

# View alerts and alert rules

The IDERA SQL Compliance Manager Alerts view allows you to view the current alerts and create and manager alert rules throughout your environment. An alert rule is a set of criteria that determines when an alert should be generated as the Collection Server processes SQL Server events collected from your audited instances. Use alert rules to detect events that occur on specific databases, users, or instances.

Available actions include:

## Page through alerts and alert rules

Allows you to page through the list of alerts and rules. Use the previous and next arrows to navigate from page to page, up and down the list.

## Filtering

Allows you to filter the listed alerts and rules by rule, rule type, server name, alert level, user email address, event log, and SNMP traps. Filtering includes a **Save View** feature that lets you select all of your filtering options, and then save the settings for future use. Click **Load View** to select a previously-saved view for use.

## View By

Allows you to select whether Alerts or Alert Rules appear in this view.

## Filtered By

Allows you to select the type of Alerts displayed in this view. You can view all Alerts, only your Event Alerts, only Data Alerts, or only Status Alerts based on this selection.

## Add New Rule

*(Only available on the Alert Rules view)* Allows you to create a new alert rule using the New Alert Rule wizard. IDERA SQL Compliance Manager stores this alert rule in the Repository.

## Import / Export

Export Alert Rules created for the associated SQL Server instance to an XML file. You can later use the exported file to import Alert Rules across multiple SQL Server instances, ensuring consistent filtering of specific events throughout your environment. Allows you to export Alert Rules created for the associated SQL Server instance to an XML file. You can later use this file to import Alert Rules across multiple SQL Server instances, ensuring consistent filtering of specific events throughout your environment.

## Enable / Disable Alert Rule

Allows you to enable or disable the selected rule. When an alert rule is enabled, SQL Compliance Manager processes audited events using the selected criteria in this rule. ***If an event matches the alert criteria and an alert action is configured***, SQL Compliance Manager writes an alert message to the application event log or email it to the specified addresses. Alert messages are also available using the Alerts tab. When an alert rule is disabled, you temporarily stop using the selected rule. SQL Compliance Manager no longer uses this alert rule when processing events. All alert messages previously generated by this rule will remain available through the Management Console and the application event log, if event log notification was configured. To reinstate this alert, enable the alert rule.

## Delete

Allows you to permanently delete the selected Alert Rule. This option removes the Alert Rule from the Repository. SQL Compliance Manager will no longer use this Alert Rule when processing events. All previously processed audit data stored in the Repository remains intact.

## Export

Allows you to export the Activity Log and Change Log information to a CSV, PDF, or XML file.

## Refresh

Allows you to update the Alert Rules list with current data.

## Import

Allows you to import Alert Rules previously exported from another SQL Server instance. By default, the imported Alert Rules are disabled.

