

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.

The screenshot shows the 'Registered SQL Server Properties' 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 tabs: 'General', 'Audited Activities', 'Trusted Users', 'Privileged User Auditing' (active), 'Auditing Thresholds', and 'Advanced'. The main content area is divided into two sections. The top section, 'Privileged users and roles to be audited:', contains a list box with 'Bulk Insert Administrators' and two buttons, 'Add...' and 'Remove'. 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 activities: '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), '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' (unchecked). The 'Filter events based on access check:' checkbox has two sub-radio buttons: 'Passed' (selected) and 'Failed' (unselected). At the bottom of the window 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 link: 'Learn how to optimize performance with audit settings.' At the very bottom are 'OK' and 'Cancel' buttons.

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.

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.

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.