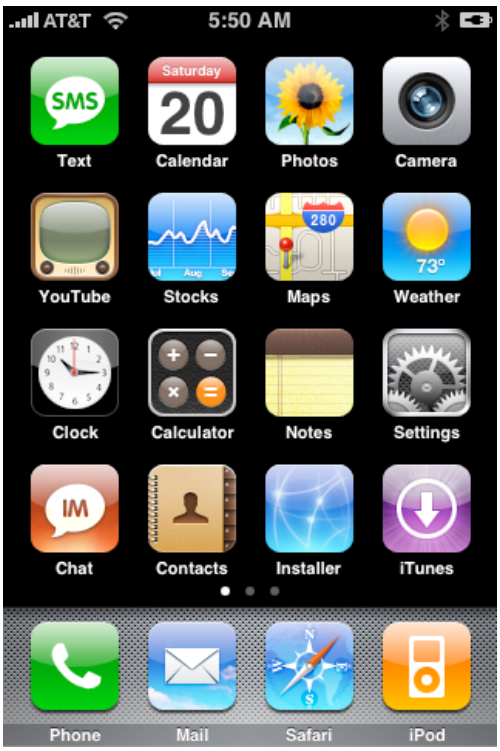
# mercurious.com presents

# How to install AppTapp 3.0 beta into iPhone 1.1.1 in 50 meticulous steps without any command-line.

**For AT&T, MacIntel, OS X 10.4.10, iTunes 7.4.2, iPhone 1.1.1 and 1.0.2 firmware users only.**




**Notes and Warnings**

1. Do not install both Trip1PogoStick and SummerBoard on 1.1.1 — you'll get startup freeze (stuck on Apple logo), especially if you've used previous 1.1.1. upgrade methods, including iNdepenence 1.2.2. and/or Trip1Prepz. We made this mistake and that's what inspired us to start fresh and document every step for you. Use iTunes to restore to a fresh 1.1.1 state if this occurs.

2. Do not install the 1.1.1 tweaks with SummerBoard. They are not compatible SummerBoard and Customize and will screw up your Springboard forcing to to restore to 1.1.1 and then start the 50 step process all over again. We attempted this and ended up with a blank Springboard, no icons, and no phone functionality. The closest we've come to a brick, yet, in all our of hacking tests.

3. Do not follow any of these steps and discard this document immediately if you are not prepared to void your warranty and any obligation of Apple or AT&T to support you in these endeavors. They have clearly stated that these modifications are in violation of their use agreements. In fact, it is not yet easy to even truly make a factory fresh iPhone, without any trace of third-party modifications, in the event that

you might want to return your device. Although using third-party applications is far less risky than unlocking your firmware to run on other networks beyond AT&T, it's still considered an unauthorized activity. No warranties are implied by these instructions. You follow these steps at your own risk as assume all liabilities herein. If you have any reservations about these activities, delete this document and forget about iPhone modding. We have no responsibility for your actions and provide this information for academic research purposes only.

**Downloads**

Prepare by downloading these files first. Newer versions of iNdependence and AppTapp may be available since this was written, perhaps rendering this guide obsolete.

1. *iNdepedence 1.2.4*
   http://independence.googlecode.com/files/iNdependence_v1.2.4.dmg

2. *iPhone 1.0.2 firmware*
   http://appldnld.apple.com.edgesuite.net/content.info.apple.com/iPhone/061-3823.20070821.vormd/iPhone1,1_1.0.2_1C28_Restore.ipsw

   - You'll need two versions of this firmware
     - An unzipped folder version
       1. Duplicate the .ipsw file or .zip file, depending on how your browser downloaded it.
       2. Make sure the file ends with .zip, and unzip the file, which will result in a folder
     - An .ipsw version
       1. Simply change the .zip extension back to .ipsw if your browser changes it as a result of the download.
       2. Otherwise, leave the .ipsw extension.

