Порядок действий при установке прошивки 2021г.

- **1. Устанавливаем прошивку** от Aleksey S (с форума на ixbt, последняя от 05.03.2018), можно скачать отсюда https://wd.hides.su/wd...imware/custom_mbl_new/ файл **mbl_rootfs_2018_05_03.zip**.

  Порядок действий:

  - Все файлы из скачанной папки (mbl_rootfs) скопировать в папку Public на устройстве
  - В папке Public переименовать файл rootfs_20180503.img в **rootfs.img**
  - Подключиться по SSH с помощью PuTTY и выполнить команды:

  ```
  cd /DataVolume/shares/Public
  chmod 777 UpgradeNas.sh
  ./UpgradeNas.sh
  ```

  Дождаться пока завершится прошивка, по окончании устройство само перезагрузится, ждать пока устройство будет готово.

  P.S. Среди скачанных файлов есть файл с кратким описанием - **readme.rus** (можно открыть любым редактором, например, "Блокнотом"). В прошивке (как и в заводской) установлен Twonky 5-й версии. Посмотрите как обновить **здесь** (и далее несколько сообщений).

- **2. Включение протокола SMB2**, чтобы не включать в Windows поддержку протокола SMB1 (SMB1.0/CIFS клиент). Для этого зайдя, например, через WinSCP в начале файла /etc/samba/smb.conf в секции [global] нужно добавить строку: **`protocol = SMB2`**, примерно так:

  ```
   [global]
  workgroup = WORKGROUP
  realm = WORKGROUP
  netbios name = MyBookLive
  server string = My Book Live Network Storage
  protocol = SMB2

  include = /etc/samba/smb-global.conf
  include = /etc/samba/smb-global_veto.conf
  include = /etc/samba/overall_share
  ```

  После этого перезапустить SAMBA

  ```
  /etc/init.d/samba restart
  ```

  или перезагрузить устройство.
  В Windows, чтобы проверить какая версия SMB протокола используется, запустить от имени администратора PowerShell, открыть на устройстве любую папку (например, Public), затем в окне PowerShell выполнить команду:

  ```
  Get-SmbConnection
  ```

  выведет табличку, в столбце **Dialect** должен быть номер версии протокола SMB: **2.0.2**.

- **3. Обновить Twonky** до версии 7.2.8. Скачайте файл **dlna-server-twonky_7.2.8-20140617_powerpc.deb**, скопируйте его в Public на устройство. Подключитесь браузером http://mybooklive (или http://ip_адрес), зайдите Настройки - Мультимедиа и остановите Twonky (снимите галочку с "включить.."). Подключитесь с помощью Putty и выполните команды:

  ```
  cd /DataVolume/shares/Public/
  dpkg --force-overwrite -i dlna-server-twonky_7.2.8-20140617_powerpc.deb
  reboot -f
  ```

  После перезагрузки подключитесь браузером http://mybooklive (или http://ip_адрес), Настройки - Мультимедиа и включите Twonky.

Подключитесь http://mybooklive:9000 (или http://ip_адрес:9000), settings - проверьте статус Twonky. Всё нормально? Ключ не требует? Если всё нормально, проверьте как работает - запустите обзор/просмотр. Если запросит ключ, введите **SEGL-WXKG-TAHC-AXPP-GKGA-BKAM-TFCM-WMAP**

Проверьте настройки Twonky: Settings - Sharing. Папка /Public указана? Галочка слева стоит? Для неё выбрана настройка "All content types" (все типы файлов)?
Если не указана - укажите, нажмите внизу кнопку "Save changes" (сохранить настройки). Галочка "Enable sharing for new media receivers automatically" стоит?

- **4. Устранение уязвимости CVE-2018-18472**

  Вчера выяснили: https://habr.com/ru/post/564956/
  Там же написано что делать. Очень показательная статья.

