

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:

- General tab
- Audited Activities tab
- Privileged User Auditing tab
- Auditing Thresholds tab
- Threshold Notification window
- Advanced tab

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.

The screenshot shows the 'Registered SQL Server Properties' window with the 'General' tab selected. The window has a title bar with a close button (X). Below the title bar is a tabbed interface with five tabs: 'General', 'Audited Activities', 'Privileged User Auditing', 'Auditing Thresholds', and 'Advanced'. The 'General' tab is active, showing the following fields and sections:

- SQL Server:** BI-ET-W2012DCENT\SQLBI_INSTANCE
- Version:** 2012
- Description:** (empty text box)
- Status:** Ok
- Date created:** Jan 10, 2017 6:47:55 AM
- Last modified:** Jan 10, 2017 6:48:29 AM
- Last heartbeat:** Jan 18, 2017 2:40:10 PM
- Events received:** Jan 18, 2017 2:42:35 PM
- Audit Settings:**
 - Audit status:** Enable
 - Last agent update:** Jan 18, 2017 7:11:56 AM
 - Audit settings status:** Current
 - Update now** (button)
- Events Database Information:**
 - Events database:** SQLcompliance_BI-ET-W2012DCENT_SQLBI_INSTANCE
 - Database integrity:** Ok
 - Last integrity check:** Never
 - Last integrity check result:** (empty text box)
- Archive Summary:**
 - Time of last archive:** Never
 - Last archive results:** (empty text box)

At the bottom of the window, there is a link: [Learn how to optimize performance with audit settings.](#) and two buttons: **Ok** and **Cancel**.

Available actions

Update now

Allows you to send audit setting updates to the SQLcompliance Agent running on this SQL Server instance. This action is available when you update audit settings between heartbeats, and the Collection Server has not yet sent your changes to the SQLcompliance Agent.

To diagnose SQLcompliance Agent issues, check the SQLcompliance Agent status and review the SQLcompliance Agent properties.

Available fields**SQL Server**

Provides the name of the selected SQL Server instance. *If you are auditing a local instance*, the SQL Server instance name is the name of the physical computer hosting this instance.

Version

Provides the version number of SQL Server running on this registered instance.

Description

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

Status

Provides the current status of this instance. The current status indicates whether SQL Server is available and the SQLcompliance Agent Service and Collection Service are running. Use the Registered SQL Servers tab to see an overview of the status of all registered SQL Server instances.

Date created

Provides the date and time when this instance was registered. By default, auditing is enabled when the instance is registered with SQL Compliance Manager.

Last modified

Provides the date and time when audit settings were last modified on this instance.

Last heartbeat

Provides the date and time when the SQLcompliance Agent auditing this instance contacted the Collect Server. This communication is called a heartbeat. Typically, the SQLcompliance Agent receives audit setting updates during a heartbeat.

Events received

Provides the date and time when the Collection Server last received audited events (SQL trace files) from the SQLcompliance Agent.

Audit Settings

Provides the following information about the status of your audit settings:

- Whether auditing is enabled on this instance
- When the SQLcompliance Agent auditing this instance received the last audit setting updates
- Whether the audit settings are current

If the audit settings are not current, you can send your updates to the SQLcompliance Agent by clicking **Update now**.

Event Database Information

Provides the following information about audited events collected on this instance:

- Name of the database where audited events processed by the Collection Server are stored
- Whether the Repository databases passed the last audit data integrity check
- When the last audit data integrity check was performed

Time of last archive

Provides the date and time when audited events collected for this SQL Server instance were last archived.

Last archive results

Provides the results of the data integrity check. SQL Compliance Manager automatically performs a data integrity check each time you archive audited events from the Repository databases.

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.

Registered SQL Server Properties [X]

General **Audited Activities** Privileged User Auditing Auditing Thresholds Advanced

Audited Activity

- ☐ Logins
- ☒ Failed logins
- ☒ Security changes (e.g. GRANT, REVOKE, LOGIN CHANGE PWD)
- ☒ Database definition (e.g. CREATE or DROP DATABASE)
- ☐ Administrative activities (e.g. DBCC)
- ☐ User defined events (custom SQL Server event type)
- ☐ Capture DML and SELECT activities using SQL Extended Events

Access Check Filter

- ☒ Filter events based on access check
 - ☒ Audit only actions that passed access check
 - ☐ Audit only actions that failed access check

Note: This screen sets the level of server level auditing only. To audit database level activity such as INSERT, UPDATE or SELECT statements, you need to designate audited databases from this server and the level of auditing for the database.