3. *Nullriver AppTapp 3.1*
   http://www.nullriver.com/~zigzag/AppTappInstaller.zip

**Downgrade**

If you've upgraded to iPhone 1.1.1 for any reason, or bought an iPhone recently which already came as version 1.1.1, you'll need to go back down to 1.0.2 to exploit the new jailbreak and AppTapp method. You'll encounter an expected error, that relates to the modem firmware not being downgradable. This is an expected result, and you'll be returning to 1.1.1 at the end of the process, so all will be in order. In any case, you should begin the process with a fully functional AT&T activated iPhone. Perform a restore to 1.1.1 with iTunes before starting if you have any doubts.

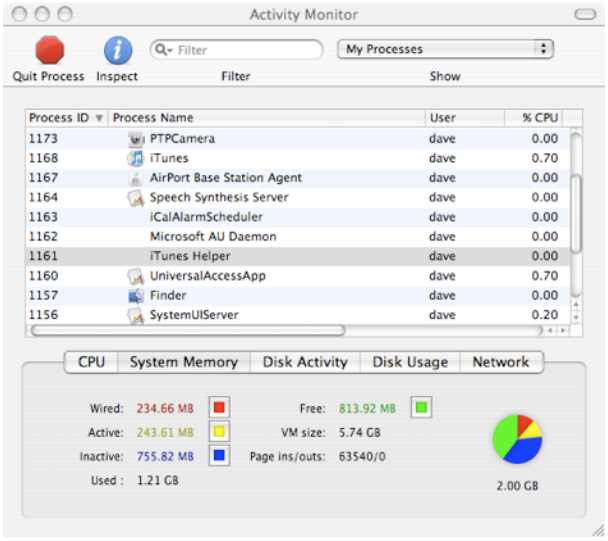
4. Sync iPhone with iTunes

5. Disable your media sync (ringtones, music, podcasts, video) to save time on the many rebuilds you're about to perform. Keep your info tab synced, in case you need to use your

phone at any point during this process, as long as it's activated.

6. Sync iPhone with iTunes again (to establish restore point) and then quit iTunes.

7. Use Activity Monitor (Applications/Utilities) to quit the iTunes Helper process.




8. Launch iNdependence 1.2.4 and choose Firmware tab, and then click "Enter DFU Mode"


9. Locate iPhone 1.0.2 firmware unzipped folder "iPhone1,1_1.0.2_1C28_Restore", not the .ipsw file.

10. If you get an error going into recovery mode (a very common issue, expect it to happen), restart iNdependence and try again. It will work the second time.

11. Quit iNdependence after confirming recovery mode message (iPhone screen will show graphic of USB dock plug and iTunes icon)

12. Launch iTunes, which will recognize iPhone in recovery mode. Click OK in iTunes to dismiss the recovery mode message.

13. Hold down Option while clicking Restore

14. Locate iPhone 1.0.2 .ipsw file “iPhone1,1_1.0.2_1C28_Restore.ipsw”

15. After the restore iTunes will return an unknown error (1013). This is expected, and not a problem. iTunes will still insist the phone is in recovery mode. Ignore the errors and quit iTunes.



16. Turn off your iPhone by holding down the sleep button, and then turn it back on. If iTunes auto-launches, it means your iTunes Helper process needs to be killed with Activity Monitor. If your iPhone stays in Recovery Mode, reboot it, launch iNdependence and click through the tabs, and just be patient. Your iPhone will snap out of recovery mode and go into Activation Mode. Quit iNdependence if necessary.

17. Launch iTunes and allow the iPhone to be reactivated and the backup and sync to perform. This should be relatively quick if you’ve disabled your media in the first few steps. If the media insists on syncing, you can safely cancel it, un-check music, video, podcasts, etc., and apply the changes. Sync one more time for good measure. You’ll notice the iPhone is in the 1.0.2 state. You might be prompted to re-enter your voicemail password.

