APNs

MDM/DDM communication relies upon Apple's APNs cloud service.

- Apple Push Notification Service
- APNs Certificate Creation & Renewal on macOS Computers
- APNs Certificate Creation & Renewal on Windows Computers

Apple Push Notification Service

What

- Like to know a new message has been sent?
- Want to see how many messages are unread from the Home Screen, per App?

> The following is really just for information, describing APNs.

Push Notifications are mostly designed to allow 3rd party Apps the ability to inform users through their App, e.g. messages, sounds, etc. some relevant detail. Users control which messages are silenced or visible and how they are visible through Settings.

Developers of Apps requiring this service register their App with Apple. This process requires an APNs token, integrated into the App's Server.

> Generation of an APNs token itself is a required action by FileWave Admins as per the other KB articles in this chapter.

For APNs to succeed, the App and 3rd party server must be able to trust Apple's APNs Cloud Service. Hence, Trust Stores must include Apple's APNs Root Certificate.

APNs Certificate Update:

At times the Root Certificate used by APNs will require replacing, prior to expiry.

APNs Cert	Service	Up to Date	From Date	Expiry Date
AAA Certificate Services root certificate	Sandbox	Jan 2025	-	Dec 31 23:59:59 2028 GMT
	Production	Feb 2025	-	
SHA-2 Root : USERTrust RSA Certification Authority certificate	Sandbox	-	Jan 2025	Jan 18 23:59:59 2038 GMT
	Production	-	Feb 2025	

Apple will supply information when this occurs, ensuring developers of Apps and providers of 3rd party servers update their products.

> FileWave Server already includes both of the above listed certificates within its Trust Store.

3rd Party Apps

The act of installing an App requiring APNs, registers that App with APNs and the device receives a Unique Device Token.

Messages pushed can include:

- Display Alert Message to User
- Apply Badge Icon to App's Icon
- Play a Sound
- Deliver Notification Silently

Both Message and Unique Device Token are sent by the App's Server when attempting to initiate a notification.

Notifications are relayed through Apple's APNs service. On receipt of the notification, the device will act accordingly, e.g. display a message to user.

In essence, the message payload therefore consists of:

- APS Dictionary: Message content
- Alert Keys: Assist notification processing, e.g. an identifier to a particular conversation of a messaging app.
- Device ID: Unique Device Token

> The App should contain the current APNs Root Certificate within its Trust Store

MDM/DDM

MDM communication also relies upon the APNs service and therefore is an example of this process, but key aspects are:

- The act of enrolment is equivalent to installing the App, initiating the receipt of the Unique Device Token.
- The App in question is a binary, included in the Operating System by Apple: '/usr/libexec/mdmclient'.
- APS dictionary should not be included in the payload from an MDM server.

MDM APNs messages are nothing more than a request for the device to contact the MDM server. Any commands are subsequently sent directly to the device, once the device responds back to the MDM server from this APNs request.

Since Apple are the developers of the 'mdmclient', Apple manage its Trust Store. Apple's list of supported Root Certificates per OS version are available from their KB:

https://support.apple.com/en-gb/103272

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.

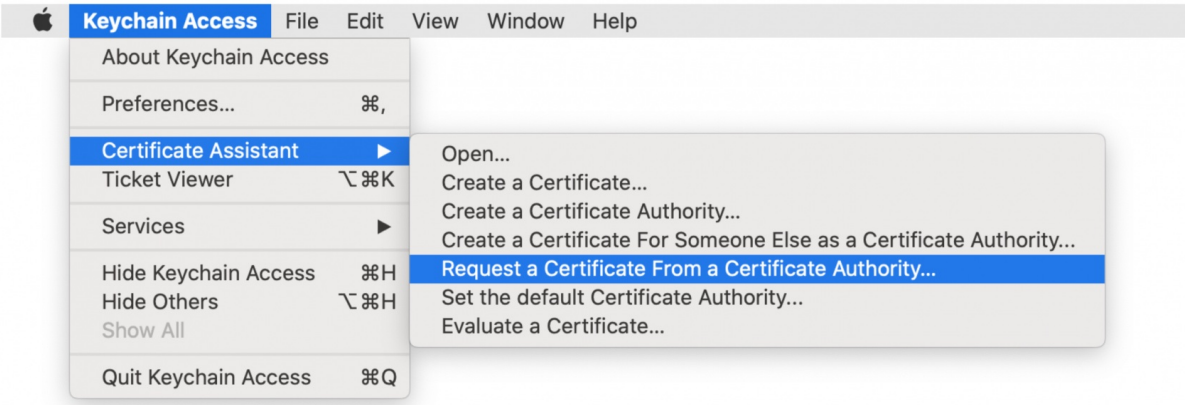
The following guide provides the steps to create and renew an APNs certificate using macOS.

> 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

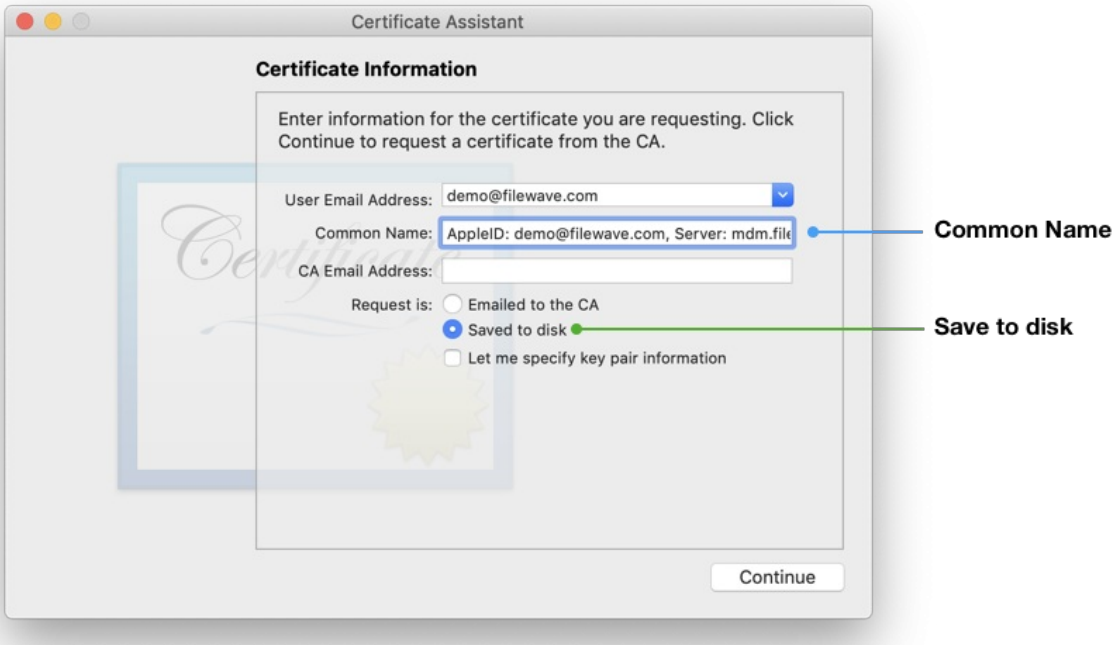
Creating the Certificate Signing Request (CSR)

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.



