

# **Yacht Devices**

## **YDNB-07 Application Note on Program encryption and protection**

© Yacht Devices Ltd., [www.yachtd.com](http://www.yachtd.com)  
Document YDNB-07-AN-001, May 05, 2022

In case you develop programs for a third-party equipment integration, such equipment may have proprietary protocols and you may be under non-disclosure obligations, preventing you to reveal the program code to end-users.

Therefore, we have implemented several program protection mechanisms.



---

*Please, read the following carefully, or you can lock your Bridge forever!*

---

The protection is managed by the PASSWORD (string from 1 to 64 symbols long) and PASSWORD\_LEVEL (values from 0 to 15) settings.

*Table 1. PASSWORD\_LEVEL bits mapping*

| Bit #   | Bit is set (1)                                   | Bit is cleared (0)   |
|---------|--|--|
| 1 (LSB) | Password protection is enabled                   | Password protection is disabled, all other bits are ignored (will be set to 0) |
| 2       | Device's serial is used for encryption           | Serial number is not used for encryption                                       |
| 3       | The program cannot be downloaded from the Bridge | Encrypted program can be downloaded from the Bridge                            |
| 4       | The Bridge can be reset using the password only  | The Bridge can be reset by user, the program will be erased                    |

To enable password protection, add the following lines to the program (YDNB.CFG file):

```
PASSWORD=abc123  
PASSWORD_LEVEL=1
```

and load YDNB.CFG file into the Bridge. On success, an encrypted copy of the program will be saved in YDNBSAVE.CFG file.

PASSWORD\_LEVEL will be saved in this file header as "Password level".

After that, this particular Bridge specimen will only accept YDNB.CFG files encrypted with the password "abc123".

Note that if the PASSWORD is empty in the user program, any PASSWORD\_LEVEL will be ignored (treated as 0) and YDNBSAVE.CFG file will not be encrypted.

You can re-sell Bridges with the user program protected from unauthorized access or modification and you can distribute encrypted program updates to your users:

- if bit 2 is set, you will need to generate individual programs tied to the bridge serial number, this gives an opportunity to sell individual program versions and prevent unauthorized distribution of programs;
- if bit 3 is set, it will be impossible to get YDNBSAVE.CFG file from the Bridge at all — user can only change the program for another one (user should check LED indication to confirm successful program upload);
- if bit 4 is set, the Bridge cannot be reset by user and Bridge can be used only with your own programs.

For example, to employ "maximum protection" set all PASSWORD\_LEVEL bits to 1:

**PASSWORD=abc123**

**PASSWORD\_LEVEL=15      # (15 is 8+4+2+1, all bits are set)**

After program upload generated YDNBSAVE.CFG will be encrypted, its header will contain a message that the program is locked and cannot be downloaded.

Note that PASSWORD\_LEVEL setting allows only to set protection bits (increase the protection).

It will not clear protection bits which were already set earlier.

The only way to reset bits (decrease the protection) is to reset the Bridge along with erasing the user program.

To reset the Bridge protection settings, load YDNB.CFG file with a special comment:

**# YD:RESET**

If bit 4 was set, a password is also required:

**# YD:RESET abc123**

To tie the program to a particular Bridge (by serial number), use `PASSWORD_SERIAL` setting, it must contain the serial number (eight digits) of the target Device.

This number will not be stored in encrypted `YDNBSAVE.CFG` file and will be used for its generation only.

When bit 2 is not set in the `PASSWORD_LEVEL`, you can use any valid number in `PASSWORD_SERIAL` (for example, 00000000), because the serial number will not be used for encryption.

When bit 2 is set in the `PASSWORD_LEVEL`:

- if `PASSWORD_SERIAL` was not given, the Bridge will use its own serial number to encrypt the `YDNBSAVE.CFG` file;
- if valid `PASSWORD_SERIAL` is given, `PASSWORD` and `PASSWORD_LEVEL` will be reset after `YDNBSAVE.CFG` file generated, so you can make encrypted programs without the burden to reset your Bridge after generation of each encrypted program.

If encrypted program was generated with `PASSWORD_LEVEL` bits 1 and 2 set, you can be sure that the program can be used with the target Bridge (serial) only.

You can ask the end-user to send you a Bridge serial number and any password he or she likes.

Then, you need to send back:

- `YDNB.CFG` with only end-user's `PASSWORD` and required `PASSWORD_LEVEL` settings (at least bits 1 and 2 set).
- `YDNB.CFG` with encrypted program (generated using end-user's serial in `PASSWORD_SERIAL` and user's password in `PASSWORD`)

Knowledge of the password allows end-user to reset the Bridge, but will not allow decryption of the program.

