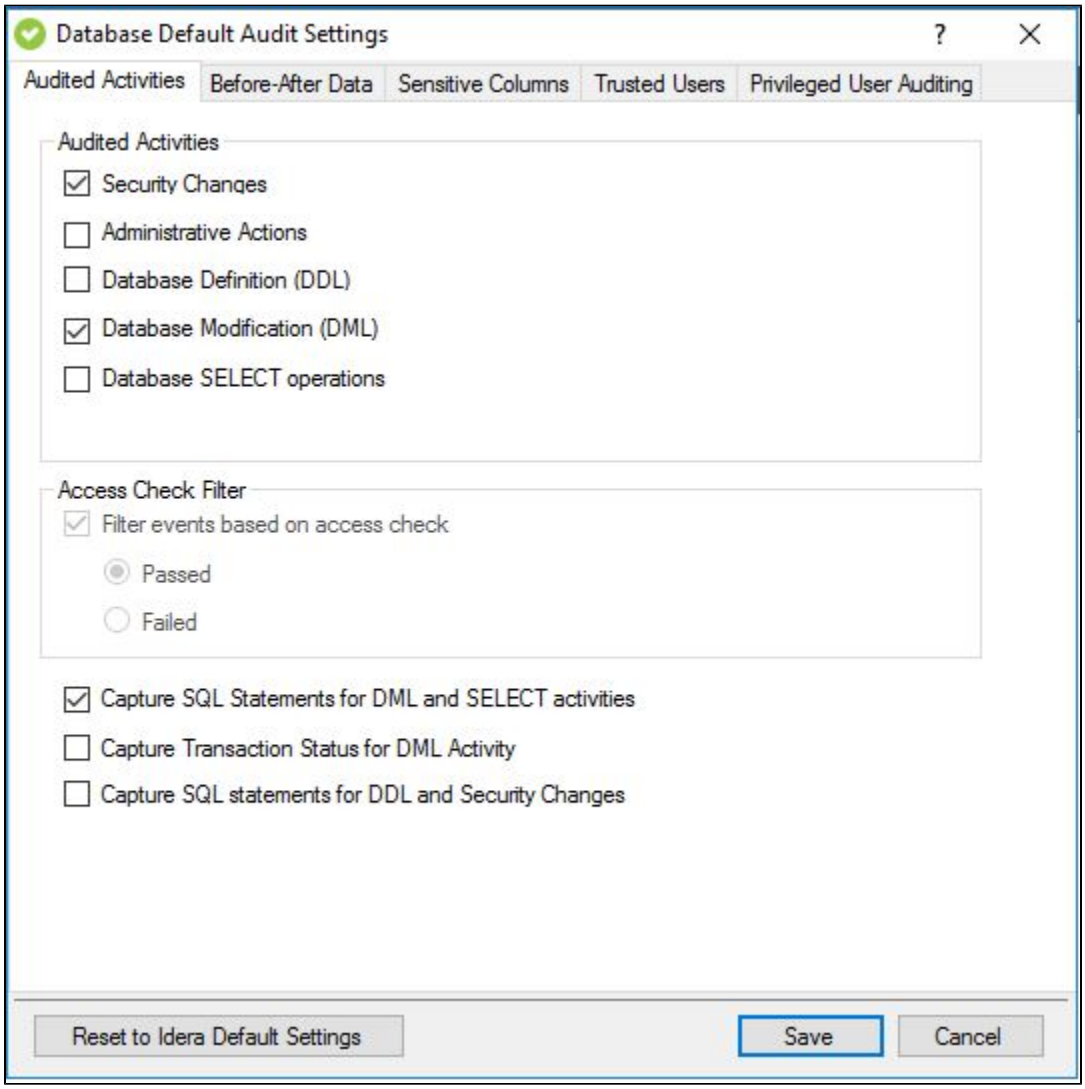
SQL Database Default Audit Settings Properties

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

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.