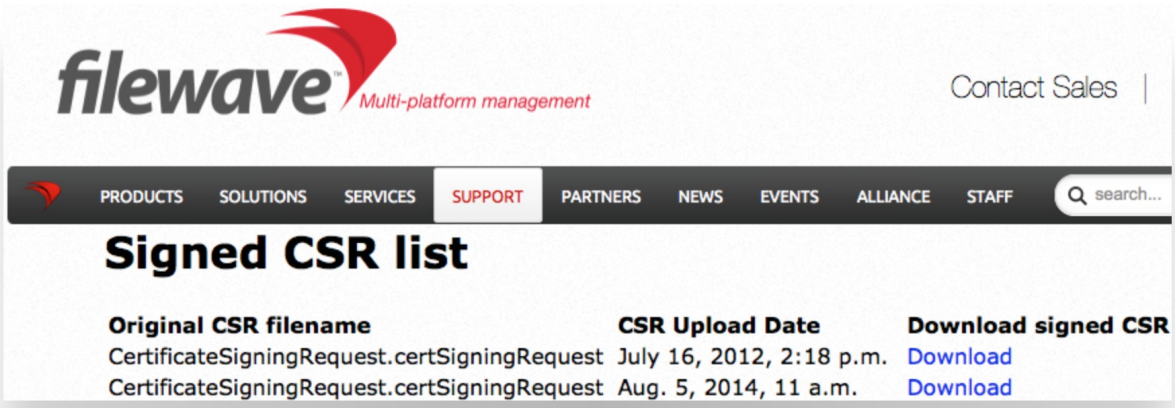
4. Select the radio button "Saved to disk" and click Continue.
5. Save the CSR request, ready to upload to FileWave in the next section.

> 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.



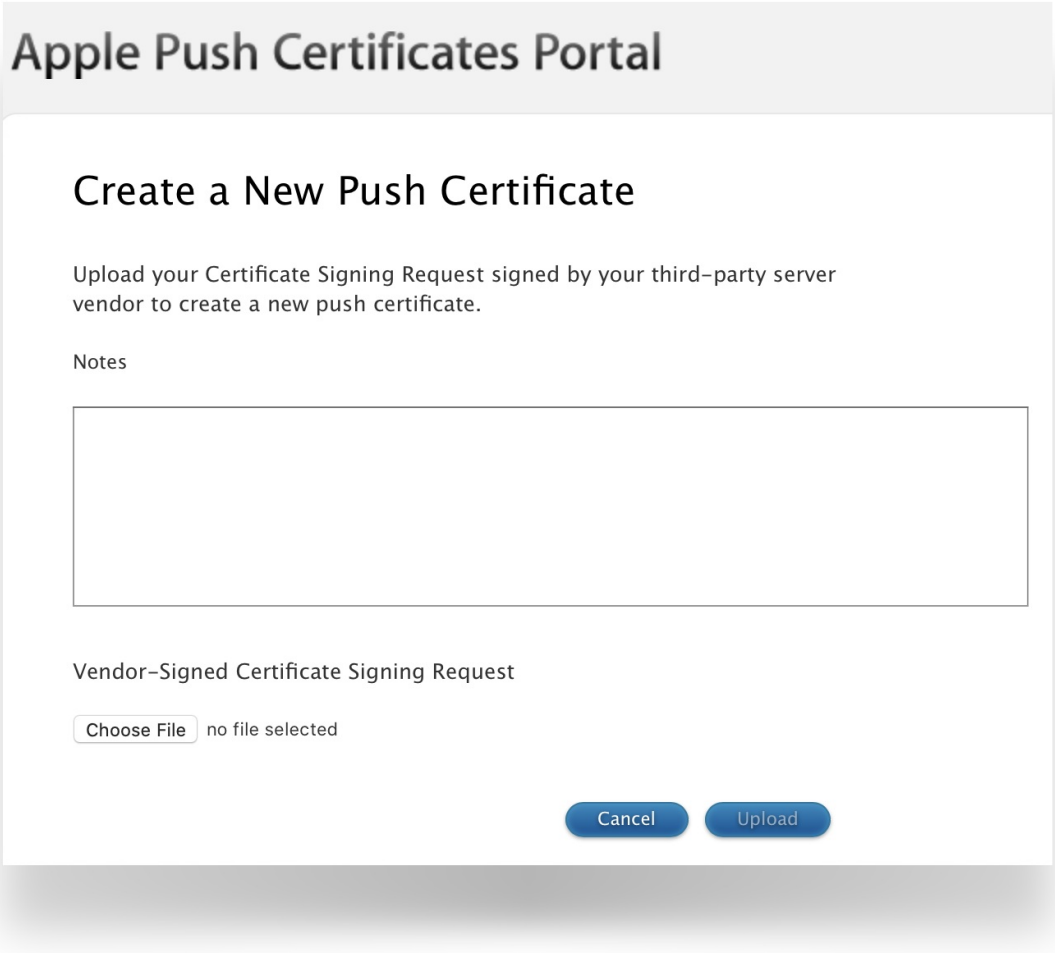
Upload the signed FileWave CSR to Apple

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'.

