Telemetry

Last Modified on 30 July 2021

Telemetry on SQL Sentry

We've worked closely with our user community and the SQL Server community to gain insight from interviews, conversations, and our experiences from working with SQL Server over the years. We want to continue working with our users to understand how they're using our software, and where we can improve it. We want our users to be active in our engineering processes, from providing feedback through to testing Beta versions. For new feature requests, we will still rely heavily on personal interaction. We've used this information to help craft a product that best suits our user and their needs; however, this data is limited. To build the best software for the Data Platform community, we need more feedback. This is where application telemetry comes in.

By enabling **Telemetry** on SQL Sentry, you provide us with valuable information and statistics that helps to fill the gaps in the data-collecting process, ensuring the best product improvements and features.

Data That's not Being Collected

By enabling **Telemetry**, SQL Sentry collects data that's a part of the SQL Sentry application. Anything that's not a part of the application isn't collected.

SQL Sentry **Telemetry** doesn't collect any of the following:

- T-SQL Queries
- Database schema information
- Data from your databases
- Usernames or passwords
- Server names
- IP addresses

⚠ **Important:** The SQL Sentry telemetry system is designed to anonymize information that the SQL Sentry installation and client are reporting. There is a consistent identifier referred to as **LocationID** and **ClientID** that allows us to process the data, but not determine from which customer it originated.

Data That's Being Collected

Collecting data through application telemetry for SQL Sentry allows us to better understand which features our customers use the most, and how customers navigate through the client. Collecting this data ensures that we update our software to provide customers with features they need as quickly as possible. Enabling **Telemetry** on SQL Sentry allows the collection of the following data:

- The features of SQL Sentry a client session is using.
- The navigation path through the SQL Sentryclient.

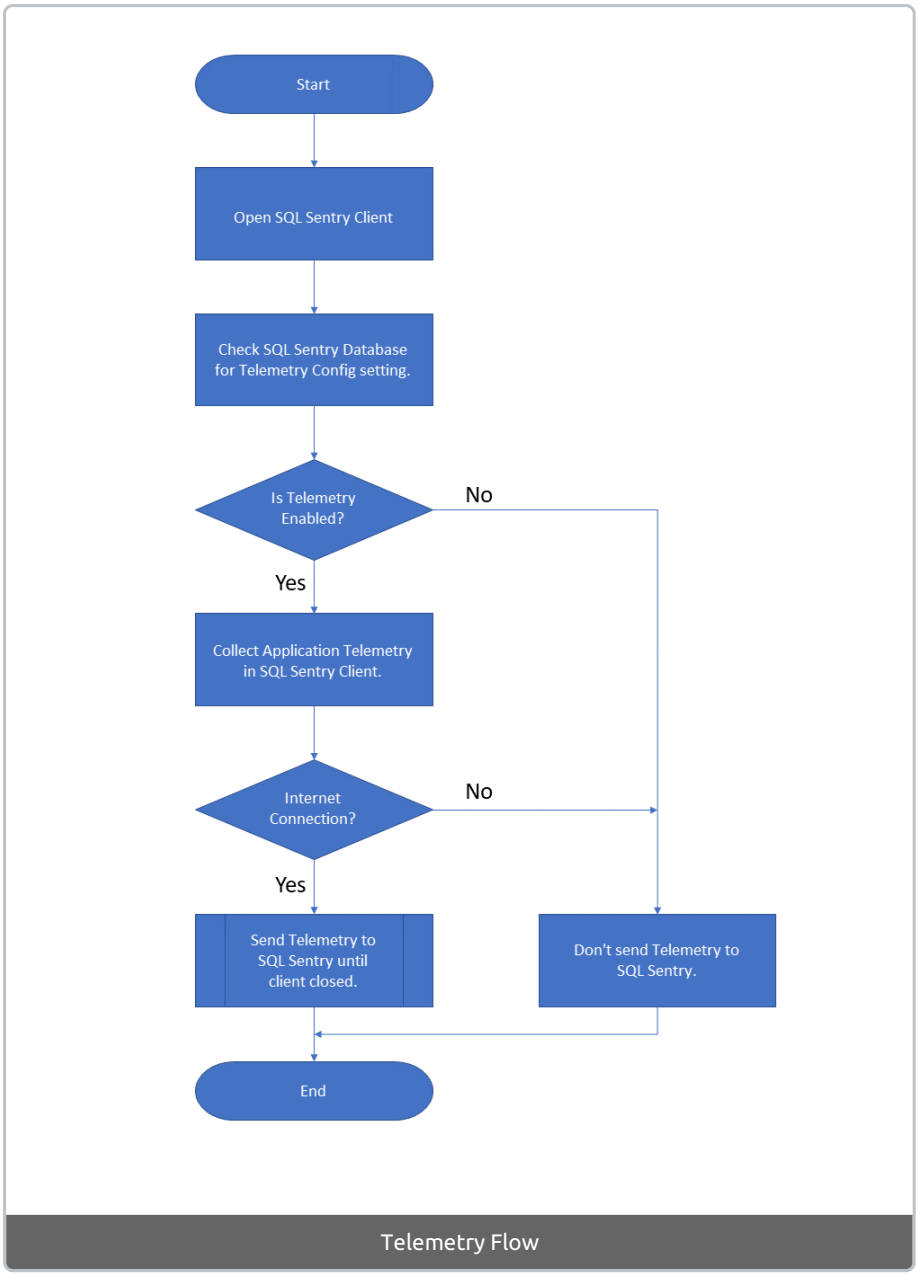
- The Environmental Health Overview (EHO) score shown in the client.
- The number of monitoring services shown in the client navigator.

