Monitoring Additional Targets

Last Modified on 09 August 2021

Terminology

When the word target is used, we are referring to the device that houses your data, whether it's a physical server, cloud installation, APS appliance, or AWS RDS for SQL Server. Instance is referring to an instance of SQL Server or SSAS.

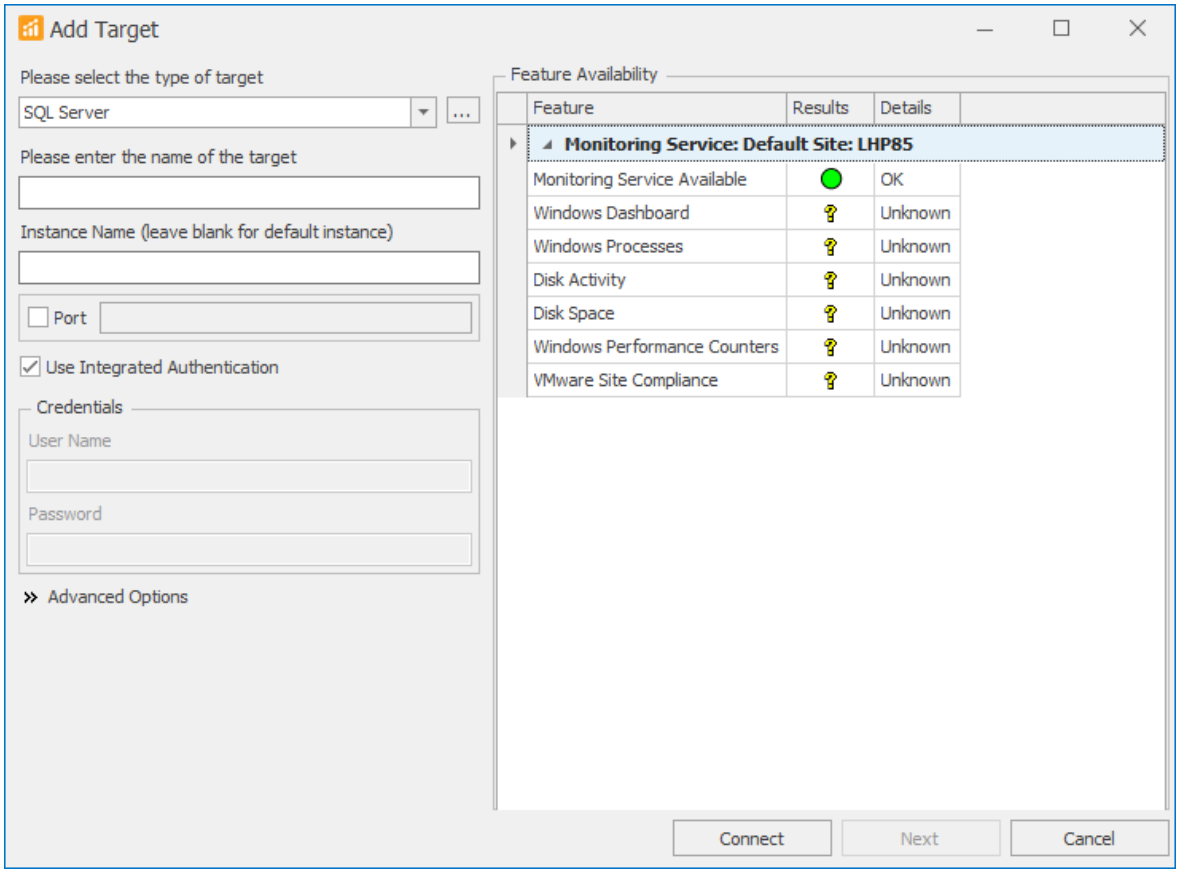
Supported Targets and Instances

Currently, SQL Sentry supports the monitoring of Windows, Azure SQL Database, SQL DW, APS appliance targets, AWS RDS for SQL Server targets, and Managed Instances. For more information about Managed Instances, see the Reaching for the cloud with SQL Sentry & Managed Instance article. Supported instances include SQL Server and SSAS. For more information about instances, including supported versions, see the System Requirements topic.