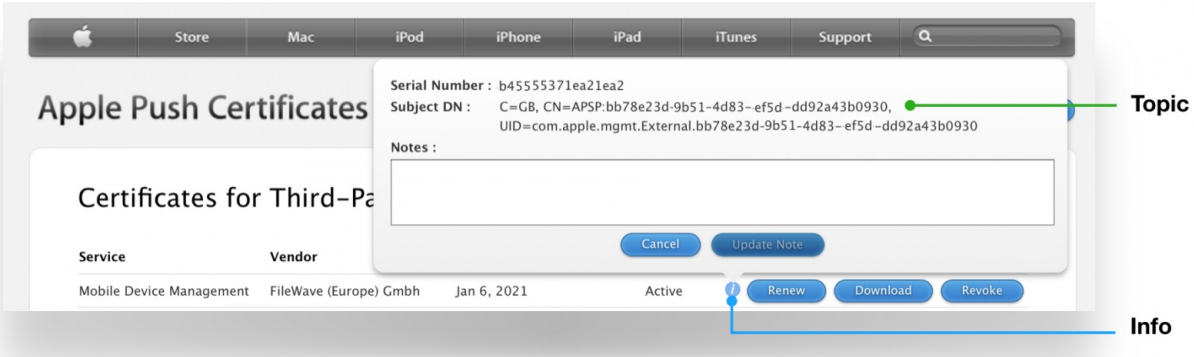


Renewing a Certificate

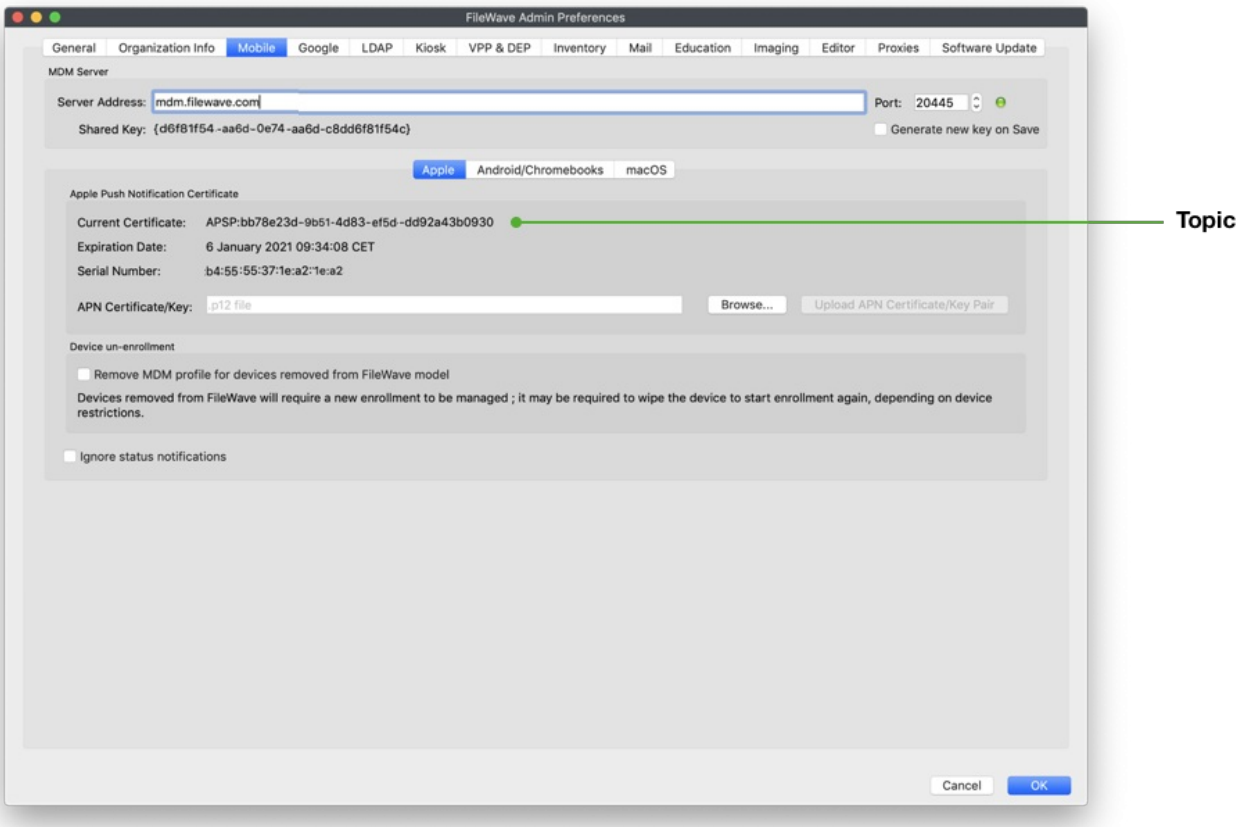
1. Navigate to: https://identity.apple.com/pushcert/ and log in with the Apple ID used to initially create the certificate.
2. Confirm the Certificate to renew.
3. Select 'Renew'.

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

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



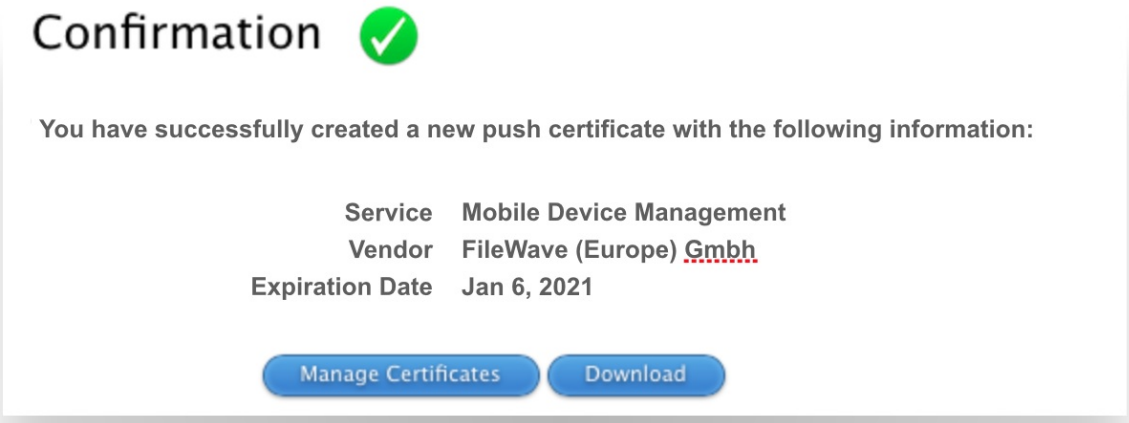
Ensure this matches with the 'Current Certificate' in FileWave Admin > Preferences > Mobile > Apple Push Notification Certificate:



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.

