High, Medium, or Low.

Email

Allows you to select whether display Alert Rules with an email associated to the rule or display Alert Rules with no email associated to it. Select All to display all Alert Rules.

Run Report

Click this button to Run the report.

Default columns

Rule

The Rule column displays the name of the alert rule.

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Alert Level

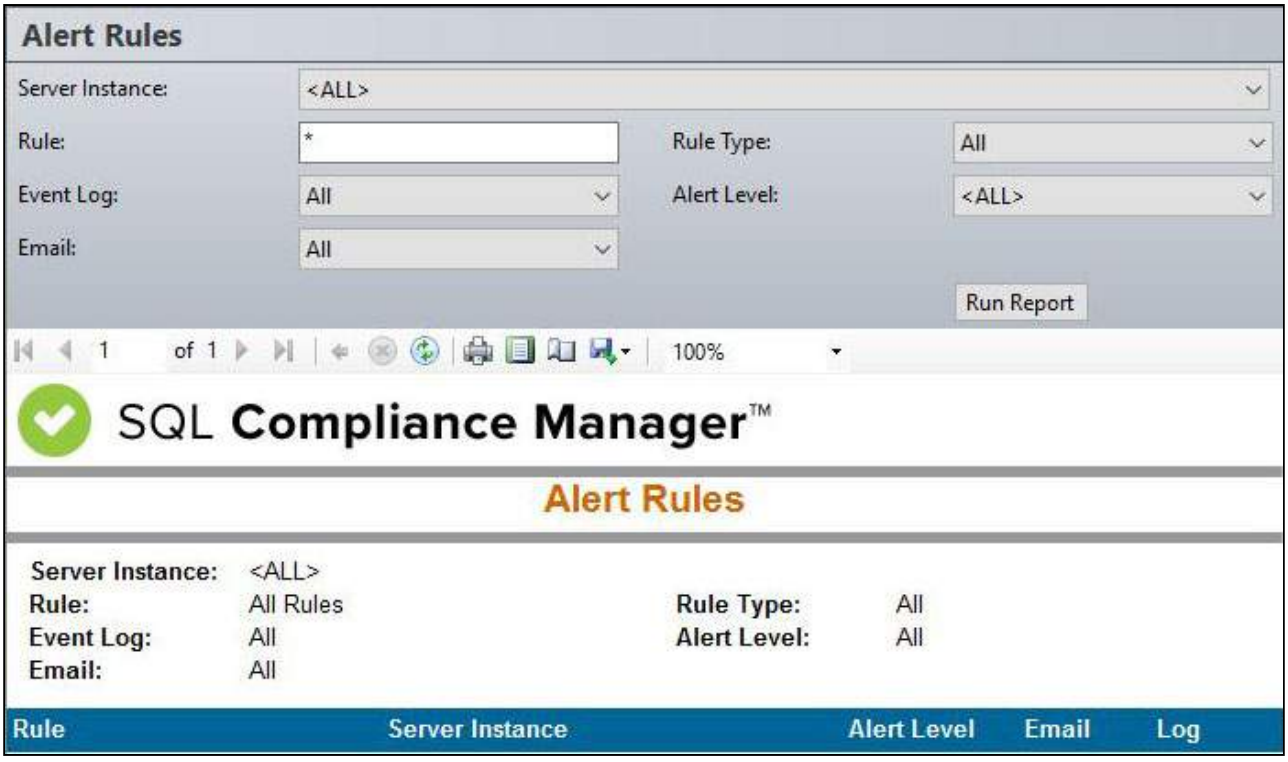
The Alert Level column displays the level the alert is configured to.

Email

The Email column specifies whether the alert rule has an email address associated to it, in order to receive the alerts.

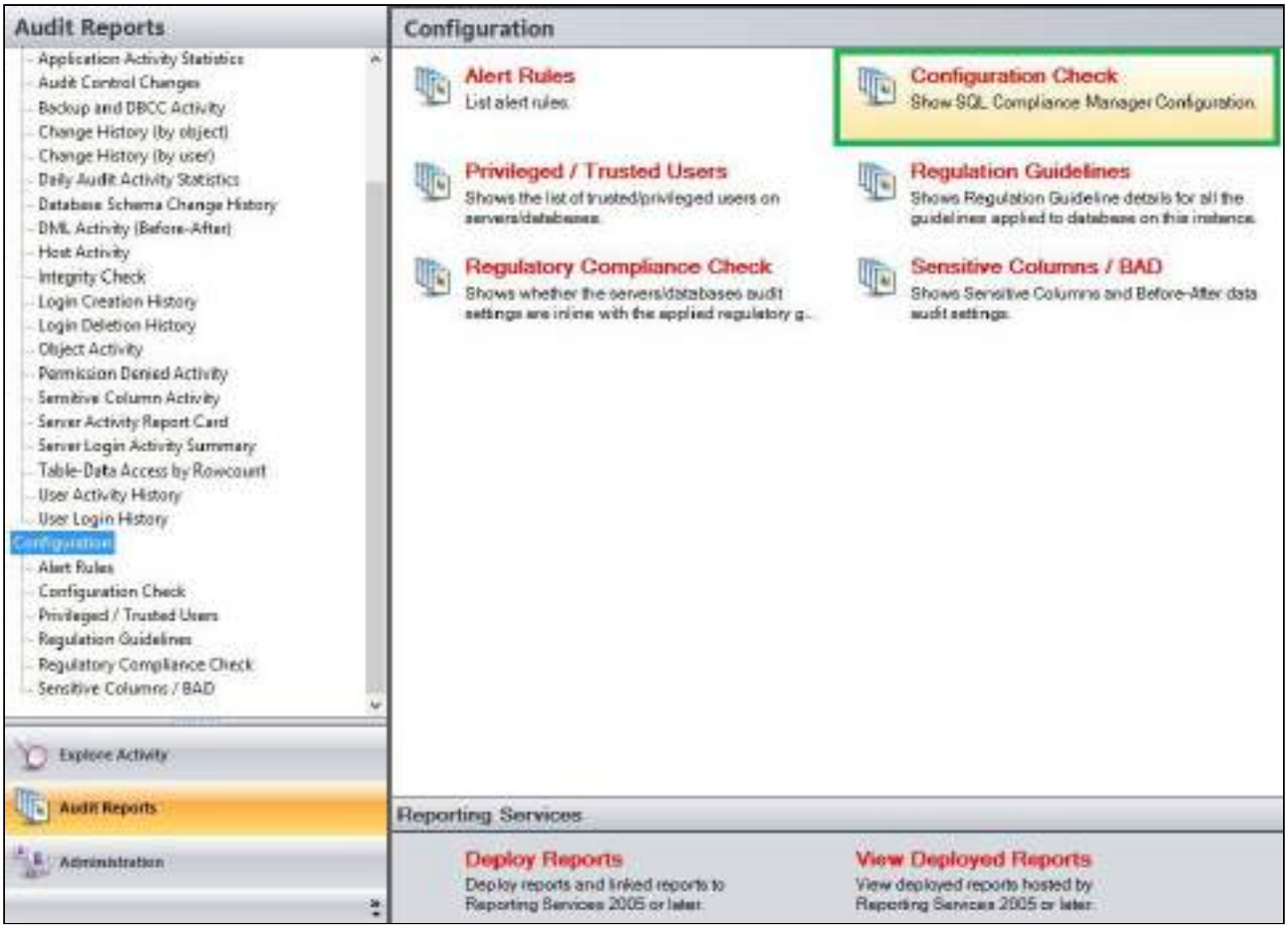
Log

The Log column specifies whether the alert rule is configured to log events.



Configuration Check Report

The Configuration Check Report lists all the configurations selected on a Server or Database. Use these reports to reconcile the differences in regards to the configurations across different servers and databases.



Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Database

Allows you to select or type the name of one or more databases on which you want to report.

Audit Setting

Allows you to filter the report by specific audit setting. Select one audit setting from the drop down menu option.

Default Status

Allows you to compare what the current value setting is set to for that Server/Database compared to what the default setting is for that setting. Define the default status you want this report to filter by selecting between the following options; All, Same (Same value as the default) or Different (Different value as the default).

Run Report

Click this button to Run the report.

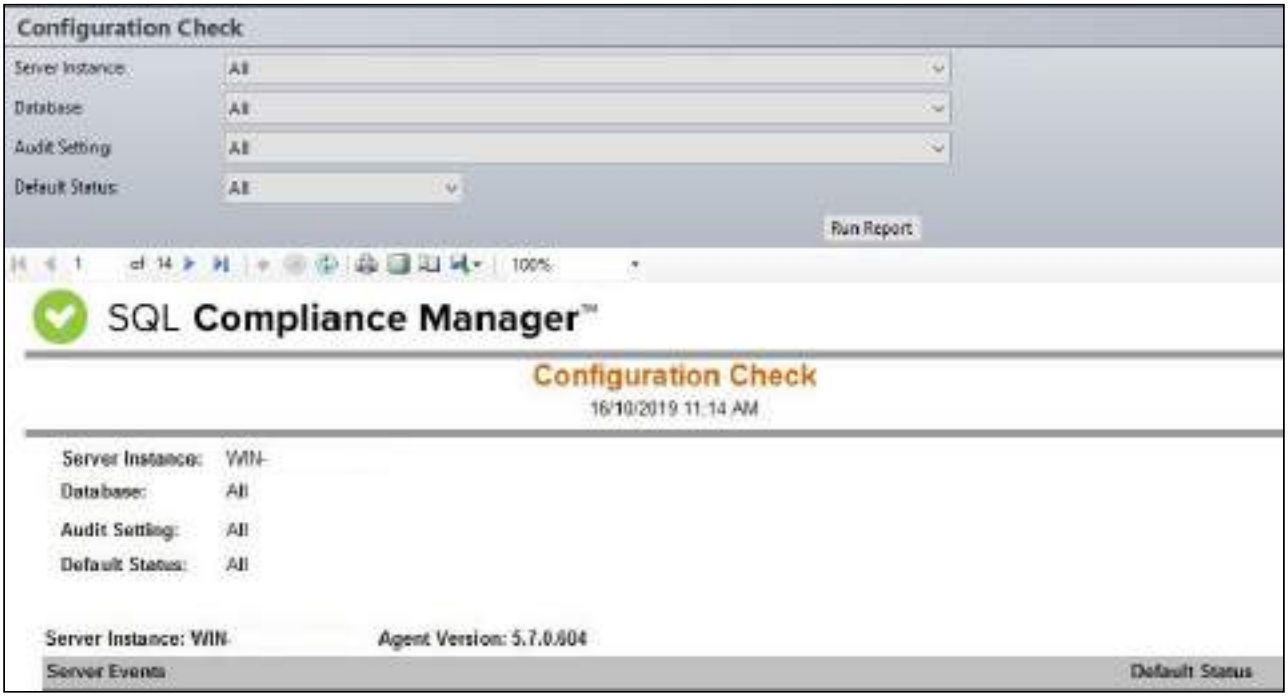
Default columns

Server Events

The Server Events column provides the name of the server event.

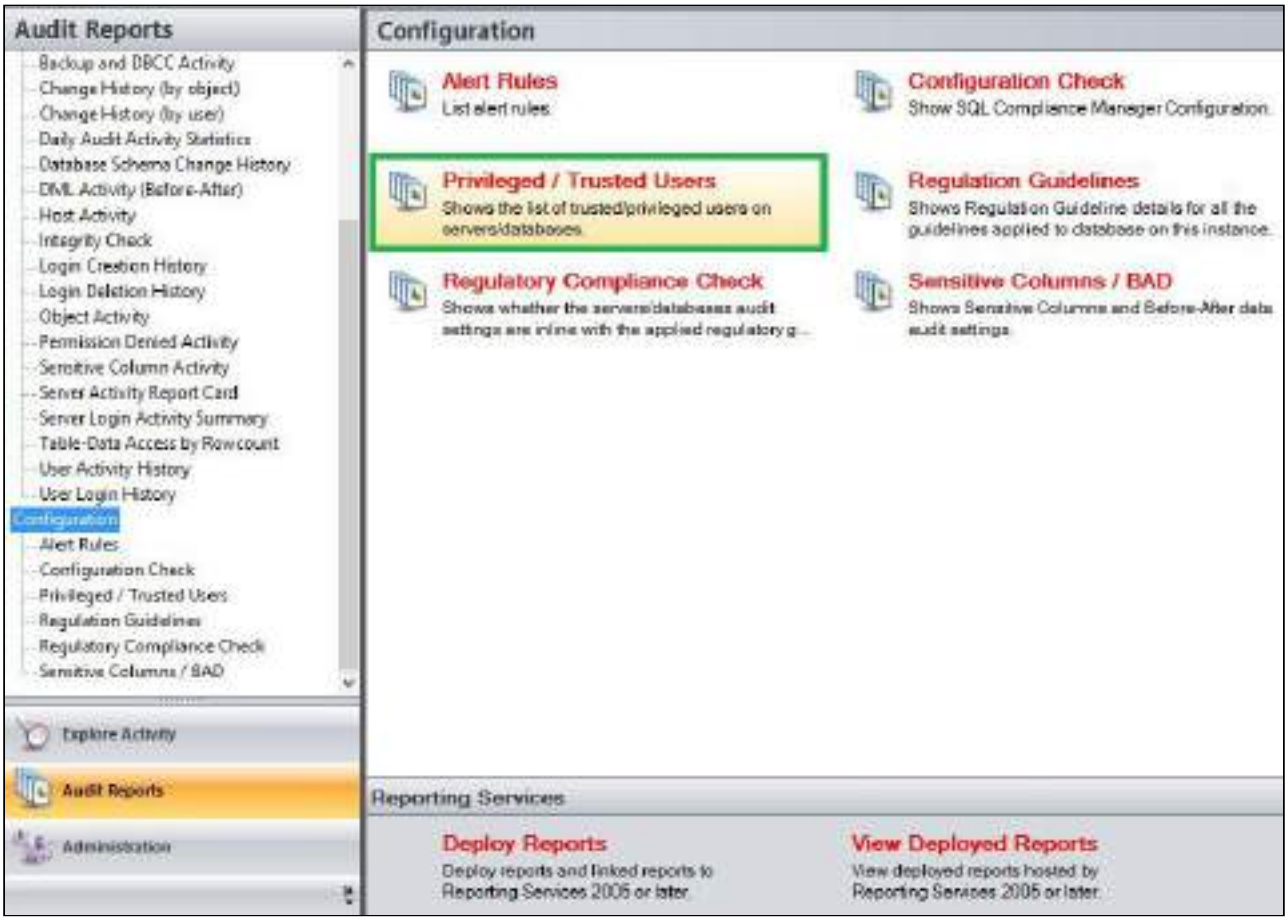
Default Status

The Default Status column allows you to compare the Individual Settings on the Server/Database with those that are set in your "Default" settings. If you have not set up "Default" Settings then it compares the settings against the IDERA Default Settings.



Privileged/Trusted Users Report

The Privileged/Trusted Users report lists all trusted and privileged users set in each server instance and database. Use this report to monitor which Trusted and Privileged Users were set to during a snapshot in time.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report.

Login

Allows you to select the login from the drop down list of available logins. Select **ALL** to report on all logins.

Role

Allows you to define the type of role for which you want this report to filter on. Select one of the Roles to filter the report on from the drop down menu option.

User Type

Allows you to select the type of user for which you want this report to filter on. Select between the following options; Both, Trusted or Privileged.

Default columns

Logins/Roles

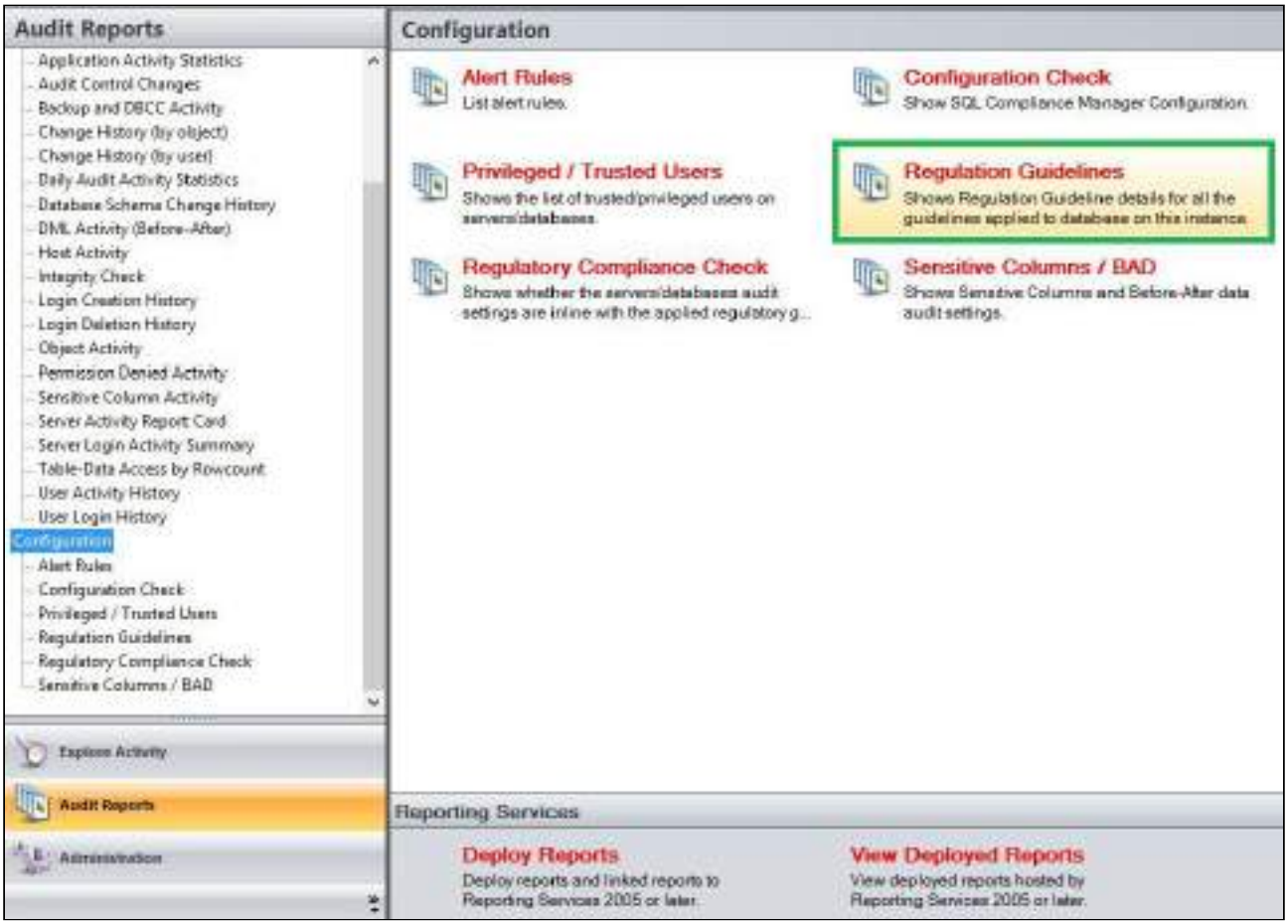
The Logins/Roles column displays the name of the login or role.

Server/Database

The Server/Database column displays the name of the server or database.

Regulation Guidelines Report

The Regulation Guideline Report shows regulation guidelines details for all the guidelines applied to database on the selected instance. Use this report to audit and monitor the regulatory guidelines applied to your SQL Server instance.



Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Run Report

Click this button to Run the report.

Default columns

Server Instance

The Server Instance column displays the name of the Instance Server where the event was captured.

Database

The Database column displays the name of the database where the event was captured.

CIS

The CIS column indicates whether the this regulation guideline is applied or not to the each database in a server.

DISA

The DISA column indicates whether the this regulation guideline is applied or not to the each database in a server.

FERPA

The FERPA column indicates whether the this regulation guideline is applied or not to the each database in a server.

GDPR

The GDPR column indicates whether the this regulation guideline is applied or not to the each database in a server.

HIPPA

The HIPPA column indicates whether the this regulation guideline is applied or not to the each database in a server.

NERC

The NERC column indicates whether the this regulation guideline is applied or not to the each database in a server.

PCI

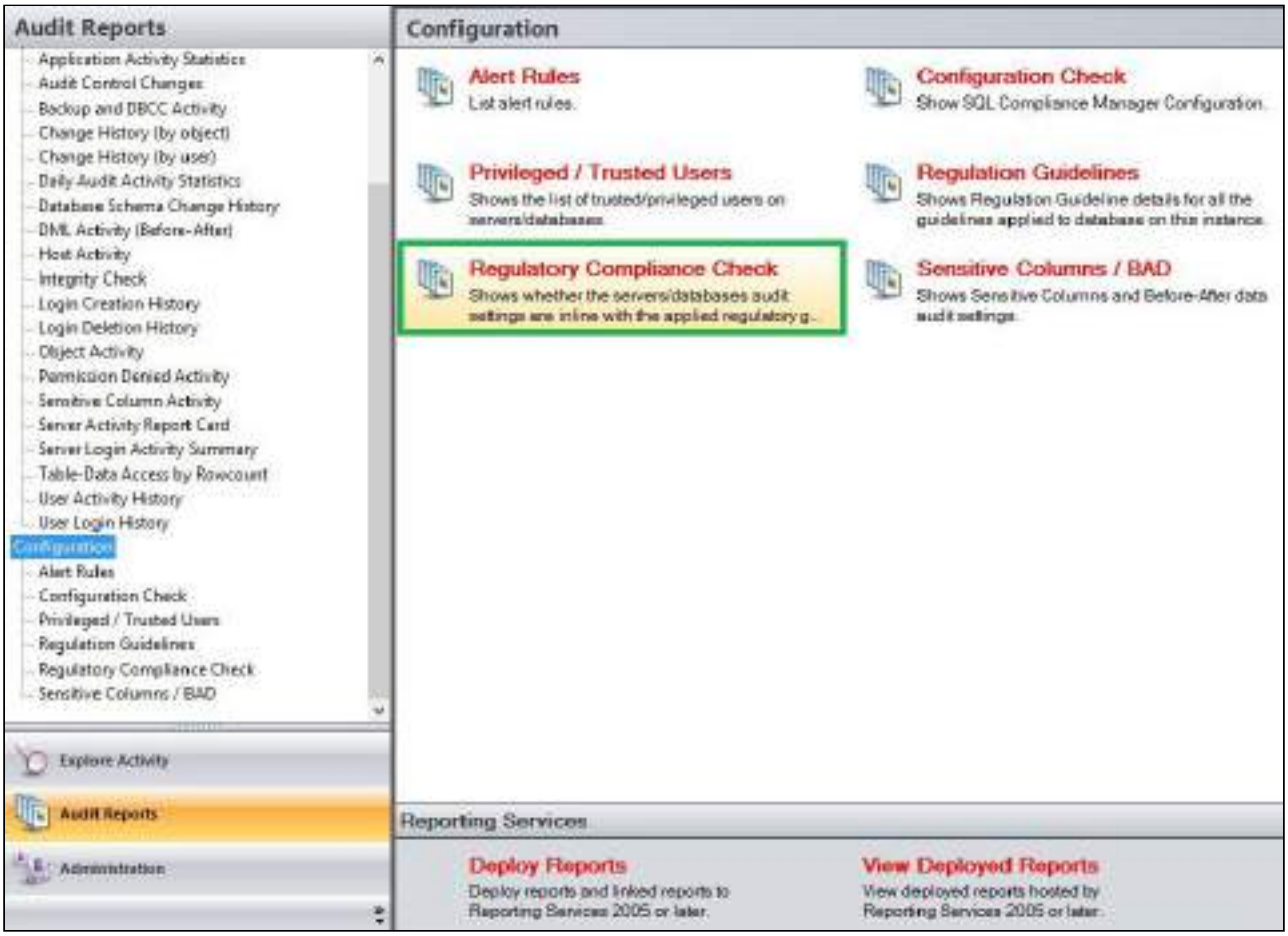
The PCI column indicates whether the this regulation guideline is applied or not to the each database in a server.

SOX

The SOX column indicates whether the this regulation guideline is applied or not to the each database in a server.

Regulatory Compliance Check Report

The Regulatory Compliance Check Report shows whether the selected servers/databases audit settings are inline with the applied regulatory guidelines. Use this report to ensure that your servers and databases continue to be in compliance with the selected regulatory guidelines.



Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select ALL to report on all instances.

Database

Allows you to select or type the name of one or more databases on which you want to report.

Audit Settings

Allows you to filter the report by specific audit settings. Select an audit setting from the drop down menu option, or select **ALL** to report on all audit settings.

Values

Allows you to filter based on the values of the audit settings. Select between the following options; Selected, Varies, Deselected or N/A.

Regulatory Guideline

Allows you to filter the report by a specific regulation guideline. Select a regulation guideline from the drop down menu option, or select **ALL** to report on all regulatory guidelines.

Run Report

Click this button to Run the report.

Default columns

Server Events

The Server Events column displays the name of the Server event.

CIS

The CIS column indicates whether the this regulation guideline is applied or not to the each database in a server.

DISA STIG

The DISA column indicates whether the this regulation guideline is applied or not to the each database in a server.

FERPA

The FERPA column indicates whether the this regulation guideline is applied or not to the each database in a server.

GDPR

The GDPR column indicates whether the this regulation guideline is applied or not to the each database in a server.

HIPPA

The HIPPA column indicates whether the this regulation guideline is applied or not to the each database in a server.

NERC

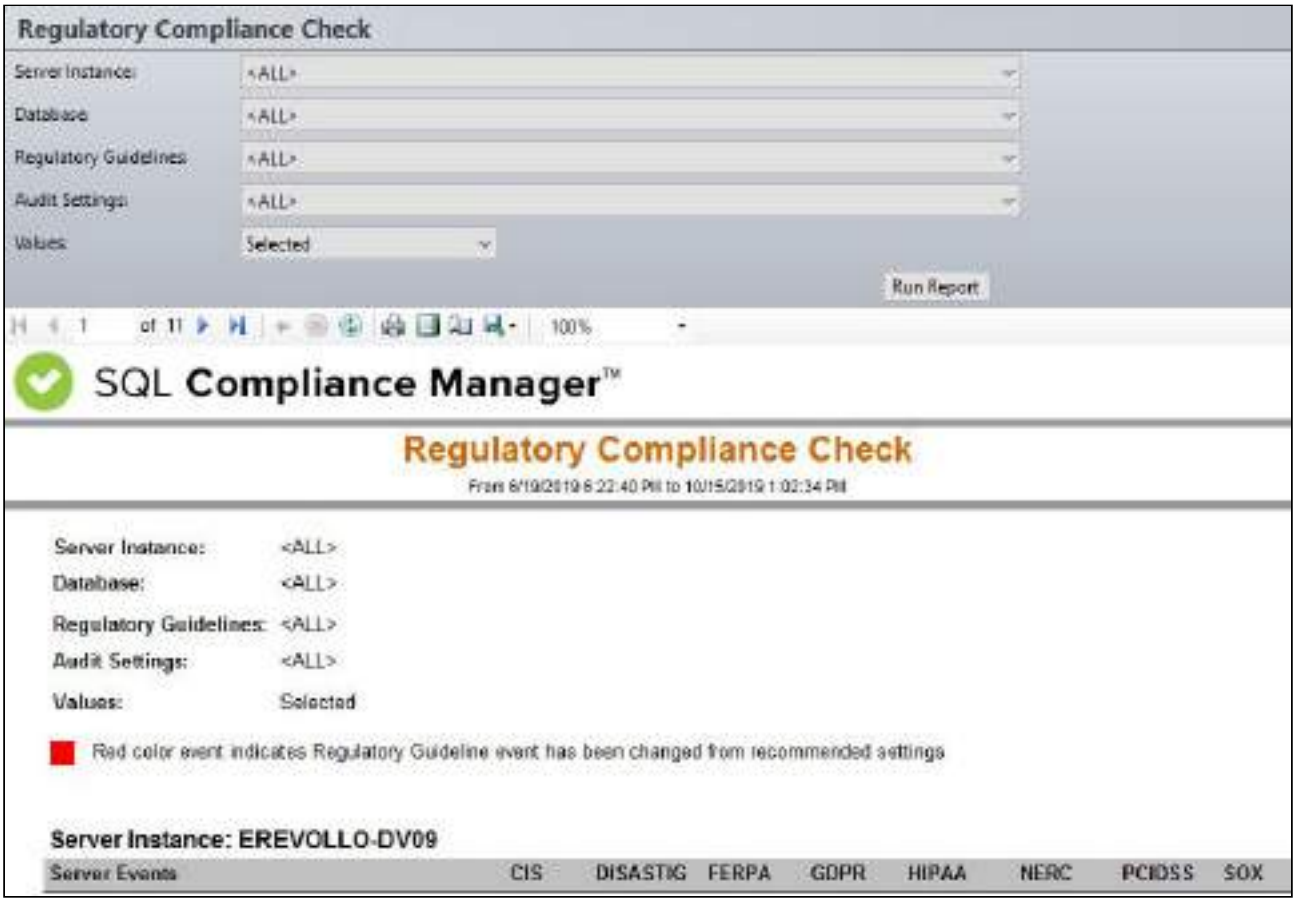
The NERC column indicates whether the this regulation guideline is applied or not to the each database in a server.

PCIDSS

The PCI column indicates whether the this regulation guideline is applied or not to the each database in a server.

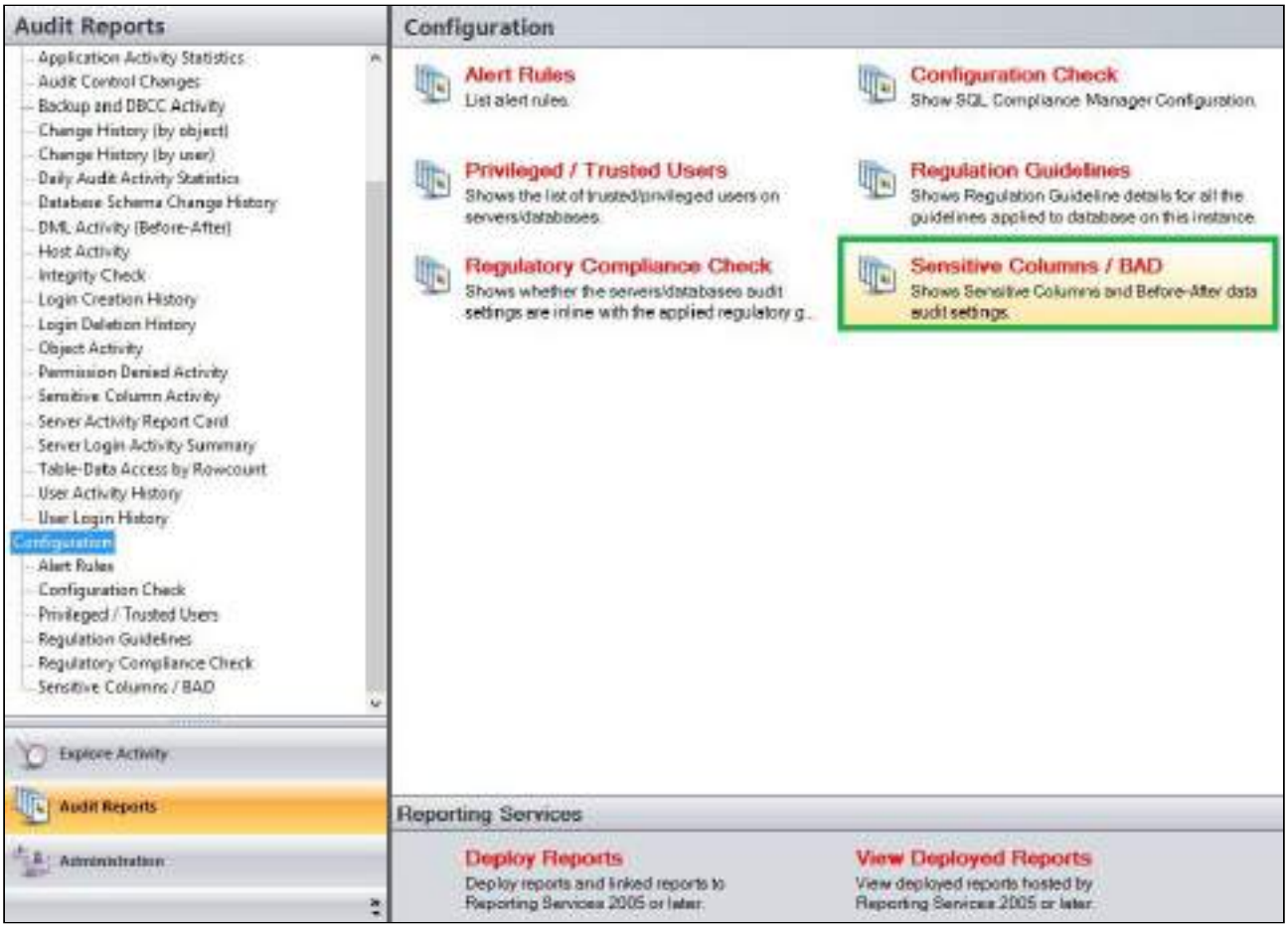
SOX

The SOX column indicates whether the this regulation guideline is applied or not to the each database in a server.



Sensitive Column and Before-After Activity Report

The Sensitive Column/BAD report lists Sensitive Column and Before-After data audit settings applied to your servers and databases. Use this report to monitor what Sensitive Columns and Before-After data auditing were set to during a snapshot in time.



A filter can include a list of wildcards, separated by commas, where a wildcard is a string, which may contain asterisks. The following parameters are specific to the selected report and enable you to filter the data to include in the report.

Available actions

Server Instance

Allows you to select a registered instance on which you want to report. Select **ALL** to report on all instances.

Databases

Allows you to select or type the name of one or more databases on which you want to report

Table Name

Allows you to select or type the name of one or more table names on which you want to report.

Schema

Allows you to type the name of the schema on which you want to report.

Column Name

Allows you to type the column names of one or more columns on which you want to report.

Data Type

Allows you to select the data type for which you want this report to filter on. Select between the following options; Both, Sensitive Column or Before After.

Run Report

Click this button to Run the report.

Default columns

Table Name

The Table Name column displays the name of the table where the event was captured.

Columns

The Columns column displays the name of the columns where sensitive data was accessed or altered.

Type

The Type column displays the whether the data was collected as part of a Dataset or from an Individual column.

Maximum Rows

The Maximum Rows column displays the maximum amount of rows altered.

9.2.4 Customize reports

You can customize any of the integrated audit reports or develop new reports that fit your unique auditing needs. First, deploy the IDERA 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.

9.2.5 Generate reports in the Console

IDERA SQL Compliance Manager includes many common audit reports. Create these reports using 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 Report**.

> Microsoft Excel supports only 32767 characters in a cell. If a SQL statement contains more than 32767 characters when exporting a report, Microsoft Excel truncates the additional characters.

9.2.6 Generate reports with Reporting Services

You can integrate the reports included with IDERA 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.

Reporting Services requirements

IDERA 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). ***To successfully use Reporting Services in 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.

Deploy reports to Reporting Services

The Deploy Reports wizard allows you to integrate IDERA 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.

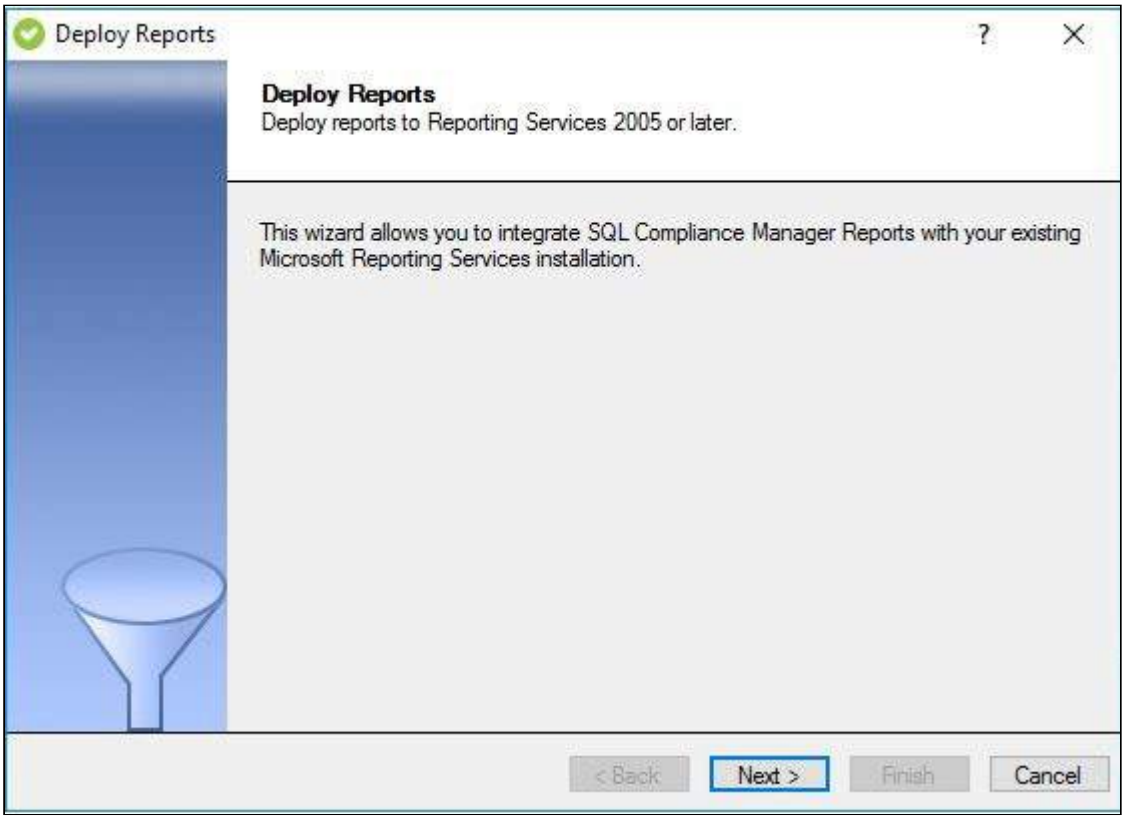
To install reports:

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 **Reporting Services**, 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**.
7. Name of the SQL Server instance that is hosting the target Repository
8. Credentials of the Windows account the Report Server should use to connect to the Repository databases
9. 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**.
10. ***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.
11. On the Summary window, click **Next**.
12. Review the progress. When deployment is complete, click **OK**.
13. 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.

Deploy Reports wizard - Welcome tab

You can deploy the IDERA SQL Compliance Manager Reports to your existing Microsoft Reporting Services installation. SQL Compliance Manager 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.

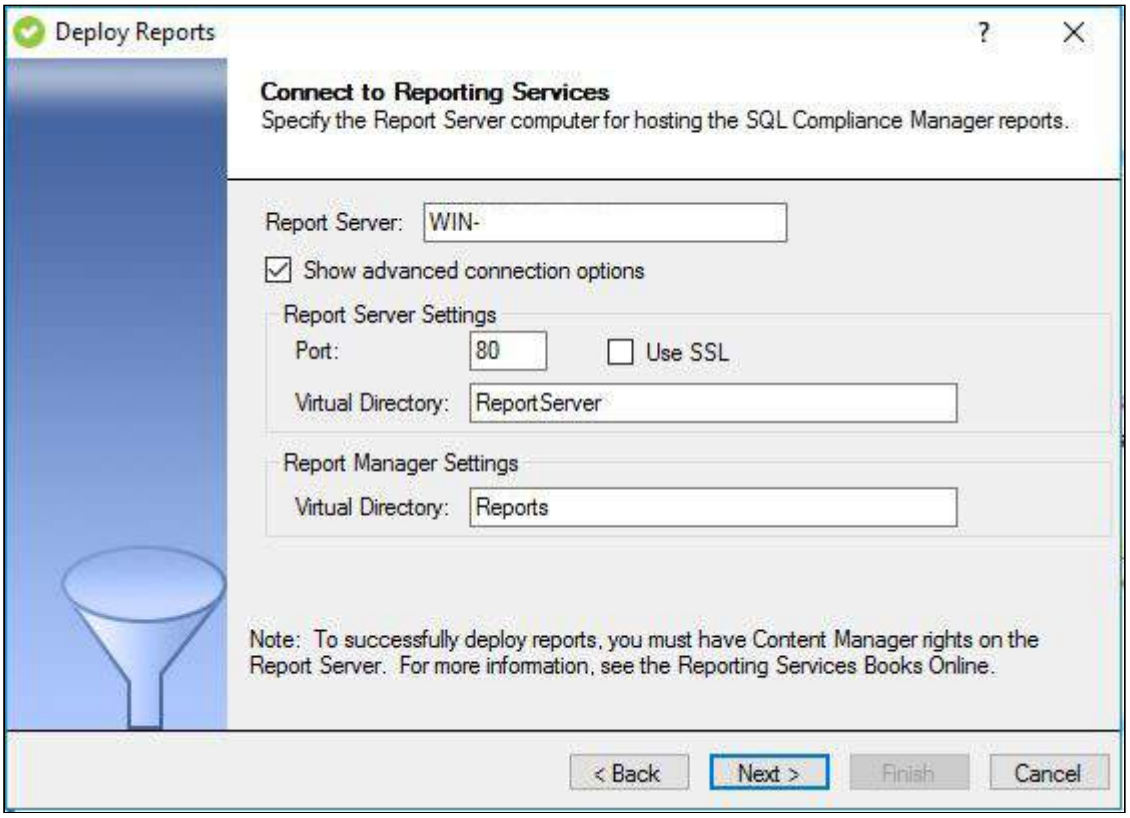


Deploy Reports wizard - Connect to Reporting Services tab

The Connect to Reporting Services tab of the Deploy Reports wizard allows you to specify the Report Server to which you want to deploy the IDERA 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.

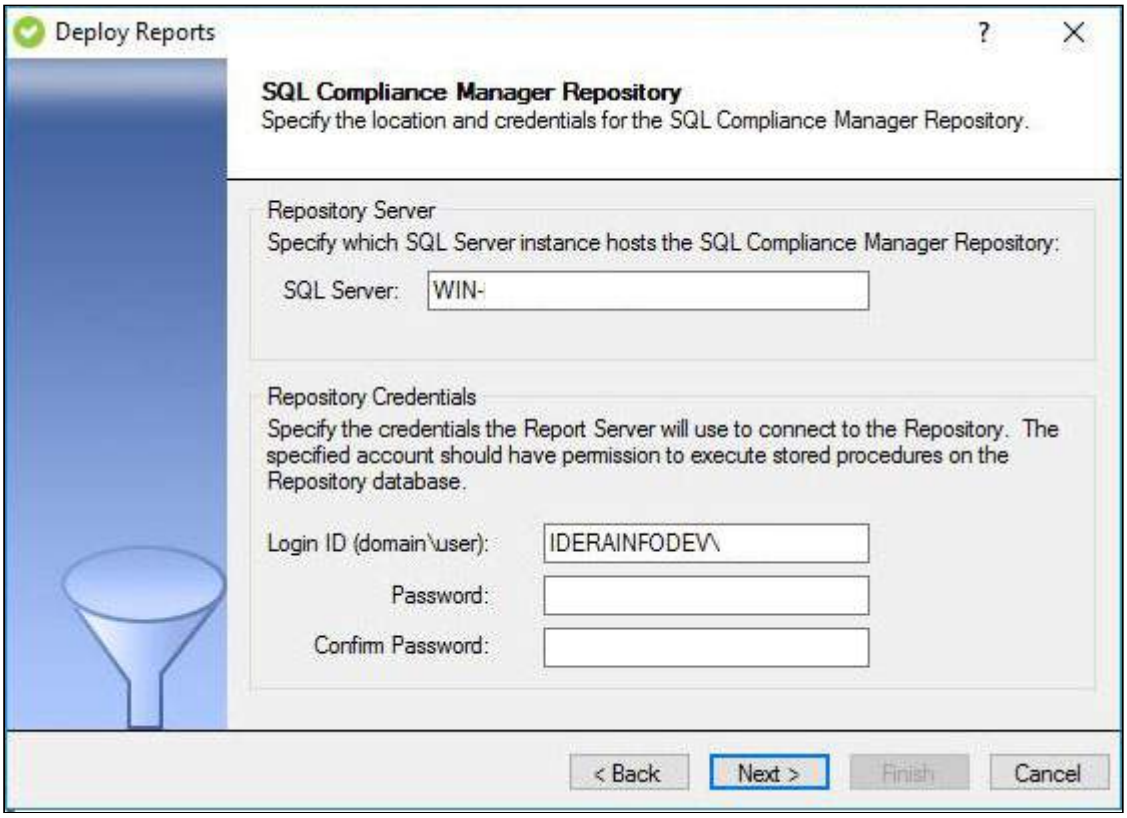
Click **Next** to continue.



Deploy Reports wizard - SQL Compliance Manager Repository tab

The SQL Compliance Manager Repository tab of the Deploy Reports wizard allows you to specify which Windows user account IDERA 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.

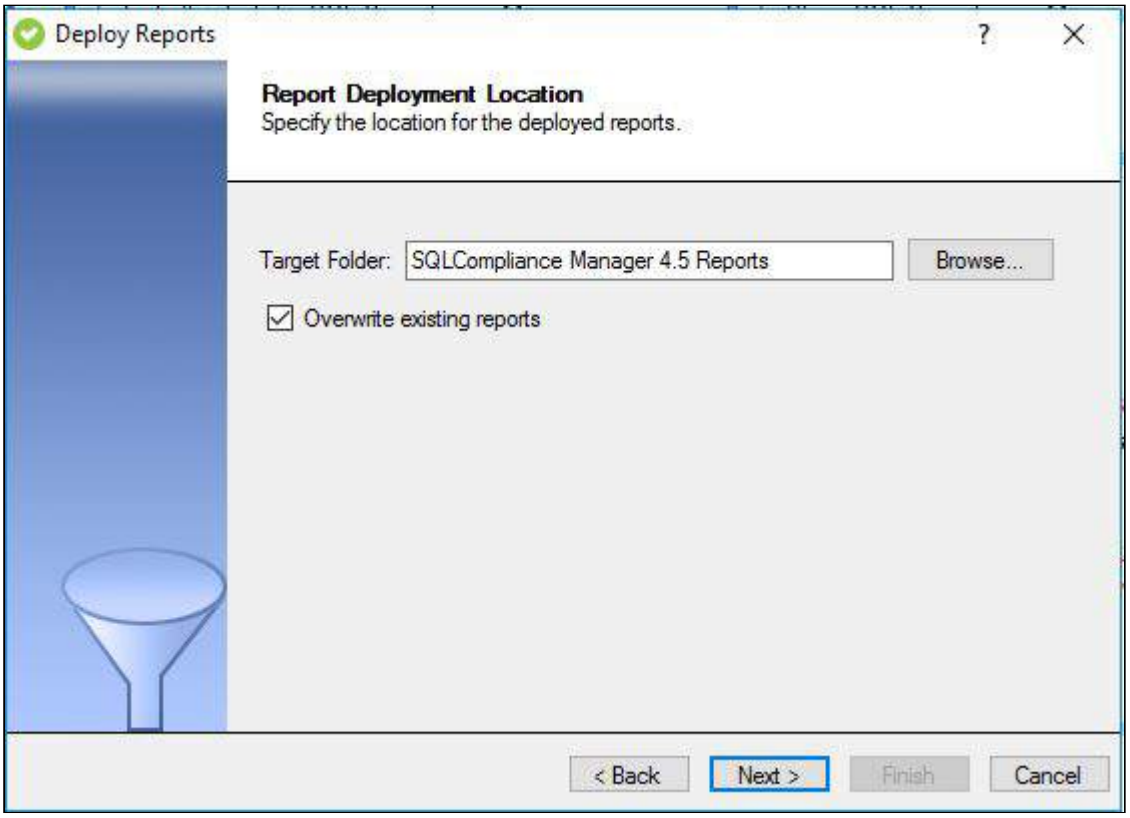
Specify the name of the SQL Server instance that hosts the Repository, enter the appropriate account credentials, and then click **Next**.



Deploy Reports wizard - Report Deployment Location tab

The Report Deployment Location tab of the Deploy Reports wizard 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.

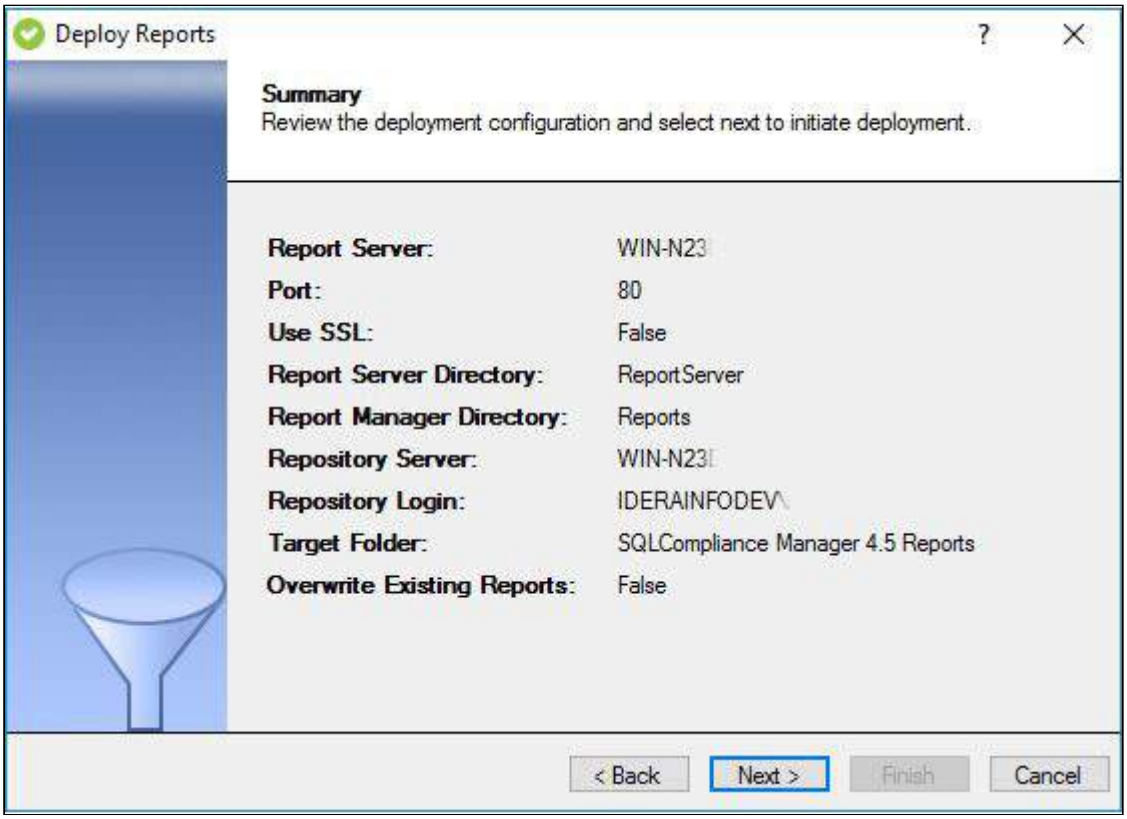
You can also specify whether you want to overwrite existing reports. By overwriting existing reports, you ensure all deployed reports are current. ***If you decide not to overwrite existing reports,*** the Deploy Reports wizard installs only the reports that are new or updated in this version of IDERA SQL Compliance Manager.



Deploy Reports wizard - Summary tab

Review the provided summary, and then click **Finish**. When you finish the Deploy Reports wizard, IDERA 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.



Test report deployment

Once you integrate IDERA SQL Compliance Manager reports into Microsoft Reporting Services, test your installation by loading Microsoft Reporting Services, and then generating each report. This step allows you to ensure that when you start generating reports, you get the results you anticipate.

For more information about 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 that the data source is 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.

9.2.7 Use reports to analyze trends over time

Use IDERA 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.

9.2.8 Use reports to establish and maintain compliance

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

Once compliance is established, SQL Compliance Manager Reports allow you to track activity and identify problems so that you can resolve these issues and maintain compliance. In addition to the ability to generate compliance reports on your SQL Server environment, you can also assign read-only access to SQL Compliance Manager to designated users so they can generate necessary reports.

9.2.9 Use report cards to track SQL Server activity

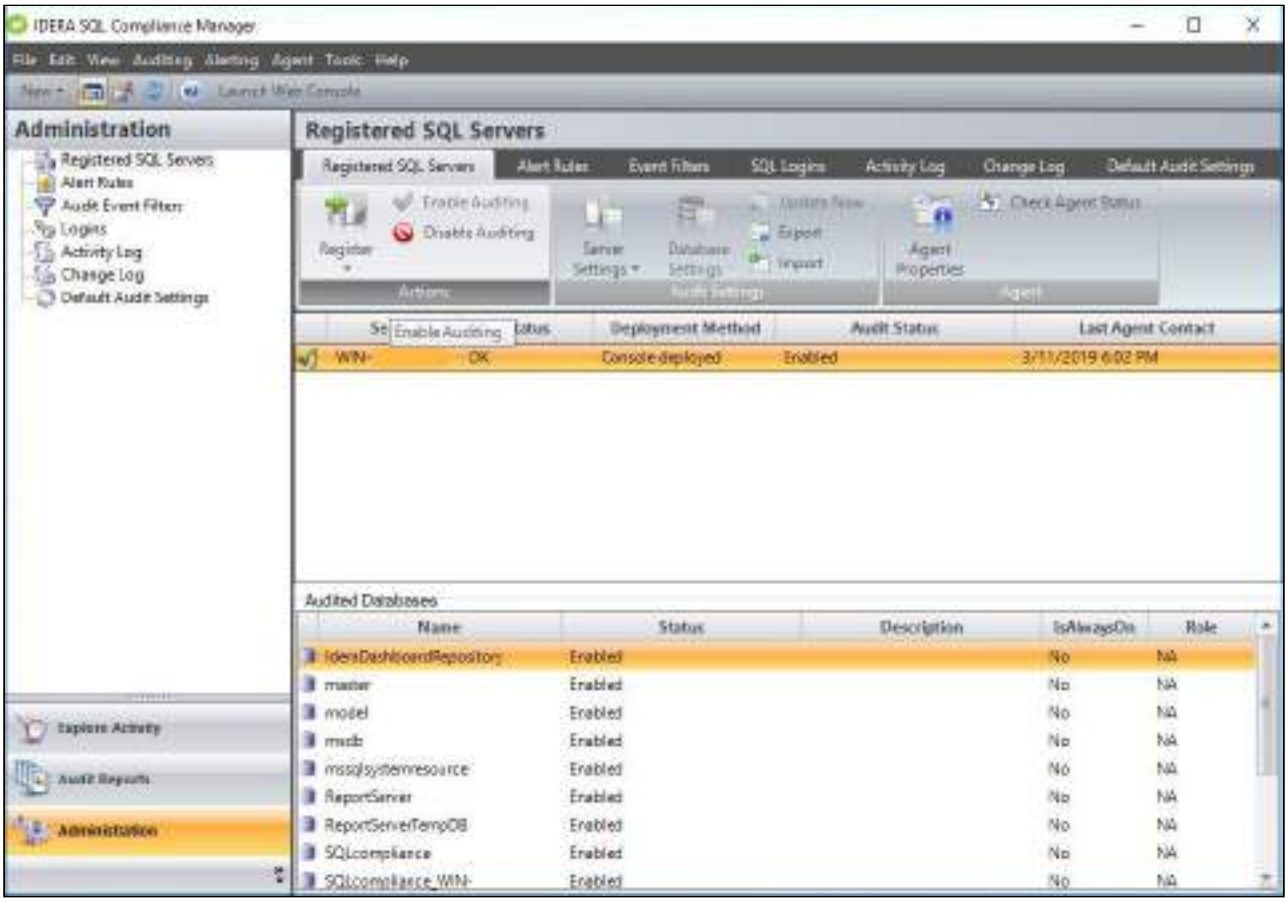
IDERA SQL Compliance Manager includes several Activity Report Cards that display up to 30 days of SQL Server activity. Activity Report Cards allow you to view the SQL Server activity at the enterprise and individual SQL Server instance levels. These report cards allow you to quickly check activity in each event category audited, view SQL Server activity statistics, and short-term activity trends. Use Activity Report Cards 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.

9.3 Administration View

The Administration view of SQL Compliance Manager allows users to control access to all the information that SQL Compliance Manager collects, letting users configure Alert Rules, Event Filters or the Default Audit Settings. In addition to controlling access, users can also configure Logins and view details of the captured data in the Activity Log and in the Change Log. Use the Administration view to help you keep track of key actions performed in your SQL Compliance Manager environment.