18. Quit iTunes. Reboot iPhone.

19. Launch the AppTapp Installer program (on your Mac, not to be confused with the one on your iPhone) and install it for firmware 1.0.2 since that’s the current state of your iPhone.



20. After AppTapp Installer installation is complete, select your WiFi network via iPhone Settings and re-input the password, as needed.

21. Launch Installer on iPhone and allow it load and refresh its packages. Resist the temptation to update Installer (version 3.0b3). We'll get to that later. It may seem useless that we went through this step, but it helped us get out of the Recovery Mode, verified the downgrade, and provided an easy jailbreak in 1.0.2 mode.

**Install SSH**

22. Launch iNdependence. iPhone should be connected, indicated firmware 1.0.2, be activated, have an AFC connection and be jailbroken. Click "SSH" tab. Click "Install SSH/SFTP/SCP" button. Follow the onscreen instructions for the reboot process.


23. Change your SSH root password. The default password “dottie” is widely known. Click “Change Password” and change it for the root account to something secure you’ll remember and use. Enter “root” for account name and then enter and confirm your new password.

24. Make sure you’re connected to your WiFi network. Click Settings > WiFi > blue arrow next to network name and note your IP address.

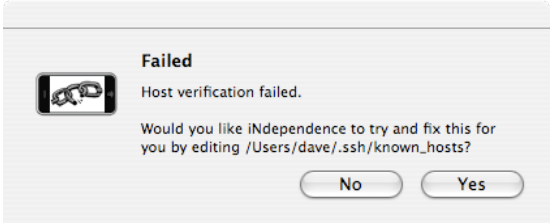
**Prepare for 1.1.1**

25. In iNdependence, click “Firmware” tab and then click “Pre 1.1.1 Upgrade” and then enter your iPhone’s IP address from noted from the previous step, as well as your new root password.

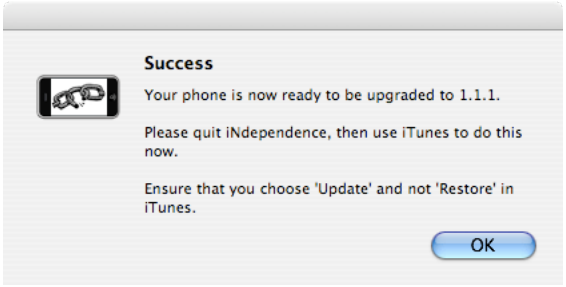
26. You’ll be instructed by iNdependence to launch iTunes which will probably perform a sync.

27. Return to iNdependence and click “OK” and you’ll see the Performing Pre 1.1.1 Upgrade process status window.

28. You’ll likely get a message saying the Host Verification failed if you’ve ever installed SSH on your iPhone previous. Click “Yes” to reset your SSH hosts and resolve this problem.



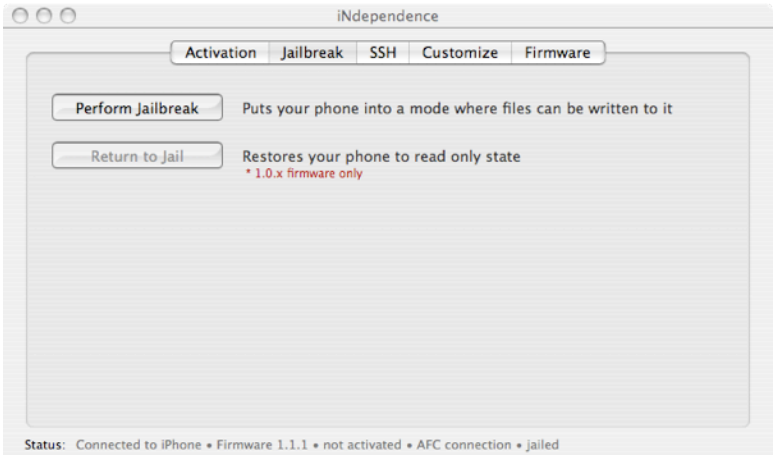

29. You should get a Success message from iNdependence. Follow the instructions to quit and then use iTunes to Update (not Restore).