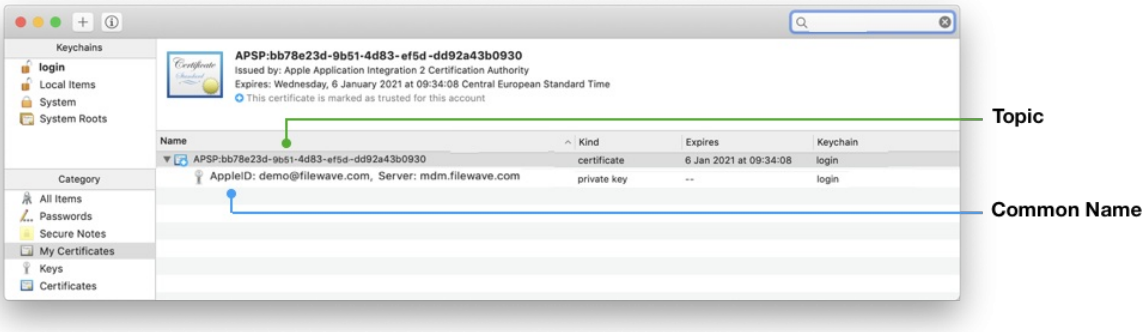
Create a ".p12" from the Signed CSR

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

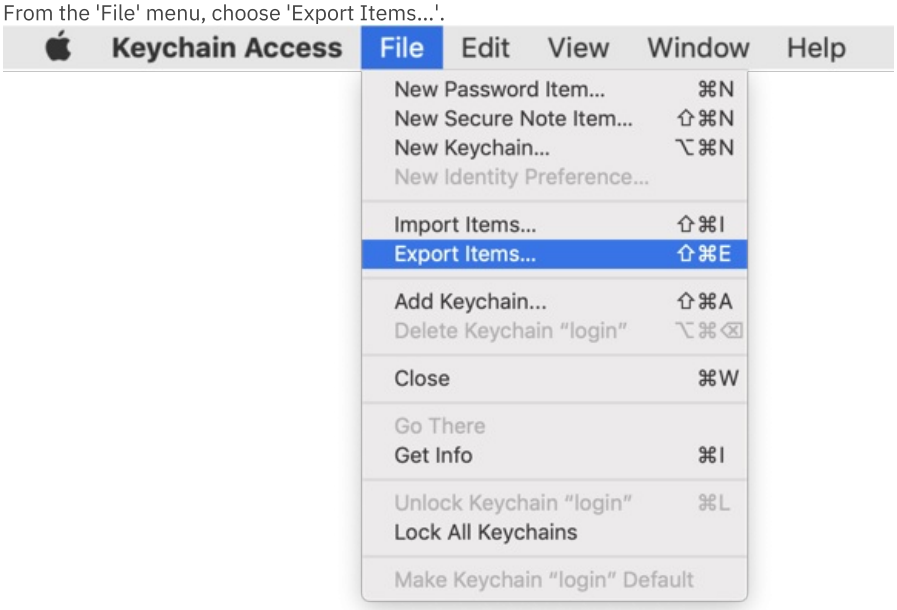
> Keychain
> If imported into the System Keychain, the Private Key will not be accessible. If 'All Items' tab is selected, private keys will not be available!

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.

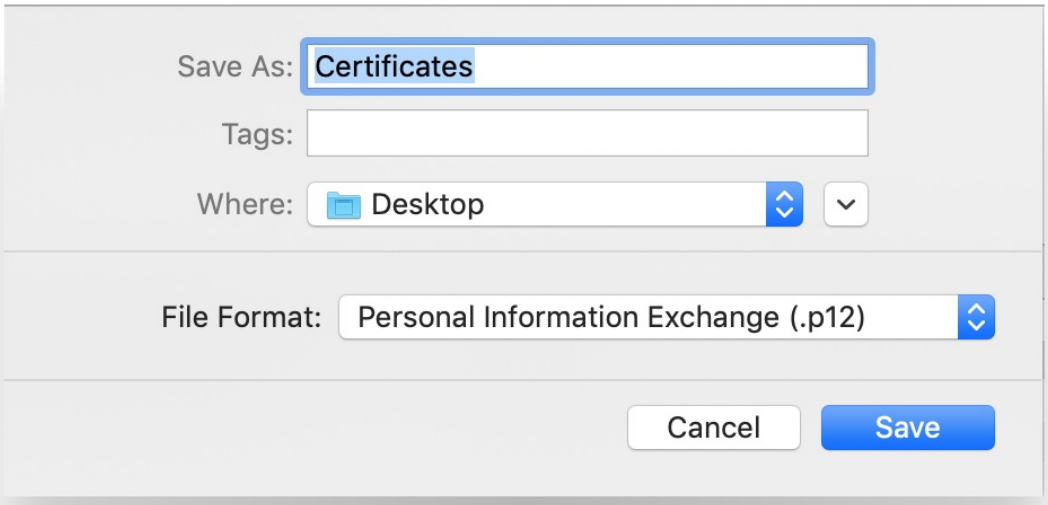
> Common Name and Topic
> The name of the Private Key will show the value defined as the "Common Name" from the creation of the CSR. Where recommendation was followed, this should list the Apple ID and Server name. Additionally the name of the Certificate is the same as the Topic.



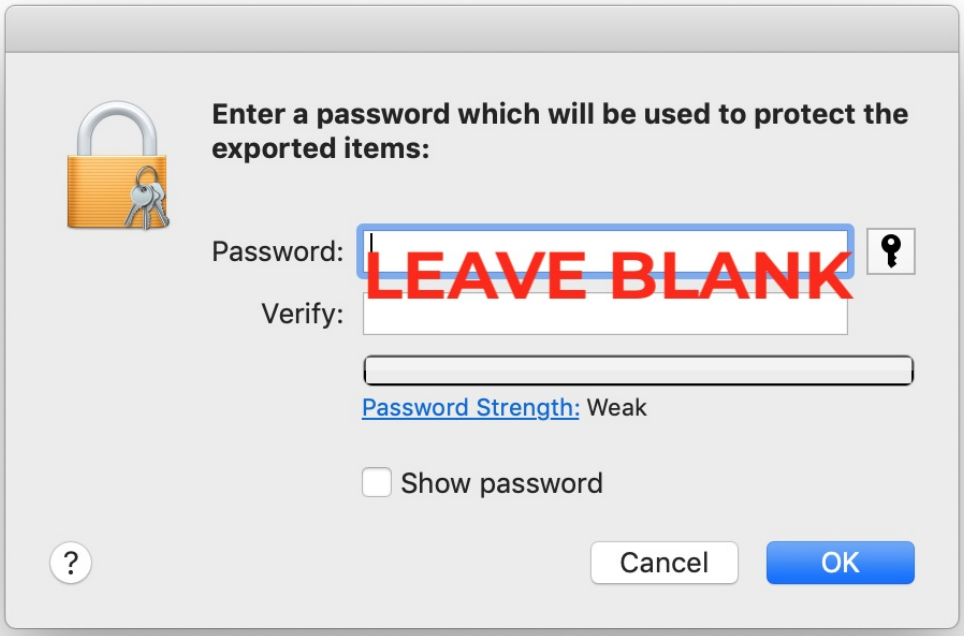
5. From the 'File' menu, choose 'Export Items...'.



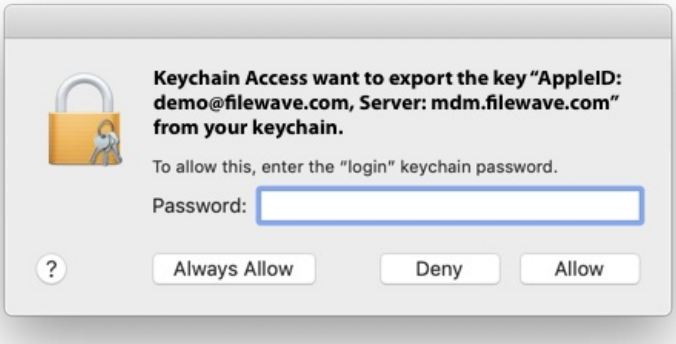
6. Export as a .p12 file. Again consider where this certificate is stored.
7. Click Save.