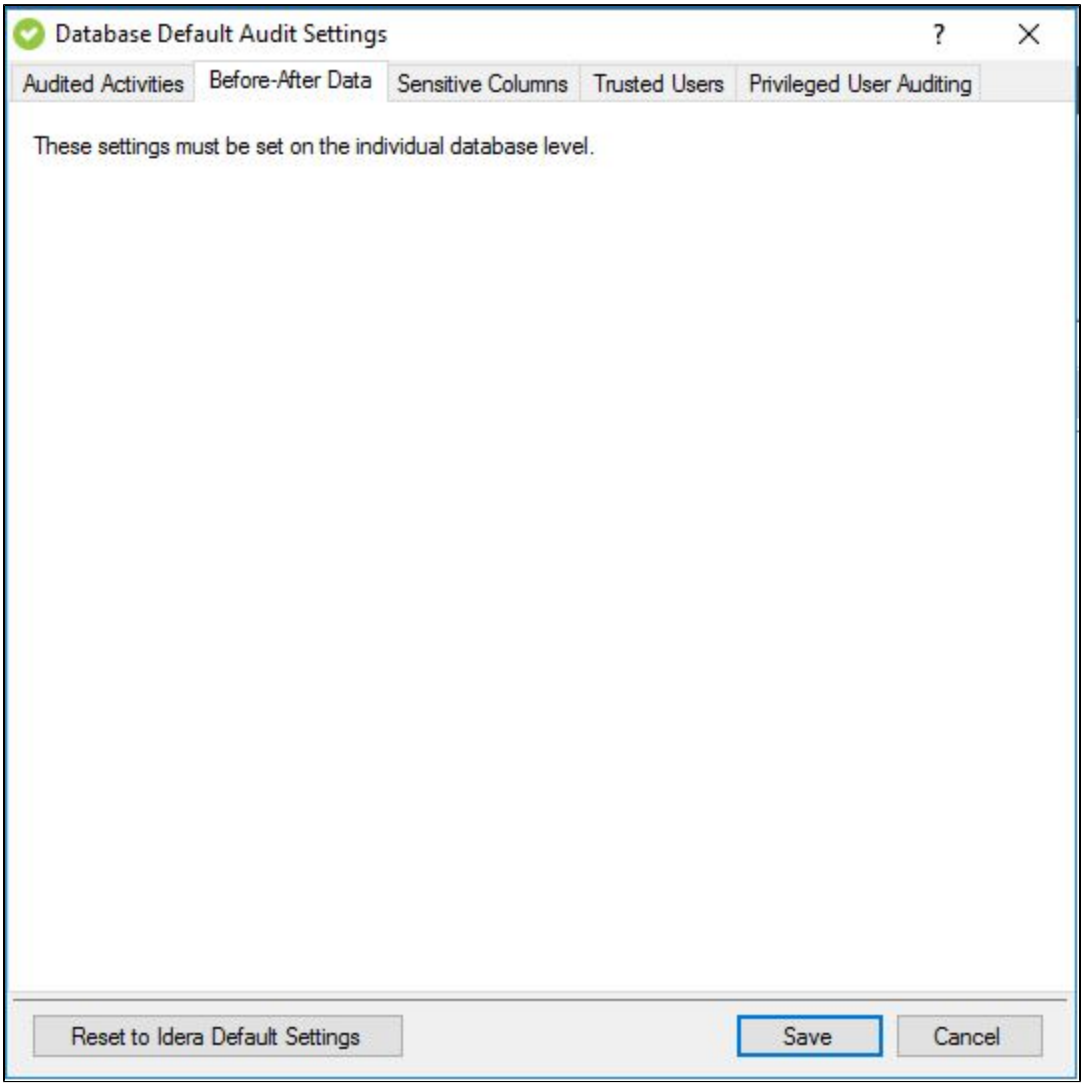
Capture SQL statements for DDL and Security Changes

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.