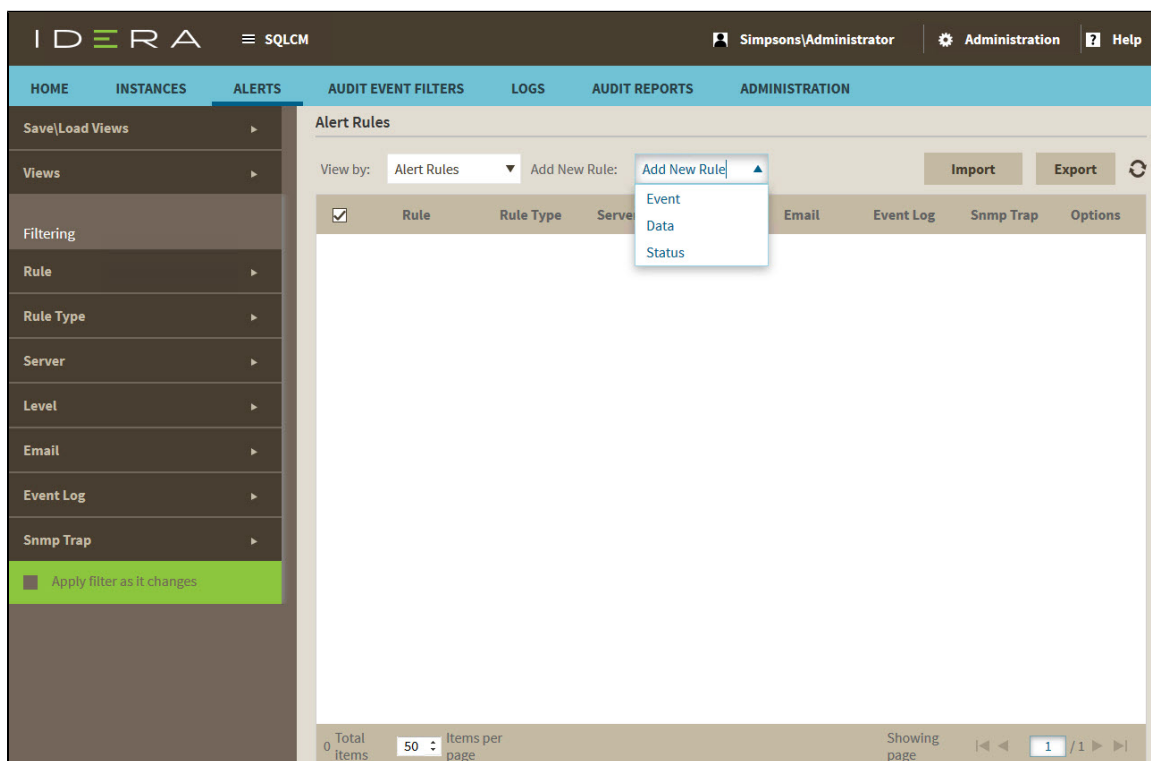
## Edit Alert Rules

Allows you to change an existing alert rule using the New Alert Rule wizard.

## From Existing

Allows you to create a new Alert Rule using a selected rule as a template. This action launches the New Alert Rule wizard, each window populated with event criteria from the selected alert rule. You can change any event criterion to meet the goals of your new Alert Rule. SQL Compliance Manager stores the new Alert Rule in the Repository. The selected Alert Rule remains unchanged.

## Alerts view



## Default columns

### Instance name

Provides the name of the audited SQL Server instance where this event occurred.

### Date

Provides the date when the alert was generated.

### Time

Provides the time when the alert was generated.

### Level

Indicates the type of alert, such as Severe or Low. Use the alert level to help you identify critical issues, sort alerts by severity, and understand the overall health of your environment. You can define the alert using the Edit Alert Rule wizard.

### Source Rule

Provides the name of the alert rule that generated this alert.

### Event

Provides the name of the audited event that triggered this alert.

### Detail

Provides additional information about the alert.

## Event Alerts view

The Event Alerts view, available from the **Filtered By** selection, allows you to view previously generated Event Alerts. An Event Alert is generated when the Collection Server processes a SQL Server event that matches the alert rule criteria. Use Event Alerts to identify and investigate suspicious activity on specific databases, users, or instances.

## Data Alerts view

The Data Alerts view, available from the **Filtered By** selection, allows you to view previously generated Data Alerts. A Data Alert is generated when the Collection Server processes a SQL Server event that matches the alert rule criteria. Use Data Alerts to identify and investigate data manipulation on specific databases, tables, or columns.



The Collection Server generates one alert per SELECT event, even though the query may have accessed multiple audited columns.

## Status Alerts view

The Status Alerts view, available from the **Filtered By** selection, allows you to view previously generated Status Alerts. A Status Alert is generated when the status of the specified product components matches the alert rule criteria. Use Status Alerts to identify and investigate possible issues with IDERA SQL Compliance Manager operations, such as deployed agents that may have stopped running.

## Alert Rules view

## Default columns

### Rule

Provides the name you specified when you created each alert rule. By default, SQL Compliance Manager names each new rule **New Rule**.

### Rule Type

Indicates whether this rule generates an Event Alert or a Status Alert.

### Server

Provides the name of the registered SQL Server instance associated with this alert rule. By default, Event and Status Alerts apply to all registered SQL Server instances. For better focused Event Alerts, you can specify a different target SQL Server using the Edit Alert Rule wizard.

