APNs Certificate Creation & Renewal on macOS Computers

Description

Apple Mobile Device Management (MDM) requires an Apple Push Notification service (APNs) certificate; renewable yearly.

> APNs Expiry
> If APNs certificates are allowed to expire, all MDM communication will be lost, until renewed.

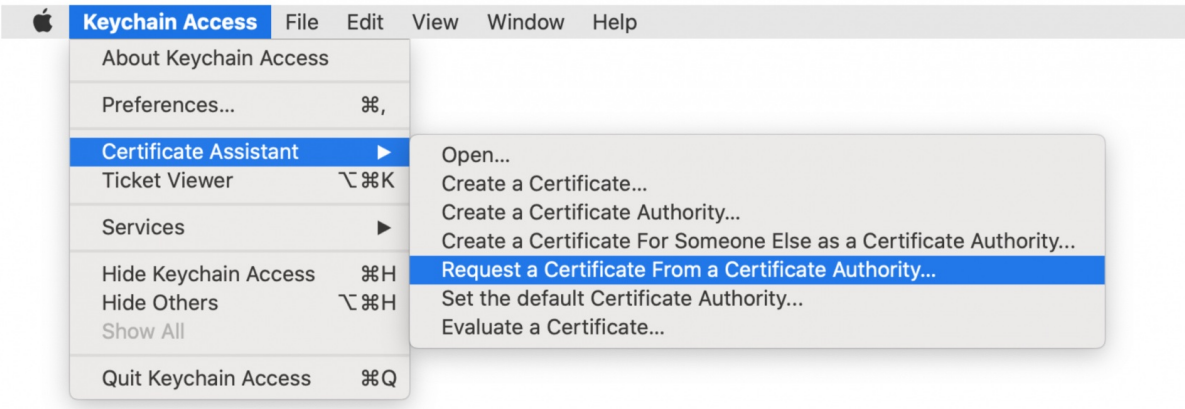
The following guide provides the steps to create and renew an APNs certificate using macOS.

> 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.

Step-By-Step Guide

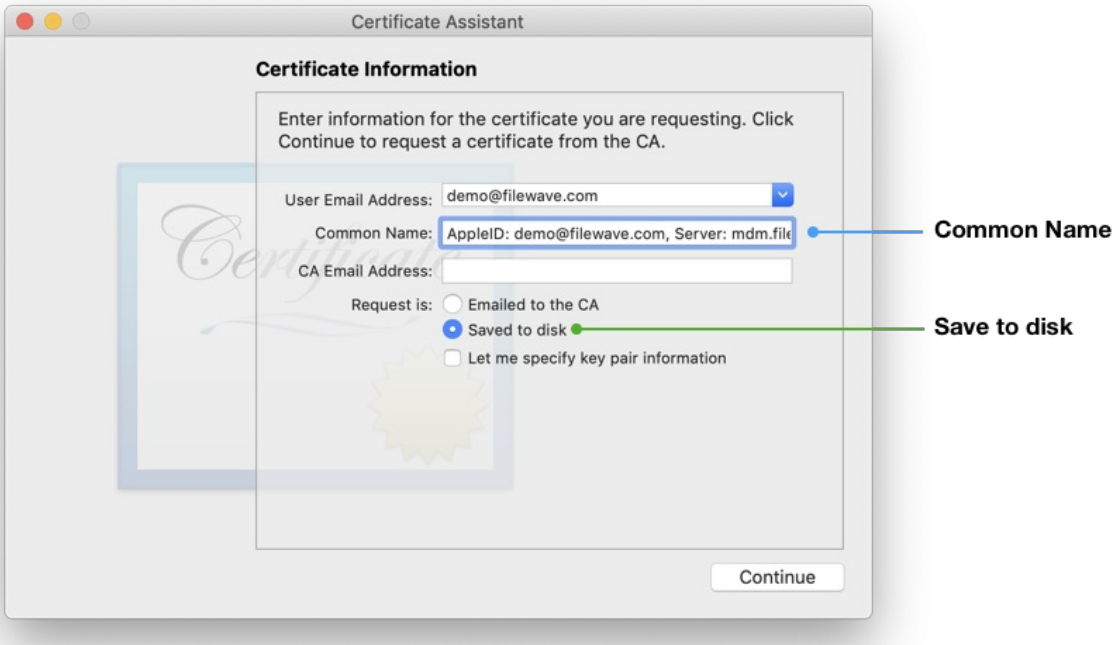
Creating the Certificate Signing Request (CSR)

1. Open Keychain Access, located in: Applications > Utilities > Keychain Access.app.
2. Create a CSR. Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority...



