

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Bypass Safetynet on MM with Custom ROM & Kernel](#)

Kotlin - January 8, 2017, 2:23 pm

(Please note that I am not responsible if your phone bricks etc. Myself and others who have also tested this bypass have had no reported issues of this bypass causing some sort of brick etc., but I cannot guarantee anything.)

Sorry for the semi-unorganized thread, will clean it up as soon as I can.

Since October 2016, Google has (yet again) changed their way on how SafetyNet works and how they can now easily figure out if your phone is rooted or not. This caused many issues for rooted Android users who wanted to play games such as PKMNGO and use apps such as Snapchat. However, there is still ways to bypass SafetyNet.

Tested Devices:

- Samsung Galaxy S6
- Samsung Galaxy S5

Looking for people with other devices to try and see if it works for themselves so I can add the device to the list.

Requirements:

- Basic Understanding on how to use Custom Recovery, flashing zip files etc.
- Running on Android 6.0 (Looking for anyone with Android 7 to see if this works for them as well.)
- Phone has a custom recovery (I suggest TWRP) and on a Custom ROM. (Stock roms "should" work too.)
- Rom should have November 1st Security update or older updates. (Have not tested with roms with November 5th Security update and higher.)
- [Magisk V10.2 & Magisk Manager 3.0](#)
- [SafetyNet Checker](#)
- Phh Super User APK. [PlayStore](#) or [2.0 Beta](#)
- Root File Explorer. I suggest [Root Browser](#)
- [Kernel Adiutor](#)
- [Root Checker](#)

Tutorial

WARNING: BIG IMAGES (Had no time to resize them, but will soon.)

Before we begin, I suggest that you make a Nandroid backup through your preferred Custom Recovery. I suggest you use TWRP however CWM "should" work, but I have not tried myself.

Step 1:

Clean Install

The first step 'is' optional, however it is recommended that you do a clean install. I will be using [Alexis Rom 8.0 Beta 2](#) for my Galaxy S6, but any rom should work. (Other than certain GraceUX ports, but am able to get it to work with other ported rom like CoreUi (a MIUI port) for the Galaxy

S6). You should also flash a kernel now as well. I use to personally use Arter97 as SuperSU is not installed in this kernel, however Arter97 is slowly starting to become unstable as it hasn't been updated and there is better kernels out there. For this tutorial, I will be using [Twisted Kernel](#).

Step 2: Removing SuperSU

This step is 'also' optional, but ONLY if your rom/kernel does not automatically install SuperSU for you. In my case, it is automatically installed.

What you will need to do is to go to the SuperSU app, go to settings.

Spoiler ([Click to View](#))

Scroll down until you see "Full unroot" and click it.

A popup will come up and click "Continue", then followed by another popup and click "NO".

Spoiler ([Click to View](#))

Once you click no, your phone will freeze and then reboot. You should then install Root Checker to verify if your phone is unrooted.

Spoiler ([Click to View](#))

(If for some reason, you are unable to use the SuperSU app but you know SuperSU is installed, I'd suggest you download [UPDATE-unSU-signed.zip](#) and flash it as it will manually remove SuperSU.)

Step 3: Installing required APKs.

You will now need to install MagiskManager 3.0, SafetyNet Helper Sample, PHH Super User APK, Root Browser and Kernel Adiutor.

Spoiler ([Click to View](#))

Step 4: Flashing MagiskV10.2

You will need to reboot into your custom recovery and flash "Magisk-v10.2.zip", followed by rebooting. If you receive ERROR: 1 in TWRP when it is trying to mount SU, I suggest reflashing a kernel (and re-remove SuperSU), uninstalling Magisk with MagiskUninstaller (in [Magisk thread](#)) and reinstall Magisk V10.2, or reinstalling your rom.

Once you have flashed the file, reboot into System and open Magisk Manager to verify you have installed Magisk. A little pop up will open to allow Magisk to have root. Make sure to click allow and set it so it has root for "Forever".

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

If it states that root isn't properly installed, manually flash [PHH Super User V266-2](#).

Step 5: Enabling Magisk Hide

In Magisk Manager, go to the side menu and go to "Settings." You will see an unchecked box that says "Enable Magisk Hide." Select it and reboot. Re-open Magisk Manager and verify that it is now

check marked. If the App crashes when you select "Enable Magisk Hide", reboot your phone and retry.

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

Step 6:

Set Permissions

In Root Browser, go to the directory `/sys/fs/selinux` and find the file "enforce" and the file "policy". On the file "enforce", change the permissions of the file from "644" to "640", and for the file "enforce", change the permissions of the file from "444" to "440". If Phh Super User pops up and asks for root access, click "Allow."

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

Once you are done, open up SafetyNet Helper Sample and it 'should' pass. If you are getting "Response Validation Failed" and the background is blue, uninstall Magisk by flashing Magisk Uninstaller, flash UPDATE-unSU-signed.zip, then reflash Magisk V10.2. Then, go back to Step 5 and enable Magisk Hide.

Spoiler ([Click to View](#))

Step 7:

Use Kernel Adiutor to automatically set permissions in init.d

This last step is 'optional', however it automates the permission setting as every time you reboot your system, the file permissions will reset. Open up Kernel Adiutor, go to the sidebar and scroll down until you see 'Init.d'. Click it and make sure "Emulate Init.d" is enabled.

Then click the plus button, set the name to "Permissions" and then add the following script:

`"chmod 640 /sys/fs/selinux/enforce"` and `"chmod 440 /sys/fs/selinux/policy"` and save the files.

Also allow root access to Kernel Adiutor!

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))

Step 8:

Reboot

Reboot your device, let Kernel Adiutor do its countdown (you will see in the notifications drop down) and once it says "Applying settings completed!", open up Safetynet and you should be passing!

Credits:

Can't forget those credits

topjohnwu - Main developer of Magisk and Magisk Supported Phh Super User

[This XDA thread](#) - Helped me figure out how to do this bypass in the first place.

CoreUi Telegram Chat - Helped me test this bypass to see if it worked on different S6 models. Join [here!](#)

If there is any mistakes I made, spelling, phrasing etc., please tell me so I can fix it. Thanks.

Aveling - January 8, 2017, 2:31 pm

Great detailed tutorial, I hope that this will help a lot of people with getting Android Pay to work on their (pre) rooted devices. (It also allows you to play Pokemon Go on a rooted device!)

Kotlin - January 8, 2017, 2:33 pm

(Jan 8, 2017 03:31 PM)Aveling Wrote: [\[CITE\]](#) Great detailed tutorial, I hope that this will help a lot of people with getting Android Pay to work on their (pre) rooted devices. (It also allows you to play Pokemon Go on a rooted device!)

Thanks. I haven't tried Android Pay as it is not available in Canada yet (I think), but I have been told that Pokemon Go DOES work from people in the Telegram group I posted at the bottom.

SIM-3420445 - January 9, 2017, 1:55 am

Thanks for the share OP, gonna check it

Kotlin - January 9, 2017, 1:15 pm

(Jan 9, 2017 02:55 AM)Triangulum Wrote: [\[CITE\]](#) Thanks for the share OP, gonna check it Great, if it works; tell me what phone you have so I can add it to the supported device list.

Red Bull™ - January 16, 2017, 2:30 pm

Confirmed NON-Working on the OnePlus3 android N. Tested on Freedom OS 2.1.1 and Oxygen OS 4.0.1.

Best of luck for the others. Hope to find a solution soon, need my snapchat.