

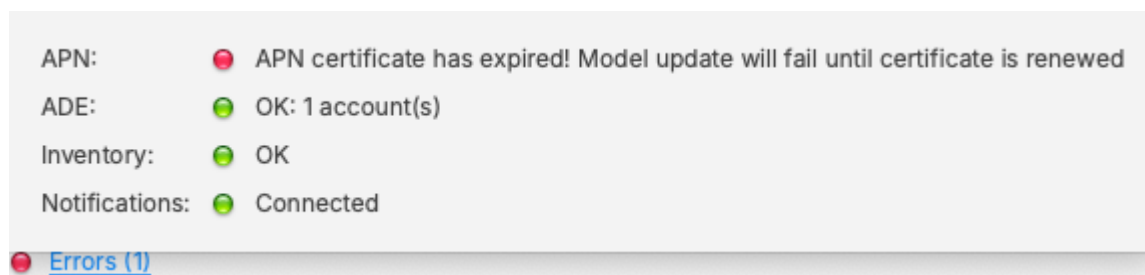
APNs Certificate Creation and Renewal on macOS with XCA

Description

Apple device management requires an Apple Push Notification service (APNs) certificate that must be renewed every year.

Do not let the APNs certificate expire

- ❗ An expired certificate stops Apple MDM communication and prevents Update Model from completing until the certificate is renewed.



This guide explains how to create the Apple Push Notification service (APNs) certificate for FileWave using an online CSR generator and the XCA certificate management tool, instead of the Apple Keychain. The Apple Keychain often causes issues with private key handling on newer macOS versions, so this method provides a more reliable alternative. You may use any online CSR generator (for example ssl.com), it does not have to be ssl.com specifically.

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

Prerequisites

- Access to the Apple Push Certificates Portal (<https://identity.apple.com/pushcert/>).
- A valid Apple Business/School Manager account or Apple ID.
- Access to the FileWave Central console.
- Installed XCA tool: <https://github.com/chris2511/xca/releases>

Step 1: Generate CSR (Certificate Signing Request)

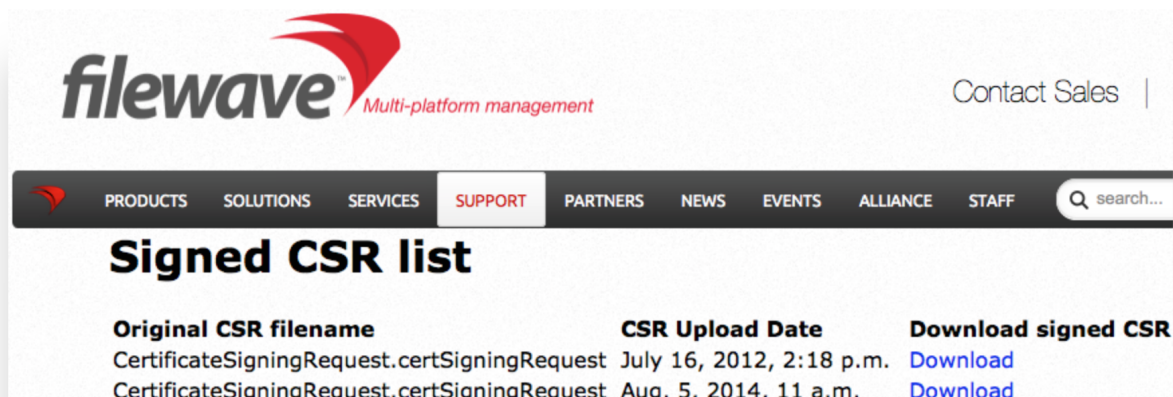
1. Open the CSR generator at [ssl.com](https://www.ssl.com/online-csr-and-key-generator/). (<https://www.ssl.com/online-csr-and-key-generator/>)
2. Enter the required details:
 - Common Name (CN): e.g. FileWave APNS
 - Organization (O): your company or school name
 - Organizational Unit (OU): optional, e.g. IT Department
 - Country (C): two-letter ISO code (e.g. DE)
3. Generate the CSR and download the files:
 - CSR file (.csr)
 - Private Key (.key)

⚠ Keep the .key file safe – you will need it later in XCA.

Step 2: Sign the CSR with FileWave

Before the CSR can be uploaded to Apple, it must be signed by FileWave.

