Requirements

.NET runtime

The Web Server computer and Base Monitor computer both require **.NET 3.5 SP1**. If you have .NET 4 installed, you still need .NET 3.5 SP1.

If you don't have .NET 3.5 SP1 installed, download it here.

If you're using IIS, SQL Monitor's application pool must be mapped to **.NET 2.0**, and not .NET 4.0.

Account permissions required

The following are the *minimum permissions* required to run SQL Monitor and monitor your servers. To test these permissions, see How do I test data collection methods?.

> ⓘ If you want to access SQL Monitor through a firewall, additional permissions are required. See How do I access SQL Monitor through a firewall?

SQL Monitor Web service account

- The account should have **Log on as service** rights.
- The account should have **Full Control** over the folder `C:\Documents and Settings\All Users\Application Data\Red Gate\SQL Monitor 3`. For Vista and Windows 7: `C:\ProgramData\Red Gate\SQL Monitor 3`.
- The account should have **Full Control** over the folder `C:\Documents and Settings\All Users\Application Data\Red Gate\Logs\SQL Monitor 3` or equivalent location.

> ⓘ The SQL Monitor Web Service is not installed if you use IIS as your Web Server.

SQL Monitor Base Monitor service account

- The account should have **Log on as service** rights.
- The account should have **Full Control** over the folder `C:\Documents and Settings\All Users\Application Data\Red Gate\Logs\SQL Monitor 3`. For Vista and Windows 7 : `C:\ProgramData\Red Gate\Logs\SQL Monitor 3`.
- The login should be a member of the **db_owner** database role on the Data Repository database (called RedGateMonitor by default).

Monitoring host Windows machines

The account should be an administrator on the machine.

Monitoring SQL Server instances

The account used to monitor your SQL Server instance should have the following permissions:

> ⓘ SQL Server 2012 is only supported by SQL Monitor 3.3 and later.

For SQL Server 2005, SQL Server 2008 and SQL Server 2012:

- member of the **db_datareader** role on the msdb system database.
- member of **SQLAgentReader** role on the msdb system database.
- member of the **db_ddladmin** database role on all databases (needed to run **DBCC SHOWCONTIG** required by the Fragmented index alert).
- **VIEW ANY DEFINITION** server permission.
- **ALTER TRACE** server permission (if you want to enable trace data).
- **VIEW SERVER STATE** and **VIEW DATABASE STATE** database permissions on all databases.
- **sysadmin** role required for Integrity check overdue alerts and to allow SQL Monitor to turn on the deadlock trace flag (this flag is required for Deadlock alerts to be raised; you can turn on the flag manually if you don't want to enable sysadmin permissions).

For SQL Server 2000:

If you want SQL Monitor to be able to collect trace data (trace data can optionally be displayed as part of some alerts), then the account must be a member of the **sysadmin** server role.

If you do not want SQL Monitor to collect trace data, then the account should have the following permissions:

- member of the **db_datareader** database role on the msdb system database.
- member of the **db_datareader** database role on the master database.

- member of the **db_ddladmin** database role on all databases (needed to run **DBCC SHOWCONTIG** required by the Fragmented index alert).

> ⓘ The sysadmin fixed role is a superset of these permissions, and can also be used, but is not explicitly required except for trace collecting.