Visit the different options below to learn more about each of the Administration View tabs:

- Registered SQL Servers tab
- Alert on Audit Data and Status
- Event Filters
- SQL Logins tab
- Activity Log tab
- Change Log tab
- Default Audit Settings tab

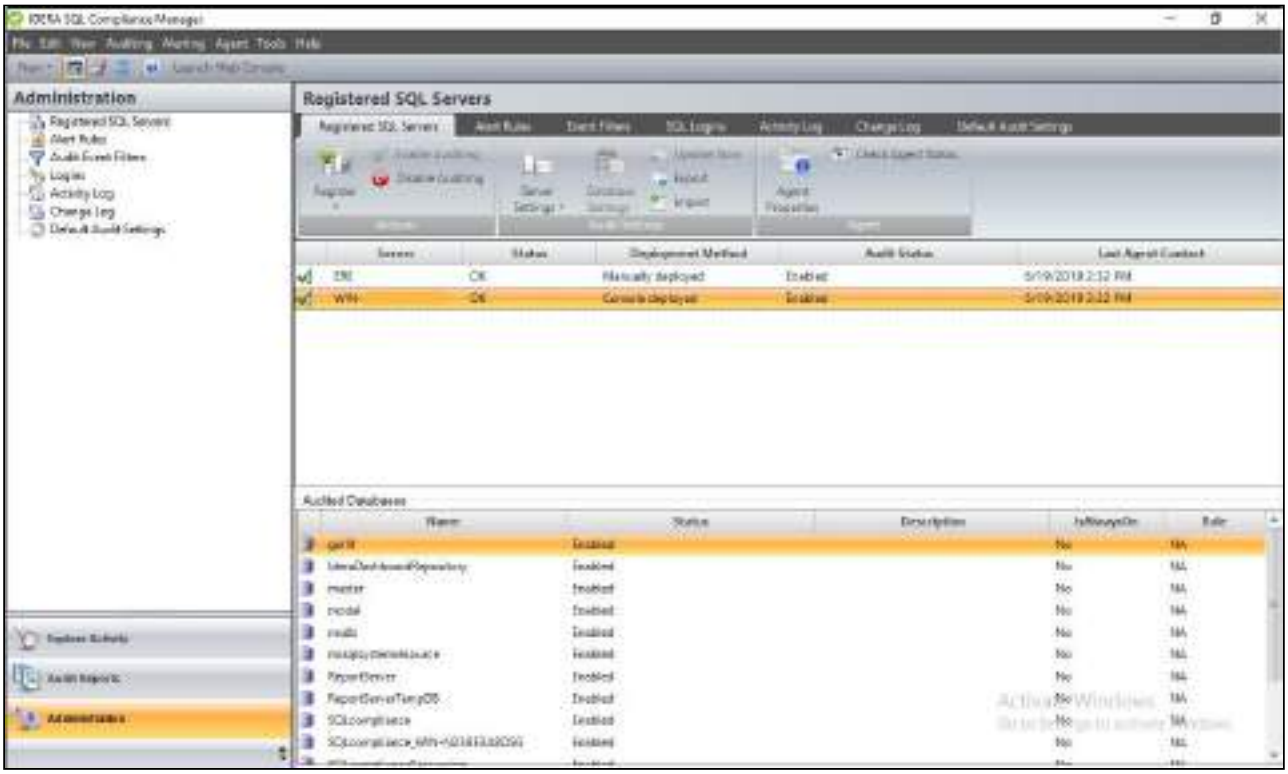
9.3.1 Registered SQL Servers tab

The Registered SQL Servers tab lists the SQL Server instances that are registered for IDERA 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 Compliance Manager. For more information, see Register a SQL Server.

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. For more information, see Add Audited Databases.

Enable Auditing

Allows you to enable auditing on the selected SQL Server instance. When you enable auditing, the SQL Compliance Manager Agent begins collecting events on the selected SQL Server instance, and sends the SQL trace files to the Collection Server. For more information, see Enable auditing on a SQL Server.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQL Compliance Manager 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. For more information, see Disable auditing on a SQL Server.

Server Settings for Audited Server Activities

Allows you to view and modify audit settings for the selected SQL Server instance. For more information, see Registered SQL Server Properties.

Server Settings for Privileged Users

Allows you to view and modify which privileged users are audited on the selected SQL Server instance. For more information, see Privileged User Auditing.

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. For more information, see Audited Database Properties.

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. For more information, see Audited Database Properties window - Trusted Users tab.

Update Now

Allows you to send your audit setting changes to the SQL Compliance Manager Agent immediately. Typically, the Collection Server sends audit setting updates at each heartbeat communication from the SQL Compliance Manager Agent. By default, a heartbeat occurs every five minutes. To view the SQL Compliance Manager Agent heartbeat details, use the General tab on the SQL Compliance Manager Agent Properties window.

Import

Allows you to import audit settings previously exported from another SQL Server instance or database. For more information, see Import your audit settings.

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. For more information, see Export your audit settings.

Collect Audit Data Now

Allows you to force the SQL Compliance Manager Agent to send trace files to the Collection Server for processing. Typically, the SQL Compliance Manager 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 SQL Compliance Manager Agent that is auditing the selected SQL Server instance. For more information, see SQL Compliance Manager Agent Properties.

Check Agent Status

Allows you to check the status of the SQL Compliance Manager Agent on the selected SQL Server instance, such as whether or not the agent is active. For more information, see Check the SQL Compliance Manager Agent status.

Deploy Agent

Allows you to deploy the SQL Compliance Manager Agent to one or more registered SQL Server instances. Deploying the agent installs the SQL Compliance Manager Agent Service on the target instance, and allows you to begin auditing events. For more information, see Deploy SQL Compliance Manager Agent wizard.

Upgrade Agent

Allows you to upgrade the SQL Compliance Manager 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. For more information, see Upgrade your deployed SQL Compliance Agents.

Change Agent Trace Directory

Allows you to specify a different trace directory for the SQL Compliance Manager 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 Compliance Manager also uninstalls the SQL Compliance Manager Agent. ***If you manually deployed the SQL Compliance Manager Agent***, you must manually uninstall it from the SQL Server computer.

If there are any backlogged audit trace files that you need to process for the instance you are considering to decommission, make sure to disable auditing and decommissioning your server only after processing these backlogged audit trace files. For additional information on how to process backlogged trace files, please contact Idera Support.

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 Compliance Manager displays an error.

If a system alert is 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.

Deployment Method

Indicates the agent deployment method for the selected SQL Server.

The values in this column can be: manually deployed, console deployed, and silent installer script.

Audit Status

Indicates whether auditing is enabled on the selected SQL Server instance. When auditing is disabled, the SQL trace is stopped and the SQL Compliance Manager Agent no longer collects events.

If a system alert is triggered, the Audit Status column instructs you to view the Activity Log to determine which event triggered this alert.

Last Agent Contact

Provides the date and time when the SQL Compliance Manager Agent last received audit setting updates from the Collection Server (also called a heartbeat). To view the SQL Compliance Manager Agent heartbeat details, use the General tab on the SQL Compliance Manager Agent Properties window.

9.3.2 Alert on Audit Data and Status

You can receive alerts when IDERA 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.

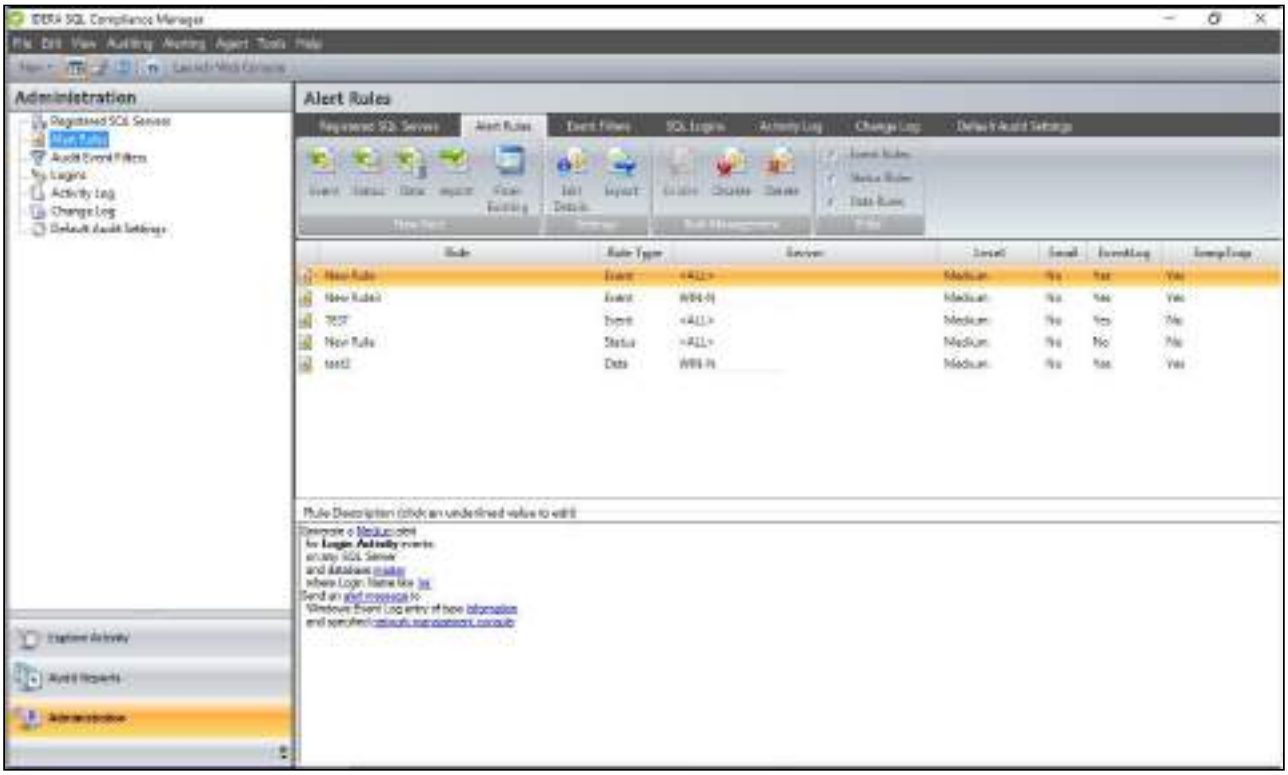
Status alerting checklist

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.

Alert Rules tab

The Alert Rules tab in IDERA 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. For more information, see Specify Alert Criteria.

New Event Alert Rule

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

Import Rules

Allows you to import alert rules previously exported from another SQL Server instance. By default, the imported alert rules are disabled. For more information. see Import your alert rules.

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 Compliance Manager stores the new alert rule in the Repository. The selected rule remains unchanged. For more information, see Use an alert rule as a template.

View Details

Allows you to view or change the alert criteria for the selected rule. For more information, see View alerts.

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. For more information, see Export your alert rules.

Enable Alert Rule

Allows you to enable the selected rule. When an alert rule is enabled, SQL Compliance Manager processes audited events using the selected criteria in this rule. ***If an event matches the alert criteria and an alert action is configured***, SQL Compliance Manager 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. For more information, see Enable an Alert.

Disable Alert Rule

Allows you to temporarily stop using the selected rule. SQL Compliance Manager 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. For more information, see Disable an Alert.

Delete

Allows you to permanently delete the selected rule. Deleting an alert rule removes the rule from the Repository. SQL Compliance Manager 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. For more information, see Groom Alerts.

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 Compliance Manager 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 Compliance Manager 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 Compliance Manager 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.

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 IDERA 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

Data you want to alert on ...	Type of Event Alert rule criteria to set ...
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

You can set IDERA SQL Compliance Manager to generate an event alert when it finds a suspicious event in your audit data. Alert rules define what a suspicious event is and how you want SQL Compliance Manager to respond. For example, create a rule to alert on DML events that occur on a sensitive database. 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 about customizing alerts, see Use Event Alerts to analyze audit data.

SQL Compliance Manager alerts only 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 SQL Compliance Manager Agent, the Collection Server uses the criteria defined by your alert rules to search for suspicious events. When the Collection Server finds a matching event, it triggers the alert. ***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 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 about aiding your system performance, see Groom alerts from Repository.

Create an Event Alert rule

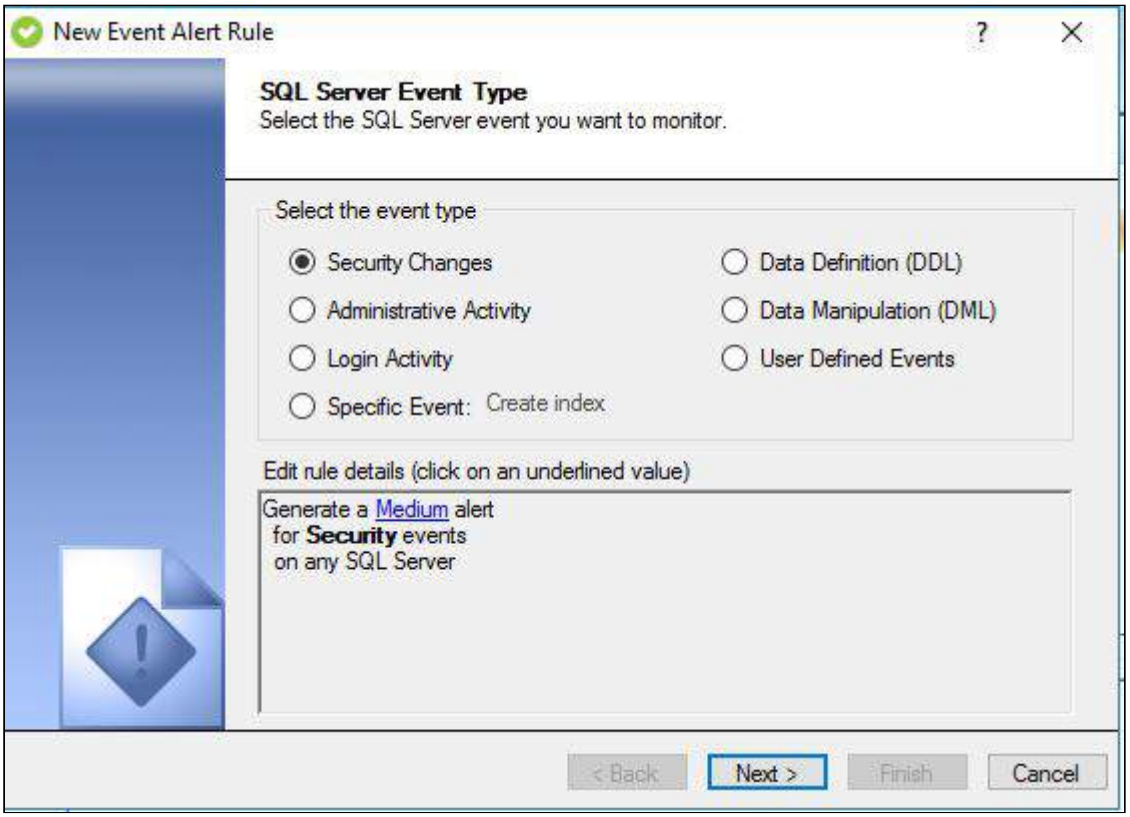
Creating an Event Alert rule allows you to begin generating alerts on audit data across your SQL Server environment. To successfully generate an alert, the alert rule criteria you select must match SQL Server event data you are currently auditing on the specified instance or database. For more information,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

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.

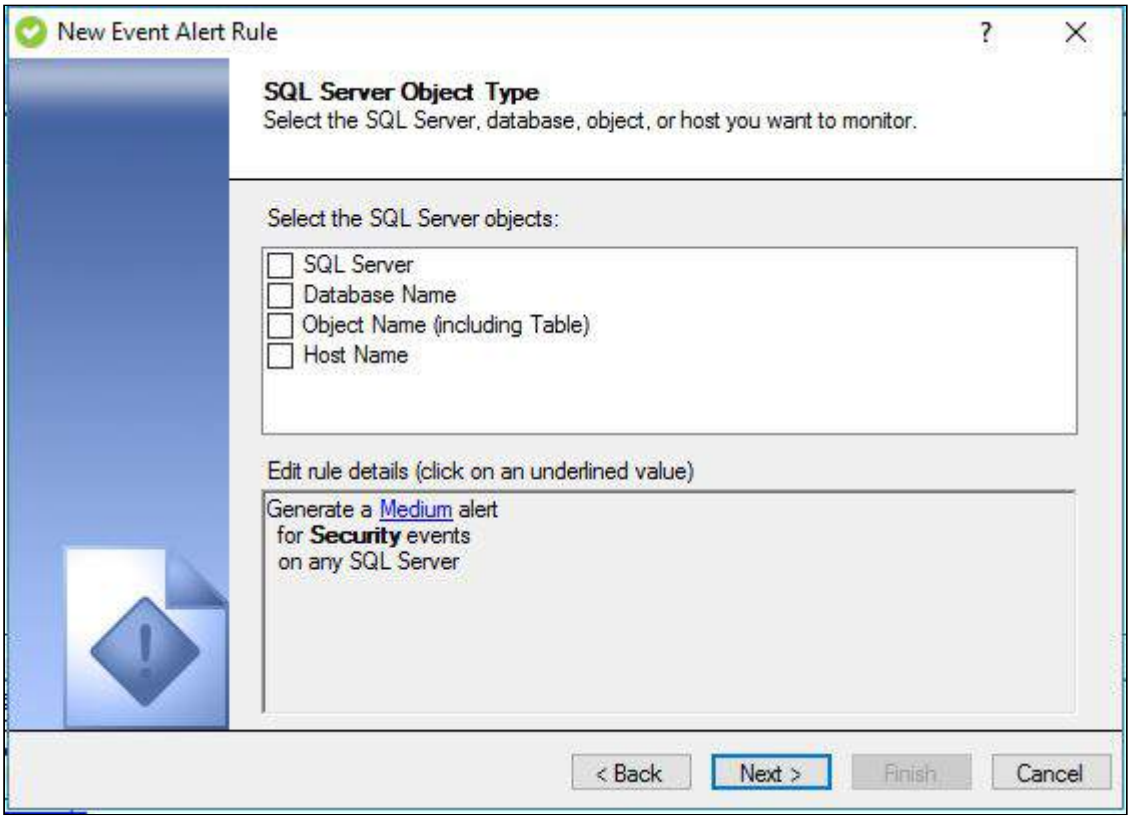
You can also select a specific event or a user defined event. A specific event can be any supported SQL Server event that occurs at the server or database level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

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

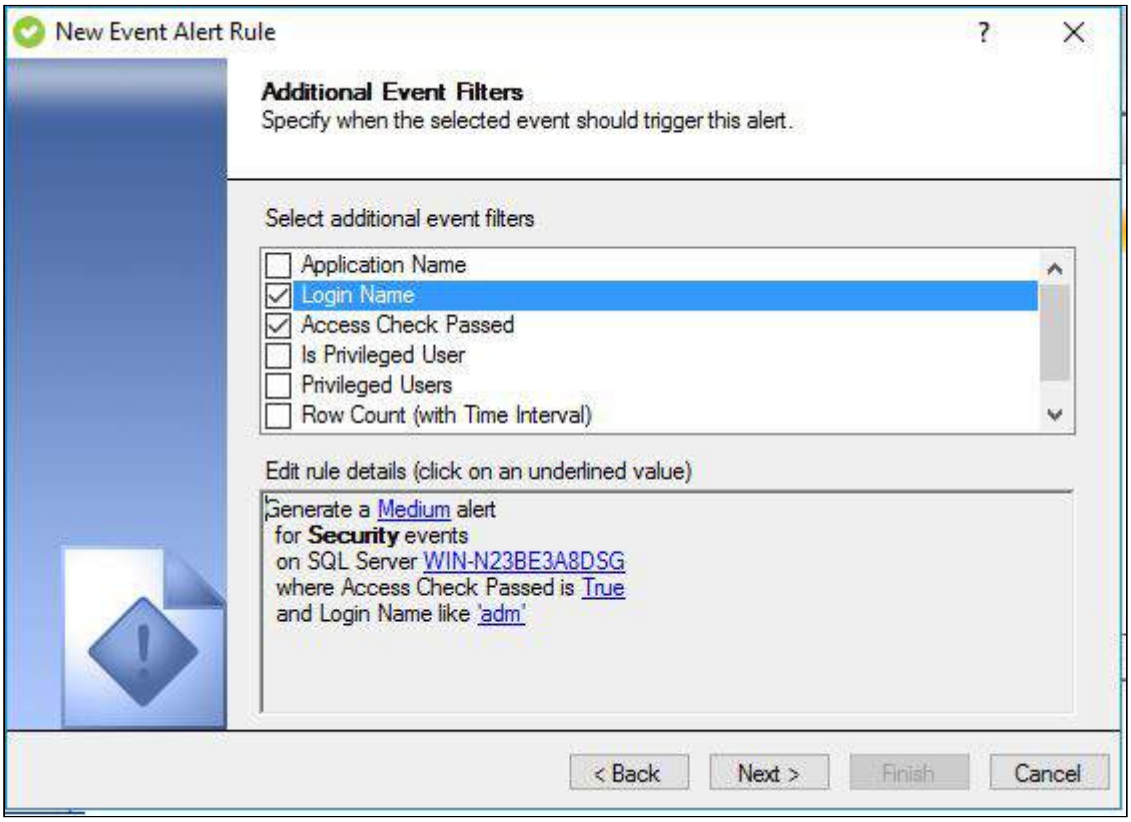
Edit rule details

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 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.

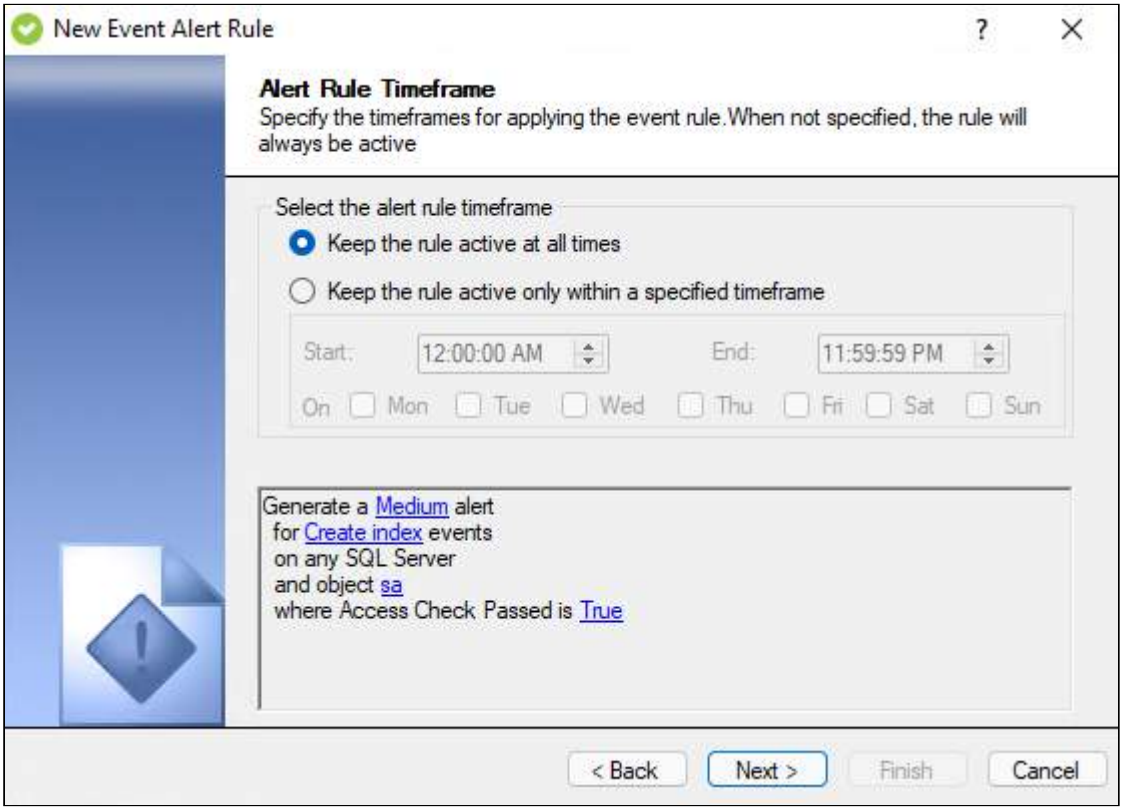
Edit rule details

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 Rule Timeframe tab

The Alert Rule Timeframe tab of the New Event Alert Rule wizard allows you to limit the number of times an alert is sent by generating alerts within a specified timeframe. Keep the rule active at all times, or choose specific days and times to keep the alert rule active within the specified timeframe.



Available actions

Select alert rule timeframe

Allows you to select a specific timeframe for applying the event alert rules.

- **Keep the rule active at all times -** Select this option to apply the event alert rule at all times.
- **Keep the rule active only within a timeframe -** Select this option to specify a timeframe for the alert rule to be enabled. Use the options below to specify the **Start** and the **End** timeframes as well as specific days of the week for the alert rule to be active.

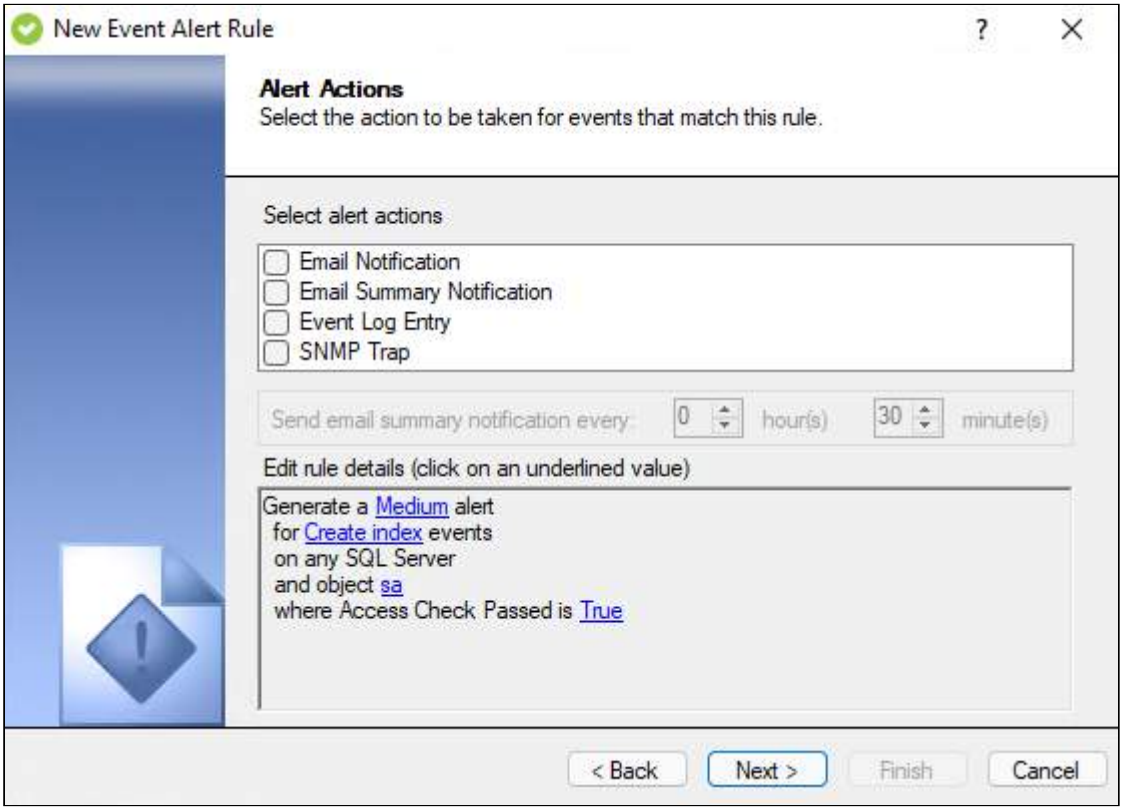
Edit rule details

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 grow 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 of the New Event Alert Rule wizard 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, IDERA SQL Compliance Manager writes an alert message to the application event log and emails 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. In addition, you can also specify how often to receive email alert notifications with a summarized list of the accumulated alerts that occurred between the selected interval timeframes.

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. The following are the available alert actions:

- **Email Notification** - Receive an email notification for every event that matches the configured alert rule.
- **Email Summary Notification** - Receive an email with a summarized list of the accumulated alerts and limit the number of notifications you get by setting up a time interval to receive email notifications.
- **Event Log Entry** - Writes the alert message as an event log entry in the application event log.
- **SNMP Trap** - Receive the alert notification as an SNMP Trap
- **Send email summary notification every** - Set up a time interval of up to 24 hours to receive email summary notifications.

> **Note**
>
> The Email Summary Notification feature requires the previous installation of the Task Scheduler service. The Task Scheduler service comes installed in Windows Server 2003, Windows XP, Windows 2000, Windows Vista, and Windows Server 2008.

Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

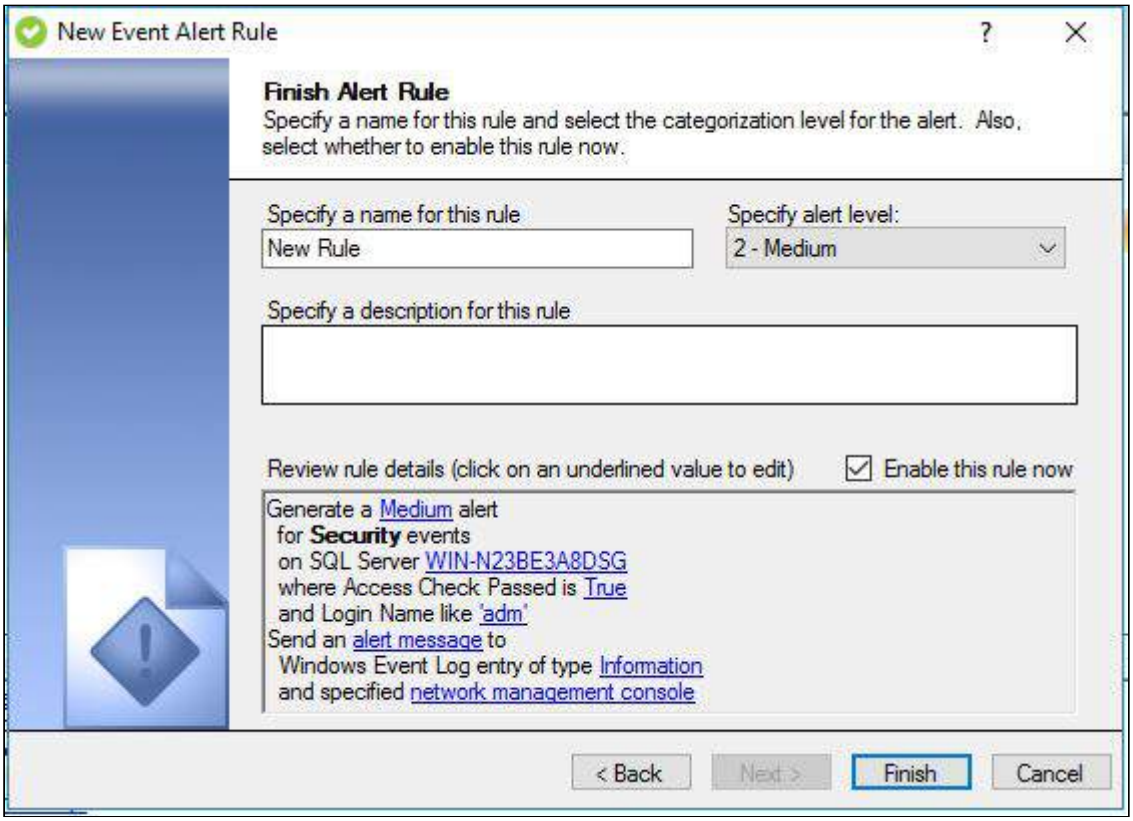
- **Email Notification** - Addresses to which the alert message should be emailed.
- **Email Summary Notification** - Addresses to which the summarized list of alert messages should be emailed at the previously specified time interval.
- **Event Log Entry** - Type of event log entry that should be written (Warning, Error, Information).
- **SNMP Trap** - Content of the alert message.

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 grow to include these additional settings. To edit previously set criteria, click the corresponding setting.

New Event Alert Rule wizard - Finish Alert Rule tab

The Finish Alert Rule tab of the New Event Alert Rule wizard 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, IDERA 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 Compliance Manager 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.

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**.

Change which event triggers the alert

Based on the criteria defined in your alert rules, IDERA 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.

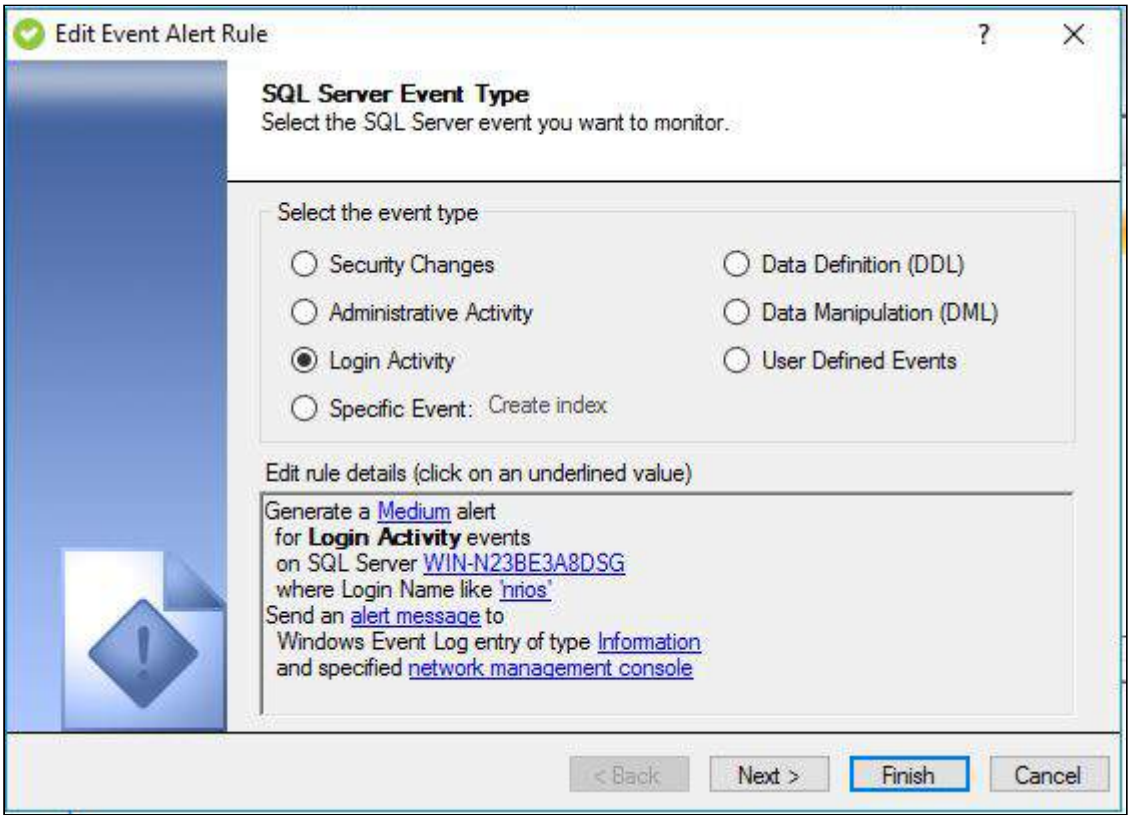
You can change the type of audit data that triggers an alert. For example, you can alert on a different event type or a different database. You can also copy an existing alert rule and use it as a template to create a new rule. For more information, see Use an alert rule as a template.

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**.

Edit Event Alert Rule wizard - SQL Server Event Type tab

The SQL Server Event Type tab of the Edit Event Alert Rule wizard 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 triggers 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.

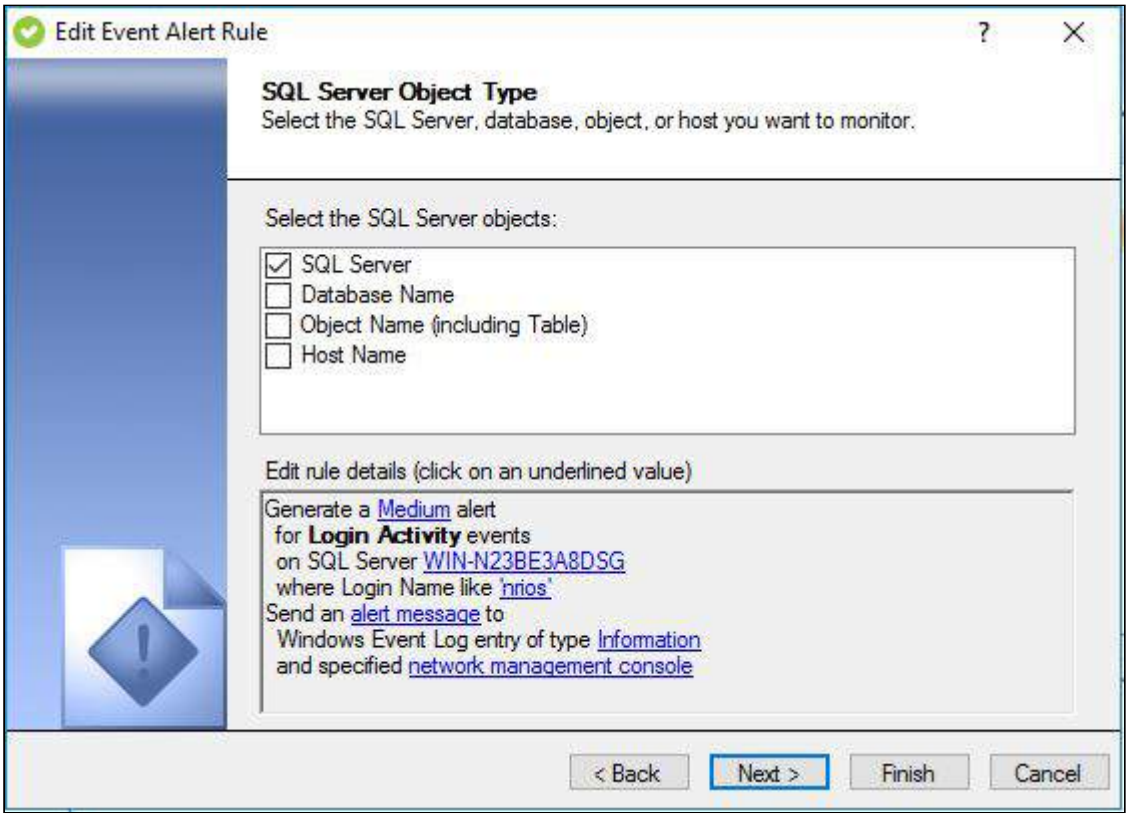
You can also select a specific event or a user-defined event. A specific event is any supported SQL Server event that occurs at the server or database level. A user-defined event is a custom event created and tracked using the `sp_trace_generateevent` stored procedure.

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

The SQL Server Object type tab of the Edit Event Alert Rule wizard 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

Type of Object	You can specify ...
Host Name	• Any host name • A specific host name

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

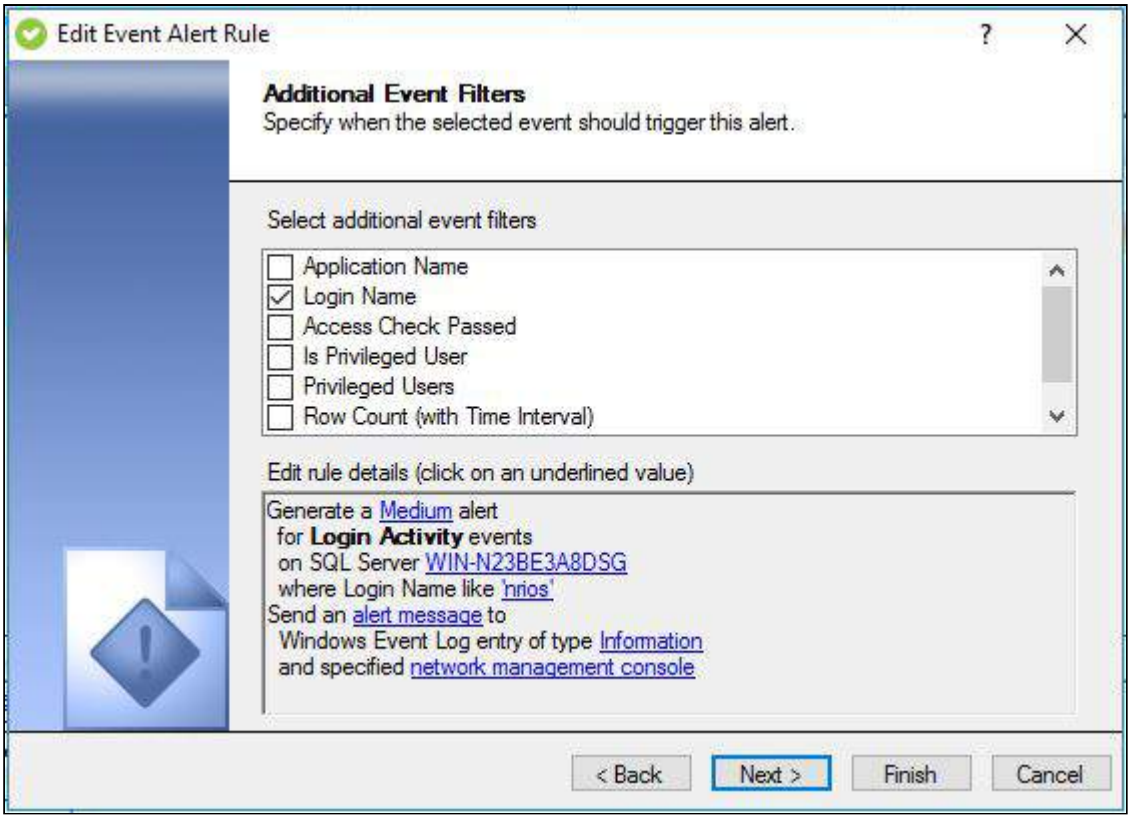
Edit rule details

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 Alert Rule wizard - Additional Event Filters tab

The Additional Event Filters tab of the edit Event Alert Rule wizard 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

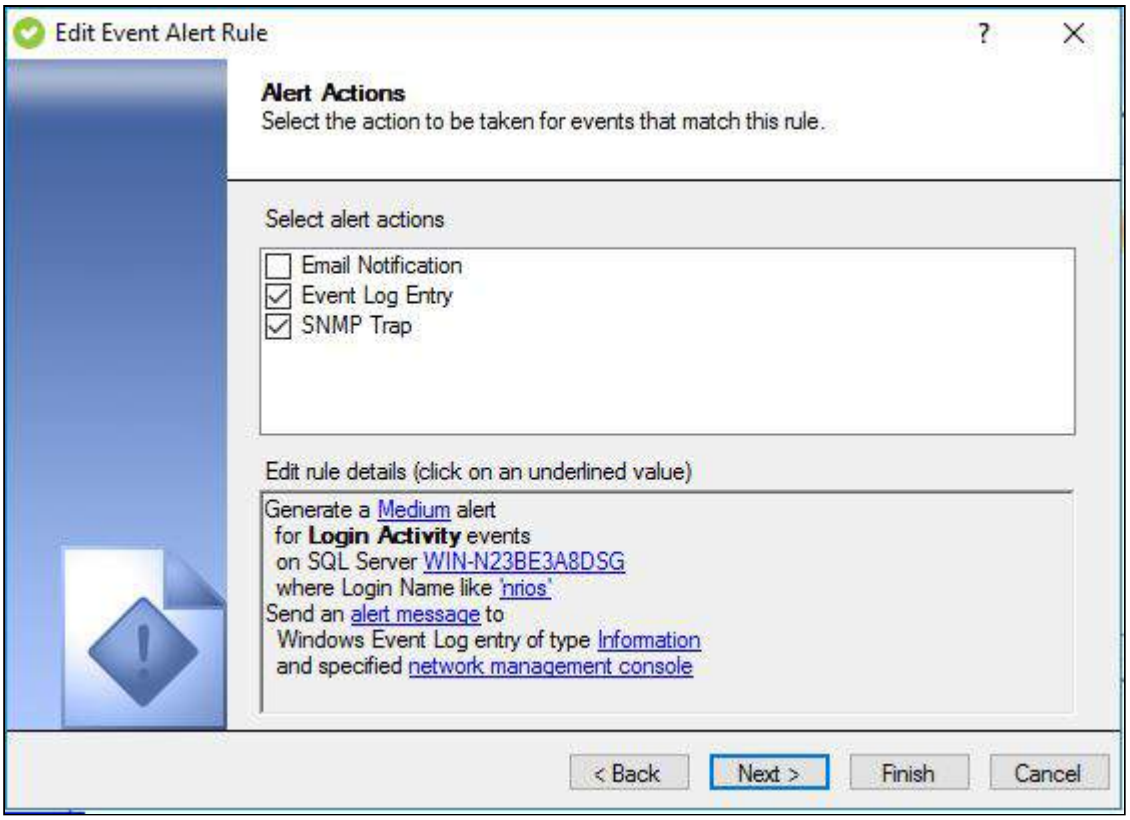
Allows you to specify a value for the selected condition, such as true or false.

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

The Alert Actions tab of the Edit Event Alert Rule wizard 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, IDERA 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 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

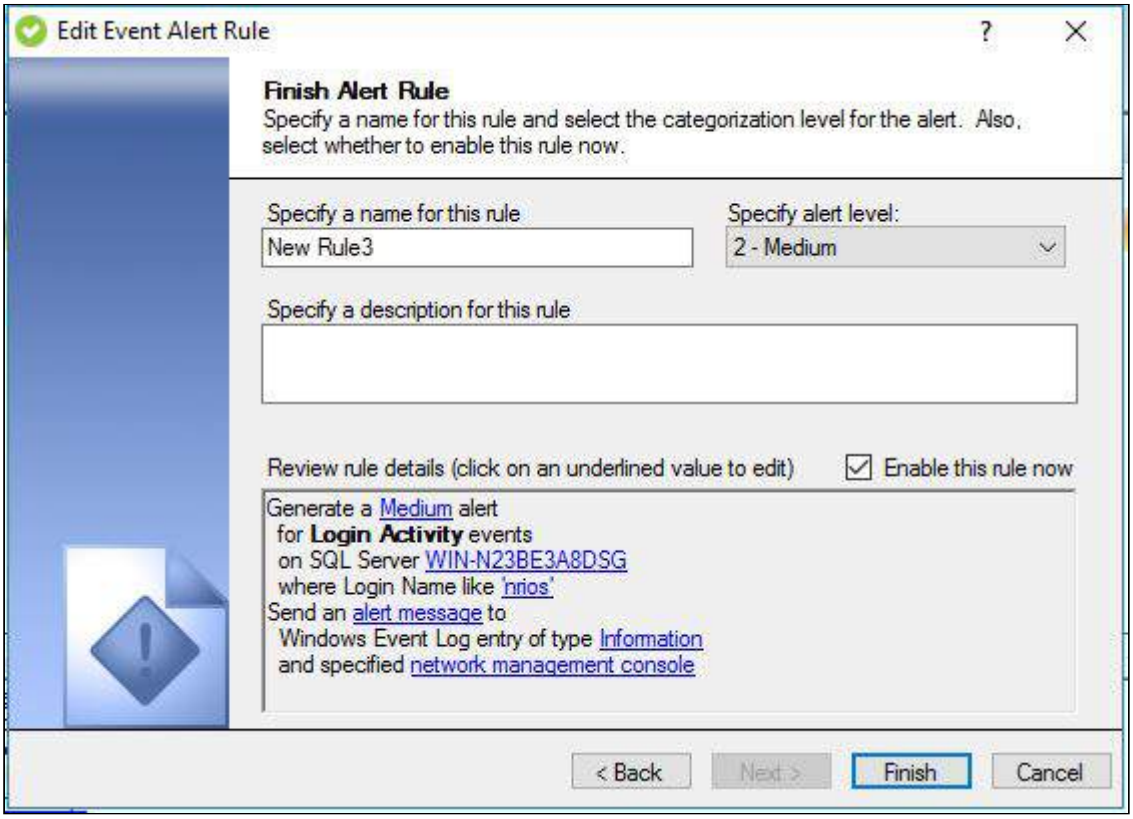
Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- 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 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**. IDERA 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 Compliance Manager 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.

Use Status Alerts to ensure compliance

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

- Confirm that your SQL Server instances are available to be audited.
- Ensure the SQL Compliance Manager 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 is consumed.

Status Alerts best practices

Alert	What it means	What is the risk	What might be wrong
Agent cannot connect to audited instance	The SQL Compliance Manager 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 are not applied to the SQL trace that is collecting events, and you will fail to collect the events you want. SQL Server continues to write trace files to the SQL Compliance Manager Agent trace directory, but the agent cannot send these files to the Collection Server. When the trace directory is full, auditing ceases, impacting SQL Server performance. ***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 automatically stops.	• The audited SQL Server instance may be offline or unable to respond. • The SQL Compliance Manager 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 SQL Compliance Manager Agent within the specified heartbeat interval.	Auditing is not immediately affected by this issue; however, you cannot apply updated audit settings. Trace files continue to queue in the trace file directory until the SQL Compliance Manager Agent Service is able to send these trace files to the Collection Server.	• The computer hosting the SQL Compliance Manager Agent may be offline. • Network firewall settings may be blocking communication between the SQL Compliance Manager Agent and the Collection Server. • The SQL Compliance Manager Agent may be stopped.

Alert	What it means	What is the risk	What might be wrong
Agent trace directory reached size limit	The trace directory folder on the SQL Server computer where the SQL Compliance Manager 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 SQL Compliance Manager Agent ceases auditing the target instances. The SQL traces stop, 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 SQL Compliance Manager Agent from sending the trace files. • Network firewall settings may be blocking communication between the SQL Compliance Manager 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.

Alert	What it means	What is the risk	What might be wrong
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 SQL Compliance Manager Agent trace directory to fill as the trace files queue up to be sent. When the SQL Compliance Manager Agent trace directory reaches its specified maximum size, the agent will cease auditing the target instances. The SQL traces stop, and no subsequent events are collected.	• You can manually stop the Collection Service and prevent trace file processing. • The Collection Service may be unable to access the Repository due to inadequate permissions or an offline Repository database. • 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.

Alert	What it means	What is the risk	What might be wrong
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

IDERA SQL Compliance Manager can generate a Status Alert when it receives a status update from the Collection Server or SQL Compliance Manager 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
- alerts that track the SQL Compliance Manager Agent status

In general, when the Collection Server or SQL Compliance Manager 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 five-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

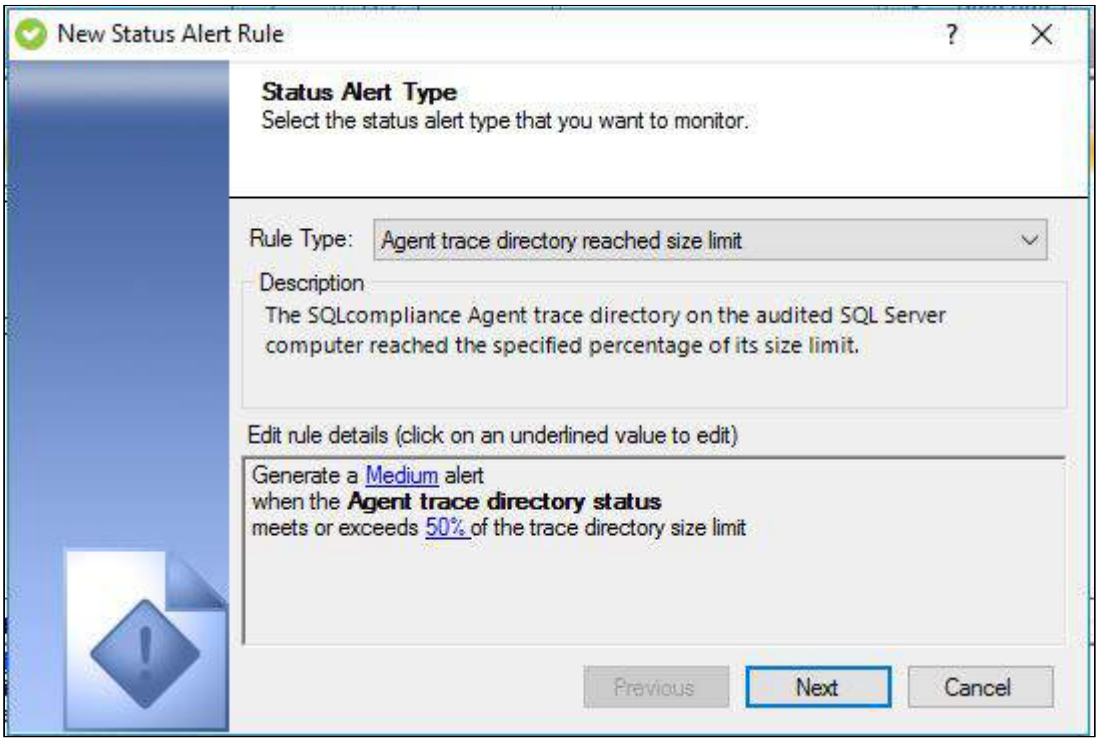
Creating a Status Alert rule allows you to proactively identify potential issues in your IDERA SQL Compliance Manager deployment that could disrupt your ability to continue auditing. For more information, see Use Status Alerts to ensure compliance.

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.

New Status Alert wizard - Status Alert Type tab

The Status Alert Type tab of the New Status Alert wizard allows you to choose the type of IDERA 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.

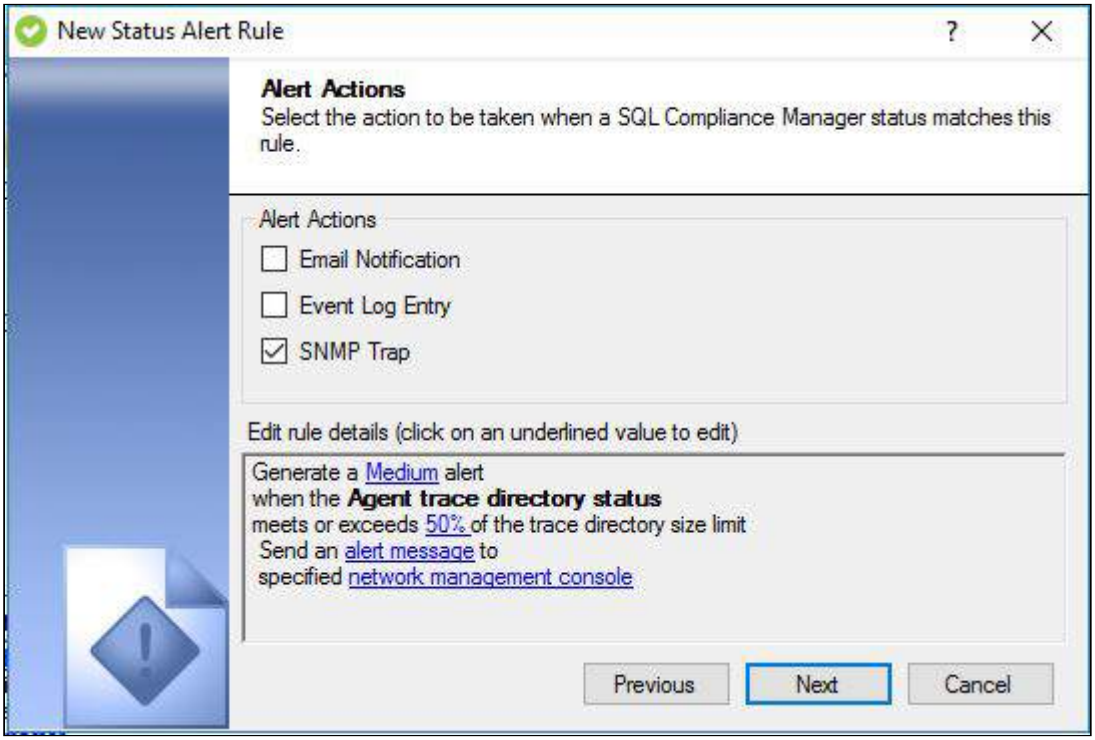
Edit rule details

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.

