APNs Certificate Creation & Renewal on Windows Computers

Description

The following guide provides the steps to create and renew an APNs certificate using Windows.

> ⚠ APNs Topic
> An APNs certificate has a unique topic, in the form of a hexadecimal string, and belongs to the Apple ID used to create the certificate. When renewing, the topic must match to ensure devices continue to communicate with the server. As such, not only must the same Apple ID be used when renewing an APNs certificate, but the current certificate must also be selected for renewal.

> ⚠ APNs Expiry
> Apple Mobile Device Management (MDM) requires an Apple Push Notification service (APNs) certificate; renewable yearly. If APNs certificates are allowed to expire, all MDM communication will be lost, until renewed.

Information

Requirements

- An appropriate copy of OpenSSL, which must be downloaded and installed.

Note, that the light version does not include the necessary configuration files.

> ℹ CMD Commands
> The cmd.exe application should be opened with 'Run as an Administrator' for all commands in this KB

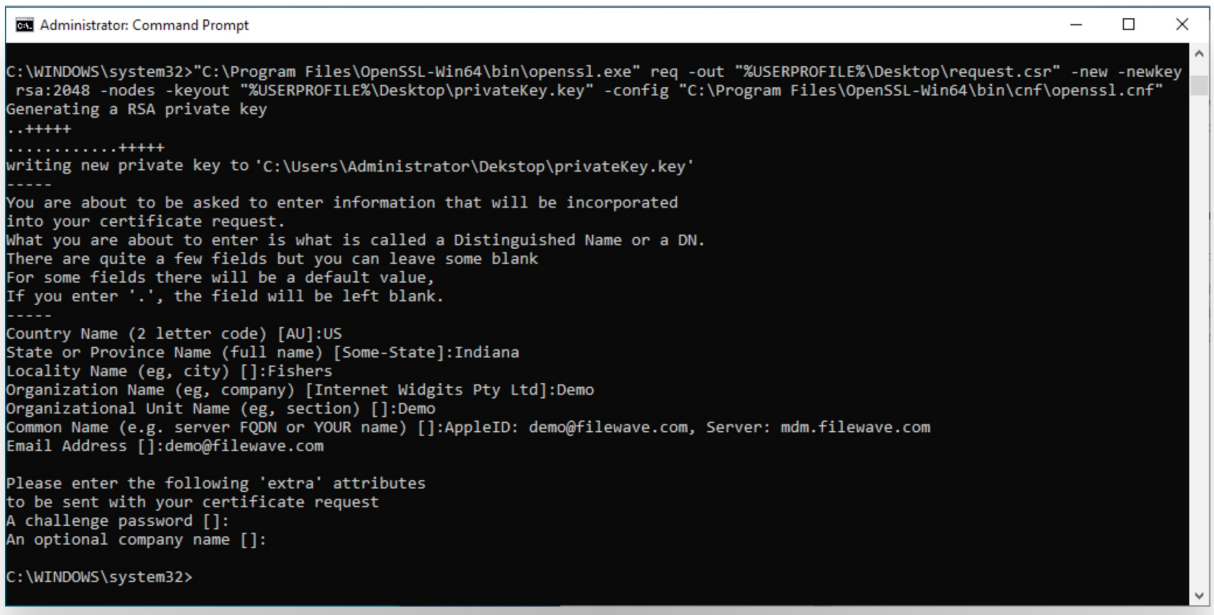
Step-By-Step Guide

Creating the Certificate Signing Request (CSR)

1. Open cmd.exe as an Administrator
2. Create a CSR. Enter the following command, which will result in two new files on the Desktop: request.csr and privateKey.key:

```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -out "%USERPROFILE%\Desktop\request.csr" -new -newkey rsa:2048 -nodes -keyout "%USERPROFILE%\Desktop\privateKey.key" -config "C:\Program Files\OpenSSL-Win64\bin\cnf\openssl.cnf"
```