[Learn how to optimize performance with audit settings.](#)

Ok Cancel

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 using SQL 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](#).

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.

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 SQLcompliance Agent sends the trace files to the Collection Server. To ensure an immediate application of your new audit settings, click **Update Audit Settings Now** on the Agent menu.

Registered SQL Server Properties

General
Audited Activities
Privileged User Auditing
Auditing Thresholds
Advanced

Privileged users and roles to be audited:

Bulk Insert Administrators
Add
Remove

Audited Activity

☐ Audit all activities done by privileged users
☒ Audit selected activities done by privileged users

☒ Logins
☒ Administrative actions
☐ Database SELECT operations
☒ Failed logins
☒ Database definition (DDL)
☐ User defined events
☒ Security changes
☐ Database modification (DML)
☒ Filter events based on access check:
☒ Passed
☐ Failed
☐ Capture SQL statements for DML and SELECT activities
☐ Capture transaction status for DML activity
☐ Capture SQL statements for DDL activities

[Learn how to optimize performance with audit settings.](#)

Ok
Cancel

Available actions

Add

Allows you to select one or more privileged users to audit. You can select privileged users by login name or by membership to a fixed server role.

Remove

Allows you to remove the selected SQL Server login or fixed server role from the list of audited privileged users. When you remove the login or role, the SQLcompliance Agent no longer collects events recorded for that login or the role members.

Available fields

Privileged users and roles to be audited

Lists the audited privileged users by login name or fixed server role. **If you are auditing privileged users in a fixed server role**, the SQLcompliance Agent collects activities executed by all members of the selected role.

Audited Activity

Allows you to specify which activities (events) you want to audit for the selected privileged users.

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Capture SQL statements for DDL activity

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 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**.

Add Users
×

Show Logins/Roles from:

Server Roles
▲

Available Logins/Roles:

 Bulk Insert Administrators	<div> ▲ </div> <div> ≡ </div> <div> ▼ </div>	Add
 Database Creators		
 Disk Administrators		

Add Users list:

Remove

Note: Specifying large numbers of users may have a performance impact on the audited SQL Server.

Ok
Cancel

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.

Registered SQL Server Properties

General
Audited Activities
Privileged User Auditing
Auditing Thresholds
Advanced

	Warning	Critical	Period	Enabled
Event Alerts	100	150	per hour ▼	<input type="checkbox"/>
Failed Logins	100	150	per hour ▼	<input type="checkbox"/>
Security	100	150	per hour ▼	<input type="checkbox"/>
DDL	100	150	per hour ▼	<input type="checkbox"/>
Privileged User	100	150	per hour ▼	<input type="checkbox"/>
Overall Activity	100	150	per hour ▼	<input type="checkbox"/>

Threshold Notification

Auditing thresholds can indicate when event activity is unusually high. If a threshold is exceeded, its status displays on the Activity Report Card tab for the event category.

[Learn how to optimize performance with audit settings.](#)

Ok
Cancel

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.

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.

Threshold Notification

Select Notification Actions

Send notification when the following thresholds have been exceeded

☒ Warning

☐ Critical

☒ Email Notification

[Threshold Message](#)

Specify email address

aadams@company.com

☒ Windows Event Log Entry

☐ SNMP Trap

Address

Port: 162

Community: public

Ok Cancel

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 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.

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.

Alert Message Template

×

Title

\$AlertLevel\$ Threshold Alert

Message

"\$AlertTypeName\$" threshold event occurred on \$ServerName\$ instance at \$AlertTime\$.

Double-click a variable to add it to the email subject or message.

Alert Level

Alert Time

Alert Type Name

Ok

Cancel

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.

Registered SQL Server Properties

General
Audited Activities
Privileged User Auditing
Auditing Thresholds
Advanced

Default Database Permissions

Select the default level of access you want to grant users on the database containing audit data for this SQL Server instance.

☒ 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 , you will need to explicitly grant users read access to the database.

SQL Statement Limit

In most cases, the high level event information gathered is sufficient for meeting audit requirements. However, some users may find that they need the extra details afforded by the collection of the actual SQL statement associated with each audited event.

Be aware that collecting SQL statement will significantly increase the amount of data gathered and should be used sparingly. Gathered SQL statements may also contain confidential information. The option to gather SQL statements is available on each audited database.

Use the following option to specify the maximum size of stored SQL statements. Statements exceeding this maximum are truncated.

☐ Store entire text of SQL statements

☒ Truncate stored SQL statements after characters

[Learn how to optimize performance with audit settings.](#)

Ok
Cancel

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.