

Tab 1

Sideloading



Sideloading

by: [u/devx7sui](#)



Created by: [u/devx7sui](#)

Discord: justindoritos

Table of Contents:

Introduction.....	2
Vocabulary/Terms.....	2
Restrictions on Sideloading.....	3
How do I sideload?.....	3
TrollStore Installation.....	5
TrollHelperOTA.....	5
TrollInstallerX.....	6
TrollHelper.....	7
TrollMisaka.....	8
TrollRestore.....	9
TrollInstallerMDC.....	10
TrollStore Lite.....	11
Enterprise Certificates.....	11
ESign.....	12
ESign Coretrust Bug.....	12
Scarlet.....	12
FlekSt0re.....	13
Developer Account.....	14
Sideloadly.....	14
AltStore.....	14
Windows.....	14
MacOS.....	15
Other.....	15

Appsync Unified.....	15
Error Fixing.....	16
DNS-Anti Revoke.....	16
Custom DNS.....	16
Questions/Concerns.....	17
Credit.....	18

Introduction

Sideloaded is a way of installing third party apps outside of the App Store. However, Apple tries to restrict this as much as possible. Learn how to install the apps without Apple's restrictions & bypass them.

Although sideloading can be used on most modern iOS versions & some legacy, old tools such as Cydia Impactor have to be used for some old iOS versions.

Vocabulary/Terms

Certificate - Almost like a passport to install apps. They can be expired by Apple, and you can also get blacklisted sometimes.

Enterprise Certificate - Used by companies, to distribute apps to LOTS of devices with no limit. However, this is often misused by people to install any .ipa they want.

Coretrust Bug - A coretrust bug was a certificate invalidation error in iOS 14 - 16.6.1 & 17, and it can install apps by bypassing app signature checks. This also allows any entitlement to work.

.ipa - A .ipa file is a file which is pretty much just an app in a file format. This is used to install apps often.

Blacklisted - Sometimes, Apple will prevent you from using the certificate if being misused. It will display an error message when trying to open an app.

Revoked - Enterprise Certificates are strictly meant for corporate apps. If being misused, it will display an error message when trying to open an app.

Restrictions on Sideloaded

Using Apple's Developer Account, a free account only allows the use of three sideloaded apps, and they expire every 7 days and need to be installed every time the 7 days has passed. For paid developer accounts, you can sign as many apps as you want, and they will expire in a year. You can also use up to 100 devices for one account. However, it costs \$99 yearly.

Using Enterprise Certificates, there is a chance you can get blacklisted which is hard to whitelist yourself back. Sometimes, if Apple finds out if you are misusing certificates, all users using the certificate will get revoked & will no longer be usable in the future.

How do I sideload?

This table below will calculate which method of sideloading works best for you! Yes, other methods exist, but I only post the most reliable and best ones.

Find out your iOS Version, and whether your device is ARM64 or ARM64e.

Find your iOS Version: Open Settings > General > About. Your iOS version should be there.

To determine your device is ARM64 or ARM64e:

The following devices below are ARM64:

iPad 7th Gen & below (A10)
iPad Air 2nd Gen & below (A8X)
iPad Pro 2nd Gen & below
iPhone X & below (A11)

^ If your device is younger than these devices or is exactly, your device is ARM64.

The following devices below are ARM64e:

iPad 8th Gen & above
iPad Air 3rd Gen & above
iPad Pro 3rd Gen & above
iPhone XR, XS & above
iPhone 11 & above
iPhone SE 2nd gen & above

^If your device is older than these devices or exactly, your device is ARM64e.

