

iOS 12 / macOS 10.14+ and self-signed certificates

iOS 12 and macOS 10.14 introduce more secured rules ; certificates must be generated from at least a 2048-bit RSA key ; certificates generated from a 1024-bit key will be rejected by the device.

If you are using a trusted CA issued certificate, you should be fine, most of the certificates you get on the market are fulfilling this requirement ; if you generated your certificated with FileWave 9.0 or later, you should be good as well, since in this version the key used to generate certificates is 2048-bit. If you are running a FileWave installation which has been setup before FileWave 9.0 with self signed certificate, or if you are using a 1024-bit key issued certificate, you need to update your setup to have iOS 12 devices trust your server.

How 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.

Recommended solution:

Use a third party, trusted Certificate Authority. Most organizations already have a wildcard certificate (for instance *.acme.org), installing this certificate on "filewave.acme.org" will make your server trusted automatically. If you don't have a certificate, several CAs provide SSL certificates which are trusted by Apple, Google or Microsoft. For more information about these trusted certificates please read [this KB article](#).

Self-Signed solution:

If you decide to stay with a self-signed certificate, you don't have another choice than renewing the certificate ; please read [this KB article](#) on how to renew the certificate.

The best approach would then be:

1. Deploy a profile with "defer software update" set to 90 days restriction ; this will give you 90 days (starting from Monday, Sept 17th) during which devices won't be upgraded
2. Follow steps described in [Renew FileWave Server Self-signed Certificate](#) KB article:
 1. create new key and certificate
 2. deploy the new certificate via profile
 3. switch to the new certificate once all devices have the profile installed
 4. recreate DEP profiles (and associations, if required)
3. Already impacted devices can be manually "healed" by installing the profile (and trusting it explicitly for SSL in trust stored).



If you have a pre-FileWave 9.0 certificate and devices have already upgraded to iOS 12, the only way to recover, assuming you can't use trusted certificate, is to manually add the new certificate in the trust store and give it permissions for SSL.

Related Content

- [iOS 12+ Profile Installation Failed](#)

🕒Revision #3

★Created 14 July 2023 18:02:48 by Josh Levitsky

🔧Updated 14 July 2023 18:12:05 by Josh Levitsky