8. Leave the password blank.

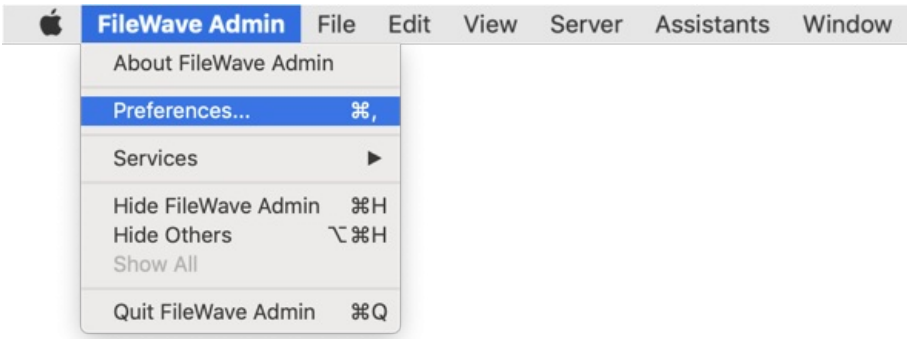


9. Enter your local admin account, when prompted, allowing Keychain to export.

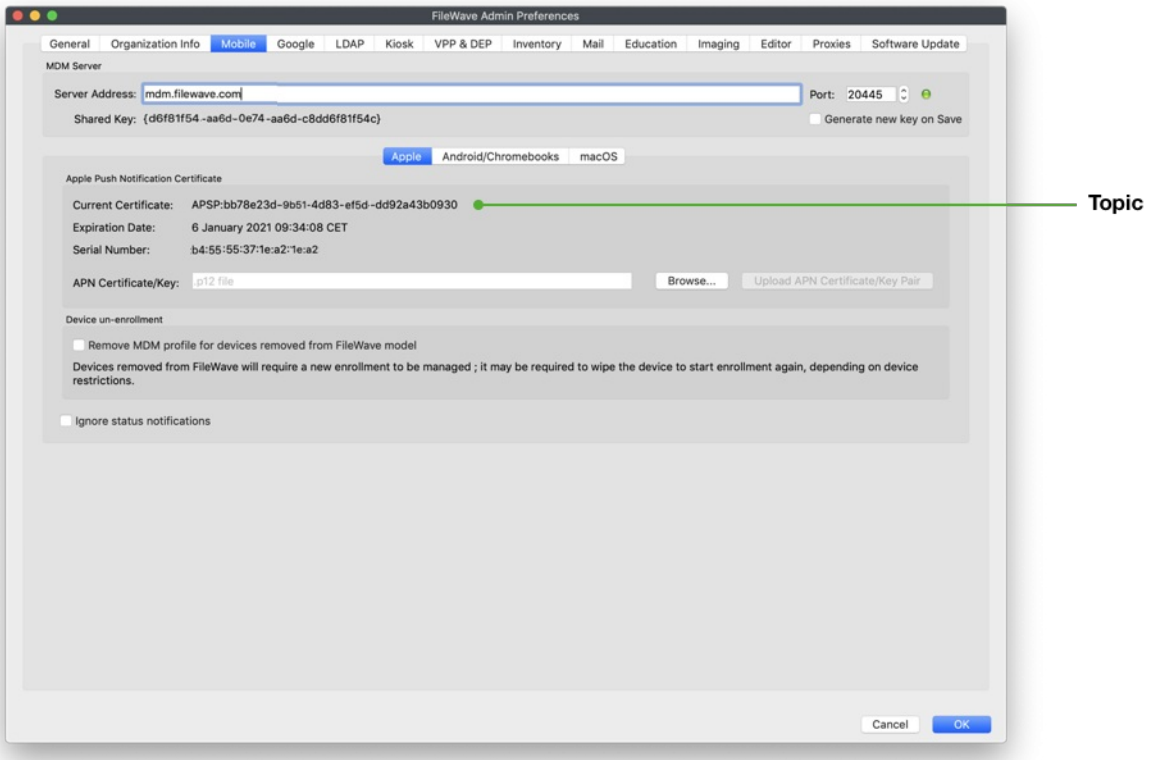


Uploading the Certificate into FileWave

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

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

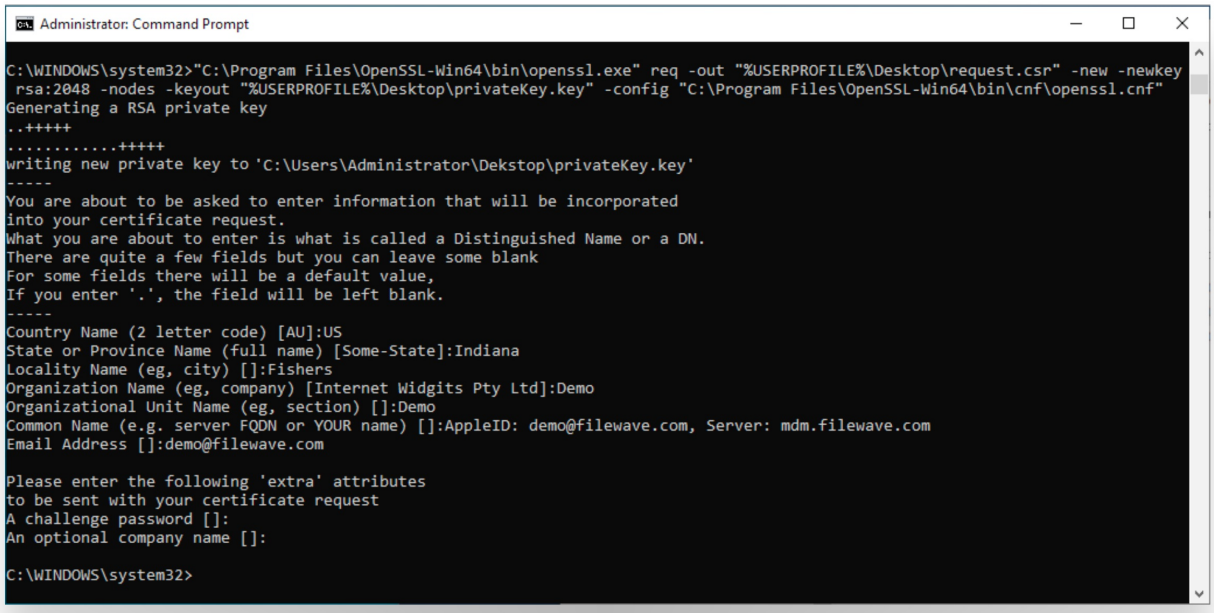
- Creating the Certificate Signing Request (CSR)
- Sign the CSR
- Upload the signed FileWave CSR to Apple
  - Creating a Certificate
  - Renewing a Certificate
- Create a ".p12" from the Signed CSR
- Uploading the Certificate into FileWave
- Related articles

