# pfSense - Bug #9421

## crypt_data() needs to support stronger key derivation

03/22/2019 08:37 AM - Jim Pingle

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Start date:** | 03/22/2019 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Jim Pingle | **% Done:** | 100% |
| **Category:** | Backup / Restore | **Estimated time:** | 0.00 hour |
| **Target version:** | 2.5.0 | | |
| **Affected Version:** | 2.5.0 | **Affected Architecture:** | All |

**Description**

On 2.5.0 snapshots, if ACB is enabled, the following error is printed in the package install output when it writes config.xml:

```
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

If ACB is disabled, the error message is not shown.

The writes succeed and backups are made, so it's not fatal.

### Associated revisions

**Revision 6765f83a - 03/22/2019 10:21 AM - Jim Pingle**

Use new/stronger openssl options for crypt_data(). Fixes #9421

Retry with legacy options if new options fail, so we can still
read old style data from previous encryption runs (e.g. old encrypted
backups, ACB entries, etc)

Better error handling and suppression to prevent issues like #9421.

### History

**#1 - 03/22/2019 08:41 AM - Jim Pingle**

This appears to be from crypt_data(), similar to #9420, so still a syntax issue remaining there.

If you run some data through crypt_data() in the PHP shell, the error is printed there. So it appears fine from the GUI, but not from the console.

**#2 - 03/22/2019 09:59 AM - Jim Pingle**

*- Status changed from New to In Progress*

*- Assignee set to Jim Pingle*

**#3 - 03/22/2019 10:24 AM - Jim Pingle**

*- Subject changed from Error message in package output during write_config() when ACB is enabled to crypt_data() needs to support stronger key derivation*

Updated subject to match actual underlying issue. Fix inbound.

#### #4 - 03/22/2019 10:30 AM - Jim Pingle

*- Status changed from In Progress to Feedback*

*- % Done changed from 0 to 100*

Applied in changeset 6765f83ae75ee99141b2cd68c6e5134a51536e09.

#### #5 - 08/26/2019 01:04 PM - Jim Pingle

*- Status changed from Feedback to Resolved*