Storing Credentials (encryption) in Open-AudIT

Device Credentials

Open-AudIT stores both the device specific and default set of credentials using the PHP mcrypt function with the RIJNDAEL 256 cypher (which is also known as AES 256).

We must use a reversible encryption method as we need to decrypt and use the plaintext of the stored credentials for device auditing (as opposed to a one way encrypt and hash check, which is what Open-AudIT does with user logon passwords).

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

AES 256 is considered secure by the US government and used by it where appropriate.

The key in use by Open-AudIT for the credential encryption is user definable (naturally we do have a default). All data (except the key which is on disk) is stored in the database.

The key is stored in the file code_igniter/application/config/config.php. You should only change this if you have no credentials currently stored as once it is changed it will not be able to read any currently stored credentials (or change it, then bulk edit and set the credentials again).

User Credentials

User logon passwords are stored using a one way algorithm (SHA 256). When a user provides credentials, the provided password is encrypted and the result compared to what is stored in the database for that user.