  В приложенном архиве готовый файл (взят из последней альтернативной прошивки) с уже внесёнными изменениями. Для устранения уязвимости CVE-2018-18472 на My Book Live, скачать архив, распаковать и заменить файл **/var/www/Admin/webapp/includes/languageConfiguration.php**, например, скопировать с помощью WinSCP. Потом проверить что права на файл такие же как у соседних (644).
  Прикрепленные файлы
  languageConfiguration.zip (1,36 КБ)

- **5. Повышение "отзывчивости" системы**

  Кратко:
  Подвисания возникают из-за нехватки памяти при интенсивной "многопоточной" работе, например: закачка/раздача торрентов - как правило, больших файлов, которые "собираются" из большого количества мелких кусочков (при этом часто каждый кусочек ещё нужно расшифровать), или интенсивный файлообмен по SMB, особенно запись большого количества достаточно мелких файлов, которые система загружает/пытается загрузить в дисковый кеш, и не может/не успевает их выгрузить (освободить память) достаточно быстро при переходе к следующему фрагменту/файлу, что приводит к сильной фрагментации памяти и повышенной загрузке процессора. Выглядит это обычно так: "диск жужжит, всё висит". Отвисает достаточно долго - иногда больше десяти минут, в определённых случаях может зависнуть совсем.
  Для устранения подобных проблем обычно рекомендуют изменить параметр ядра **min_free_kbytes**. Данный параметр говорит ядру стараться держать указанный объём памяти свободной (не использовать под кеш) а, чтобы удовлетворить это требование, ядру приходится запускать встроенный механизм дефрагментации/освобождения памяти раньше. Если задать слишком малое значение, то дефрагментация не успевает запуститься вовремя и в **top** можно наблюдать интенсивные попытки высвобождения страниц памяти (freepages). Рекомендуемое значение вычисляется так: (5 - 6 % от физической памяти в килобайтах -> округлить в большую сторону, кратно 4K)/(количество ядер), где 1K = 1024. Для 256MB получается ~ 16000 округляем до 16384. Учитывая, что у My Book'а памяти и так не много, можно попробовать начать с меньших значений увеличивая шагами относительно текущего, например: **4096**, **8192**, **12288**, заканчивая **16384**.

  Посмотреть текущее значение можно командой:

  ```
  cat /proc/sys/vm/min_free_kbytes
  ```

  Задать можно командой:

  ```
  sysctl -w vm.min_free_kbytes=16384
  ```

  Значение сохранится до перезагрузки, можно понаблюдать, при необходимости выставить следующее значение и снова понаблюдать.
  Чтобы внести постоянные изменения, добавить в файл /etc/sysctl.conf строку:

  ```
  vm.min_free_kbytes=16384
  ```

  тогда значение будет восстанавливаться при перезагрузке.

- **6. Установка и использование chroot-среды** (transmission-daemon, miniDLNA...)

  Скачайте и запустите скрипт автоустановки chroot-среды

  Для чего выполните в консоли **последовательно** команды

  ```
  wget --no-check-certificate
  https://github.com/MyBookLive/chroot/raw/master/install.sh
  ```

```
sh ./install.sh
```
Примечание: *в моём случае скачивание пакетов обрывалось с ошибкой* ***«Не удаётся разрешить адрес github.com»****, необходимо было в файле* **`etc/resolv.conf`** *прописать строчку с адресом DNS сервера, в моём случае:* **`nameserver 192.168.1.1`**

Начнётся установка базового набора файлов дистрибутива Debian Wheezy, которая может занят от 20 до 40 минут в зависимости от загруженности NAS'a и ширины интернет-канала. После чего будет возможность установить по вашему желанию медиасервер miniDLNA и\или торрент-клиент Transmission. После установки можно (опционально) запустить установленные сервисы без перезагрузки устройства.

Вход в chroot-среду:

```
chroot /DataVolume/debian
```

Перед вами полноценная Debian Wheezy. К примеру, можете установить файловый менеджер mc:

```
apt-get update
```

```
apt-get install mc
```

```
mc
```

Использование chroot среды:

Запуск

Скрипт установки прописывает всё необходимое для запуска выбранных сервисов в chroot-среде. Сервисы, которые будут стартовать при включении My Book Live перечислены в файле

`/DataVolume/debian/chroot-services.list`, по одному сервису в строчке.

Подсказка: в `chroot-services.list` *перечислены имена файлов из* `/DataVolume/debian/etc/init.d`*, которые необходимо запустить*

Даже если никаких сервисов в chroot-среде пока не запускается, перед входом в неё необходимо выполнить скрипт запуска для монтирования необходимых каталогов:

```
/etc/init.d/chroot_debian.sh start
```

Вход и выход из работающей chroot-среды

Выполните

```
chroot /DataVolume/debian
```

Выполнив ls / вы поймёте, что уже не в окружении прошивки. Так же изменилось приглашение с MyBookLive:~# на (chroot-debian)~#. Здесь уже можно без боязни выполнять apt-get update, устанавливать, конфигурировать или удалять любые пакеты: перед вами полноценный дистрибутив Debian Stable, который можно использовать практически без ограничений. Из-за того, что всё происходит в изолированной "песочнице", файлам прошивки навредить не выйдет при всём желании. После окончания конфигурирования новых сервисов не забудьте внести их имена в chroot-services.list. Для выхода из chroot-среды выполните exit и вы вернётесь в привычное окружение прошивки.