Collecting and Sending

The telemetry engine resides in the SQL Sentry client, and each client installation handles the data sending process.

> ⚠ **Important:** The SQL Sentry monitoring service plays no part in **Application Telemetry**.

The process establishing if the client sends telemetry is illustrated with the following diagram:



Telemetry Flow

The process checks to see if an administrator has enabled **Application Telemetry**. This approach avoids

different settings within a customer organization. Centralized control means if Telemetry is set to **Off**, subsequent client installations maintain this setting rather than prompting an install.

> ⚠ **Important:** The client won't attempt to send telemetry data to SQL Sentry when there isn't an internet connection.

Receiving and Storing

The client sends telemetry data from the SQL Sentry client to our systems using a secure messaging protocol to Azure Event Hubs, ensuring that the data remains protected during transit with TLS. Once it reaches our back-end systems, the data is stored in a combination of Azure Data Lake Store and CosmosDB. PowerBI is used to visualize the usage data that we receive. Once the data has arrived in the storage and processing layer, we make use of the various Azure functionalities that exist to secure the data at rest.

> ℹ **Note:** Data collected with telemetry is stored in the Microsoft Azure regions in North America.

Insights from this data influence the way we build our software. Monitoring feature usage over time provides new navigation paths, and puts different SQL Sentry SKUs in play.

Common Questions

We're always looking to build better software. It's important that we understand how our solutions are being used by our customers. The following are three key questions we ask about how our customers are using SQL Sentry:

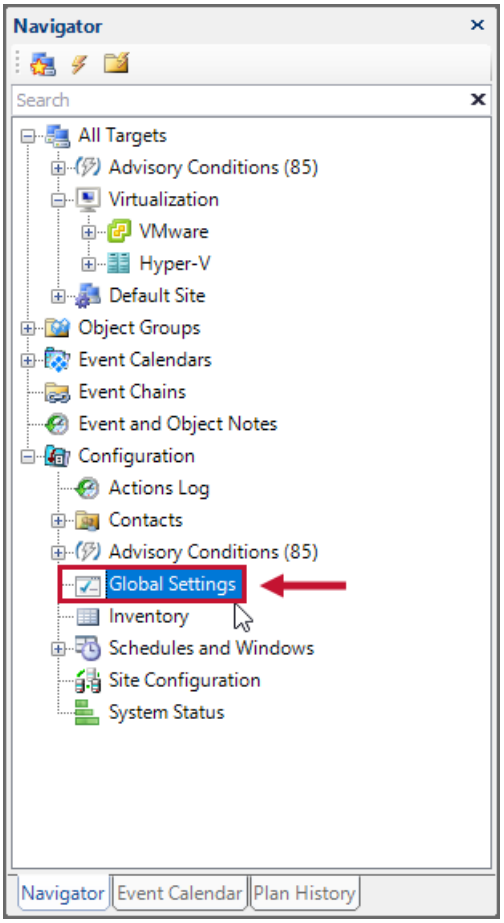
- Which features deliver the most value to our users?
- What are the most common navigation paths through our software that our users take?
- Which features are SQL Sentry users not leveraging?

With these three questions, it's possible to understand how we can make our software more accessible. These questions allow us to focus our efforts on building surveys for customers that focus on the areas used most heavily, further allowing us to focus engineering time on refining these areas to add value to all SQL Sentry customers. Focusing on these questions also highlights features in the software that need more awareness.

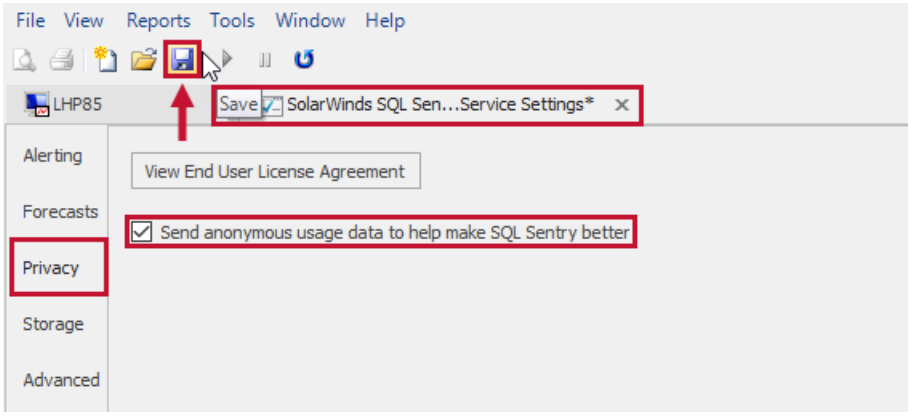
Enabling and Disabling Telemetry in SQL Sentry

Existing 11.2.x or above Installation

Once 11.2.x or above has been installed and configured, the option for the client to send telemetry is managed globally. To manage **Telemetry** settings, select the **Global** settings node (**Navigator** > **Configuration** > **Global Settings**) to open the **SQL Sentry Monitoring Service Setting** window.



In the **Monitoring Service** window, select the **Privacy** tab. Enable **Telemetry** by selecting the **Send anonymous usage data to help make SQL Sentry better** checkbox, and then select **Save** on the toolbar to save your settings.



Disable **Telemetry** by deselecting the **Send anonymous usage data to help make SQL Sentry better** checkbox, and then selecting **Save** on the toolbar to save your settings.


File View Reports Tools Window Help
LHP85
Save
SolarWinds SQL Sen...Service Settings*
Alerting
Forecasts
Privacy
Storage
Advanced
View End User License Agreement
Send anonymous usage data to help make SQL Sentry better