Access Level

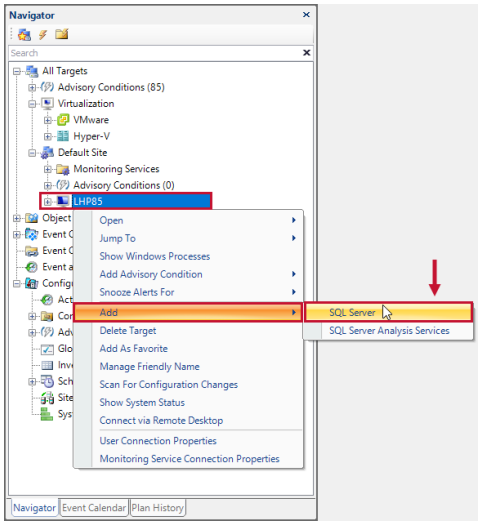
When adding a new target, the first step is completing a feature availability test. The results of this test determine whether the target is added with full access or limited access. When a target is added with full access, the monitoring service collects Windows level metrics and provides you with full access to the features of performance analysis.

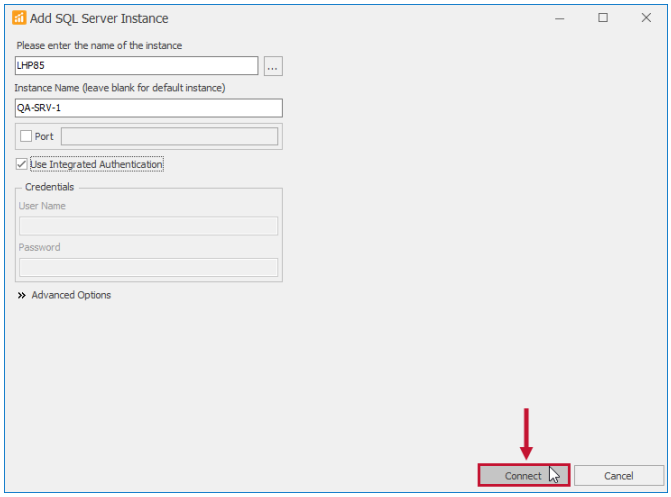
If the target fails the feature availability test, select the troubleshooting link, and attempt to resolve the issue. After applying a solution, retest the target. There are some situations in which limited access is the only option. For example, if you are monitoring a cloud-based SQL Server instance, you likely don't have access to the OS. When limited access is applied, the monitoring service doesn't collect performance counters, and access to the Windows Dashboard, Disk Activity tab, Disk Space tab, and Windows Processes tab are restricted. For more information about adding a Windows target, see the Performance Analysis for Windows topic.



Adding Instances

Add additional monitored instances to your SQL Sentry environment. Right-click either the shared groups node, a site node, a target group node, or an existing target node in the **Navigator** pane, and then select **Add**, or select **File** to add an instance. In the **Add** dialog box, choose the desired instance type from the drop-down menu, and then select **Connect**.





Note:

- When adding a new target, SQL Sentry attempts to resolve the name/IP address of the target

