

Adding SQL Server instances

In order to manage an instance, access its details, and add it to your monitored environment, you need to register it with IDERA SQL Compliance Manager.

You can find the **Add** or **Add SQL Server Instance** option on the following views:

- **Instances** - The **Add** button is located in the action items bar.
- **Administration** - Located in the Instances section.

Below you can see the tabs and sections where you can find **Add** or **Add SQL Server Instance**.

The screenshot shows the IDERA SQL Compliance Manager interface with the 'INSTANCES' tab selected. The 'Audited Instances' table lists three instances: CMWIN8X6..., QA-LF-W2K..., and QA-ZB-WIN... The 'Add' button in the action bar is highlighted with a red box.

Instance N...	Status Text	Number Of...	SQL Serve...	Audit Status	Last Agent...	Options
CMWIN8X6...	OK	4	Microsoft S...	Enabled	May 11 201...	⚙
QA-LF-W2K...	No Contact ...	10	Microsoft S...	Enabled	May 05 201...	⚙
QA-ZB-WIN...	SQL Trace E...	8	Microsoft S...	Enabled	May 05 201...	⚙

The screenshot shows the IDERA SQL Compliance Manager interface with the 'ADMINISTRATION' tab selected. The 'Add SQL Server Instance' link is highlighted with a red box.

Administration

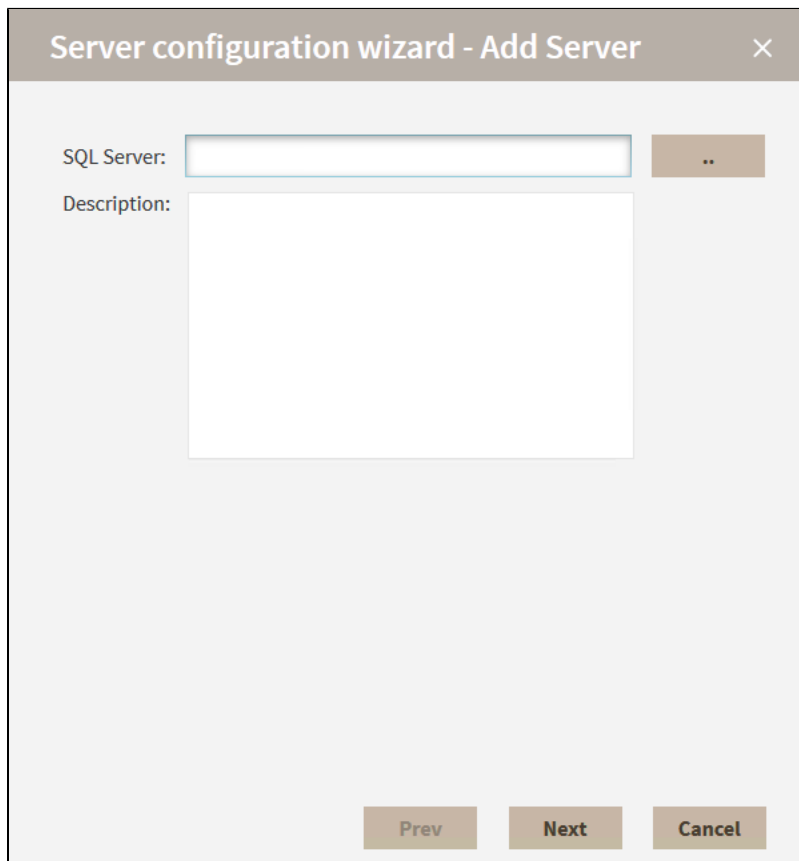
Users
Give users permission to use SQL Compliance Manager. Create, edit and delete users and subscribe to alerts using the Manage Users action.
[Manage Users](#)

Licensing
A license is required to access SQL Compliance Manager features. View license status and add a license key using the Manage License action.
[Manage License](#)

Instances
SQL Compliance Manager monitors SQL Server instances and their host computers. Add instances to be monitored using the Add SQL Server Instance action.
[Add SQL Server Instance](#)
[Import SQL servers](#)
[Manage SQL Servers Instances](#)

Configuration
Allows configuration of Web Console.
[Web Console Refresh Rate](#)

The Add Server window of the Server Configuration wizard allows you to specify the SQL Server instance you want to register with IDERA SQL Compliance Manager. Once you register an instance, you can begin auditing database activity on that server.



