



Using Trusted SQL Server Connection *with Sentry-go*

Last Updated Thursday, 19 April 2012

© 3Ds (UK) Limited
<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

This guide gives full details of how you can use both SQL Server logins and trusted connections with Sentry-go & the Sentry-go Enterprise Option.

Types of Connection

With SQL Server, there are two primary types of login you can create – an internal SQL Server-maintained login or an integrated Windows user ID. Both have their advantages but the type you use may be dictated by your database administrator or environment.

- **SQL Server Login.**

This is an ID that is created within the database and maintained by SQL Server itself. It has its own password & rules associated with it.



When access SQL Server from Sentry-go - either to monitor the database, monitor the SQL Server locking system or to log alert information, or when subscribing to the Sentry-go Enterprise Option, we recommend using SQL Server Logins wherever possible.

- **Integrated Windows (Trusted) ID**

It is also possible to access SQL Server using your Windows ID. This means that SQL Server knows about the ID and trusts Windows, or Active Directory etc. to authenticate it.



When using a trusted connection, it is the underlying “logged on” user that connects, rather than a specifically named ID.

Using a SQL Server Login (recommended)

From within Sentry-go, using a SQL Server login is the simplest and recommended option. To do this, simply enter the SQL Server user ID & password on the appropriate Sentry-go configuration window. SQL Server will then authenticate these details when the connection is made.

Add Query/Connection Test

Scan Criteria | Schedule | Response

Please define your ODBC connection & optionally SQL query below ...

Which ODBC connection do you wish to verify ?

Refer to this check as : Connection

Connect using DSN : Sentry-goAudit

User : sentry-go Password : *****

Test

Sentry-go will check the above connection. If this fails, the defined response will be run. If successful, you can optionally run the SQL query defined below ...

After connecting, also run this SQL Query ...

Returns a data type of : Number (Int) of length : 0

Cancel changes after running query (Rollback)?

Trigger an alert if ...

The query cannot be executed successfully

No. rows affected/returned is ... equal to 0

Returned data (col 1, row 1) is ... equal to

OK Cancel Help

Using a Trusted Connection

When using a trusted connection, it is the underlying user – the user running the software that makes the connection as opposed to a named user/password. Within Sentry-go, to use a trusted connection, leave the SQL Server user & password blank or tick the “use trusted connection” option as appropriate.



Users associated with trusted connections are still defined to SQL Server. However, their passwords are maintained by Windows or Active Directory, not SQL Server itself.

When using a trusted connection, it is important to consider the ID that will access the database to ensure it has sufficient access rights & permissions to do so. In most cases, it will be the Sentry-go monitor (a Windows service) that will connect to the database and as such, it is the user running that that will connect.

To configure this correctly, you have two choices ...

- Run the Sentry-go monitoring service as a domain user that has access to the SQL server.
- Grant SQL Server access to the local system account, the account that by default runs Windows services such as Sentry-go.

Running Sentry-go as a Domain User

By default, the Sentry-go monitor is configured to run as the “Local System” user. However, where additional permissions, network access or SQL Server access is required, it can be run as a domain user.

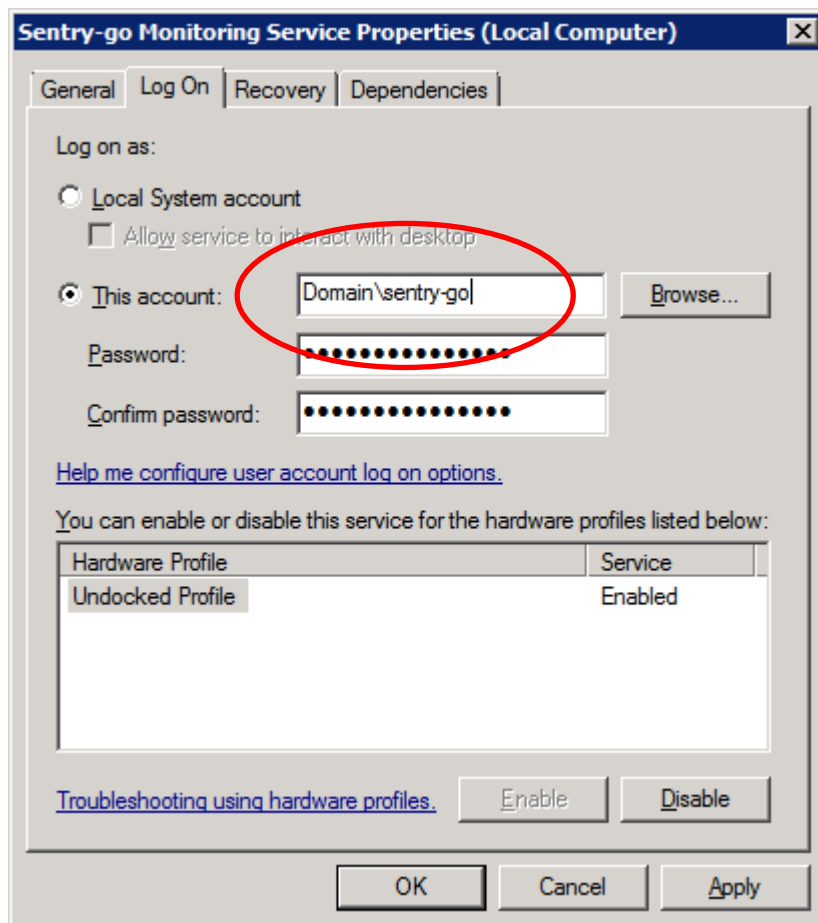
Create a New Domain User

Although you could use an existing user, we recommended that you create a domain user for use solely by Sentry-go. This can then be configured to allow the appropriate access the monitor will need, including access to the appropriate SQL Server databases.