3. Enter the AppleID and Server name that you are going to be associating with this certificate in the "Common Name" field.

> Common Name
> Certificate Private Key names are visible in Keychain 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.



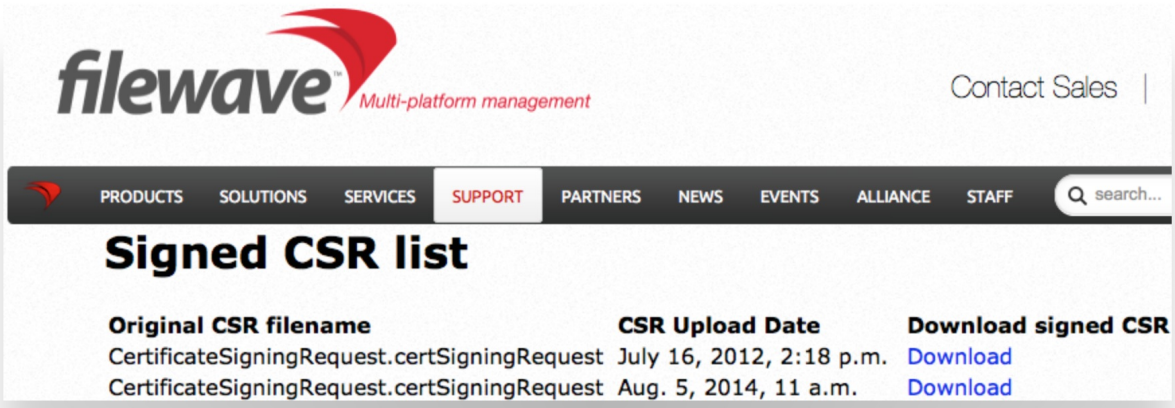
4. Select the radio button "Saved to disk" and click Continue.
5. Save the CSR request, ready to upload to FileWave in the next section.

> Certificate Storage
> Consider creating a secure location to store the created certificates and sub divide them using the date or year, e.g folder named: 'MDM APNs certificates 2020'.

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/ 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.