#### Level

Provides the alert level, such as High. Depending on the rule type, you can change the alert level using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

#### Email

Indicates whether the alert rule criteria includes email notification. When email notification is configured, SQL Compliance Manager sends an alert message to the specified addresses. Depending on the rule type, you can set up email notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

#### Event Log

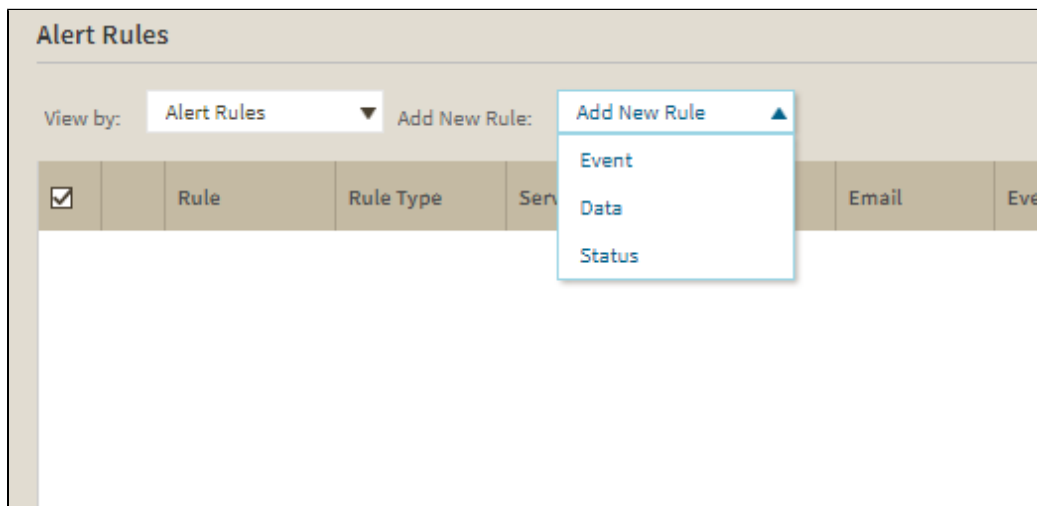
Indicates whether the alert rule criteria includes event log notification. When event log notification is configured, SQL Compliance Manager writes an alert message to the application event log. Depending on the rule type, you can set up event log notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

#### SNMP Trap

Indicates whether the alert rule criteria includes sending SNMP Trap messages to a specified network management console. When SNMP Trap is configured, SQL Compliance Manager sends an alert message to the specified network management console. Depending on the rule type, you can set up SNMP Trap notification using either the Edit Event Alert Rule or Edit Status Alert Rule wizard.

## New Event / Data / Status Alert Rule wizard

When you select to create a new alert rule, IDERA SQL Compliance Manager allows you to select whether you want to create an event alert rule, a data alert rule, or a status alert rule. The **Add New Rule** option allows you to create a new alert using the New Alert Rule wizard. SQL Compliance Manager stores this alert rule in the Repository.



## New Event Alert Rule

The Alerts view allows you to specify on which type of SQL Server event you want to alert.

## SQL Server Event Type window

The SQL Server Event Type tab allows you to specify on which type of SQL Server event you want to alert.

## Available actions

Specify a name

Type a short but descriptive name for the new alert. Remember that this name appears when you are searching for or viewing a list of alerts, so keep that in mind when implementing any sort of naming convention.

### Specify alert level

Select the level of criticality for this alert where:

- Level 4 = Severe
- Level 3 = High
- Level 2 = Medium
- Level 1 = Low

### Select type of event that triggers this alert

Allows you to select the SQL Server event type that should trigger this alert. When the Collection Server processes an audited event that matches the specified event type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

You can also select a specific event or a user defined event. A specific event can be any supported SQL Server event that occurs at the server or database level. A user defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure. Note that additional selections activate when you select **Specific Events**.

## SQL Server Object Type and Additional Event Filters window

The SQL Server Object Type and Additional Event Filters window allows you to specify the type of SQL Server object that should be monitored by this alert rule. Select from the additional event filters to narrow your results. You can generate alerts for objects on currently audited databases and SQL Server instances.

