



Pwn Plug Elite 1.1

Factory Image Installation Guide

Contents:

- [Download the factory image package](#)
- [Configure a TFTP server](#)
- [Connect to the Pwn Plug serial console](#)
- [Upgrade the Pwn Plug U-boot software](#)
- [Install the Pwn Plug Linux kernel](#)
- [Install the Pwn Plug root filesystem](#)
- [Update the Pwn Plug to patch 1.1.3](#)

WARNING:

This installation process will permanently erase all data on your Pwnie Express device. Any data you wish to preserve should be backed up to an SD card or USB flash drive before proceeding.

Download the factory image package

If you haven't done so already, download the factory image package from here:

<http://www.pwnieexpress.com/pages/downloads>

Note: The current factory image file name is `pwnplug_1.1_Elite_5-3-2012.tar.gz` with an MD5 checksum of: `cdeff830e175ab3896d3e6fa57fc000e`

Configure a TFTP server

Your Pwn Plug will download the installation files from this TFTP server during the installation process.

Note: These instructions are specific to Ubuntu/Debian-based distributions. Other *nix variants may be used as your TFTP server, though the specific configuration steps may vary.

1. Open a command terminal on the Linux computer you'll be using as the TFTP server.
2. Enter the following commands (as the root user) to set up the TFTP server:

```
# mkdir /tftpboot
```

```
# chmod 777 /tftpboot
```

```
# apt-get install openbsd-inetd tftpd
```

```
# echo "tftp dgram udp wait nobody /usr/sbin/tcpd  
/usr/sbin/in.tftpd /tftpboot" > /etc/inetd.conf
```

```
# service openbsd-inetd restart
```

Tip: If a software firewall is running on your TFTP server, either disable it during this installation process or create a rule allowing inbound connections to UDP port 69.

3. Copy the Pwnie Express factory image package to the TFTP root:

```
# cp pwnplug_1.1_Elite_5-3-2012.tar.gz /tftpboot
```

4. Extract the contents of the Pwnie Express factory image package:

```
# cd /tftpboot
```

```
# tar zxvf pwnplug_1.1_Elite_5-3-2012.tar.gz
```

Connect to the Pwn Plug serial console

1. Power up your Pwn Plug and connect the Ethernet interface to the same network as the TFTP server.
2. Connect the supplied mini-USB cable between your Plug's mini-USB serial port and a Linux machine. On some older Linux kernels, the following commands may be required:

```
# modprobe usbserial  
# modprobe ftdi_sio vendor=0x9e88 product=0x9e8f
```

Tip: For Windows/Mac systems see: http://plugcomputer.org/plugwiki/index.php/Serial_terminal

3. Connect to your Pwn Plug's serial console using screen:

```
# screen /dev/ttyUSB0 115200
```

Tip: If screen terminates after a few seconds, use "dmesg" to confirm the plug is showing up as a USB serial device. Example:

```
[15360.948161] usb 5-3: FTDI USB Serial Device converter now attached to ttyUSB0
```

If the serial interface is showing up as something other than "ttyUSB0" (such as ttyUSB1), adjust the "screen" command accordingly.

1. Press ENTER twice

Tip: If a login/command prompt does not appear, try CTRL+C.

2. At the login prompt, login as "root". The default root user password is: pwnplug8000

Tip: To exit a screen session, press CTRL+A, then backslash (\)

Upgrade the Pwn Plug U-boot software

Tip: Copying the U-boot commands directly from this document and pasting into the Marvell>> prompt is recommended whenever possible.

1. In the Pwn Plug bash prompt type "reboot" and press ENTER.
2. When the prompt "*Hit any key to stop autoboot:*" appears press any key to enter the U-boot console ("Marvell>>").

Tip: If you miss the 3-second startup window, use a paperclip to press the plug's reset button. The reset button is behind the small hole to the right of the plug's SD card slot.

3. Check your U-boot version by entering the following command:

```
version
```

4. If your U-boot version matches the output below, your U-boot is already up to date - skip to the section "Upgrade the Pwn Plug Linux kernel". Otherwise, continue to the next step.

```
U-Boot 2011.12 (Jan 08 2012 - 21:53:47)
Marvell-Sheevaplug - eSATA - SD/MMC
gcc (Debian 4.6.2-9) 4.6.2
GNU ld (GNU Binutils for Debian) 2.22
```

5. Enter the following command at the Marvell>> prompt.

```
print ethaddr
```

Tip: Do *not* press any navigational keys (arrow keys, Home/End, etc) while in the U-boot console as this may interfere with your terminal commands.