New Status Alert wizard - Alert Actions tab

The Alert Actions tab of the New Status Alert wizard allows you to select the action you want this alert rule to perform when the IDERA SQL Compliance Manager status 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 Compliance Manager is configured to connect to your mail server. For more information about using email notifications, 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:

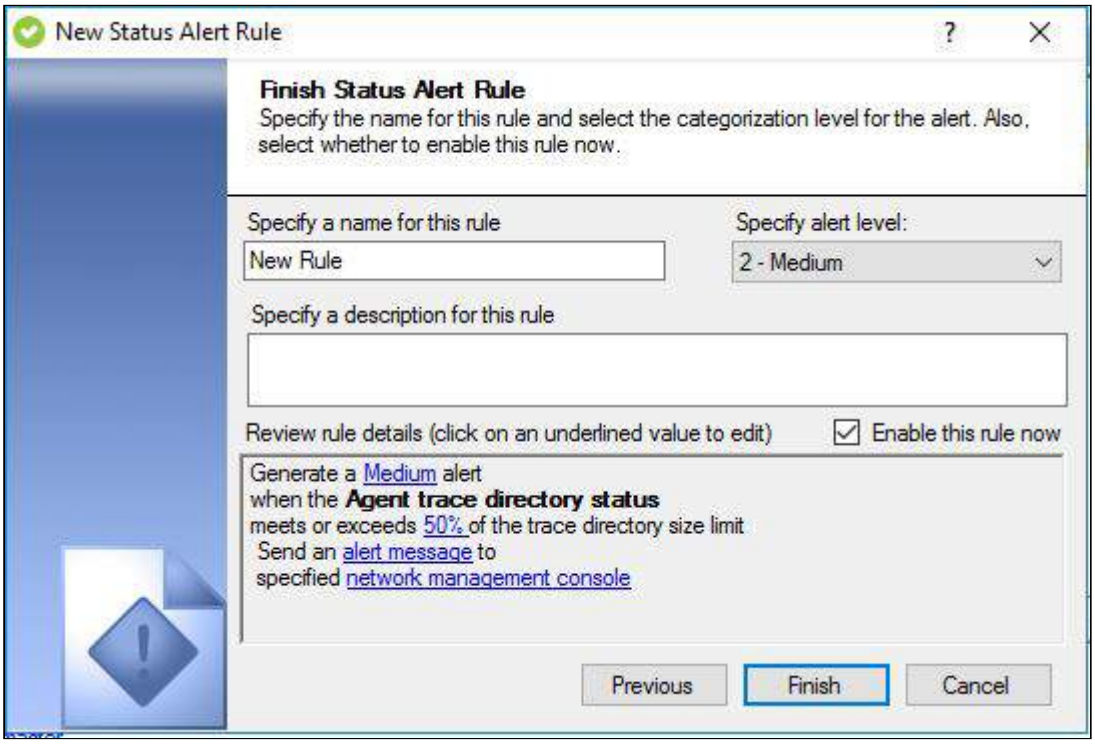
- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed

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 of the New Status Alert wizard allows you to specify a name for the new alert rule, review the rule details, and then click **Finish**. When you finish this wizard, IDERA 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

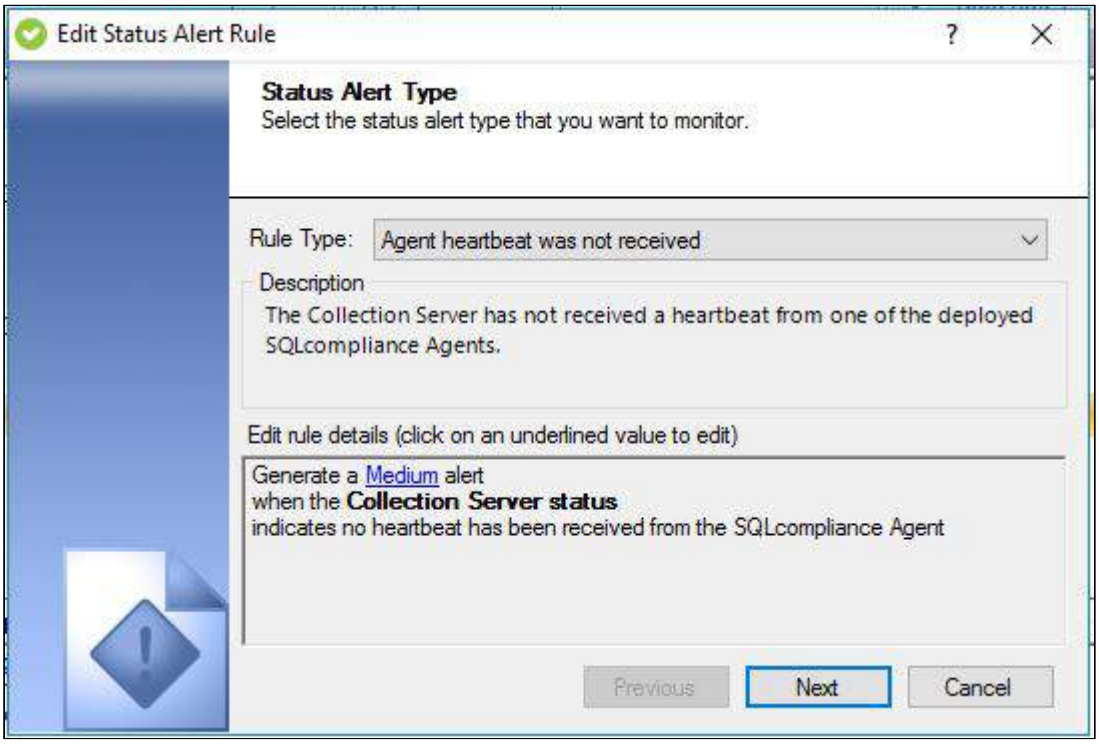
Indicates that you want SQL Compliance Manager to begin monitoring the product component status using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

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.

Edit Status Alert wizard - Status Alert Type tab

The Status Alert Type tab of the Edit Status Alert wizard allows you to change the type of IDERA 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.

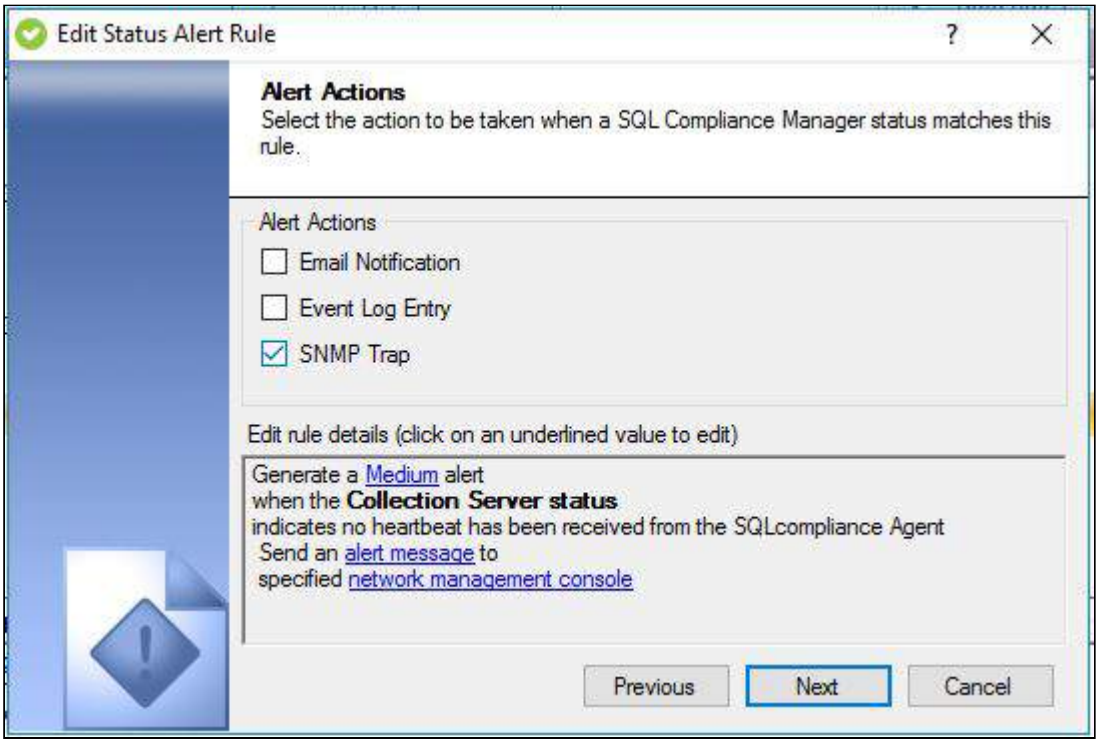
Edit rule details

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.

Edit Status Alert wizard - Alert Actions tab

The Alert Actions tab of the Edit Status Alert wizard allows you to change the action you want this alert rule to perform when the IDERA SQL Compliance Manager status 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 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

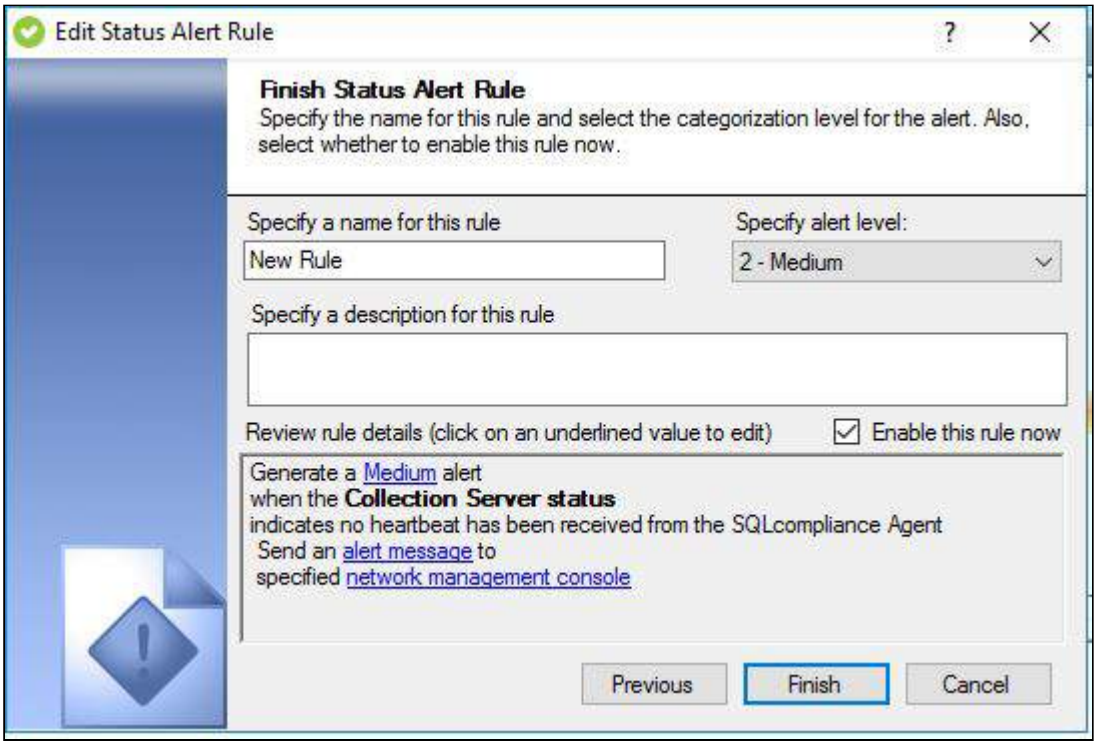
Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- 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 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

Using the Finish Status Alert Rule tab of the Edit Status Alert wizard, specify a name for the different alert rule, review the rule details, and then click **Finish**. When you finish this wizard, IDERA 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 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.

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, IDERA 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.

How Data Alerts work

IDERA 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 SQL Compliance Manager 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

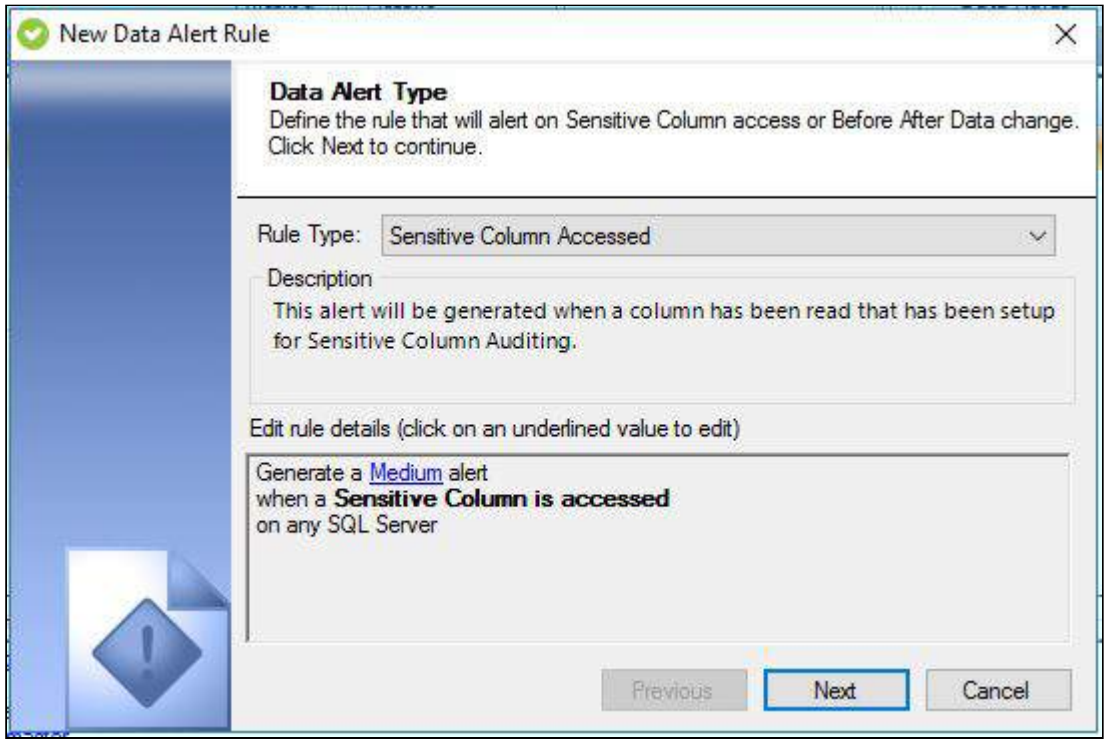
Creating a Data Alert rule allows you to begin generating alerts on audit data across your SQL Server environment. To successfully generate an alert, the alert rule criteria you select must match SQL Server event data you are currently auditing on the specified instance or database. For example, to alert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

New Data Alert Rule wizard - Data Alert Type tab

The Data Alert Type tab of the New Data Alert Rule wizard allows you to start setting up an alert that tracks when someone accesses a sensitive column.



Available actions

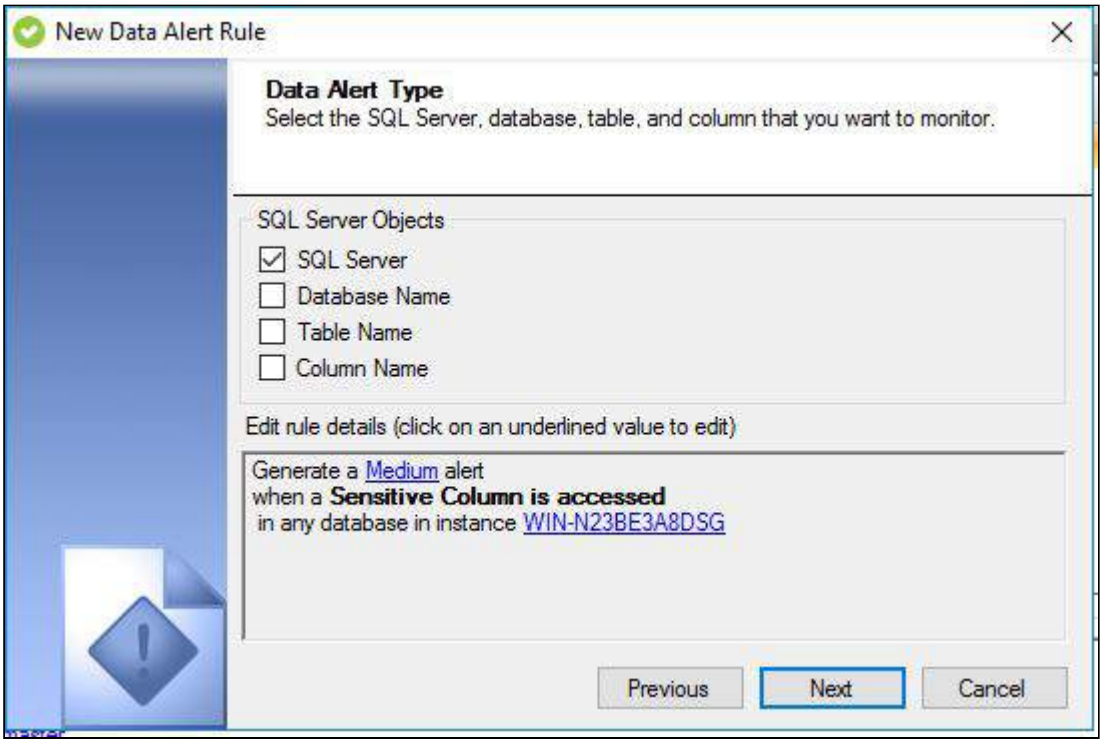
Edit rule details

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 - SQL Server Object Type tab

The SQL Server Object Type tab of the New Data Alert Rule wizard 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 IDERA 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

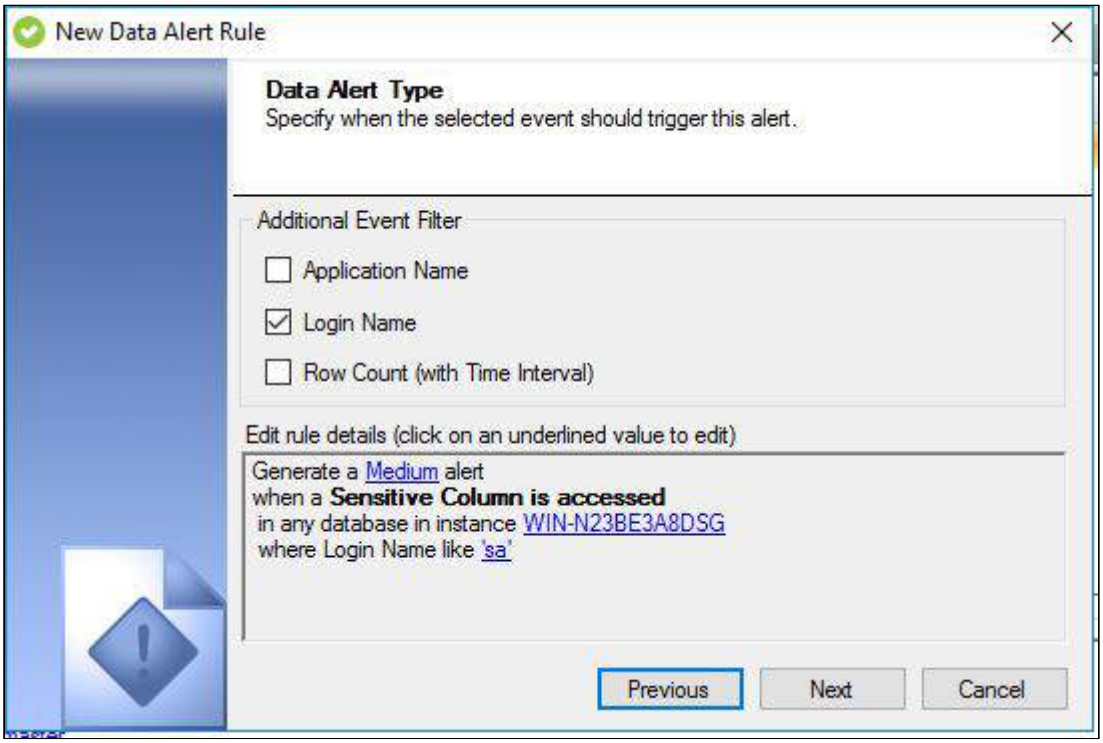
Edit rule details

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 Data 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 an Application Name, Login Name or by Row Count.

Edit rule details

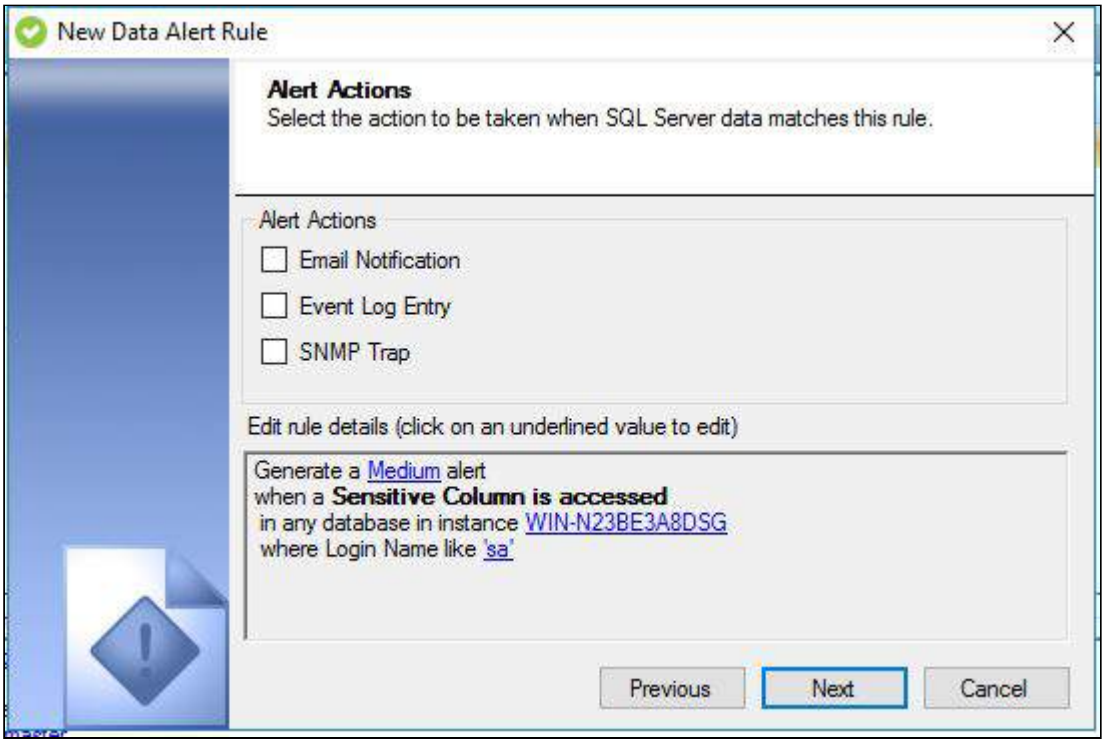
Allows you to specify a value for the selected condition, such as true or false.

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 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 - 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, IDERA 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 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, emailed to a specific address or distribution list, or send SNMP Trap messages to a specified network management console. SQL Compliance Manager 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:

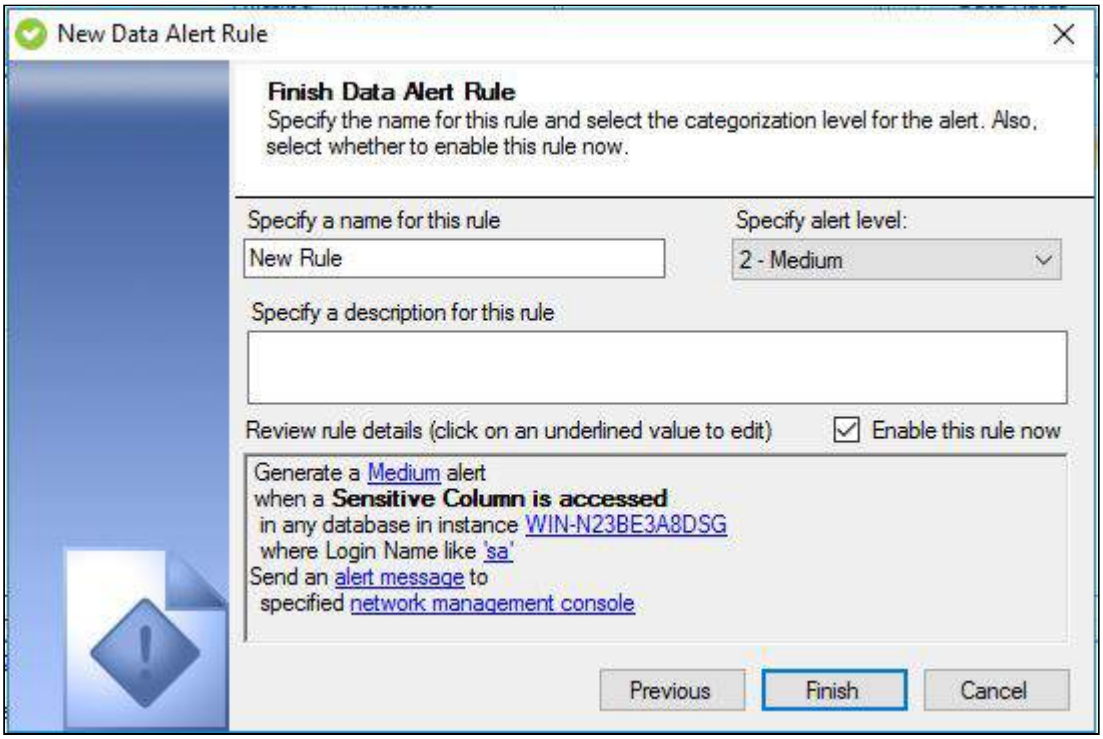
- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)
- Addresses to which the alert message should be emailed
- Server address, port number, and community name of the network management console

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 - 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, IDERA 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 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

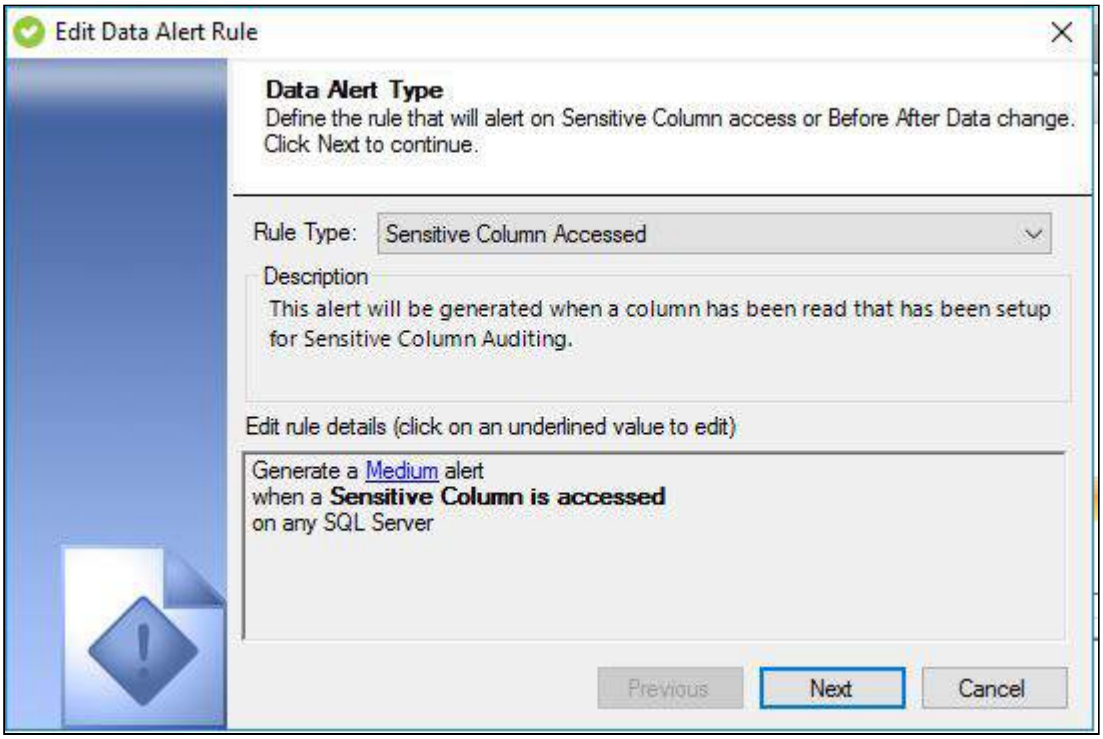
Indicates that you want SQL Compliance Manager to begin monitoring audit data using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.

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 - Data Alert Type tab

The Data Alert Type tab of the Edit Data Alert Rule wizard allows you to change the criteria of this alert rule by editing its parameters in the **Edit rule details** pane.



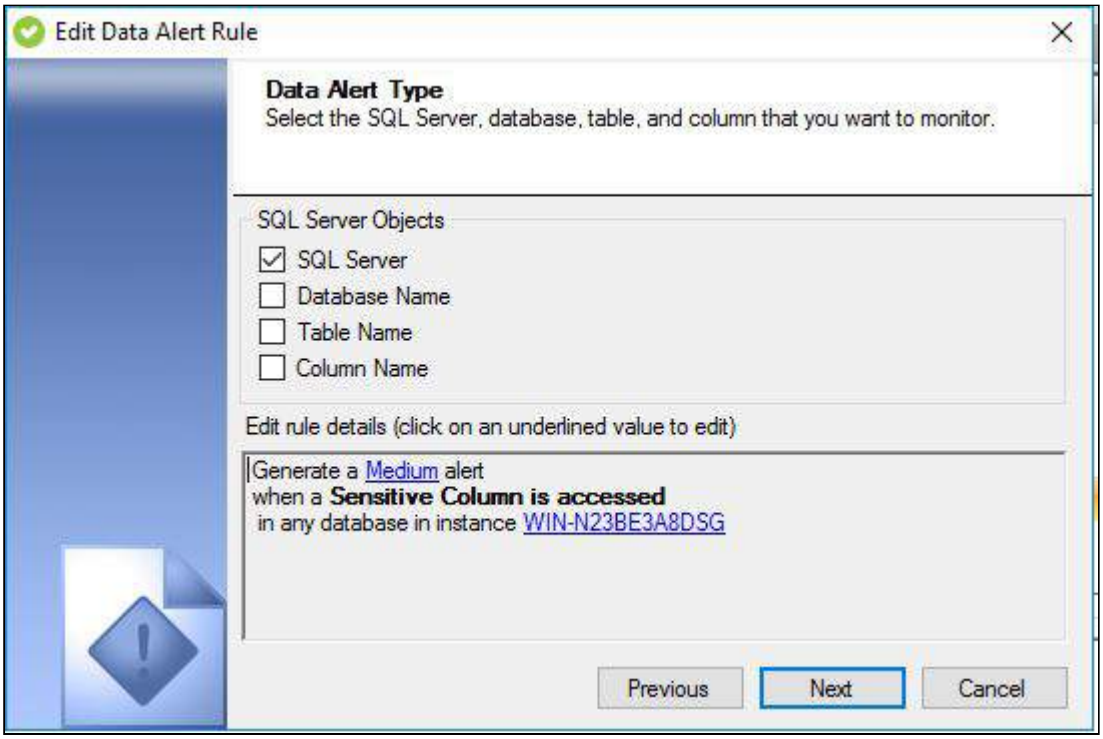
Available actions

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 - SQL Server Object Type tab

The SQL Server Object Type tab of the Edit Data Alert rule wizard 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 IDERA 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

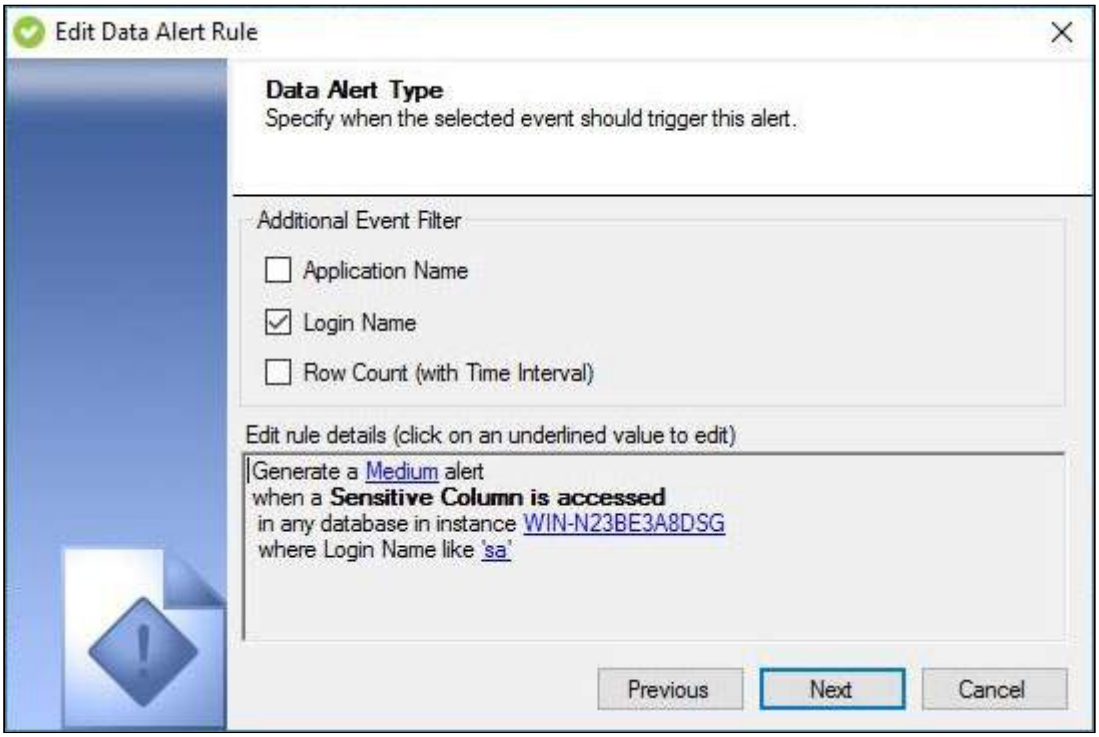
Allows you specify which SQL Server objects the alert rule should use to identify audit data to alert on.

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 Data Alert Rule wizard - Additional Event Filters tab

The Additional Event Filters tab of the edit Event Alert Rule wizard 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.

Edit rule details

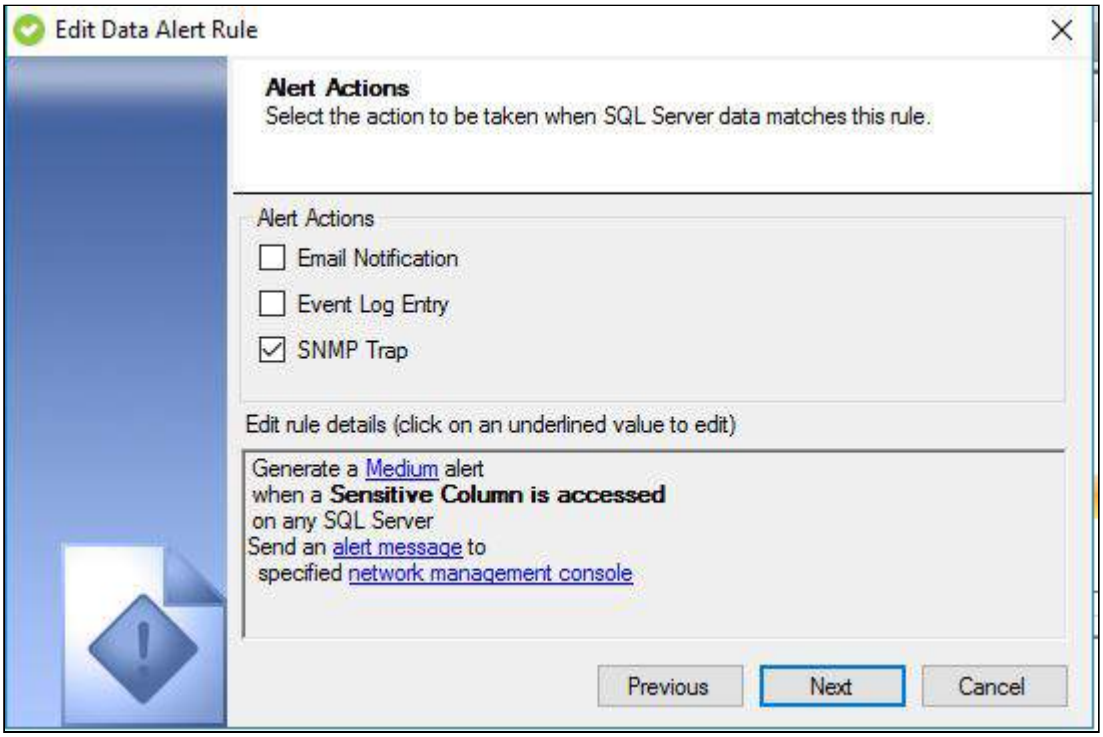
Allows you to specify a value for the selected condition, such as true or false.

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 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 - Alert Actions tab

The Alert Actions tab of the Edit Data Alert Rule wizard 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, IDERA 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 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

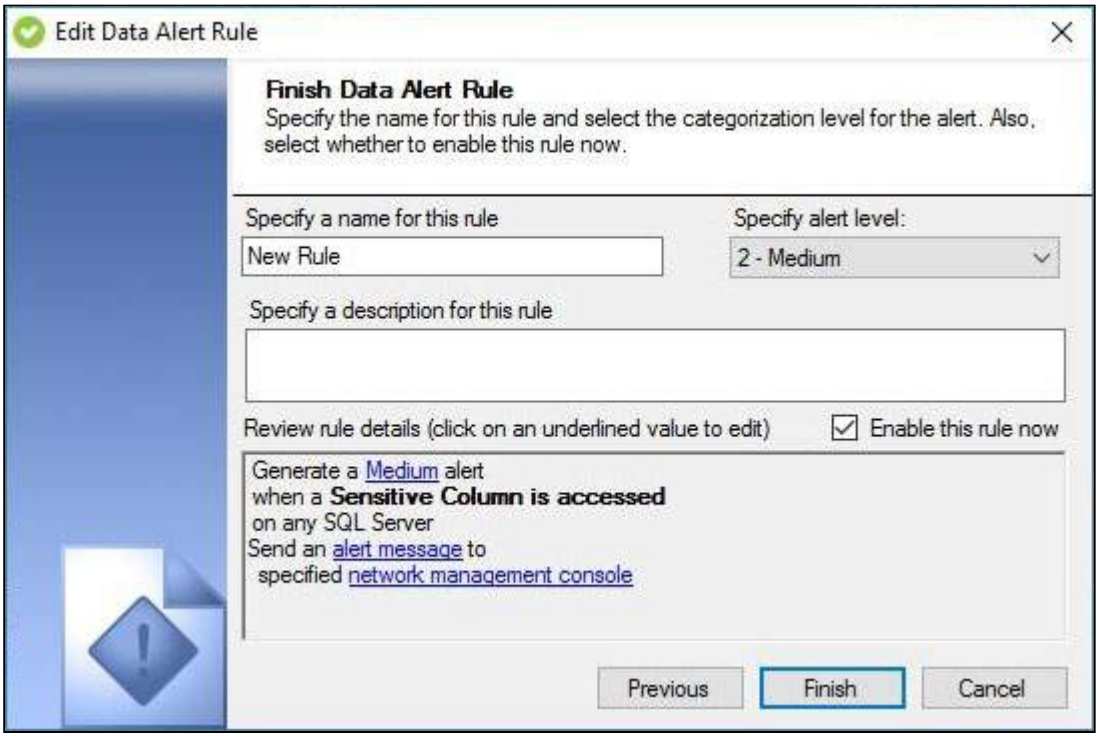
Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- 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 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**. IDERA 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 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 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.

Import your alert rules

As you configure or modify alert rules for your SQL Server instances in IDERA SQL Compliance Manager, 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 and reduce 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**.

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, IDERA 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.

Change the action an alert performs

Based on the criteria defined in your alert rules, IDERA 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 Compliance Manager takes when the event or Status Alert is triggered.

If you want to receive alert email notifications, configure 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**.

Export your alert rules

IDERA SQL Compliance Manager saves exported alert rules in XML format for you to apply 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**.

Enable an alert

You can resume IDERA SQL Compliance Manager 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.

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, IDERA 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.

Groom alerts

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

View alerts

You can use the IDERA SQL Compliance Manager 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**.

Receive alerts through email

You can configure IDERA 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 either the Edit Event Alert Rule wizard 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 about alert actions, see Change the action an alert performs.

Specify Alert Criteria windows

The Specify Alert Criteria 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

If you want to match ...	Use ...	Examples		
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:* Test00Test01test0101test4 metest#1TEST? htest*devtestertest

<Alert criteria> to match

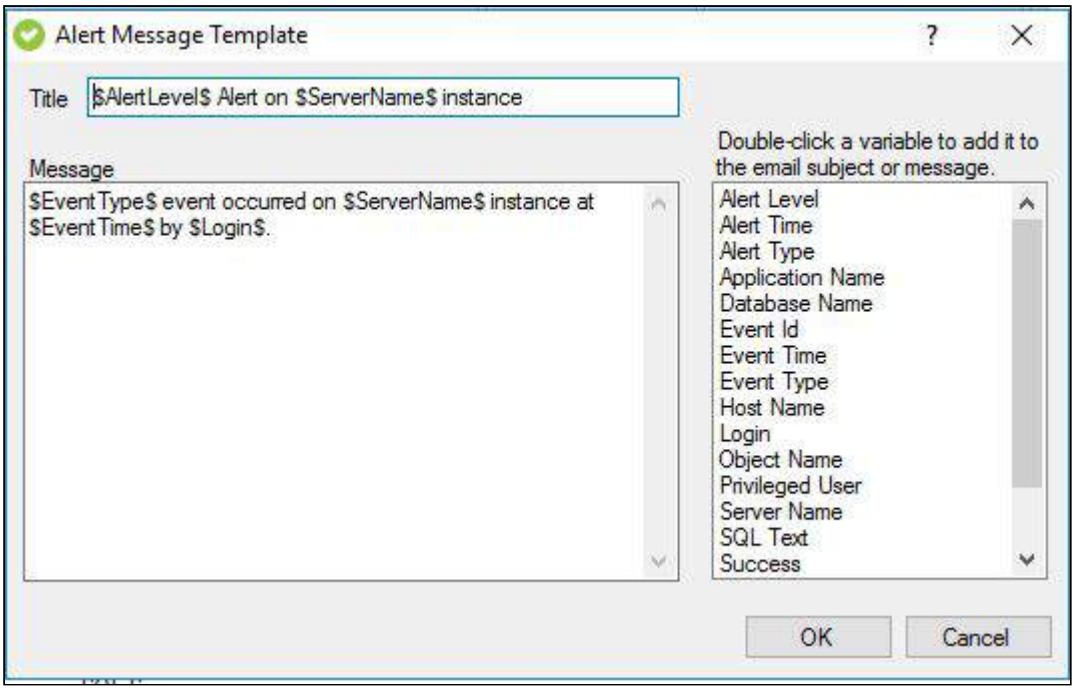
Allows to you change the list of match criteria. You can add a new criterion or remove an existing criterion.

Alert Message Template window

The Alert Message Template window allows you to define a custom alert message. When an alert is triggered, IDERA 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.

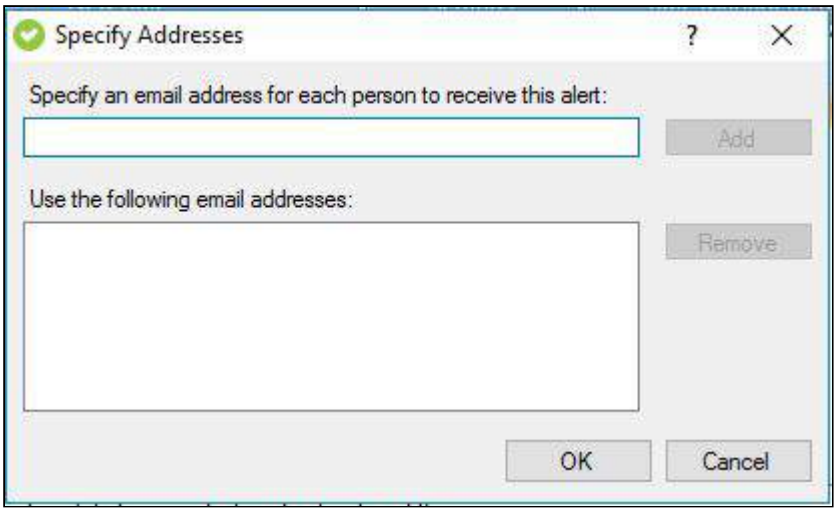
You can accept the default alert message or compose a custom message using the provided variables.



Specify Addresses window

The Specify Addresses 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**.



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.

9.3.3 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 Works

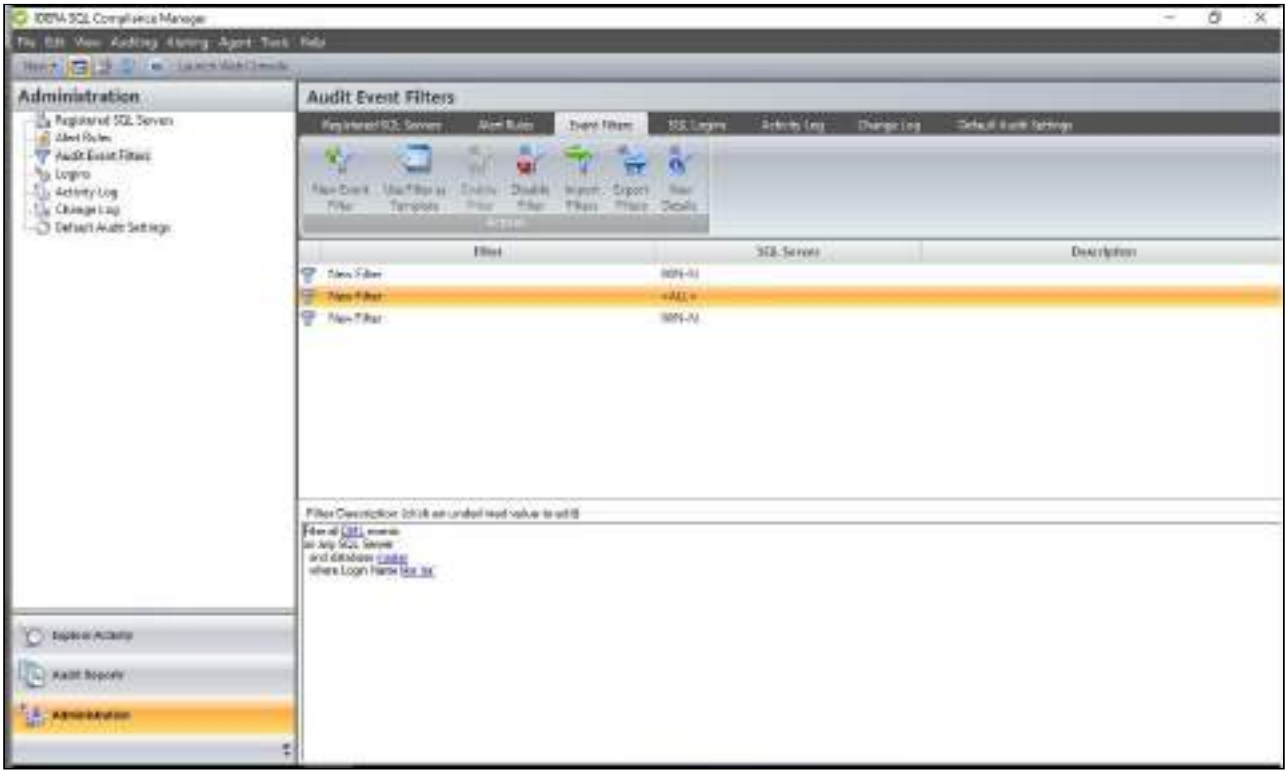
Event Filters determine which collected SQL events should be kept for processing by the Collection Server. Same as your audit settings, the Event Filters should correlate with the events you need to track on the SQL server in order to meet your compliance objectives.

After receiving the trace files from the SQL Compliance Manager 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 enabling Sensitive Column auditing on a table, the Collection Server preserves all SELECT and DML events associated with the audited columns even though you may have created an event filter to exclude SELECT and/or DML events. Therefore, when using an Event Filter for a specific Login, all events captured get filtered except for the Sensitive Column SELECT and/or DML operations.

Event Filters tab

The Event Filters 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. IDERA 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 Compliance Manager stores the new event filter in the Repository. The selected filter remains unchanged. For more information. see Use an Event Filter as a template.

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 Compliance Manager removes the event from the audit data. Use the Audit Events tab to see the resultant set of processed events. For more information, see Enable an Event Filter.

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. For more information, see Disable an Event Filter.

Import Filters

Allows you to import Event Filters previously exported from another SQL Server instance. By default, the imported Event Filters are disabled. For more information, see Import your Event Filters.

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. For more information, see Export your Event Filters.

View Details

Allows you to view or change the criteria for the selected filter. For more information, see Change which audit data the filter excludes.

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 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.

Create an Event Filter

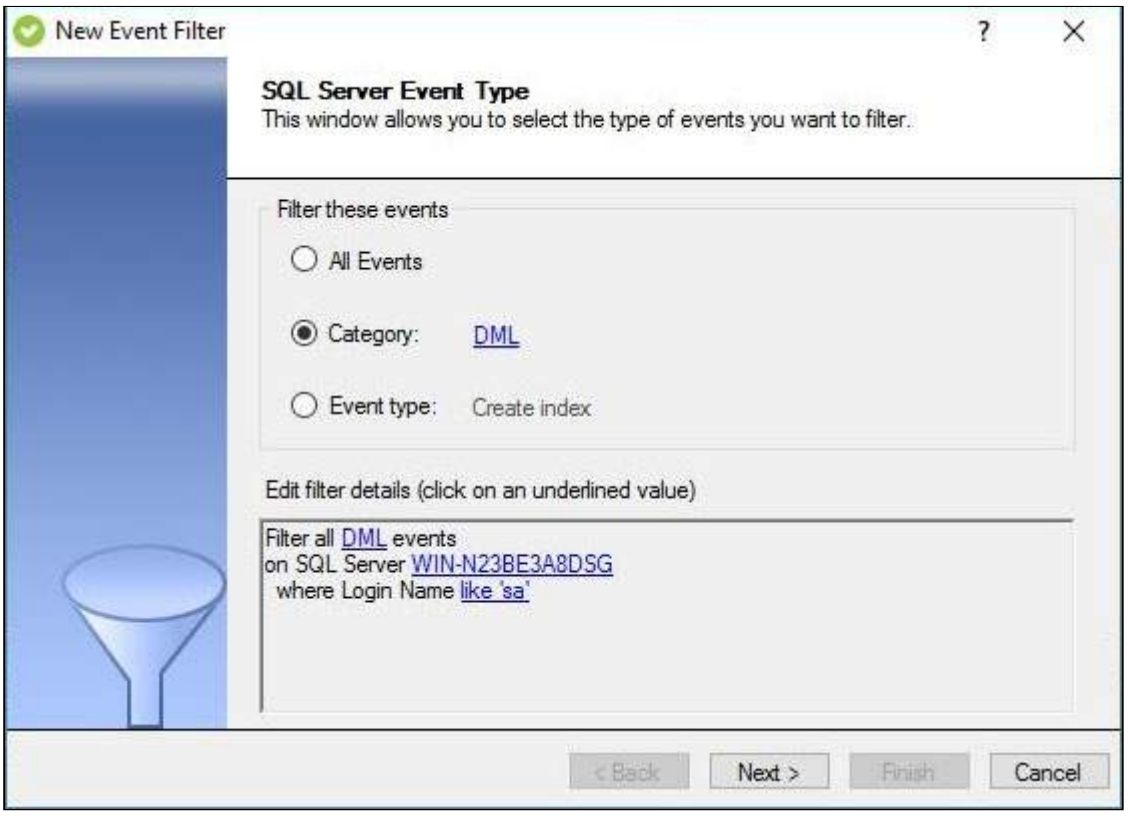
An Event Filter allows you to exclude specific events from your audit data. This approach helps you collect only the audit data you need. Event Filters can also help performance by reducing the size of the Repository databases and the processing load on the Collection Server.

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.

New Event Filter wizard - SQL Server Event Type tab

The SQL Server Event Type tab of the New Event Filter wizard 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

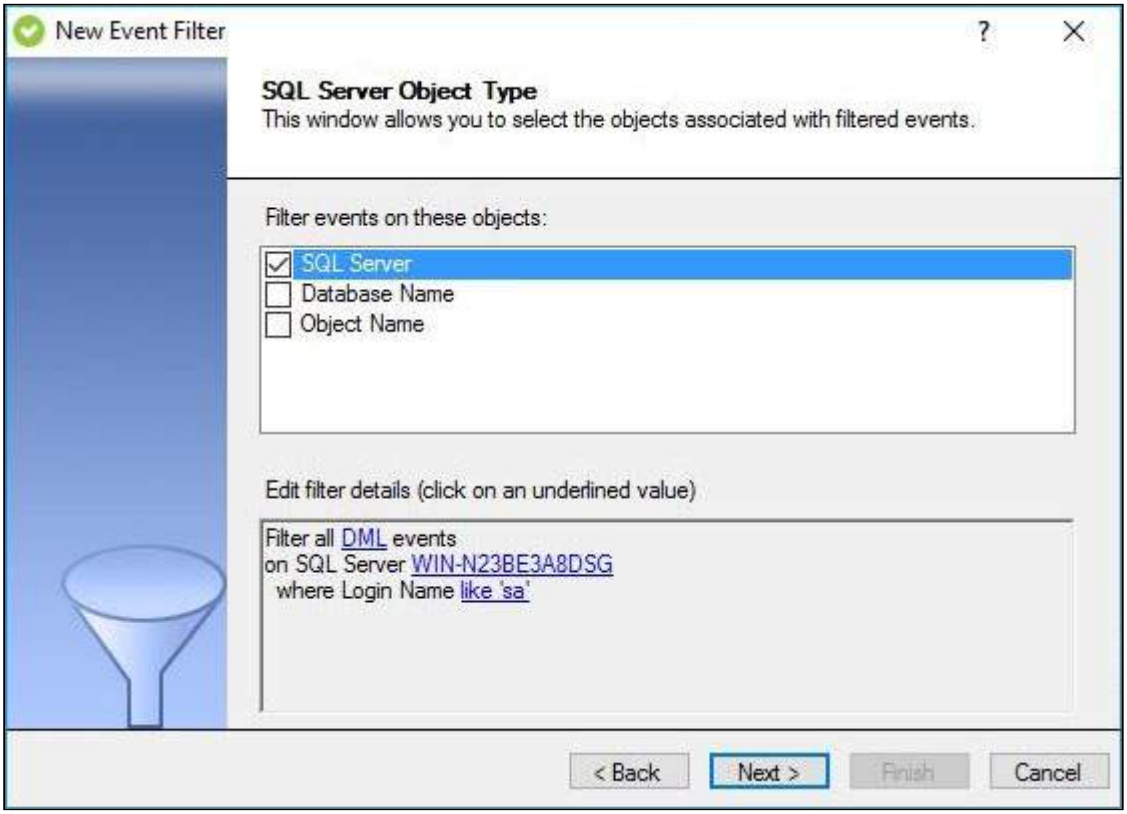
Allows you to select the specific SQL Server event category or type you want to filter from your audit data. When the Collection Server processes an audited event that matches the specified event type, the filter is run to see whether the identified event matches the other filter criteria.

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 of the New Event Filter wizard 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

Type of Object	You can specify ...
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

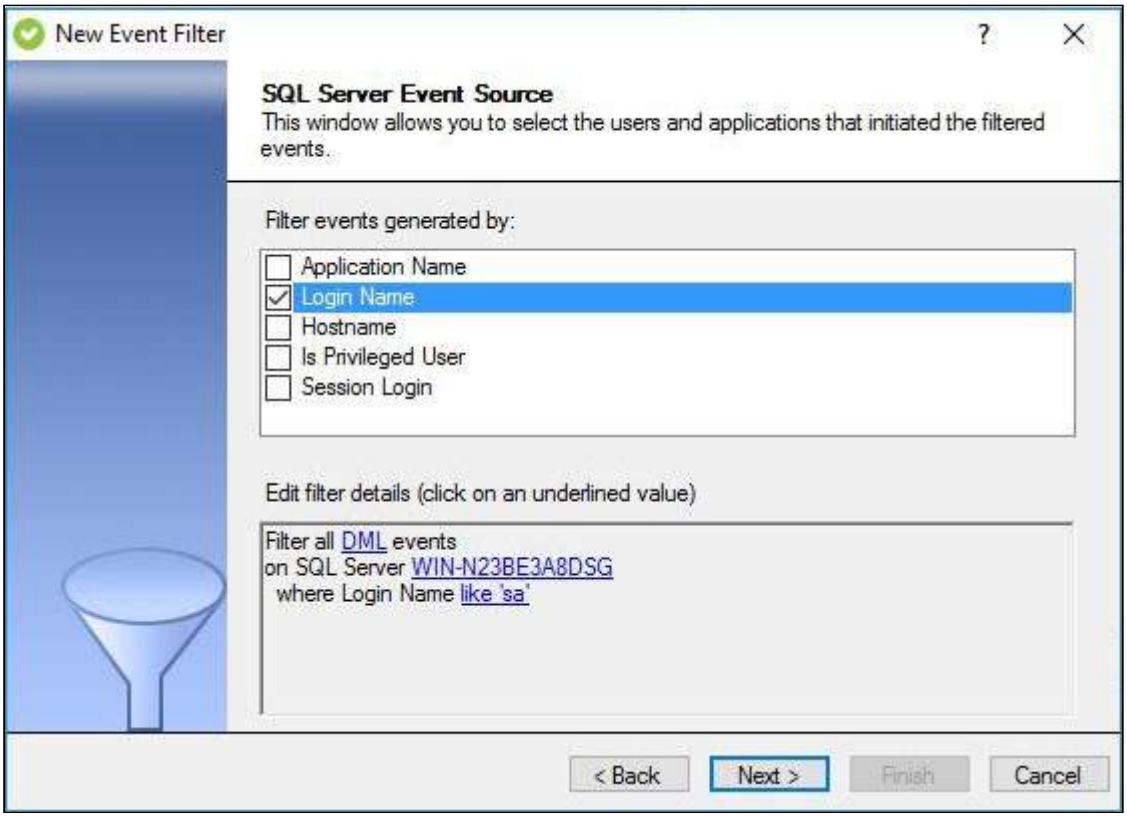
Edit filter details

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 Event Filter wizard - SQL Server Event Source tab

The SQL Server Event Source tab of the 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.

