iOS 12 Enhances USB Restricted Mode

By Oleg Afonin

Published: 2018-09-20 · Archived: 2026-04-05 17:00:18 UTC

The release of iOS 11.4.1 back in July 2018 introduced USB Restricted Mode, a feature designed to defer passcode cracking tools such as those developed by Cellerbrite and Grayshift. As a reminder, iOS 11.4.1 automatically switches off data connectivity of the Lightning port after one hour since the device was last unlocked, or one hour since the device has been disconnected from a USB accessory or computer. In addition, users could manually disable the USB port by following the S.O.S. mode routine.

iOS 12 takes USB restrictions one step further. According to the new iOS Security guide published by Apple after the release of iOS 12, USB connections are disabled immediately after the device locks if more than three days have passed since the last USB connection, or if the device is in a state when it requires a passcode.

“In addition, on iOS 12 if it’s been more than three days since a USB connection has been established, the device will disallow new USB connections immediately after it locks. This is to increase protection for users that don’t often make use of such connections. USB connections are also disabled whenever the device is in a state where it requires a passcode to re-enable biometric authentication.”

Source: Apple iOS Security, September 2018

Why the Additional Security Measures?

According to Apple itself, the additional security measures were required because “the USB accessory ecosystem doesn’t provide a reliable way to identify accessories before establishing a data connection”. Below is the full explanation of how USB Restricted Mode works in iOS 11.4.1. According to Apple iOS Security, September 2018:

To improve security while maintaining usability, iOS 11.4.1 or later requires Touch ID, Face ID, or passcode entry to activate the USB interface if USB hasn’t been used recently. This eliminates attack surface against physically connected devices such as malicious chargers while still enabling usage of USB accessories within reasonable time constraints. If more than an hour has passed since the iOS device has locked or since a USB connection has been detached, the device won’t allow any new connections to be established until the device is unlocked. This hour period:

- *Ensures that frequent users of connections to a Mac or PC, to USB accessories, or wired to CarPlay won’t need to input their passcodes every time they attach their device.*

- *Is necessary because the USB accessory ecosystem doesn't provide a reliable way to identify accessories before establishing a data connection.*

Back in July, we discovered this was exactly the issue with USB Restricted Mode in iOS 11.4.1. In particular, USB restricted mode could be deferred by using a digital Lightning adapter (more in This $39 Device Can Defeat iOS USB Restricted Mode). Being aware of this situation, Apple attempted to address the issue in iOS 12. Considering the lack of "*reliable way to identify accessories before establishing a data connection*", this is the best Apple could do:

"In addition, on iOS 12 if it's been more than three days since a USB connection has been established, the device will disallow new USB connections immediately after it locks. This is to increase protection for users that don't often make use of such connections. USB connections are also disabled whenever the device is in a state where it requires a passcode to re-enable biometric authentication."

Source: Apple iOS Security, September 2018

iOS 12 USB Restricted Mode at a Glance

Below is a brief summary of USB Restricted Mode in iOS 12.

In iOS 12, USB Restricted Mode engages if any of the following conditions is met:

- One hour after the phone has been is locked, or one hour since the phone was disconnected from a USB accessory (whichever is later). Basically, one hour since last unlock/last disconnect.
- Immediately after the phone is locked if 72 hours or more have passed since the phone last established connection with a USB device. If the 72 hours have passed, USB Restricted Mode will engage immediately every time the iPhone's screen is locked.
- After S.O.S. mode
- If the iPhone is in a state where it requires a passcode to re-enable biometric authentication ("Your passcode is required to enable Touch ID/Face ID" message is displayed); basically, USB Restricted Mode now engages under the same rules as Touch ID/Face ID expiry. Comprehensive analysis of Touch ID expiration rules in Fingerprint Unlock Security: iOS

What Happens Once USB Restricted Mode Is Engaged

Once USB Restricted Mode is engaged on a device, no data communications occur over the Lightning port. A connected computer or accessory will not detect the iPhone as a "smart" device. If anything, an iPhone in USB Restricted Mode acts as a dumb battery pack: in can be charged, but cannot be identified. Moreover, once an iPhone engages USB Restricted Mode, it may be unable to charge from the computer's USB port (most 'dumb' chargers will work as usual).

USB restricted mode effectively deters the ability of third-party forensic tools to crack iPhone's passcodes.

Is It Still Possible to Fool USB Restricted Mode with a USB Accessory?