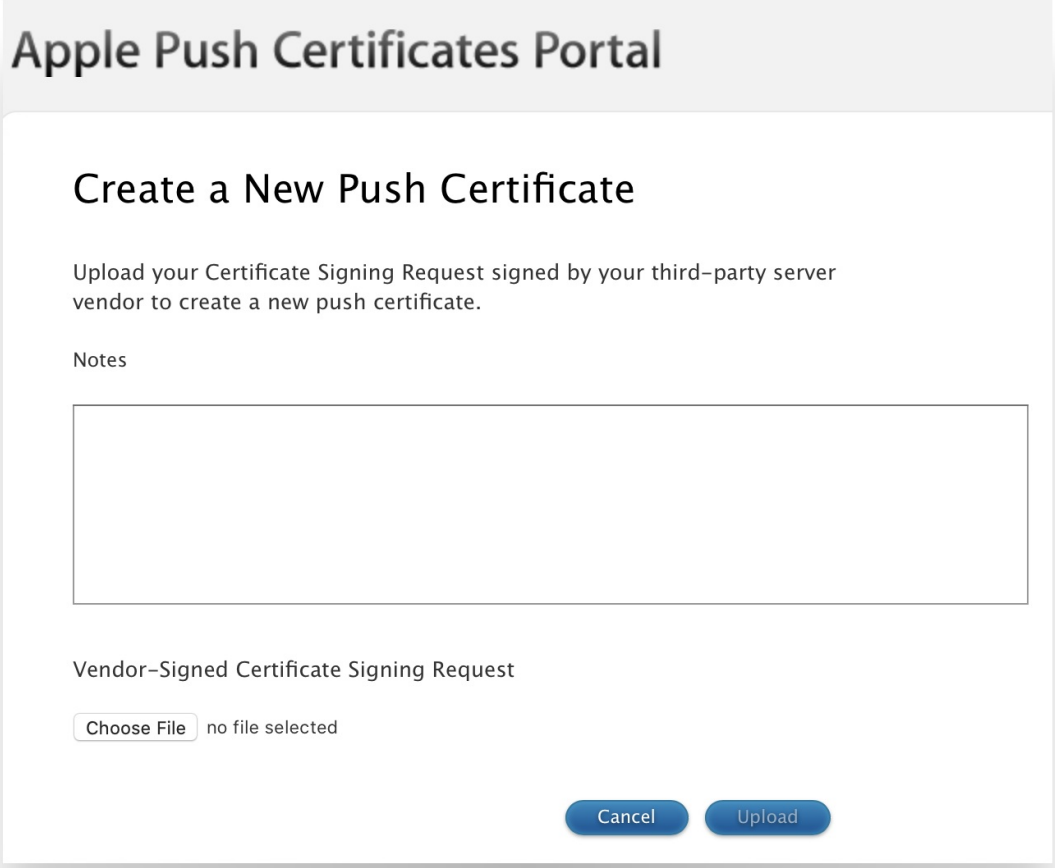
Upload the signed FileWave CSR to Apple

Creating a new Certificate

If you are renewing a certificate then jump to Renewing 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.

