SQL Sentry Monitoring Service Security

Last Modified on 04 August 2021

The SQL Sentry monitoring service is a Windows service that runs in the context of a domain account. It is used by **SQL Sentry Software** (i.e. SQL Sentry) and **SQL Sentry Monitor**.

Security Requirements

⚠**Important:** Prior to version 19.1.1, the account must have **sysadmin** privileges on each **watched** SQL Server. We do not support watching targets on SQL Server version 2008 R2 or earlier without **sysadmin** privileges in any version of SQL Sentry.

- If the monitoring service account and interactive user do not have **sysadmin** privileges, then:
  - They must, at a minimum, be a principal on the SQL Server target with the **Control server** permission granted.
  - They must be a member of the **SQLAgentOperatorRole** role on the **msdb** database.
    - This automatically adds membership to the **SQLAgentReaderRole** and **SQLAgentUserRole**.
  - The **securityadmin** server role may be required to guarantee the collection of SQL Agent Log events, depending on the exact SP/CU of the SQL Server version.
    - See the Update to change permissions for running sp_readerrorlog and sp_enumerrorlogs in SQL Server article from Microsoft for additional information.
- The account must also have **Windows Administrator** privileges on any computer with a **watched** Windows Task Scheduler instance to collect system level performance metrics with SQL Sentry **Performance Analysis**. If the monitoring service does not have **Windows Administrator** privileges, instance level metrics can still be collected using the **Limited Access** option.
- It isn't necessary for this account to be a domain administrator account.
  - It's recommended that the service account be a standard user domain account that's added to the local administrators group of each monitored target.
  - For more information about security and SQL Sentry **Performance Analysis**, see the Performance Analysis Security Requirements topic.
- **GMSA** (Group Managed Service Accounts) is supported through the Service Configuration Utility (see the Monitoring Service Logon Account article for instructions) and EPI Commands.

⚠**Important:** There are some limitations when not using **sysadmin** privileges:

- SQL Sentry will not be able to collect VLF and log file data for targets that are on SQL Server version 2016 SP 1 or earlier.
- Last DBCC CHECKDB time is available only if the targets have the following SQL Server versions with the appropriate SP or CU:

    - 2014 SP 3+
    - 2016 SP 2+
    - 2017 CU 7+
    - 2019+
- You will not be able to start or stop the SQL Server Agent from the SQL Sentry client unless the target **Access Level** is **Full Access** and the interactive user is a Windows admin on the associated Windows target for that watched SQL Server.
- The watch status of SQL Agent Alerts cannot be changed.

Additional Information: See the SQL Sentry v19.1.1 : Monitoring Service Security Requirements blog post for additional details on not using sysadmin privileges.

Note: As of SQL Server 2008 the local administrators group of a Windows server isn't automatically given access to a SQL Server instance installed on that Windows server. Keep this in mind when installing SQL Sentry for use with SQL Server 2008 and above.

Important: Adding the service account to the local Windows Administrators group for the SQL Sentry database server doesn't automatically grant the service user access to the SQL Sentry database.

Monitoring Azure

See the Microsoft Azure SQL Database and Data Warehouse Security article for account and firewall information required to monitor these target types.

Changing the Monitoring Service Credentials

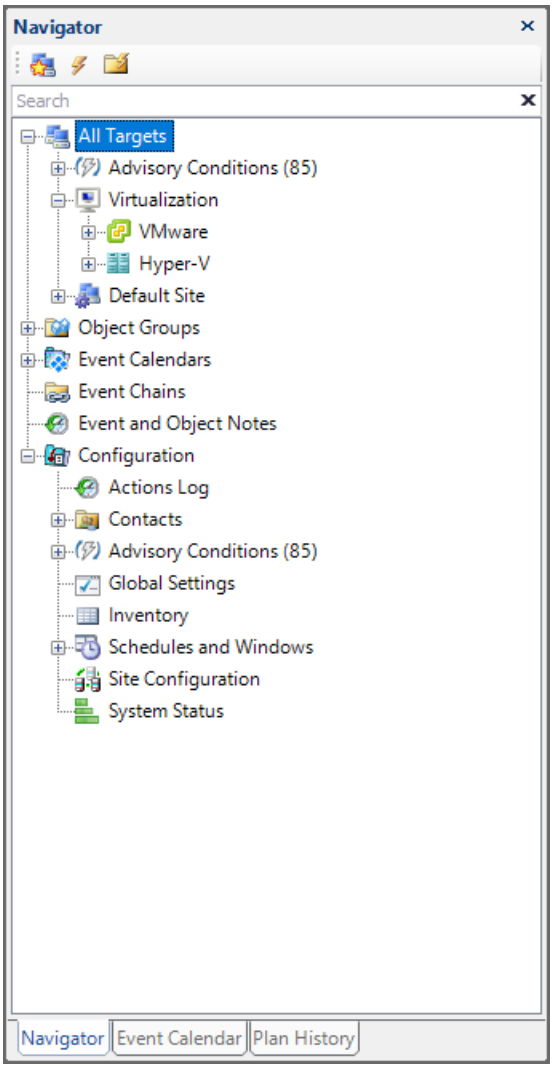
After the initial installation, the **Service Configuration Utility** is used to update or change the credentials of the SQL Sentry monitoring service account. See the Monitoring Service Logon Account article for instructions.