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"
```

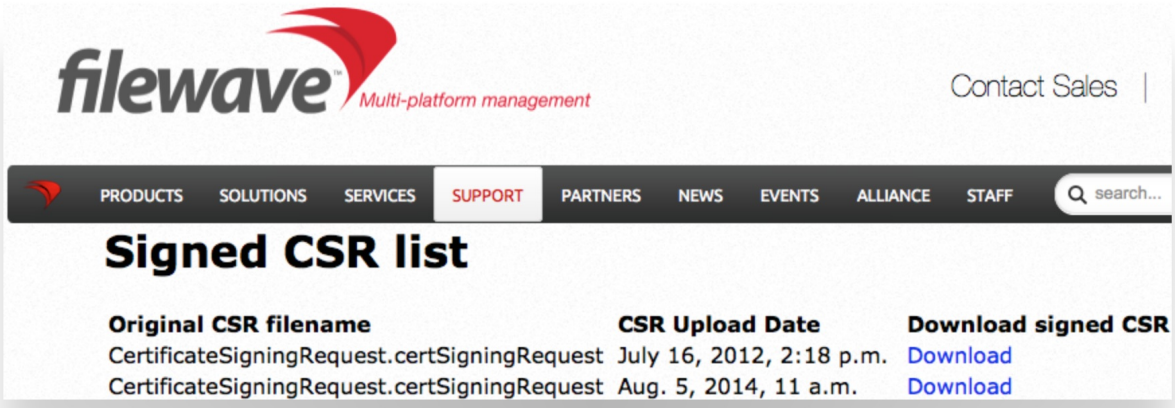
> ℹ Certificate Private Key names are visible from openssl commands and the Common Name is used to set the Private Key name. Supplying the Apple ID and Server as the Common Name, ensures the Apple ID used to generate the certificate will be stored for future reference.



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.



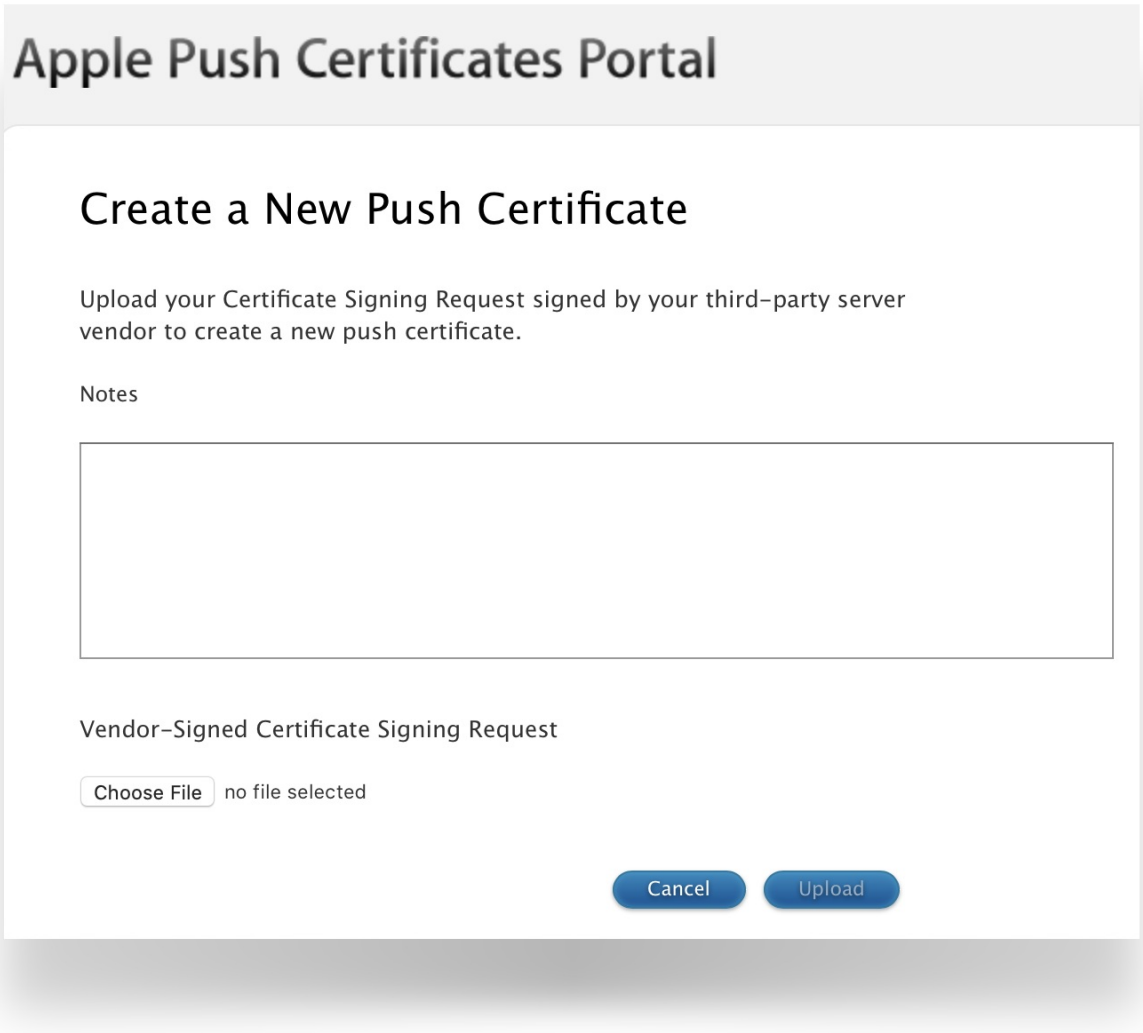
Upload the signed FileWave CSR to Apple

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'.

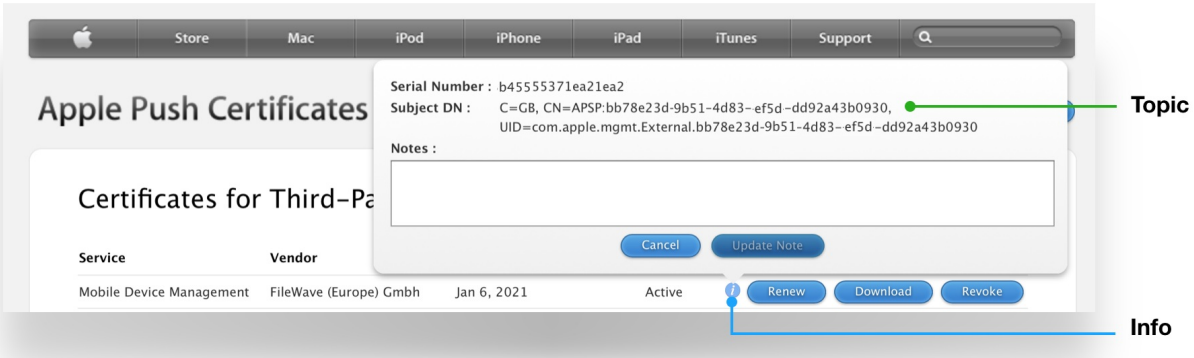


Renewing a Certificate

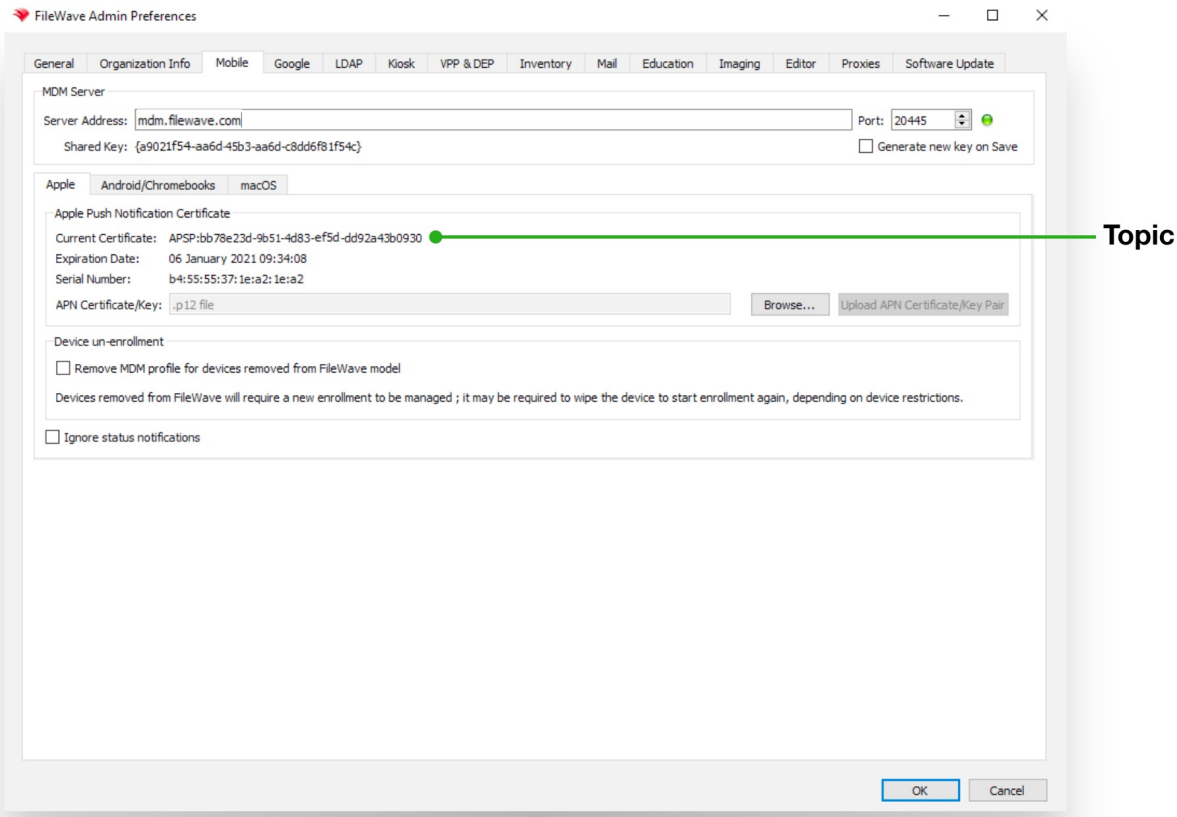