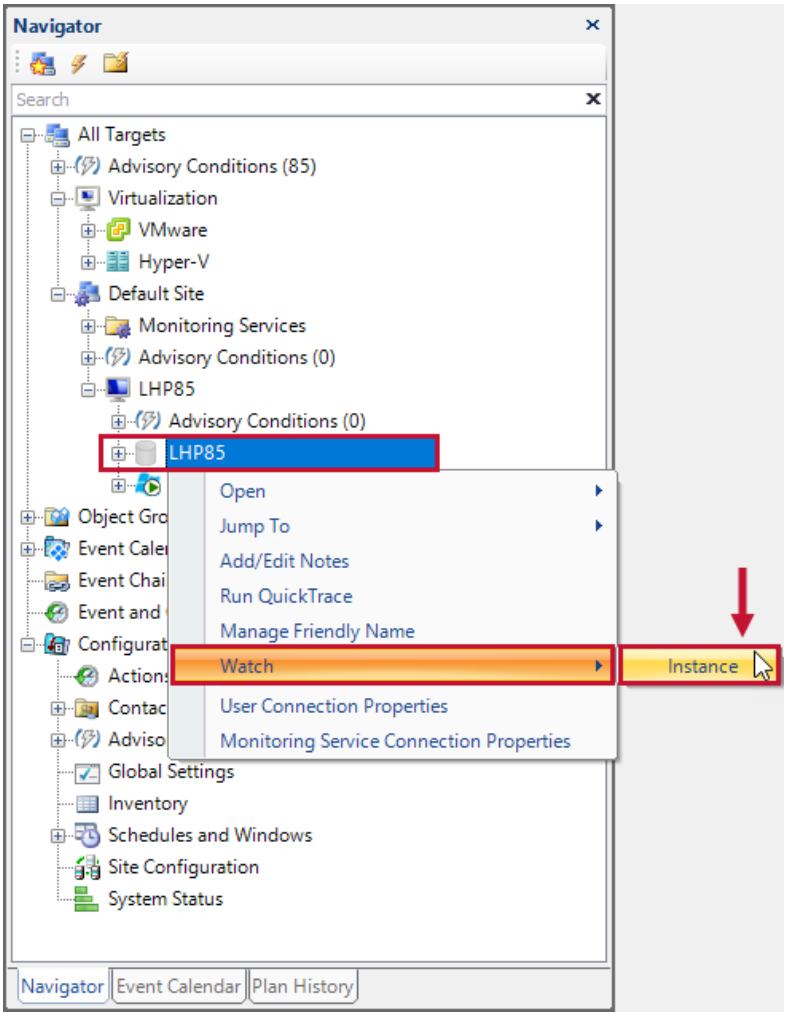
being added. There are no scans of IP ranges or subnets.

- See the Watched Target Objects article for information about objects added to the target.

Watching Instances

When you add a new instance to your environment it's monitored by default unless you explicitly decide not to watch the new instance. SQL Sentry monitors instances or objects with a status of **Watched**. Instances or objects that are not being watched are displayed with a grayed-out icon next to their name in the **Navigator** pane.

Unwatched instances or objects can have their status set to **Watched** through their respective context menus by selecting **Watch**. Once you watched a new instance, the SQL Sentry monitoring service starts actively monitoring the instance and its objects and begins honoring any associated configured conditions and actions.