**Example of the encrypted program (YDNBSAVE.CFG file), note that  
PASSWORD\_LEVEL = 1 allows to download the program from the Bridge:**

```
# Current configuration of Yacht Devices NMEA 2000 Bridge
# Firmware: 1.30 01/07/2019
# Serial: 00000000, Password level: 1

2688FAA0DB2E6A85B8F0ED7FDDC6CFD24406BA954A1D51761C2B101DFD5BFE1841
38BC4992658FBAD6192A196BE1CB4E8B53AB8948B7AC0E0A4720DF302247AD57CC
C275988B0E5935FFC637FD1C4953AC11200EBE32406FA62C6DBC92E2A72B2E162
F351E368B89B4E05149AB3C1F7C8F538FF32A808C90B64B386A8B7D3EE4F7B22A1
91A3B3C4FEEBC09DA27B75B8D641552E5A00761A77B97BAB7B37E9A1230F42CC91
31B440EFB16B8D7794C7F5C11732643E9668B29E6D471FC0EBD141293DB2678613
675E9E990455F0034CBC17E4BE6FDDE1DE5F291E552BF57D6221452791F63AB814
4FE4C1220E7DB408CCA62BDA8BEDC523AD30FE06423E3F04194FA0F34CDB560E5E
3B3111AED176162FE200CA04E7781049A41FBADFCE82067770E73D1ED1550792B9
FCEAD3B989687BAB2CE0AE06E99D6FE432979E5C5CC1C0792049EC8B22232E8311
7912C5ADCAF836A4B7ED3283645FB7F2308519F99011A5B81B7475A19C19176E02
2AE4C0D640915FB80BD74E8BFB68DD09FD4C5BFCAABDE6803011ED54DBBFC86142
2E28990265EEF21F26341944DC259D9AEE334934E1E94722855D475512B053721A
0335E956BFA0F6CB29EB9A49BEEBC2DFF19400DF3696CC1BA49543992B59116F08
3184AC088AAECD6ECE6F600CA9A76B2A8BDC65E7E4D8B5BD142FC3C85291753BAC
30338D2C6E3D00571955F6C6D5AAFEFC9F4B2A98D1C01ABD201EA0270CA1E3DC19
4BCF2AD40A5F5F626C275978A0C651353D358FE2F873A5B85536BD2DCBE0755426
EBB234BC7164E95B930D72C090661B4CCB7C6B6E98E68A6FC4CB17646E934826E5
9B2D08C77966A28715C074D574DF08E005488A84C90DAB4FC82F486F23C9A9B91F
87496D613334EAB7B7C0237A8F10F1E07FEDB5493933F37E0885926C809D5E73EA
9F82D2E9DB66881B8DA0C61EE42579E7EC52C4B47361BDA6A7C28147C0FAC402D8
30F76872269C1DDD8524DBDA08A55C4D572D04D69B3761F49FF0548F04E87ECD9F
441D90FB32150D5C902FE984FA0B54649373442EE80A85547F6AA0F2DCE30D1120
7728794E9CF71DB2E8488DB391893EC0D7DA8BD387AC3D04C7B3EAB3AF5F52519B
4A0A6383667EF4F2FEE2D791361186282A9BC10C68F9DE2D4FC5AFA5C790AA10B8
3EE88D0E5372DFB2C0F1B05E1374031109DA6AE661D55141EA23893B98706D8436
6676F557C2D85B2649B2A5F5FBDE9D8056F43CA21CEF5312FF655130527A5E9005
6F134BFA3C5199CC4A77841B181B16E4207B9D168C866F23F730D49CB132326B4F
EE340F129838FAF127DC6526E998887793384AA76213D9CDBC259EDDB0E605535
56EEF25EAA73FF6158AF0F1A789E4537113BD60E10D88154E53168D712CD602276
2602298D3EA58201C2BE22A61852B6A84C1CFBABA03ABC7B9EBC9AF86E0D9A60D4
314BA213F0BD47BAC20B361A4D8967B57849BEEDD200A3AFB2B5F1A15C898C856D
189974283DA2EC82094C6A470D80177E2EF382CC04E40D7BA2E1A5811CB9F37C8E
AF17E6254AA089941FD780F5178EE01D1A4855B4A293D8745844BD6B093BB47A07
7195C3CC71371FD7680C387BC7F13348F63DD9BDC2D900649D3CBAF96C1840E58A
9319E3DB58C45F9D65E48D5C85E078DB03B80D8EB4A5A5F37BE64AC68A6A518CF5
2BD8AEAD137CBBDE3CFE86C407AC2FCDF03388DAD6C7F6BD6D4816EDEEB25BAAEB
BA013D2DB4DB51BB2F1F8BAB9EA94EAEF6F5E0FD715E6460FF52E0F716177812C1
849F69BD2372ED7D7778461F3B9310125D32CD8FF306EF42CED7D3F60A2212660
A8DFBF4BEDC4AE22EAA3CFFF426BB8E76D0A29443AED9FEB5E83BCCB77A246CFE3
4AB4BF131074BD6BB567FF213F3AD00E3EE3E43C1F90B5D553902000F3B00FA9E7
83FB281BB2AD757076EBE76DC93B3CF49D6030C954DDD0B946A9779FBC6F1BB49D
1F7FF91CE9E4E01187CEBB4B120F18960E1637CEAD3B3F898EF04C0B2FB2232B78
52E6BD670F31F50815A45E1F16224EEC8A1FCF2822521D2ECE6C15034969AAA9F7
7AF75FA03C50FBC020220C002A0FAC5E8C8DE97D9FD7E7EF32F89B068A5C4F4762
1ED25D3FD4CFCF65360FE8E4F55FD9409F3B569EC6D024B2C8AB951DD8CD7BF555
0C56ED969F0D82FDCF86A8A7188D2BE7A2CCFDCC38EC11000E7F1A72A7E5A23361
9B7E43304BA18C99D34E621C71E57A6770E2E061633734A561450F175029185228
2C44962D0B7258D6FB2287459665BC635FAB45111AB4404D83B42F8B64C20C37F6
B0B68A2173EC63A5E2C7F908BAB52D9002E39376E8DCFFA7CD889B76CCB9205506
A1289491B75ABA6574248F345149584A9254427635CFC3F0040COBDADC7DBACDDF
E3F18A338483088366F6E7546DCF1EBA4AA539165B06F275055B454D8D77519AB5
F38A3C92B2B8BA33D2E5F4048CD1E4770017119876AAC97565413D2D8645485DA7
```