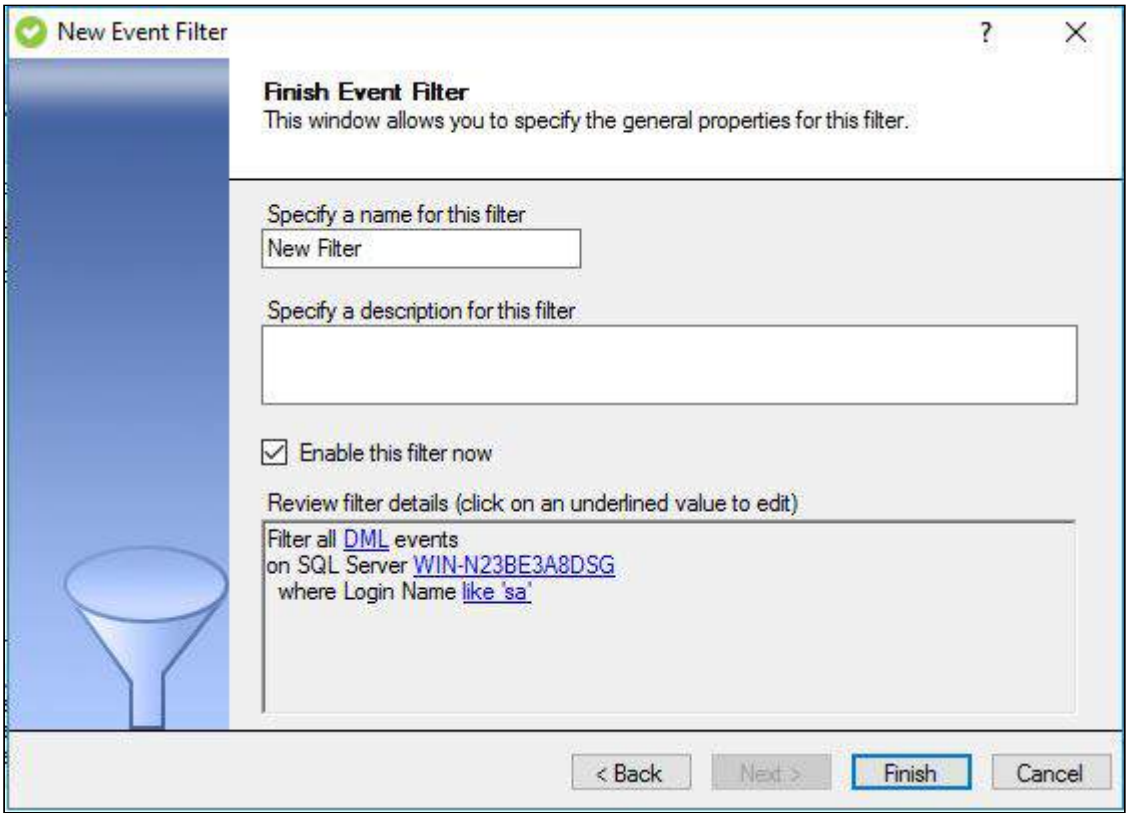
Edit filter details

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 - Finish Event Filter tab

The Finish Event Filter tab of the New Event Filter wizard allows you to specify a name for the new event filter, review the filter details, and then click **Finish**. When you finish this wizard, IDERA 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.

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, IDERA 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.

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, IDERA 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**.

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.

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**.

Change which audit data the filter excludes

Based on the criteria defined in your Event Filters, IDERA 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 Works.

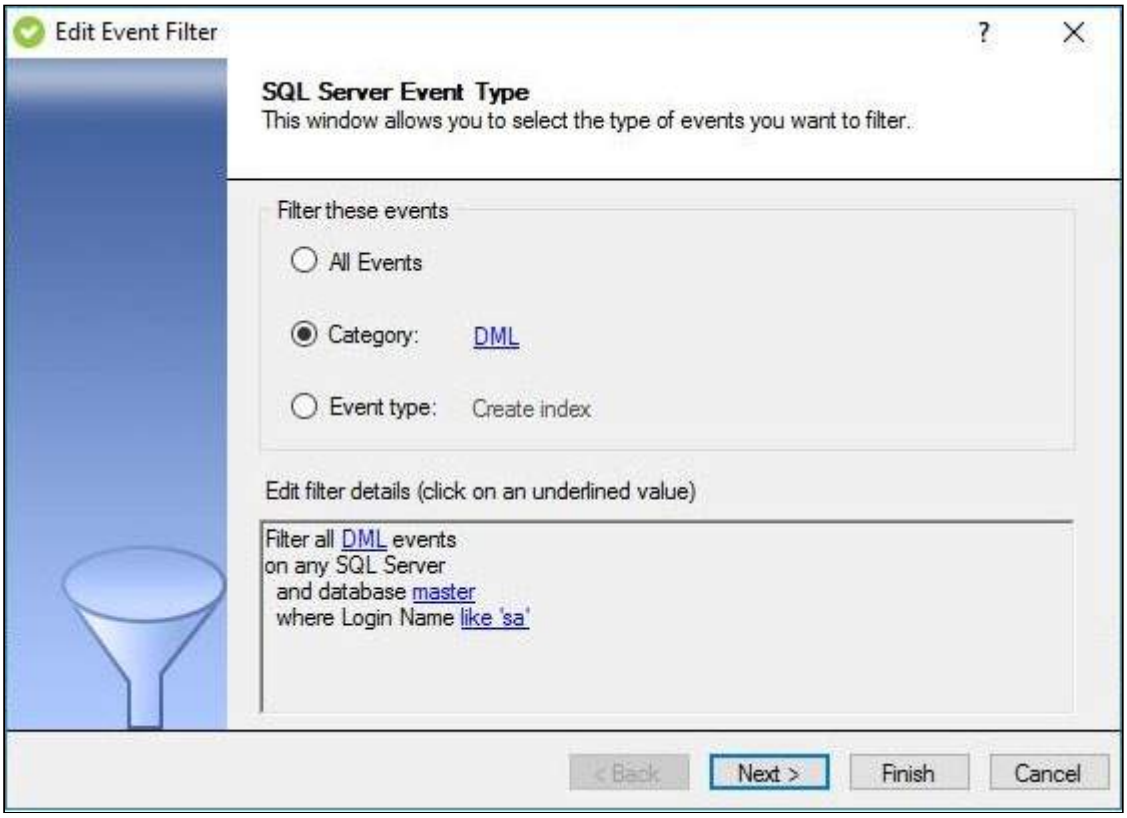
By changing the filter criteria, you can change the type of audit data that is excluded. You can also copy an existing Alert Rule and use it as a template to create a new rule.

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**.

Edit Event Filter wizard - SQL Server Event Type tab

The SQL Server Event Type tab of the Edit Event Filter wizard 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

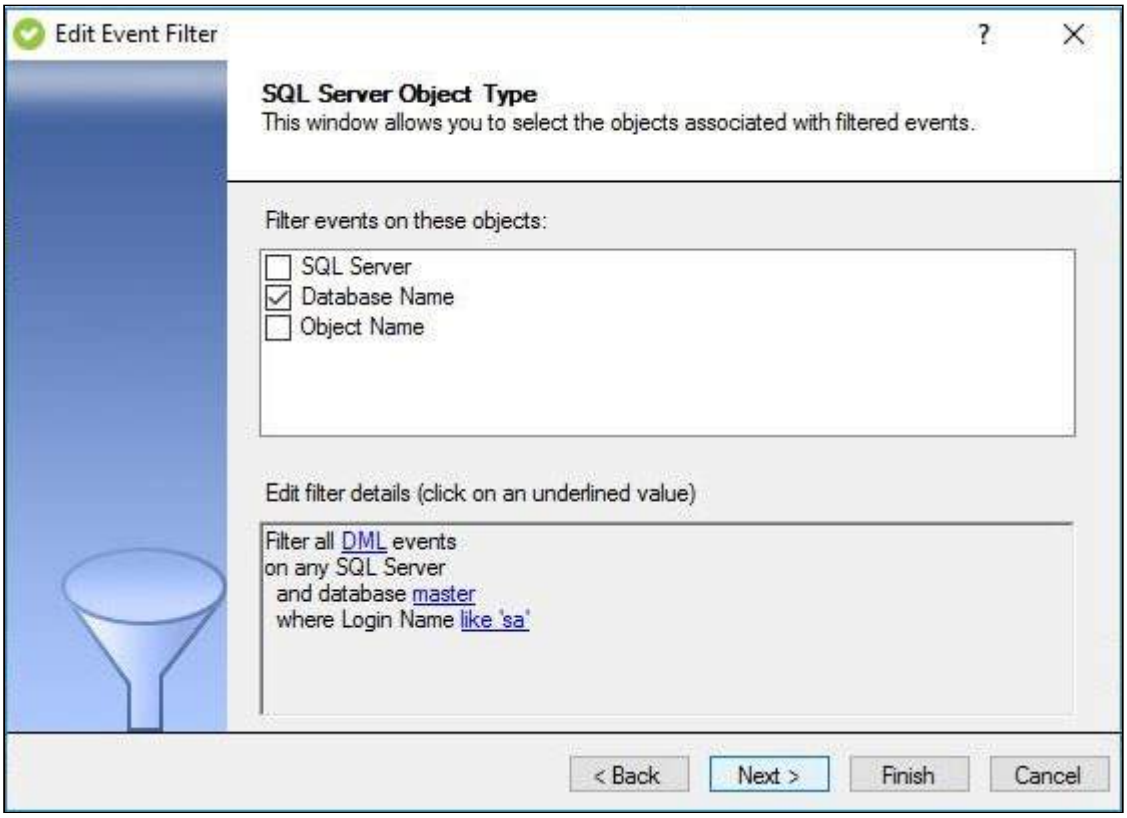
Allows you to select the specific SQL Server event category or type you want to filter from your audit data. When the Collection Server processes an audited event that matches the specified event type, the filter is run to see whether the identified event matches the other filter criteria.

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 Event Filter wizard - SQL Server Event Object Type tab

The SQL Server Event Object Type tab of the Edit Event Filter wizard 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

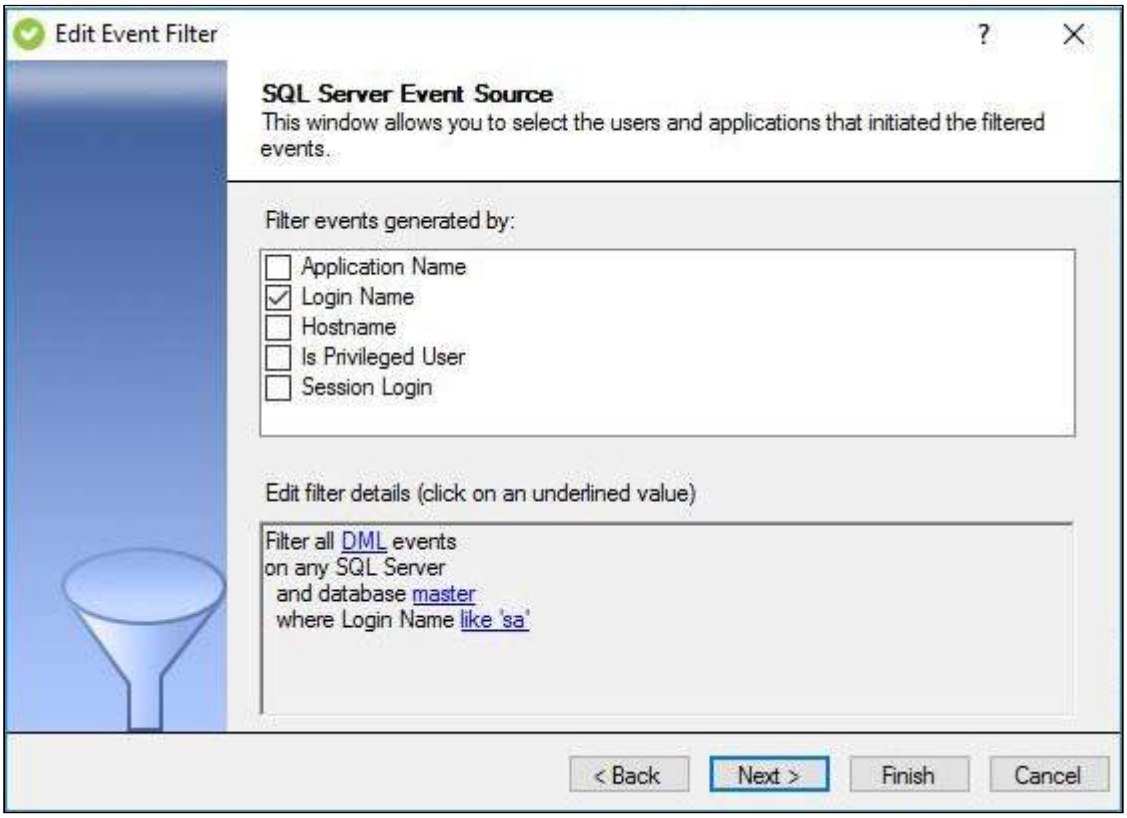
Edit filter details

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

The SQL Server Event Source tab of the Edit Event Filter wizard 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.

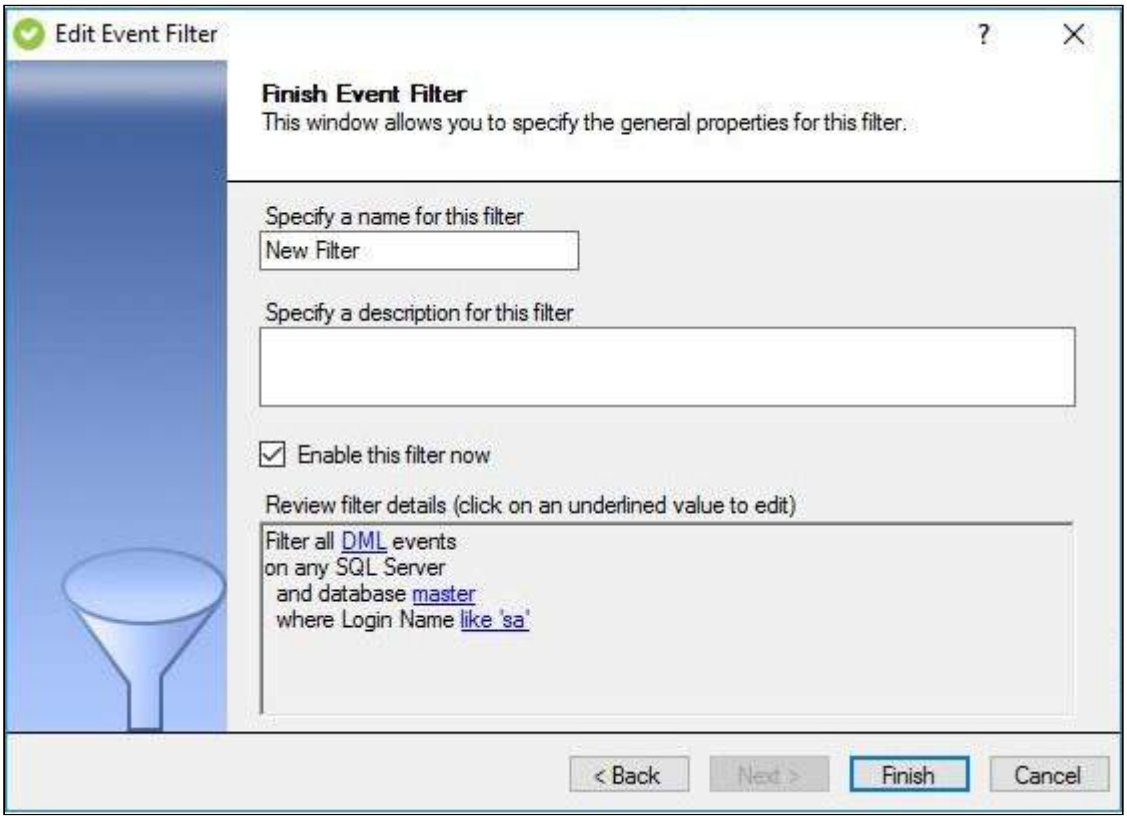
When the Collection Server processes an audited event that was initiated by the specified application, computer, or user, the filter is run to see whether the identified event matches the other filter criteria.

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 - Finish Event Filter tab

Use the filter details pane to review your changes, and then click **Finish**. When you finish this wizard, IDERA 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.

Specify Event Filter Criteria windows

The Specify Event Filter Criteria 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.

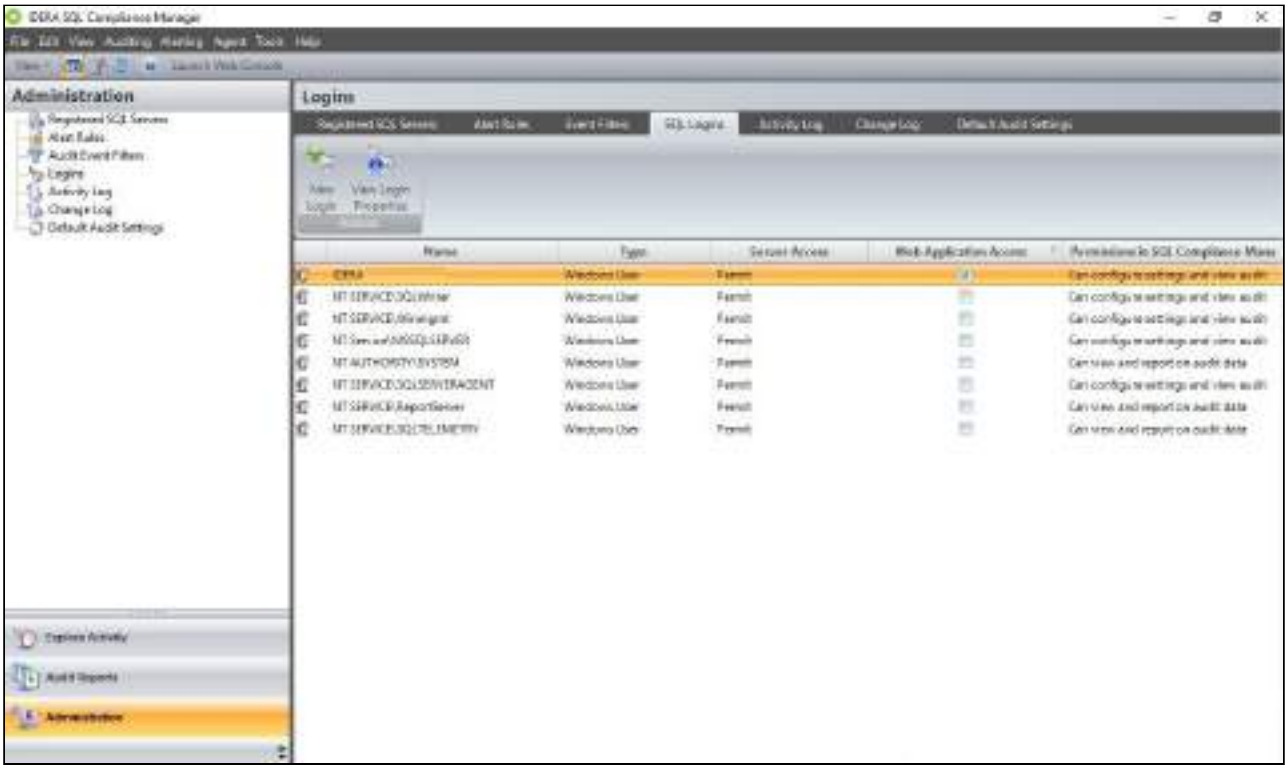
9.3.4 SQL Logins tab

The SQL Logins 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 IDERA 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. For more information, see Create a login.

View Login Properties

Allows you to view details about permissions settings and database access. For more information, see Assign permissions to a login.

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.

> **Warning**
>
> Deleting a SQL Server login from the SQL CM´s security, will also delete the SQL Server login and all associated databases users (if any) from the repository SQL Server´s security.

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.

Web Application Access

Indicates whether the login has permissions to the Web Application Access or if it does not.

Permissions in SQL Compliance Manager

Indicates which SQL Compliance Manager permission the selected login has on the Repository databases.

Secure Audit Data

IDERA 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.

How Console security works

IDERA 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 IDERA SQL Compliance Manager user has a SQL Server login. When you grant SQL Compliance Manager permissions to a login, SQL Compliance Manager 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 about setting your default permissions, see Understanding default permissions.

Understanding default permissions

If your security policies require more granular access control, you can grant or deny IDERA 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 IDERA 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.

☑	**Follow these steps ...**
☐	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 Create a login.

Available login permissions

IDERA SQL Compliance Manager permissions allow a user to access specific SQL Compliance Manager features. When you assign a 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 Compliance Manager 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 Compliance Manager 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 Compliance Manager 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, IDERA 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:

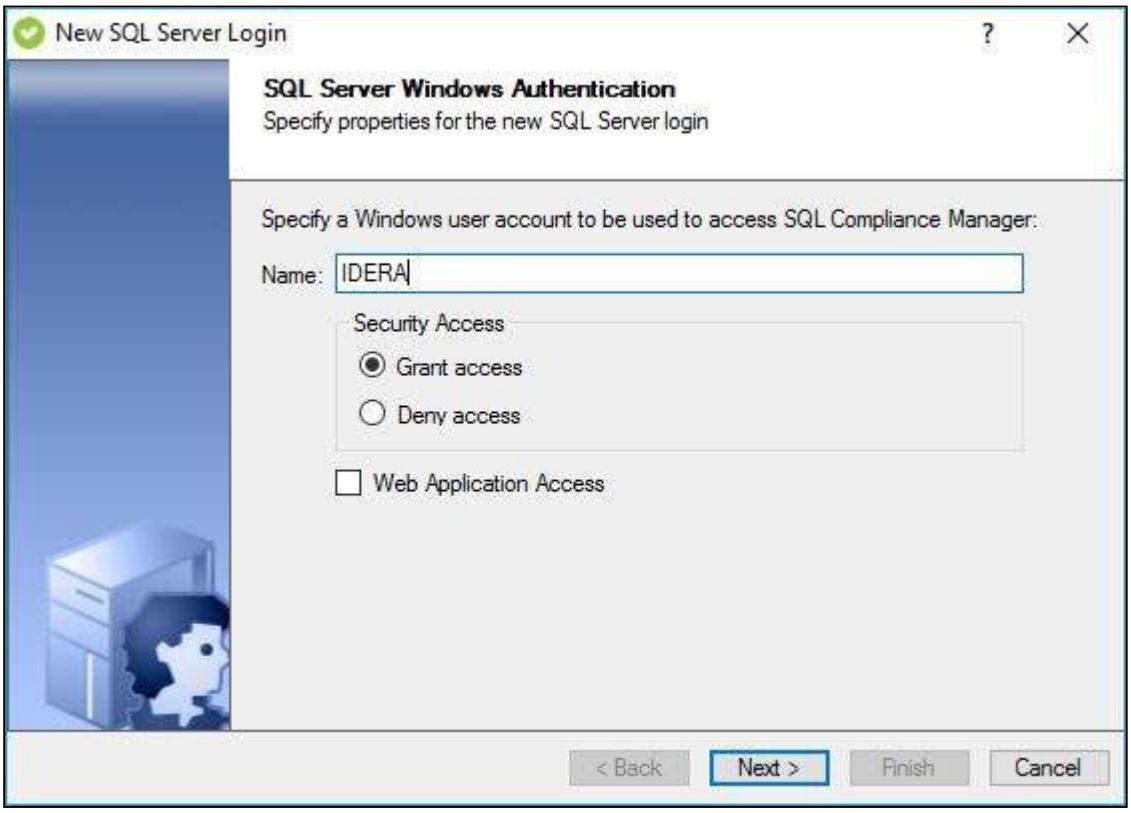
1. Select **Logins** in the **Administration** tree, and then click **New Login**.

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**.

New SQL Server Login wizard - SQL Server Windows Authentication tab

The SQL Server Windows Authentication tab of the New SQL Server Login wizard allows you to specify which Windows user account should be used when creating the SQL Server login to access IDERA 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**.

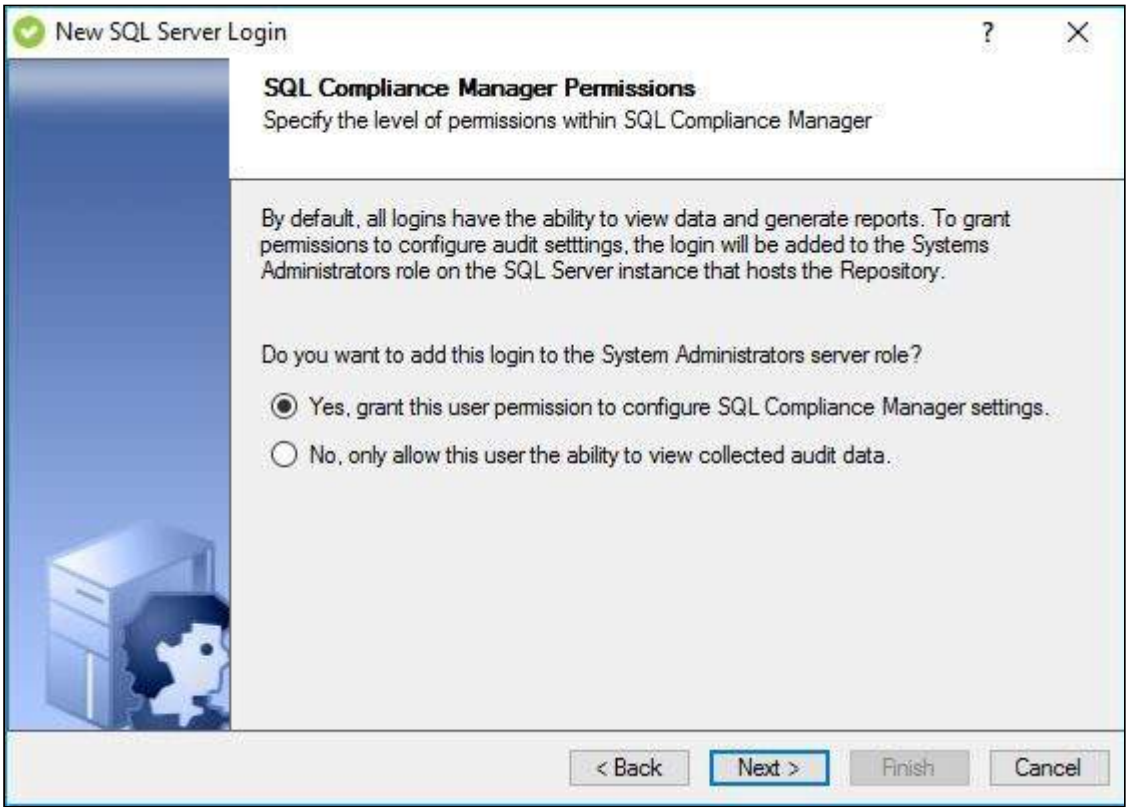


New SQL Server Login wizard - SQL Compliance Manager Permissions tab

The IDERA SQL Compliance Manager Permissions tab of the New SQL Server Login wizard allows you to specify the level of permissions that you want this login to 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 Compliance Manager adds the login to the Systems Administrator (sysadmin) fixed server role on the SQL Server instance that hosts the Repository databases.

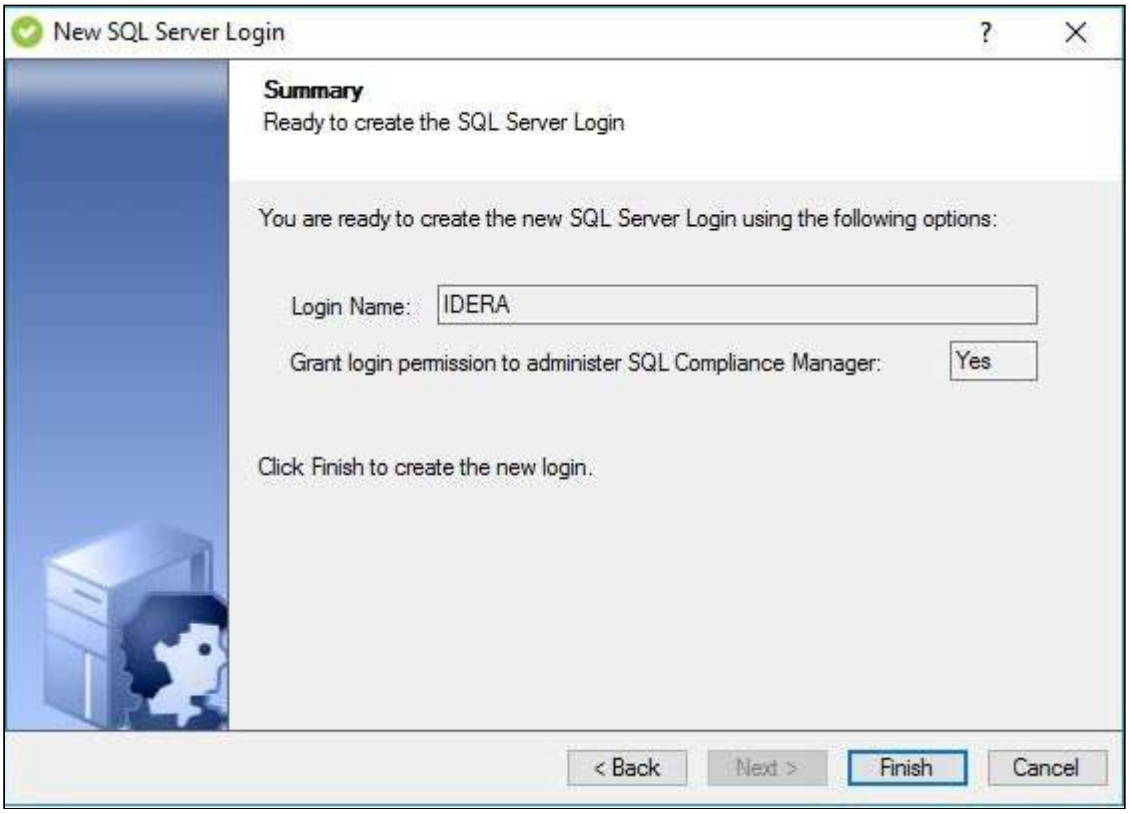
Select the appropriate SQL Compliance Manager permission, and then click **Next**.



New SQL Server Login wizard - Summary tab

The Summary tab of the New SQL Server Login wizard allows you to review the provided summary, and then click **Finish**. When you finish this wizard, IDERA 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.



Assign permissions to a login

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

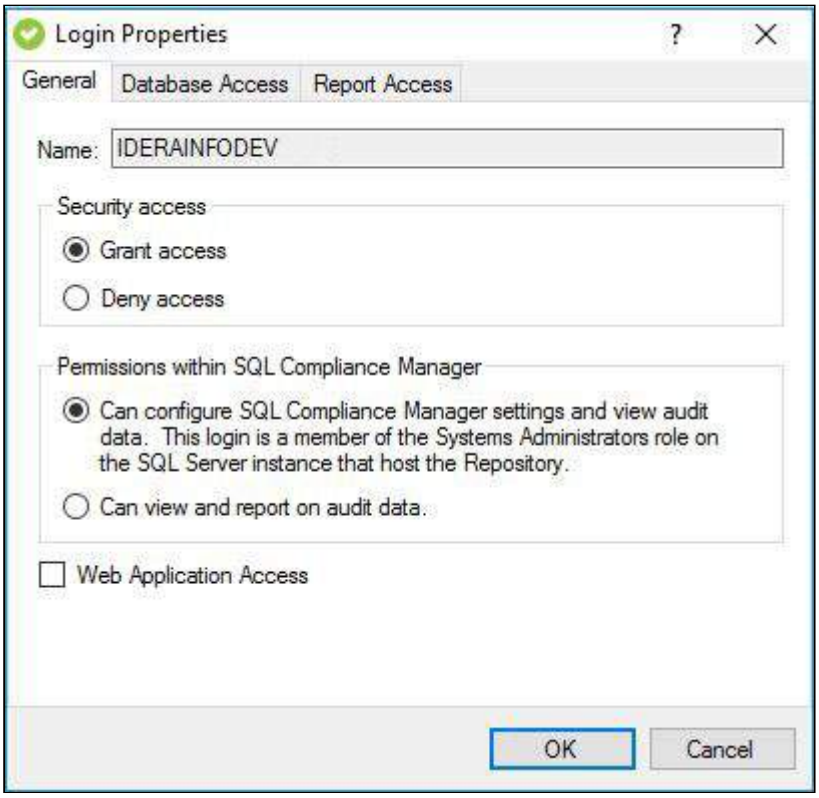
Because you are granting SQL Server privileges, applying permissions to a login also applies the same permissions in SQL Server. You can assign login permissions when you create a login, or modify permissions for existing logins. The following procedure allows you to modify permissions for existing logins.

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 and the Report Access tab to select appropriate permission on each report.
5. Click **OK**.

Login Properties window - General tab

The General tab of the Login Properties window allows you to change the security access and IDERA 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

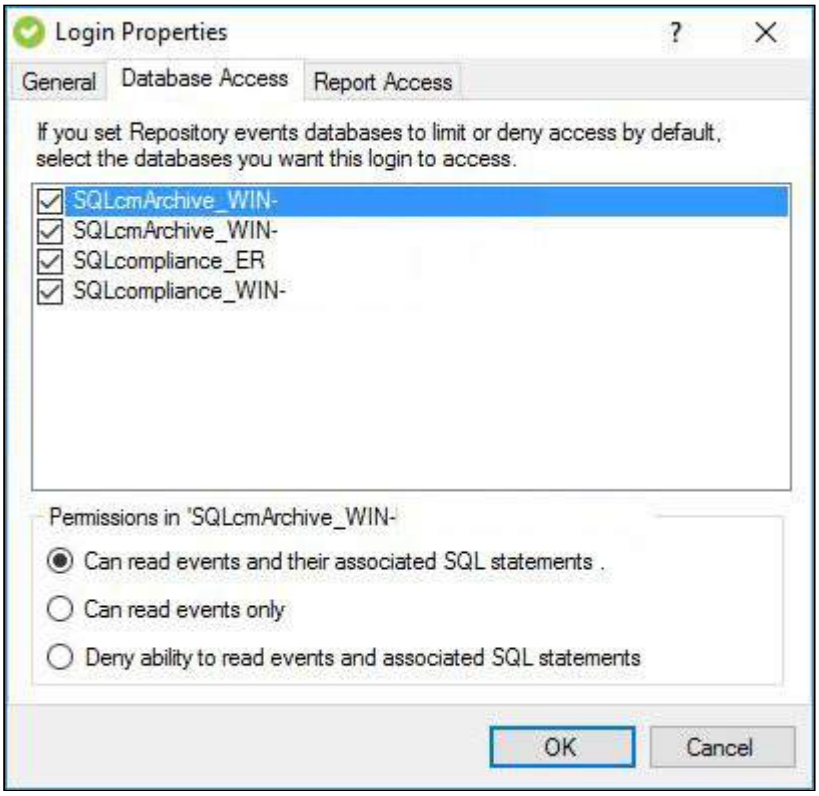
Allows you to indicate which SQL Compliance Manager permissions this login should have. You can grant the login permission to configure audit settings or view audit data. By default, all logins on the Repository SQL Server instance have read access to audit data. Read access allows the user to view and report on audit data stored in the Repository and archive databases.

Login Properties window - Database Access tab

The Database Access tab of the Login Properties window 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.



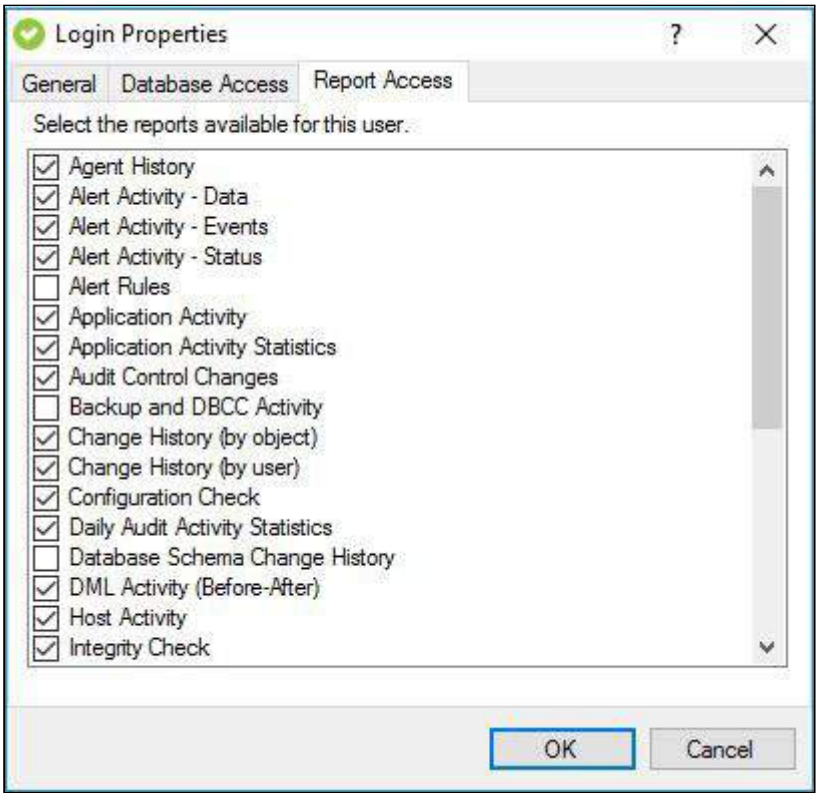
Login Properties window - Report Access tab

The Report Access tab of the Login Properties window allows you to limit user access to specific reports. Use this tab if your environment requires permissions settings that tightly control report access by limiting user access to only be able to see the selected reports. For example, you can deny access to the Configuration Reports by default, but grant a specific login access to those specific Reports.

As an Administrator select the Login on which you want to set permissions, and then select the appropriate report permissions for that user.

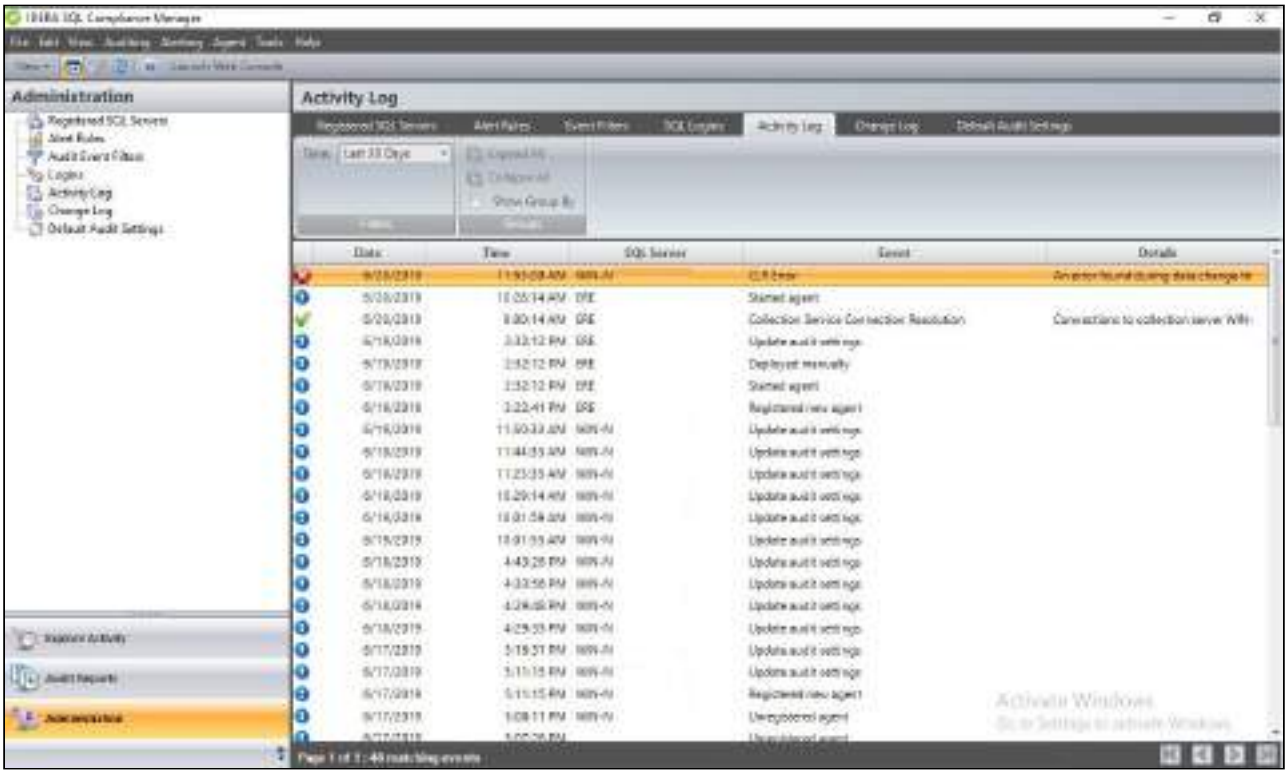
Your selections are applied along with any default permissions you set when you registered the corresponding SQL Server instance.

> ⚠ These updates are for the Windows Console only, and are not available via the Web Console or the SSRS reports.



9.3.5 Activity Log tab

The Activity Log tab lists events and alerts initiated by the IDERA SQL Compliance Manager components, allowing you to monitor SQL Compliance Manager 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. For more information, see Activity Log Properties window.

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 SQL Compliance Manager Agent configuration file (.bin) Error loading the new configuration	File is successfully saved SQL Compliance Manager 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	SQL Compliance Manager Agent configuration update or health check is successful

System Alert	Caused by ...	Resolves when ...
Server Connection Error	Error when connecting to the audited instances, due to invalid permissions or the offline SQL Server instance	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.

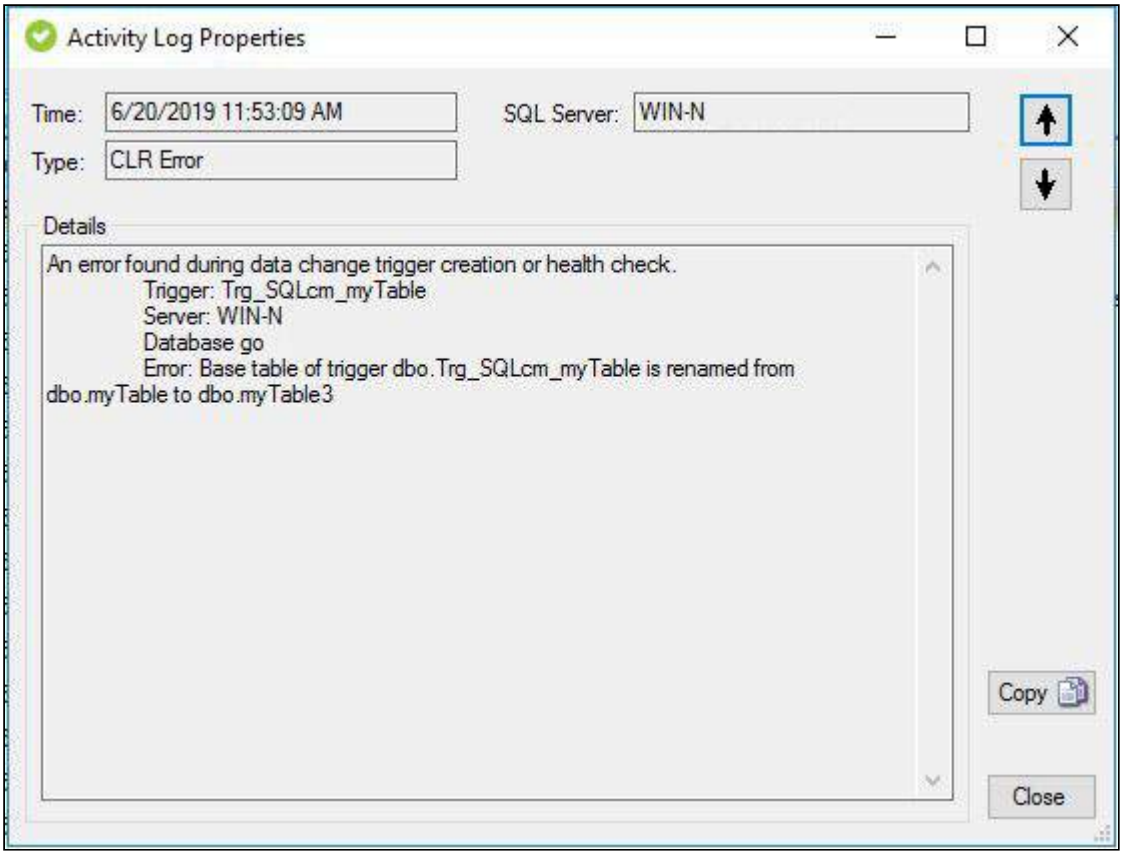
Activity Log Properties window

The Activity Log Properties 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

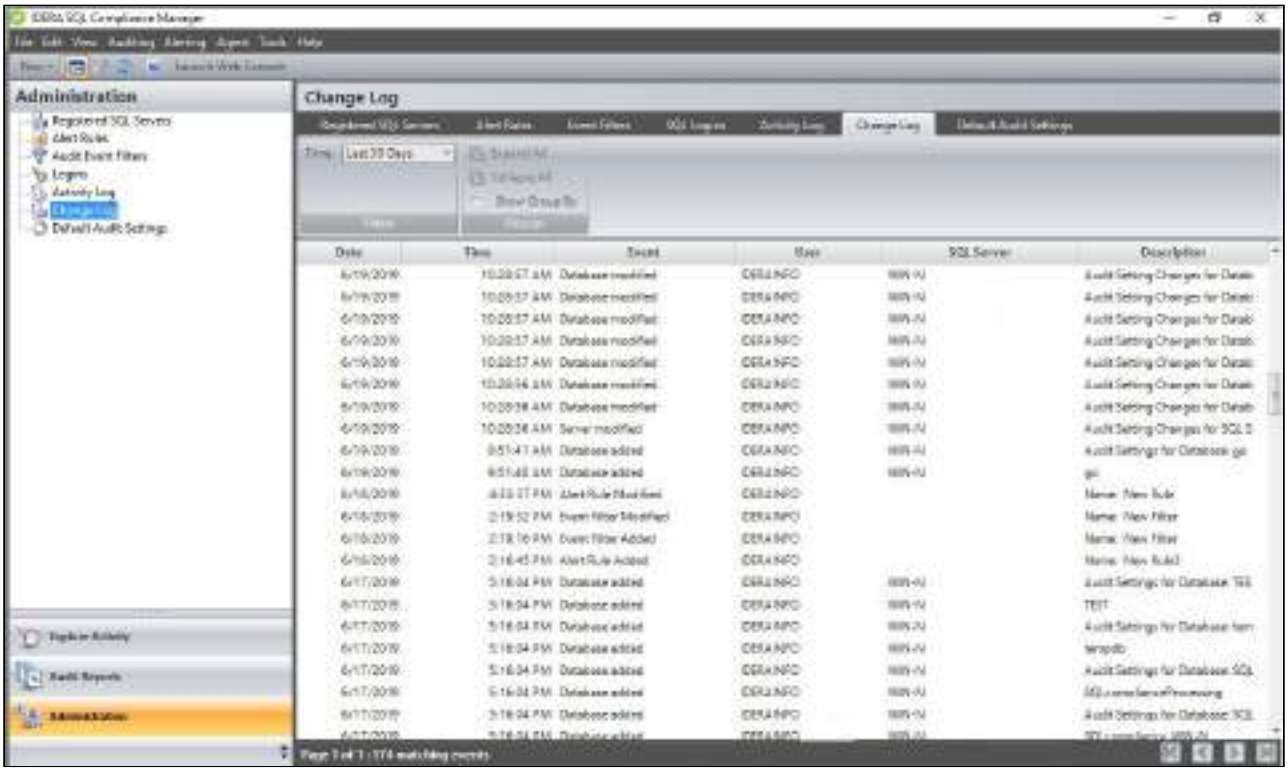
To scroll from one event to the next, use the up and down arrows.

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.



9.3.6 Change Log tab

The Change Log tab lists changes and events initiated through the Management Console and the Collection Server, allowing you to monitor IDERA 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.

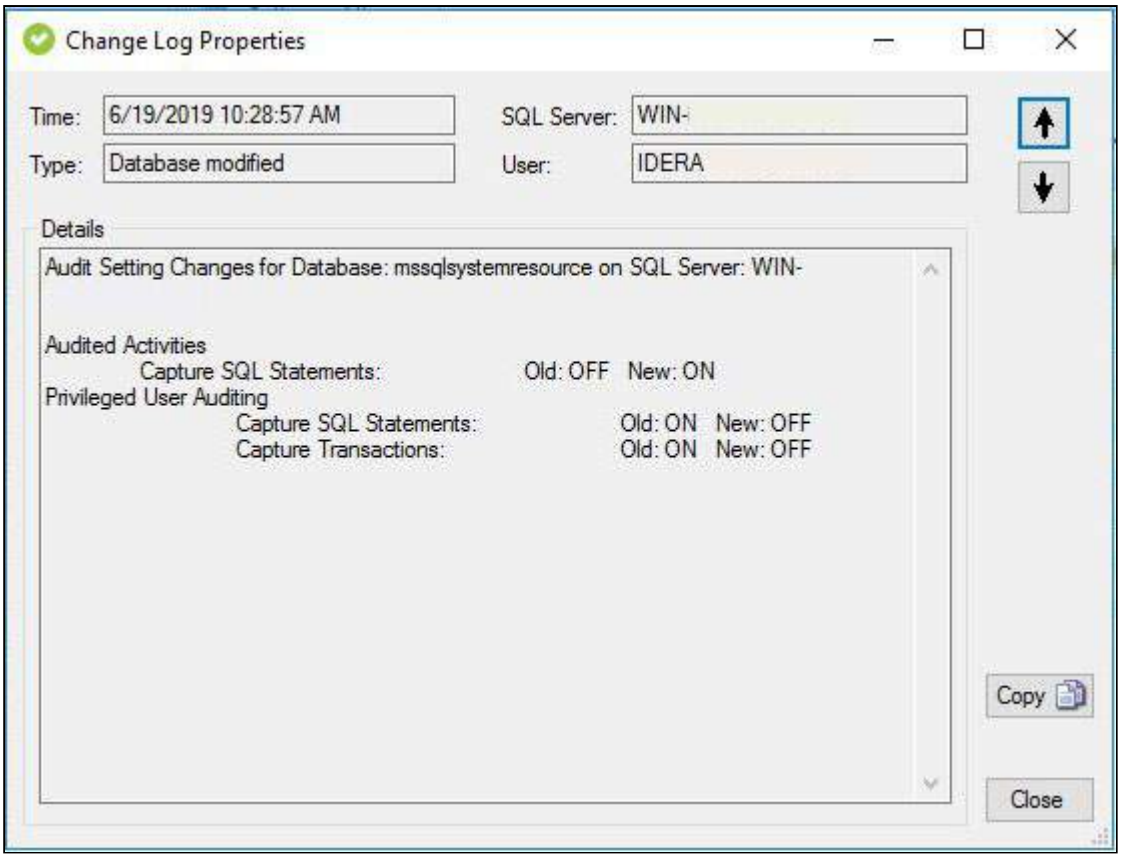
Change Log Properties window

The Change Log Properties 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.



9.3.7 Default Audit Settings tab

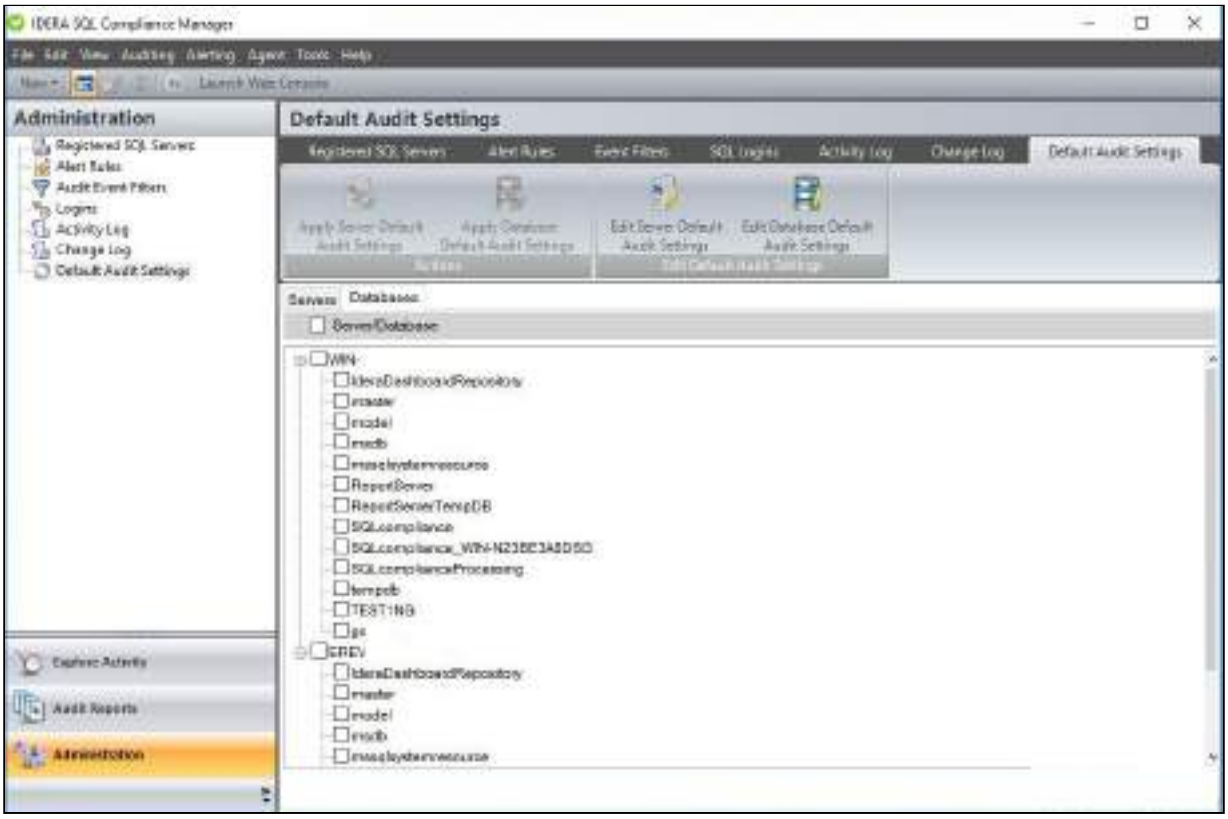
SQL Compliance Manager 5.6 implemented the capability to set default settings at both the Server Level and the Database Level. Previously, when a new server or database was registered users had the option to use the IDERA defaults, choose from a Regulation Guideline or customize the audit settings.

This new functionality makes it easy to set new Servers and Databases exactly the way users want without having to make additional updates to the configurations. In addition, users have the option to apply the previously configured default settings to selected Servers and Databases that are already being audited.

The default settings are the same settings that you would see in the properties for the Server or Database (except that they apply to the default and not a given Server or Database). Initially settings are set to the Idera Default Settings, subsequent visits to this page will reflect the default settings saved by the user. To learn more about the Idera default audit settings please visit the Idera default audit settings page.

The Default Audit Settings tab in the Administration view provides users with a list of their audited Servers and Databases to which they can choose to apply the default settings. Once your desired default audit settings are set, select from the list of servers or from the list of databases, the ones to which you wish to apply the default audit settings. For more information on how to edit the default settings please visit the Edit Server Default Audit Settings page or the Edit Database Default Audit Settings page.

> ⚠ Sensitive Columns and BAD are not available for the Database Default settings since those tables will vary greatly from database to database.



Available actions

Apply Server Default Audit Settings

Applies your previously configured Server Default Audit Settings to all the selected Servers from the Servers list. For more information, see Apply Server Default Audit settings.

Apply Database Default Audit Settings

Applies your previously configured Database Default Audit Settings to all the selected Databases from the Databases list. For more information, see Apply Database Default Audit settings.

Edit Server Default Audit Settings

Allows you to configure your desired server default audit settings. These settings can later be applied to any server registered in your environment. For more information, see Edit Server Default Audit Settings.

Edit Database Default Audit Settings

Allows you to configure your desired database default audit settings. These settings can later be applied to any audited database in your environment. For more information, see Edit Database Default Audit Settings.

Available columns

Servers

Displays a list of all registered servers available for selection.

Databases

Expand the Server to displays a list of all audited databases available for selection.

Idera Default Audit Settings

IDERA SQL Compliance Manager provides users with a default basic set of settings to begin auditing. These are just the Idera default settings, and users can modify these settings on individual servers and databases to accommodate their auditing needs. These settings will apply to newly added servers and databases. Users can reset back to the Idera default settings at any time by clicking the **Reset to Idera Default Settings** button.