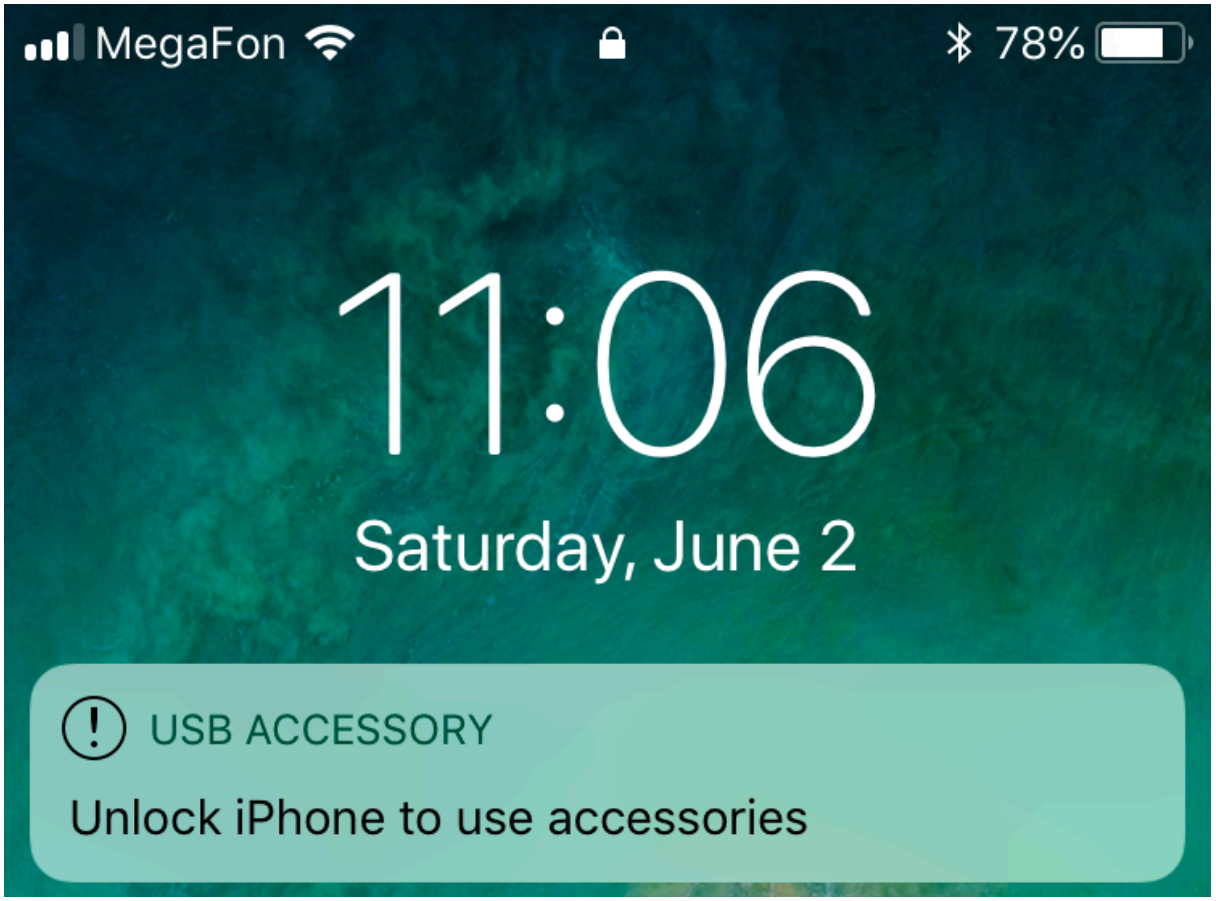
In This $39 Device Can Defeat iOS USB Restricted Mode, we recommended connecting the seized iPhone to a compatible accessory in order to defer USB Restricted Mode. Prior to iOS 11.4.1, isolating the iPhone inside a Faraday bag and connecting it to a battery pack would be enough to safely transport it to the lab. For iOS 11.4.1, we recommended the following procedure:

1. Connect the iPhone to a compatible Lightning accessory (such as the official Lightning to USB 3 Camera Adapter).
2. Plug external battery pack to the adapter (to avoid iPhone battery drain).
3. Place the entire assembly in a Faraday bag.

This main goal of this procedure was deferring the activation of USB Restricted Mode, allowing safely transporting the iPhone to the lab. The key word here is “deferring”. If USB Restricted Mode has already engaged (for any reason), there is literally nothing you can do to enable the USB port other than unlocking the phone. Below is the new recommended procedure.

Verifying whether the phone engaged USB Restricted Mode:

1. Attempt to connect the iPhone to a compatible Lightning accessory (such as the official Lightning to USB 3 Camera Adapter).
2. If the iPhone issues a triple vibration and displays the message below, USB Restricted Mode is already active. At this point, there is nothing you can do to defer USB Restricted Mode other than asking the owner to unlock the device.



3. If the iPhone was able to connect to the accessory, immediately place the device into the Faraday bag and connect it to the charger. By using a compatible accessory, you will be able to safely transport the phone to the lab without USB Restricted Mode being engaged.

Conclusion

iOS 12 is not only a major update, it’s a major upgrade as well. Delivering significant performance improvements to older devices and supporting devices as old as the iPhone 5s, iOS 12 will undoubtedly become the most popular version of iOS on all compatible devices, old and new. Law enforcement and forensic specialists will have to adapt to this situation by at least being aware of the potential issues brought by this version of Apple’s mobile operating system.
