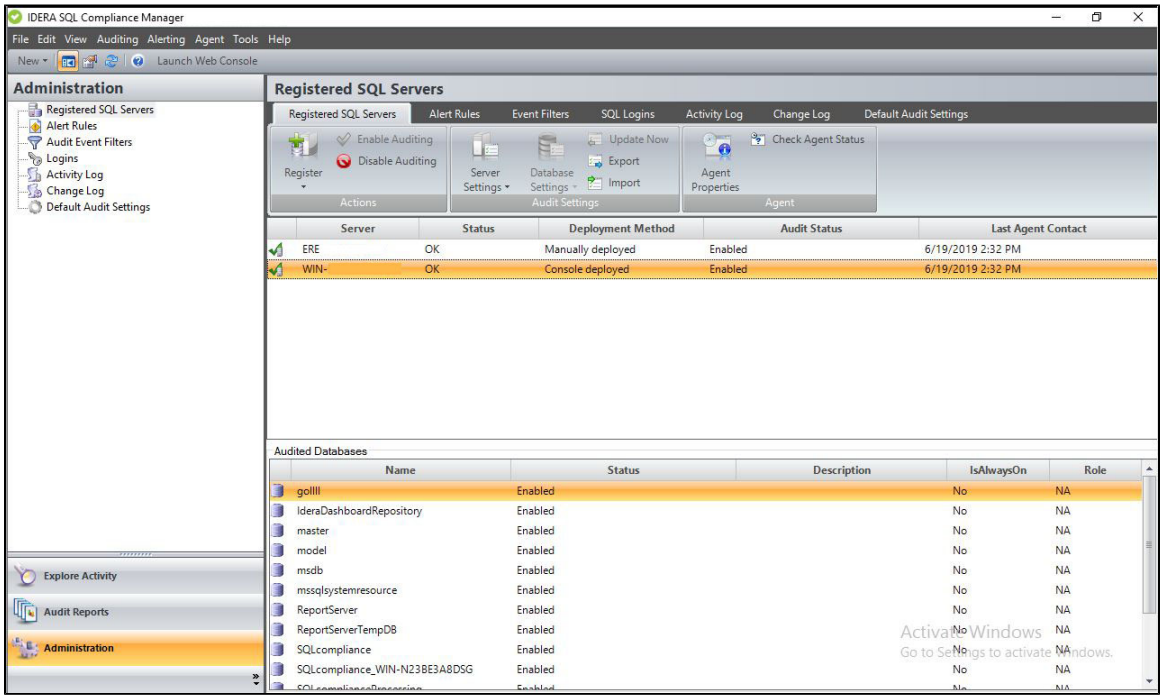
Registered SQL Servers tab

The Registered SQL Servers tab lists the SQL Server instances that are registered for IDERA SQL Compliance Manager to audit. This list includes the following types of registered servers:

- SQL Server instances running in trusted domains
- SQL Server instances running in non-trusted domains or workgroups
- Virtual SQL Servers hosted by Microsoft failover clusters (Microsoft Cluster Services)

Registering a SQL Server instance allows you to audit events at the server and database levels. You can configure audit settings for each registered instance and hosted database.

This tab lists the registered SQL Server instances you have audited. Auditing allows you to collect specific events from the SQL Server trace. This list contains SQL Servers you are currently auditing. ***If you disabled auditing on a SQL Server instance***, this window continues to list the server until you remove the server.



Available actions

Register New Server

Allows you to register an additional SQL Server instance with SQL Compliance Manager. For more information, see Register a SQL Server.

Register New Database

Allows you to enable auditing and configure audit settings for a database on the selected SQL Server instance. To manage settings for a database you are currently auditing, use the Audited Database Properties window. For more information, see Add Audited Databases.

Enable Auditing

Allows you to enable auditing on the selected SQL Server instance. When you enable auditing, the SQL Compliance Manager Agent begins collecting events on the selected SQL Server instance, and sends the SQL trace files to the Collection Server. For more information, see Enable auditing on a SQL Server.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQL Compliance Manager Agent stops collecting new event data, and stops the corresponding SQL trace. You can continue to view and report on previously audited events or archived events. For more information, see Disable auditing on a SQL Server.

Server Settings for Audited Server Activities

Allows you to view and modify audit settings for the selected SQL Server instance. For more information, see Registered SQL Server Properties.