Monitoring Service Connection Properties

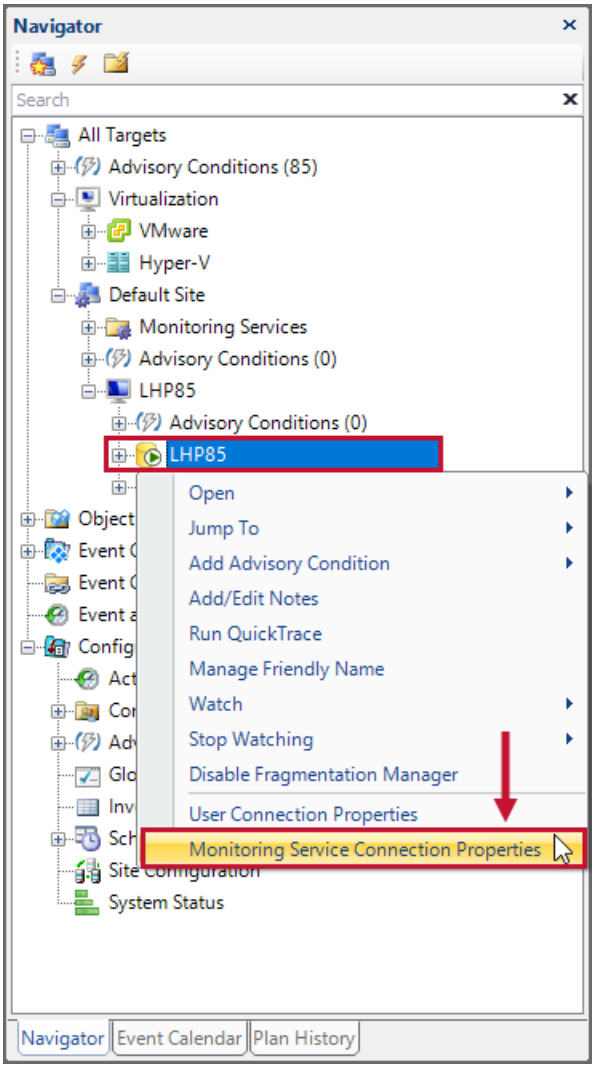
If the **Monitor Performance** setting is set to **False** for a target, and you don't need to utilize **General Performance Monitoring** features, you may configure the monitoring service to use **SQL Server Authentication**. This is done through an instance's **Monitoring Service Connection Properties**.

To access the **Monitoring Service Connection Properties** for an instance complete the following steps:

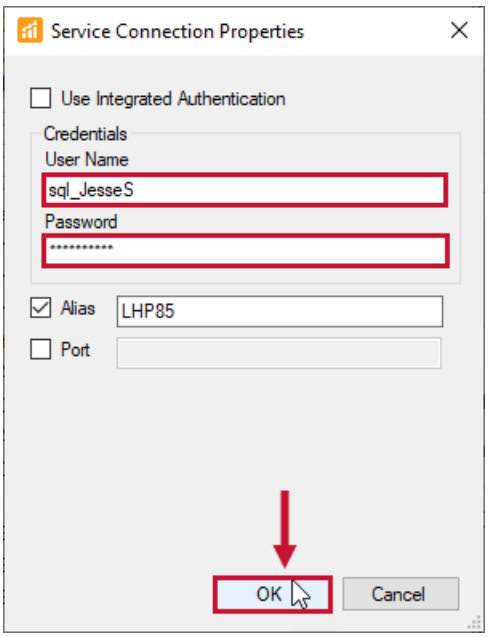
1. Open the **Navigator** pane (**View** > **Navigator**).



2. Right-click the desired instance, and then select the **Monitoring Service Connection Properties** command to open the **Service Connection Properties** dialog.



3. Uncheck **Use Integrated Authentication**, and then enter the **SQL Server Authentication** account you'd like the monitoring service to use for the instance. Select **OK** to save your changes.