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

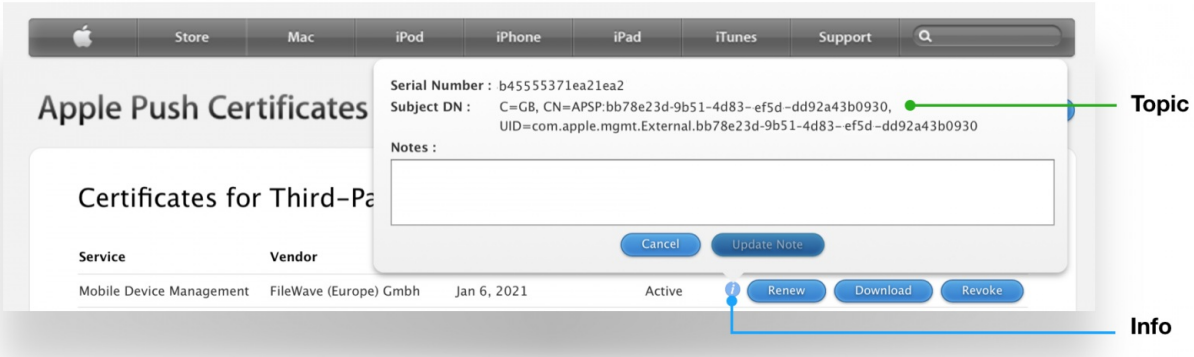


Renewing a Certificate

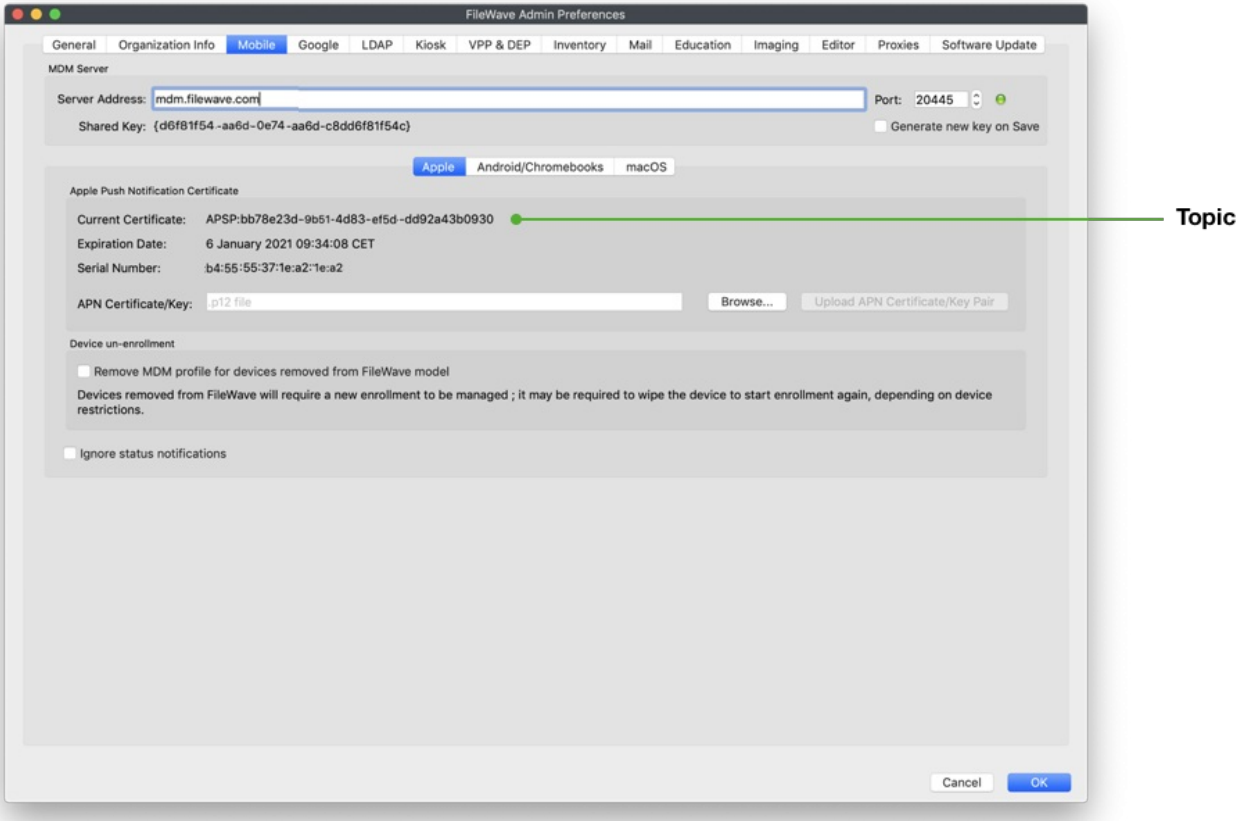
1. Navigate to: https://identity.apple.com/pushcert/ and log in with the Apple ID used to initially create the certificate.
2. Confirm the Certificate to renew.
3. Select 'Renew'.

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

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



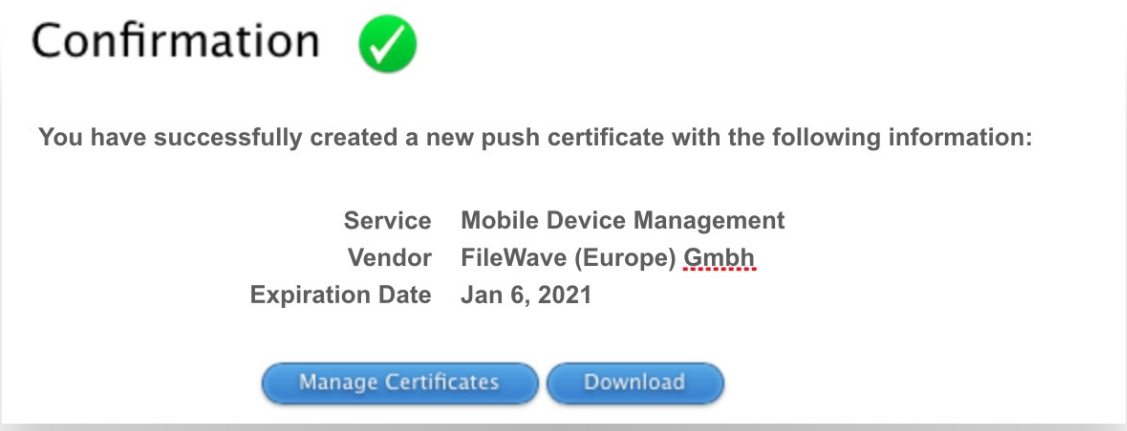
Ensure this matches with the 'Current Certificate' in FileWave Admin > Preferences > Mobile > Apple Push Notification Certificate:



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.