iOS Version From	iOS Version To	ARM64 (A8)	ARM64 (A9 - A11)	ARM64e (A12+, M1+)
7	13.7	Appsync Unified		
14.0.1 beta 2	14.8.1	TrollInstallerX	TrollInstallerX	TrollHelperOTA
15	15.5 beta 4	TrollHelperOTA		
15.5	15.5	TrollInstallerMDC	TrollInstallerX	TrollHelperOTA
15.7	15.7.1	TrollInstallerMDC	TrollInstallerX	
15.7.2	15.8.3	TrollMisaka/TrollHelper	TrollInstallerX	TrollInstallerX
16 beta 1	16 beta 3	ESign	TrollInstallerX	TrollHelperOTA
16 beta 4	16.6.1	ESign	TrollInstallerX	TrollInstallerX
16.7 RC	16.7 RC	ESign	TrollRestore	TrollRestore
16.7	16.7.10	ESign		
17.0 beta 1	17.0 beta 4	ESign	TrollInstallerX	TrollRestore
17.0 beta 5	17.0	TrollHelper	TrollRestore	TrollRestore
17.0.1	18.1	TrollStore Lite	TrollStore Lite	ESign
		THE REST OF THIS TABLE IS EMPTY TO PRESERVE FOR OTHER NEW VERSIONS & SIDELOADERS.		

TrollStore Installation

TrollHelperOTA

TrollHelperOTA is a TrollStore installer for iOS 15 - 16, with some exceptions.

1. Paste this link into Safari:
`itms-services://?action=download-manifest&url=https://jailbreaks.app/cdn/plists/TrollHelper.plist`
2. When prompted to install an app, click it.
3. Once finished installed, there is an app called "GTA Car Tracker". This is just the TrollStore Helper app.
4. Open it and click "Install TrollStore".
5. Your device should respring, and a new app called "TrollStore" should be on your home screen.

TrollInstallerX

TrollInstallerX is a TrollStore installer for iOS 14 - 16.6.1, with some exceptions.

Requirements:

- A computer with Windows or MacOS
- A lightning cable

Right now, <https://jailbreaks.app> currently has TrollInstallerX signed. Click on it, and go to TrollInstallerX, and click Install.

Sideloadling the App using Sideloadly

1. Install the latest version of Sideloadly
2. Install the latest version of iTunes and iCloud (On Windows, do not install from the Microsoft Store. Instead, get it from Apple's website)
3. Obtain the latest .ipa of TrollInstallerX.
(<https://github.com/alfiecg24/TrollInstallerX/releases/tag/1.0.3>)
4. Open the app on your computer.
5. Connect your device to a computer.
6. Drag or drop the .ipa into the box.
7. Login to your Apple ID. This is used to install the app and the username & password will NOT be sent to Sideloadly's servers and will only be sent to Apple.

8. The app should be on your home screen.

On iOS 16+, you need to enable developer mode. To do so, open Settings > Privacy & Security, scroll to the bottom and click Developer Mode.

Installing TrollStore

1. Open the app.
2. Click "Install TrollStore".

If your device is stuck on "Exploiting Kernel", reboot your device.

3. When prompted to register a system app with TrollStore, do a random one you care about the least.
4. Once the process is done, open the system app you registered as TrollStore, and click "Install TrollStore".
5. Your device should respring, and a new app called "TrollStore" should be on your home screen.

TrollHelper

TrollHelper is a TrollStore installer for iOS 14 - 16.6.1 & 17. It requires a jailbreak to run.

If your device requires TrollMisaka, it is recommended you jailbreak your device, then install TrollStore Helper while jailbroken. Then, register an app as a persistence helper, then unjailbreak.

Requirements:

- A computer with Linux or MacOS (ARM64 only)
- A lightning cable (MUST be USB-A to Lightning or USB-C) (ARM64 only)
- A functioning package manager
- A jailbroken device running iOS 14 - 16.6.1 & 17

Installing TrollStore

1. Open the package manager (Sileo or Zebra)
2. Make sure you have have "<https://havoc.app>" added as a source
3. Search "TrollStore Helper"
4. Install the package
5. Once installed, a device called "TrollHelper" will appear
6. Open it, and click "Install TrollStore"
7. Your device should respring, and a new app called "TrollStore" should be on your home screen.