Idera Default Server Audit Settings

Audited Activities tab

Allows you to select the type of activity you want to audit. The following are the Idera Default Database Audit Settings:

- Failed Logins
- **Access Check Filter** - Filter events based on access check
    - Audit only actions that passed access check
- **Capture DML and Select Activities**
    - Via Trace Events

Trusted Users tab

No users selected

Privileged Users Auditing tab

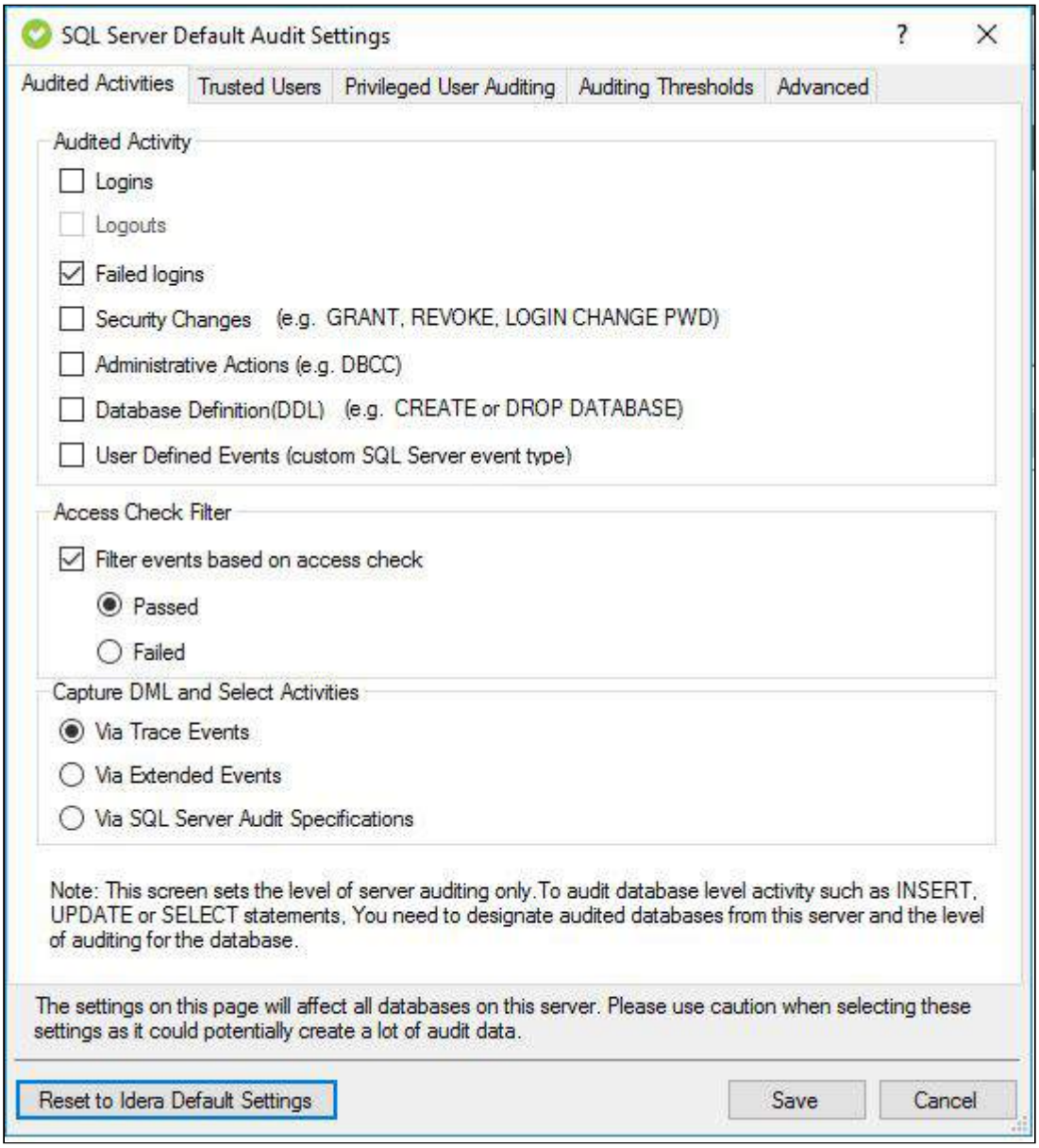
No users selected

Auditing Thresholds tab

No settings enabled

Advanced tab

- **Default Database Permissions**
  - Grant right to read events and their associated SQL statements
- **SQL Statement Limit**
  - Truncate stored SQL statements after 512 characters



Idera Default Database Audit settings

Audited Activities tab

Allows you to select the type of activity you want to audit. The following are the Idera Default Database Audit Settings:

- Security changes
- Database Modification (DML)
- Access Check Filter - setting selected at server level.

Before-After Data

These settings must be set on the individual database level.

Sensitive Columns tab

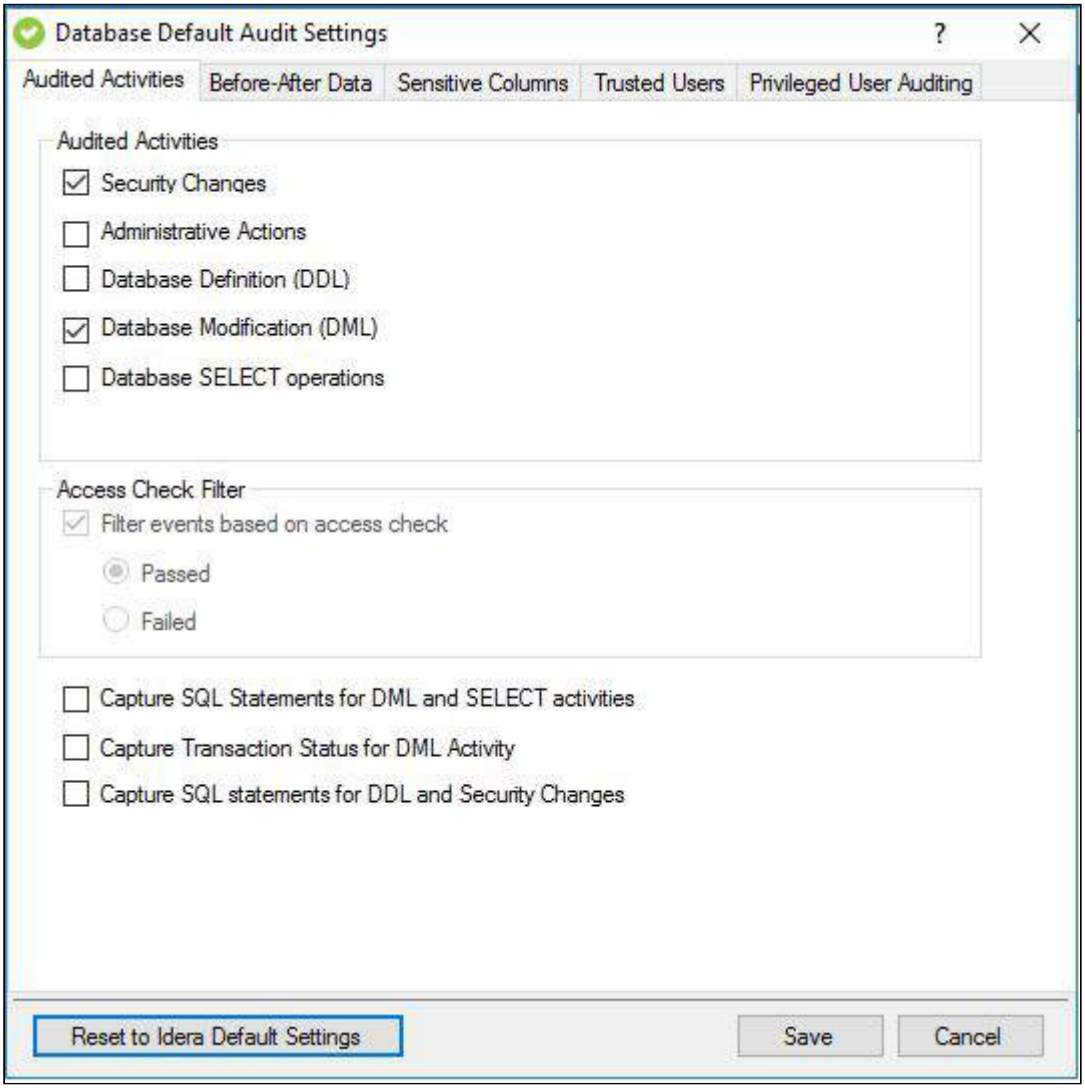
These settings must be set on the individual database level.

Trusted Users tab

No users selected

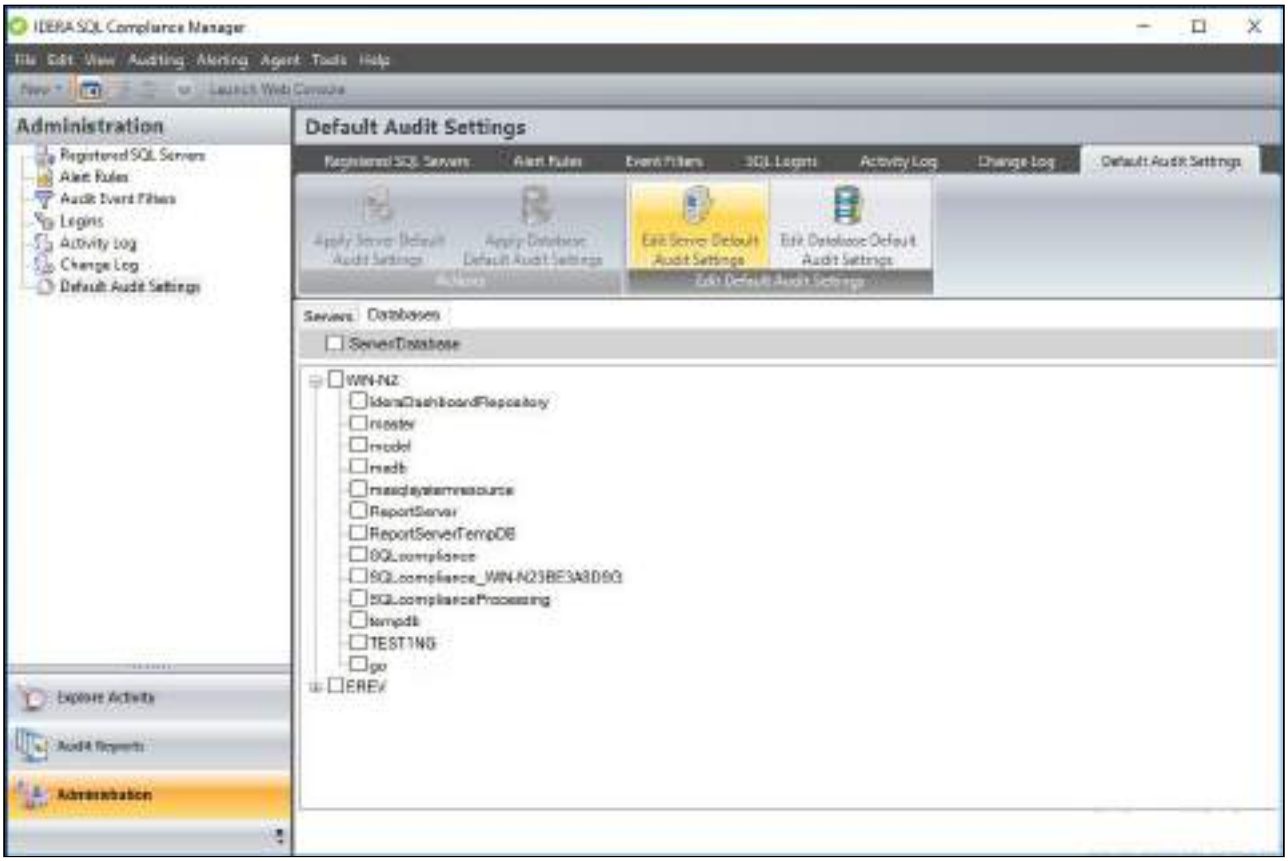
Privileged Users Auditing tab

No users selected



Edit Server Default Audit Settings

Use the Edit Server Default Audit Settings options to configure your Server Default auditing needs exactly the way you want without having to make additional updates to your configurations.. The Default Server Settings can later be applied to your registered servers or to newly added SQL Servers.



To Edit Server Default Audit Settings follow the steps below:

1. From the **Administration** view, select the **Default Audit Settings** tab.
2. Click the **Edit Server Default Audit Settings** option.
3. Set your desired SQL Server Default Audit Settings, for more information on how to configure these settings, visit the SQL Server Default Audit Settings page.
4. Once done configuring your desired settings, Click **Save.**

Users can reset back to the Idera Default Audit Settings at any time by clicking the **Reset to Idera Default Settings** button.

SQL Server Default Audit Settings Properties

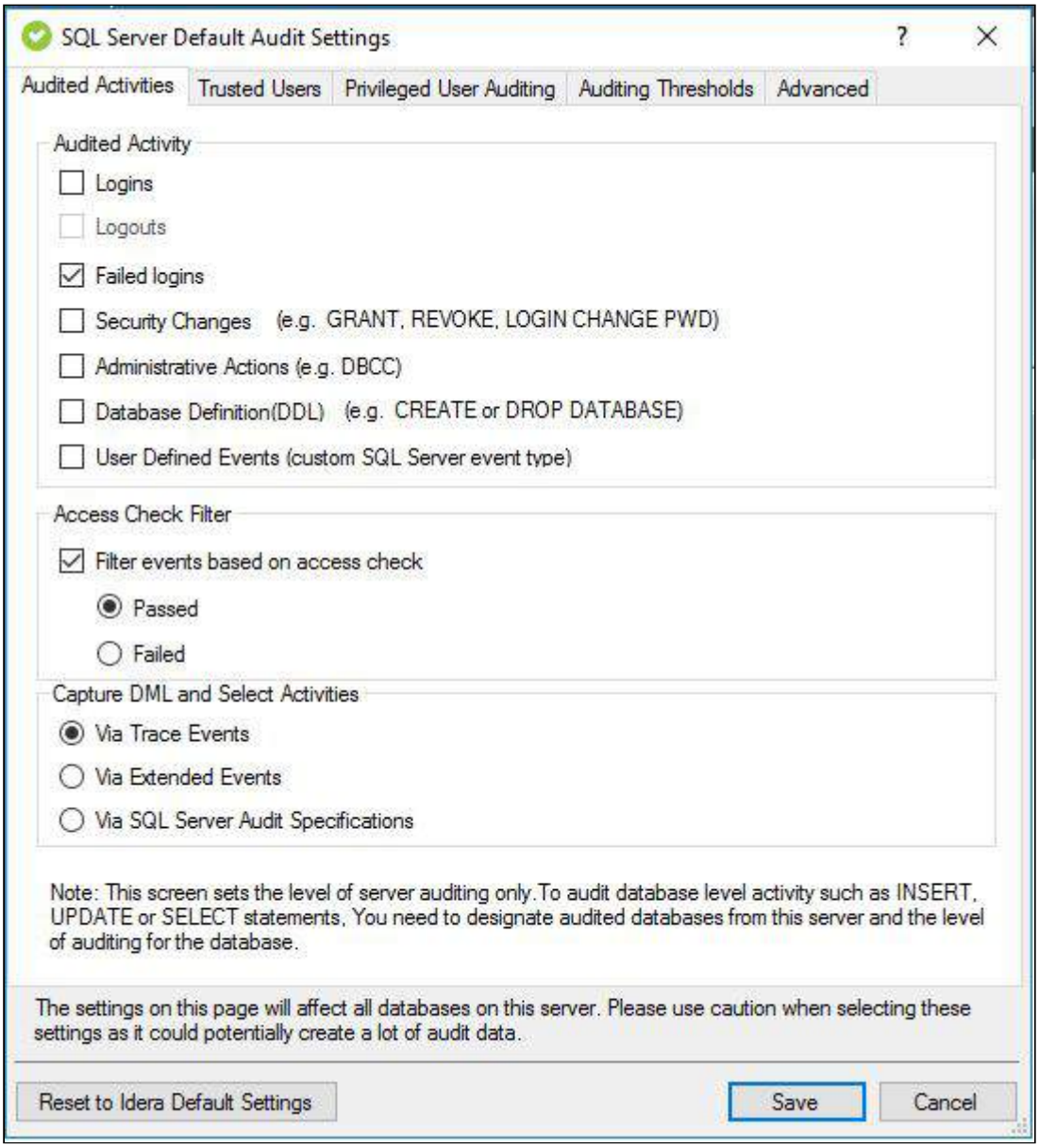
The IDERA SQL Compliance Manager SQL Server Default Audit Settings window allows you to configure your default server settings.

This topic reviews the following tabs:

- Audited Activities tab
- Trusted Users tab
- Privileged User Auditing tab
- Auditing Thresholds tab
- Advanced tab

Audited Activities tab

The Audited Activities tab allows you to change which types of SQL Server events you want to audit. IDERA SQL Compliance Manager audits these events at the server level only.



Available fields

Audited Activity

Allows you to select the type of activity you want to audit. Based on your selections, SQL Compliance Manager 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 at the server level. A user-defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

⚠ Audited Activities selected at Default Server-level audit settings are automatically pre-selected and disabled for selection for Default Server level Privileged Users added at the Server-level Privileged User Auditing.

Access Check Filter

Allows you to refine your SQL Server login data audit trail 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 Compliance Manager 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.

Capture DML and SELECT Activities

The option Extended Events is configured by default for each instance registered to capture DML and Select activities.

Via Trace Events - Allows you to select Trace Events as your event handling system for DML and SELECT activities. For more information about this feature, see Understanding Traces.

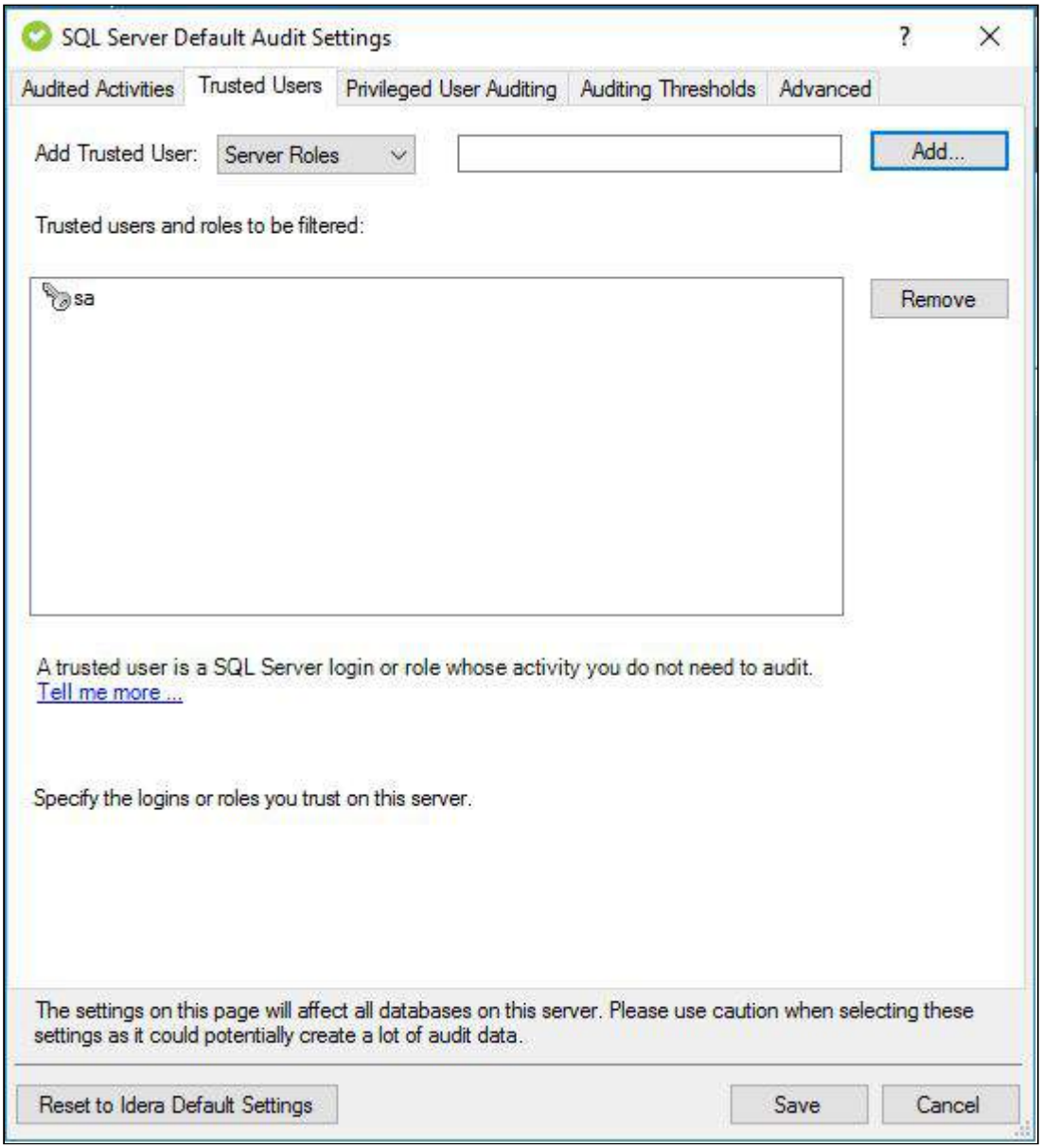
Via Extended Events - Allows you to select SQL Server Extended Events as your event handling system for DML and SELECT events for SQL Server 2012 and later versions. For more information about this feature, see Using SQL Server Extended Events.

Via SQL Server Audit Specifications - Allows you to select SQL Server Audit Logs as your event handling system for DML and SELECT events for SQL Server 2017 and later versions. For more information about this feature, see Using SQL Server Audit Logs.

⚠ SQL Compliance Manager does not support Extended Events functionality on SQL Server releases earlier than SQL Server 2012; therefore, for the registration of SQL Server instances with versions lower than SQL Server 2012, the Capture DML and Select Activities option is set to Via Trace Events.

Trusted Users tab

The Trusted Users tab of the SQL Server Default Audit Settings window allows you to add Trusted Users at the server level and set the default audit settings to be applied on SQL Server instances. Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited server or 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. This exclusion occurs for all auditing, including DML and SELECT events related to sensitive columns and before and after data.



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

Suppose you are auditing privileged user activity, and the trusted user is also a privileged user. In that case, IDERA 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, select the SQL Server login or role you want to trust and then click **Add**.

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 login or role is designated as trusted, the SQL Compliance Manager Agent omits all database-level activity generated by these logins from the audit data trail.

Remove a user or role from the trusted list

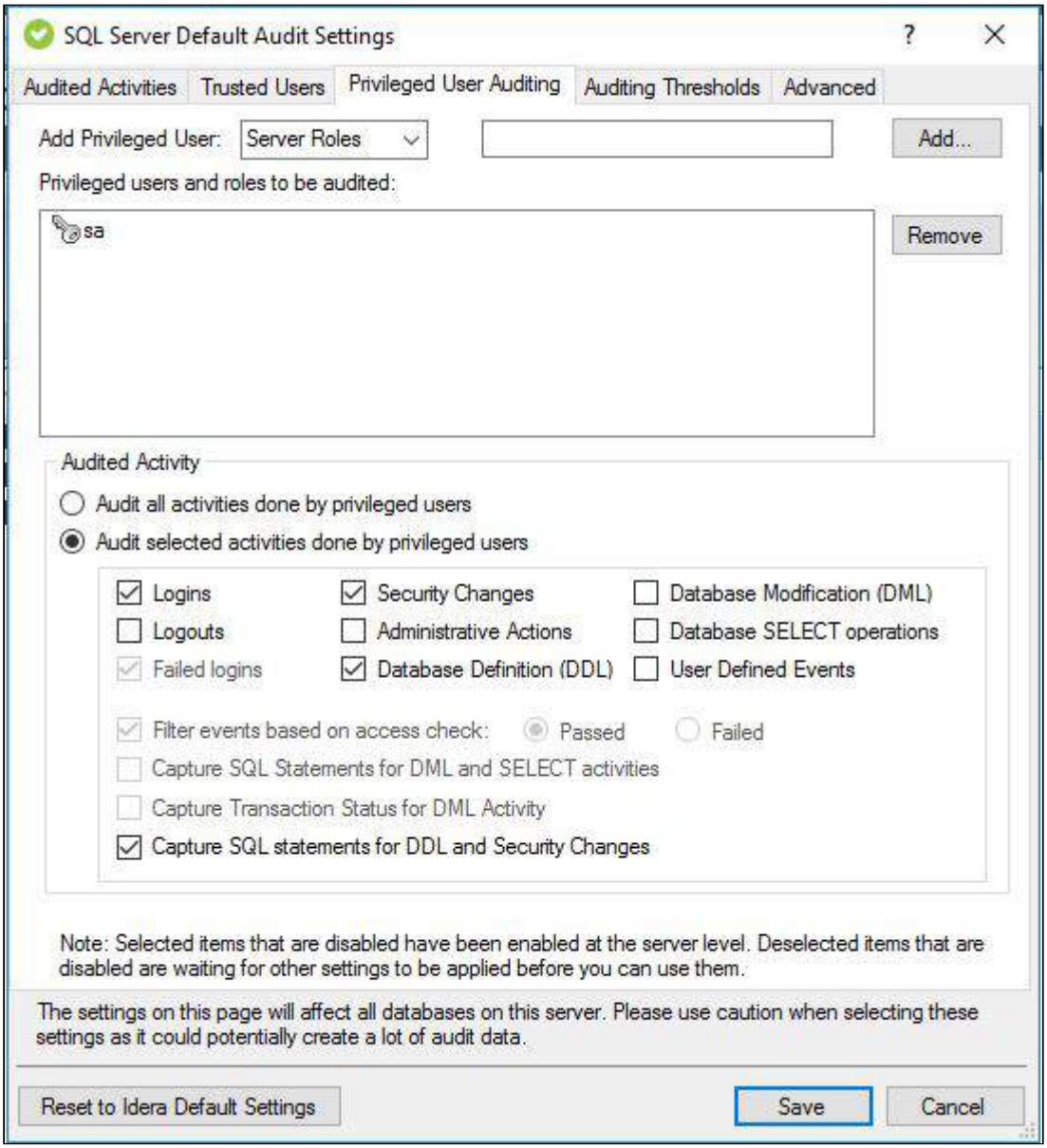
Allows you to designate a previously trusted user or SQL Server role as non-trusted. When login or role becomes non-trusted, SQL Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

Privileged User Auditing tab

The Privileged User Auditing tab of the SQL Server Default Audit Settings window allows you to add Privileged Users at the server level and set the default audit settings to be applied on SQL Server instances. 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 SQL Compliance Manager 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 Server Roles or by Server Logins.

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 SQL Compliance Manager Agent no longer collects events recorded for that login or the role members.

Note

Any Privileged Users added at the Server-level Default audit settings are automatically added and disabled for selection at the Default Database Privileged Users settings.

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 SQL Compliance Manager 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.

Capture SQL statements for DDL and Security Changes

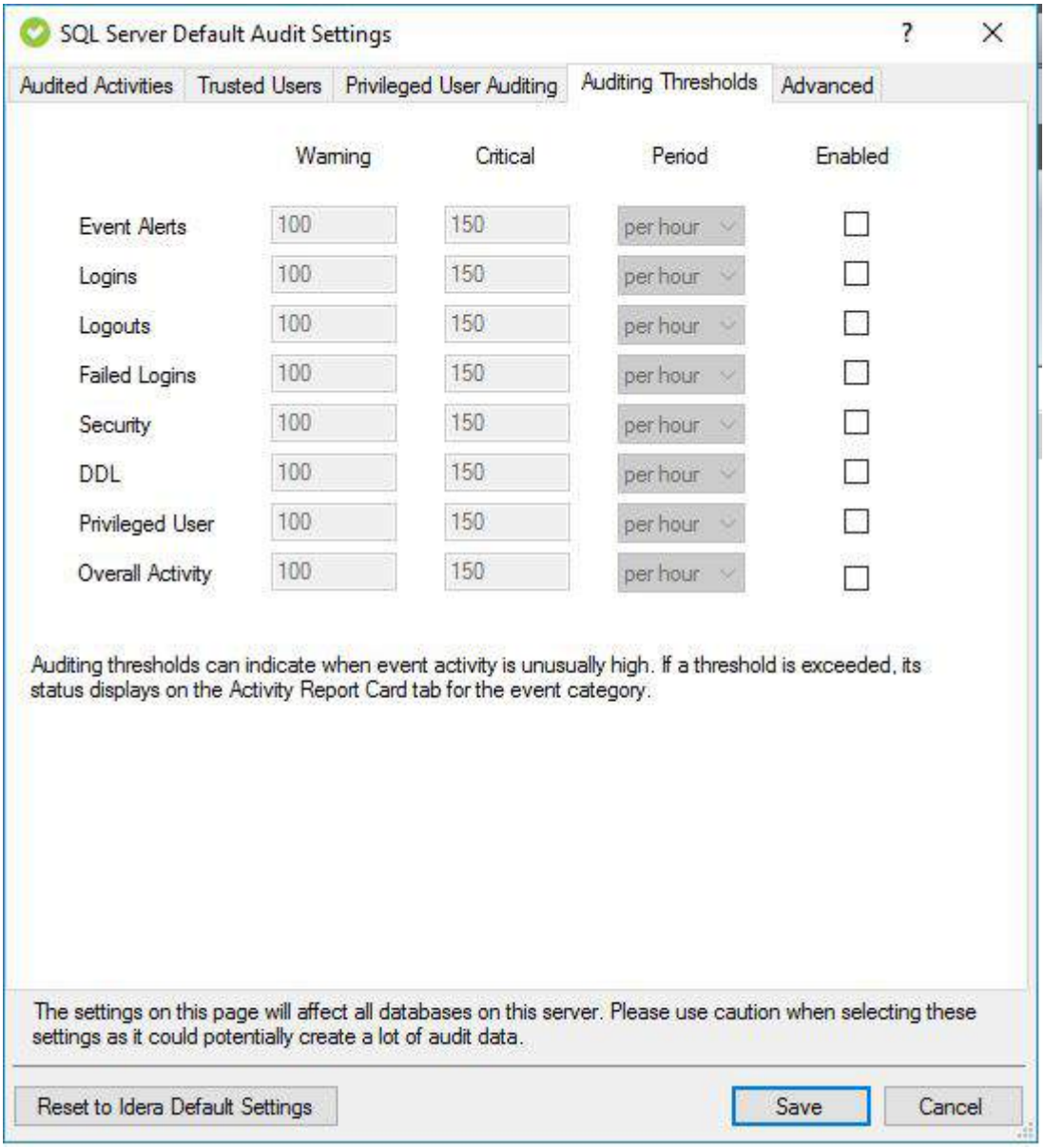
Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

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.

Auditing Thresholds tab

The Auditing Thresholds tab of the SQL Server Default Audit Settings window allows you to set auditing thresholds to identify unusual activity on SQL Server instances. IDERA 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 in 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 in this instance.

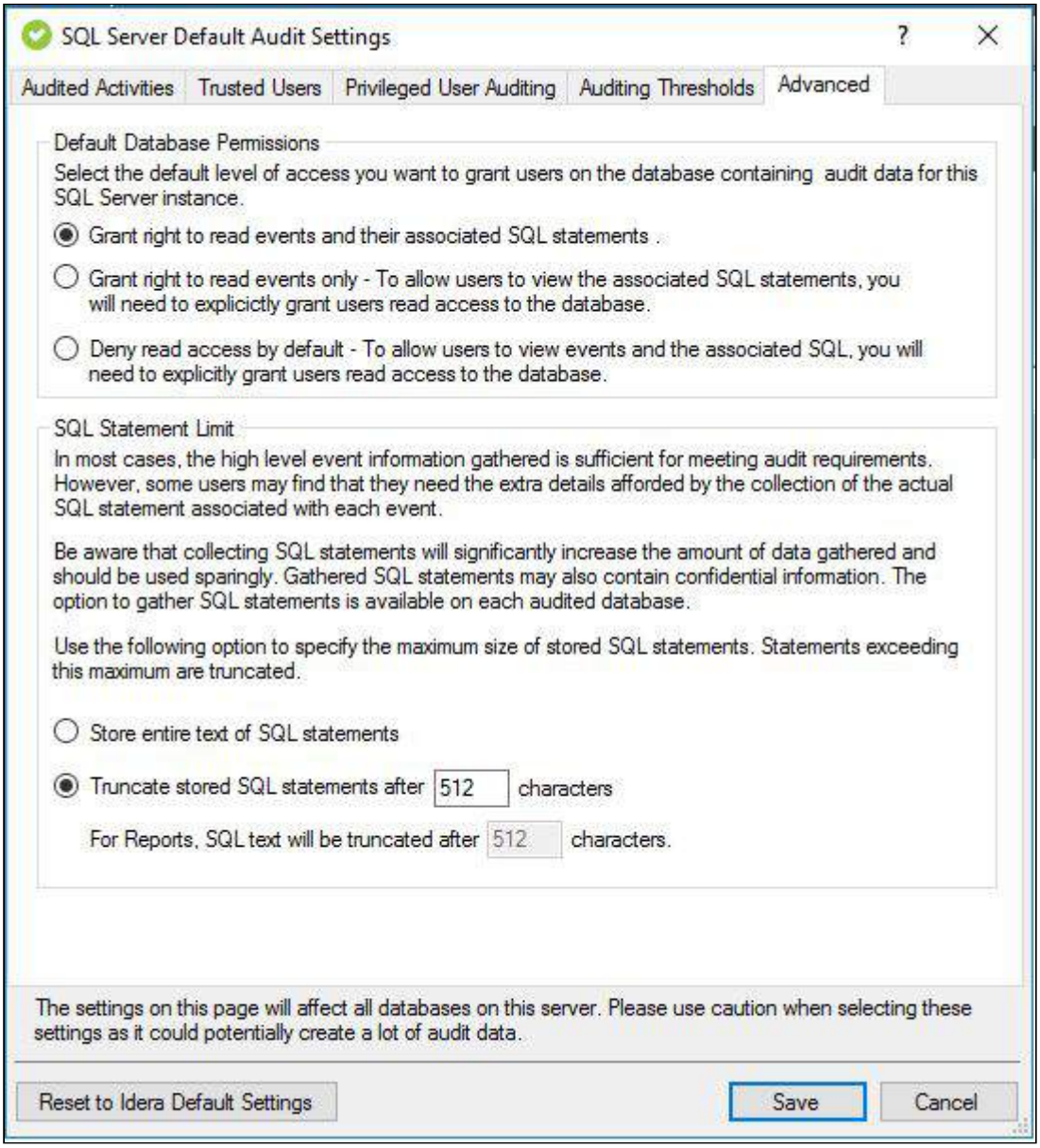
Enabled

Allows you to enable (select) or disable (clear) auditing thresholds for a particular event category.

Advanced tab

The Advanced tab of the SQL Server Default Audit Settings window 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:

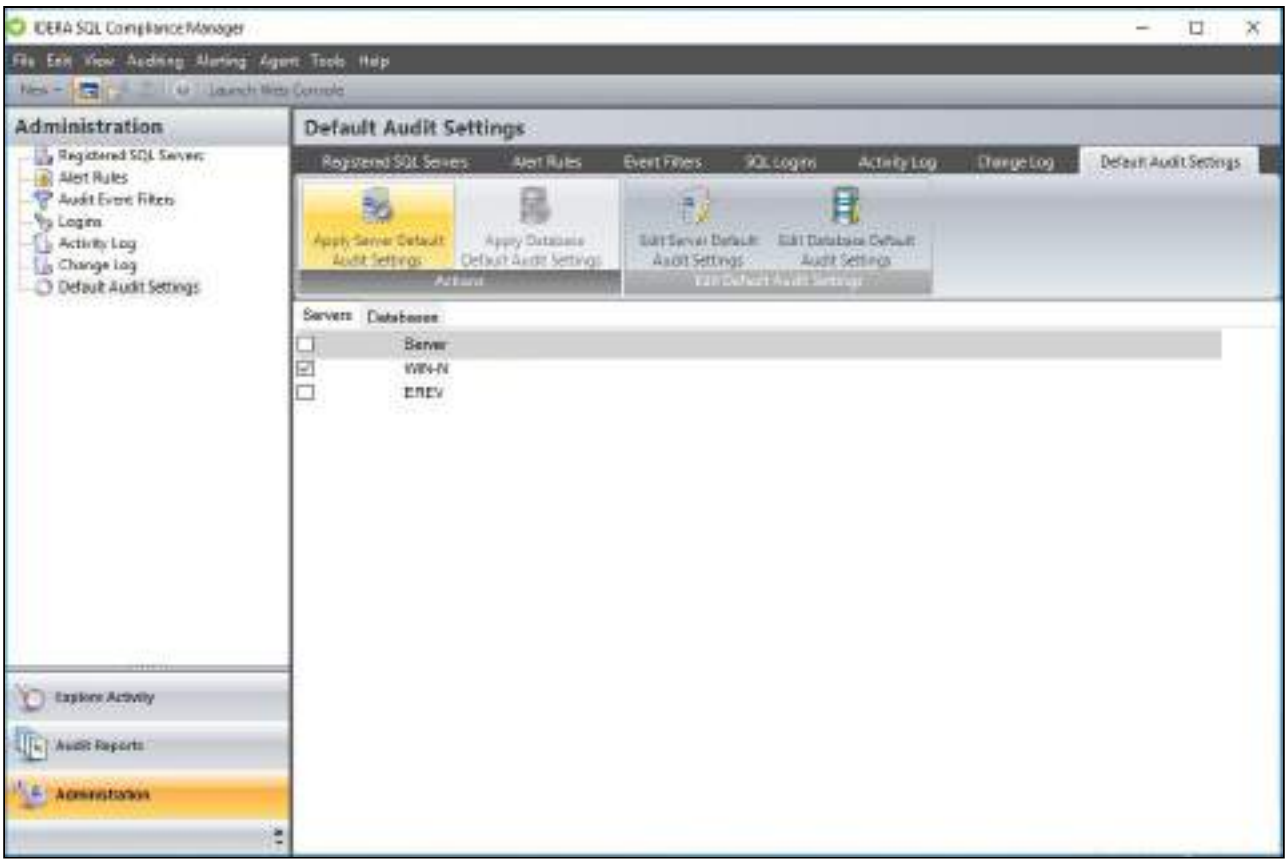
- Grant permission to view events and associated SQL statements
- Grant permission to view events only
- Deny permission to view events or SQL statements

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.

Apply Server Default Audit Settings

Use the Apply Server Default Audit Settings option to apply your configured Server default audit settings across your registered SQL Servers. Once you edit and configure your desired SQL Server Default Audit settings, select from the list of registered servers the ones to which you wish to apply your Server default settings.



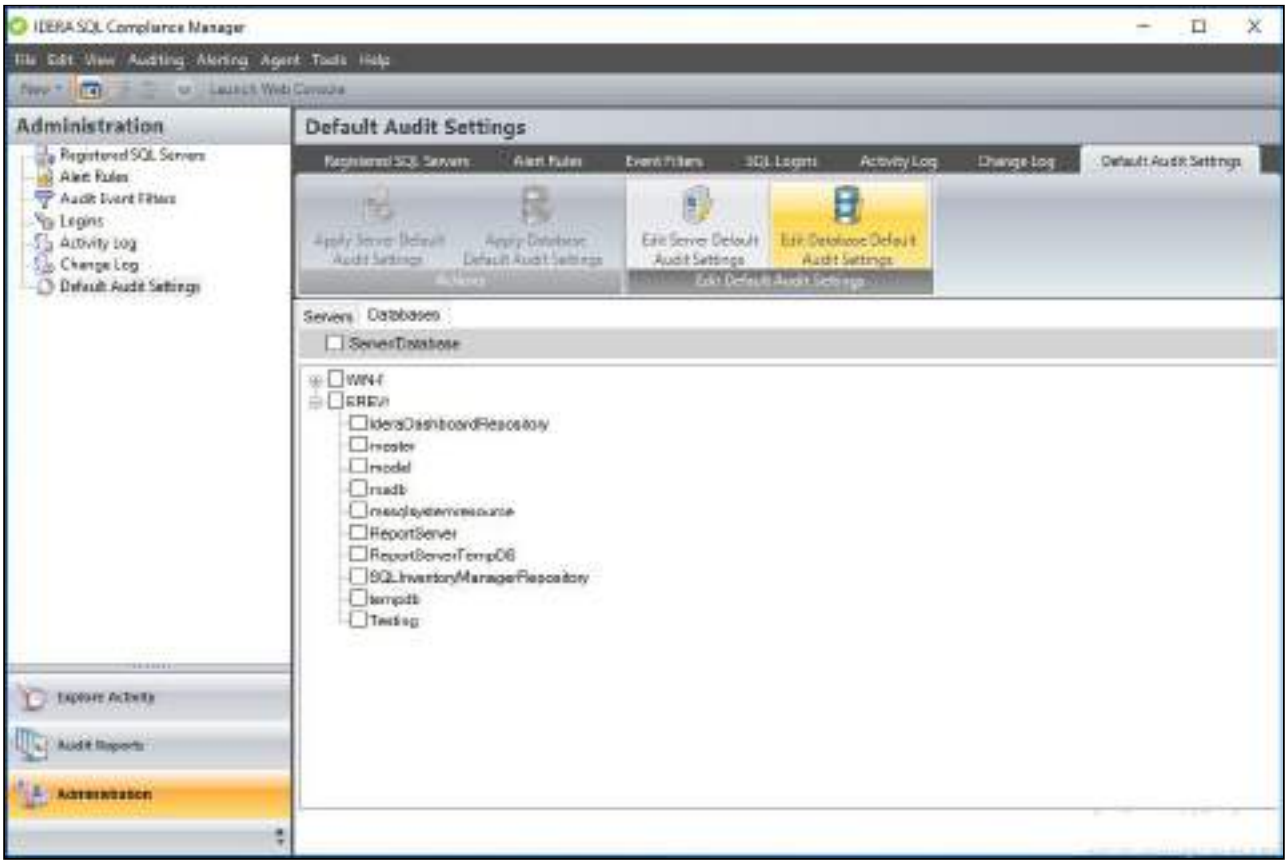
To Apply Server Default Audit Settings follow the steps below:

1. From the **Administration** view, select the **Default Audit Settings** tab.
2. Configure your desired Server Default Settings, for more information on how to configure Server Default Settings, visit the Edit Server Default Audit Settings page.

3. Under the **Servers** tab, select the SQL Server Instances to which you want to apply the Default Server settings and click the **Apply Server Default Audit Settings** option.
4. Review the confirmation window and click the **Apply Server Default Audit Settings** button.

Edit Database Default Audit Settings

Use the Edit Database Default Audit Settings window to configure your Default Database audit settings exactly the way you want without having to make additional updates to your configurations. You can later choose to apply these default settings to any audited database or to newly added databases.



> ⚠ Sensitive Columns and BAD are not available for the Database Default settings since those tables will vary greatly from database to database.

To Edit Database Default Audit Settings follow the steps below:

1. From the **Administration** view, select the **Default Audit Settings** tab.
2. Click the **Database Server Default Audit Settings** option.
3. Set your desired SQL Database Default Audit Settings, for more information on how to configure these settings, visit the SQL Database Default Settings page.
4. Click **Save.**

Users can reset back to the Idera Default Audit Settings at any time by clicking the **Reset to Idera Default Settings** button.

SQL Database Default Audit Settings Properties

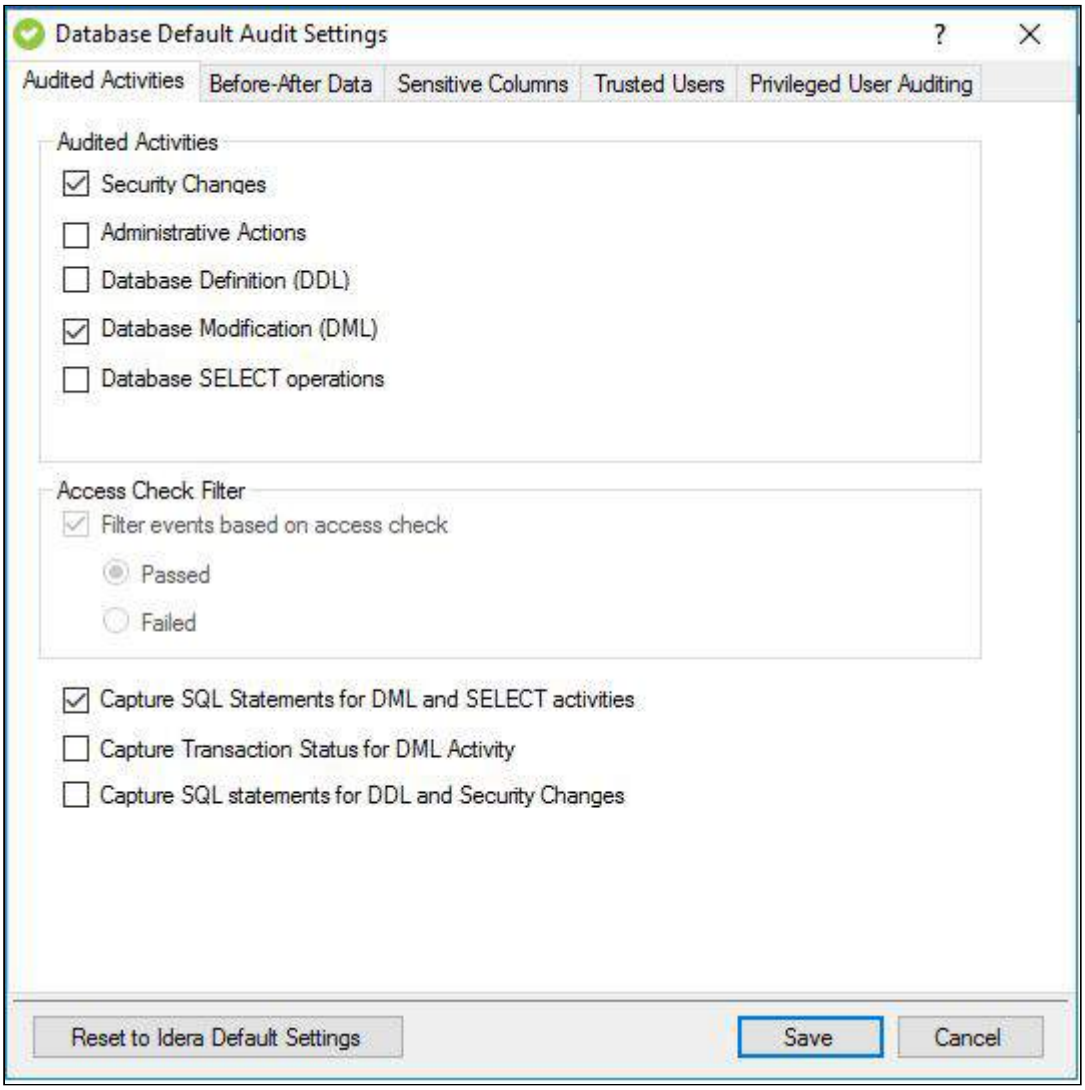
The IDERA SQL Compliance Manager SQL Database Default Audit Settings window allows you to configure your default database settings.

This topic reviews the following tabs:

- Audited Activities tab
- Before and After Data
- Sensitive Columns
- Trusted Users tab
- Privileged User Auditing tab

Audited Activities tab

The Audited Activities tab allows you to change which types of SQL Server events you want to audit. IDERA SQL Compliance Manager audits these events at the server level only.



Available fields

Audited Activity

Allows you to select the type of activity you want to audit. Based on your selections, SQL Compliance Manager collects and processes the corresponding SQL Server events.

The following are the activities you can audit:

Security changes

Administrative Actions

Database Definition (DDL)

Database Modification (DML)

Database SELECT operations

Note

Audited Activities selected at the Default Database level settings are automatically pre-selected and disabled for selection when adding new Privileged Users at the Default Database Privileged User auditing configurations.

Note

When deselecting an audited activity, choose between deselecting at Database level auditing only or at the Database level and Privileged Users auditing.

Access Check Filter

Allows you to refine your SQL Server login data audit trail 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 Compliance Manager 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.

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.

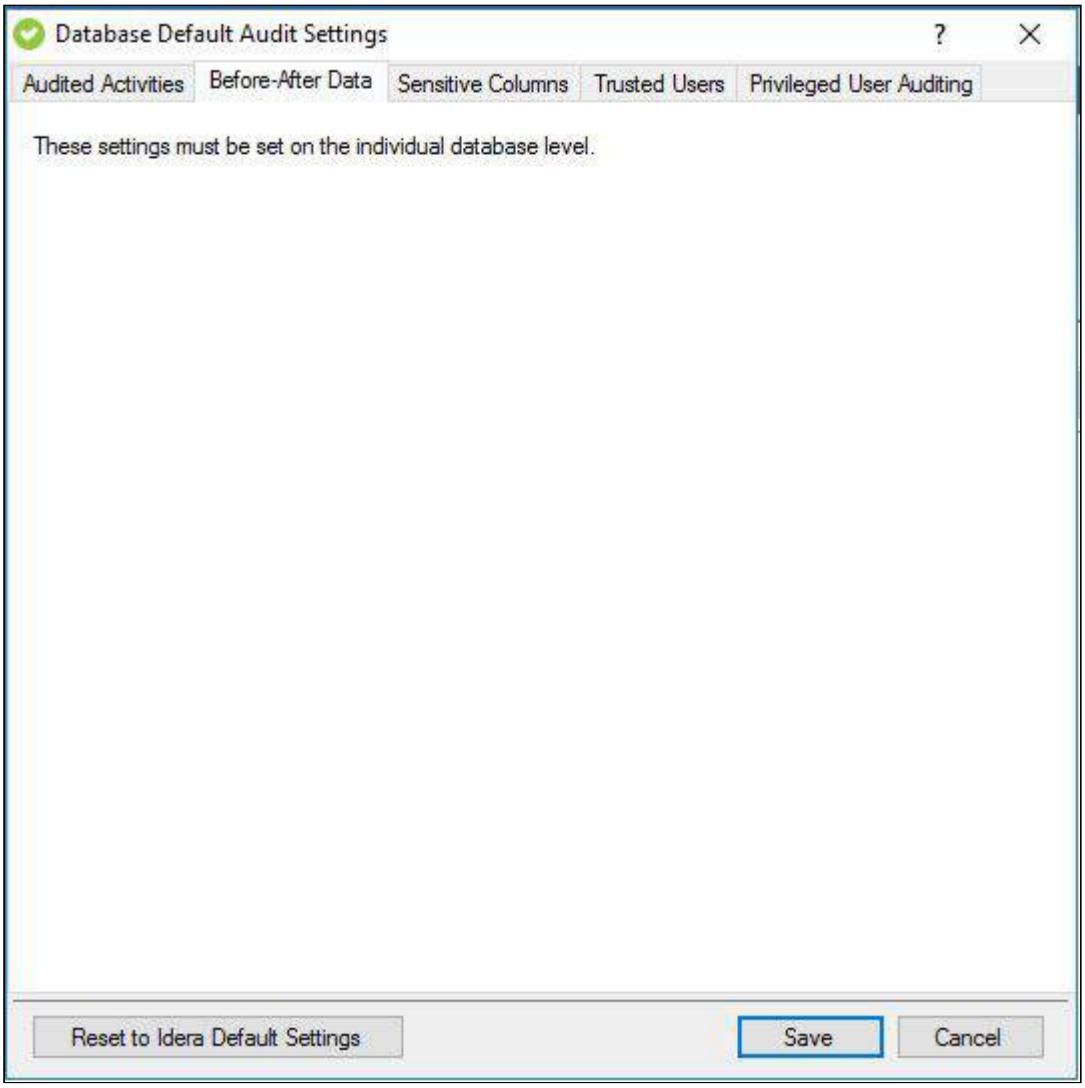
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

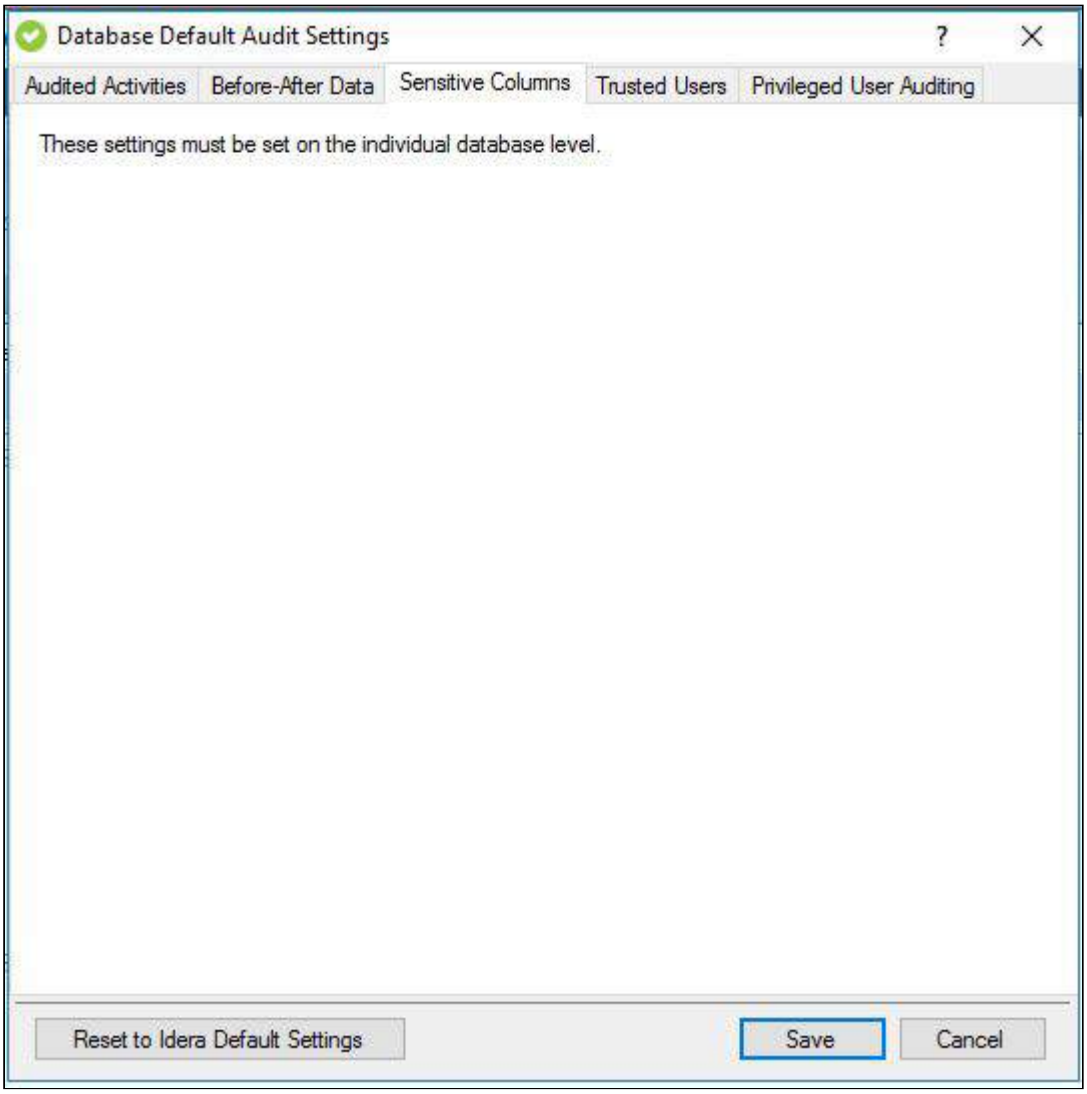
Before and After tab

These settings must be applied on the individual database level. For more information on applying this feature to individual databases, please see Audited Database Properties - Before and After Data.



Sensitive Columns tab

These settings must be applied on the individual database level. For more information on how to apply this feature on individual databases, please see Audited Database Properties - Sensitive Columns.



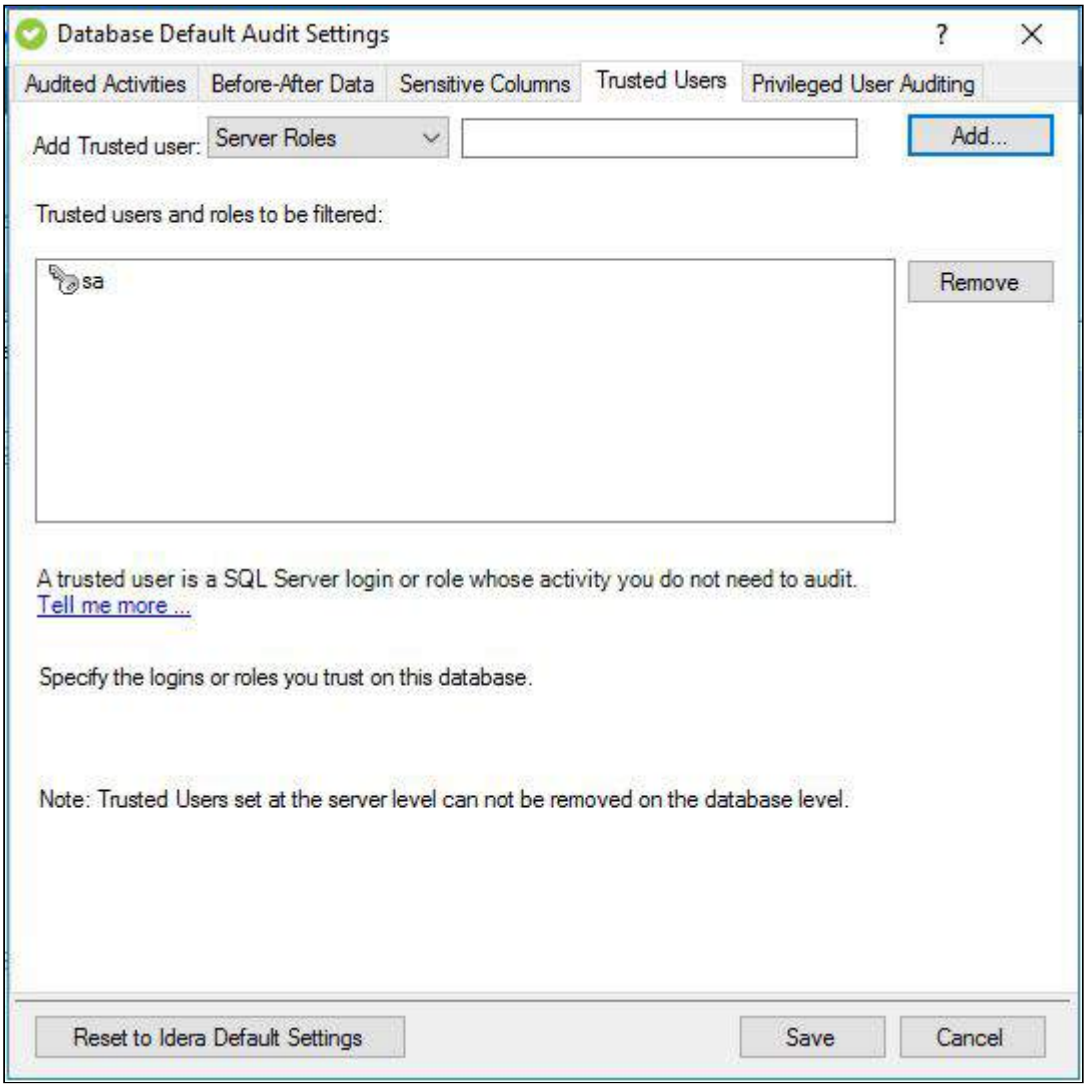
Trusted Users tab

The Trusted Users tab of the SQL Database Default Audit Settings window allows you to add Trusted Users at the database level and set the default audit settings. Trusted users are SQL Server logins and members of SQL Server roles that you trust to read, update, or manage a particular audited server or 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. This exclusion occurs for all auditing, including DML and SELECT events related to sensitive columns and before and after data.

