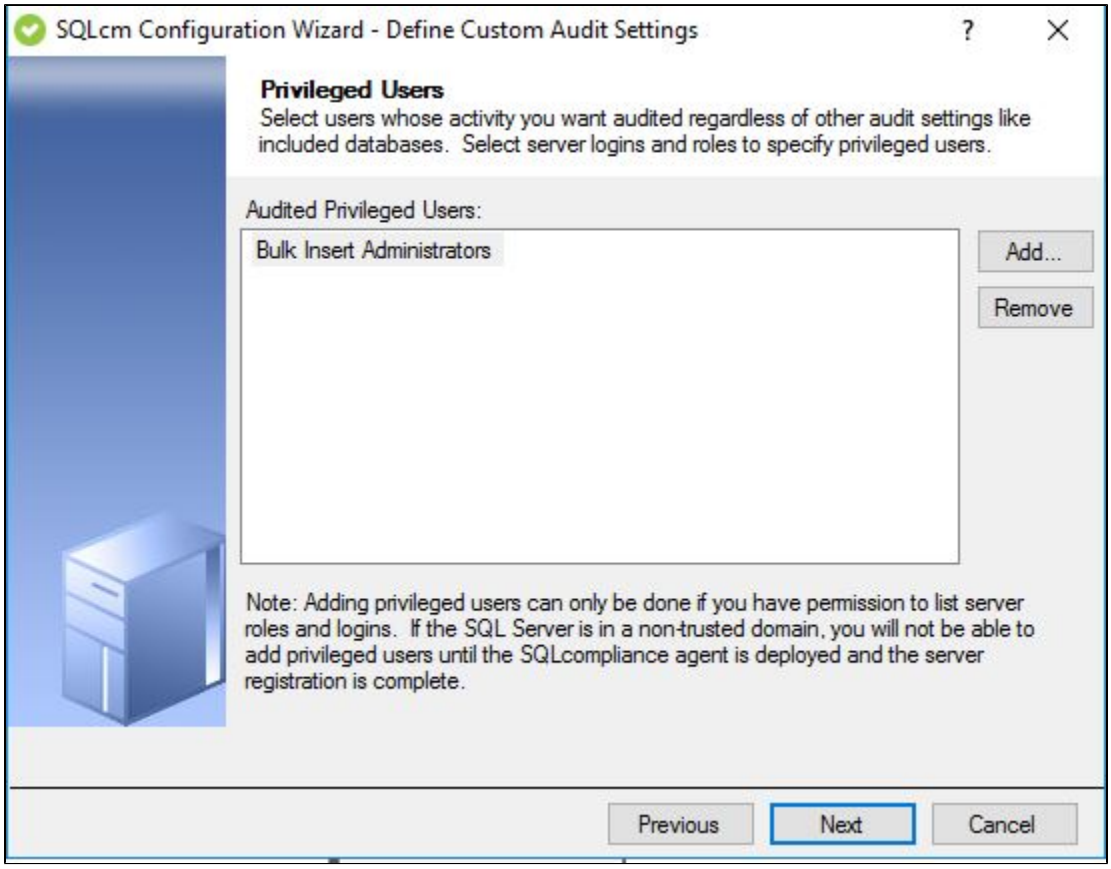
Configuration wizard Apply Regulation - Privileged Users window

The Privileged Users window of the Configuration wizard allows you to select which privileged users you want to audit using IDERA SQL Compliance Manager. You can audit individual SQL Server logins with privileged access as well as logins that belong to specific server roles.

To successfully configure privileged user audit settings, the Management Console must have trusted access to the physical computer hosting the target SQL Server instance.

If you are auditing a virtual SQL Server, configure privileged user audit settings after you have deployed the SQL Compliance Manager Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQL Compliance Manager Agent. For more information about installing and configuring the SQL Compliance Manager Agent for a virtual SQL Server, see Audit a virtual SQL Server instance.

If you are auditing a SQL Server instance running in a non-trusted domain or workgroup, configure privileged user audit settings after you have deployed the SQL Compliance Manager Agent to the computer hosting the instance.



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 server role.

Remove

Allows you to remove the selected SQL Server login or server role from the list of audited privileged users. ***If you remove the login or role***, the SQL Compliance Manager Agent will continue collecting events recorded for that login or the role members when these events belong to an audited event category. For example, if you are auditing DML events, any DML event initiated by a privileged user will be included in your audit trail.