1. Navigate to <https://csr.filewave.com/> and log in with your FileWave account.
2. Upload the previously created .csr file.
3. Under Download signed CSR, your uploaded CSR should now appear as signed.
4. Download this newly signed CSR – this is the file you will upload to Apple in the next step.
5. Store the file in a secure location.



Signed CSR list		
Original CSR filename	CSR Upload Date	Download signed CSR
CertificateSigningRequest.certSigningRequest	July 16, 2012, 2:18 p.m.	Download
CertificateSigningRequest.certSigningRequest	Aug. 5, 2014, 11 a.m.	Download

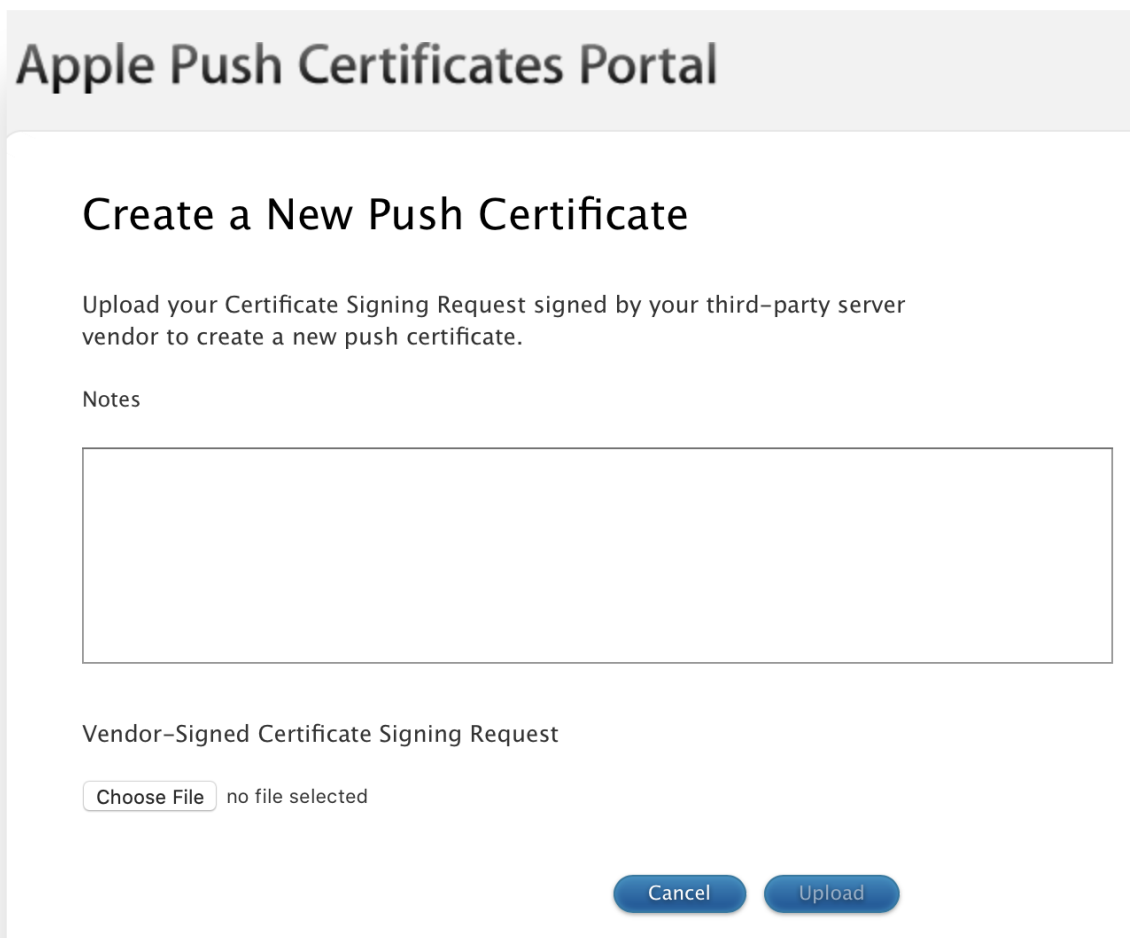
Step 3: Upload the signed FileWave CSR to Apple

If you are renewing a certificate then jump to [Renewing a Certificate](#)

Creating a new certificate

1. Go to the Apple Push Certificates Portal: <https://identity.apple.com/pushcert/>.
2. Sign in with an Apple ID (⚠ do not use a personal Apple ID – use a generic business or institution Apple ID for long-term use).
3. Click Create.
4. Accept Apple's Terms of Use.
5. Click Choose File and upload the signed FileWave CSR.
6. Click Upload – Apple will confirm the request.