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

Suppose you are auditing privileged user activity, and the trusted user is also a privileged user. In that case, IDERA 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, select the SQL Server login or role you want to trust and click **Add**.



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 SQL Compliance Manager 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.

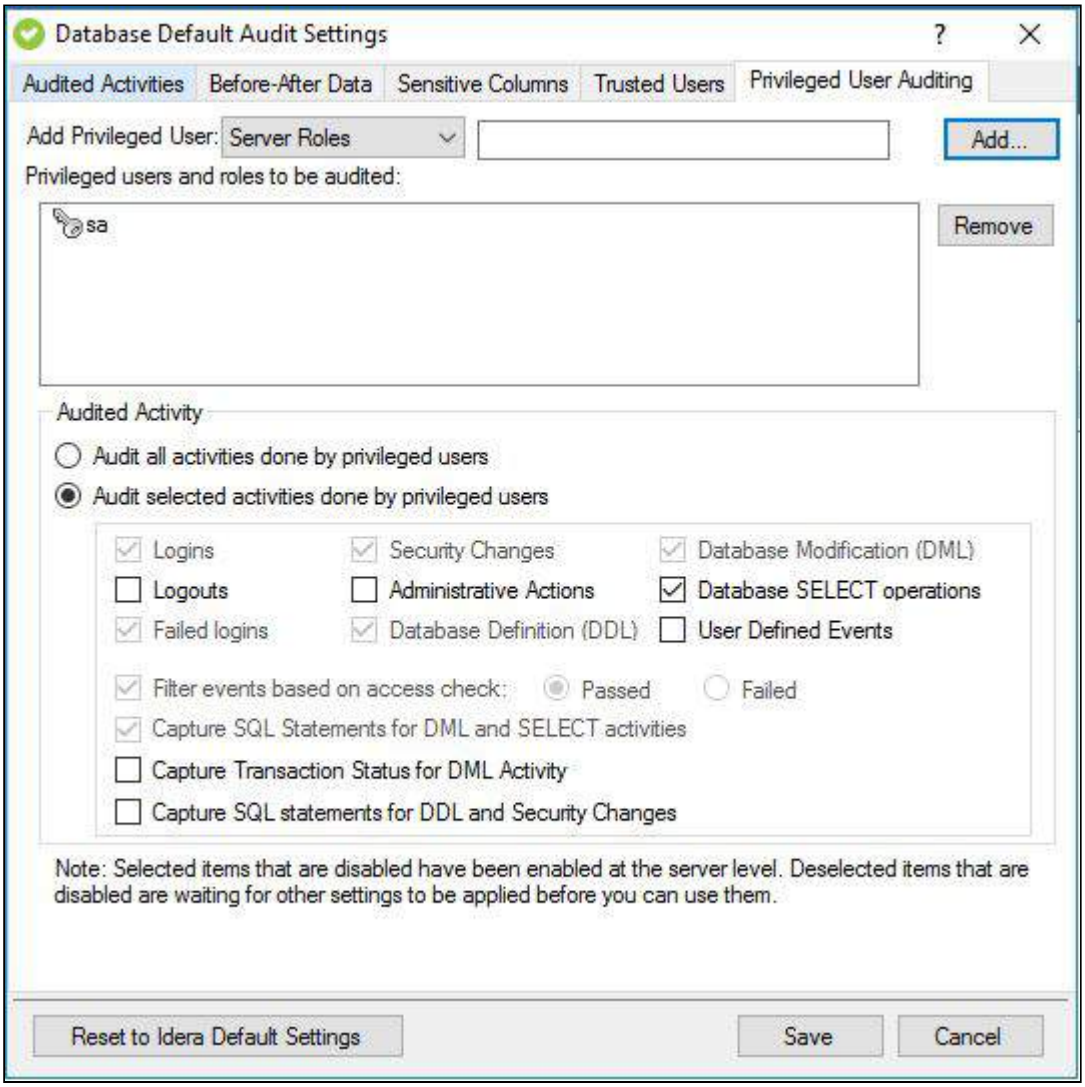
Privileged User Auditing tab

The Privileged User Auditing tab of the SQL Server Default Audit Settings window allows you to add Privileged Users at the server level and set the default audit settings to be applied on SQL Server instances. 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 SQL Compliance Manager 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 add one or more privileged users to audit. You can add privileged users by Server Roles or by Server Logins.

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 SQL Compliance Manager Agent no longer collects events recorded for that login or the role members.

> **Note**
>
> Privileged Users selected at the Default Server level auditing are pre-selected and disabled for selection. These Privileged Users can be removed only at the Default Server level Privileged Users auditing.

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 SQL Compliance Manager 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.

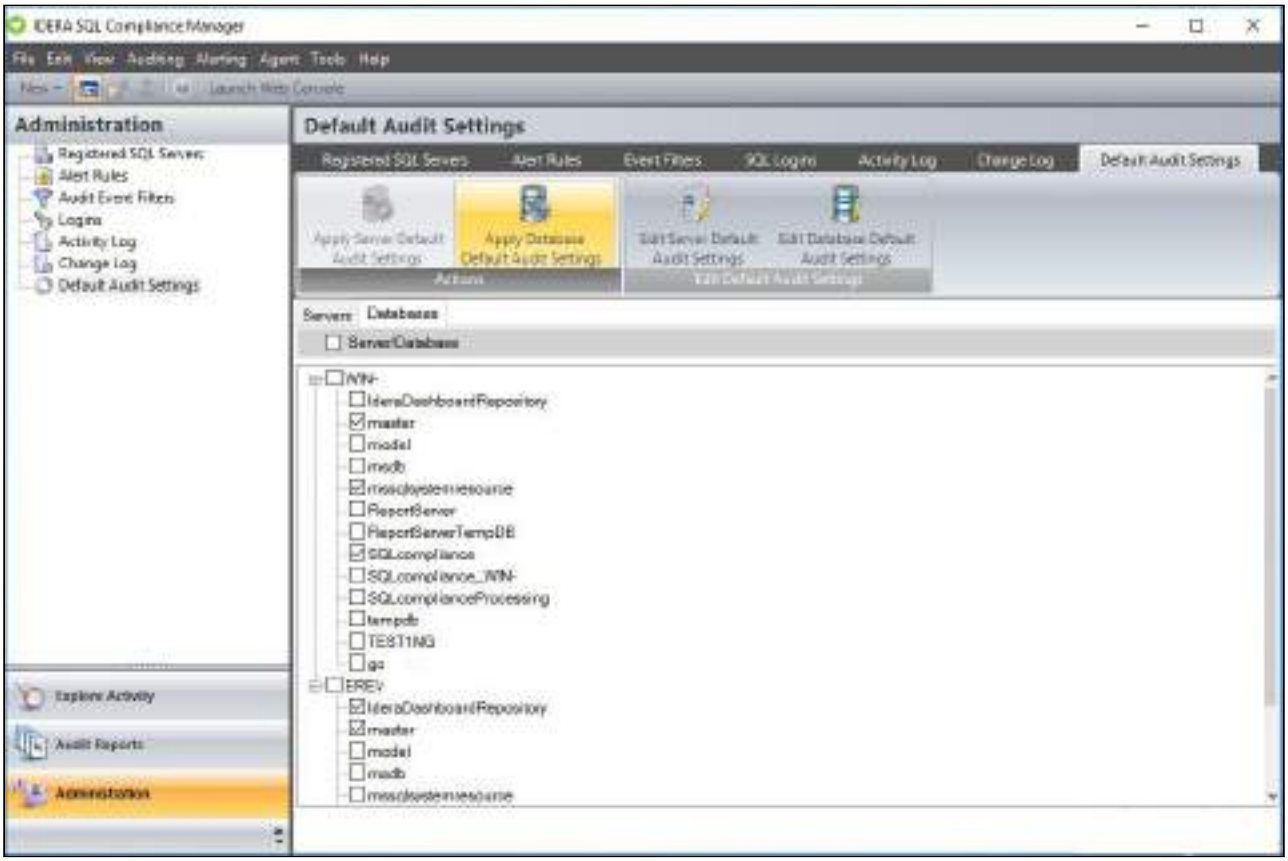
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

Apply Database Default Audit Settings

Use the Apply Database Default Audit Settings option to apply your configured database default settings across your audited databases. Once you edit and configure your desired SQL Database Default Audit settings, select from the list of audited databases the ones to which you wish to apply your database default settings.



To Apply Database Default Audit Settings follow the steps below:

1. From the **Administration** view, select the **Default Audit Settings** tab.
2. Configure your desired Database Default Settings, for more information on how to configure default database settings, visit the Edit Database Default Audit Settings page.
3. Under the **Databases** tab, select one or more databases from the list to which you want to apply the Default Server settings and click the **Apply Database Default Audit Settings** option.
4. Review the confirmation window and click the **Apply Database Default Audit Settings** button.

9.4 SQL Compliance Manager Menu

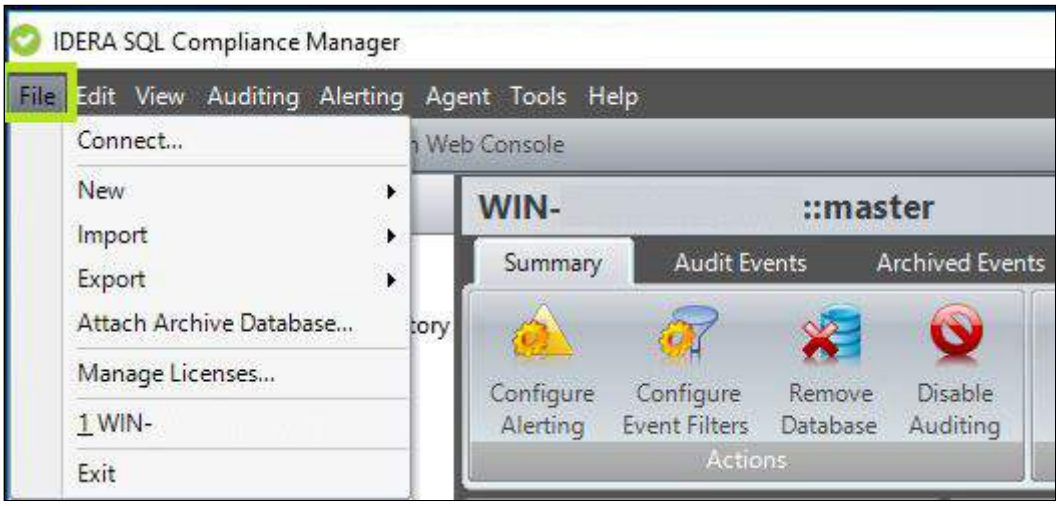
The SQL Compliance Manager Menu provides users the ability to perform quick actions regarding auditing, alerting and agent activity. Users can also use the menu options to change the console display or configure the console preferences. Explore the different Menu options with the links below.

Click on the options below to learn more about each of the SQL Compliance Manager Menu options:

- SQL Compliance Manager Menu - File
- SQL Compliance Manager Menu - Edit
- SQL Compliance Manager Menu - View
- SQL Compliance Manager Menu - Auditing
- SQL Compliance Manager Menu - Alerting
- SQL Compliance Manager Menu - Agent
- SQL Compliance Manager Menu - Tools

9.4.1 SQL Compliance Manager Menu - File

The File option from the SQL Compliance Manager Menu allows users perform a series of activities such as to add new SQL Servers, Databases or Logins. Users can perform quick Import or Export operations as well as to Manage their Product Licenses.



Available actions

Connect

The Connect to Repository window allows you to connect to a different installation of the IDERA SQL Compliance Manager Repository. You can type the name of the SQL Server instance that hosts the Repository databases or browse for the instance

New

Registered SQL Server - Starts the New Registered SQL Server wizard, allowing you to enable and configure auditing on another SQL Server instance.

Audited Databases - Starts the New Audited Database wizard, allowing you to enable auditing on additional databases hosted by this SQL Server instance. For more information, see Add Audited Databases.

SQL Server 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. For more information, see Create a login.

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

Event Filter - Allows you to create a new event filter using the New Event Filter wizard. IDERA SQL Compliance Manager stores this event filter in the Repository.

Import

Audit settings - Allows you to import audit settings previously exported from another audited instance or database. For more information, see Import your audit settings wizard.

Alert Rules - Allows you to import alert rules previously exported from another SQL Server instance. By default, the imported alert rules are disabled. For more information. see Import your alert rules.

Event Filters - Allows you to import Event Filters previously exported from another SQL Server instance. By default, the imported Event Filters are disabled. For more information, see Import your Event Filters.

Export

Audit settings - 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.

Alert 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. For more information, see Export your alert rules.

Event 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. For more information, see Export your Event Filters.

Attach Archive Database

The Attach Archive Database window allows you to open an archive database so you can view and report on previously collected audit data. For more information, see Attach Archive Database window.

Manage Licenses

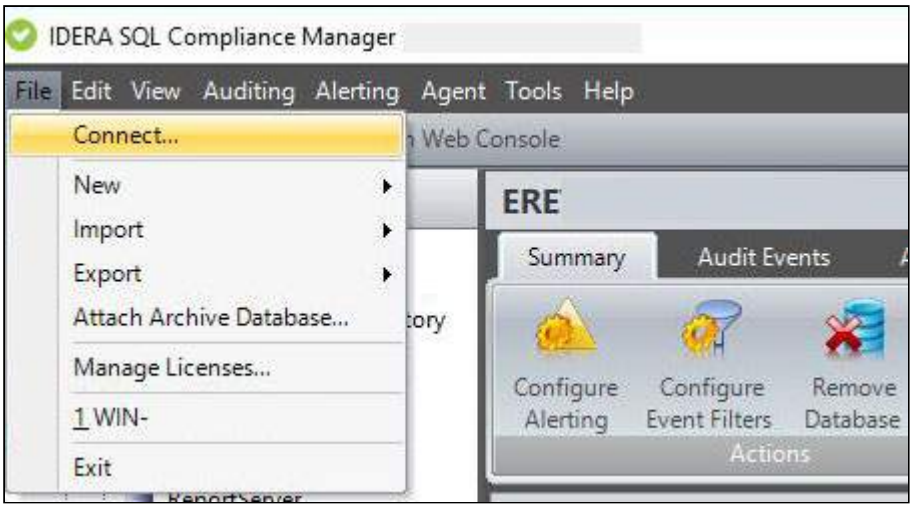
The Manage SQL Compliance Manager Licenses window allows you to view details about your IDERA SQL Compliance Manager product license.

Exit

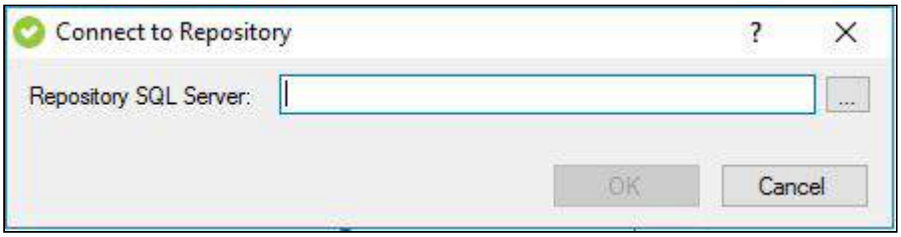
Exits the SQL Compliance Manager Windows Console.

Connect to Repository window

The Connect to Repository window allows you to connect to a different installation of the IDERA 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.**



Attach Archive Database window

The Attach Archive Database window allows you to open an archive database so you can view and report on previously collected audit data.

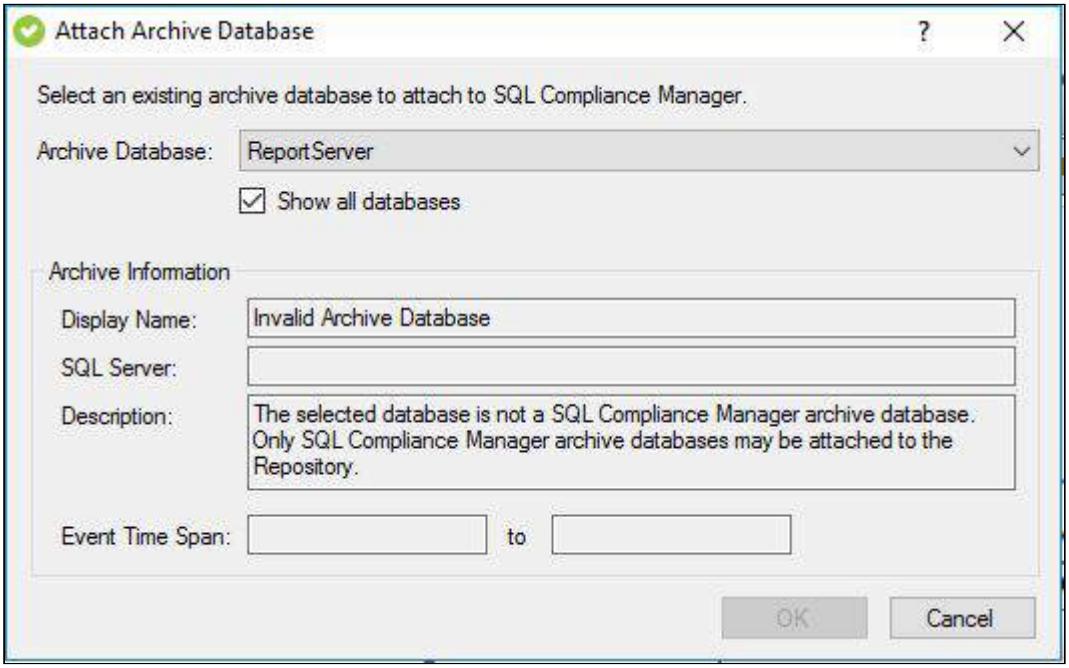
Available fields

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.



Manage SQL Compliance Manager Licenses window

The Manage SQL Compliance Manager Licenses window allows you to view details about your IDERA 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

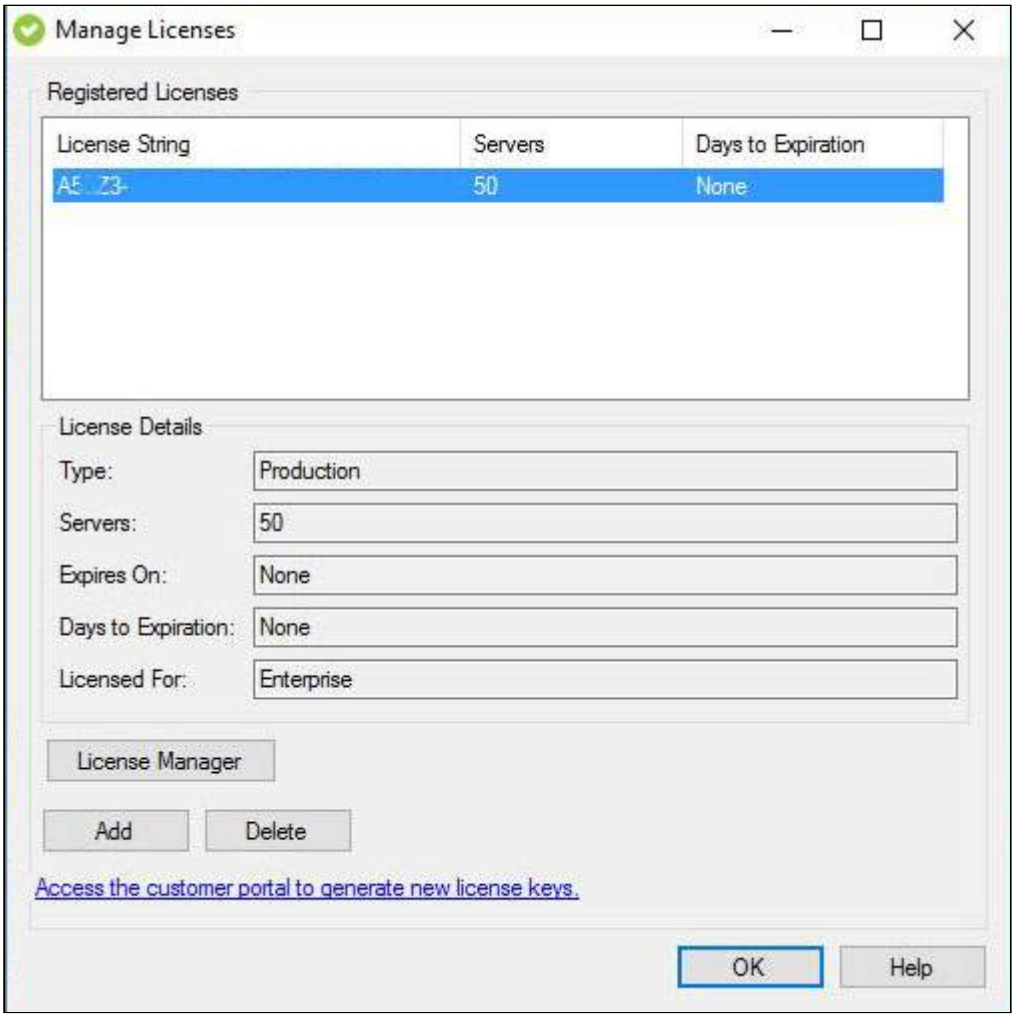
Available actions

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**.

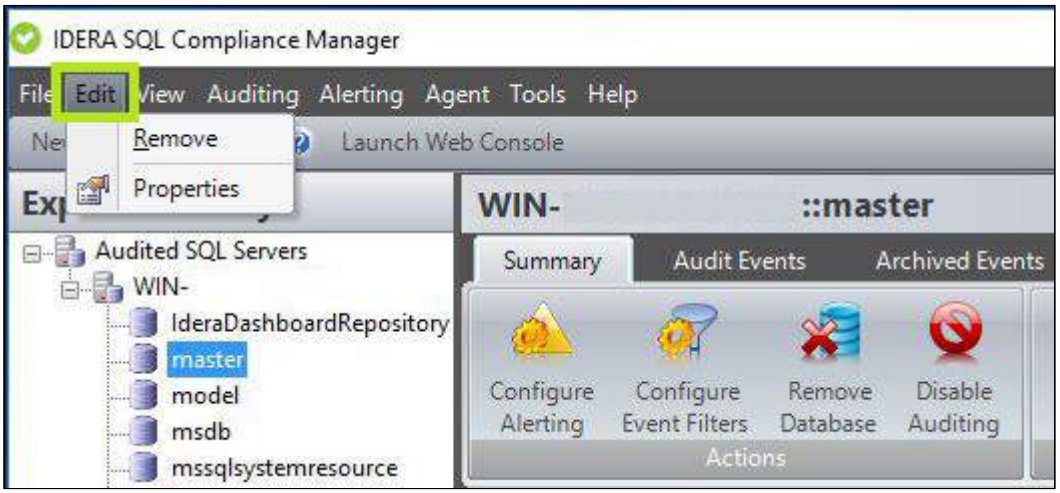
Delete

Allows you to permanently decommission a license key. This action removes the license key from the Repository.



9.4.2 SQL Compliance Manager Menu - Edit

The Edit option from the SQL Compliance Manager Menu allows users configure their desired SQL Server and Databases Properties, as well as to Remove any undesired SQL Server or Database.



Available actions

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 Compliance Manager also uninstalls the SQL Compliance Manager Agent. ***If you manually deployed the SQL Compliance Manager Agent,*** you must manually uninstall it from the SQL Server computer.

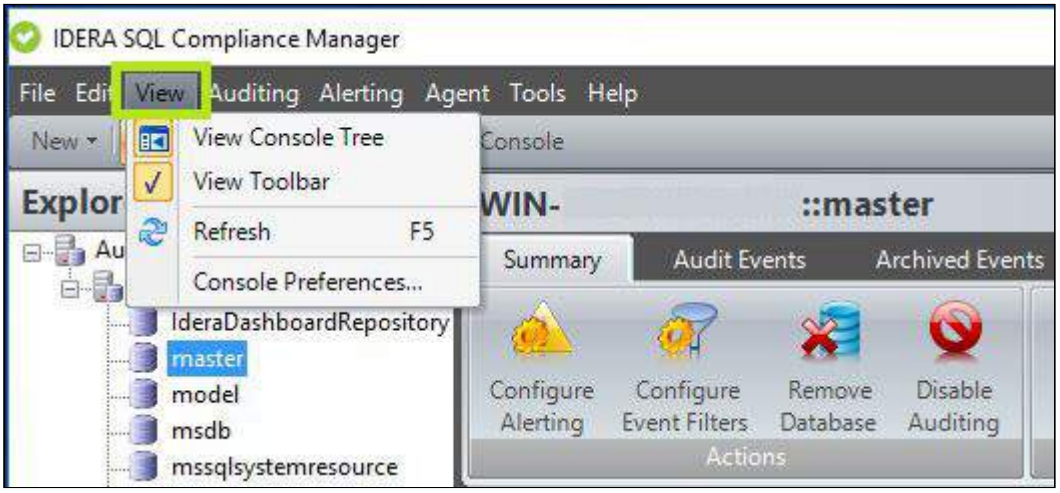
⚠ If there are any backlogged audit trace files that you need to process for the instance you are considering to decommission, make sure to disable auditing and decommissioning your server only after processing these backlogged audit trace files. For additional information on how to process backlogged trace files, please contact Idera Support.

Properties

Allows you to change the audit settings for the selected SQL Server instance. For more information, see Registered SQL Server Properties.

9.4.3 SQL Compliance Manager Menu - View

The View option from the SQL Compliance Manager Menu allows users to configure the Console Preferences, as well as to choose whether to display or not the Console Tree view and the Toolbar view.



Available actions

View Console Tree

Allows users to choose whether to display or to hide the Console Tree pane.

View Toolbar

Allows users to choose whether to display or to hide the Toolbar.

Refresh

Refresh the SQL Compliance Manager Windows Console.

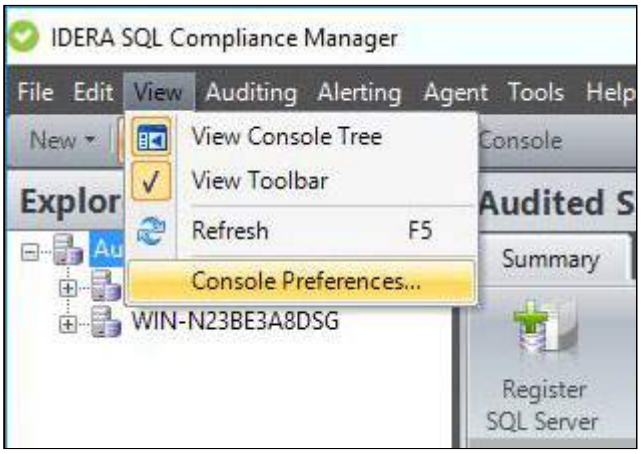
Console Preferences

Opens the Console Preferences window, allowing users to configure how the IDERA SQL Compliance Manager Management Console displays events in the Audited Events tab. In the Console Preferences users can also define the number of alerts that display per view page.

Console Preferences window - Event Views window

The Event Views window allows you to configure how the IDERA SQL Compliance Manager 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.

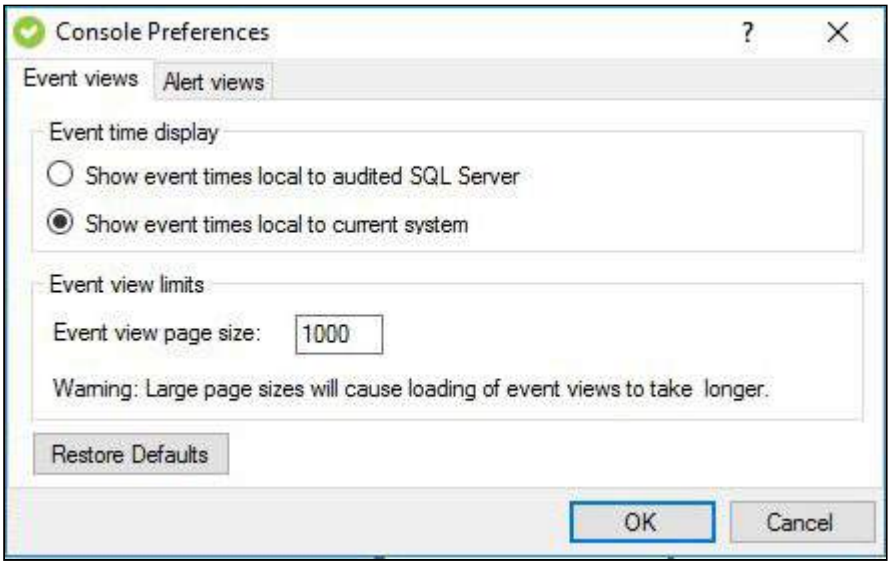
Available fields

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.

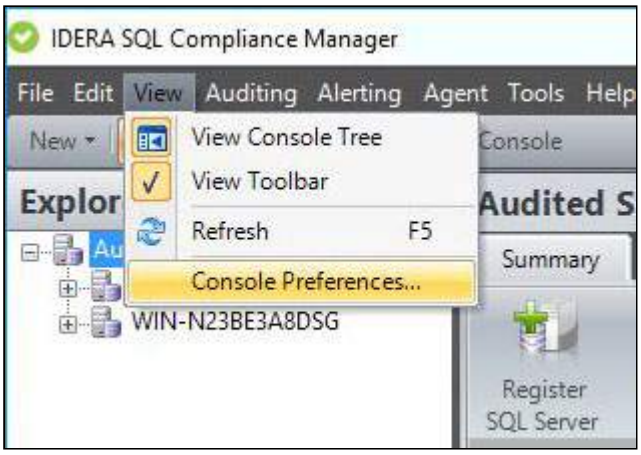
Event view limits

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.



Console Preferences window - Alert Views window

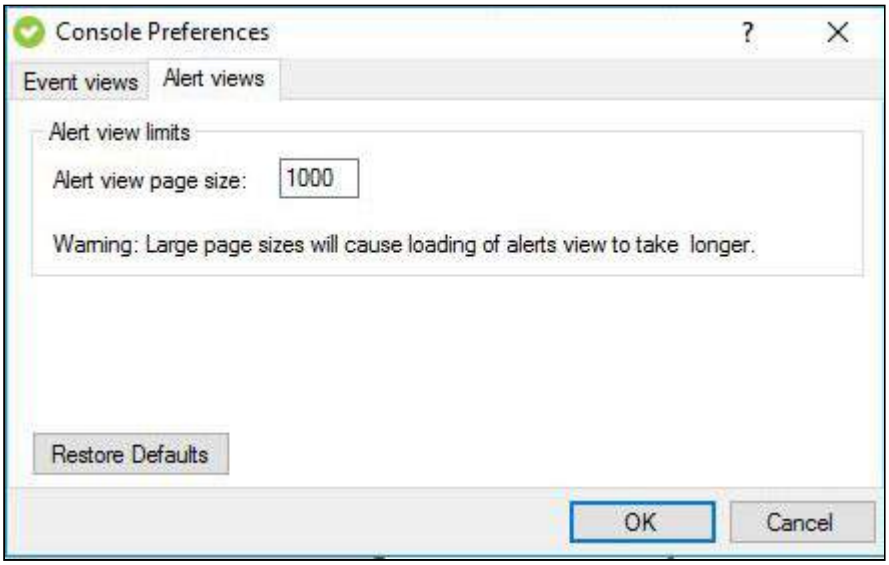
The Alert Views window allows you to define the number of alerts that display per view page. Specify the appropriate value, and then click **OK**.



Available actions

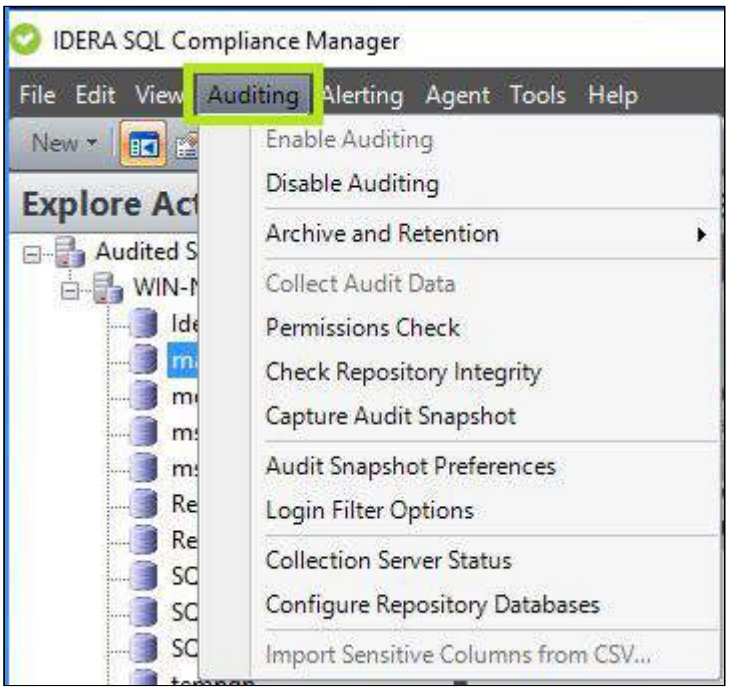
Restore Defaults

Allows you to restore the console settings to the default values.



9.4.4 SQL Compliance Manager Menu - Auditing

The Auditing option from the SQL Compliance Manager Menu allows users to quickly perform various auditing activities, such as to Check the Repository Integrity, Disable Auditing, Capture Snapshots or to Configure Repository Databases. Perform a Permissions Check on your audited databases and registered servers, or quickly configure your Login Filter Options using the SQL Compliance Manager Auditing Menu option.



Available actions

Enable Auditing

Server level - 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 Enable auditing on a SQL Server.

Database level - Enabling auditing on the database allows you to capture SQL events at the database level. For more information, see Enable auditing on a database.

Disable Auditing

Server level - You can disable auditing on any registered SQL Server instance and the associated databases. When you disable auditing, IDERA 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. For more information, see Disable auditing on a SQL Server.

Database level - You can disable auditing on any database associated with a registered SQL Server instance. When you disable auditing, IDERA 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. For more information, see Disable auditing on a database.

Archive and Retention

Archive Audit Data Now - Allows you to archive audit data. 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. For more information, see Archive Audit Data Now window.

Groom Audit Data Now - 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. For more information, see Groom Audit Data Now window.

Archive Preferences - 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. For more information, see Archive Preferences window.

Collect Audit Data

Allows you to force the SQL Compliance Manager Agent to send trace files to the Collection Server for processing. Typically, the SQL Compliance Manager Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

Permissions Check

Displays the results of a check of the permissions required by IDERA SQL Compliance Manager on the SQL Server instance you want to monitor. This check runs automatically each time you register a new instance. For more information, see Permission Check.

Check Repository Integrity

Allows you to check for unexpected changes in your audit data, detecting when events are modified, added, or deleted by a script or an application other than IDERA SQL Compliance Manager. For more information, see Check Repository Integrity window.

Capture Audit Snapshot

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. For more information, see Capture Audit Snapshot window.

Audit Snapshot Preferences

Allows you to indicate whether you want IDERA SQL Compliance Manager to capture a snapshot of your audit settings at a regular interval (days). For more information, see Audit Snapshot Preferences window.

Login Filter Options

The Login Filtering Options window allows you to set login filtering. Login filtering reduces the number of login events stored in your audit data. For more information, see Login Filtering Options window.

Collection Server Status

Allows you to review the basic properties and status of the Collection Server. For more information, see Collection Server Properties window.

Configure Repository Databases

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 also view the status of your Repository databases and update indexes if necessary. For more information, see Configure Repository Databases window.

Import Sensitive Columns from CSV

Allows you to import a list of sensitive columns from a .csv file to speed the process of configuring your sensitive column auditing. Note that the .csv file must have a row for each database you want to add for sensitive column auditing. For more information, see Import Sensitive Columns window.

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.

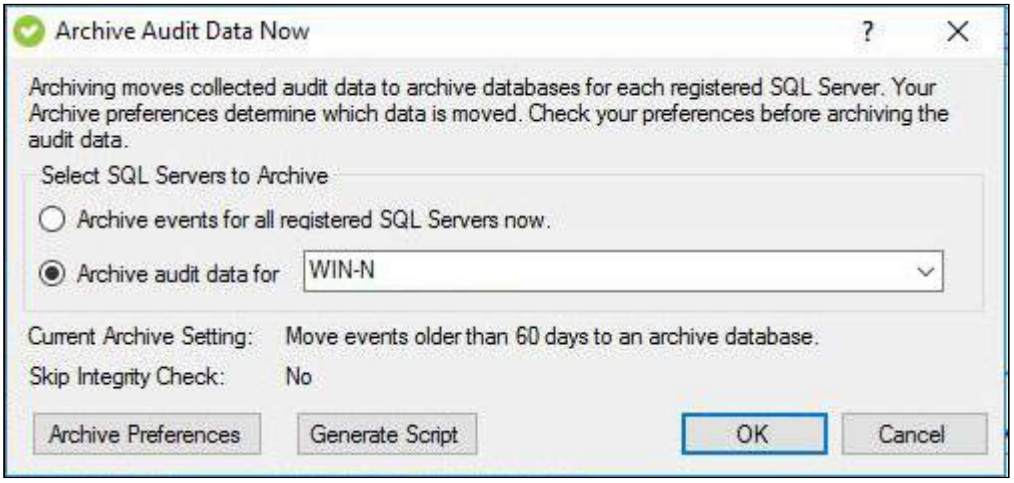
Your archive preferences determine which data is moved. Check your preferences before archiving the audit data.

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,*** IDERA 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.

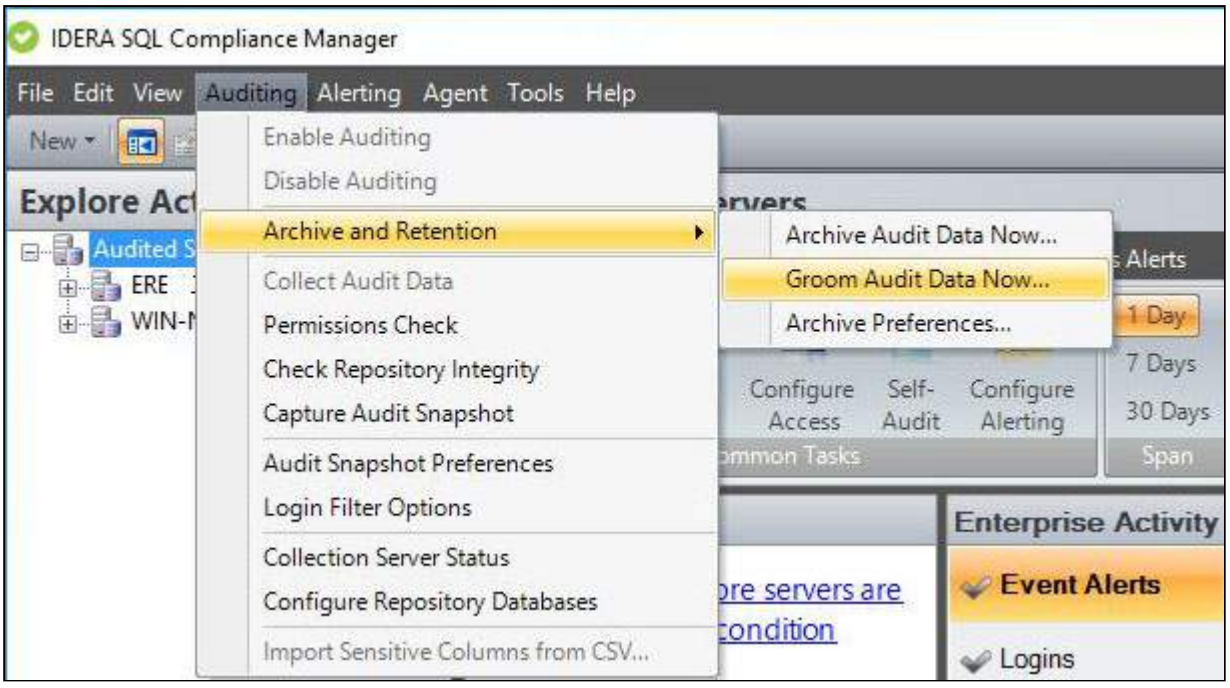
Available fields

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.

Groom Audit Data Now window

The Groom Audit Data Now 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

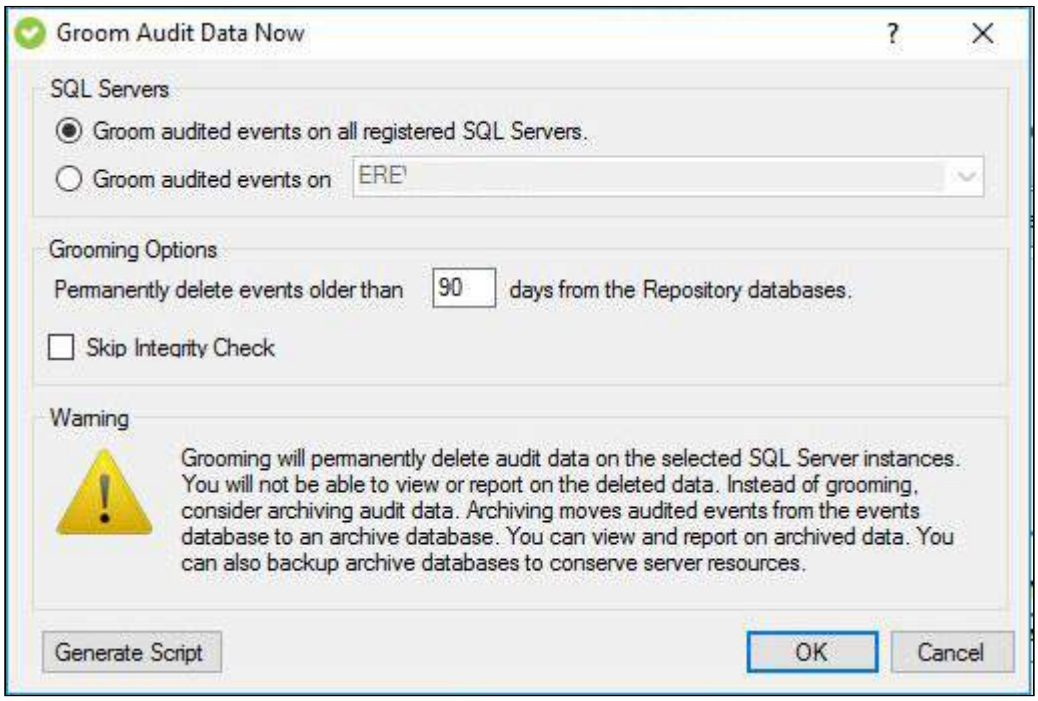
Allows you to select which SQL Server instance you want to groom. You can groom audit data for all registered SQL Server instances or for a particular SQL Server instance.

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.

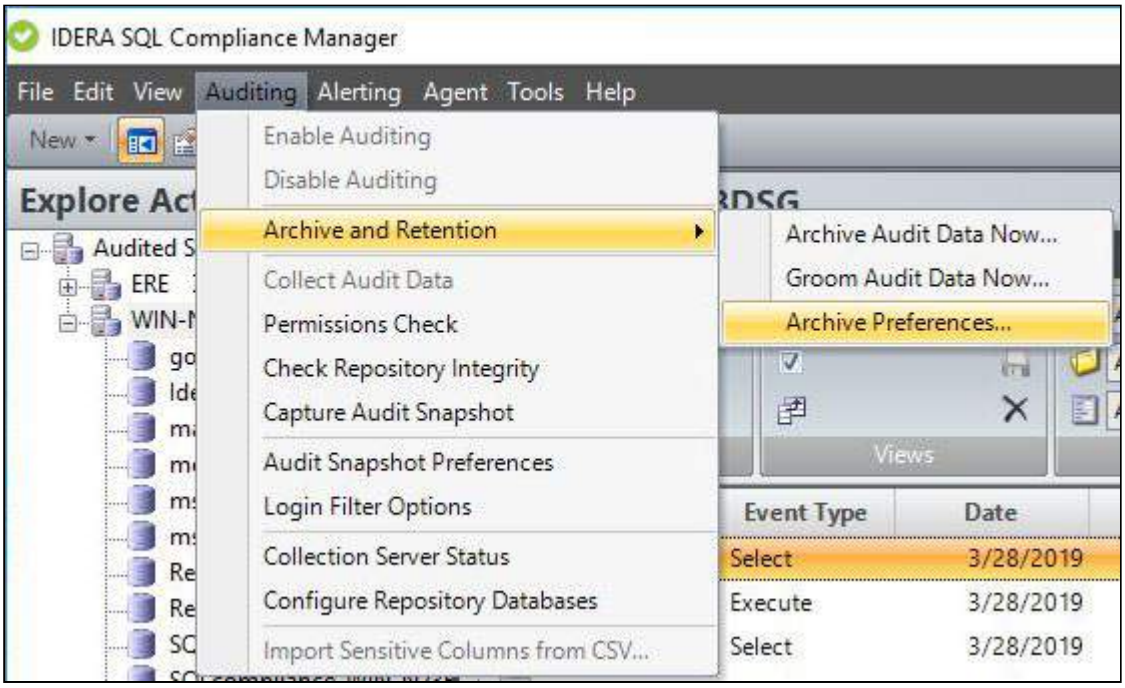
The Collection Server will not groom events that are younger than the specified age.

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,*** IDERA SQL Compliance Manager does not groom the data.



Archive Preferences window

The Archive Preferences 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. IDERA 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 Compliance Manager usually performs before archiving your collected events. ***If the audit data for the selected SQL Server instance fails this integrity check,*** SQL Compliance Manager 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.

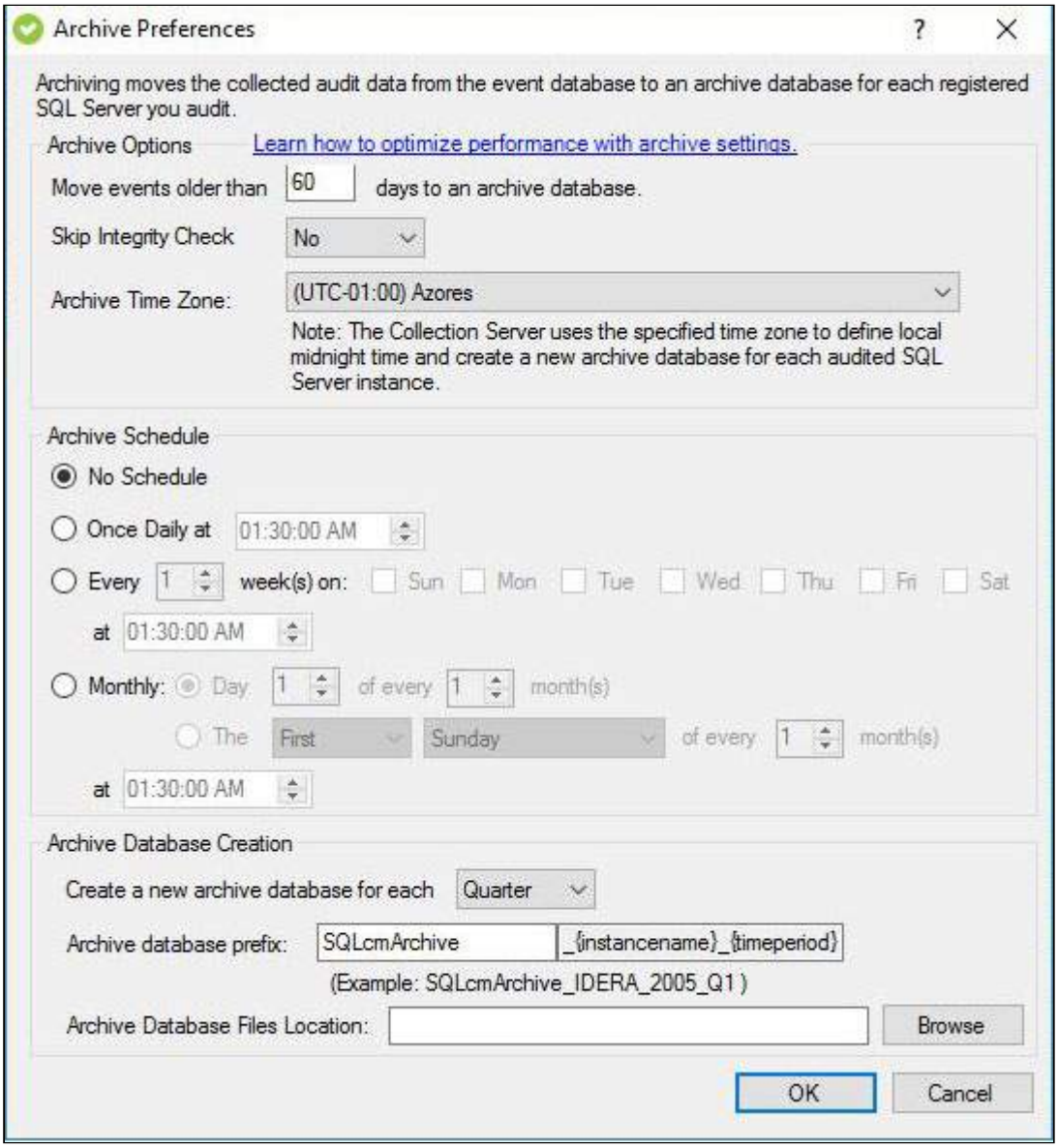
Archive Database Creation

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

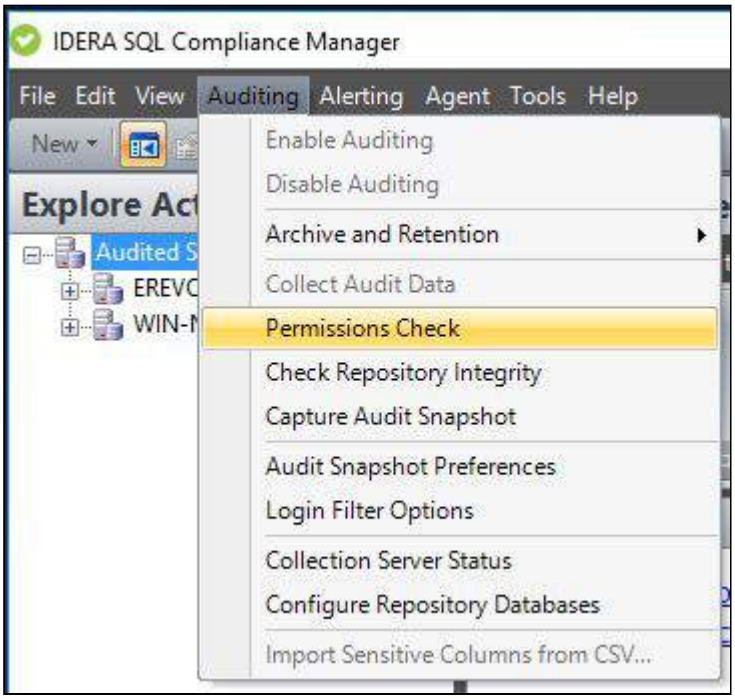
By default, the Collection Server creates a new archive database at midnight (GMT) when the specified time period (month, quarter, year) ends. For example, if you set archive creation to occur every month,

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.



Permissions Check

The Permissions Check window displays the results of a check of the permissions required by IDERA SQL Compliance Manager on the SQL Server instance you want to monitor. This check runs automatically each time you register a new instance. You can run a Permissions Check at any point in time from the Auditing menu bar.



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 is complete, click **Next** to continue.

Required permissions include:

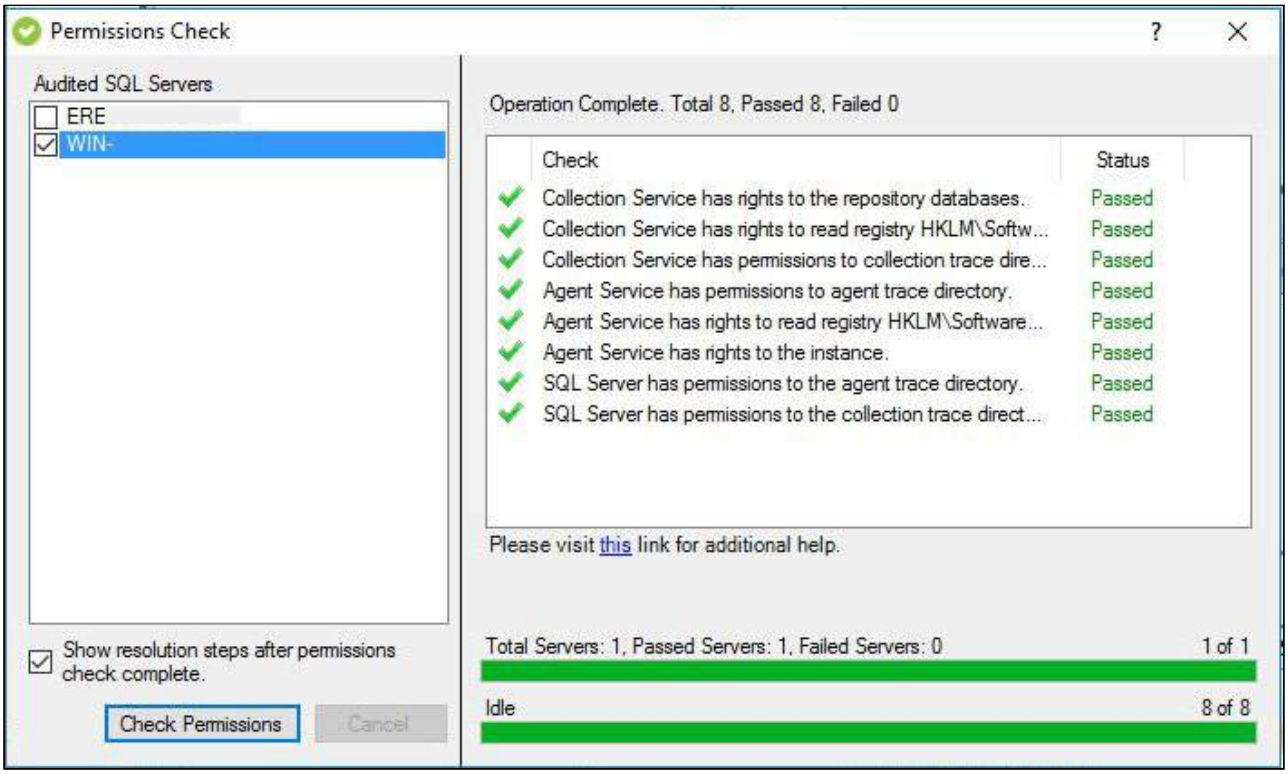
- Collection Service must have rights to the Repository databases
- Collection Service must have rights to read the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance`
- Collection Service must have permissions to the collection trace directory
- Agent Service must have permissions to the agent 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.

To successfully run and pass the Permissions Check, make sure you are logged in as one of the following users while registering an instance:

- SQL Compliance Agent Service User
- SQL Server Service User
- Current Logged-in User

For more information, see SQL Compliance Manager Permissions Requirements.