30. After the restore is complete, iPhone will need to be reactivated, but iTunes won't recognize it. This is normal. Quit iTunes.

**Jaillbreak 1.1.1**

31. Open iNdependence. The status should read "Connected to iPhone • Firmware 1.1.1 • not activated • AFC connection • jailed" and click "Jailbreak" and "Perform Jailbreak" button. Don't use iNdependence to Activate your iPhone. If you're an AT&T customer, you should use iTunes for activation only. This feature is for users who unlock their iPhones for use on other networks.




32. Wait for jailbreak and follow onscreen reboot instructions, awaiting Success message.

**Install SSH (again)**

33. Click "SSH" tab and "Install SSH/SFTP/SCP" and then follow onscreen reboot procedure.


34. Change SSH password again, as in step #23.

**Install AppTapp Installer**

35. Locate the AppTapp Installer on your Mac in the Finder. Right-click (or control-click) and choose “Show package contents”

36. Navigate to “Contents/Resources/”

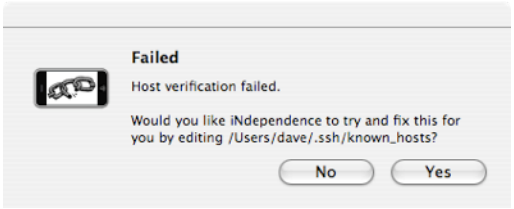
37. In iNdependence, click “Customize” tab

38. Navigate to “Applications/System”

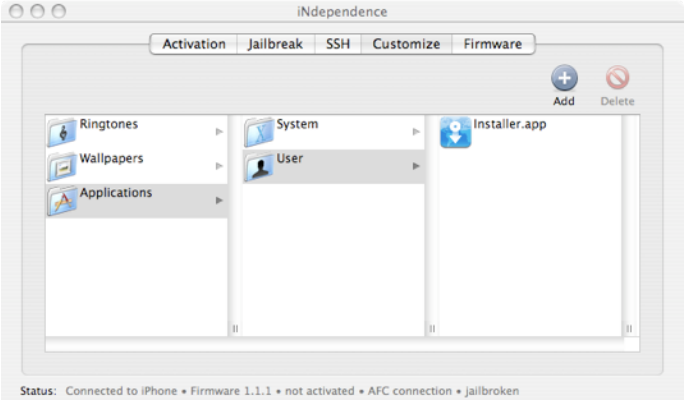
39. Drag and drop the “Installer” file from the package you opened within the Finder (in step #35-36) into iNdepdence’s System Applications column. A green + icon should appear on the cursor if all is well. Use the “+ Add” button, and locate the Installer file as an alternative.

40. Enter your iPhone’s IP address and new root password.

41. Click “Yes” if you get the Host Verification Failed message regarding the fix for known hosts.




42. The Installer.app will appear in the User applications. This is OK.




43. Quit iNdpendence.

**Activate iPhone in iTunes**

44. Launch iTunes.

45. iTunes should activate iPhone for AT&T.

46. Launch YouTube and iTunes WiFi Music Store to confirm they're activated properly. Scroll to the bottom of the iTunes WiFi Music Store to verify that your Apple ID is associated. If you had used iNdependence to activate your iPhone, these two features would probably not work without further steps.

**Update AppTapp Installer to 3.0 beta**

47. Tap Installer on iPhone and allow it refresh its packages.

48. Tap the Installer version 3.0b3 (or later) and Update. Restart by tapping OK and then clicking the Home button.

49. Tap the Installer and start to install third-party applications, especially the Community Sources, the BSD Subsystem, etc.

50. Re-sync your iTunes media by re-checking the Music, Podcasts, and Video, as needed. You are finally done restoring, updating and re-syncing and rebooting your iPhone.