Registering a Persistence Helper

On iOS 14, this is not required. Otherwise, you need to do so in order to access TrollStore in a non-jailbroken state.

1. Open TrollStore
2. On the bottom bar, click Settings
3. Click on "Register Persistence Helper"
4. Select a system app you don't care about. (Example: Tips)

TrollMisaka

TrollMisaka is a TrollStore Installer for iOS 14 - 15.8.2.

Please note that TrollMisaka is heavily unreliable due to a low success rate. Some people prefer to jailbreak to install TrollStore, and it is advised you do so too using the "TrollHelper" installation vector.

Requirements:

- A computer with Windows or MacOS
- A lighting cable

Sideload the app using Sideloadly

1. Install the latest version of Sideloadly
2. Install the latest version of iTunes and iCloud (On Windows, do not install from the Microsoft Store. Instead, get it from Apple's website)
3. Obtain the latest .ipa of TrollMisaka
4. [.\(https://github.com/straight-tamago/TrollMisaka/releases/tag/2.0-Beta\)](https://github.com/straight-tamago/TrollMisaka/releases/tag/2.0-Beta)
5. Open the app on your computer.
6. Connect your device to a computer.
7. Drag or drop the .ipa into the box.

8. Login to your Apple ID. This is used to install the app and the username & password will NOT be sent to Sideloadly's servers and will only be sent to Apple.
9. The app should be on your home screen.

On iOS 16+, you need to enable developer mode. To do so, open Settings > Privacy & Security, scroll to the bottom and click Developer Mode.

These next steps may take a couple tries to complete.

Installing TrollStore

1. Open the app. Do not close it
2. Open Settings > General > Keyboard > Keyboards > Add New Keyboard
3. Click on TrollMisaka. Allow full access
4. Reopen TrollMisaka and reboot your device

Injecting TrollStore

1. Unlock your device
2. Open spotlight search immediately
3. Tap on the globe icon and switch to TrollMisaka
4. Tap kopen
5. Tap Install TrollStore

If the keyboard app refreshes, try again.

Installing

1. Reopen TrollMisaka from the app switcher
2. Open it and click Install TrollStore

TrollRestore

TrollRestore is a TrollStore installer for iOS 15.2 - 16.7 RC (20H18) and 17.

Requirements:

- A computer with Windows, MacOS or Linux
- Latest version of iTunes
- Latest version of python3
- A lightning cable

Before proceeding, please disable Find My. After TrollStore has been installed, feel free to turn on Find My.

Running the application

1. On your computer, go to <https://github.com/JJTech0130/TrollRestore/releases/tag/1.0> and find the version that corresponds with your computer OS
2. Connect your iOS device into the computer
3. Run the application. You may need to unzip files if compressed
4. If asked to replace a system app with a TrollStore binary, type in the app name. For example, "Tips". Type in an app you do not care about.

Your device should reboot soon with the TrollStore Binary installed.

Installing TrollStore

1. Open the app you selected as a TrollStore Binary
2. Click "Install TrollStore"
3. Your device should respring, and a new app called "TrollStore" should be on your home screen.

TrollInstallerMDC

TrollInstallerMDC is a TrollStore installer for iOS 15 - 16.1.2.

Requirements:

- A computer with Windows or MacOS
- A lightning cable

Sideload the app using Sideloadly

1. Install the latest version of Sideloadly
2. Install the latest version of iTunes and iCloud (On Windows, do not install from the Microsoft Store. Instead, get it from Apple's website)
3. Obtain the latest .ipa of TrollInstallerMDC
4. (.<https://dhinakg.github.io/apps.html>)
5. Open the app on your computer.
6. Connect your device to a computer.
7. Drag or drop the .ipa into the box.
8. Login to your Apple ID. This is used to install the app and the username & password will NOT be sent to Sideloadly's servers and will only be sent to Apple.
9. The app should be on your home screen.