Server configuration wizard - Add Server

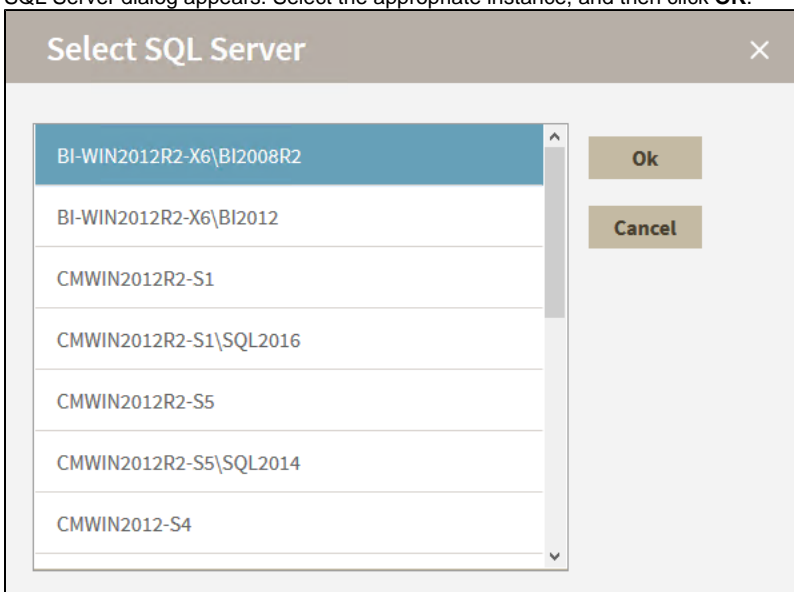
SQL Server: ..

Description:

Prev Next Cancel

To add an instance:

1. In the Add Server page of the Server Configuration wizard, type the name of the target SQL Server instance you want to register in the **SQL Server** field, and then click **Next**. To browse through the instances in your environment, click the available search button. The Select SQL Server dialog appears. Select the appropriate instance, and then click **OK**.



Select SQL Server

BI-WIN2012R2-X6\BI2008R2
BI-WIN2012R2-X6\BI2012
CMWIN2012R2-S1
CMWIN2012R2-S1\SQL2016
CMWIN2012R2-S5
CMWIN2012R2-S5\SQL2014
CMWIN2012-S4

Ok Cancel

2. In the Cluster Server window, check **This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server** if the instance is part of a clustered environment, and then click **Next**. Leave this box clear if the instance is not in a clustered environment.

Server configuration wizard - Add Server

☐ This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server.

Prev Next Cancel

3. In the SQLcompliance Agent Deployment window, select whether you want to deploy the SQLcompliance Agent now or later, or if you want to manually install the Agent.
- **Deploy Now.** Installs the SQLcompliance Agent when you complete the wizard. You must have a connection between the SQL Server that you want to audit and the Management Console.
 - **Deploy Later.** Does not install the SQLcompliance Agent. Select this option when you plan to install the SQLcompliance Agent later using the Management Console, such as installing during off-hours.
 - **Manually Deploy.** Does not install the SQLcompliance Agent. Select this option when you want to manually install the agent directly on the physical computer hosting the SQL Server instance. Note that this option is required for virtual SQL Server instances and instances located across a domain trust boundary.

If you are auditing a virtual SQL Server, you must manually deploy the SQLcompliance Agent to each cluster node hosting the server. Use the Cluster Configuration Console to deploy and configure the SQLcompliance Agent. For more information about installing and configuring the SQLcompliance Agent for a virtual SQL Server, see [Deploy the SQL Compliance Agent to cluster nodes](#).

If you are auditing a SQL Server instance hosted by a computer that belongs to a non-trusted domain or a workgroup, you must manually deploy the SQLcompliance Agent to the host computer using the SQL Compliance Manager setup program.

The screenshot shows the 'Server configuration wizard - Add Server' dialog box. It has a title bar with a close button (X). The main area contains three radio button options for deployment:

- ☒ **Deploy Now** - Installs the SQLcompliance agent at this time. This option requires that a connection be established between the SQL Server to be audited and the Management Console.
- ☐ **Deploy Later** - Indicates that you will install the SQLcompliance Agent using the Management Console at a later time such as during off-hours.
- ☐ **Manually Deploy** - Indicates that you will manually install the agent at the physical computer that hosts the SQL Server instance. Note that this option is required for virtual SQL Server and SQL Servers located across a domain trust boundary.