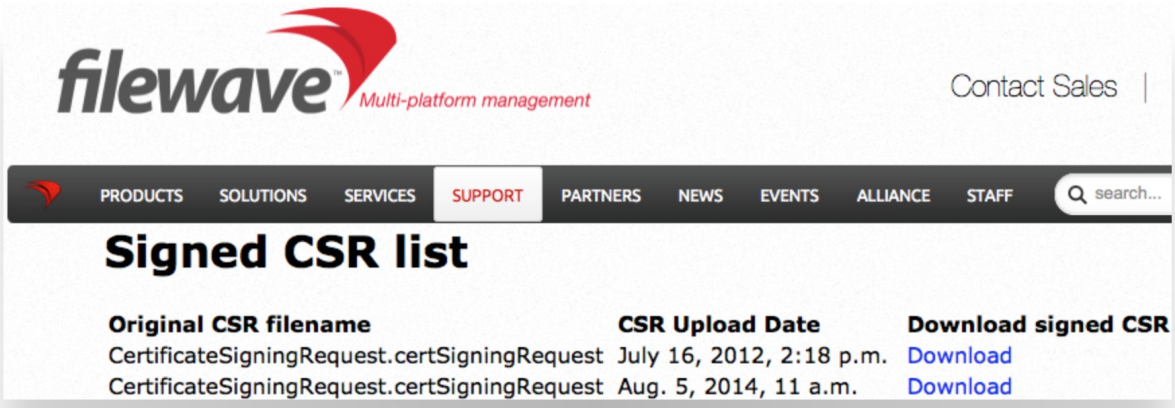
> ℹ Certificate Private Key names are visible from openssl commands and the Common Name is used to set the Private Key name. Supplying the Apple ID and Server as the Common Name, ensures the Apple ID used to generate the certificate will be stored for future reference.



Sign the CSR

CSR requests must be signed before uploading to Apple. FileWave has a portal for this process, which requires an active FileWave account.

1. Navigate to https://csr.filewave.com/list_csr and login.
2. Upload the previously created CSR.
3. 'Download signed CSR' should list this uploaded and now signed CSR.
4. Download this newly signed CSR, ready for upload to Apple in the next section. Again consider where this certificate is stored.