Run Sentry-go as the Domain User

Now configure the Sentry-go monitoring service to run as this user. To do this ...

- Run the “Services” application in Windows Control Panel or under Administrative Tools.
- From the list select the Sentry-go service, click “Properties” and select the “Log On” tab ...



To pick up these changes, restart the Sentry-go monitoring service.

- ⚠ Once the user has been changed, verify that other checks continue to function correctly. Additional permissions on the local machine may need to be granted (e.g. local administrator rights) in order to perform some checks.

Running Sentry-go as a Domain User

As an alternative to the above, you can also grant SQL Server access to the “Local System” account so that it can continue to run the monitoring service.



The local system account is a built-in account which has extensive privileges on the local server/PC. It is internal to Windows and as such does not have a password or groups etc. You also won't find it listed in User Manager or in Active Directory. It can, however, run services & applications, be granted access to files/directories and, where configured, access SQL Server.

Configuring SQL Server

To configure the System account to **access SQL Server located on the same server ...**

- Start the SQL Server Management Studio (or Enterprise Manager etc.).
- Locate logins within the Security section.
- Create a new login for the “System” user ...
 - Enter the user name “NT AUTHORITY\SYSTEM”.
 - Set “Windows Authentication” for the user type.
 - Set the appropriate options for the new user language and the default database.
- Set the appropriate database role(s) for the new user.

To configure the System account to **access SQL Server located on a remote (different) server ...**

- Start the SQL Server Management Studio (or Enterprise Manager etc.) and connect to the appropriate SQL Server.
- Locate logins within the Security section.
- Create a new login for the “System” user ...
 - Enter the user name, including the domain & machine name, in the format “YourDomain\YourMachine\$”.
 - This is an internal Window user; remember to include the “\$”.
 - Set “Windows Authentication” for the user type.
 - Set the appropriate options for the new user language and the default database.
- Set the appropriate database role(s) for the new user.

Testing SQL Server access from within Sentry-go

Verifying SQL Server access from within Sentry-go is easy, using the Sentry-go Client Console ...

- Depending on the connection method chosen above, ensure the monitoring service is running as the appropriate user account.
- Run the Sentry-go Client Console & configure the appropriate monitor.
- Select the appropriate configuration tab to display the connection settings.
- Create/select the appropriate ODBC connection you wish to use.
- Next ...
 - If using SQL Server authentication, enter the SQL Server user/password.
 - If using a trusted connection, leave the SQL Server user/password and/or select "Use Trusted Connection" as appropriate.
- Click the "Test" button.
- The Console will establish a connection to the monitor which in turn will verify connectivity using the parameters entered.
- Results will be displayed in the web page.

The image shows two overlapping windows. The top window is the 'Add Query/Connection Test' dialog box. It has tabs for 'Scan Criteria', 'Schedule', 'Response', and 'Alert'. The 'Schedule' tab is active. The dialog prompts the user to define an ODBC connection. Fields include 'Refer to this check as:' (LiveAccess), 'Connect using DSN:' (Sentry-go Native Client), 'User:' (sentry-go), and 'Password:' (masked). A red circle highlights the 'Test ...' button. Below these fields, there are options for running an SQL query and returning data. The bottom section is for alerting, with radio buttons for 'The query cannot be executed successfully', 'The query takes more than ...', 'No. rows affected/returned is ...', and 'Returned data (col 1, row 1) is ...'. The bottom window is a web browser displaying the 'Sentry-go Monitoring System v5 Web Reporting' page. The page title is 'Sentry-go® Verify Configuration Option'. It shows system health information: 'Server: WALTON-04', 'Licence: 3Ds (UK) Limited', 'Generated on: 13th April 2011 at 12:18:04', and 'System Health: 33% check success'. Below this, it states 'Sentry-go Monitoring Service has performed the requested action and returned the following results ...'. The results show: 'Request from client: 127.0.0.1', 'Configuration check: Verify Database/DSN Access', 'DSN Name: Sentry-go Native Client', 'User: sentry-go', and 'Results: OK, database connection established successfully'. A link to 'View the Sentry-go monitor's log file' is provided. The Sentry-go logo is at the bottom of the page.

More Information, Help & Support

More information can be found in the guides that accompany the Sentry-go software. You can also access the following resources ...

- For the very latest information & product updates, please visit <http://www.Sentry-go.com>
- For sales advice, please e-mail Sales@Sentry-go.com
- For technical support, please e-mail Support@Sentry-go.com

