

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>

🔄Revision #2

★Created 10 December 2024 13:28:41 by Sean Holden

✍Updated 10 December 2024 14:06:33 by Sean Holden