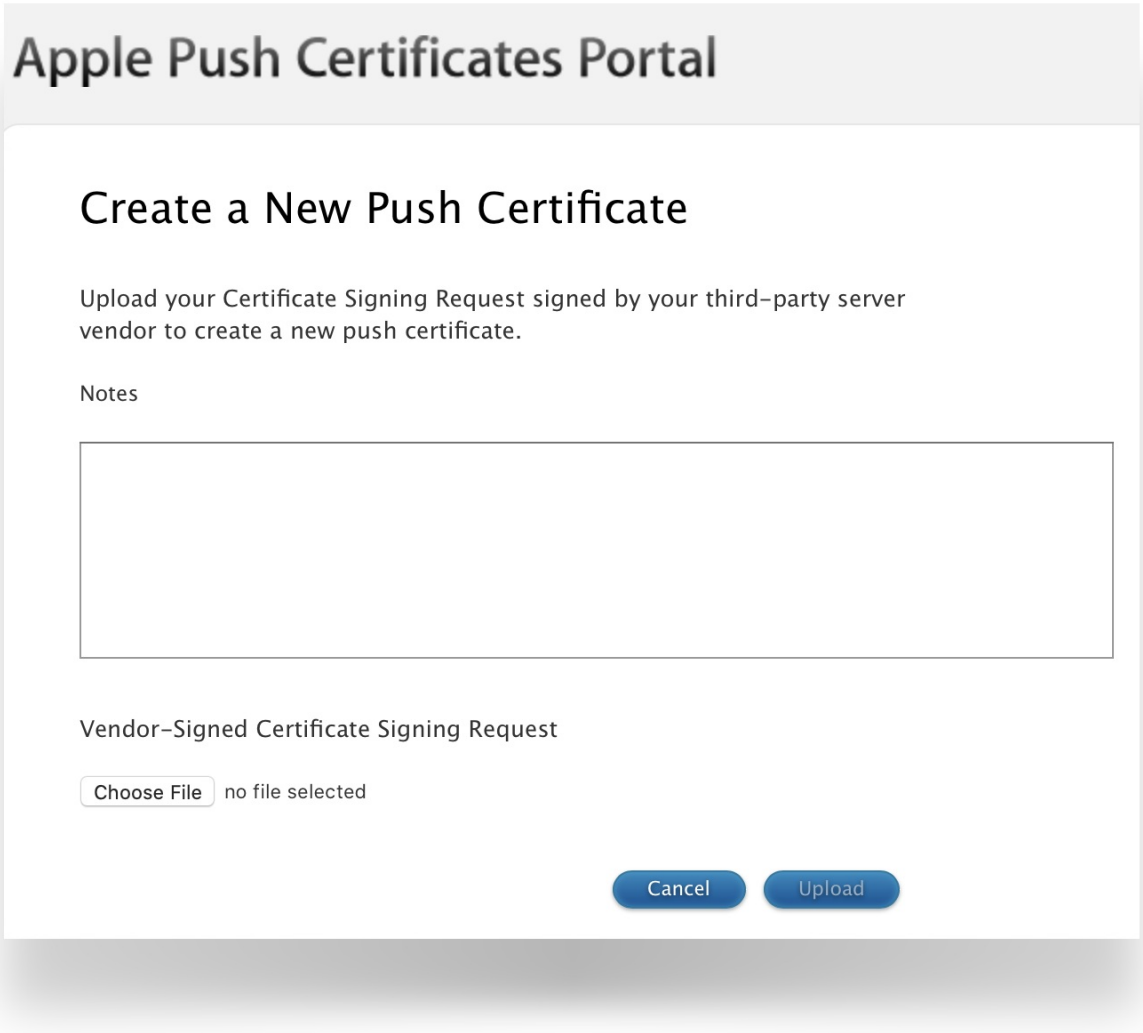
Upload the signed FileWave CSR to Apple

Creating a Certificate

1. Navigate to: https://identity.apple.com/pushcert/ and log in with an Apple ID.

> This Apple ID will own the certificate and is required for every renewal. Do not use a personal Apple ID, to avoid complications if that person where to leave the business or institution.