At the bottom, there are three buttons: 'Prev', 'Next', and 'Cancel'.

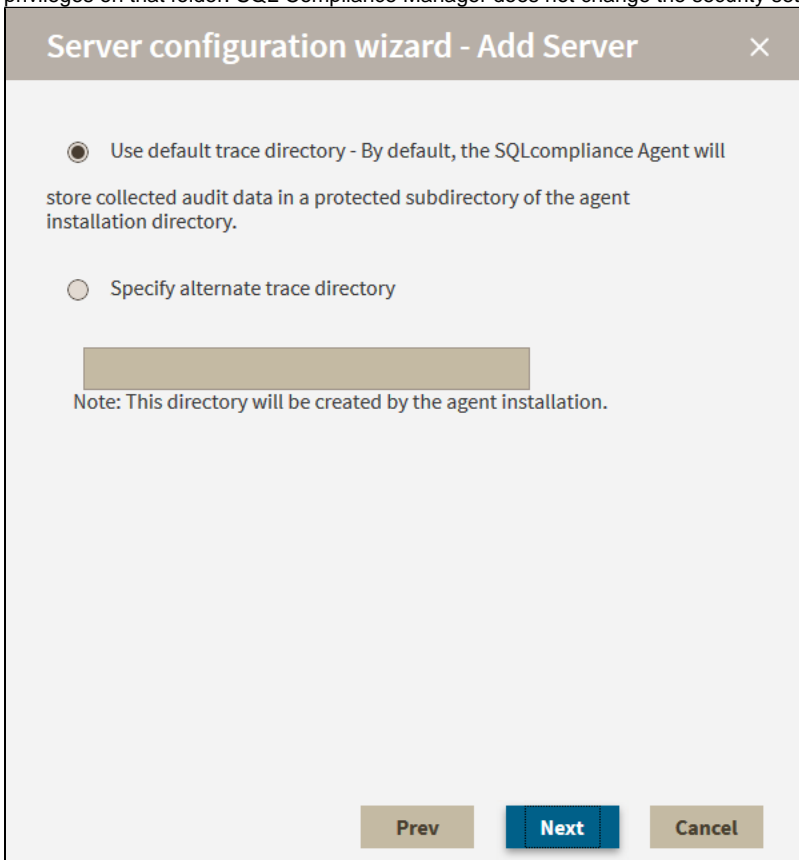
4. Click **Next**.
5. In the SQLcompliance Agent Service Account window, type the service account name and password, confirm the password, and then click **Next**. The SQLcompliance Agent Service uses this account to stop and start SQL Server traces, execute stored procedures, manage trace files, and communicate with the Collection Server. Ensure you specify a valid Windows account that has SQL Server System Administrator privileges on the target SQL Server instance as well as read and write access to the specified trace directory.

The screenshot shows the 'Server configuration wizard - Add Server' dialog box, Step 2: SQLcompliance Agent Service Account. It has a title bar with a close button (X). The main area contains a section titled 'SQLcompliance Agent Service Account' with three input fields:

- Login account
- Password
- Confirm password

At the bottom, there are three buttons: 'Prev', 'Next', and 'Cancel'. The 'Next' button is highlighted in blue.

- In the SQLcompliance Agent Trace Directory window, choose whether you want to use the default path for the agent trace directory, and then click **Next**. **If you specify a different directory path**, ensure the SQLcompliance Agent Service account has read and write privileges on that folder. SQL Compliance Manager does not change the security settings on existing folders.



Server configuration wizard - Add Server [X]

☒ Use default trace directory - By default, the SQLcompliance Agent will store collected audit data in a protected subdirectory of the agent installation directory.