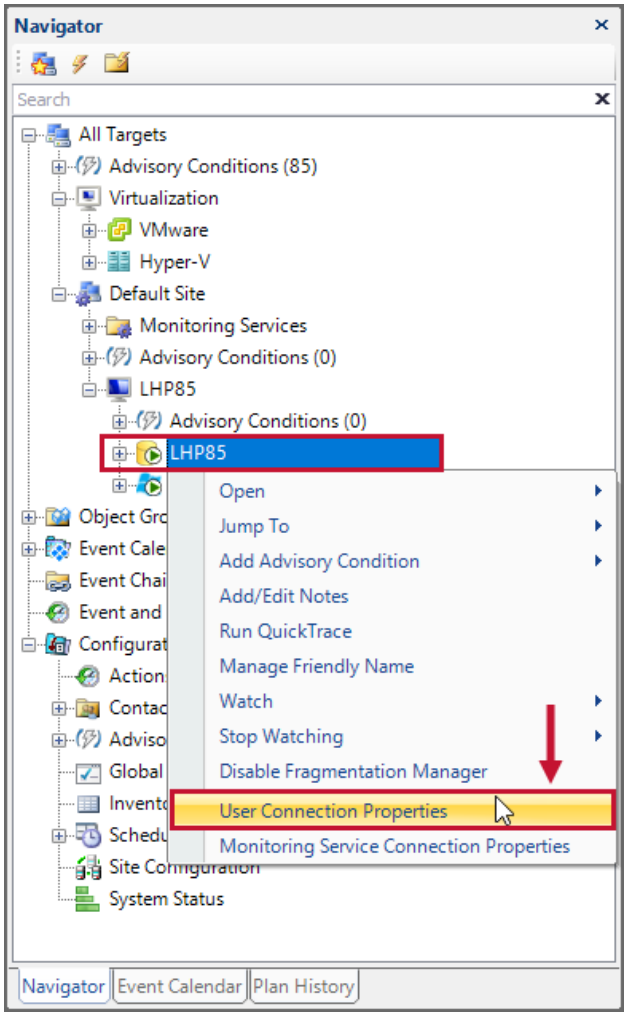


Note: Immediately after adding an instance or setting an instance to a **watched** status, SQL Sentry begins to synchronize with that instance. Exactly how long the synchronization process takes depends on the number of objects associated with the instance, the amount of historical data available, and how many instances are being watched at the same time. The **watched** status window keeps you informed of the process and alerts you to any errors.

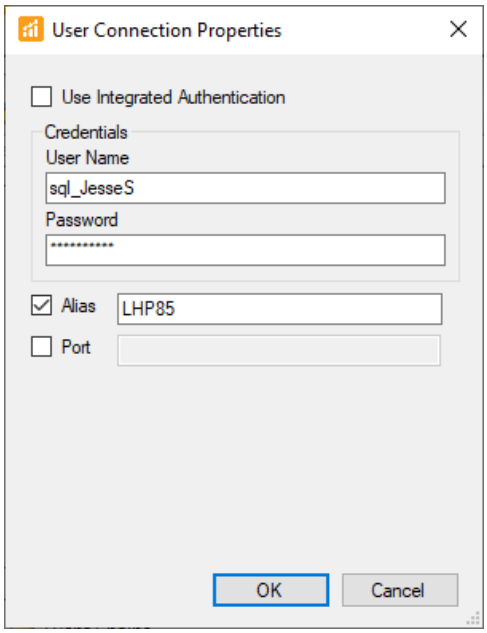
Modifying Instance Properties

After you've added an instance, you may need to change how SQL Sentry connects to the target. You'll see two options for connection properties when right-clicking on an instance:

Property	Description
User Connection Properties	Defines how your SQL Sentry client connects to a monitored server for the current user. These properties can vary for each client in your environment. The SQL Sentry client only connects directly to a monitored server under specific scenarios. For more information about the scenarios and specific security requirements, see the Client Security topic.
Monitoring Service Connection Properties	Defines how the SQL Sentry monitoring service connects to the selected server. The setting can be applied from any SQL Sentry client. Right-click on the instance, and then select **Monitoring Service Connection Properties** to configure the monitoring service connection. For more information, see the Monitoring Service Security topic.



Within the connection properties window, there are several properties that can be changed:



Property	Description
Enable Integrated Authentication	Tells what instance to use for the integrated Windows account information.
Credentials	Where you enter SQL Server credentials if you're not using integrated authentication.
Alias	By default, you'll see the server name that you initially entered when adding the instance.
Port	Used to connect to the SQL Server if it has been configured to a non-standard port.
Access Level	Used to assign the level of access that SQL Sentry has to the selected target. A target with limited access is not able to access Windows-based features, such as the Windows Dashboard, Windows Processes tab, Disk Space tab, or Disk Activity tab. Limited Access targets also don't have access to PerfLib performance counters for that target.

Note: All of these settings are available for SQL Server instances. SSAS instances only offer the **Port** setting. Targets offer the **Access Level** setting.

If you're monitoring the instance with Performance Analysis, changing the **Monitoring Service Connection Properties** to SQL Server credentials isn't supported. For more information, see the Performance Analysis Security Requirements topic.