1. Click 'Create'.
2. 'Accept' Apple's 'Terms of Use'.

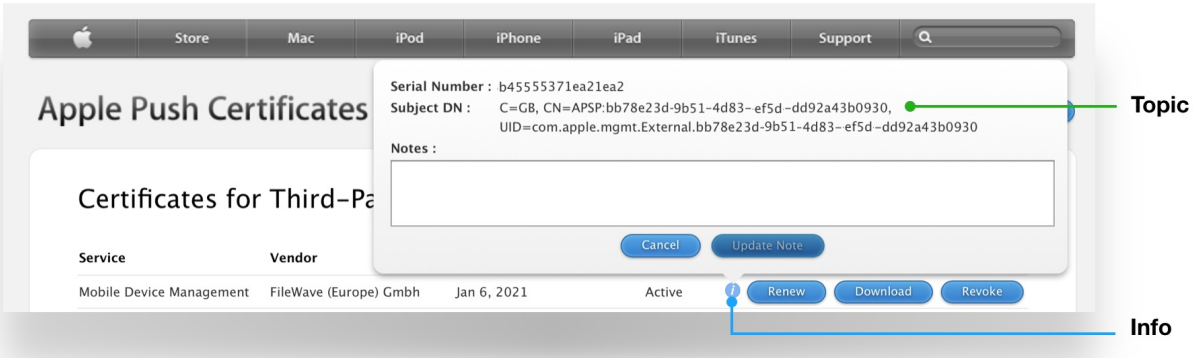


Renewing a Certificate

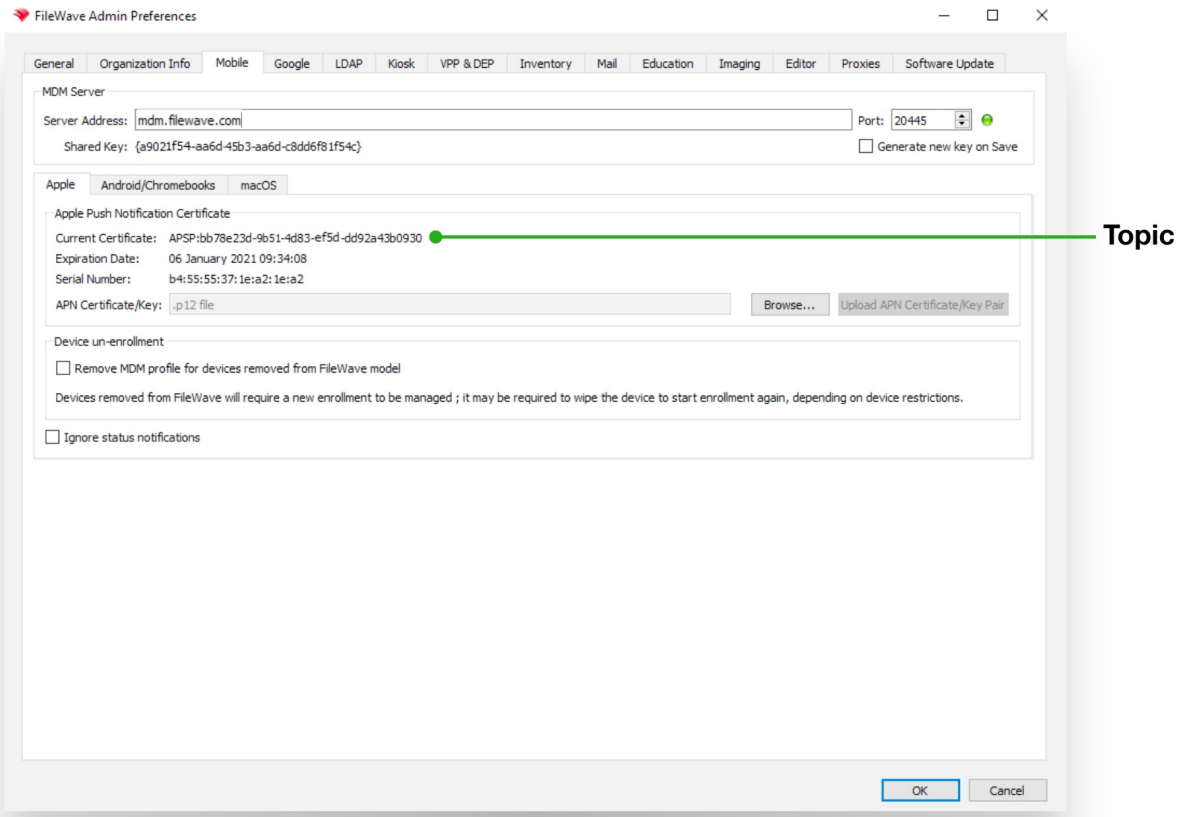
1. Navigate to: https://identity.apple.com/pushcert/ and log in with the Apple ID used to initially create the certificate.
2. Confirm the Certificate to renew.
3. Select 'Renew'.

To confirm the certificate, compare the Subject DN (Topic) and current certificate.

Clicking the 'i' button will show the certificate details, including the Topic:



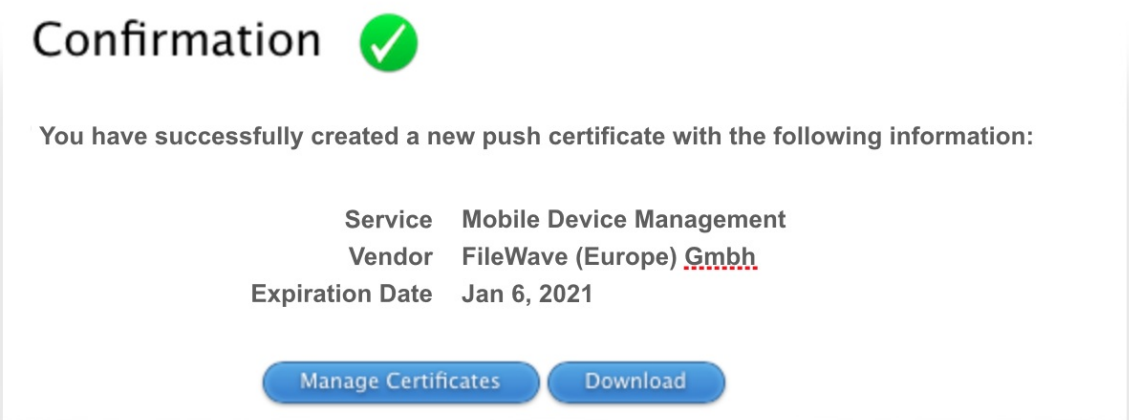
Ensure this matches with the 'Current Certificate' in FileWave Admin > Preferences > Mobile > Apple Push Notification Certificate:



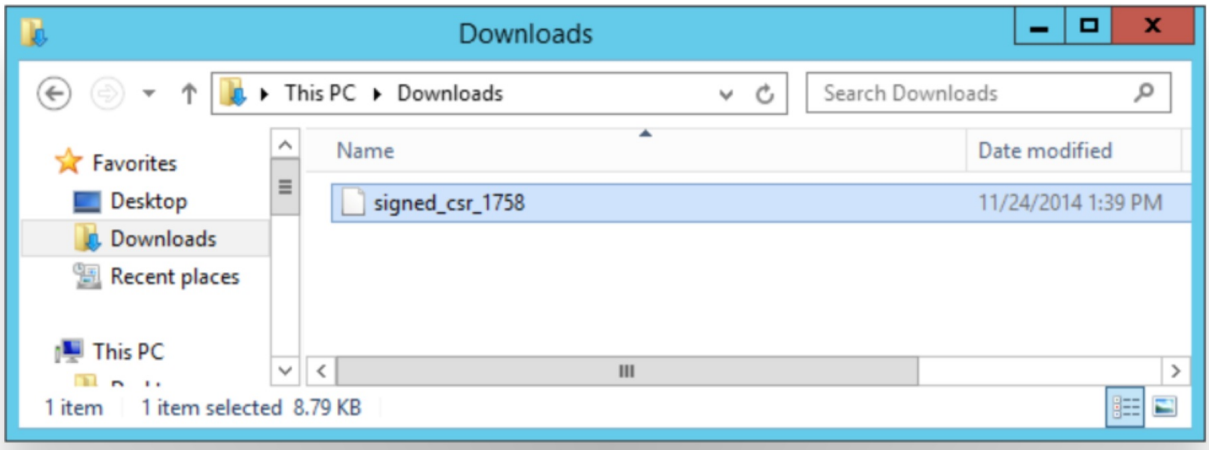
If the 'Topics' do not match do not continue. If the correct certificate is not in the list on Apple's website, this is the wrong Apple ID. If this guide was followed in creating the original certificate, the previously used Apple ID will be viewable from the certificate "Private Key".

Click 'Choose File' and browse to the signed FileWave CSR from the previous section.

Click 'Upload' and Apple will return a 'Confirmation'.



Click 'Download' and save the ".pem" file. Again consider where this certificate is stored.



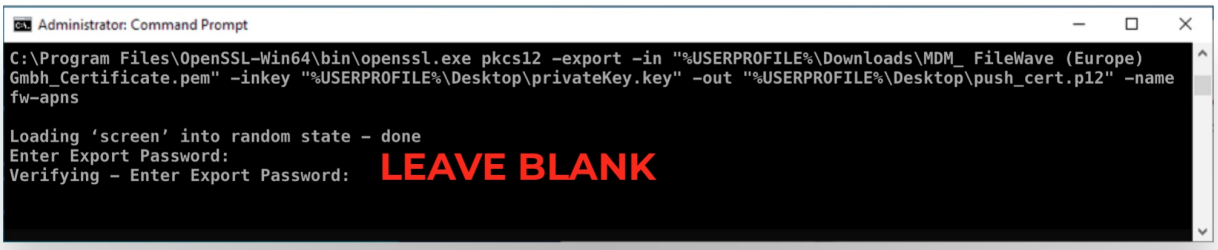
Create a ".p12" from the Signed CSR

1. Open cmd.exe as an Administrator
2. Create a ".p12". Entering the following command will create the ".p12" on the Desktop:

```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -export -in "%USERPROFILE%\Downloads\MDM_ FileWave (Europe) Gmbh_Certificate.pem" -inkey "%USERPROFILE%\Desktop\privateKey.key" -out "%USERPROFILE%\Desktop\push_cert.p12" -name fw-apns
```

> If the output errors in creating the .p12 certificate file, replace the %USERPROFILE% location by pathing out the exact file location instead.