On iOS 16+, you need to enable developer mode. To do so, open Settings > Privacy & Security, scroll to the bottom and click Developer Mode.

Injecting TrollStore Helper

1. Open TrollInstallerMDC
2. When opened, it should say "Successfully replaced Tips binary"
3. Leave the app

Installing TrollStore

1. Open the Tips app
2. Click "Install TrollStore"
3. Your device should respring, and a new app called "TrollStore" should be on your home screen.

TrollStore Lite

TrollStore Lite is a sideloader for iOS 14 to the latest version of iOS.

Although similar to TrollStore, this requires a jailbreak to run & install TrollStore Lite. If your device becomes non jailbroken or is in a stock iOS state, TrollStore Lite will no longer function & will not open. You need to re-jailbreak every time.

On iOS 17.0.1+ - Requires palera1n to run

On iOS 14 - Requires Taurine or unc0ver

On iOS 15/16.6.1 - Requires Dopamine

If you have access to normal TrollStore, please use that.

Requirements:

- A functioning package manager
 - A jailbroken device
1. Open your package manager
 2. Make sure you have <https://havoc.app> in your sources
 3. Search "TrollStore Lite"
 4. Find it & click install

Enterprise Certificates

Sideloaders that use Enterprise Certificates to sign apps.

ESign

ESign is a sideloader that uses enterprise certificates & a DNS server method to sign apps without Apple revoking them on iOS 12+. You can also import your own certificate to sign apps. (The one we will be installing uses enterprise certificates)

There are lots of ESign versions, where one uses the coretrust bug to sign apps, and some require certificates. The one we use is the certificate one.

Installing ESign

1. Open this URL: <https://khoindvn.io.vn/>
2. Near the top of the page, there should be two white boxes that lead to URL's and downloads. Click the one that says "Download Esign Certificate"
3. Scroll down until you find the "ESign Bypass Revoke". Some may be revoked, keep doing them until you find one that works
4. When prompted, install the app
5. Open the app (Trust the enterprise certificate in Settings).
6. In files (in ESign), import the .zip file you previously downloaded
7. Unzip the package by clicking on it
8. The contents will lead to certificates with the files ending in ".esigncert". Click on the file and import it to Certificate Management.

Signing the App

1. Get the .ipa you want to install.
2. Import it to the files section of ESign
3. Tap on it and click "Import to App Library"
4. Once the app finished installing, go to Apps, head to Unsigned, and find the app you have just installed, and click "Signature".

5. Select the certificate (if you imported more than one), click “Signature”.
6. After signing, you will get a prompt to install another app. Click “Install”

DNS-Anti Revoke

A DNS Anti-Revoke will bypass Apple’s revoke message & blacklist, which will allow apps to open & function even if it is revoked.

There are some known issues with using this DNS method. Such as failing to log in, websites are blocked or may not appear as normal, and more. In some certain scenarios, the DNS-method may fail, making you revoked or blacklisted.

Some users may prefer to create their own DNS for privacy reasons, in which on this document you can scroll to the “DNS Anti-Revoke” section.

1. Open this URL into your browser:
<https://raw.githubusercontent.com/toasty-dev/Khomod/main/khomod.mobileconfig>
2. Install the configuration profile and follow the on-screen instructions

ESign Coretrust Bug

Similar to TrollStore, ESign is a sideloader that uses the coretrust bug to sideload apps on iOS 14 - 15.6 beta 1.

ESign might be preferred over TrollStore, as it can change app names, bundle ID, app icon, along with a repo reader & more. ESign is less user friendly but packed with more features.

1. Visit <https://esign.yyyue.xyz/>
2. Check the table to see which device is compatible
3. Find the one and use the one that works for your device

Installing ESign

An app called JetSign will appear. Open it and click “Install ESign”.

Scarlet

Scarlet is a sideloader that uses enterprise certificates to sign apps.