### Available actions

#### Select type of event that triggers this alert

Allows you to specify the SQL Server object type that should trigger this alert. When the Collection Server processes an audited event associated with the specified object type, the alert rule is run to see whether the identified event matches the other alert rule criteria.

By default, the alert rule applies your alert criteria against events on any audited SQL Server instance.

You can specify one or more objects:

Type of Object	You can specify ...
SQL Server instance	<ul style="list-style-type: none"> <li>Any instance</li> <li>A specific instance by name</li> </ul>
Database	<ul style="list-style-type: none"> <li>A specific database by name</li> <li>Any database whose name matches a naming convention or phrase</li> </ul>
Database object name	<ul style="list-style-type: none"> <li>A specific database object by name</li> <li>Any database object whose name matches a naming convention or phrase</li> </ul>
Host name	<ul style="list-style-type: none"> <li>A specific database host by name</li> <li>Any database object whose name matches a naming convention or phrase</li> </ul>

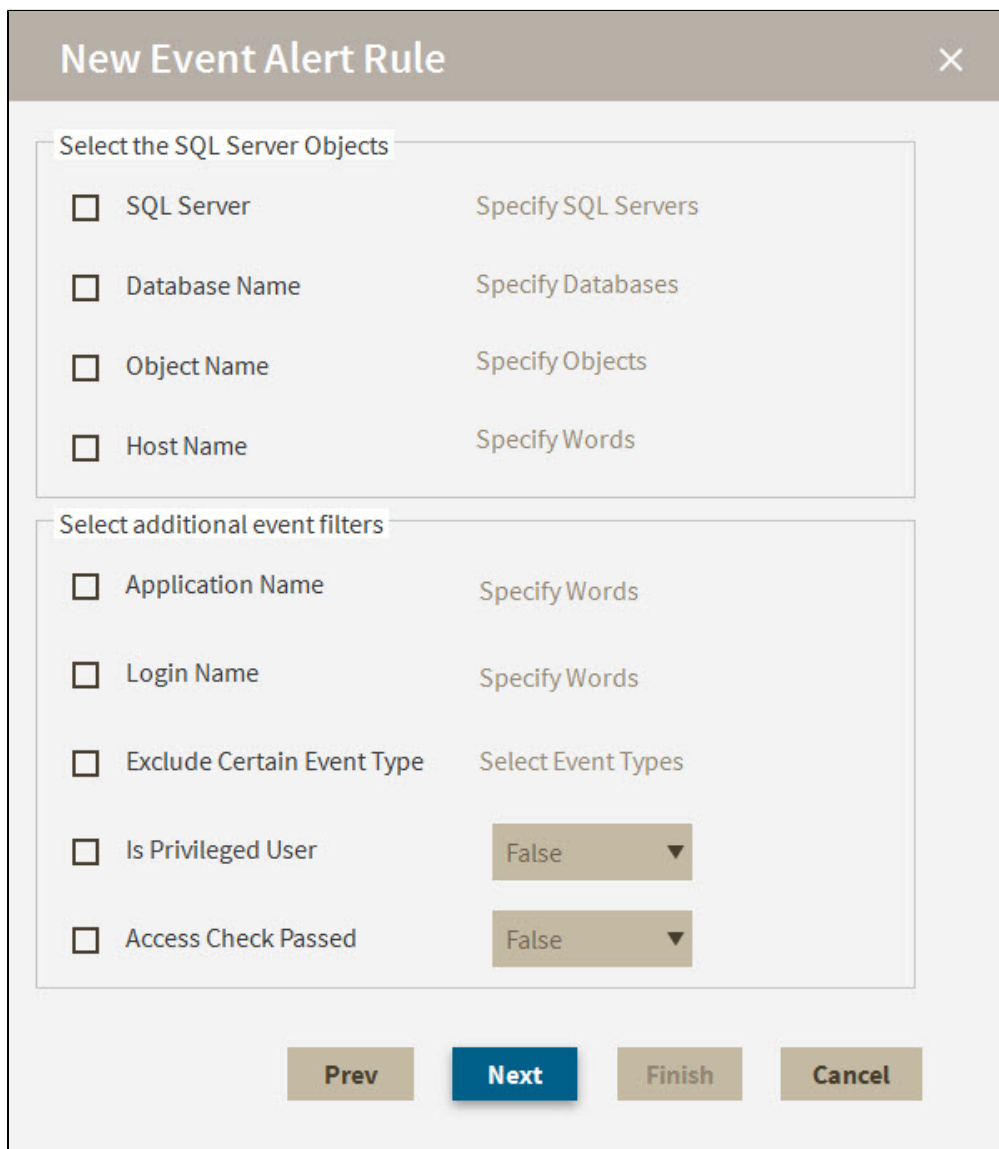
For example, you can specify the following objects:

- Any database whose name contains the word test on the LABSERVER instance
- The model database on any audited instance
- The Salary table in the HR01 database hosted by the Chicago instance

#### Edit rule details

Allows you specify the word or phrase the alert rule should use to identify events associated with the object you want to alert on.

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting



The dialog box is titled "New Event Alert Rule" with a close button (X) in the top right corner. It contains two main sections: "Select the SQL Server Objects" and "Select additional event filters".

**Select the SQL Server Objects**

<input type="checkbox"/> SQL Server	Specify SQL Servers
<input type="checkbox"/> Database Name	Specify Databases
<input type="checkbox"/> Object Name	Specify Objects
<input type="checkbox"/> Host Name	Specify Words

**Select additional event filters**

<input type="checkbox"/> Application Name	Specify Words
<input type="checkbox"/> Login Name	Specify Words
<input type="checkbox"/> Exclude Certain Event Type	Select Event Types
<input type="checkbox"/> Is Privileged User	False ▼
<input type="checkbox"/> Access Check Passed	False ▼

At the bottom, there are four buttons: "Prev" (disabled), "Next" (active), "Finish" (disabled), and "Cancel" (disabled).

## Alert Actions window

The Alert Actions window of the New Event Alert Rule wizard allows you to select the action you want this alert rule to perform when an audited event matches the specified criteria. Depending on the actions you select, IDERA SQL Compliance Manager writes an alert message to the application event log and email it to a specific email address or distribution list. You can use the default alert message or customize it to display the information you need most.

To successfully use email notification, ensure SQL Compliance Manager is configured to connect to your mail server.

## Available actions

### Select alert action

Allows you to select whether you want an alert message to be generated when this alert is triggered. You can configure an alert message to be written to the application event log and emailed to a specific address or distribution list. SQL Compliance Manager uses the same alert message content for the event log entry and email notification.

### Edit rule details

Allows you to specify one or more of the following attributes, depending on the alert action you selected:

- Content of the alert message
- Type of event log entry that should be written (Warning, Error, Information)

- Addresses to which the alert message should be emailed

The rule details pane also allows you to change your specified alert rule criteria at any time as you create your new alert rule. As you specify criteria using the New Event Alert Rule wizard, the rule details grows to include these additional settings. To edit previously set criteria, click the corresponding setting.

**New Event Alert Rule** [X]

**Select Alert Actions**

☐ Email Notification

Alert Message  
Specify email address

☐ Windows Event Log Entry

Information ▼

☐ SNMP Trap

Address [Text Field]

Port 162 [Spinner]

Community public [Text Field]

Prev Next Finish Cancel

## Finish Status Alert Rule window

The Finish Alert Rule window of the New Event Alert Rule wizard allows you to specify a name for the new Event Alert rule, review the rule details, and then click **Finish**. When you finish this wizard, IDERA SQL Compliance Manager enables the alert rule and begins applying your alert criteria against audited events associated with the selected objects.

## Available actions

### Enable rule now

Indicates that you want SQL Compliance Manager to begin monitoring audited events using this alert rule criteria immediately after you finish creating the rule. By default, all alert rules are enabled upon creation.



## New Event Alert Rule

☒ Enable this rule now.

Generate a **Medium** alert for **Security Changes** events on any SQL Server

Prev

Next

Finish

Cancel

SQL Compliance Manager audits all activity on your server. [Learn more > >](#)

[IDERA Website](#) | [Products](#) | [Buy](#) | [Support](#) | [Community](#) | [About Us](#) | [Resources](#) | [Legal](#)