1. Leave the 'Export Password' blank

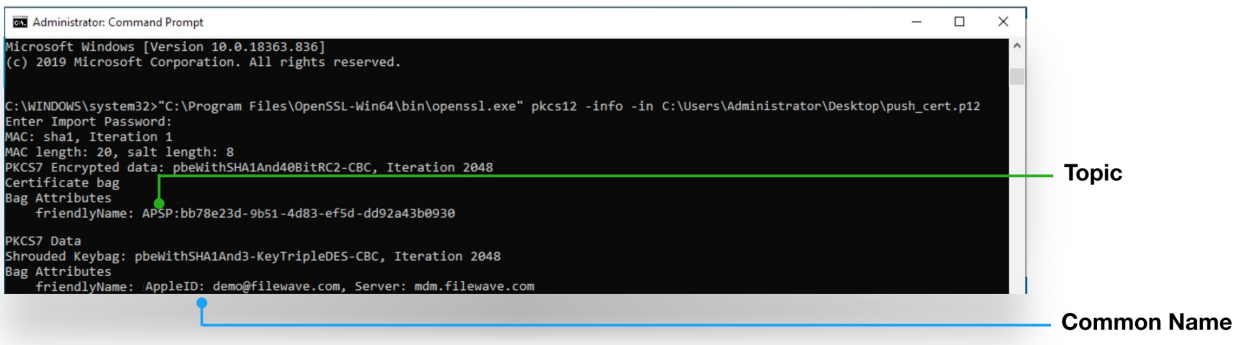


1. Certificate details may be checked:

> Common Name and Topic
> The name of the Private Key will show the value defined as the "Common Name" from the creation of the CSR. Where recommendation was followed, this should list the Apple ID and Server name. Additionally the name of the Certificate is the same as the Topic.

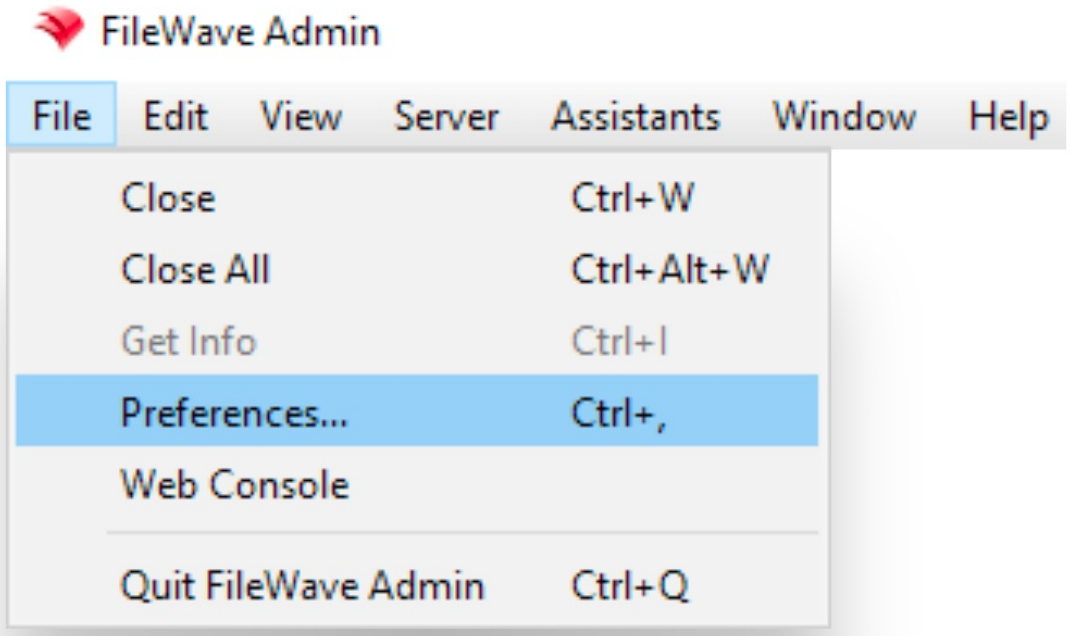
```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -info -in C:\Users\Administrator\Desktop\push_cert.p12
```

Note, below image has been edited to remove some details and highlight the two key items of interest.