Scarlet is known to have many often revokes & the website has lots of ads. Please do not click on them, and if you get a new tab opened, just close it and move on.

Installing Scarlet

1. Visit <https://usescarlet.com>
2. Scroll to the bottom & click "Install"
3. If prompted to another tab, close it and click "Install" again
4. There are many options to install Scarlet, click the top one that says "Direct Install".
5. Again, if prompted to another tab, close it & click the same button
6. If you get a prompt to install, install it

Extra Steps

1. Open Settings > General and scroll to the bottom to VPN & Device Management.
Allow the enterprise certificate to be trusted.

DNS Anti-Revoke

A DNS Anti-Revoke will bypass Apple's revoke message & blacklist, which will allow apps to open & function even if it is revoked.

There are some known issues with using this DNS method. Such as failing to log in, websites are blocked or may not appear as normal, and more. In some certain scenarios, the DNS-method may fail, making you revoked or blacklisted.

Some users may prefer to create their own DNS for privacy reasons, in which on this document you can scroll to the "DNS Anti-Revoke" section.

3. Open this URL into your browser:
<https://raw.githubusercontent.com/toasty-dev/Khomod/main/khomod.mobileconfig>
4. Install the configuration profile and follow the on-screen instructions

FlekSt0re

FlekSt0re is a sideloader that uses imported certificates to sign apps.

You will need to purchase(or have) a certificate or be a part of the Apple Developer Program in order to install apps.

1. In Safari, visit <https://flekstore.com>
2. Tap Get
3. Once visited to a website where it states to add it to your home screen, click the share button near the top and click Add to Home Screen.

Developer Account

All apps need to be renewed every 7 days and you can only install 3 apps at a time.

On Developer Accounts, you can install as many apps as you want, and you need to renew every 365 days.

Sideloadly

Sideloadly is a sideloader that uses developer accounts to sideload apps on Windows 7+ & MacOS 10.12+.

Requirements:

- USB-C or USB-A to lightning cable or USB-C
- Latest version of iTunes
- Latest version of iCloud

On Windows, you must download iTunes and iCloud NOT from the microsoft store. You need to obtain the versions from Apple's websites. You can find it at sideloadly.io .

1. Install the latest version of Sideloadly on sideloadly.io
2. Install the latest version of iTunes and iCloud NOT from the Microsoft Store on Windows
3. Open Sideloadly
4. Connect your device to your computer
5. Drag & drop the .ipa selected you want to install
6. Log-in to your Apple ID. This will only be sent to Apple and not a third party server.

On iOS 16+, you need to enable developer mode. To do so, visit Settings > Privacy & Security > Scroll to the bottom and select Developer Mode. Follow on-screen instructions.

AltStore

AltStore is a sideloader that uses developer accounts to sideload apps on Windows 10+ and MacOS 11+.

Windows

Requirements:

- Latest version of iTunes
- Latest version of iCloud

1. Install AltServer on Windows
2. Uncompress the .zip and run the setup.exe
3. Go to your search in your Windows task bar, type in AltServer and run as administrator. If asked, allow private networks. AltServer will then appear in the taskbar.
4. Connect your device to your computer.
5. Open iTunes and enable "Sync with this iPhone over Wi-Fi"
6. On the bottom right taskbar click the AltServer logo. Then go to Install AltStore.
7. Type in your Apple ID. This will only be sent to Apple's servers to authenticate. You can always use an alternate ID.

On iOS 16+, you need to enable developer mode. To do so, visit Settings > Privacy & Security > Scroll to the bottom and select Developer Mode. Follow on-screen instructions.

MacOS

1. Install AltServer on MacOS
2. Copy .app to /Applications
3. Open AltServer
4. Connect your device to your computer.
5. Open iTunes and enable "Sync with this iPhone over Wi-Fi"
6. Click the AltServer icon in the menu bar, and then click "Install AltStore".
7. Type in your Apple ID. This will only be sent to Apple's servers to authenticate. You can always use an alternate ID.

