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 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.

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.

If you are auditing privileged user activity and the trusted user is also a privileged user, SQL CM 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.

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 SQLcompliance 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 CM begins auditing database-level activity generated by this login or role, based on your current audit settings.