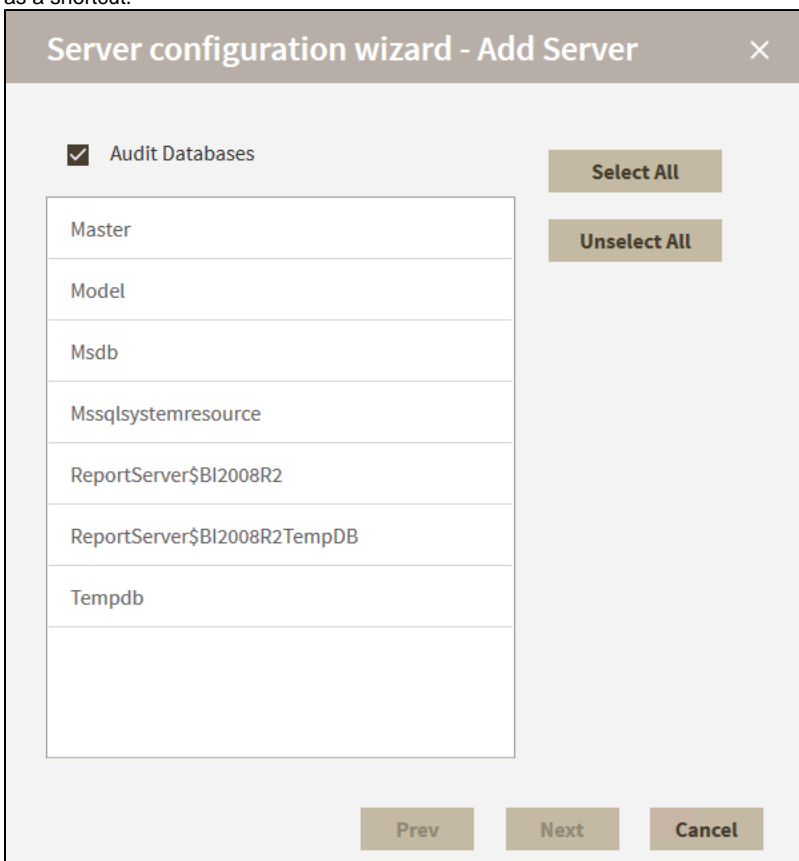
☐ Specify alternate trace directory

[Text Box]

Note: This directory will be created by the agent installation.

[Prev] [Next] [Cancel]

- In the Database Selection window, select the database(s) you want to be audited, and then click **Next**. Note that you can click **Select All** as a shortcut.



Server configuration wizard - Add Server [X]

☒ Audit Databases

[Select All] [Unselect All]

Master
Model
Msdb
Mssqlsystemresource
ReportServer\$BI2008R2
ReportServer\$BI2008R2TempDB
Tempdb

[Prev] [Next] [Cancel]

8. In the Server Audit Settings window, specify which types of SQL Server events you want to audit on the selected instance, and then click **Next**. Based on your selections, SQL Compliance Manager collects and processes the corresponding SQL Server events. You can choose to audit event categories and user defined events. An event category includes related SQL Server events that occur at the server level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

- **Default.**
- **Custom.**
- **Regulation.**

Server configuration wizard - Add Server ✕

Audit Collection Level

☒ **Default** - Audits events and activities most commonly required by auditors This collection level meets most auditing needs

☐ **Custom** - Allows you to specify specific audit settings. This collection level is recommended for advanced users only. Before selecting specific audit settings, review the events gathered by the Custom collection level and review the help to better understand your choices

☐ **Regulation** - Configures your audit settings to collect the event data required by specific regulatory guidelines, such as PCI or HIPAA

[Tell me more](#)

Prev Next Cancel

9. The Permissions Check window of the Configuration wizard displays the results of a check of the permissions required by IDERA SQL Compliance Manager on the SQL Server instance you want to monitor.

If the check fails, review the issue, make the required change to the target SQL Server instance, and then click **Re-check**. Once the check is complete, click **Next** to continue.