On iOS 16+, you need to enable developer mode. To do so, visit Settings > Privacy & Security > Scroll to the bottom and select Developer Mode. Follow on-screen instructions.

Other

Appsync Unified

Appsync Unified is a sideloader that uses a codesign bypass in jailbreaks to sign apps. This requires a jailbreak to install and must remain in a jailbroken state otherwise apps will not open. This supports iOS 5+.

The source used is currently down. Until it is up, users need to download archived versions which may not support some iOS versions.

Installing Appsync Unified

1. Visit the website listed below

<https://www.ios-repo-updates.com/repository/karen-s-repo/package/net.angelxwind.appsyncunified/>

2. Install Filza, or any file manager
3. Install the .deb, or you can do so using a package manager.

Now, you can grab any .ipa and install it using Filza or a file manager.

Certificate Purchasing

Users can also purchase certificates


Error Fixing

“The app integrity could not be verified”.

For sideloaders that use enterprise certificates, the certificate has been revoked. This is something you cannot change or fix.

“An internet connection is required to trust ...”

This means that you have been blacklisted by the certificate. To fix this, you need to follow this other guide I made, which states how to fix it.

 [How to fix "An internet connection is required to trust the developer"](#)

DNS-Anti Revoke

A DNS-Anti revoke is used to prevent Apple from displaying revoke or blacklist messages to your device. This method should only be used when using enterprise certificates.

Custom DNS

Custom is recommended, as prebuilts can read your internet traffic & access data and the websites that you visit. Using custom can give you full control & prevents developers from seeing your internet data.

Note: If you are using a VPN, this method will not work for some VPN's. Find out which VPN works for you, otherwise your apps may be revoked once enabled, as this filters internet traffic.

1. Create an account at NextDNS.
2. Head to the tab that displays "denylist"
3. Add the following URL's to the list:

ocsp.apple.com
ocsp2.apple.com
valid.apple.com
crl.apple.com
certs.apple.com
appattest.apple.com
vpp.itunes.apple.com

Once done, head to the Setup tab, and install the configuration profile.

Questions/Concerns

Will TrollStore ever come out for iOS 17.0.1 and above?

Unlikely, unless another exploit comes out for those versions above iOS 17, but it's gonna be a long time until it happens.

What is the best sideloader?

Benefits	Appsync Unified	Developer Account (Sideloadly, AltStore)	Enterprise Certificates	TrollStore
JIT	YES (IF JAILBREAK SUPPORTS JIT)	DEPENDS	NO	YES
App Limit	NO	3 or UNLIMITED	UNLIMITED	NO
Revokes	NO	NO	YES	NO
ALL ENTITLEMENT SUPPORT	UNKNOWN	DEPENDS	NO	YES
Renew Often	NO	DEPENDS	NO	NO
Other Notes	<ul style="list-style-type: none">- Must be jailbroken to install apps- Currently, the repo for it is down, so it only supports rootful at the moment.	<ul style="list-style-type: none">- 10 app ID's max	<ul style="list-style-type: none">- Can be a good tool if DNS is used	<ul style="list-style-type: none">- All apps are registered as system- Higher chance of malware attack; although rare at the same time.

TrollStore & Appsync Unified are the best sideloaders.

Can you convert a .ipa to .apk or vise versa?

No.

Credit

- Thank you to u/PuReEnVyUs for the ESign guide & custom-DNS method
- Thank you to ios.cfw.guide for some parts of the TrollStore installation vectors (of course I didn't copy word for word). Check out their website.

Unauthorised distribution, modification, or duplication without permission of the owner is prohibited, and can result in copyright actions. Users have the right to create copies of the document and are permitted to distribute the copies (or copy) to other people as long as it has not been altered or modified in any shape or form.

Created October 7th, 2024
Published October 15th, 2024