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

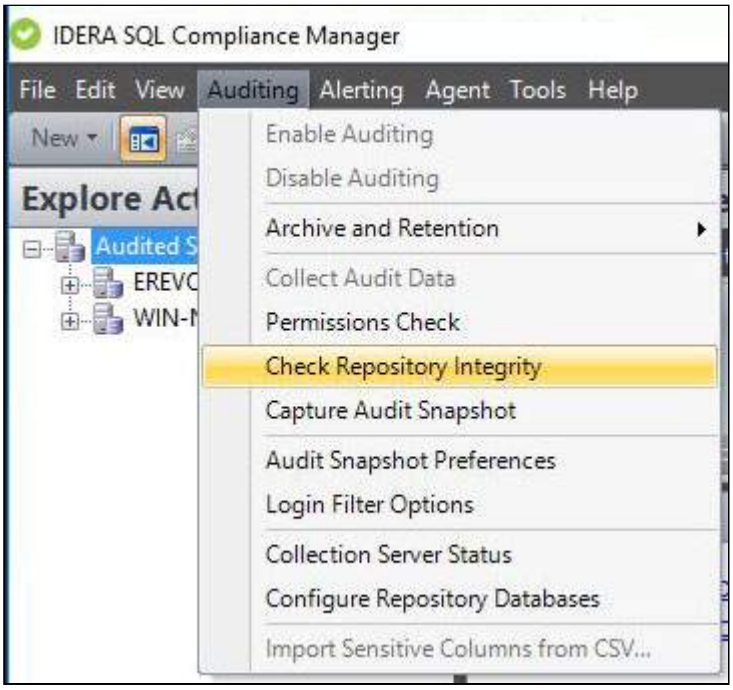
Displays the list of permissions checked in this step.

Status

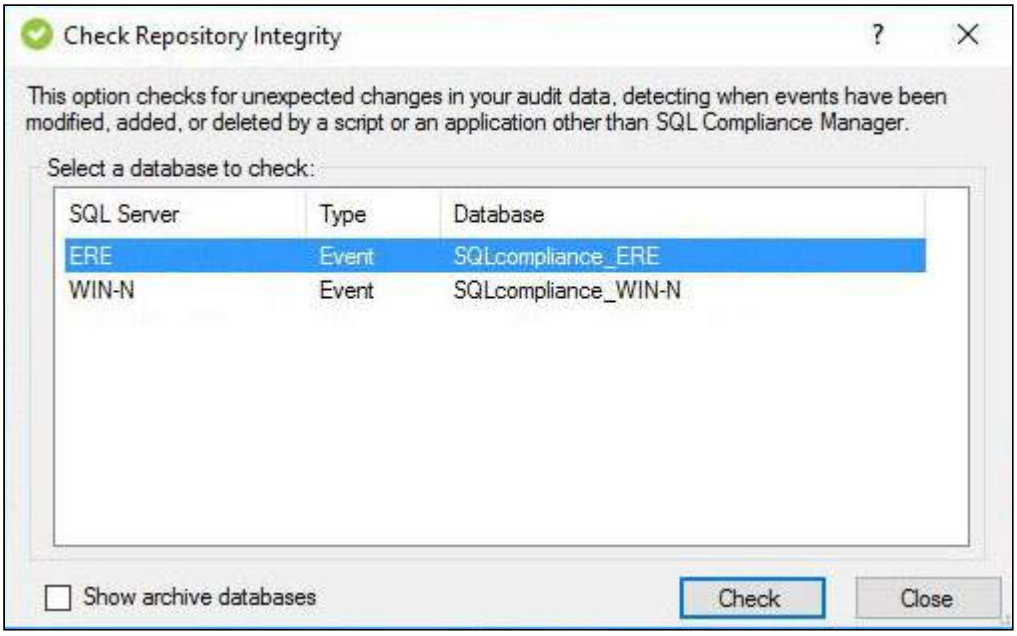
Displays the current status of the associated check. All checks display **Waiting** until run.

Check Repository Integrity window

The Check Repository Integrity window allows you to check for unexpected changes in your audit data, detecting when events are modified, added, or deleted by a script or an application other than IDERA SQL Compliance Manager.



To verify repository integrity, select the Repository database you want to verify, and then click **OK**. To perform an integrity check on an archive database, select **Show archive databases**.



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 were 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 is compromised as well.

The integrity check results indicate:

- How many individual event entries are compromised
- How many entries of Before-After change data and column data are compromised
- How many Sensitive Column entries are compromised

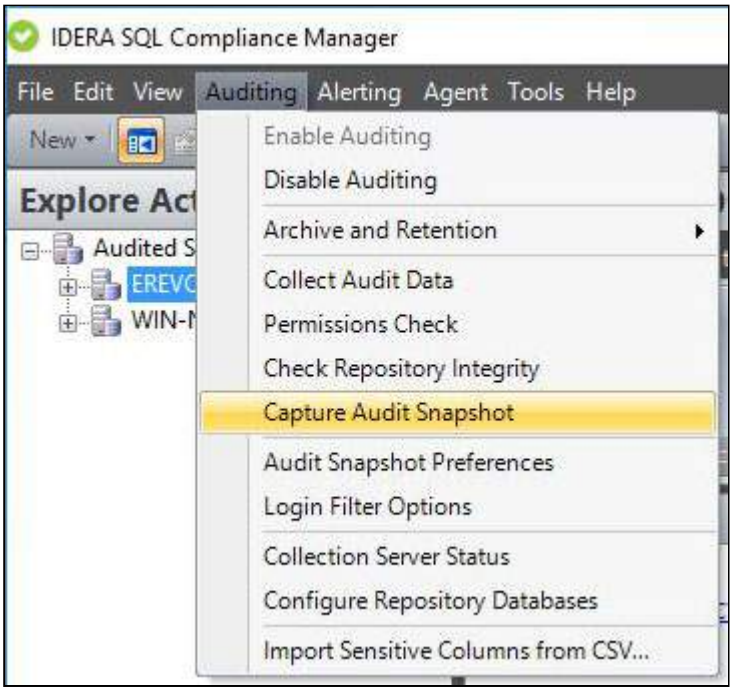
You can choose whether to mark each compromised event entry in the audit data. Marking these events changes the event class to reflect the compromise and changes the event category to Integrity Check. Use the marked audit data to help diagnose the issues and begin a forensic analysis.

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**.

Capture Audit Snapshot window

The Capture Audit Snapshot 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.

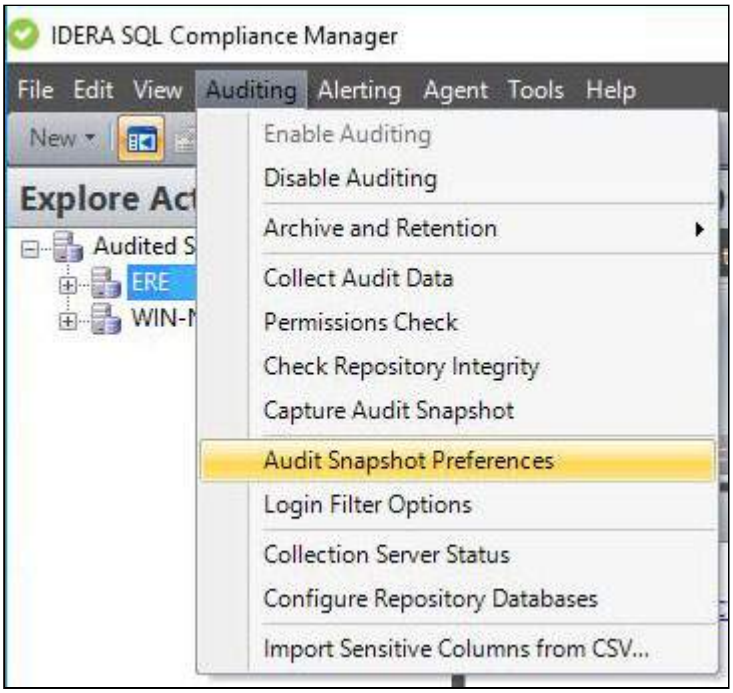


Select the type of audit snapshot you want to capture, and then click **OK**.

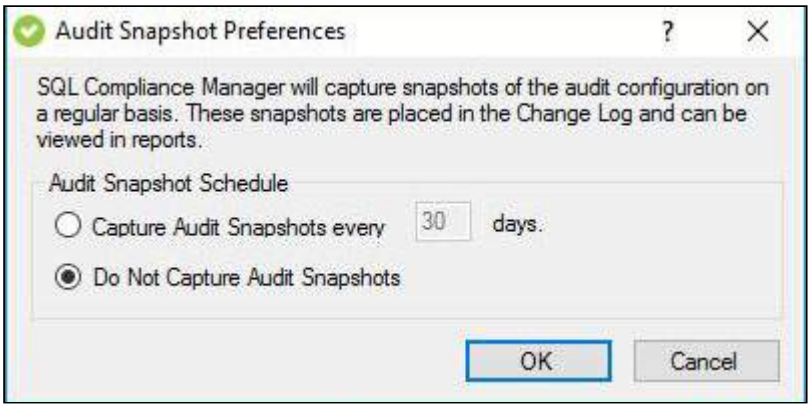
If you want to capture audit snapshots on a routine basis, consider scheduling snapshots.

Audit Snapshot Preferences window

Allows you to indicate whether you want IDERA 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 Compliance Manager does not capture audit snapshots.

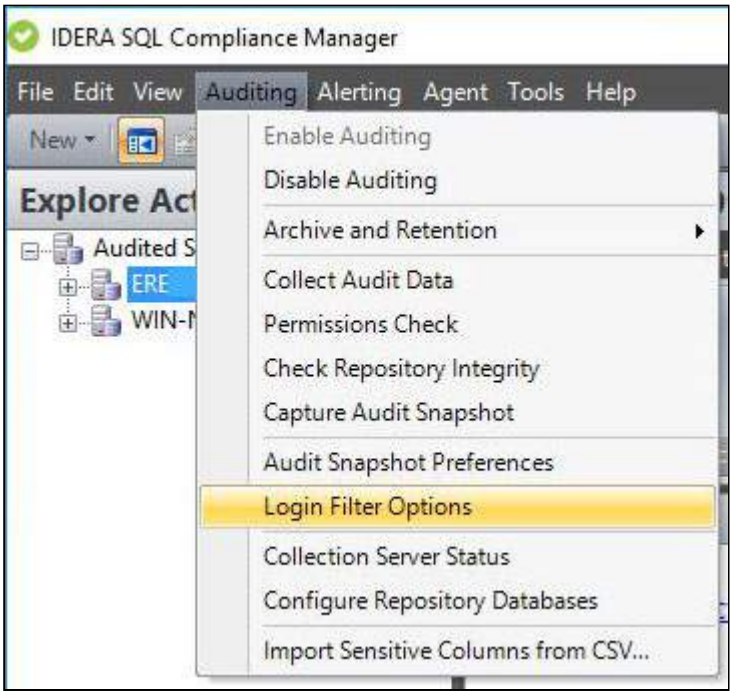


To schedule audit snapshot captures, specify the appropriate frequency, and then click **Capture Audit Snapshots**.



Login Filtering Options window

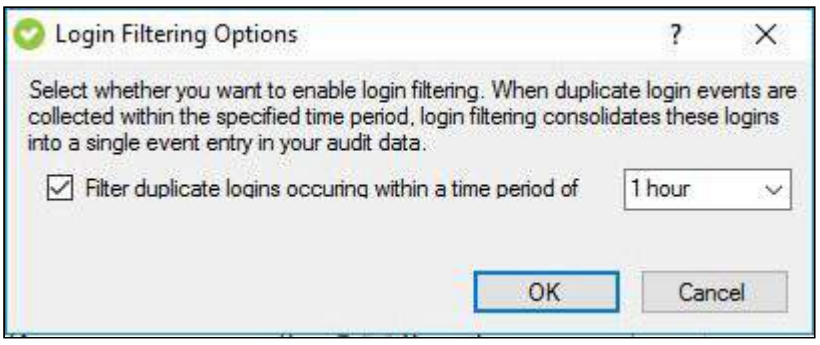
The Login Filtering Options window allows you to set login filtering. Login filtering reduces the number of login events stored in your audit data. When login filtering is enabled, the Collection Server searches the trace files sent by the SQL Compliance Manager Agent for duplicate logins that occurred 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.

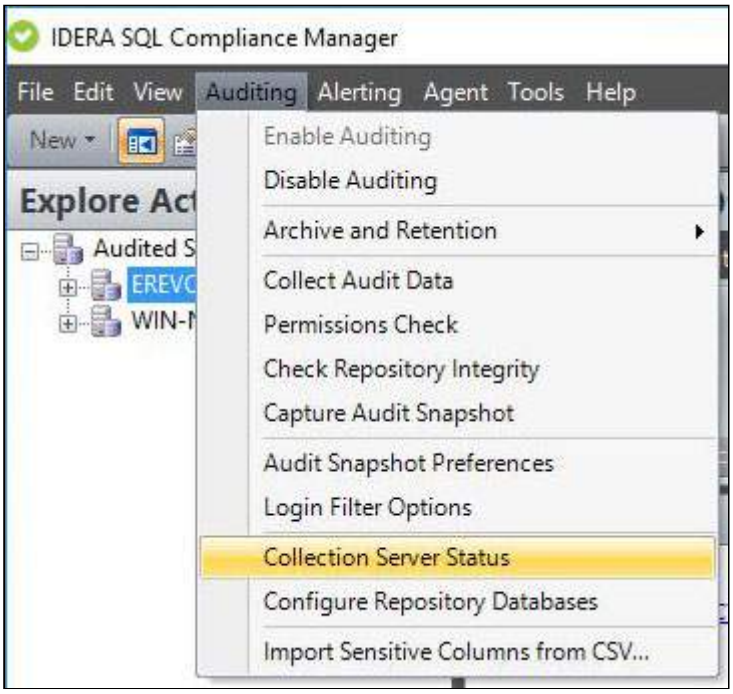


Collection Server Properties window

The Collection Server Properties 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 SQL Compliance Manager Agent
- Version of Collection Server software (should be the same as the IDERA SQL Compliance Manager build and version number)

- Date and time the last heartbeat was received from the SQL Compliance Manager Agent
- Logging levels set at the Collection Server and the SQL Compliance Manager 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 CM maintenance activities, such as re-indexing the Repository databases. By default, the heartbeat interval is five minutes.

NOTE

During the heartbeat, the Collection Service requests a list of the Database Names and ID´s in order to update the table stored in the event database.

Start Service

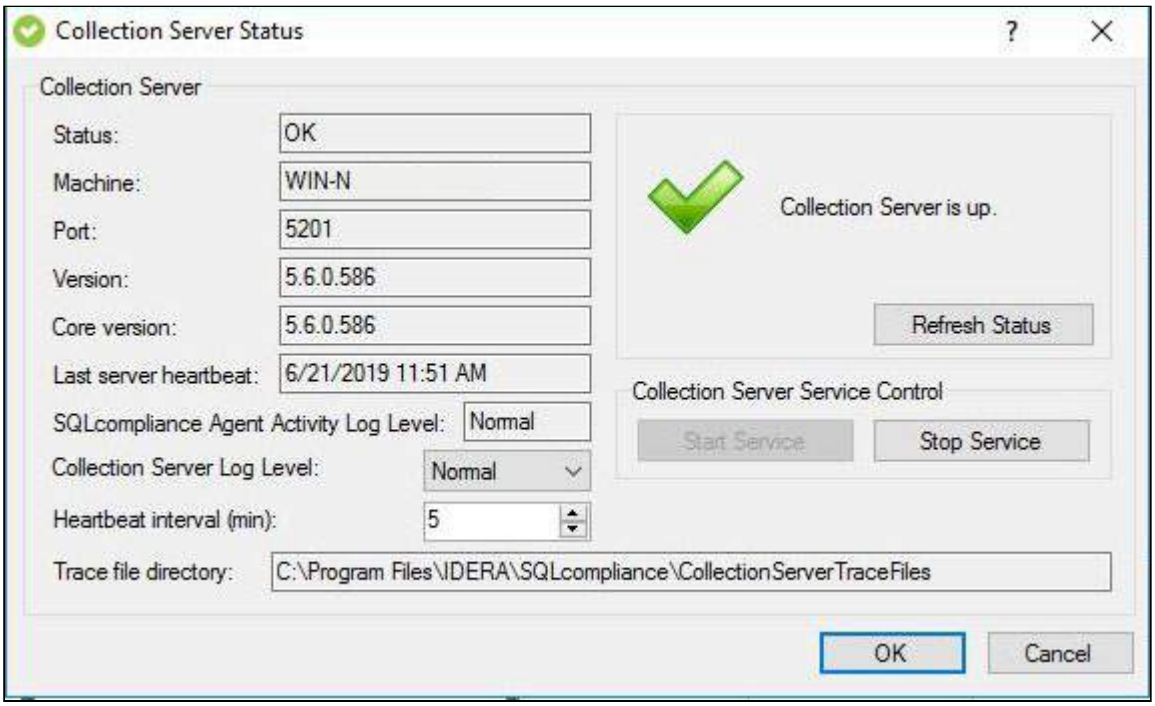
Allows you to restart the Collection Service from the Management Console. Use this feature if the Collection Service has stopped running on the Collection Server computer and requires a manual restart.

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.

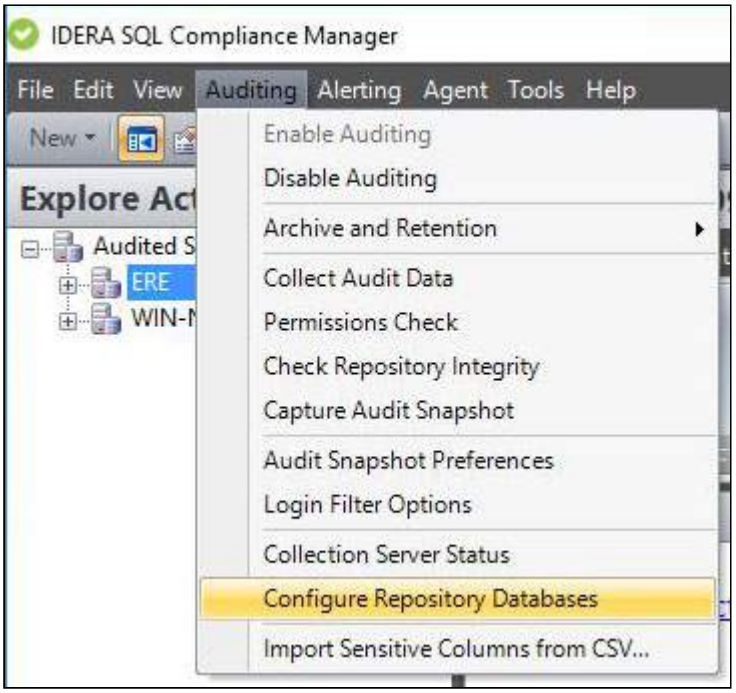
Refresh Status

Allows you to refresh the status fields with the most recent data from the Collection Server.



Configure Repository Databases window - Recovery Model tab

The Recovery Model tab of the Configure Repository Databases window 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.



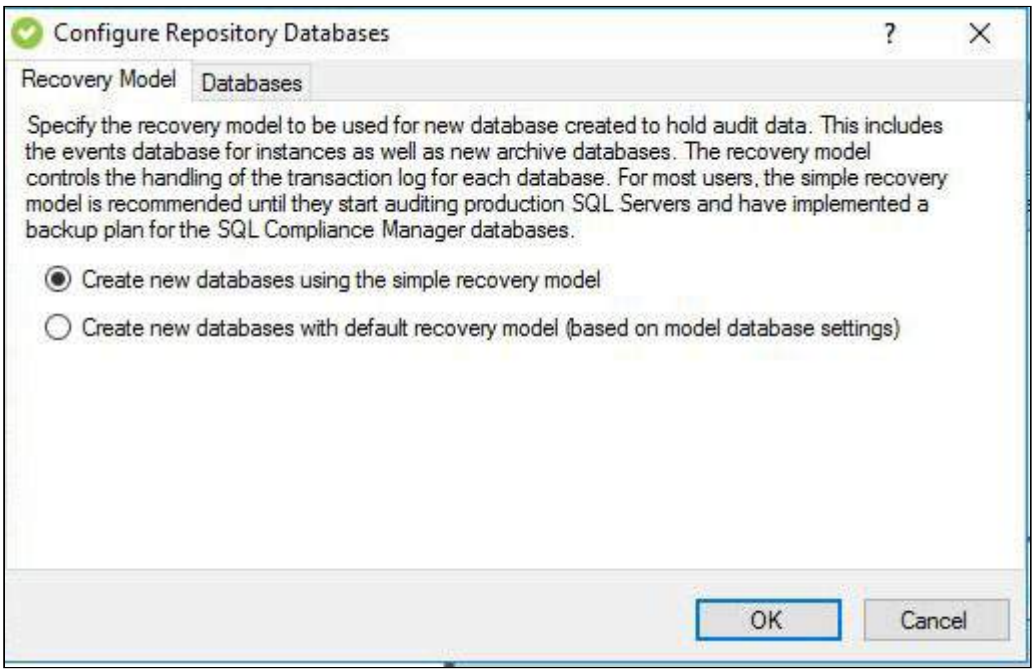
A database recovery model controls whether transaction logs are backed up for each database. The simple model does not allow you to back up transaction logs for a database. The default model does allow you to back up transaction logs for a database. The default model is the recovery model configured 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.

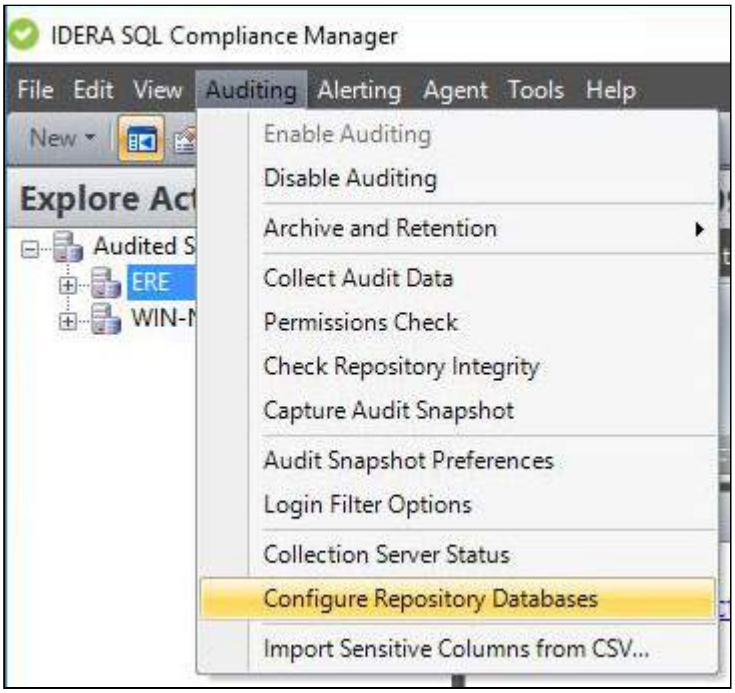
Select the appropriate database recovery model, and then click **OK**.

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 Repository Databases window - Databases tab

The Databases tab of the Configure Repository Databases window allows you to view the status of your Repository databases and update event and attached archive databases created by earlier versions of IDERA 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

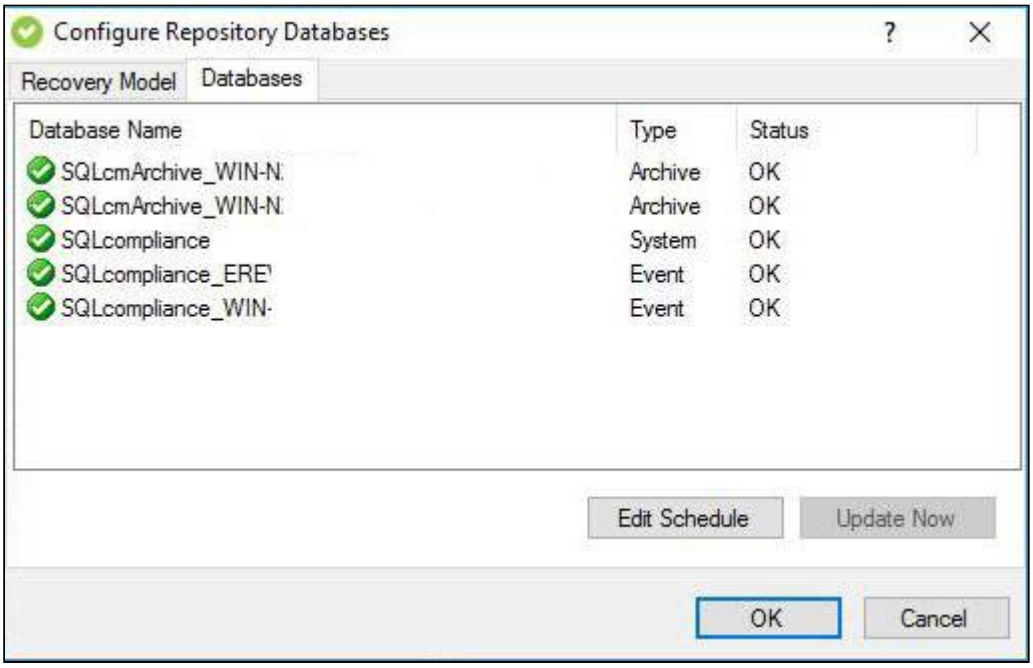
Provides the name of an individual Repository database.

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.



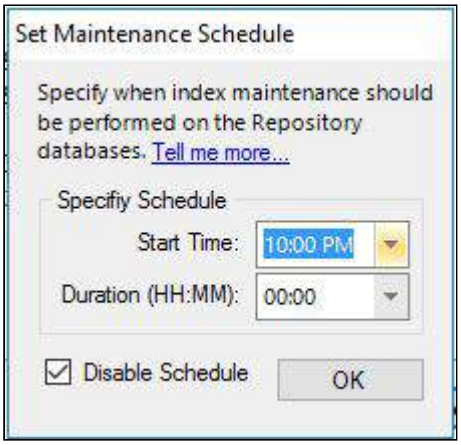
Set Maintenance Schedule window

The Set Maintenance Schedule window allows you to specify when IDERA SQL Compliance Manager should perform maintenance tasks on the Repository, such as rebuilding indexes in the event and archive databases. Because these tasks occasionally are resource-intensive and require extra disk space, consider specifying a time period with slow activity.

During the specified time each day, SQL Compliance Manager continues to execute the required maintenance tasks on any event databases or attached archive database that is not yet 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.

> Specify a duration time that is larger than the Collection Server heartbeat interval. By default, the Collection Server heartbeat is five minutes.



Update Indexes window

The Update Indexes 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.

Import Sensitive Columns from CSV window

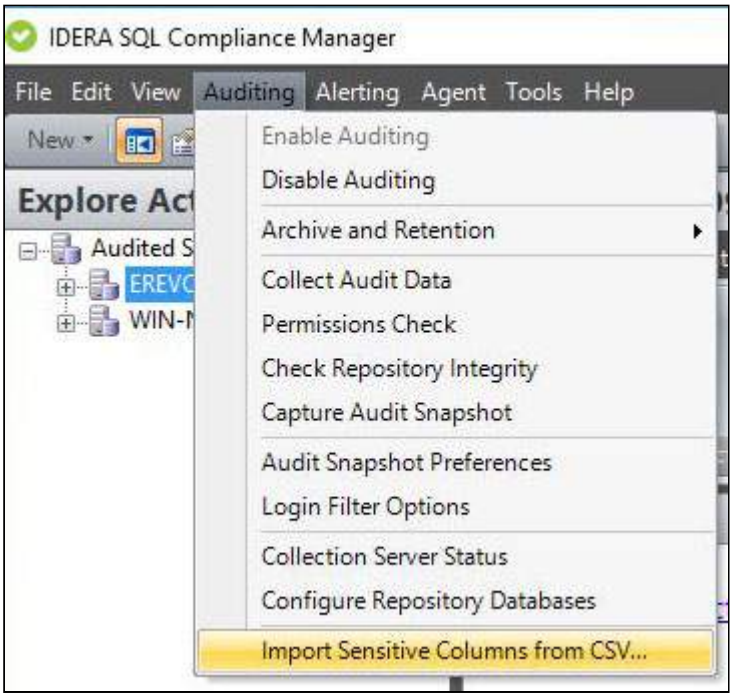
The Import Sensitive Columns window allows you to import a list of sensitive columns from a .csv file to speed the process of configuring your sensitive column auditing. Note that the .csv file must have a row for each database you want to add for sensitive column auditing. The first row value must be the **database name**, the second value must be the **table name** followed by values for table's **column names**. If a row has only two values, first for database name and second for table name, all the columns will be selected for sensitive columns. A row with only one value is invalid and will be ignored. See the following examples:

```
Database1, Table1, Column1, Column2 (Valid Row)
```

```
Database2, Table2 (Valid Row)
```

```
Database3 (Invalid Row)
```

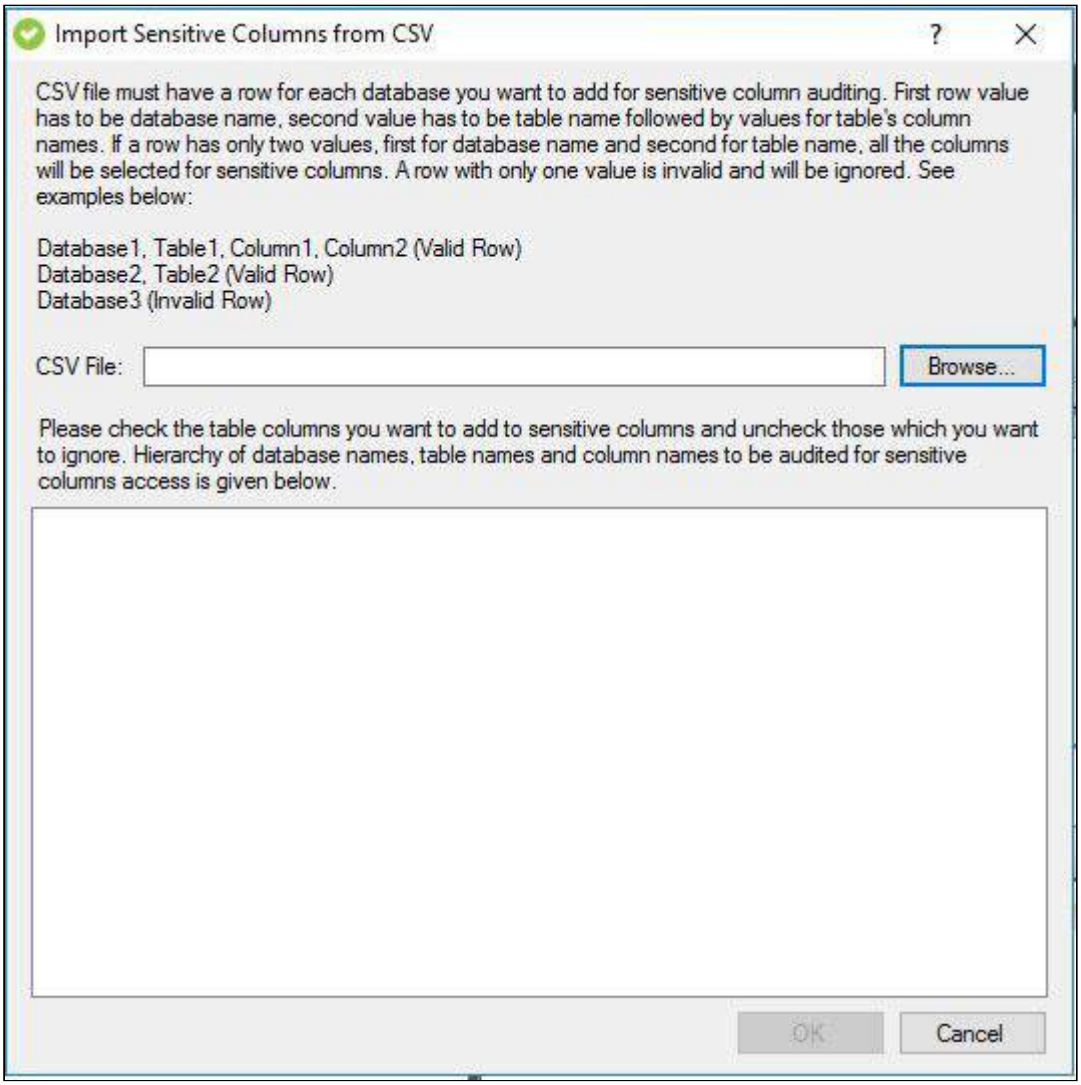
You can access this window from the Instance Details view by selecting Import Sensitive Columns from the drop-down list available below the Audited Databases section.



Importing Sensitive Columns from .CSV

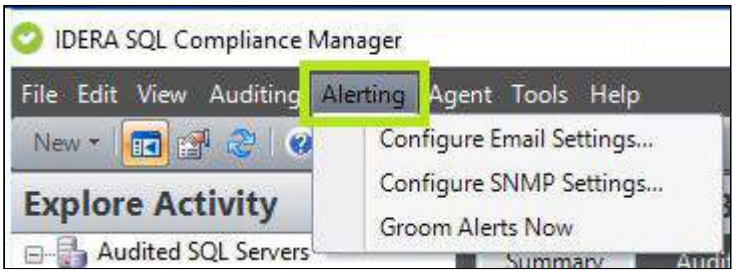
To import a .csv file containing sensitive column search details:

1. Click **Browse** to search for and then select the .csv file you want to import.
2. Check the table columns you want to include as sensitive columns and uncheck those table columns you want to ignore.
3. Click **OK** to import the file.



9.4.5 SQL Compliance Manager Menu - Alerting

The Alerting option from the SQL Compliance Manager Menu allows users to configure their preferred email and SNMP settings, as well as to groom undesired alerts on your SQL Servers.



Available actions

Configure Email Settings

The Configure Email Settings window allows you to configure IDERA SQL Compliance Manager to connect to your mail server. This configuration is required to send alert email notifications. For more information, see Configure Email Settings window.

Configure SNMP Settings

The SNMP Configuration window allows you to specify the server address, port number, and community name of the network management console that you want to receive a IDERA SQL Compliance Manager alert notification as SNMP Trap messages. For more information, see SNMP Configuration window.

Groom Alerts Now

The Groom Alerts Now 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. For more information, see Groom Alerts Now window.

Configure Email Settings window

The Configure Email Settings window allows you to configure IDERA 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 Compliance Manager 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

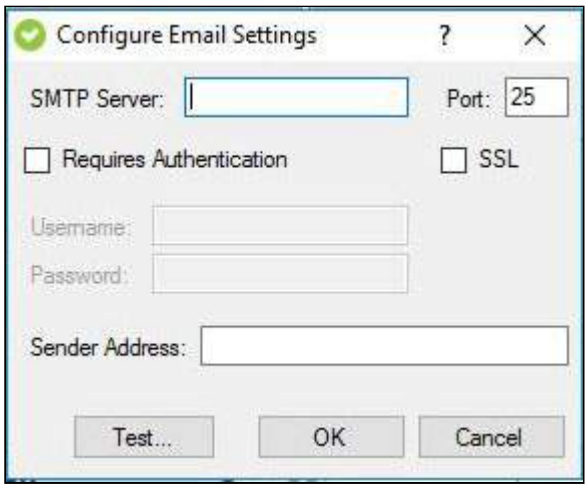
Allows you to indicate whether the mail server requires authentication to connect to the server. ***If authentication is required***, provide the user name and password SQL Compliance Manager should use to access the mail server.

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 Compliance Manager should use to send the alert email notification.

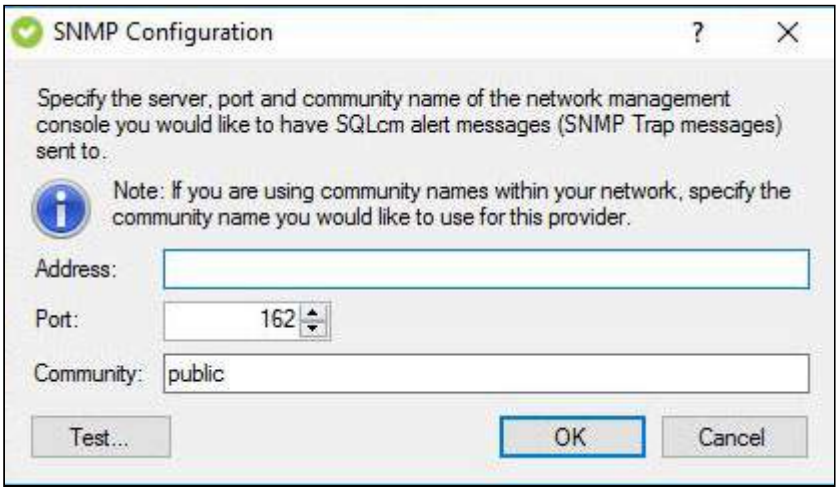


SNMP Configuration window

The SNMP Configuration window allows you to specify the server address, port number, and community name of the network management console that you want to receive a IDERA SQL Compliance Manager 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.



Groom Alerts Now window

The Groom Alerts Now 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

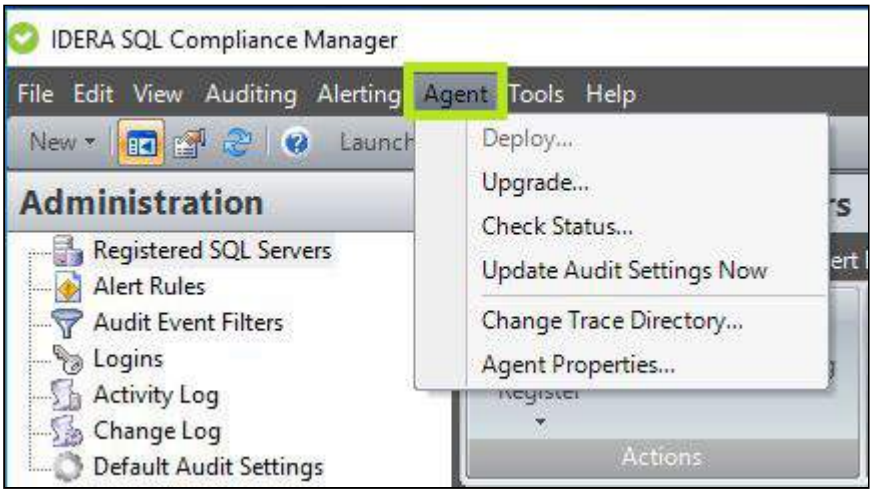
Allows you to select which SQL Server instance you want to groom. You can groom alerts for all registered SQL Server instances or for a particular SQL Server instance.

Grooming Options

Allows you to specify the age (in days) at which an alert message should be groomed. The Collection Server does not groom alert messages that are younger than the specified age.

9.4.6 SQL Compliance Manager Menu - Agent

The SQL Compliance Manager 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. Use the Agent Menu option to perform SQLcompliance Agent related activities.



Available actions

Deploy

Opens the Deploy SQL Compliance Manager Agent wizard. For more information, see Deploy SQL Compliance Manager Agent wizard.

Upgrade

Performs an upgrade to your deployed SQL Compliance Agents. For more information, see Upgrade your deployed SQL Compliance Agents.

Check Status

Allows you to quickly check the status of a SQL Compliance Manager Agent that is deployed to a registered SQL Server instance you are auditing. For more information, see Check the SQL Compliance Manager Agent status.

Update Audit Settings Now

You can ensure the SQL Compliance Manager Agent is using your most recent audit settings by performing a manual update.

Change Trace Directory

Allows you to change the location of the agent trace directory. The SQL Compliance Manager Agent temporarily stores collected SQL Server events in the trace directory until the files can be sent to the Collection Server. For more information, see SQL Compliance Manager Agent Trace Directory window.

Agent Properties

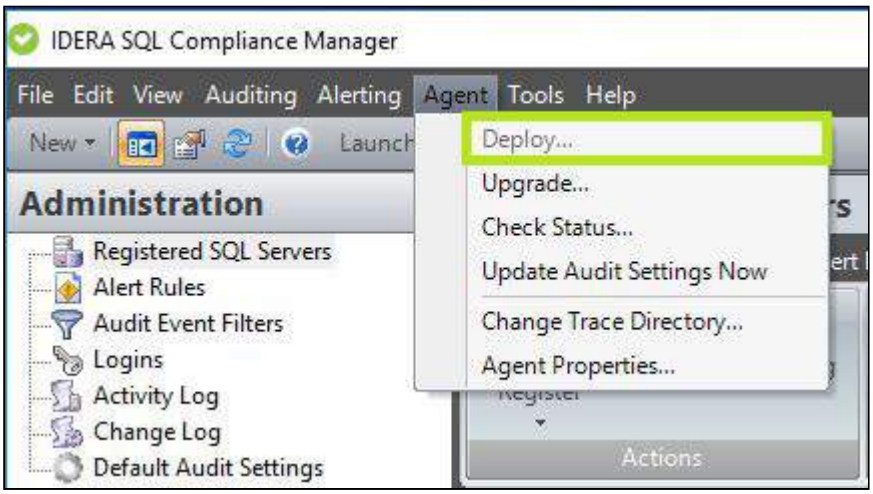
Allows you to view or change the properties, such as the heartbeat interval and the collection interval, of the SQL Compliance Manager Agent deployed to the selected SQL Server instance. For more information, see SQL Compliance Manager Agent Properties.

Deploy SQL Compliance Manager Agent wizard

The SQL Compliance Manager 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 SQL Compliance Manager Agent to each SQL Server computer that hosts the instances and databases you want to audit.

For more information see:

- Deploy the SQL Compliance Manager Agent manually
- Deploy the SQL Compliance Manager Agent remotely



Follow the wizard steps below to deploy your SQL Compliance Manager Agent:

- Deploy SQL Compliance Manager Agent wizard - SQL Compliance Manager Agent Services Account window
- Deploy SQL Compliance Manager Agent wizard - SQL Compliance Manager Agent Trace Directory window
- Deploy SQL Compliance Manager Agent wizard - Summary tab

Deploy SQL Compliance Manager Agent wizard - SQL Compliance Manager Agent Services Account window

The SQL Compliance Manager Agent Services Account window of the Deploy SQL Compliance Manager Agent wizard allows you to specify the credentials of the Windows user account under which the SQL Compliance Manager Agent Service runs. The SQL Compliance Manager 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 SQL Compliance Manager Agent wizard - SQL Compliance Manager Agent Trace Directory window

The SQL Compliance Manager Agent Trace Directory window of the Deploy SQL Compliance Manager Agent wizard 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 SQL Compliance Manager 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 SQL Compliance Manager Agent Service account has read and write privileges on that folder. IDERA 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**.

SQL Compliance Manager Agent Trace Directory window

The SQL Compliance Manager Agent Trace Directory window allows you to change the location of the agent trace directory. The SQL Compliance Manager 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 SQL Compliance Manager Agent Service account has read, write, and delete privileges on that folder. IDERA 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 Compliance Manager applies this change to the active node in the cluster hosting the virtual SQL Server. SQL Compliance Manager 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**.

Deploy SQL Compliance Manager Agent wizard - Summary tab

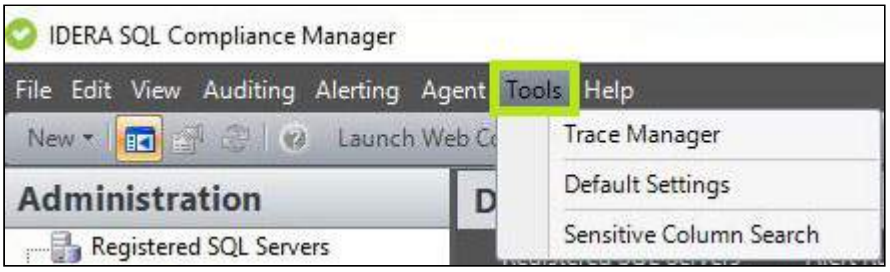
Review the Summary tab of the Deploy SQL Compliance Manager Agent wizard, and then click **Finish**. When you finish this wizard, IDERA SQL Compliance Manager installs the SQL Compliance Manager Agent on the computer that hosts the selected SQL Server instance, and starts the SQL Compliance Manager Agent Service.

When you enable auditing on this SQL Server instance, the SQL Compliance Manager 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 SQL Compliance Manager Agent Properties window.

9.4.7 SQL Compliance Manager Menu - Tools

Use the Tool option from the SQL Compliance Manager Menu to mange your Trace Files with the Trace Manager tool or set your desired Default Audit Settings.



Available actions

Trace Manager

Opens the Trace Manager window, where users are able to view, start or stop their Registered Traces and are also able to decompress their trace files. For more information on this tool, contact Idera Support.

Default Settings

Opens the Default Audit Settings tab in the Administration view, allowing users to customize their desired default audit settings and apply those settings to their audited Servers and Databases. For more information, see Default Audit Settings.

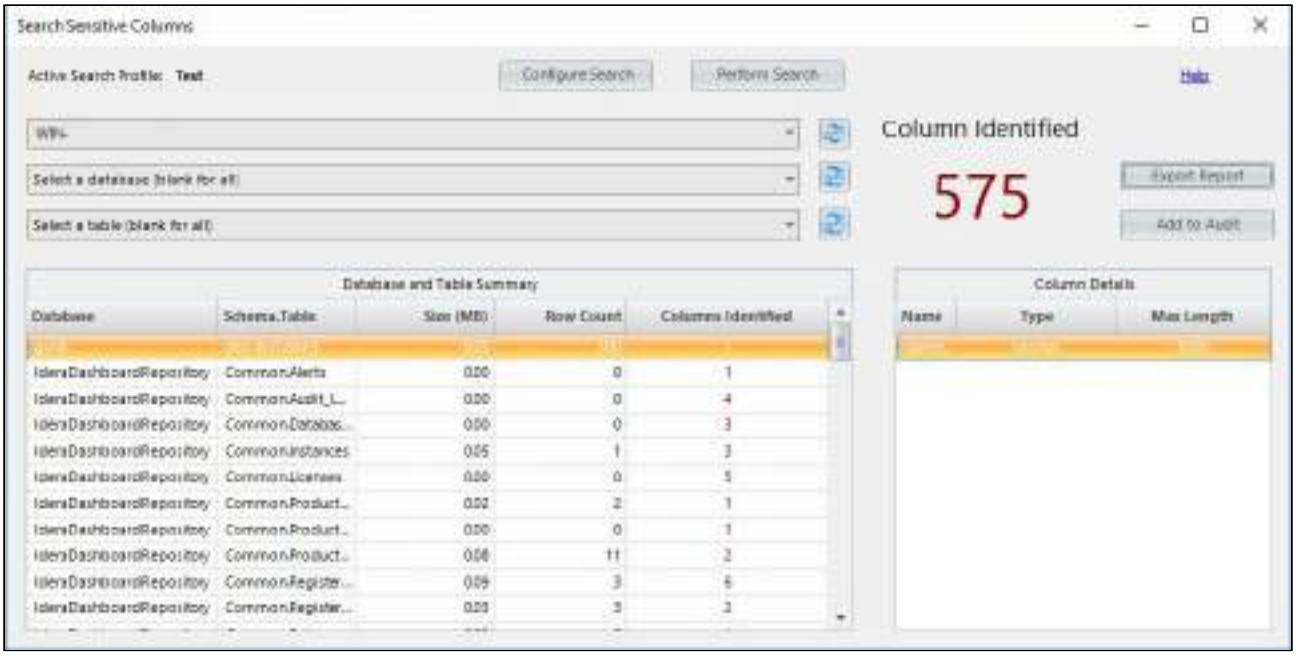
Sensitive Column Search

Allows you to search all of the tables and columns on a targeted database to help you identify potential sensitive data that needs to be audited. For more information, see Sensitive Column Search window.

Sensitive Column Search

The Sensitive Column Search window allows you to search all of the tables and columns on a targeted database to discover the location of sensitive data that needs to be audited. The Sensitive Column Search feature includes pre-configured common sensitive data strings for you to select from, or you can define specific strings in order to customize your Search Profile exactly the way you want. Define your search to a specific table within a database or search an entire instance and export your successful search results to a CSV format to easily analyze results.

You can access this window from the Tools option of the SQL Compliance Manager Menu and select Sensitive Column Search from the drop-down list available, or by right clicking any registered Database or Instance and selecting the Sensitive Column Search option.

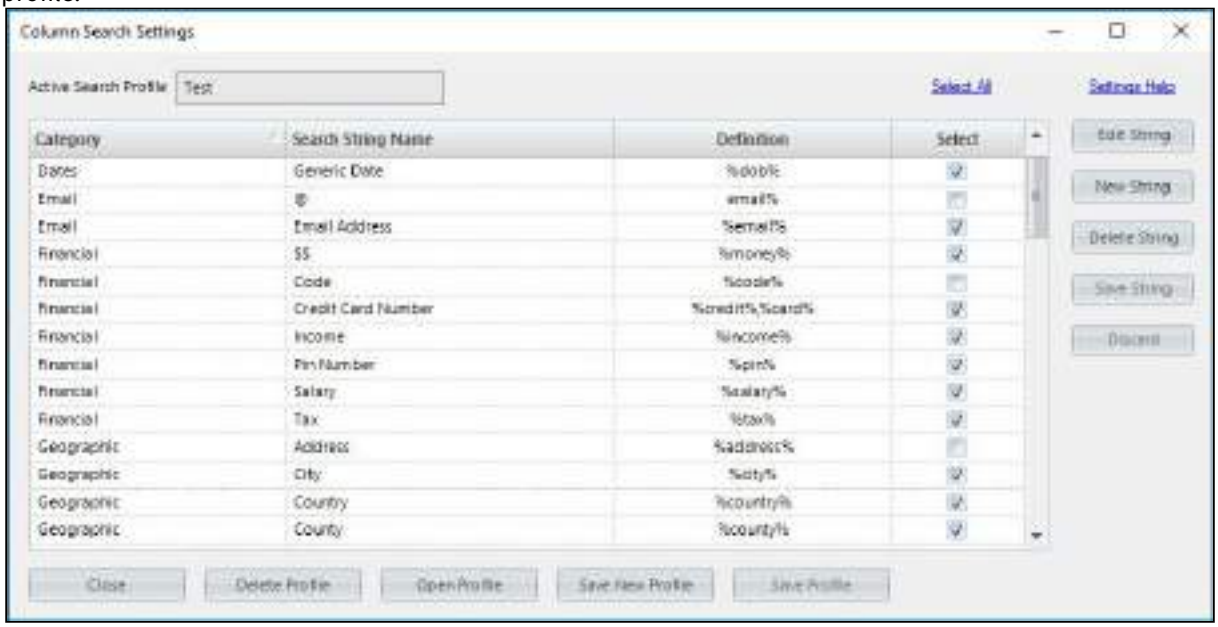


Performing a search

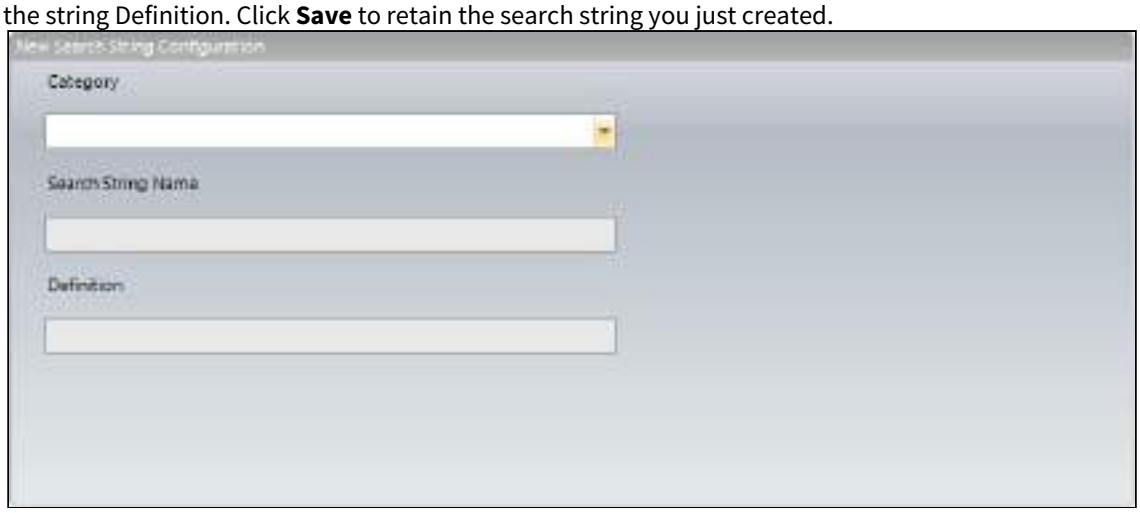
To search for Sensitive Columns within one or more databases:

1. Select the target server name from the available list. To search all databases, leave the list at the default **Select a database** option.
2. ***If you selected a specific database,*** select a target table name. Note that you cannot select a table if you did not select a target database.
3. Select a search profile, and then continue with the next step. ***If no profiles are configured or if you want to edit an existing profile,*** click **Configure Search**. SQL Compliance Manager displays the Column Search

Settings window for you to configure a search profile. Use the following subset of steps to configure a search profile.

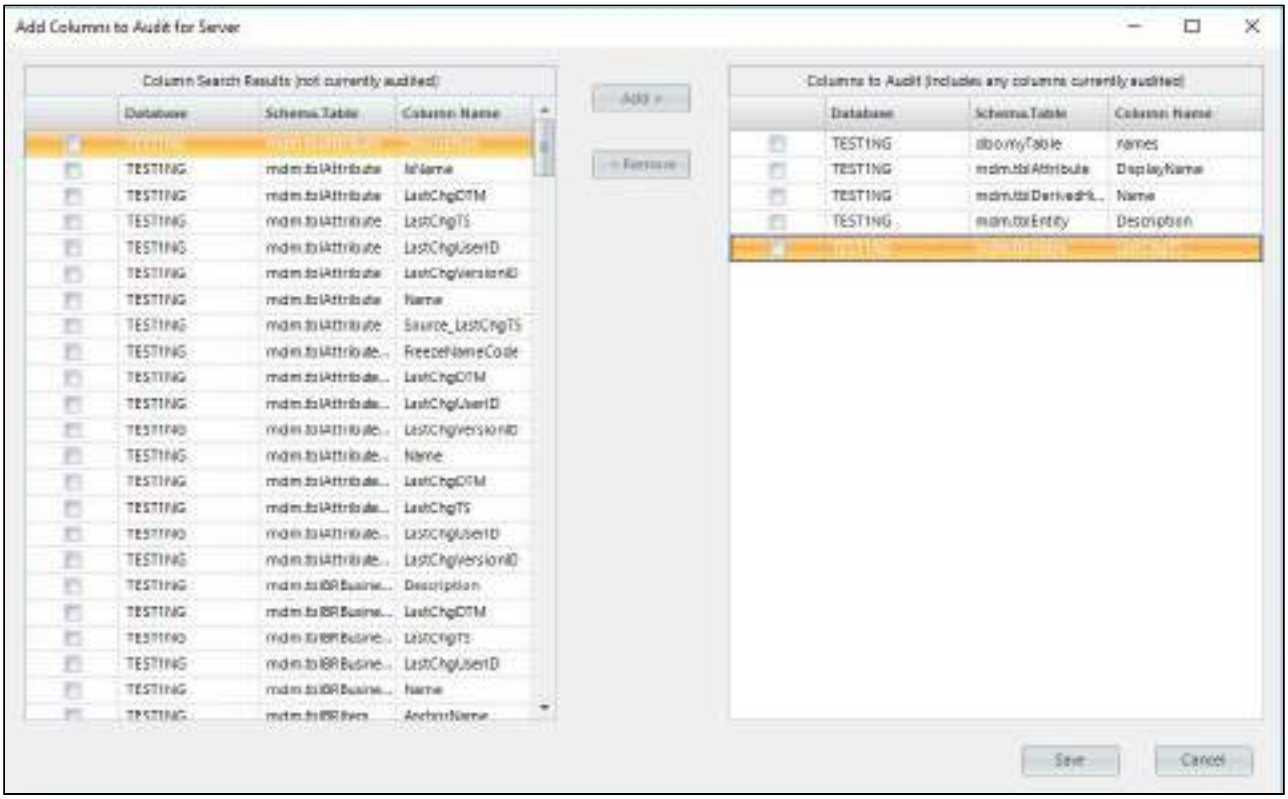


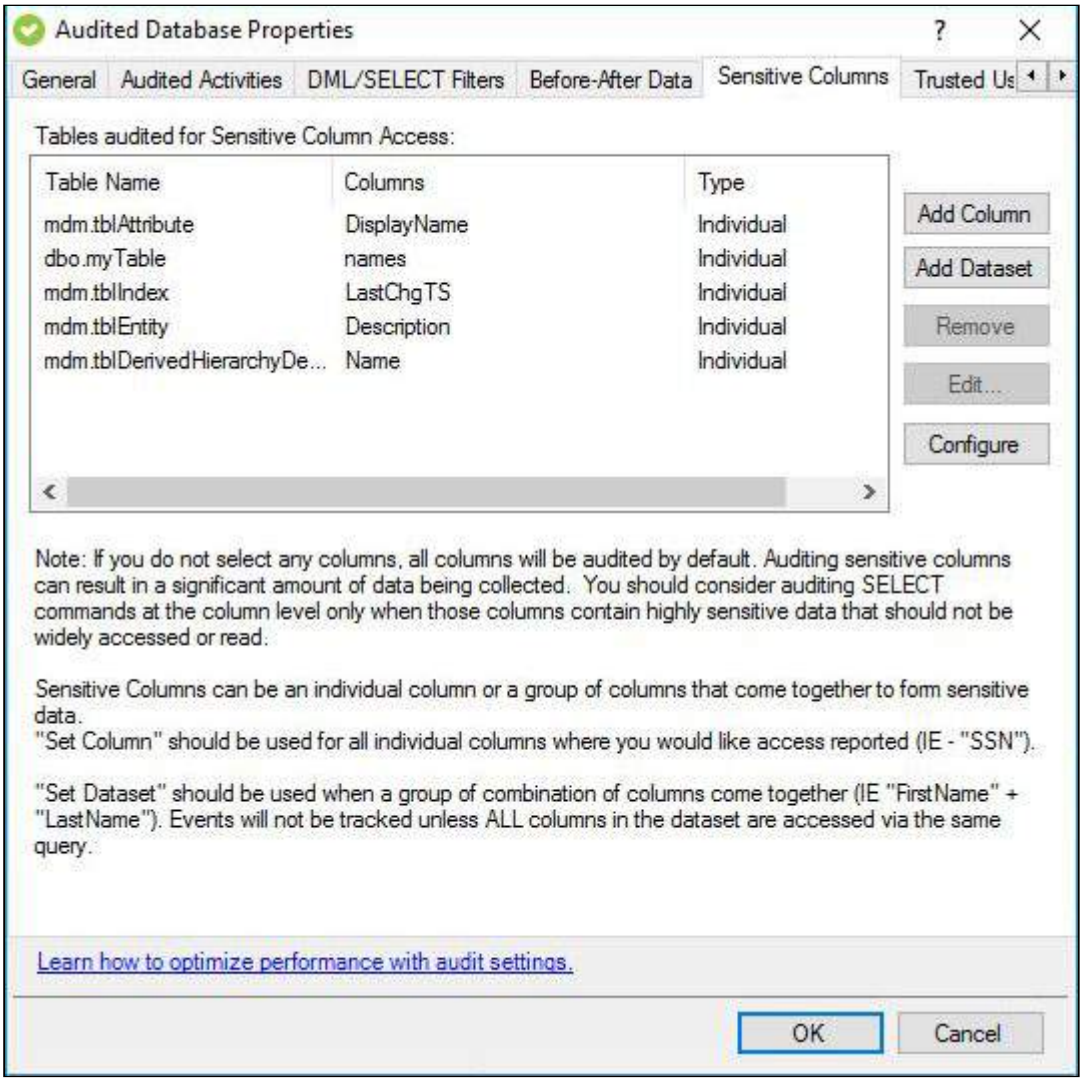
a. In the Column Search Settings window, select one or more search strings you want to include in the search profile. Click **Select All** to include all of the available search strings in this profile.
b. ***If the search string you want to use does not exist and you want to create a new search string,*** click **New**. This option allows you to select a category, type a name for the search string, and then include the string Definition. Click **Save** to retain the search string you just created.



c. Once you select all of the search string you want in the profile, click **Save Profile**. The profile is now available for you to select on the Sensitive Column Search window.

