

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.

The screenshot shows the 'SQL Server Default Audit Settings' window with the 'Audited Activities' tab selected. The window has a title bar with a green checkmark icon, a question mark, and a close button. The tabs are 'Audited Activities', 'Trusted Users', 'Privileged User Auditing', 'Auditing Thresholds', and 'Advanced'. The 'Audited Activity' section contains a list of activities with checkboxes: 'Logins' (unchecked), 'Logouts' (unchecked), 'Failed logins' (checked), 'Security Changes (e.g. GRANT, REVOKE, LOGIN CHANGE PWD)' (unchecked), 'Administrative Actions (e.g. DBCC)' (unchecked), 'Database Definition(DDL) (e.g. CREATE or DROP DATABASE)' (unchecked), and 'User Defined Events (custom SQL Server event type)' (unchecked). The 'Access Check Filter' section has a checked checkbox 'Filter events based on access check' with two radio buttons: 'Passed' (selected) and 'Failed' (unselected). The 'Capture DML and Select Activities' section has three radio buttons: 'Via Trace Events' (selected), 'Via Extended Events' (unselected), and 'Via SQL Server Audit Specifications' (unselected). A note at the bottom states: 'Note: This screen sets the level of server 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.' Below the note is a warning: 'The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.' At the bottom are three buttons: 'Reset to Idera Default Settings', 'Save', and 'Cancel'.

SQL Server Default Audit Settings

Audited Activities | Trusted Users | Privileged User Auditing | Auditing Thresholds | Advanced

Audited Activity

- ☐ Logins
- ☐ Logouts
- ☒ Failed logins
- ☐ Security Changes (e.g. GRANT, REVOKE, LOGIN CHANGE PWD)
- ☐ Administrative Actions (e.g. DBCC)
- ☐ Database Definition(DDL) (e.g. CREATE or DROP DATABASE)
- ☐ User Defined Events (custom SQL Server event type)

Access Check Filter

- ☒ Filter events based on access check
 - ☒ Passed
 - ☐ Failed

Capture DML and Select Activities

- ☒ Via Trace Events
- ☐ Via Extended Events
- ☐ Via SQL Server Audit Specifications

Note: This screen sets the level of server 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.

The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.

Reset to Idera Default Settings | **Save** | Cancel

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.

The screenshot shows the 'SQL Server Default Audit Settings' dialog box with the 'Trusted Users' tab selected. The 'Add Trusted User' section has a dropdown menu set to 'Server Roles' and an empty text box, with an 'Add...' button to the right. Below this, a list box titled 'Trusted users and roles to be filtered:' contains a single entry 'sa' with a key icon. A 'Remove' button is to the right of the list. At the bottom, there are three buttons: 'Reset to Idera Default Settings', 'Save', and 'Cancel'. A warning message at the bottom states: 'The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit 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.

The screenshot shows the 'SQL Server Default Audit Settings' window with the 'Privileged User Auditing' tab selected. The window has a title bar with a green checkmark icon and standard window controls. Below the title bar are five tabs: 'Audited Activities', 'Trusted Users', 'Privileged User Auditing' (selected), 'Auditing Thresholds', and 'Advanced'. The main content area is divided into two sections. The top section, 'Add Privileged User:', features a dropdown menu set to 'Server Roles', an empty text input field, and an 'Add...' button. Below this is a list box titled 'Privileged users and roles to be audited:' containing a single entry 'sa' with a key icon. To the right of the list box is a 'Remove' button. The bottom section, 'Audited Activity', contains two radio buttons: 'Audit all activities done by privileged users' (unselected) and 'Audit selected activities done by privileged users' (selected). Below the radio buttons is a grid of checkboxes for various activity categories: 'Logins' (checked), 'Logouts' (unchecked), 'Failed logins' (checked), 'Security Changes' (checked), 'Administrative Actions' (unchecked), 'Database Definition (DDL)' (checked), 'Database Modification (DML)' (unchecked), 'Database SELECT operations' (unchecked), and 'User Defined Events' (unchecked). Below the grid are three more checkboxes: 'Filter events based on access check:' (checked) with 'Passed' (selected) and 'Failed' (unselected) radio buttons, 'Capture SQL Statements for DML and SELECT activities' (unchecked), 'Capture Transaction Status for DML Activity' (unchecked), and 'Capture SQL statements for DDL and Security Changes' (checked). At the bottom of the window, there is a note: 'Note: Selected items that are disabled have been enabled at the server level. Deselected items that are disabled are waiting for other settings to be applied before you can use them.' Below the note is a warning message: 'The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.' At the very bottom are three buttons: 'Reset to Idera Default Settings', 'Save' (highlighted with a blue border), and 'Cancel'.