**Optional Steps**
Explained in far less detail, here are interesting next steps, now that you're more comfortable with iPhone 1.1.1 modifications.

1. Install **SummerBoard**. This allows you to scroll the SpringBoard, apply themes and do many other special customizations, including download the numerous Summerboard themes available on AppTapp Installer. It's more customizable than Trip1PogoStick which also allows the page scrolling of the SpringBoard home screen. Avoid the 1.1.1 tweaks called iPod2 and iPod3 like The Plague. They are not compatible with SummerBoard or Customize and will force to you to start the whole process over.

2. Install **Customize**. This allows you to reorder the icons on the SpringBoard, as well as change all kinds of graphics and sounds available on AppTapp Installer. At this time of this writing, Customize was still buggy with 1.1.1 even though the author denies it. It did launch without crashing, eventually, after several restarts. Its rSBT feature allows the icon re-ordering. Try moving the icons you want on the first screen into the main SpringBoard after choosing 16 icons in the Settings tab. Then, drag the icons into the Extended SpringBoard that you want to appear in the secondary SpringBoard "pages."

3. Install **NES**. You'll need to obtain game ROMs and use an SFTP program like CyberDuck to login to your iPhone via its IP address and copy the ROM files to /var/root/Media/ROMs/NES/

4. Install a **chat program**. MobileChat looks most like iChat, while Apollo allows you to login into multiple chat networks simultaneously. It's great having two solid IM programs to choose from.

5. Install some **eBooks**. Some great free literature is appearing all the time thanks to AppTapp.

**Glossary**
The arcane terms of iPhone modding translated into plain English.

*command-line*
Text-based control of a computer, without the modern graphical user interface, generally mouse, icon and menu based interactions. Experts tend to enjoy being able to control a computer from the command-line, while intermediate and beginner users tend to stick to graphical interfaces.

*jailbreak*
Apple ships the iPhone and iPod touch with their file systems locked to prevent modifications. This technique modifies the UNIX filesystem to allow system read and write. This is one of the key efforts of the iPhone DevTeam and venerated as a continued accomplishment despite the best efforts of Apple's developers to thwart this type of access. The command-line tool iPHUC is generally what runs behind the scenes when GUI tools modify iPhone.

*SpringBoard*
The technical name for the iPhone and iPod touch home screen, comprised of the grid of native application icons. *SummerBoard* is the unauthorized modification of SpringBoard that allows it to be extended with additional icons, themes and other custom features.

*firmware*
iPhone comprises a flash memory hard disk and re-writable chips. The firmware chips that control the radio, modem and other hardware features of the device can be updated at the time of iPhone software updates. Some firmware updates (such as the modem) cannot be reversed, downgraded.

*Trip1PogoStick*
An early variation of SummerBoard, less developed, featured, but first to emerge as the compatible means to modify the 1.1.1 SpringBoard, hard-coded by Apple to thwart modification.

*Trip1Prepz*
An early variation of the tool provided by iNdependence which exploit the use of a symlink, or UNIX alias (Mac speak) or shortcut (Windows speak) to reference direction location, in order to modify the update process from 1.0.2 to 1.1.1

*SSH*
A secure remote file access protocol, usually built-in to UNIX, removed by Apple, which allows login and file transfer access over the Internet. Allows you to login to iPhone, browse, transfer, and modify files in standard interfaces, such any SFTP program.

**Acknowledgments**
Various contributors helped make every aspect of the iPhone customizing community possible. They include the original team of hackers who released the basic exploits, subsequent programmers and luminaries, and native application developers. Rather than list specific names, we offer a collective praise to the community at-large. The actual names of contributors can easily be retrieved via web search.

**Final Disclaimer**
This document was generated by trial and error from a fellow enthusiast. There could be faulty information and research described in this document. The author acknowledges that the information is likely to become obsolete, and thus, deprecated, shortly after publishing, due to software updates, improvements and further lock-downs and hacks.