Остановка

```
/etc/init.d/chroot_debian.sh stop
```

Восстановление автостарта после обновления прошивки

Необходимо вернуть на законное место скрипт запуска chroot-сервисов:

```
/DataVolume/debian/chroot_debian.sh install
```

Удаление chroot-среды

Остановите chroot-сервисы и удалите скрипт их автозапуска

```
/etc/init.d/chroot_debian.sh stop
/etc/init.d/chroot_debian.sh remove
```

Перегрузите WD My Book Live и удалите все файлы Debian Wheezy

```
rm -fr /DataVolume/debian/
```

- **7. Обновить сертификат, чтобы работал облачный доступ**

Первый способ:
Скопировать файл в Public на устройство.
После этого выключить облачный доступ, подключиться по SSH (если необходимо, предварительно подключиться http://mybooklive/UI/ssh или http://IP_адрес/UI/ssh , чтобы включить SSH доступ) и выполнить команды:

```
cd /usr/local/orion/openvpnclient
mv ca.crt ca.crt.org
cp /shares/Public/ca.crt.txt /usr/local/orion/openvpnclient/ca.crt
chmod 744 ca.crt
```

Перезагрузить устройство и включить облачный доступ.

Второй способ:
Выключить облачный доступ. Подключиться к устройству с помощью программы **WinSCP** и открыть папку /usr/local/orion/openvpnclient/, переименовать старый файл (ca.crt -> ca.crt.org), скопировать на его место новый (в последних версиях можно перетащить файл прямо в окно), переименовать его (ca.crt.txt -> ca.crt), выставить права на файл (по правой кнопке -> Свойства внизу ввести 0744).
Перезагрузить устройство и включить облачный доступ.

Информация о сертификате ca.crt.txt

```
# openssl x509 -in /DataVolume/shares/Public/ca.crt.txt -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
d4:31:d4:f1:45:d3:f1:19
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=CA, L=SanFrancisco, O=WD, OU=Branded, CN=4grelay/name=Ben/emailAddress=ben.roque@wdc.com
Validity
Not Before: Mar 18 01:08:47 2020 GMT
Not After : Feb 23 01:08:47 2120 GMT
Subject: C=US, ST=CA, L=SanFrancisco, O=WD, OU=Branded, CN=4grelay/name=Ben/emailAddress=ben.roque@wdc.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:ba:7e:24:1e:c0:74:16:52:7e:ba:a0:1e:8b:b3:
75:7b:06:29:b9:89:bd:f4:54:27:0d:7c:e6:29:a6:
75:51:77:f1:43:ff:38:7b:f2:27:e8:a0:e0:c1:86:
37:5a:01:f9:38:21:1b:e5:be:68:08:ba:52:f6:d6:
9e:40:f0:c0:39:f3:14:0d:a3:e1:70:58:74:01:1a:
7a:31:e1:e2:ce:bb:f6:a2:16:e9:af:09:4b:cc:3f:
58:69:f5:f3:eb:f6:66:5c:a6:c2:f9:20:6a:1a:d2:
fb:e4:3c:78:33:ce:c3:8e:32:c8:f8:2b:13:92:5e:
ea:f1:7d:70:06:05:43:76:d5
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
F5:A8:05:60:1A:0D:79:22:60:AA:13:0B:A1:91:83:65:3E:B4:EF:99
X509v3 Authority Key Identifier:
keyid:F5:A8:05:60:1A:0D:79:22:60:AA:13:0B:A1:91:83:65:3E:B4:EF:99
DirName:/C=US/ST=CA/L=SanFrancisco/O=WD/OU=Branded/CN=4grelay/name=Ben/emailAddress=ben.roque@wdc.com
serial:D4:31:D4:F1:45:D3:F1:19

X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
09:79:a6:cf:6d:64:cd:a2:84:bd:a6:80:34:61:82:ff:af:8d:
68:fc:1f:cd:ff:ce:c9:00:10:0c:f2:a6:d7:ed:73:5a:18:67:
ba:62:4f:06:cc:be:e2:5e:01:5a:89:04:90:d9:d7:bd:b1:b3:
87:40:9c:4b:cf:42:99:68:1f:1c:0f:72:b9:fe:d7:3f:f1:43:
87:87:fa:12:6a:f6:2d:c5:68:ca:ac:b3:6b:05:da:db:fa:99:
70:28:eb:4a:0f:19:fc:9d:87:5a:10:d6:12:02:e0:3c:50:04:
5d:54:3d:c2:d5:bc:65:4e:e5:10:22:67:17:67:0c:23:e6:db:
fb:d9
#
```

