

Registered SQL Server Properties window - Auditing Thresholds tab

The Auditing Thresholds tab of the Registered SQL Server Properties window allows you to set auditing thresholds to identify unusual activity on the selected SQL Server instance. IDERA SQL Compliance Manager reports threshold violations through the Activity Report Cards on the Summary tabs.

Use auditing thresholds to display critical issues or warnings when a particular activity, such as privileged user events, is higher than expected. These thresholds can notify you about issues related to increased activity levels, such as a security breach, that may be occurring on this instance. Auditing thresholds can also inform you when an audited SQL Server instance is becoming non-compliant. Use thresholds to supplement the alert rules you have configured for your environment.

	Warning	Critical	Period	Enabled
Event Alerts	100	150	per hour	<input type="checkbox"/>
Logins	100	150	per hour	<input type="checkbox"/>
Logouts	100	150	per hour	<input type="checkbox"/>
Failed Logins	100	150	per hour	<input type="checkbox"/>
Security	100	150	per hour	<input type="checkbox"/>
DDL	100	150	per hour	<input type="checkbox"/>
Privileged User	100	150	per hour	<input type="checkbox"/>
Overall Activity	100	150	per hour	<input type="checkbox"/>

Auditing thresholds can indicate when event activity is unusually high. If a threshold is exceeded, its status displays on the Activity Report Card tab for the event category.

[Learn how to optimize performance with audit settings.](#)

OK Cancel

Available fields

Warning

Allows you to specify the number of events you expect to occur in a given event category for the selected time period. When the warning threshold is exceeded, this violation indicates an unusually high number of events. A warning threshold violation can lead to a non-compliant database or SQL Server instance.

Critical

Allows you to specify the maximum number of events that should occur in a given event category for the selected time period. When the critical threshold is exceeded, this violation indicates a serious issue, such as a security breach, which is compromising your ability to remain in compliance with your corporate and regulatory policies.

Period

Allows you to set an acceptable rate, or time span, for the warning and critical thresholds. For example, you may expect overall activity to be no more than 200 events per day on this instance.

Enabled

Allows you to enable (select) or disable (clear) auditing thresholds for a particular event category.