Adjusting Target Access Level

You may wish to monitor an instance where OS level metrics through WMI and/or the Windows Performance Library are inaccessible. This is occasionally the case for cloud based or hosted servers. In these circumstances, a target may be added with **Limited Access**. This suspends attempts to access resources that are required for some functionality like the **Disk Space** and **Activity** tabs, and **Windows Metrics** on the **Performance Analysis Dashboard**. If access to those resources have been resolved, the **Access Level** can be set to **Full Access** in the **Monitoring Service Connection Properties** at the target level in the **Navigator** pane. Similarly, if a **Watched** target starts generating errors due to connectivity issues with the OS level resources that can't be resolved, changing the **Access Level** to **Limited** allows you to continue monitoring non-OS metrics without triggering connectivity errors for the target.

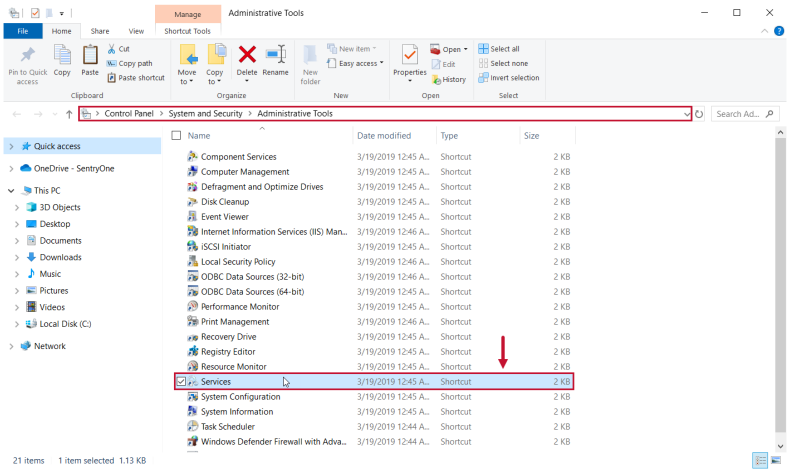
> ⚠ **Important:** If you configure **SQL Authentication** for an instance that's being monitored with SQL Sentry **Performance Analysis**, **Performance Analysis** won't be able to collect Windows level metrics for that instance. This is because **Performance Analysis** collects various performance and configuration data directly from Windows, and requires a higher level of access to the operating system than **Event Calendar**. For more information, see the Performance Analysis Security Requirements topic.

Starting the Monitoring Service

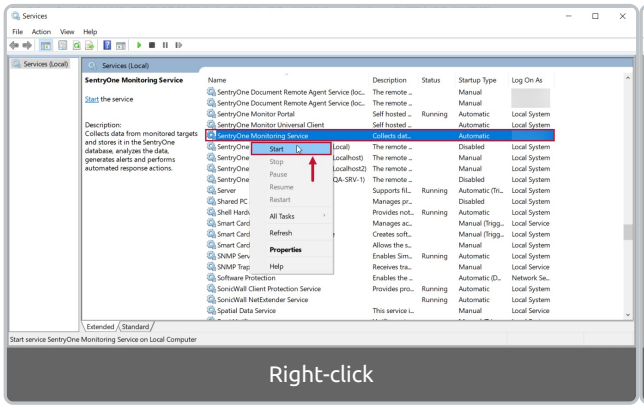
If the service fails to start, complete the following steps to start the service manually.

> ℹ **Note:** The SQL Sentry monitoring service starts automatically after installation.
>
> - For **SQL Sentry Software**, it activates upon detecting a valid license on the SQL Sentry database.
> - For **SQL Sentry Monitor**, it activates upon entering valid credentials to the SQL Sentry **Cloud Login** dialog during onboarding. If valid credentials are not entered, the monitoring service will not be able to validate your license.
> - Depending on the software version, this may be the **SQL Sentry Monitoring Service** or **SentryOne Monitoring Service**.

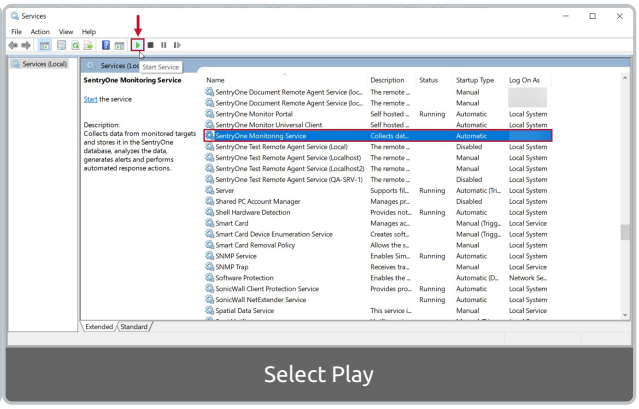
1. Open the **Services** window in Windows by selecting **Control Panel** > **System and Security** >**Administrative Tools** > **Services**.



2. Select **SentryOne Monitoring Service** from the list of services. Right-click **SentryOne Monitoring Service**, and then select **Start** from the context menu or select the **Play** button on the toolbar to start the service.



Right-click



Select Play

Success: You've manually started the **SQL Sentry Monitoring Service**.