

Enable auditing on a database

Enabling auditing on the database allows you to capture SQL events at the database level. You can enable database-level auditing when you register the SQL Server instance. For more information, see [Register your SQL Servers](#).

When you enable auditing on a database, you can control the [Audit collection levels](#) per each database, choosing whether to apply the built-in default audit settings, [enforce a regulatory guideline](#), or define custom audit settings.

 After you enable auditing on your databases, set up the audited database properties to enable more advanced auditing, such as [Sensitive Columns](#) and [Before-After Data](#) in tables.

If you disable auditing for any reason, you can easily re-enable database-level auditing. On the **Explore Activity** tree, expand the SQL Server instance on which the database resides. Right-click the name of the database on which you want to enable auditing, and then select **Enable Auditing**. This action enables auditing at the server and database levels.

Use the SQL Compliance Manager Configuration wizard to enable auditing on a database

You can use the SQL Compliance Manager Configuration wizard to add a database and apply one of the following audit settings:

To enable database auditing through the Configuration wizard:

1. In the **Explore Activity** tree, select the SQL Server instance that hosts the new database.
2. Select **Audited Database** from the **New** drop-down.
3. Select the user databases you want to audit, and then click **Next**.
4. Select which audit collection level you want to use, and then click **Next**.
5. **If you chose to use the Custom audit collection level**, select the appropriate audit settings for these databases, and then click **Next**. SQL Compliance Manager audits only the activities and results you select. For information, see [Database-level audit settings](#).
6. **If you chose to use the Custom audit collection level and you are auditing DML and SELECT events**, select the objects SQL Compliance Manager should audit for these events, and then click **Next**.
7. **If you chose to use the Custom audit collection level**, select any trusted users you do not want to audit, and then click **Next**.
 - Trusted users are database users, SQL Server logins, or members of SQL Server roles that you trust to read, update, or manage a particular audited database. SQL Compliance Manager does not audit trusted users. Trusted users are designated on the Add Trusted Users window of the New Audited Database wizard.
 - **If you are auditing privileged user activity and the trusted user is also a privileged user**, SQL Compliance Manager continues 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.
8. Click **Finish**.

Use the import audit settings feature to apply audit settings to a database

You can use the [Import your audit settings](#) feature to apply an audit template you [previously exported](#) from an audited database. To successfully apply the template, first add the database to SQL Compliance Manager.

Use the CLI to enable auditing on a database

You can use the command line interface to enable auditing on a new database and apply audit settings. The audit settings can be configured using a [specific regulation](#) 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 the instance that hosts this database.
- The auditdatabase command does not support enabling auditing of a database that belongs to a virtual SQL Server instance hosted on a Windows cluster.
- The auditdatabase command supports case-sensitive named instances. Ensure you are using the appropriate case when you cite the instance and database names.
- The CLI does not support configuring Before-After data auditing.
- You can apply either a built-in regulation guideline or an XML template file.

SQL Compliance Manager includes sample database audit settings templates (Sample_Database_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 enable database auditing and apply the Typical (default) audit settings:

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] auditdatabase instance database`.

To enable database auditing and apply a HIPAA or PCI regulation guideline:

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] auditdatabase instance database -Regulation {PCI | HIPAA | PCI, HIPAA}`.

To enable database auditing and apply a FERPA regulation guideline:

 The FERPA regulation guideline is provided as an XML templates (FERPA_Database_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] auditdatabase instance database -config "FERPA regulation guideline file path"`.

Use the CLI to enable auditing on a database

To enable database auditing and apply a SOX regulation guideline:

 The SOX regulation guidelines is provided as an XML template (SOX_Database_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] auditdatabase instance database -config "SOX regulation guideline file path"`.

To enable database auditing and apply a custom audit template:

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