1. Navigate to: https://identity.apple.com/pushcert/ and log in with the Apple ID used to initially create the certificate.
2. Confirm the Certificate to renew.
3. Select 'Renew'.

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

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



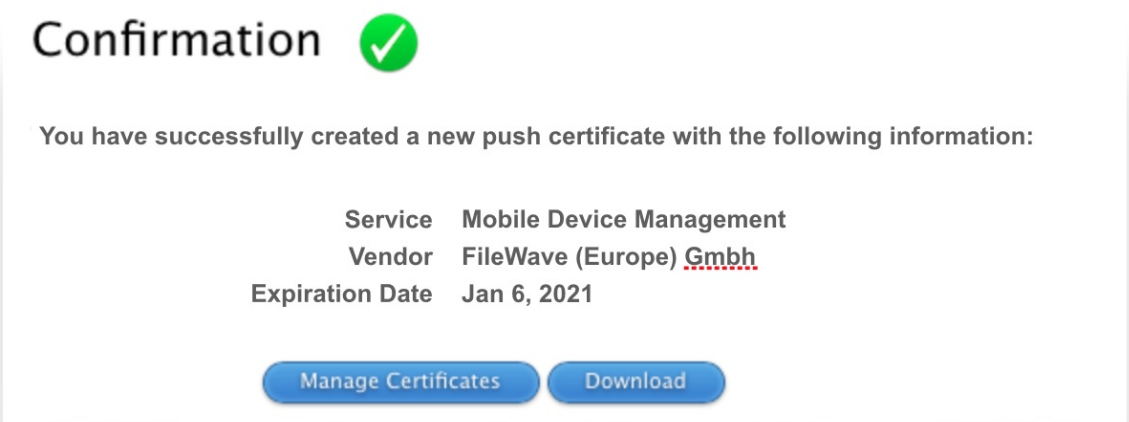
Ensure this matches with the 'Current Certificate' in FileWave Admin > Preferences > Mobile > Apple Push Notification Certificate:



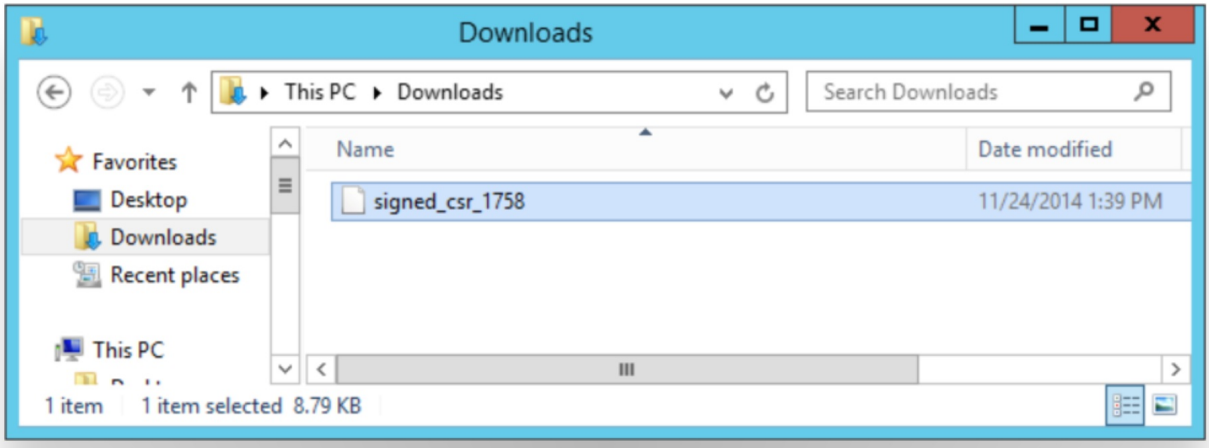
If the 'Topics' do not match do not continue. If the correct certificate is not in the list on Apple's website, this is the wrong Apple ID. If this guide was followed in creating the original certificate, the previously used Apple ID will be viewable from the certificate "Private Key".

