

---

## LOGbinder SQL event collection from Microsoft SQL Server

The IBM® Security QRadar® DSM for Microsoft SQL Server can collect LOGbinder SQL events.

The following table identifies the specifications for the Microsoft SQL Server DSM when the log source is configured to collect LOGbinder SP events:

*Table 1. LOGbinder for Microsoft SQL Server specifications*

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft SQL Server
RPM file name	DSM-MicrosoftSQL-QRadar_version-build_number.noarch.rpm
Supported versions	LOGBinder SQL V2.0
Protocol type	Syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	LogBinder SQL website ( <a href="http://www.logbinder.com/products/logbindersql/">http://www.logbinder.com/products/logbindersql/</a> )  Microsoft SQL Server website ( <a href="http://www.microsoft.com/en-us/server-cloud/products/sql-server/">http://www.microsoft.com/en-us/server-cloud/products/sql-server/</a> )

The Microsoft SQL Server DSM can collect other types of events. For more information about other Microsoft SQL Server event formats, see the Microsoft SQL Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SQL Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the Microsoft SQL Server DSM RPM.
2. Configure your Microsoft SQL Server device to send LOGbinder events to QRadar.
3. If the log source is not automatically created, add a Microsoft SQL Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

*Table 2. Microsoft SQL Server log source parameters for LOGbinder event collection*

Parameter	Value
Log Source type	Microsoft SQL Server
Protocol Configuration	Syslog

---

## Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar

To collect Microsoft SQL Server LOGbinder events, you must configure your LOGbinder SQL system to send events to IBM Security QRadar.

### Before you begin

Configure LOGbinder SQL to collect events from your Microsoft SQL Server. For more information, see your LOGbinder SQL documentation.

### Procedure

1. Open the LOGbinder SQL Control Panel.
2. Double-click **Output** in the Configure pane.
3. Double-click **Syslog-Generic** in the Outputs pane.
4. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
5. Click **OK**.
6. To restart the LOGbinder service, click the **Restart** icon.