Действителен до: (Validity -> Not After :) **Feb 23 01:08:47 2120 GMT**

- **8. Настроить web-доступ**

  На устройстве в настройках удалённого доступа -> Веб-доступ -> Регистрация, выбрать пользователя (по умолчанию admin), ввести в "имя фамилия" admin, ввести почтовый адрес, нажать "Отправить", дождаться письма и перейти по ссылке из него. После регистрации к устройству можно подключиться "отовсюду" с помощью браузера, после прохождения аутентификации на сайте mycloud.com.
  Для мобильных устройств можно также не генерировать код, а подключиться указав эту учётную запись.
  Если создано несколько пользователей на устройстве, для каждого из них можно создать учётную запись на mycloud.com, они будут получать доступ к своей папке, а также к тем, к которым adnin разрешит доступ на чтение или запись.
  Подробности: **MY BOOK LIVE - Руководство пользователя** -> стр. 108

  P.S. При проблемах подключения через http://mycloud.com (можно сразу http://files.mycloud.com), открыть "Подробнее" на странице с сообщением об ошибке и "Принять сертификат устройства". После этого подключиться через http://mycloud.com заново. Если пишет "подключение не защищено", то "подробнее" -> "перейти на Web страницу" / "всё равно подключиться".

  Чтобы работал облачный доступ, устройство (используя сертификат для авторизации) должно добраться до сайта **www.wd2go.com** по https (в файле **/usr/local/config/dynamicconfig_config.ini** параметр: SERVER_BASE_URL="https://www.wd2go.com").
  При первом подключении / первой регистрации (иногда и после сброса) получить уникальные имена вида **device1234567-12345678.wd2go.com** и **device1234567-12345678-local.wd2go.com**.
  При повторных подключениях подтвердить имена/отметиться как подключённое, после этого имена должны находиться через DNS запросы. Имена сохраняются локально в файле dynamicconfig_config.ini.
  Если IP "белый", то первое имя - это внешний IP роутера (как бы свой DynDNS от WD). Если IP "серый", то первое имя - это адрес сервера WD, через который осуществляется доступ к устройству по VPN туннелю.
  Второе имя (local) - это IP адрес устройства во внутренней сети, на него после авторизации перебрасывает устройства, подключённые к домашней сети, которые авторизуются через mycloud.com, например, при подключении к устройству через браузер с компьютера или мобильное приложение, настроенное на авторизацию через mycloud.com. Чтобы периодически не перерегистрировать второе имя, а также для удобства использования устройства во внутренней сети, за ним в настройках роутера и закрепляют IP-адрес ("привязывают" IP-адрес к MAC-адресу устройства).

  Если даже просто включить облачный доступ в настройках устройства (не указывая учётную запись mycloud.com), подключение облачного доступа устанавливается, только не происходит привязка к учётной записи, после указания учётной записи и привязки к ней устройства, становится возможным подключение через авторизацию на mycloud.com.
  Если что-то связанное с устройством настраивали в роутере - удалите и проверьте что в роутере включён UPnP. Иногда помогает простая перезагрузка роутера или роутера и устройства поочерёдно.

  Если пишет при попытке принять обновление сертификата на сайте mycloud.com
  Не удается получить доступ к сайту. Не удалось найти IP-адрес сервера deviceXXXXXXX-XXXXXXXX.wd2go.com. Речь идёт о сертификате Web-сервера устройства. Так как состояние подключения облачного доступа не "Подключено", устройство не отметилось как "подключённое", то в DNS записи не активны, по имени устройство (или сервер доступа) не находит.

  Была похожая ситуация: не находило все серверы WD и *-local.wd2go.com через DNS серверы провайдера (настройки роутера по умолчанию). Но всё находило через GoogleDNS / YandexDNS и т.п... В настройках DHCP сервера роутера указал выдачу клиентам своих настроек DNS вместо провайдерских, после чего всё заработало.