MySQL SSL

Added in tiki12

For some system, e.g. cloud based systems such as Windows Azure, it is recommended to use an SSL connection to the MySQL database.

To enable a MySQL SSL connection, 3 key files must be specified, in PEM format:

- Client key. Filename must end with `-key.pem`
- Client cert. Filename must end with `-cert.pem`
- CA cert. Filename must end with `-ca.pem`

These files are placed in the `tikiroot/db/cert` folder. Tiki will detect these files and initiate an SSL connection. The `db/cert` folder could look something like this (Azure Clear DB sample):

```
.htaccess
59458e6c4a0ac-cert.pem
59458e6c4a0ac-key.pem
cleardb-ca.pem
web.config
```

*Note: It is assumed that the folder only contains 1 set of keys.*

The MySQL SSL status can be checked in the Admin / Security panel.

```
General Security  Spam protection

OpenPGP

MySQL SSL connection is active

Smartly Security
```

Starting in Tiki 12.1, the check can also be run from tiki-check.php

If any one of the key files are missing, a regular non-SSL connection is used.

Connecting using SSL requires:

- PHP extension `php_openssl.dll` must be enabled
- The MySQL server has activated SSL
- Tiki is configured with the 3 key files.