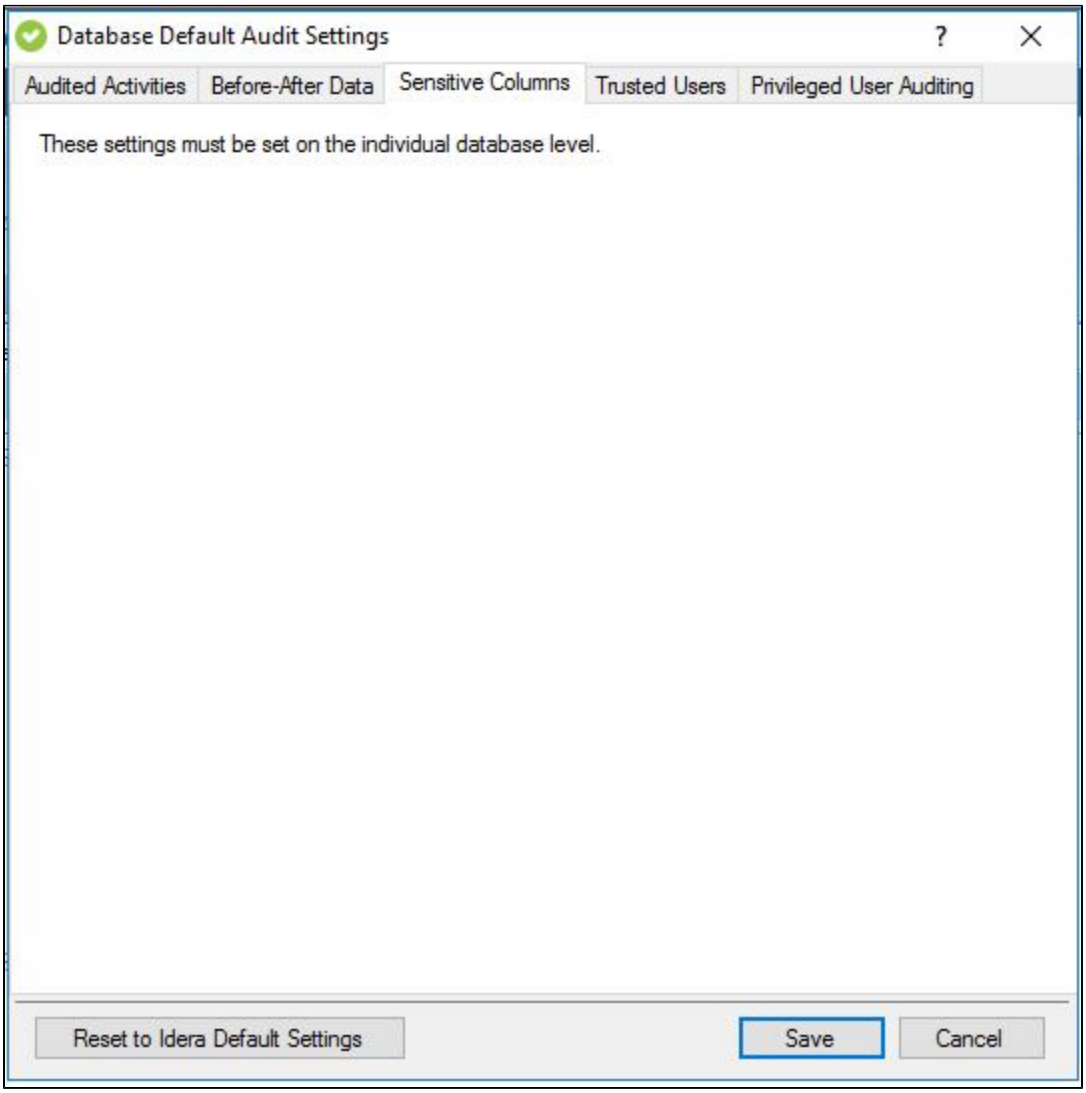
Before and After tab

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.