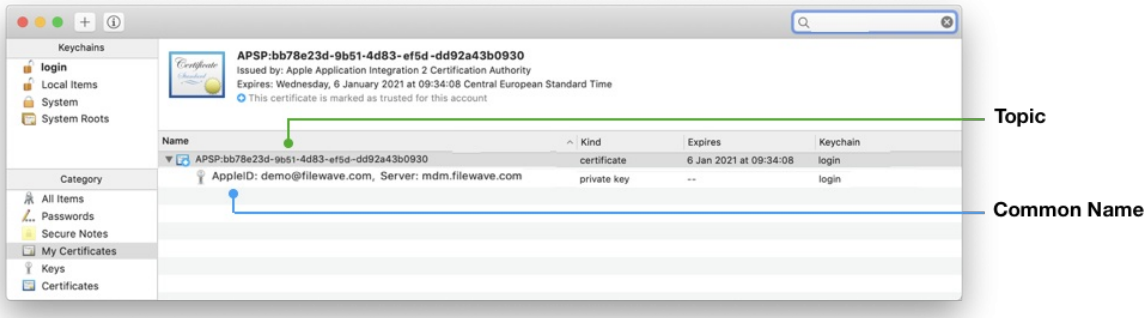
Create a ".p12" from the Signed CSR

1. Open Keychain Access app, select login from the Keychains list and then choose 'My Certificates' tab.

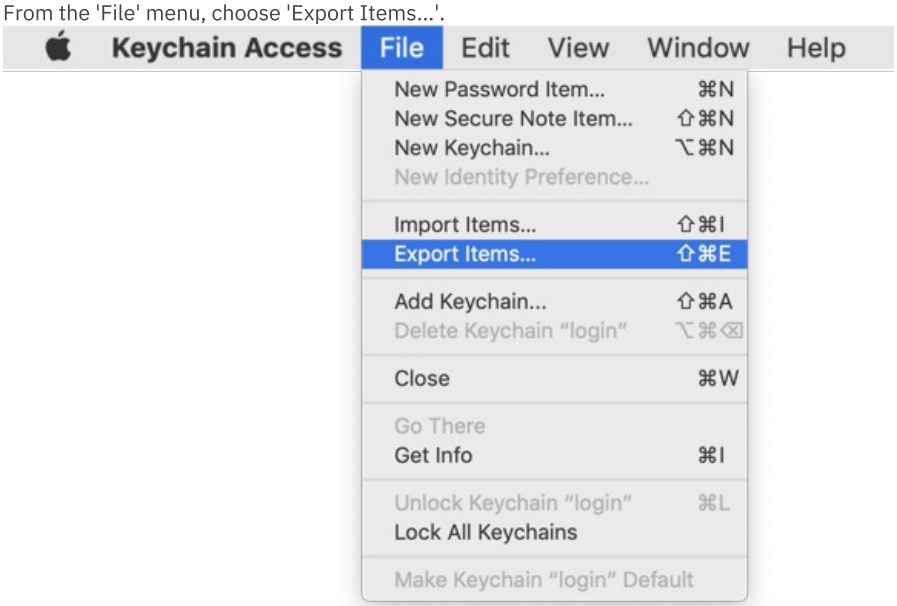
   Keychain
   If imported into the System Keychain, the Private Key will not be accessible. If 'All Items' tab is selected, private keys will not be available!

2. Drag the downloaded PEM file into the Keychain main window.
3. Locate the imported certificate. It will begin with "APSP:".
4. Click the disclosure triangle and select the expanded private key.