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

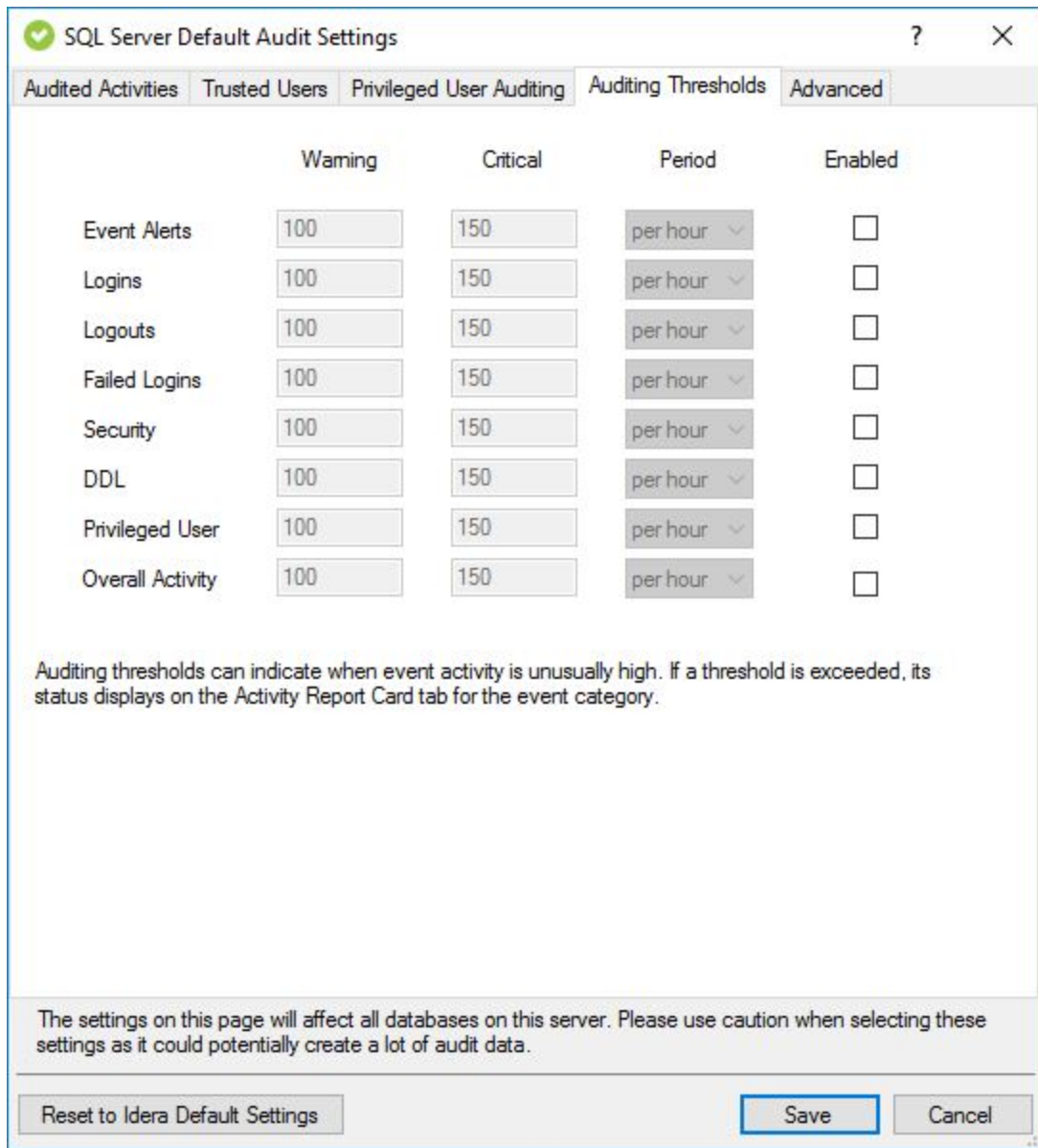
Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

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.



The dialog box is titled "SQL Server Default Audit Settings" and has five tabs: "Audited Activities", "Trusted Users", "Privileged User Auditing", "Auditing Thresholds", and "Advanced". The "Auditing Thresholds" tab is selected. It contains a table with columns: "Warning", "Critical", "Period", and "Enabled". The table lists eight event categories: "Event Alerts", "Logins", "Logouts", "Failed Logins", "Security", "DDL", "Privileged User", and "Overall Activity". Each category has input fields for "Warning" and "Critical" thresholds (all set to 100), a "Period" dropdown menu (all set to "per hour"), and an "Enabled" checkbox (all unchecked). Below the table, there is a note: "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." At the bottom, there are three buttons: "Reset to Idera Default Settings", "Save", and "Cancel".

| | Warning | Critical | Period | Enabled |
|------------------|---------|----------|----------|--------------------------|
| Event Alerts | 100 | 150 | per hour | <input type="checkbox"/> |
| Logins | 100 | 150 | per hour | <input type="checkbox"/> |
| Logouts | 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"/> |

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.

The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.

Reset to Idera Default Settings Save 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 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.

The screenshot shows the 'SQL Server Default Audit Settings' window with the 'Advanced' tab selected. The window has a title bar with a green checkmark icon, a question mark, and a close button. Below the title bar are five tabs: 'Audited Activities', 'Trusted Users', 'Privileged User Auditing', 'Auditing Thresholds', and 'Advanced'. The 'Advanced' tab is active and contains two main sections: 'Default Database Permissions' and 'SQL Statement Limit'. The 'Default Database Permissions' section has a description and three radio button options. The 'SQL Statement Limit' section has a description, a warning, and two radio button options with a character limit input field. At the bottom, there is a warning message and three buttons: 'Reset to Idera Default Settings', 'Save', and 'Cancel'.

SQL Server Default Audit Settings

Audited Activities **Trusted Users** **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 event.

Be aware that collecting SQL statements 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

For Reports, SQL text will be truncated after characters.

The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.

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.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)