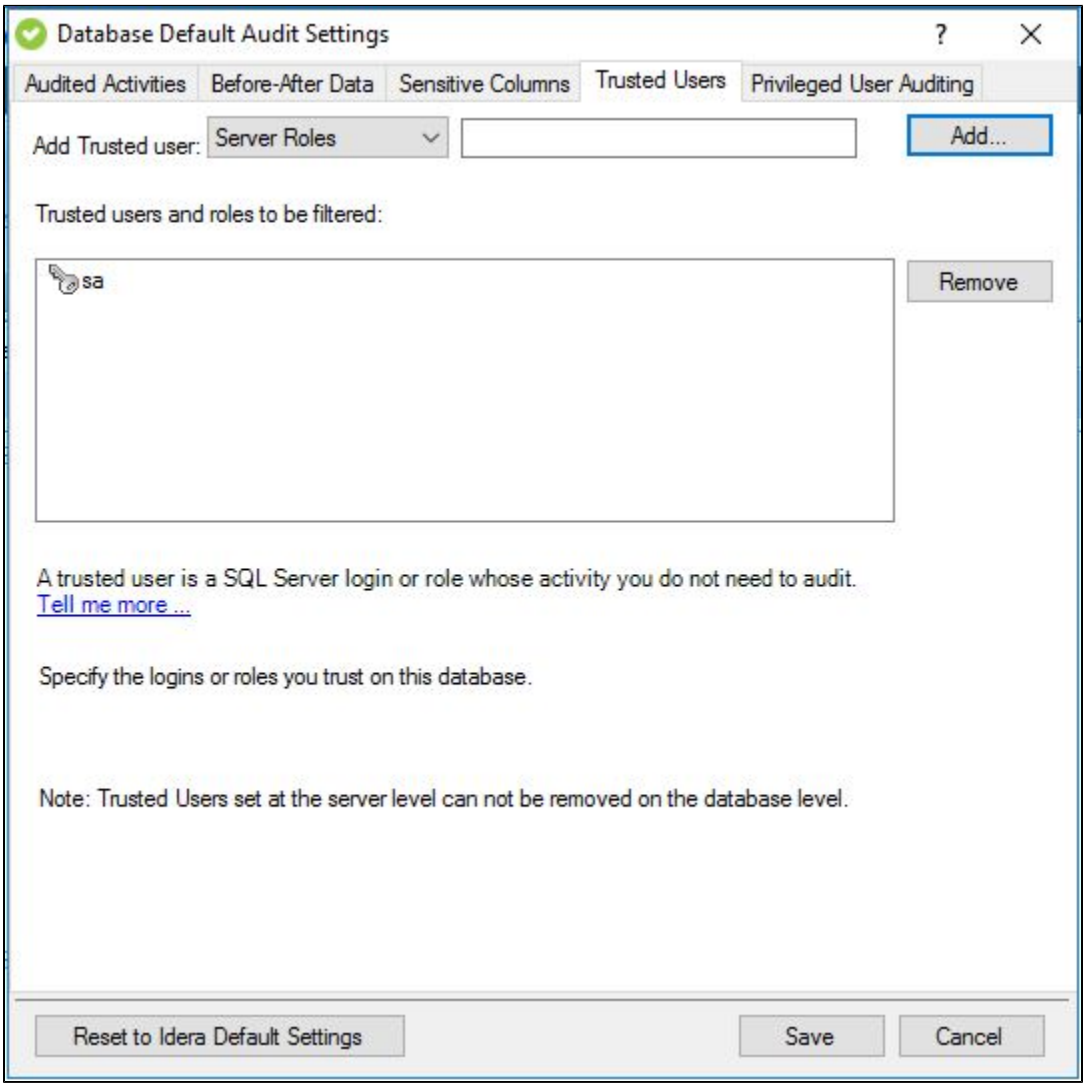


Trusted Users tab

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

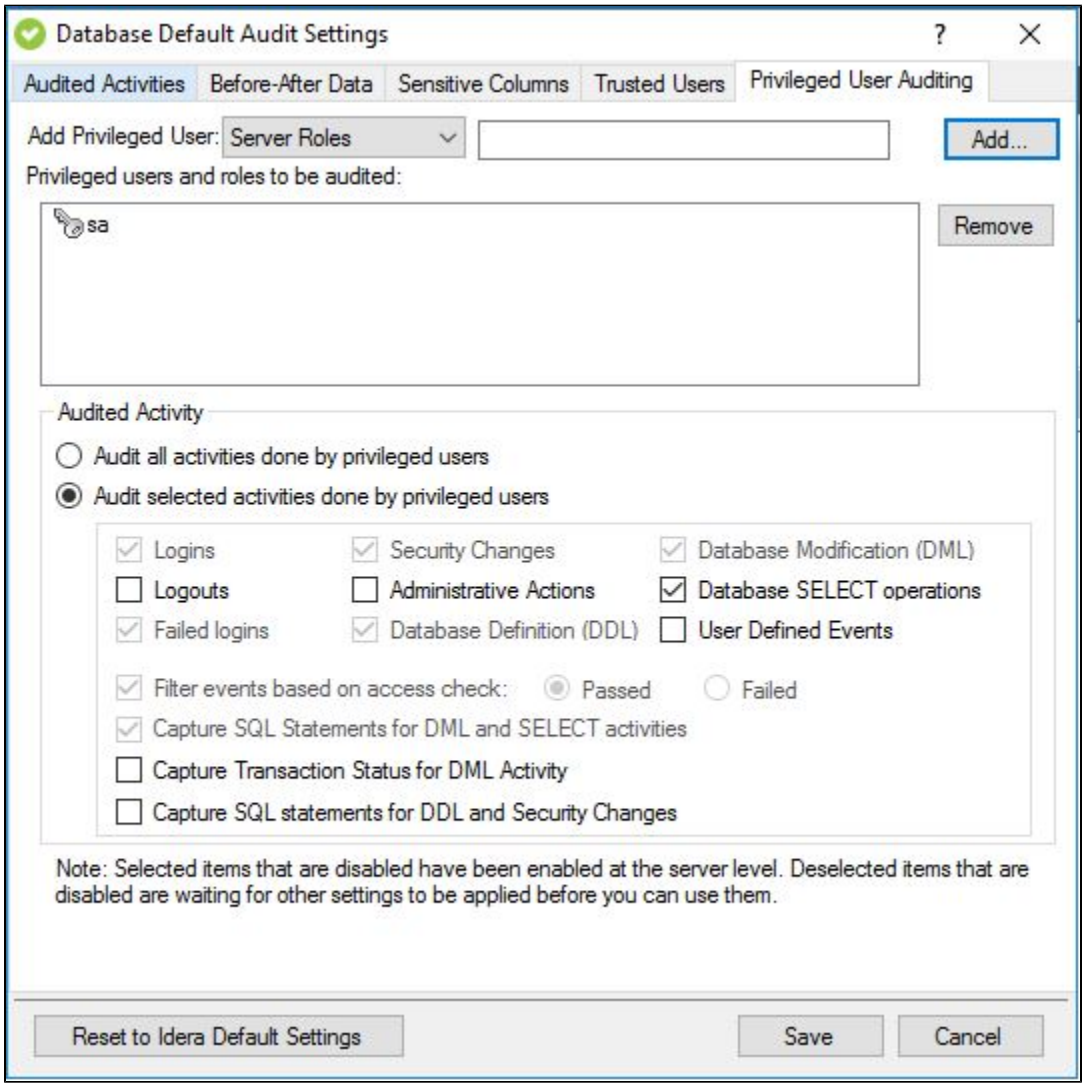
Allows you to designate a previously trusted user or SQL Server role as non-trusted. When a login or role becomes non-trusted, SQL Compliance Manager begins auditing database-level activity generated by this login or role, based on your current audit settings.

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.