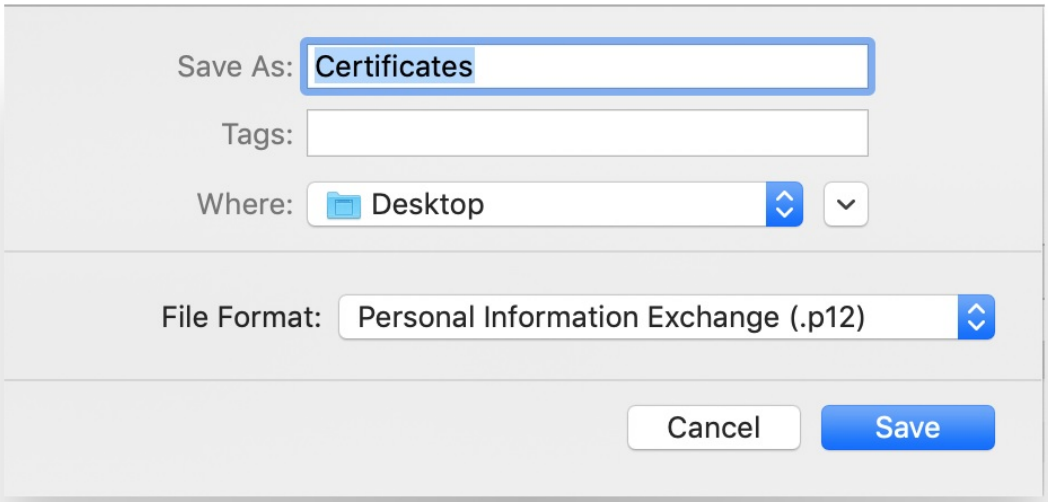
   Common Name and Topic
   The name of the Private Key will show the value defined as the "Common Name" from the creation of the CSR. Where recommendation was followed, this should list the Apple ID and Server name. Additionally the name of the Certificate is the same as the Topic.



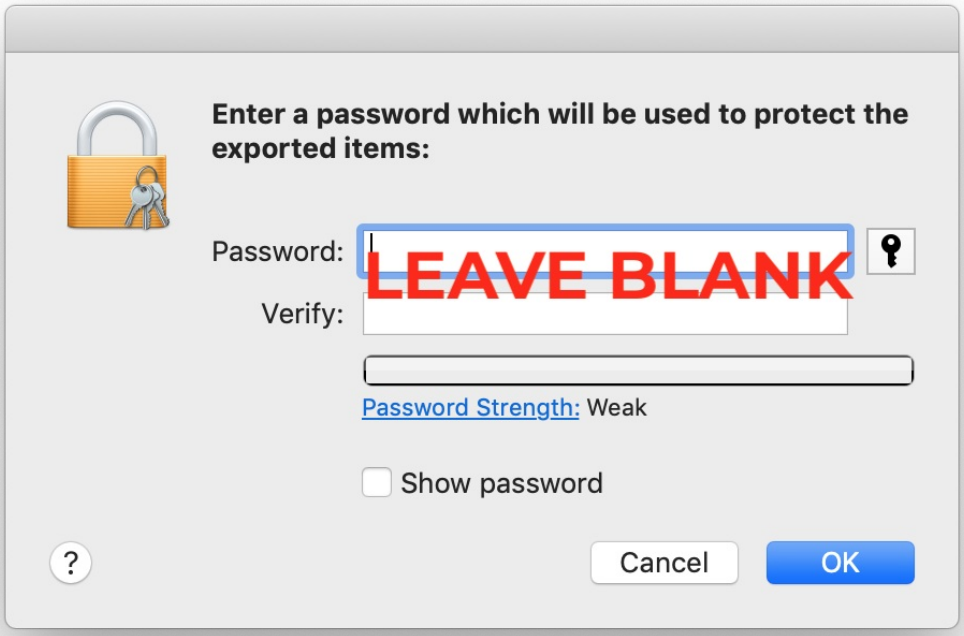
5. From the 'File' menu, choose 'Export Items...'.



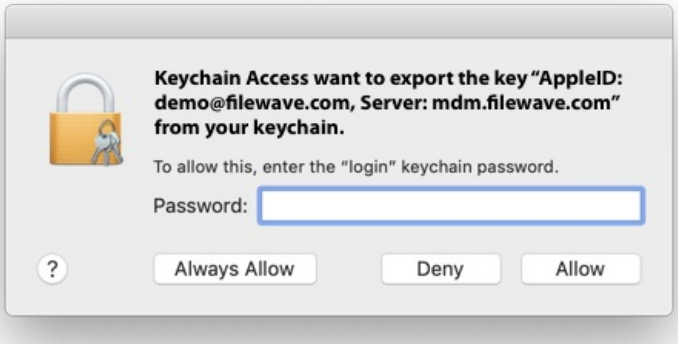
6. Export as a .p12 file. Again consider where this certificate is stored.
7. Click Save.