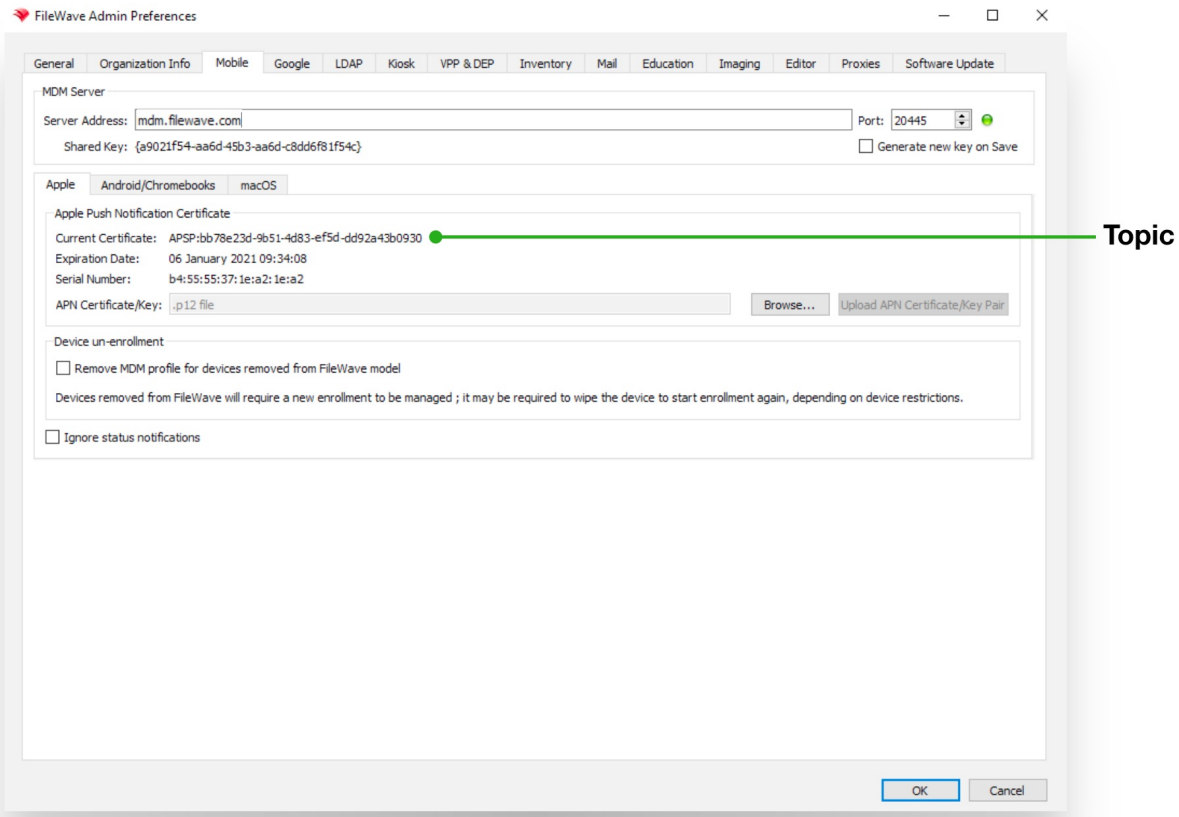


Uploading the Certificate into FileWave

1. Launch the FileWave Admin and login to the FileWave server.
2. Open the FileWave Admin žPreferences.



1. Select the 'Mobile' tab.
2. Click 'Browse' and navigate to the saved ".p12" APNs certificate.
3. Select the exported ".p12" certficate.
4. Click 'Upload APN Certificate/Key Pair'.
5. The topic should match the previous topic.



1. That is it! FileWave may now manage Apple devices using Apple's Push Notification Service.

> APNs certificates require yearly renewals. Through FileWave Admin > Dashboard > Alert Settings, automated emails may configured. Consider adding 'APN for MDM'. Note this requires the Email preferences in Admin to be configured.

Related Articles

APNs Certificate Creation and Renewal on macOS

Revision #10
★Created 12 July 2023 15:08:22 by Andrew Kloosterhuis
Updated 8 January 2024 18:50:22 by Josh Levitsky