Alert on Audit Data and Status

You can receive alerts when IDERA SQL Compliance Manager detects a specific event or operational status Alerting on event data collected from your audited SQL Server instances and databases provides the information you need to immediately correct issues that threaten your compliance with federal and corporate security and privacy policies. Alerting on operational status allows you proactively identify performance issues before your SQL Compliance Manager deployment is impacted.

You can also generate reports on alert activity, allowing you to provide forensic information and demonstrate policy enforcement. For more information, see Report on Audit Data.

Event alerting checklist

Use the following checklist to help you prepare your environment to successfully use Event Alerts to analyze audit data collected from your SQL Server instances and databases.

	Follow these steps ...
✓	Ensure your Windows logon account has sysadmin privileges on the SQL Server instances hosting the Collection Server. For more information, see Hardware requirements.
✓	Review how the alert process works and which SQL events you can detect using alerts. For more information, see How Event Alerts work.
✓	Identify the types of audit data you want to be alerted on. Determine which events should generate alerts and the conditions under which the alert should be generated. Also consider whether you want an alert message written to the event log or emailed to a specific account. For more information, see Use Event Alerts to analyze audit data.
✓	For each type of audit data you want to alert on, create an alert rule using the criteria you identified. For more information, see Create an Event Alert rule.
✓	***If you want to receive alert notifications through your email account***, test your email configuration settings to ensure SQL Compliance Manager can access your SMTP server. For more information, see Receive alerts through email.
✓	Review how you can implement Reports in your SQL Server environment. For more information, see Report on Audit Data.

Status alerting checklist

Use the following checklist to help you prepare your environment to successfully use Status Alerts to identify performance or operational issues in your SQL Compliance Manager deployment.

	Follow these steps ...
✓	Ensure your Windows logon account has sysadmin privileges on the SQL Server instances hosting the Collection Server. For more information, see Hardware requirements.
✓	Review how the alert process works and which SQL events you can detect using alerts. For more information, see How Status Alerts work.
✓	Identify the product components whose status you want to audit.
✓	For each type of status data you want to alert on, create an alert rule using the criteria you identified. For more information, see Create a Status Alert.
✓	***If you want to receive alert notifications through your email account***, test your email configuration settings to ensure SQL Compliance Manager can access your SMTP server. For more information, see Receive alerts through email.
✓	Review how you can implement Reports in your SQL Server environment. For more information, see Report on Audit Data.