8. Leave the password blank.

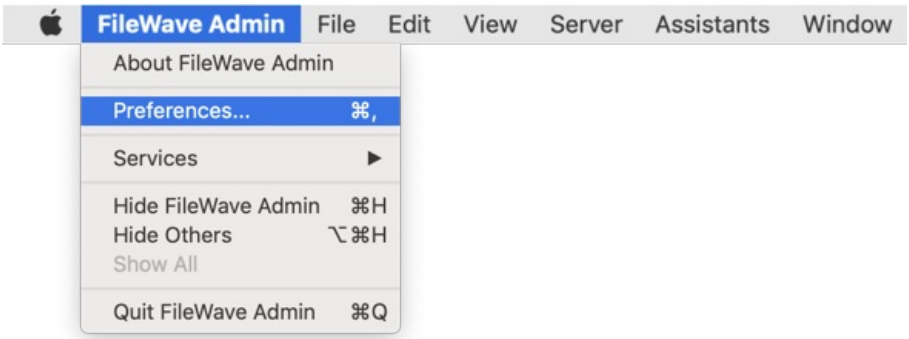


9. Enter your local admin account, when prompted, allowing Keychain to export.

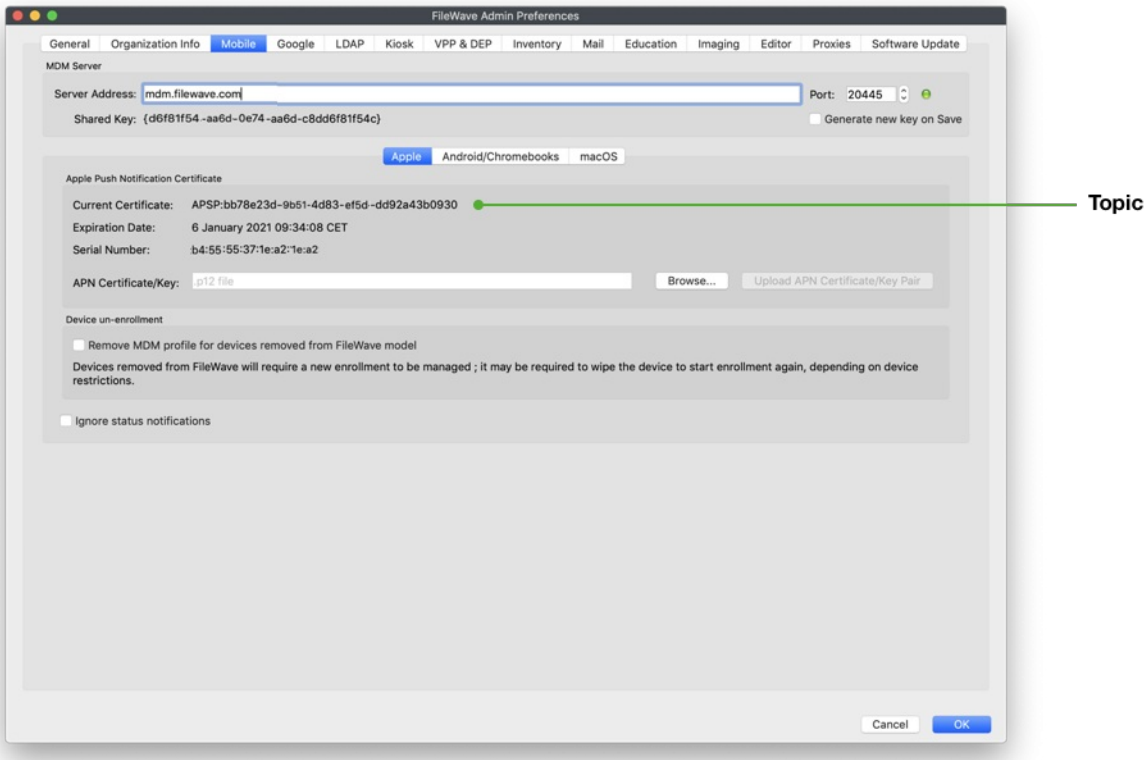


Uploading the Certificate into FileWave

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



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



8. 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 & Renewal on Windows

Revision #9
Created 11 May 2023 16:48:18 by Andrew Kloosterhuis
Updated 10 December 2024 14:05:26 by Sean Holden