4. Click **Perform Search** to execute the search on the selected database(s) and table(s) based on the selected **Active Search Profile**. SQL Compliance Manager runs the Sensitive Column search and displays the results.
5. Click **Export Report** to export the results in .csv format. This function allows you to save the data in a format that is compatible with the Import Sensitive Columns feature.
6. Click **Add to Audit** to open the Add Columns to Audit for Server window where you can Add or Remove your Column Search Results to the Columns to Audit section.


Add Columns to Audit for Server
Column Search Results (not currently audited)
Database
Schema.Table
Column Name
TESTING
mdm.tblAttribute
IsName
LastChgDTM
LastChgTS
LastChgUserID
LastChgVersionID
Name
Source_LastChgTS
FreezeNameCode
Add >
< Remove
Columns to Audit (includes any columns currently audited)
TESTING
dbo.MyTable
names
DisplayName
mdm.tblDerivedHi...
Description
mdm.tblEntity
Save
Cancel


Audited Database Properties
General
Audited Activities
DML/SELECT Filters
Before-After Data
Sensitive Columns
Trusted Us
Tables audited for Sensitive Column Access:
Table Name
Columns
Type
mdm.tblAttribute
DisplayName
Individual
dbo.myTable
names
Individual
mdm.tblIndex
LastChgTS
Individual
mdm.tblEntity
Description
Individual
mdm.tblDerivedHierarchyDe...
Name
Individual
Add Column
Add Dataset
Remove
Edit...
Configure
Note: If you do not select any columns, all columns will be audited by default. Auditing sensitive columns can result in a significant amount of data being collected. You should consider auditing SELECT commands at the column level only when those columns contain highly sensitive data that should not be widely accessed or read.
Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data.
"Set Column" should be used for all individual columns where you would like access reported (IE - "SSN").
"Set Dataset" should be used when a group of combination of columns come together (IE "FirstName" + "LastName"). Events will not be tracked unless ALL columns in the dataset are accessed via the same query.
Learn how to optimize performance with audit settings.
OK
Cancel

10 Cluster Configuration Console User Interface

The IDERA 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.

10.1 Add SQL Compliance Manager Agent Service wizard - Collection Server tab

The Collection Server tab lets you to specify which computer is currently hosting the Collection Server. The SQL Compliance Manager Agent Service receives audit settings from the Collection Server and sends collected SQL events to the Collection Server for processing. Ensure the SQL Compliance Manager Agent Service has access to the Collection Server computer.

Specify the Collection Server to which the SQL Compliance Manager Agent Service should connect, and then click **Next**.

10.2 Add SQL Compliance Manager Agent Service wizard - General tab

The General tab of the Add SQL Compliance Manager Agent Service wizard 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**.

10.3 Add SQL Compliance Manager Agent Service wizard - SQLcompliance Agent Service Account tab

The SQL Compliance Manager Agent Service Account tab of the Add SQL Compliance Manager Agent Service wizard lets you specify the account credentials the SQL Compliance Manager Agent Service account should use to connect to the Collection Server and the virtual SQL Server. The SQL Compliance Manager 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 SQL Compliance Manager Agent Service should run under, and then click **Next**.

10.4 Add SQL Compliance Manager Agent Service wizard - SQL Compliance Manager Agent Trace Directory tab

The SQL Compliance Manager Agent Trace Directory tab of the Add SQL Compliance Manager Agent Service wizard lets you specify which folder should be used for the SQL Compliance Manager Agent trace directory. The SQL Compliance Manager Agent stores SQL Server trace files in this directory until the files are sent to the Collection Server for processing. The specified folder must reside on a shared data disk for the specified virtual SQL Server. Ensure that 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 creates 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 SQL Compliance Manager 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 SQL Compliance Manager Agent should store SQL Server trace files, and then click **Next**.

10.5 Add SQL Compliance Manager Agent Service wizard - CLR Trigger Location tab

The CLR Trigger Location tab of the Add SQL Compliance Manager Agent Service wizard 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 IDERA SQL Compliance Manager when you enable before-after auditing for a specific SQL Server database. The SQL Compliance Manager 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 SQL Compliance Manager Agent should store CLR trigger assembly files, and then click **Next**.

10.6 Add SQL Compliance Manager Agent Service wizard - Summary tab

Review the provided summary, and then click **Finish**. When you finish this wizard, the Cluster Configuration Console installs the SQL Compliance Manager Agent Service on this cluster node.

When you enable auditing on the virtual SQL Server, the SQL Compliance Manager 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.

10.7 Cluster Configuration Console window

The IDERA SQL Compliance Manager Cluster Configuration Console window lets you install and configure the SQL Compliance Manager 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 SQL Compliance Manager Agent.

10.7.1 Available actions

Add Service

Allows you to install and configure the SQL Compliance Manager 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 SQL Compliance Manager Agent Service that is auditing the selected virtual SQL Server. To view all properties of the SQL Compliance Manager Agent installed on this cluster node, use the Management Console.

Remove Service

Allows you to uninstall the SQL Compliance Manager Agent Service from this cluster node.

10.7.2 Available fields

SQL Compliance Manager Agent Version

Provides the version number of the SQL Compliance Manager Agent installed on this cluster node.

10.8 SQL Compliance Manager Agent Details window

The IDERA SQL Compliance Manager SQL Compliance Manager Agent Details window lets you view a subset of SQL Compliance Manager Agent properties. To view all properties for the SQL Compliance Manager Agent, use the Management Console.

- Name of the virtual SQL Server audited by this SQL Compliance Manager Agent
- Name of the Collection Server computer that is processing events collected by the SQL Compliance Manager Agent
- Name and location of the trace directory where the SQL Compliance Manager 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 SQL Compliance Manager Agent Service under which the SQL Compliance Manager Agent is running
- Name and path of the SQL Compliance Manager Agent Service registry key that is replicated across the cluster nodes

10.8.1 Available actions

To copy either the SQL Compliance Manager Agent Service name or the registry key, click the copy button beside the corresponding field, and then click **OK**.

Copy the SQL Compliance Manager Agent Service name

Allows you to copy the name of the SQL Compliance Manager Agent Service to your clipboard. Use this feature to specify the service name when registering the SQL Compliance Manager Agent Service through Microsoft Cluster Administrator. You can paste the copied service name into the required field.

Copy the SQL Compliance Manager Agent Service registry key

Allows you to copy the path of the SQL Compliance Manager 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 SQL Compliance Manager Agent Service through Microsoft Cluster Administrator. You can paste the copied service name into the required field.

10.9 Specify CLR Trigger Directory window

The Specify CLR Trigger Directory 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 IDERA SQL Compliance Manager when you enable before-after auditing for a specific SQL Server database. The SQL Compliance Manager

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 SQL Compliance Manager Agent should store CLR trigger assembly files, and then click **OK**.

11 Upgrade SQL Server in your audited environment

You can choose one of the following IDERA 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.

11.1 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 SQL Compliance Manager 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.

11.2 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.

11.3 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 IDERA 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.

11.3.1 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.

☑	**Follow these steps ...**
☐	Back up your trace directories, especially the Collection Server Trace Directory.
☐	Run the Microsoft SQL Server Upgrade Advisor utility on the target instance. For more information about upgrading SQL Server, see Upgrade Advisor on the Microsoft web site.

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 SQL Compliance Manager Agent service. Use the Microsoft Services administrative tool to stop the SQL Compliance Manager Agent service (SQL Compliance Manager 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 (SQL Compliance Manager 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 SQL Compliance Manager Agent service. Use the Microsoft Services administrative tool to restart the SQL Compliance Manager Agent service (SQL Compliance Manager Agent) running on the Collection Server computer.
8. ***If you upgraded SQL Compliance Manager to the latest version***, also upgrade the SQL Compliance Manager Agent remotely.
9. Upgrade the SQL Server software on the computers hosting your audited instances.
10. Begin auditing any new SQL Server instances.

11.4 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 2008 environment and a SQL Server 2012 environment. For example, you could deploy one Collection Server to dedicated SQL Server 2008 instance in one environment and a second Collection Server to a dedicated SQL Server 2012 instance in another environment. Use the following checklist and instructions to successfully deploy a second Collection Server.

11.4.1 Deployment checklist

☑	**Follow these steps ...**
☐	Determine whether you want to upgrade to the latest version of IDERA 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.

☑	**Follow these steps ...**
☐	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 2012, install the Collection Server on computer hosting SQL Server 2012. • Meets the product hardware, software, and permissions requirements.

11.4.2 Deploy new Collection Server after the SQL Server on an audited instance is upgraded

To deploy a new Collection Server to an upgraded SQL Server on an audited instance:

1. ***If you want to use the latest version of SQL Compliance Manager***, upgrade your deployment.
2. Use Custom install in the SQL Compliance Manager 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 SQL Compliance Manager Agent to communicate with the new Collection Server.

11.4.3 Deploy new Collection Server to audit new instances

To deploy a new Collection Server to audit new SQL Server 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 Compliance Manager setup program to install the new Collection Server.
3. Register the instances you want to audit.
4. Begin auditing your new SQL Server instances.

12 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 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.

12.1 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.

12.2 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 SQL Compliance Manager 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.

12.3 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 SQL Compliance Manager 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

12.4 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.

12.4.1 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

12.4.2 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.

12.5 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

12.5.1 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.

12.6 Deploy the new Collection Server

Please make sure to review the Collection Server requirements before installing. By default, IDERA SQL Compliance Manager is being installed with a trial license. Please update the license key to reflect your current production license.

12.6.1 Installing the Collection Server:

1. Log in with an administrator account to a computer or any other VM in which you want to install the Collection Server.
2. Run `SQLCMInstall.EXE` in the root of the installation kit.
3. Review the information you need to start the installation, and then click **Next.**
4. Review and accept the license agreement by selecting the ***I accept the terms and conditions of the End User License Agreement*** checkbox.
   Select the **SQL Compliance Manager Management components** *only* setup and then click **Next.**
5. Specify if you want to register SQL Compliance Manager with an existing IDERA Dashboard.
6. Accept the default folder for your SQL Compliance Manager installation, type or click **Browse** to specify a different folder, and then click **Next**.
7. Specify the SQL Server Instance on which you restored the Repository databases and a form of authentication to create the SQL Compliance Manager repository.
8. Indicate that you want to use the existing Repository databases, and then click **Next**.
9. ***If you want to audit the Repository or other databases associated with the selected SQL Server instance***, click **Yes**, and then click **Next**.
10. Specify the location where the Collection Server should store audit data received from the SQL Compliance Manager Agent, and then click **Next**. The specified folder will be the trace file directory on the Collection Server.
11. Type the appropriate credentials in the provided fields under which IDERA services run, and then click **Next**. IDERA uses this account to connect, discover, and gather configuration information from SQL Servers in your Business environment. The installer grants the "Log on as a Service" right to the account that you specify.
12. Review the installation settings and click **Install.**

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

12.7 Configure the SQL Compliance Agent connection

To ensure you successfully continue auditing your registered SQL Servers within IDERA SQL Compliance Manager, configure each SQL Compliance Manager 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\SQLCM\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 SQL Compliance Manager 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.

12.7.1 To configure the SQL Compliance Manager Agent using a script:

1. Define variables for the computers that host the SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent deployed to your registered SQL Servers.

13 Audit a virtual SQL Server instance

IDERA SQL Compliance Manager supports auditing a virtual SQL Server instance including the local instance on a cluster running the Collection Server.

After you install and configure the SQL Compliance Manager 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.

13.1 To audit the virtual SQL Server:

1. Verify that the SQL Compliance Manager 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.

When you decide to stop auditing a virtual SQL Server instance, use the following procedure to remove your configuration settings and uninstall the SQL Compliance Manager Agent.

13.2 To stop auditing the virtual SQL Server:

1. Use the Microsoft Cluster Administrator tool to remove the registered generic service you created for the SQL Compliance Manager 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 SQL Compliance Manager Agent Service. This action deletes the SQL Compliance Manager 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 SQL Compliance Manager 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.

13.3 Start auditing the virtual SQL Server

After you install and configure the SQL Compliance 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.

13.3.1 To audit the virtual SQL Server:

1. Verify that the SQL Compliance 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.

13.4 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 SQL Compliance Agent.

13.4.1 To stop auditing the virtual SQL Server:

1. Use the Microsoft Cluster Administrator tool to remove the registered generic service you created for the SQL Compliance 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 SQL Compliance Agent Service. This action deletes the SQL Compliance 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 SQL Compliance 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.

14 JIC2 Copy of How to install SQL Compliance Manager

IDERA SQL Compliance Manager versions 4.5 and older. For installations of SQL Compliance Manager 5.0 and newer, including the IDERA Dashboard, see How to install SQL Compliance Manager and the IDERA Dashboard.

Before installing IDERA 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 or higher instance.

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

14.1 To install SQL Compliance Manager:

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 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 Compliance Manager installation, or click **Browse** to specify a different folder.
7. Select whether you want the SQL Compliance Manager 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 SQL Compliance Manager Management Console

Setup Type	Description
Agent Only	Allows you to install only the SQL Compliance Manager Agent
Custom	Allows you to select the individual SQL Compliance Manager components you want to install

9. ***If you chose the Custom type***, select one or more SQL Compliance Manager components, and then click **Next**. Using the Custom setup type, you can install SQL Compliance Manager components in the following ways:
   - Collection Server and Repository with SQL Compliance Manager Agent
   - Collection Server and Repository
   - Management Console with SQL Compliance Manager Agent
   - Management Console only
   - SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent should use to connect to associated databases, and then click **Next**.
    e. Select whether you want to start the SQL Compliance Manager 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.

⚠ The SQL Compliance Manager installer detects if the local machine has an older version of the SQL Server 2012 Native Client installed and if needed SQL CM upgrades the Native Client to the latest version and proceeds with the installation. If no Native Client is installed on the server, then SQL CM installs the latest Native Client version and proceeds with the installation.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

15 JIC Copy of How to install SQL Compliance Manager

IDERA SQL Compliance Manager versions 4.5 and older. For installations of SQL Compliance Manager 5.0 and newer, including the IDERA Dashboard, see How to install SQL Compliance Manager and the IDERA Dashboard.

Before installing IDERA 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 or higher instance.

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

15.1 To install SQL Compliance Manager:

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 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 Compliance Manager installation, or click **Browse** to specify a different folder.
7. Select whether you want the SQL Compliance Manager 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 SQL Compliance Manager Management Console

Setup Type	Description
Agent Only	Allows you to install only the SQL Compliance Manager Agent
Custom	Allows you to select the individual SQL Compliance Manager components you want to install

9. ***If you chose the Custom type***, select one or more SQL Compliance Manager components, and then click **Next**. Using the Custom setup type, you can install SQL Compliance Manager components in the following ways:
    - Collection Server and Repository with SQL Compliance Manager Agent
    - Collection Server and Repository
    - Management Console with SQL Compliance Manager Agent
    - Management Console only
    - SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager 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 SQL Compliance Manager Agent should use to connect to associated databases, and then click **Next**.
    e. Select whether you want to start the SQL Compliance Manager 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.

⚠ The SQL Compliance Manager installer detects if the local machine has an older version of the SQL Server 2012 Native Client installed and if needed SQL CM upgrades the Native Client to the latest version and proceeds with the installation. If no Native Client is installed on the server, then SQL CM installs the latest Native Client version and proceeds with the installation.

⚠ SQL Compliance Manager is ONLY compatible with IDERA Dashboard version 4.6 and with limited support.

16 JIC Navigate the IDERA Dashboard web console

The IDERA Dashboard is a a common technology framework designed to support the entire IDERA product suite. The IDERA Dashboard allows users to get an overview of the status of their SQL Server instances and hosted databases all in a consolidated view, while providing users the means to drill into individual product overviews for details. The IDERA Dashboard supports multiple copies of each product installation.

16.1 IDERA Dashboard menu bar

In the IDERA Dashboard menu bar, you can perform the following actions:

- Select the product content you want to view through the **Product** menu.
- Access administration tasks through the **Admin** menu.
- Access to a number of assistance topics through the **Help** menu.

16.1.1 Product menu

The Product menu allows you to quickly toggle between all of your installed IDERA products. You can customize the default order of your products in the Product menu by selecting the **Customize** option from the drop-down list and then clicking, holding, and dragging the product labels to the desired order. After selecting the order, click **Save** to save the changes.

> If the product list is long, the IDERA Dashboard displays the option **More** at the bottom of the menu. Click **More** to expand the next products in the list.

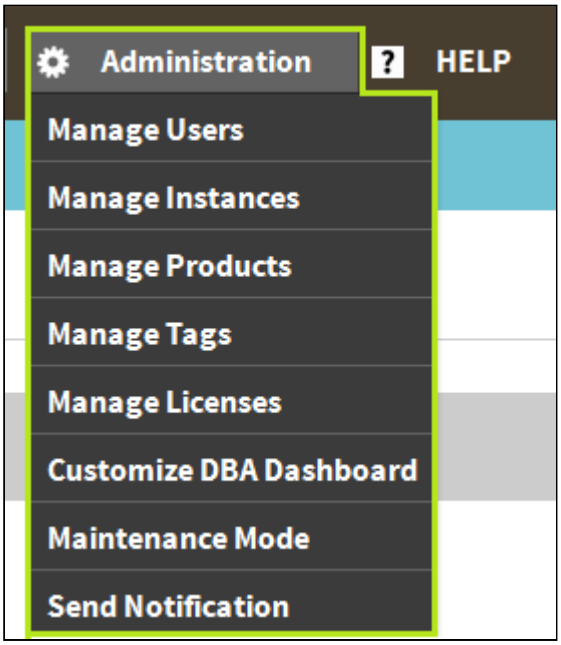
16.1.2 Welcome user

The user menu, which displays **<domain\username>**, allows you to manage the user account (if the user has the Product Administrator role) and log out of the IDERA Dashboard session. Click **Manage Accounts** to display the Manage Users view with the current user account selected and the details displayed in the User/Group Details pane.

16.1.3 Administration menu

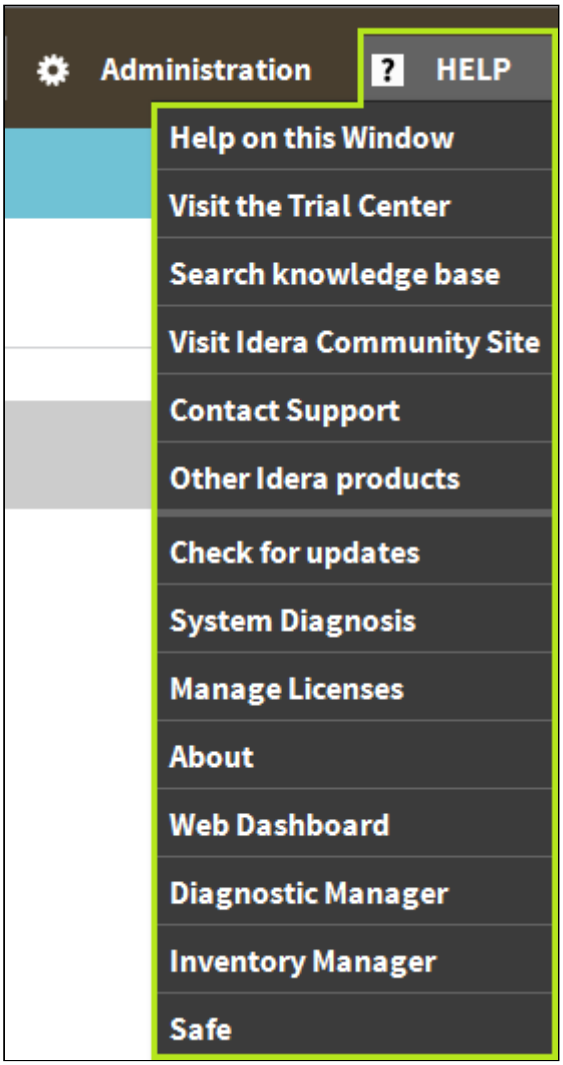
The **Administration** menu provides a list of shortcuts to the views available on the Administration tab.

> If a menu item is displayed but disabled, the current user account **does not have** the permission necessary to perform the associated function.



16.1.4 Help menu

The Help menu provides links to helpful areas such as the IDERA Knowledge Base or the IDERA Customer Support.



16.2 IDERA Dashboard Tabs

The IDERA Dashboard is comprised of the following tabs:

- Overview
- Details View
- Alerts
- Administration

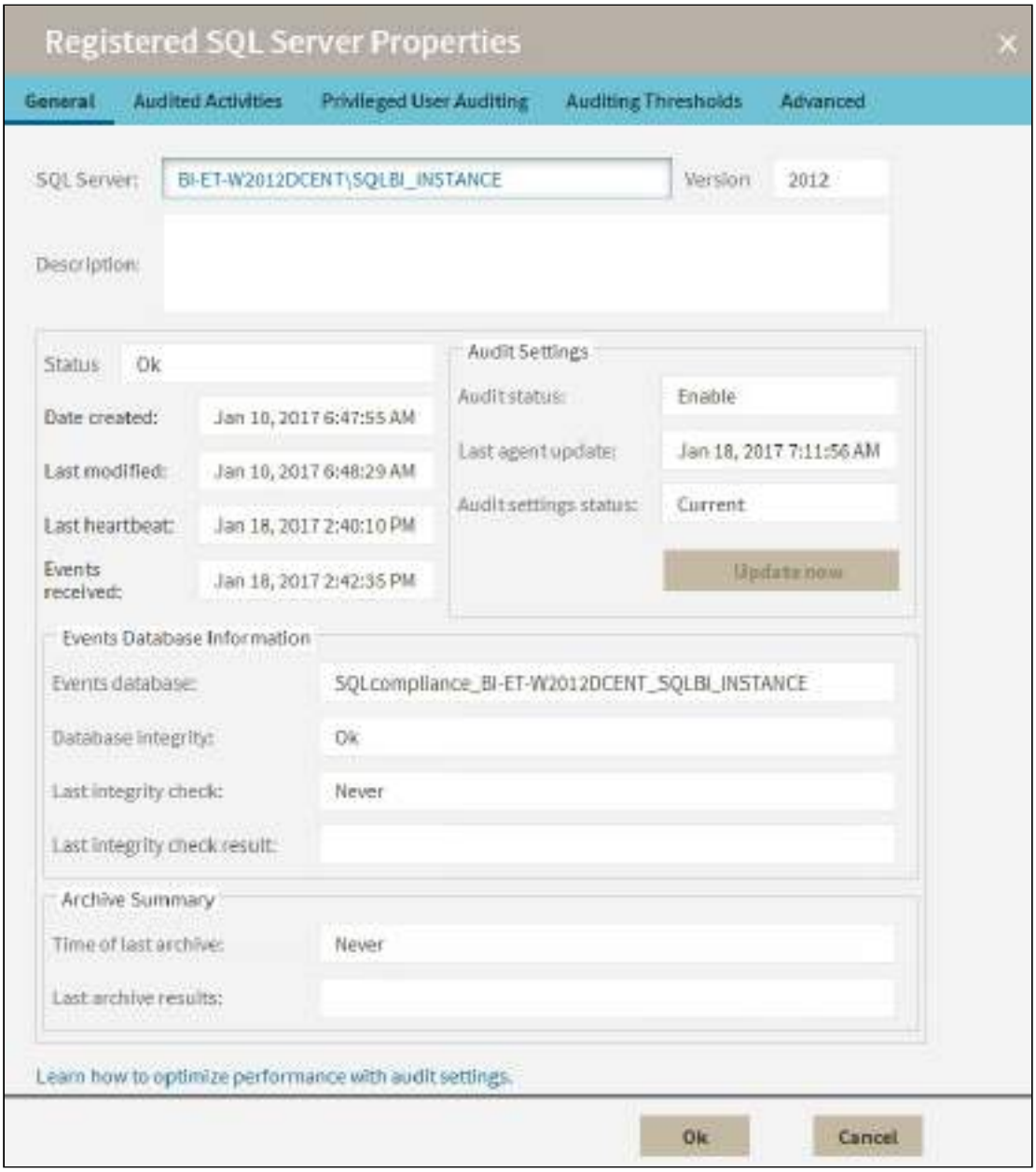
17 Manage instance properties

The IDERA SQL Compliance Manager Instance Properties window allows you to view and manage settings on the server hosting your SQL Server instance.

This topic reviews the following tabs:

17.1 General tab

The General tab of the Registered SQL Server Properties window allows you to change the description of this registered SQL Server instance, and view general properties such as audit settings.



17.1.1 Available actions

Update now

Allows you to send audit setting updates to the SQL Compliance Manager 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 SQL Compliance Manager Agent.

To diagnose SQL Compliance Manager Agent issues, check the SQL Compliance Manager Agent status and review the SQL Compliance Manager Agent properties.

17.1.2 Available fields

SQL Server

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 SQL Compliance Manager 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 in this instance.

Last heartbeat

Provides the date and time when the SQL Compliance Manager Agent auditing this instance contacted the Collect Server. This communication is called a heartbeat. Typically, the SQL Compliance Manager 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 SQL Compliance Manager Agent.

Audit Settings

Provides the following information about the status of your audit settings:

- Whether auditing is enabled on this instance
- When the SQL Compliance Manager 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 SQL Compliance Manager 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

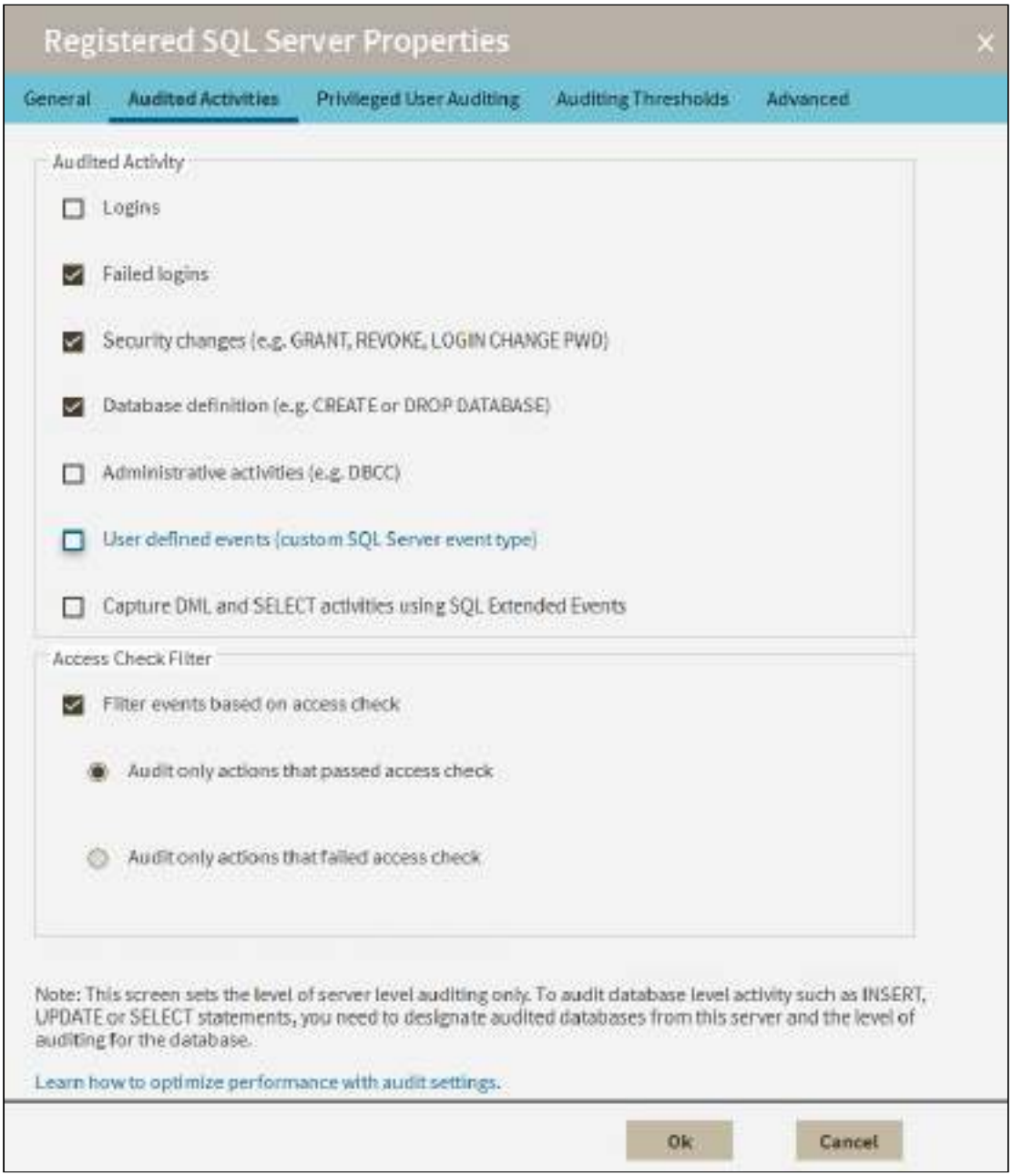
Provides the date and time when audited events collected for this SQL Server instance were last archived.

Last archive results

Provides the results of the data integrity check. SQL Compliance Manager automatically performs a data integrity check each time you archive audited events from the Repository databases.

17.2 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. IDERA SQL Compliance Manager audits these events at the server level only.



17.2.1 Available fields

Audited Activity

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.

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.

Capture DML and SELECT Activities

Via Trace Events - Allows you to select Trace Events as your event handling system for DML and SELECT activities. For more information about this feature see, Understanding Traces.

Via Extended Events - Allows you to select SQL Server Extended Events as your event handling system for DML and SELECT events for SQL Server 2012 and later versions. For more information about this feature, see Using SQL Server Extended Events.

Via SQL Server Audit Specifications - Allows you to select SQL Server Audit Logs as your event handling system for DML and SELECT events for SQL Server 2017 and later versions. For more information about this feature, see Using SQL Server Audit Logs.

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 Compliance Manager 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.

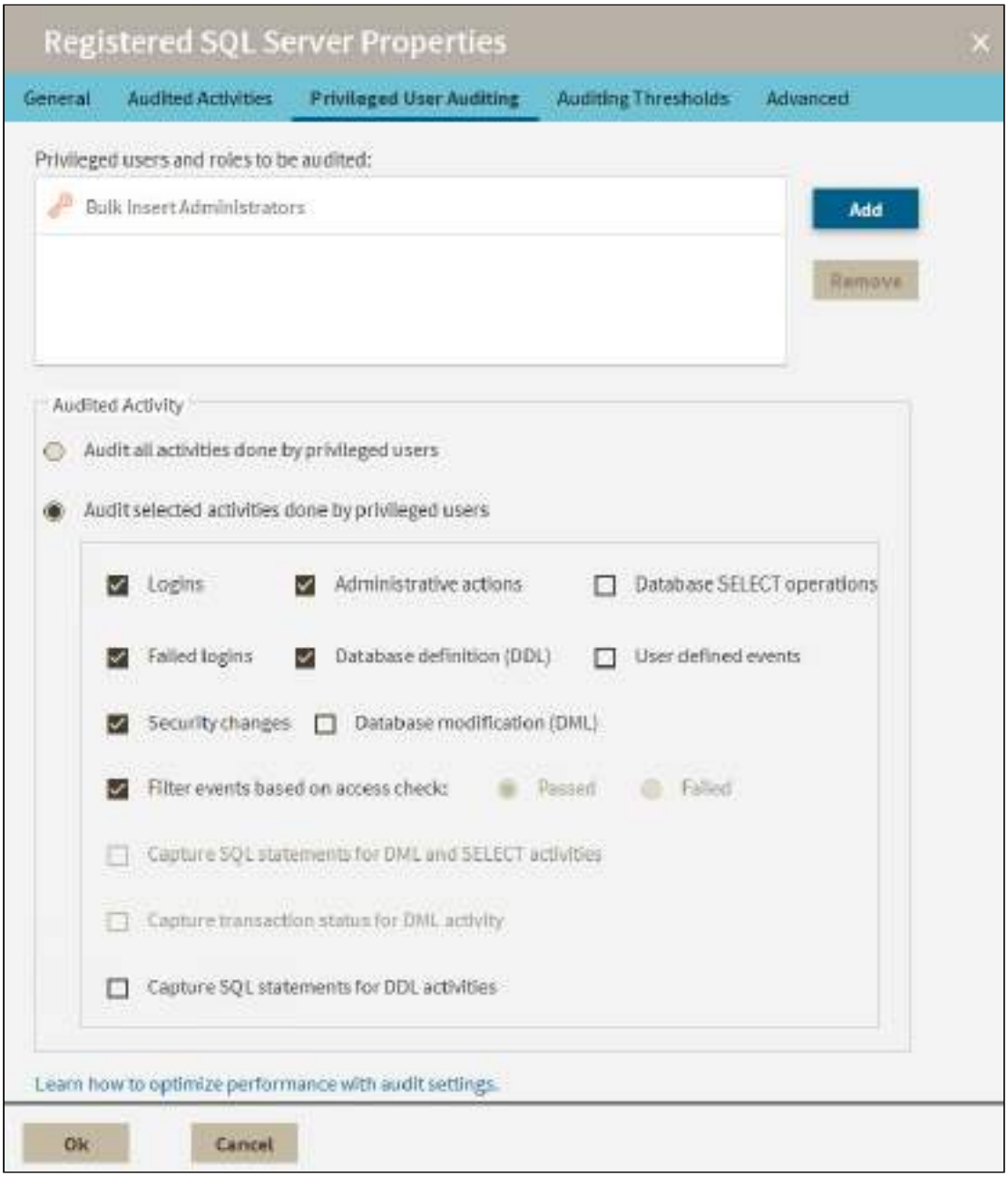
Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL Server.
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server.

17.3 Privileged User Auditing tab

The Privileged User Auditing tab of the Registered SQL Server Properties window 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 SQL Compliance Manager 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.



17.3.1 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 SQL Compliance Manager Agent no longer collects events recorded for that login or the role members.

17.3.2 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 SQL Compliance Manager 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.

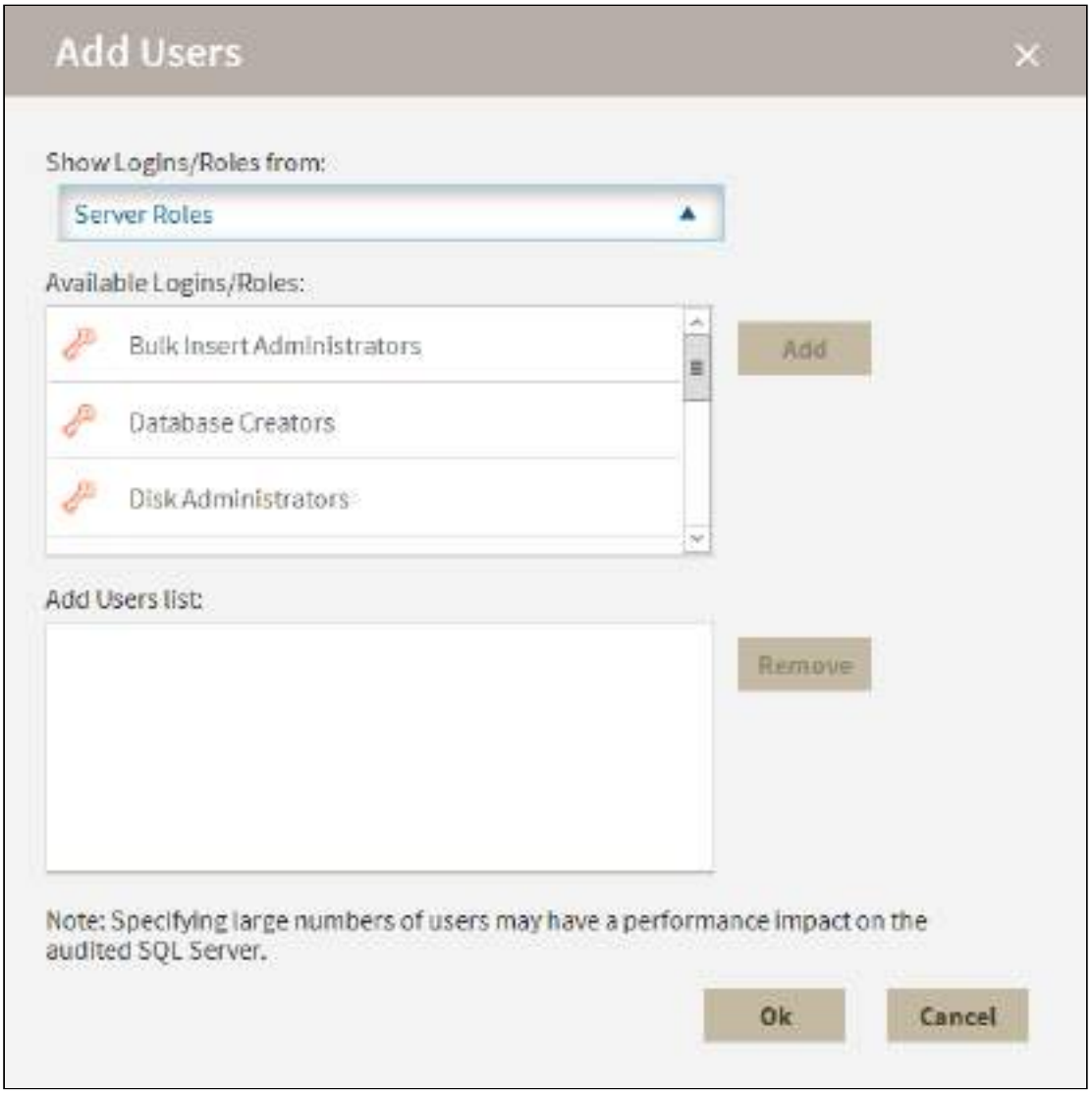
Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL 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.

17.3.3 Add Users window

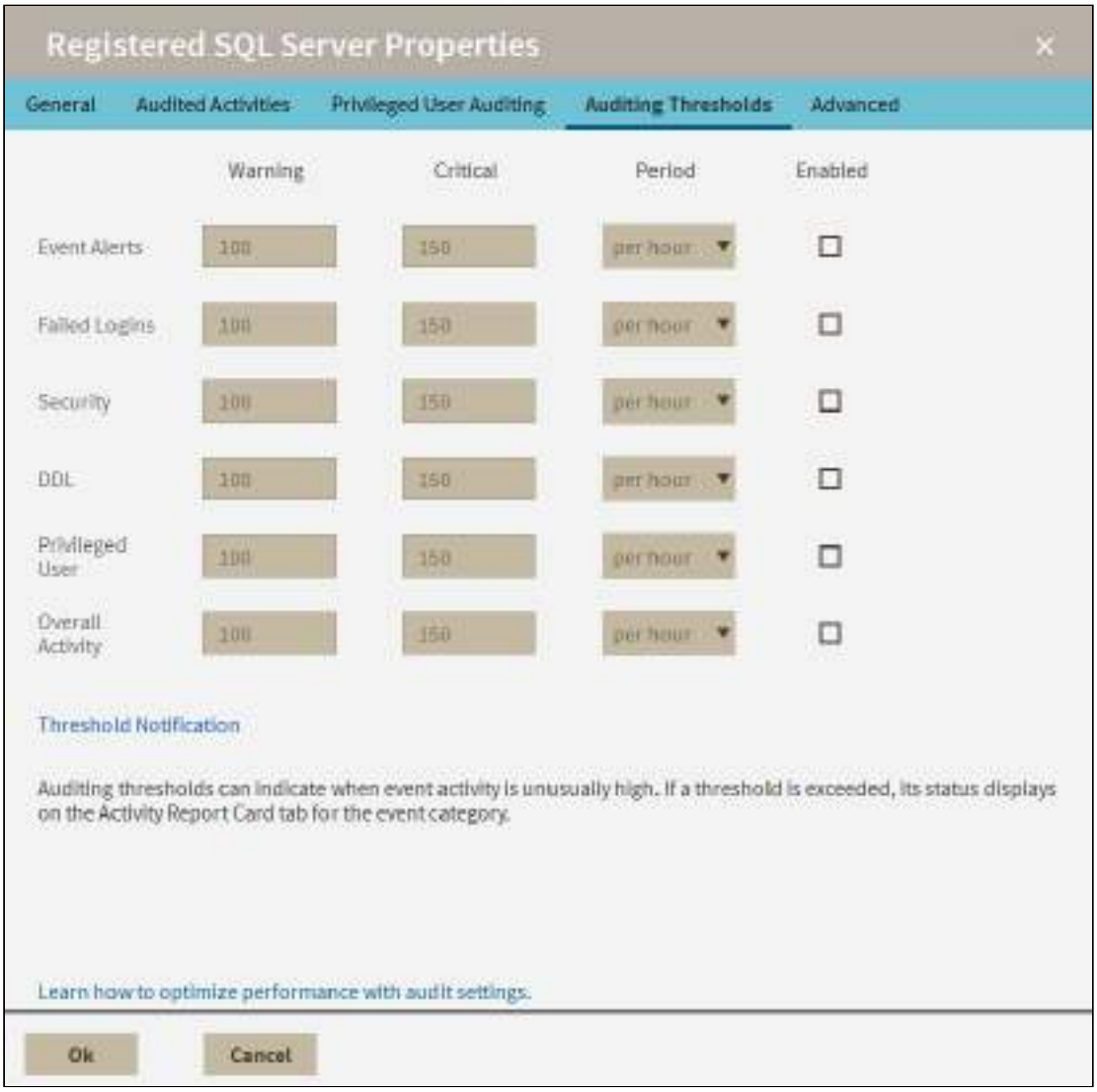
The Add Users window is accessed by clicking **Add** on the Privileged User Auditing tab while viewing Registered SQL Server Properties. Use this window to include selected login accounts and roles as privileged. Added logins/roles may be removed by selecting the item in the Privileged User Auditing tab, and then clicking **Remove**.



17.4 Auditing Thresholds tab

The Auditing Thresholds tab of the Registered SQL Server Properties window allows you to set auditing thresholds to identify unusual activity on the selected SQL Server instance. IDERA 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.



17.4.1 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

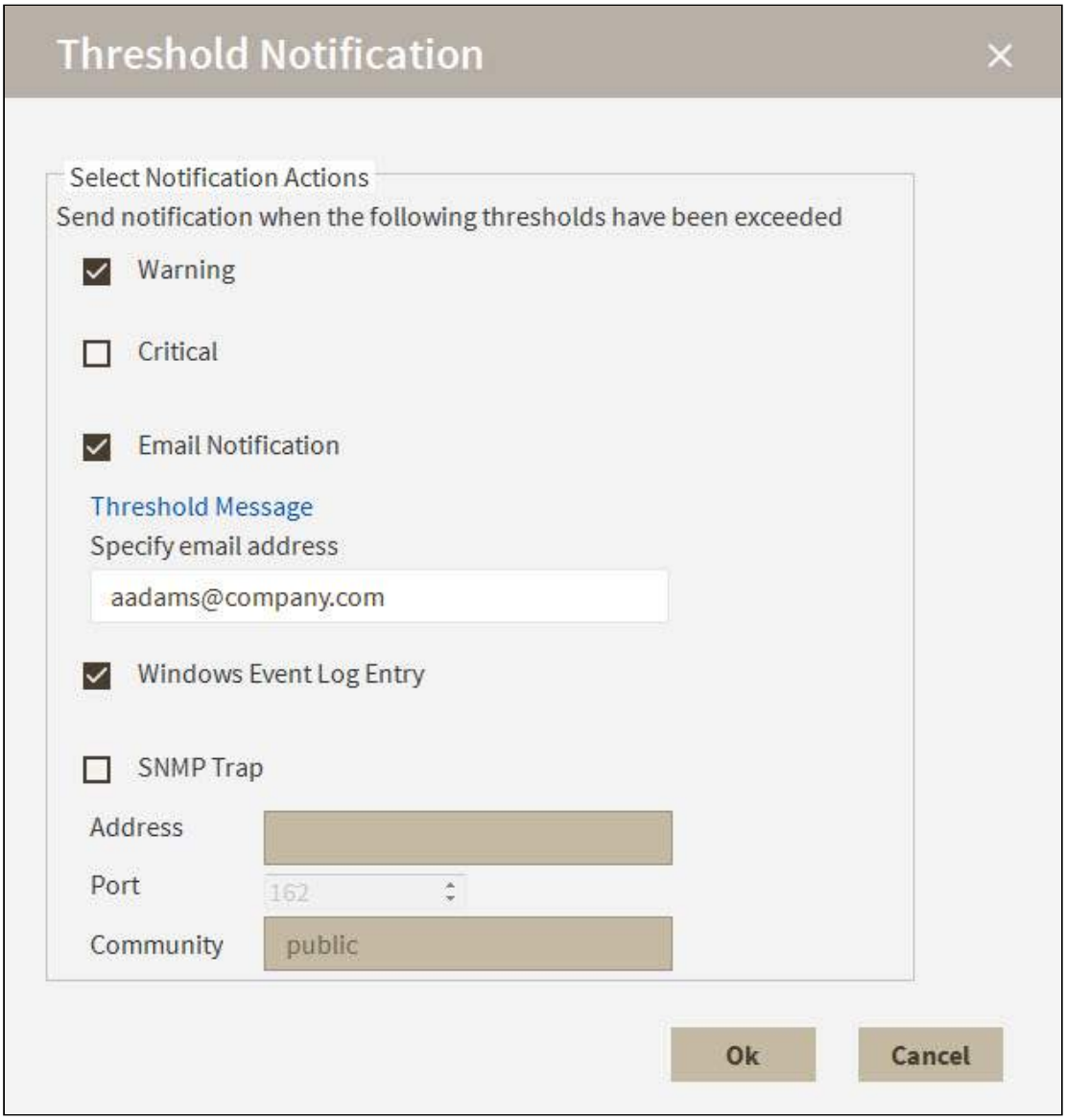
Allows you to set an acceptable rate, or time span, for the warning and critical thresholds. For example, you may expect overall activity to be no more than 200 events per day on this instance.

Enabled

Allows you to enable (select) or disable (clear) auditing thresholds for a particular event category.

17.5 Threshold Notification window

The Threshold Notification window is accessed by clicking **Threshold Notification** on the Auditing Threshold tab while viewing Registered SQL Server Properties. Use this window to set up notifications for when thresholds are exceeded. Set up notifications independently for each event threshold. Note that notifications are sent only if both the threshold and notification are enabled.



17.5.1 Available fields

Event alert level

Allows you to select whether you want the notification sent when the threshold is at **Warning** and/or **Critical** level.

Notification type

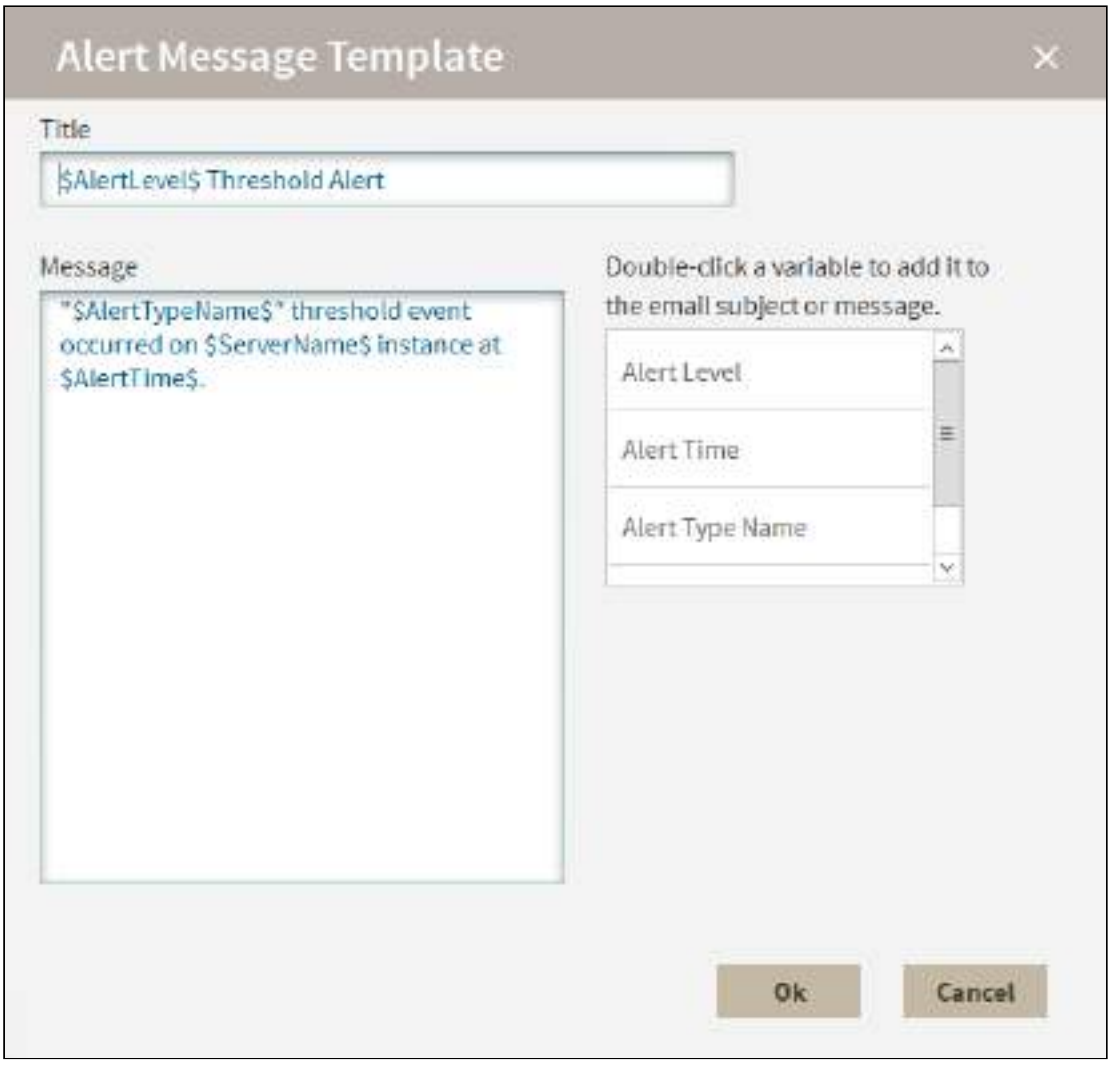
Allows you to select whether you want notifications by email, Windows event log, and/or SNMP traps. ***If you select to receive an email notification***, you must include a valid email address. ***If you select to receive SNMP trap notification***, you must include the SNMP trap address, port, and community. ***If you select to receive Windows event log notification***, note that the event is logged as informational.

Threshold message

Allows you to create and manage alert notification messages in the Alert Message Template window and then sent to the email address included in the **Email Notification** area of the Threshold Notification window. Use the list of available variables to help you create an alert notification message that contains all of the important information for the recipient to understand what is affected and how.

17.5.2 Alert Message Template window

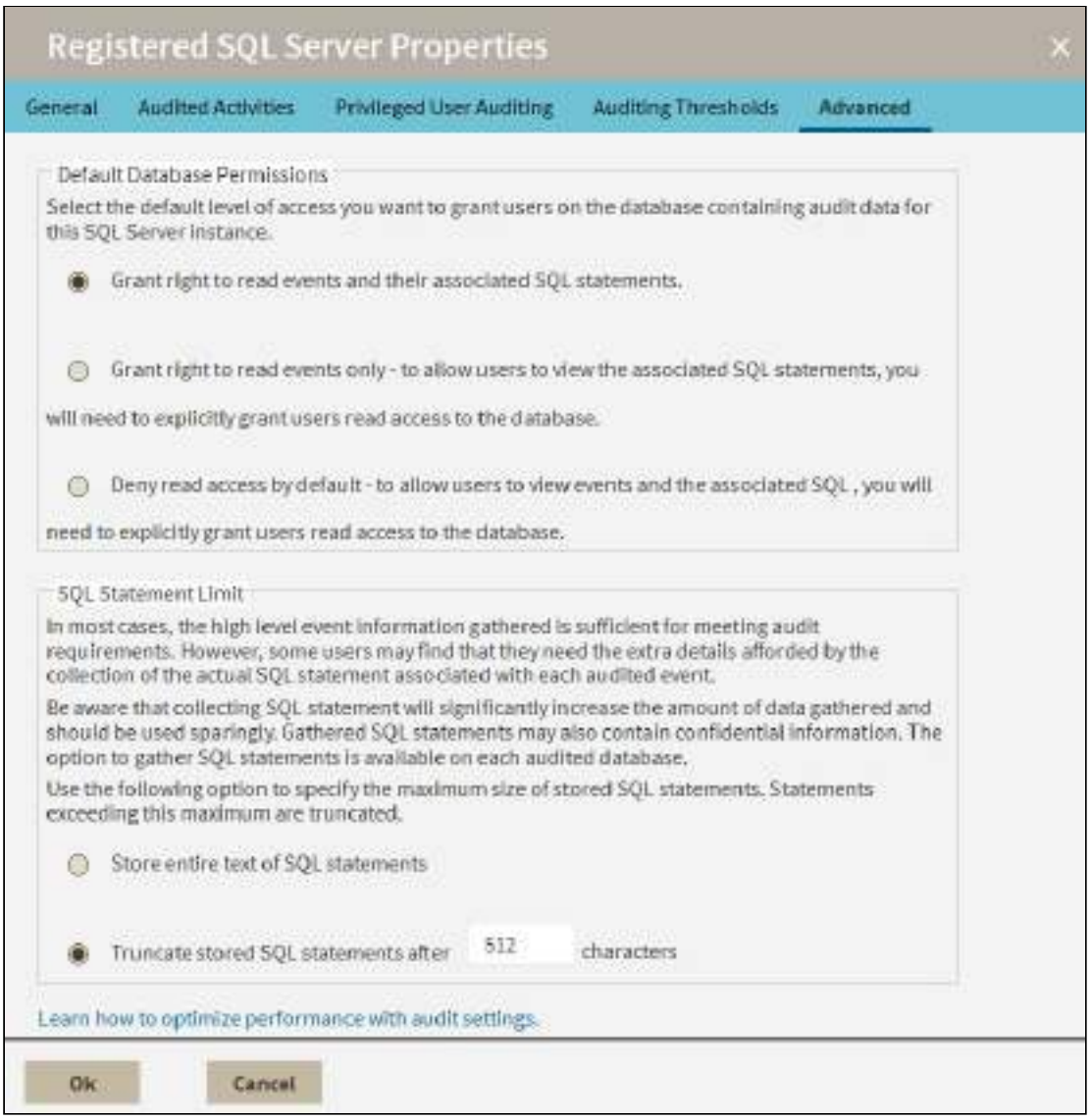
The Alert Message Template window is accessed by clicking **Threshold Message** on the Threshold Notification window while viewing Registered SQL Server Properties. Use this window to create an effective message to be sent to the email address in the Threshold Notification window when thresholds are exceeded. Use the list of available variables to help you create an alert notification message that contains all of the important information for the recipient to understand what is affected and how.



17.6 Advanced tab

The Advanced tab of the Registered SQL Server Properties window 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.



17.6.1 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.