6. Copy the MAC address provided and paste it into a temporary text file (you will need it later).
7. Enter the following command to acquire an IP address from your DHCP server.

```
dhcp
```

Tip: As an alternative to using DHCP, you can set the IP address by typing **setenv ipaddr x.x.x.x** (where x.x.x.x is the IP address you want to assign to the Pwn Plug)

8. Once the IP address has been acquired via DHCP or manually assigned type the following command to confirm connectivity to your TFTP server (where x.x.x.x is the IP address of your TFTP server).

```
ping x.x.x.x
```

9. If the plug does not immediately respond with "Host x.x.x.x is alive", verify the plug and TFTP server are on the same network.
10. Enter the following command (where x.x.x.x is the IP address of your TFTP server).

```
setenv serverip x.x.x.x
```

11. Enter the following command to download the new U-boot image to a temporary location in memory. You will see a string of "#" symbols during the download.

```
tftpboot 0x0800000 u-boot.kwb
```

Important: If you see “Loading: T T T ...”, this indicates a timeout while trying to contact the TFTP server. If this occurs, verify network connectivity between the plug and the TFTP server, verify the TFTP server is running and listening on UDP port 69, then reset the plug and return to step 1 in this section.

12. Enter the following two commands to erase the U-boot partition and write the new U-boot image.

```
nand erase 0x0 0x60000
```

```
nand write 0x0800000 0x0 0x60000
```

13. Enter the following command to reboot the plug, then immediately tap the ENTER key during plug startup to re-enter the U-boot console ("Marvell>>" prompt).

```
reset
```

14. Enter the following command (where xx:xx:xx:xx:xx:xx is the MAC address copied in step 4).

```
setenv ethaddr xx:xx:xx:xx:xx:xx
```

15. Enter the following command to save your changes.

```
saveenv
```

16. Enter the following command to reboot the plug

```
reset
```

Install the Pwn Plug Linux kernel

Tip: Copying the U-boot commands directly from this document and pasting into the Marvell>> prompt is recommended whenever possible.

1. Enter the following command to download the Linux 2.6.37 kernel image (where x.x.x.x is the IP address of your TFTP server).

```
dhcp 0x2000000 x.x.x.x:sheeva-2.6.37-uImage
```

Tip: As an alternative to using DHCP, you can use the setenv ipaddr command

2. Enter the following two commands to erase the kernel partition and write the new kernel image.

```
nand erase 0x100000 0x400000
```

```
nand write 0x2000000 0x100000 0x400000
```

Install the Pwn Plug root filesystem

Tip: Copying the U-boot commands directly from this document and pasting into the Marvell>> prompt is recommended whenever possible.

1. Enter the following command to download the root filesystem image (where “x.x.x.x” is the IP address of your TFTP server). Note the download may take several minutes.

```
dhcp 0x2000000 x.x.x.x:pwnplug_1.1_Elite_ubinized_5-3-2012.img
```

2. Enter the following two commands to erase the filesystem partition and write the new filesystem image. Note that writing the filesystem image to flash memory (“nand write” command) typically takes 3-5 minutes.

```
nand erase 0x500000 0x1fb00000
```

```
nand write.e 0x2000000 0x500000 0x14800000
```

3. Copy the following command block and paste into the Marvell>> prompt. Note this is all one command.

```
setenv bootargs console=ttyS0,115200  
mtdparts=orion_nand:0x400000@0x100000(uImage),0x1fb00000@0x500000  
(rootfs) ubi.mtd=1 root=ubi:rootfs rootfstype=ubifs;setenv  
bootcmd 'nand read.e 0x800000 0x100000 0x400000; bootm  
0x800000';setenv mainlineLinux yes;setenv arcNumber 2097
```

4. Enter the following two commands to save your changes and reset your plug.

```
saveenv
```

```
reset
```

5. Allow the plug to fully boot the newly flashed operating system (do not press any keys during

startup).

6. Login (root:pwnplug8000) and verify the Pwnie Express splash message is displayed, showing the newly flashed kernel version and Pwn Plug software version.
7. Run the following command:

```
# touch /var/pwnplug/script_configs/sms_message_config.sh
```

Update the Pwn Plug to patch 1.1.3

To update the Pwn Plug to patch 1.1.3 please refer to the *Pwn Plug Academic Edition Update Guide*.