7. Download the issued APNS certificate (.pem or .cer).



The screenshot shows the 'Apple Push Certificates Portal' interface. At the top, the title 'Apple Push Certificates Portal' is displayed in a large, bold, dark font. Below this, the main heading 'Create a New Push Certificate' is centered. A paragraph of instructions follows: 'Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.' Below the instructions is a section labeled 'Notes' with a large, empty rectangular text area. Underneath the text area is the label 'Vendor-Signed Certificate Signing Request'. Below this label is a file selection interface consisting of a button labeled 'Choose File' and the text 'no file selected'. At the bottom right of the form are two blue buttons: 'Cancel' and 'Upload'.

Renewing an existing certificate

1. Go to <https://identity.apple.com/pushcert/> and log in with the same Apple ID that owns the certificate.
2. Locate the certificate to renew, confirm the Subject DN (Topic) matches the certificate in FileWave Central.
3. Click Renew.
4. Upload the signed FileWave CSR.
5. Download the renewed APNS certificate (.pem or .cer).

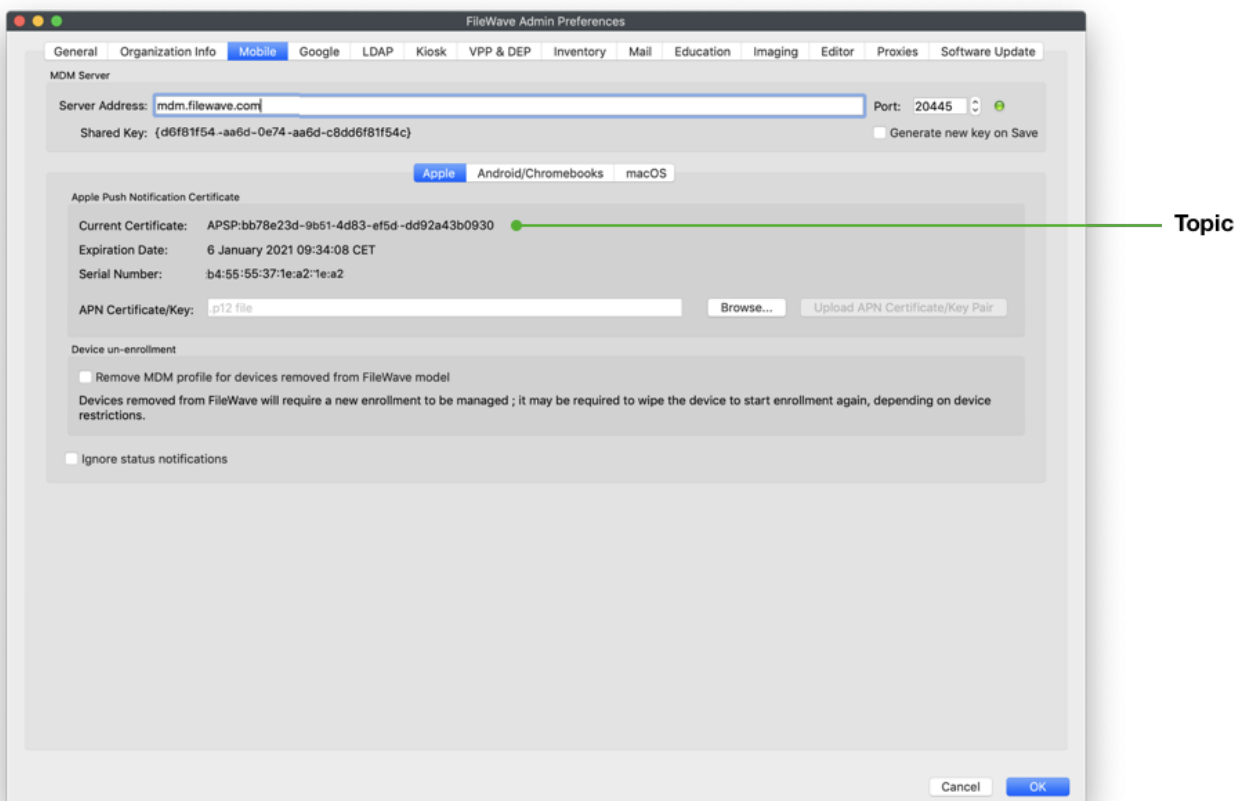
i If the topics do not match, do not continue. If the correct certificate is not in the list on Apple's website, this is the wrong Apple ID. If this guide was followed in creating the original certificate, the previously used Apple ID will be viewable from the certificate "Private Key".