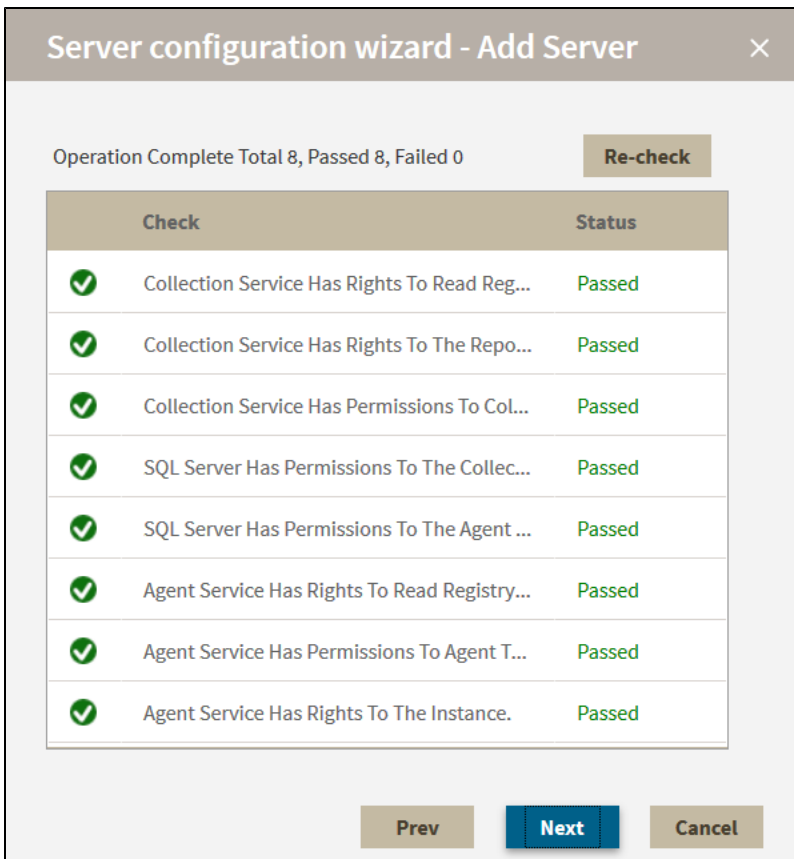
Required permissions include:

- Collection Service must have rights to the Repository databases
- Collection Service must have rights to read the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance`
- Collection Service must have permissions to the collection trace directory
- Agent Service must have permissions to the agent trace directory
- Agent Service must have rights to read the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance`
- Agent Service must have rights to the SQL Server instance
- SQL Server must have permissions to the agent trace directory
- SQL Server must have permissions to the collection trace directory



You can make changes to the registry at `HKEY_LOCAL_MACHINE\Software\Idera\SQLcompliance` to update permissions for your services. for more information about the registry key, see [Manage the registry key](#).

Re-check allows you to re-check the required permissions after making an update to the target SQL Server instance in case the preliminary check fails.



10. In the Summary window, review the provided summary, and then click **Finish**. When you complete this wizard, SQL Compliance Manager enables auditing on the selected databases. The Collection Server uses the settings you specified to process the raw audit data (SQL Server events) collected from the SQL Server instance.

If you want to change a setting now, click **Prev** to return to the appropriate window. You can also change audit settings later using the Audited Database Properties window.

Server configuration wizard - Add Server

Audit Level: Default

Server: BI-WIN2012R2-X6\BI2008R2

Databases:

Master

Model

MsdB

Mssqlsystemresource

ReportServer\$BI2008R2

ReportServer\$BI2008R2TempDB

Tempdb

Prev

Finish

Cancel

Once complete, the newly-added SQL Server instance appears in the Audited Instances list.

HOME

INSTANCES

ALERTS

AUDIT EVENT FILTERS

LOGS

AUDIT REPORTS

ADMINISTRATION

Filtering

Status

OK

Error

Instance name

Status Text

Number of Audited DBs

SQL Server version

Audit Status

Last agent contact

SimpsonsAdministrator

Administration

Help

Audited Instances

Add

Remove

Export

Edit

	Instance N...	Status Text	Number Of...	SQL Serve...	Audit Status	Last Agent...	Options
<input type="checkbox"/>	BI-WIN2012...	OK	7	Microsoft S...	Enabled	May 11 201...	<div></div>
<input type="checkbox"/>	CMWIN8X6...	OK	4	Microsoft S...	Enabled	May 11 201...	<div></div>
<input type="checkbox"/>	QA-LF-W2K...	No Contact ...	10	Microsoft S...	Enabled	May 05 201...	<div></div>
<input type="checkbox"/>	QA-ZB-WIN...	SQL Trace E...	8	Microsoft S...	Enabled	May 05 201...	<div></div>

4 Total Items

50 Items per page

Showing page 1 / 1

SQL Compliance Manager monitor, audit and alert on SQL user activity and data changes.

IDERA | Products | Purchase | Support | Community | Resources | About Us | Legal

8