# Snare Enterprise MSSQL

## Know who is doing what to your data

## Why do you need to monitor MSSQL logs if I am already monitoring the Windows Server?

That's because the Windows OS logs do not contain the critical MSSQL trace logs needed to explain who is doing what to your data. Our MSSQL Agent service interfaces with Microsoft SQL Server to initiate, read, filter and send trace logs from MSSQL to a remote host, local log file or to our Snare Central. Agent logs are available which allow the agent to send status message to the collection device, such as agent memory usage, service start/stop messages and any errors or warnings that trigger during operations. The Agent can send out regular heartbeats letting collection devices know the agent is working even when no logs are being generated. The MSSQL Agent also:

- Tracks sensitive data access
- Masks sensitive data in SQL statements
- Provide separation of duties between compliance and security activities

The Agent can be configured to monitor a variety of MSSQL installation types, with the default being the local MSSQL instance. This can also be modified to specify a named MSSQL instance and database.

### MSSQL has three distinct deployment scenarios:

#### Stand-Alone

- This scenario involves a single system running one or more instances of MS SQL Server.

#### Active / Passive Cluster

- This scenario involves two or more systems, operating as a Windows failover cluster, running one or more instances of MSSQL Server. Each service will have the capability to continue monitoring its assigned MSSQL instance in the event of a system failure and will follow the SQL instance as it migrates from one node to another.

#### Active / Active Clusters

- In this scenario there can be two or more systems that are active all the time and the MSSQL agent binds itself to each clustered instance on each node to track the specified activity.

The Snare MSSQL Agent has powerful functionality and capabilities.

- There is an **easy-to-use installer** with a silent install option.
- Admin can control remotely through a standard web browser or via the Snare Central agent management tool for **flexible centralized management**.
- The agent management supports either a single or multiple policy configurations by system or database functions.
- UDP/TCP protocols when sending events (TCP recommended for reliable delivery).
- TLS encryption for **secure log delivery**.
- If the destination is unavailable, the agent has **configurable caching** that allows the system to store and later send the event messages once the destination server is available once more. The Snare MSSQL service can be configured to monitor a variety of MSSQL installation types.
- Configure trace log collection based on "objectives". This allows granular control over the monitoring of specifically required activities.
  - For example, monitor all activity for users in the SYSADMIN role only and ignore other user activity or all users for a specific table in a database.
- Objectives monitor a list of specified MSSQL trace log events from selected databases, users or user group levels and propagate the information according to the network configuration.

### Contact us


Toll Free US: 1 (800) 834 1060
Denver Office: 1 (303) 771 2666
Asia Pacific: +61 8 8213 1200
UK/Europe: +44 (797) 090 5011

### US Headquarters

8480 E Orchard Rd. Suite 4350
Greenwood Village, CO 80111

### Corporate Headquarters

Level 1, 76 Waymouth Street
Adelaide, South Australia 5000, Australia