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

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



Confirm that it matches Current Certificate in FileWave Central under Preferences > Mobile > Apple Push Notification Certificate:

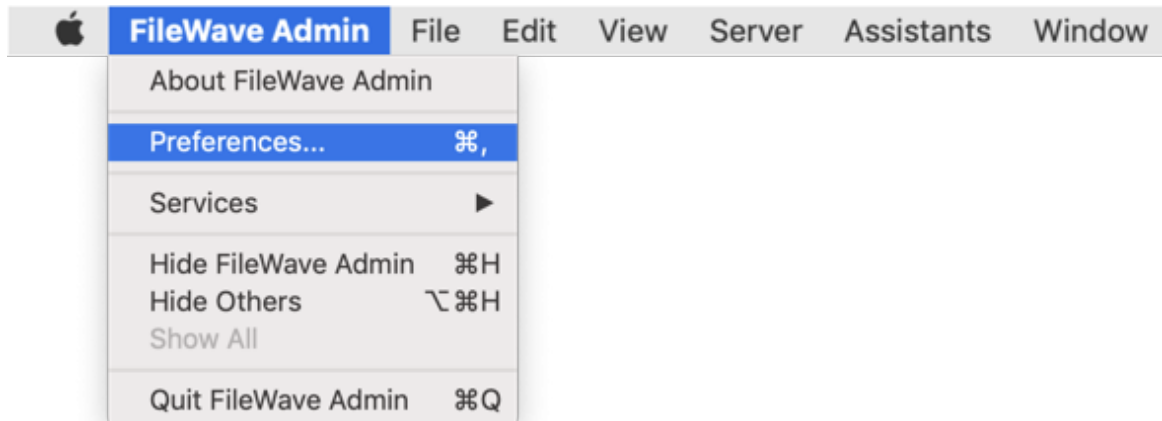


Step 4: Import and process the certificate in XCA

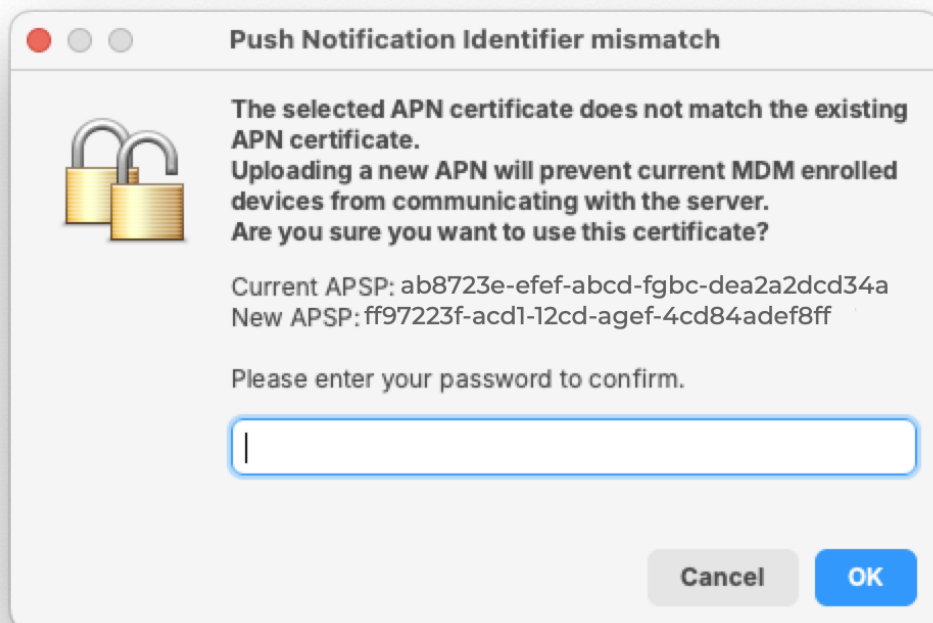
1. First, download XCA for macOS: <https://github.com/chris2511/xca/releases>
2. Install and start XCA.
3. Go to Private Keys → Import and select the previously saved .key file from Step 1.
4. Go to Certificates → Import and load the APNS certificate you downloaded from Apple (.cer/.pem).
5. Link the certificate with the corresponding private key in XCA.
6. Export the certificate as a PKCS #12 (.pfx) file – important: without a password.
7. After export, rename the .pfx file to .p12 (FileWave requires the .p12 extension).

