Register your SQL Servers

Registering a SQL Server instance allows you to audit this instance and the associated databases. For each database you want to audit, register the corresponding SQL Server instance. When you register the instance, you can also deploy the SQL Compliance Manager Agent to begin auditing SQL events on this instance.

Use the Console to register your SQL Servers

To register your SQL Server instance:

1. Ensure the SQL Server instance you want to register meets the hardware and software requirements.
2. Decide which SQL Server events you want to audit on this instance.
3. Start the Management Console, and then click **New > Registered SQL Server**.
4. Specify or browse to the SQL Server instance you want to register with SQL Compliance Manager, and then click **Next**. You can also specify the description SQL Compliance Manager uses when listing this instance in the Management Console.
5. ***If the SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server***, select the checkbox. Click **Next**.
6. Indicate whether you want to deploy the SQL Compliance Manager Agent now or later, and then click **Next**. You can also choose to deploy the SQL Compliance Manager Agent manually, allowing you to install the agent at the physical computer that is hosting the registered SQL Server instance.

   > ***If you are auditing a virtual SQL Server or a SQL Server instance running in a non-trusted domain or workgroup*** , you must manually deploy the SQLcompliance Agent to the computer hosting the instance. For more information, see Deploy the SQL Compliance Manager Agent manually.

7. ***If you chose to deploy the SQLcompliance Agent now***, specify the appropriate service account credentials for the agent, and then click **Next**. For more information, see Permissions requirements.
8. ***If you chose to deploy the SQLcompliance Agent now***, indicate whether you want the SQL Compliance Manager Agent to use the default trace directory, and then click **Next**. By default, the trace directory path is:
   `C:\Program Files\Idera\SQLcompliance\AgentTraceFiles`
   If you designate a different directory path, ensure the SQL Compliance Manager Agent Service account has read and write privileges on the specified folder.
9. Select the server databases you want to audit, and then click **Next**. ***If you do not want to audit any databases***, clear the **Audit Databases** check box.
10. Select the collection level of server activities you want to audit, and then click **Next**.
11. ***If you chose to create a custom audit collection***, select the server activities you want to audit, and then click **Next**. You can also indicate whether you want to audit successful or failed access checks.
12. ***If you chose to create a custom audit collection***, specify which privileged users you want to audit, and then click **Next**. ***If you are auditing a virtual SQL Server or 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.
13. ***If you chose to create a custom audit collection***, select the database activities you want to audit, and then click **Next**. You can also indicate whether you want to audit successful or failed access checks, capture SQL statements for DML and SELECT activity, or capture the transaction status for DML activity.
14. ***If you chose to create a custom audit collection***, specify which privileged users you want to audit, and then click **Next**.
15. Specify whether you want to grant the assigned SQL logins read access to events audited on this SQL Server instance, and then **Next**. For more information, see How Console security works.
16. Click **Finish**.

Use the CLI to register a SQL Server instance

You can use the command line interface to register a new SQL Server instance and apply audit settings. The audit settings can be configured using the Typical auditing settings or an audit template (audit settings you exported to an XML file).

Keep in mind the following requirements and limitations:

- This process requires manually deploying the SQL Compliance Manager Agent to this instance.
- You cannot apply the built-in HIPAA or PCI regulation guidelines at the server level using the CLI.
- The `register` command supports case-sensitive named instances. Ensure you are using the appropriate case when you cite the instance name.
- The `registerinstance` command does not support registering a virtual SQL Server instance hosted on a Windows cluster.

SQL Compliance Manager includes a sample instance audit settings template (Sample_Server_AuditSettings.xml) for your convenience. Use this sample template to familiarize yourself with how specific audit settings are defined. By default, the sample template is located under `C:\Program Files\Idera\SQLcompliance`.

To register an instance and apply the Typical (default) audit settings:

1. Use the SQL Compliance Manager setup program to the target instance.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance`.

To register an instance and apply a FERPA regulation guideline:

The FERPA regulation guideline is provided as an XML template (`FERPA_Server_Regulation_Guideline.xml`) stored in the SQL Compliance Manager installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the FERPA template reflects the directory you chose during installation.

1. Use the SQL Compliance Manager setup program to manually deploy the SQL Compliance Manager Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "FERPA regulation guideline file path"`.

To register an instance and apply a SOX regulation guideline:

The SOX regulation guideline is provided as an XML template (`SOX_Server_Regulation_Guideline.xml`) stored in the SQL Compliance Manager installation directory (`C:\Program Files\Idera\SQLcompliance`). Ensure the path you cite for the SOX template reflects the directory you chose during installation.

1. Use the SQL Compliance Manager setup program to manually deploy the SQL Compliance Manager Agent to the instance that hosts the target database.
2. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "SOX regulation guideline file path"`.

To register an instance and apply a custom audit template:

1. Determine which currently audited SQL Server instance has the audit settings you want to apply to the new instance.
2. Export your audit settings from the source instance.
3. Use the SQL Compliance Manager setup program to manually deploy the SQL Compliance Manager Agent to the target instance.
4. In Windows Command Prompt, use the following syntax: `SQLcmCmd [-host CollectionServer] [-port number] registerinstance instance -config "exported audit settings file path"`.

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.