Server Settings for Privileged Users

Allows you to view and modify which privileged users are audited on the selected SQL Server instance. For more information, see Privileged User Auditing.

Database Settings for Audited Database Activities

Allows you to view and modify audit settings for the selected database. This action is available when you select a database from the **Audited Databases** list. For more information, see Audited Database Properties.

Database Settings for Trusted Users

Allows you to view and modify which users are considered trusted users on the selected database. Trusted users are not audited. For more information, see Audited Database Properties window - Trusted Users tab.

Update Now

Allows you to send your audit setting changes to the SQL Compliance Manager Agent immediately. Typically, the Collection Server sends audit setting updates at each heartbeat communication from the SQL Compliance Manager Agent. By default, a heartbeat occurs every five minutes. To view the SQL Compliance Manager Agent heartbeat details, use the General tab on the SQL Compliance Manager Agent Properties window.

Import

Allows you to import audit settings previously exported from another SQL Server instance or database. For more information, see Import your audit settings.

Export

Allows you to export audit settings configured for this SQL Server instance to an XML file. You can later use this file to import audit settings across multiple SQL Server instances or databases, ensuring consistent alerting on activity throughout your environment. For more information, see Export your audit settings.

Collect Audit Data Now

Allows you to force the SQL Compliance Manager Agent to send trace files to the Collection Server for processing. Typically, the SQL Compliance Manager Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

Agent Properties

Allows you to view and modify settings for the SQL Compliance Manager Agent that is auditing the selected SQL Server instance. For more information, see SQL Compliance Manager Agent Properties.

Check Agent Status

Allows you to check the status of the SQL Compliance Manager Agent on the selected SQL Server instance, such as whether or not the agent is active. For more information, see Check the SQL Compliance Manager Agent status.

Deploy Agent

Allows you to deploy the SQL Compliance Manager Agent to one or more registered SQL Server instances. Deploying the agent installs the SQL Compliance Manager Agent Service on the target instance, and allows you to begin auditing events. For more information, see Deploy SQL Compliance Manager Agent wizard.

Upgrade Agent

Allows you to upgrade the SQL Compliance Manager Agent on the selected SQL Server instance to the current version. This option is available if the agent was remotely deployed through the Management Console. To upgrade an agent that was manually deployed, run setup.exe from the SQL compliance manager installation kit on the target SQL Server computer. For more information, see Upgrade your deployed SQL Compliance Agents.

Change Agent Trace Directory

Allows you to specify a different trace directory for the SQL Compliance Manager Agent. The agent uses the specified folder to store trace files before sending these files to the Collection Server for processing.

Refresh

Allows you to update the Registered SQL Servers list with current information.

Remove

Allows you to unregister the selected SQL Server instance. When you remove a SQL Server instance, SQL Compliance Manager disables all auditing at the server and database levels on the SQL Server instance. ***If the selected instance is the last instance to be audited on this SQL Server***, SQL Compliance Manager also uninstalls the SQL Compliance Manager Agent. ***If you manually deployed the SQL Compliance Manager Agent***, you must manually uninstall it from the SQL Server computer.

If there are any backlogged audit trace files that you need to process for the instance you are considering to decommission, make sure to disable auditing and decommissioning your server only after processing these backlogged audit trace files. For additional information on how to process backlogged trace files, please contact Idera Support.

Available columns

SQL Server

Provides the name of the SQL Server instance, using the format *SQLServerName\InstanceName*.

Status

Indicates whether SQL Compliance Manager detected an auditing or configuration issue. For example, if the selected SQL Server instance is unavailable, SQL Compliance Manager displays an error.

If a system alert is triggered, the **Status** column displays the alert type. System alerts notify you when the health of your SQL Compliance Manager deployment may be compromised. For more information, see the Activity Log tab.

Deployment Method

Indicates the agent deployment method for the selected SQL Server.

The values in this column can be: manually deployed, console deployed, and silent installer script.

Audit Status

Indicates whether auditing is enabled on the selected SQL Server instance. When auditing is disabled, the SQL trace is stopped and the SQL Compliance Manager Agent no longer collects events.

If a system alert is triggered, the Audit Status column instructs you to view the Activity Log to determine which event triggered this alert.

Last Agent Contact

Provides the date and time when the SQL Compliance Manager Agent last received audit setting updates from the Collection Server (also called a heartbeat). To view the SQL Compliance Manager Agent heartbeat details, use the General tab on the SQL Compliance Manager Agent Properties window.