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.



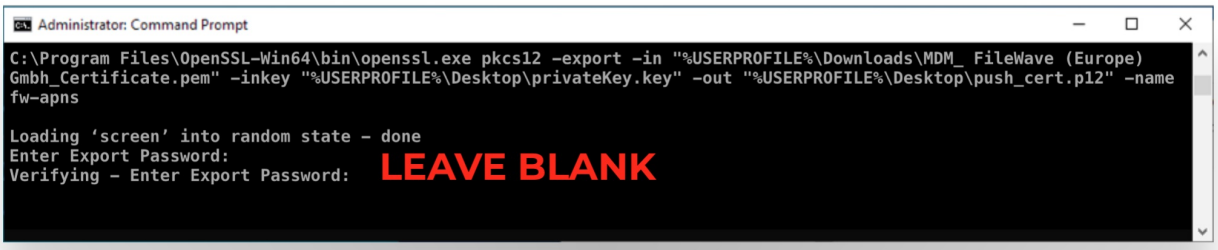
Create a ".p12" from the Signed CSR

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

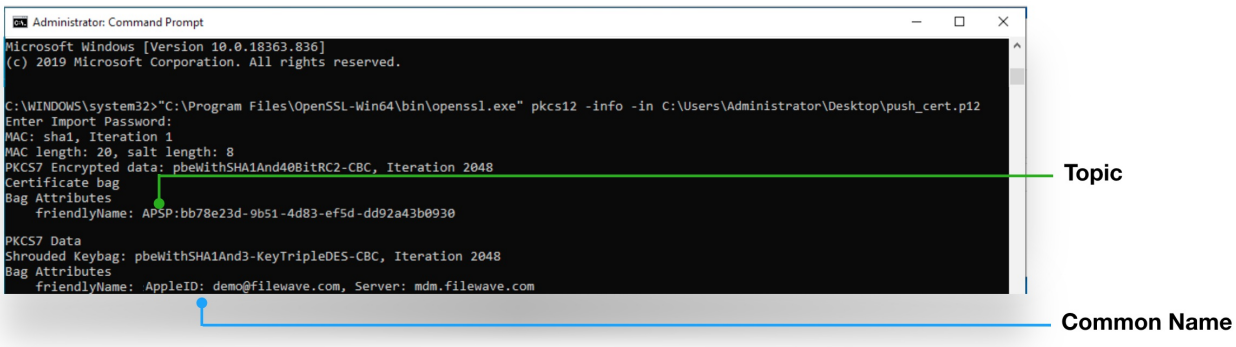


1. Certificate details may be checked:

> 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.

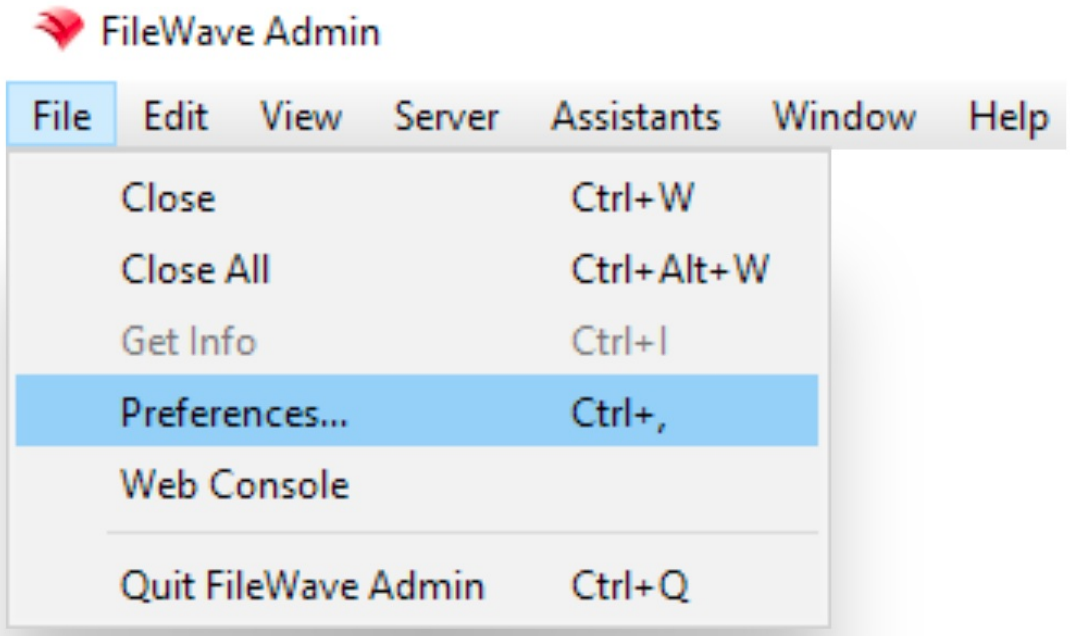
```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -info -in C:\Users\Administrator\Desktop\push_cert.p12
```

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

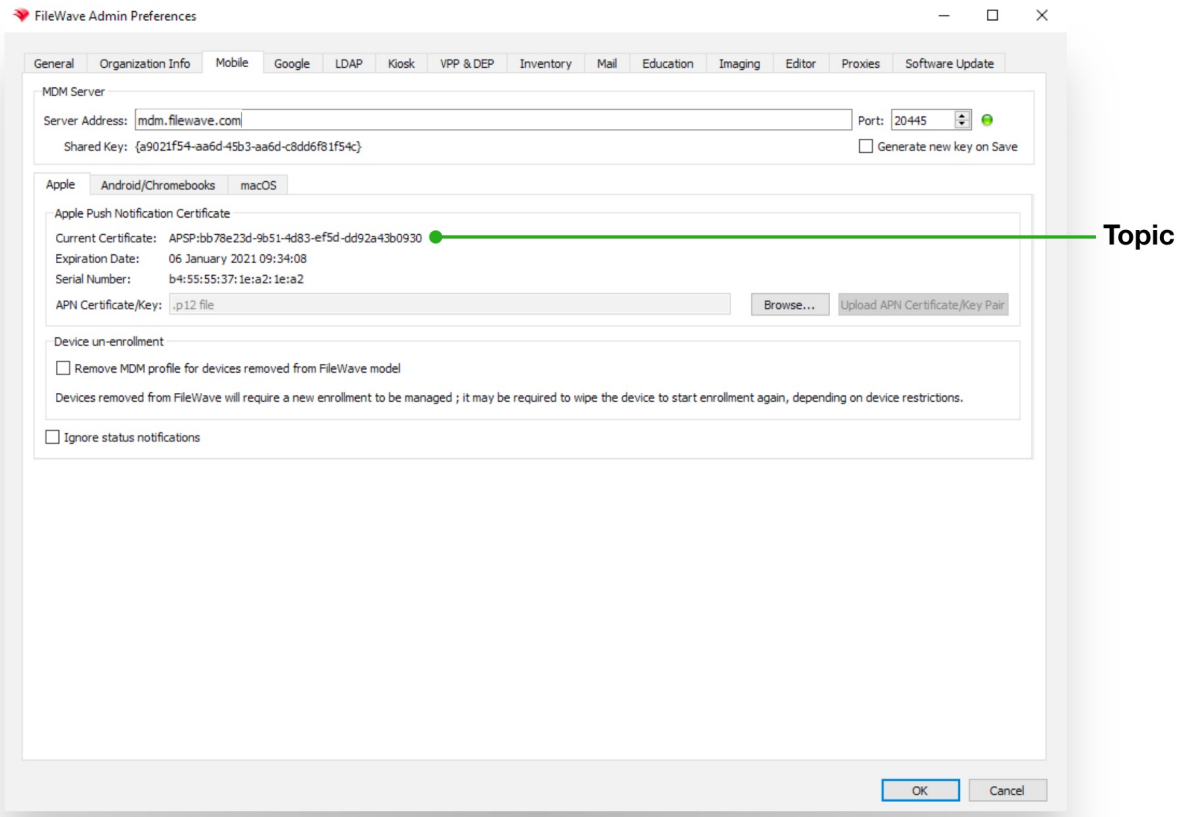


Uploading the Certificate into FileWave

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