Troubleshooting

- Apple ID prompt still appears even when Activation Lock Bypass Code is used during Remote Wipe
- FileWave iOS Kiosk (IPA) Location Tracking Problem
- iOS 12+ Profile Installation Failed

Apple ID prompt still appears even when Activation Lock Bypass Code is used during Remote Wipe

PROBLEM

When executing a Remote Wipe against a Supervised iOS 7.1+ device and the "Remove Activation Lock" option is checked, the expected behaviour is that on activation of the iOS device, the AppleID username and password will not be required. Instead, the stored Activation Lock Bypass code (FileWave Admin> Assistants> Activation Lock Management...) should be used to remove the Activation Lock. In some circumstances, we have experienced that the username / password dialog is still presented to the user.

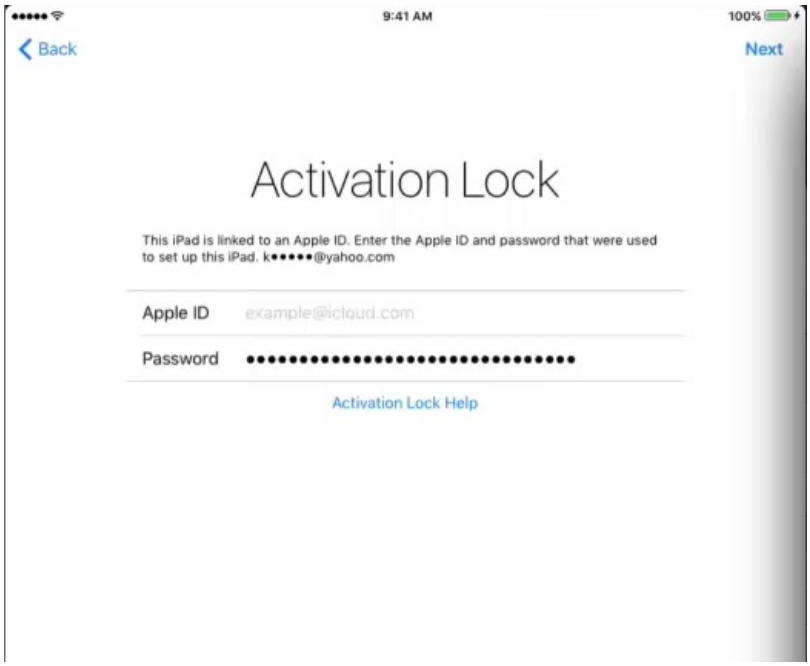
ENVIRONMENT

- iOS Supervised Devices
- FileWave MDM

RESOLUTION

Instead of entering the username and password in the dialog presented on the iOS device after the Remote Wipe command executes, enter the Bypass code for that device (found in FileWave Admin> Assistants> Activation Lock Management...) in the password field. Enter the code exactly as it appears in the Activation Lock Management dialog, as the code is case sensitive and also requires the dashes.

Keep the username (Apple ID) field empty.



ADDITIONAL INFORMATION

- Use Mobile Device Management and Find My iPhone Activation Lock

FileWave iOS Kiosk (IPA) Location Tracking Problem

We have been made aware of an issue with our FileWave Kiosk Enterprise IPA app with regard to location tracking. Simply put, iOS no longer allows our application to be approved once, and then allowed to collect geo-location information for all time.

Even when location tracking for the app is set to "Allow While Using", the application will re-prompt for permission on each application restart (usually multiple times).

We are currently investigating what changes will be required to make the Kiosk IPA less intrusive to your customers and will update here as we have more information. In the mean time, here are some mitigation suggestions:

1. Don't deploy the Enterprise IPA at all:
    - This may seem an odd suggestion, but this application was initially developed before the concept of "Lost Mode", and has largely outlived it's purpose
    - "Lost Mode" is much more effective at location lookup, because it doesn't suffer from the same pre-requisites that the IPA does, and it works even if the end-user has location services turned off
    - "Lost Mode" does not require the IPA
    - Outside of geo-location in "Tracked" mode, the IPA serves no other purpose, and tracking in this mode is delicate to manage at best, and largely ineffective since the user can disable it at any time
    - Apple, and other privacy advocates, are heavily leaning away from this type of location tracking, and before long it may not be possible at all
2. If you don't want to change how you are deploying the IPA currently, consider setting your devices to "Untracked"
    - The issue of user prompts is only seen if FileWave believes the device is in a "Tracked" state
    - By moving devices to "Untracked" you'll avoid customer complaints while we work on a possible fix for this issue

iOS 12+ Profile Installation Failed

Description

On attempting to enrol iOS 12 devices, we have seen some instances of the profile installation failing. In these cases it has been related to the server certificate. As of iOS 11 and macOS High Sierra, Apple introduced stricter rules regarding MDM server to device communication:

https://support.apple.com/en-gb/HT207828

However, it appears that these have not been fully implemented, until iOS 12, with respect to certificates. Certificates of RSA key sizes below 2048 have still managed to work on iOS 11. iOS 12 no longer allow this.

> Self-Signed Certificate
> As 3rd party suppliers have been supplying appropriate keys now for some time, this is likely to impact Self-Signed Certificates only.

Directions

The following command may be used to check the certificate RSA key size.

macOS, Linux:

```
openssl x509 -in /usr/local/filewave/certs/server.crt  -text -noout | grep Public-Key
```

Windows

```
C:\OpenSSL-Win64\bin\openssl.exe x509 -in C:\ProgramData\FileWave\FWServer\certs\server.crt -text -noout | FINDSTR
Public-Key
```

Windows does not have openssl installed as standard so you will need to go to https://slproweb.com/products/Win32OpenSSL.html and download the appropriate version of OpenSSL for your environment.

If the output is anything less than 2048, then the server certificate will need to be updated.

If you are using a Self-Signed Cert, you will need to either:

- Re-use your process for generating the certificate to update to ensure it has a RSA key size of 2048 or larger
- Consider moving to an official 3rd party certificate

Please take into consideration the following KB when moving to a new certificate: Root Trusted SSL Certificate (Using and Renewing)