Security and Authentication

The fact that SQL DM for MySQL is a dedicated and specialized web server also makes it very secure.

- **SQL DM for MySQL - by design is very secure:** It is practically immune to any kind of malicious code. Whether they be unwanted popups, advertisements, trojans, attempts at phishing, hijacking or the like. Any HTML pages with such content are not sent by SQL DM.
- **Password protection:** During install you (or your SysAdmin) provided a password. Your browser prompts you for this password whenever you connect to the SQL DM for MySQL service. You cannot access the stream of data from the SQL DM for MySQL service if you are not able to provide the correct password.
- **Additional security considerations:** Note that on the server the SQL DM for MySQL password is stored obfuscated in the MONyog.ini file . Also, the SQL DM for MySQL embedded database has stored credentials (user IDs and passwords for MySQL servers, SSH, and SMTP servers).

The SQL DM for MySQL authentication system to work, must have cookies enabled in the browser. A 'medium high' security setting are appropriate for most users. The exact setting (and how it is named) varies from browser to browser.