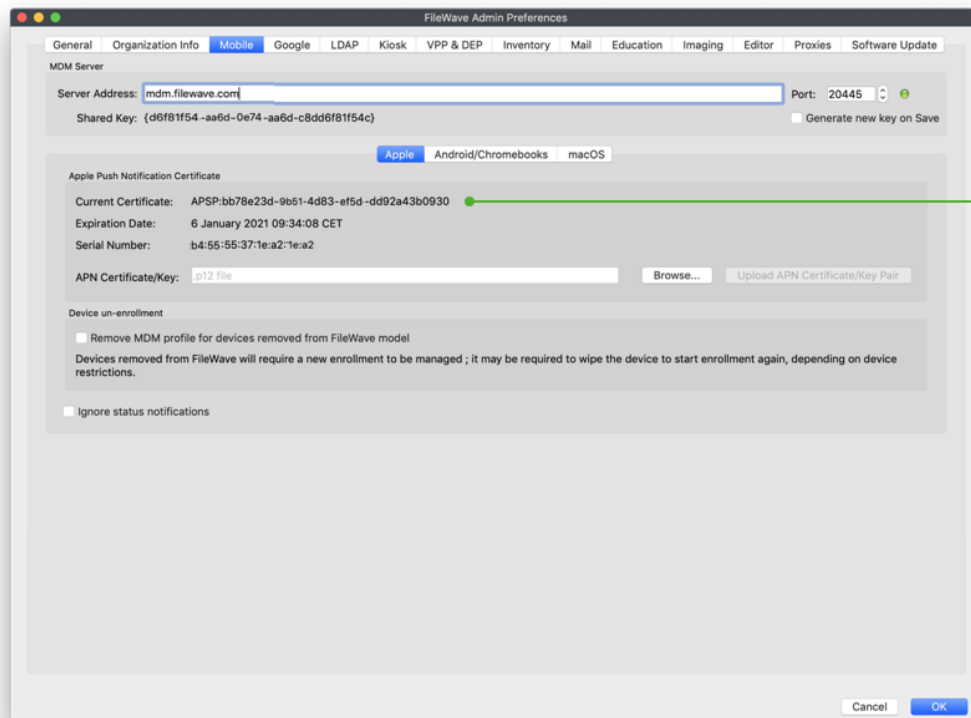
Step 5: Import the certificate into FileWave

1. Open the FileWave Admin.
2. Go to Preferences → Mobile.



3. Import the .p12 file you exported from XCA by browsing to the file and then picking to Upload. For a renewal, the topic must match the previous certificate. FileWave Central warns if the topics do not match before accepting the upload.





4. Save the settings by clicking OK to close the preferences dialog and verify that devices are communicating.

Step 6: Verification

- Test whether new or existing MDM clients correctly connect to the APNS service.
- Check the logs in FileWave Admin to ensure there are no certificate errors.



Set a renewal reminder. In FileWave Central, open Dashboard > Alert Settings and add the APN for MDM email alert. Automated alerts also require the email settings in Central to be configured.

Contact Apple for help

If you cannot identify the Apple ID associated with the Apple Push Notification certificate, contact Apple for help.

[Contact Apple for help with APNs certificates](#)

Related articles

- [APNs Certificate Creation & Renewal on macOS Computers \(Keychain\)](#)
- [APNs Certificate Creation & Renewal on Windows](#)

🕒 Revision #8

★ Created 2025-10-01 12:55:22 UTC by Josh Levitsky

✎ Updated 2026-08-05 12:58:36 UTC by Josh Levitsky