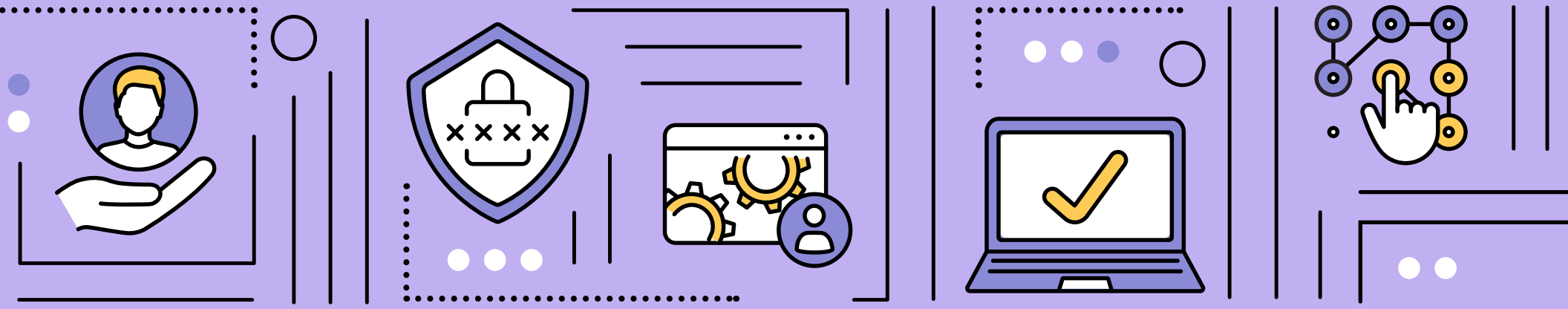
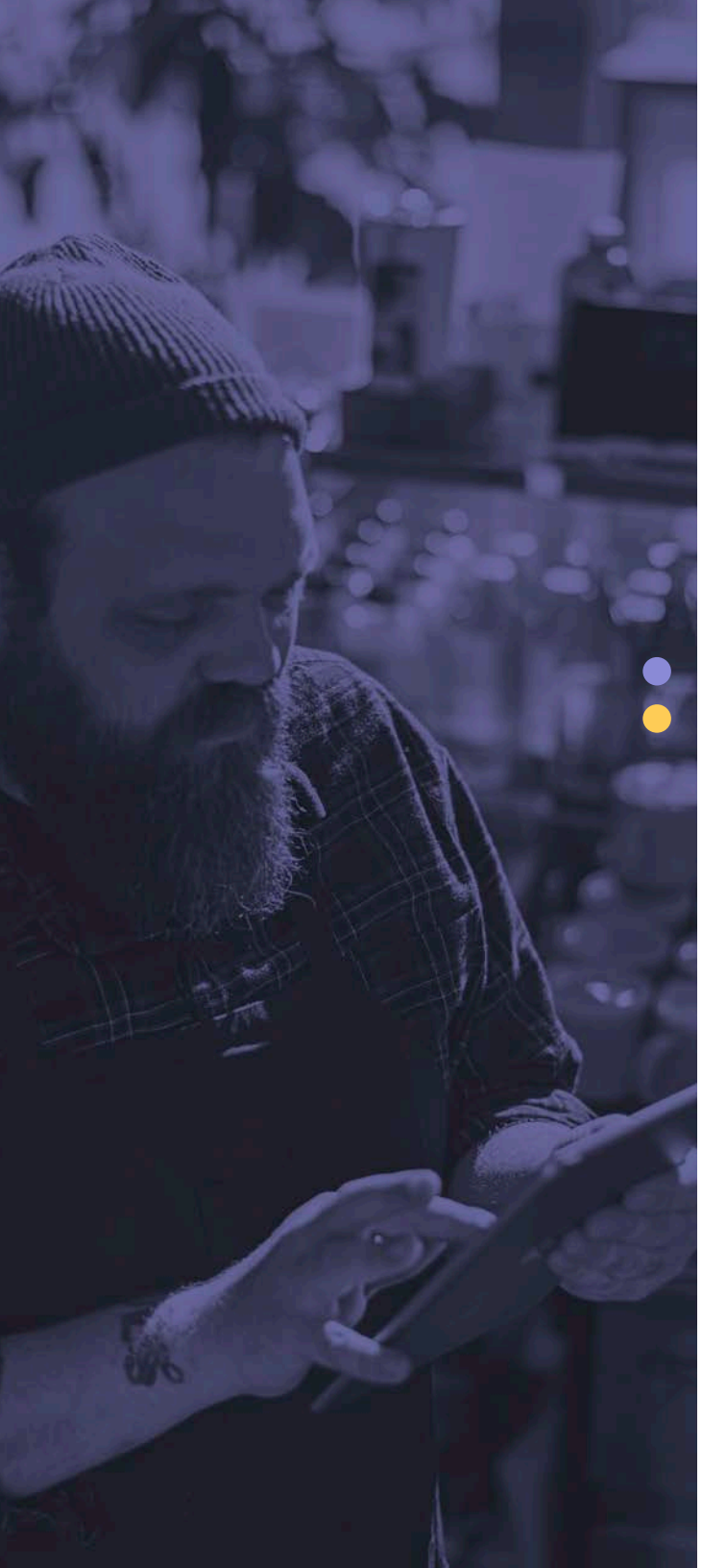
jamf

Apple Push Notification Service

for Beginners

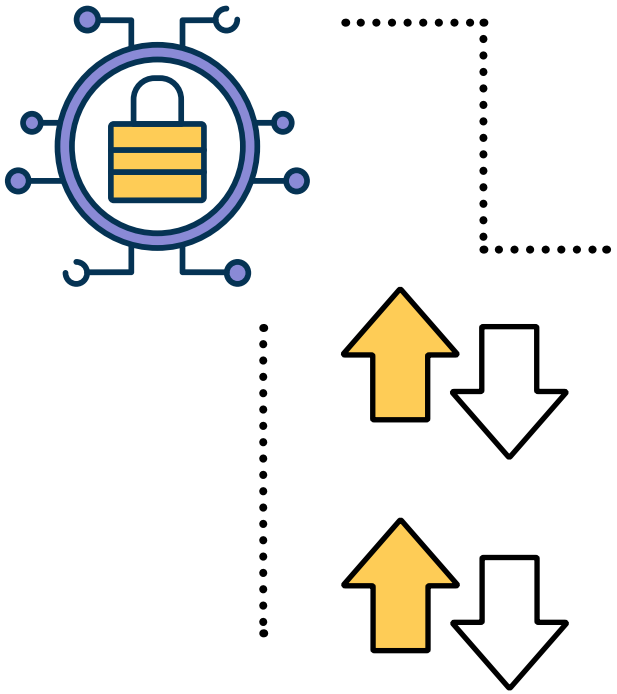




Managing devices in the Apple ecosystem can be a straight-forward process when it comes to basic management commands.

If you wish to reboot a computer remotely, simply highlight the device's record in your mobile device management (MDM) solution and select the "Restart Device" button to issue the command. Easy, right? But exactly how does that magic happen?

The answer to that question is the Apple Push Notification service – or APNs, for short – which serves as the crux for communication between the endpoint and MDM server. This will be the topic covered in this document, from initial steps to set up through confidently ensuring the notification service remains operational.



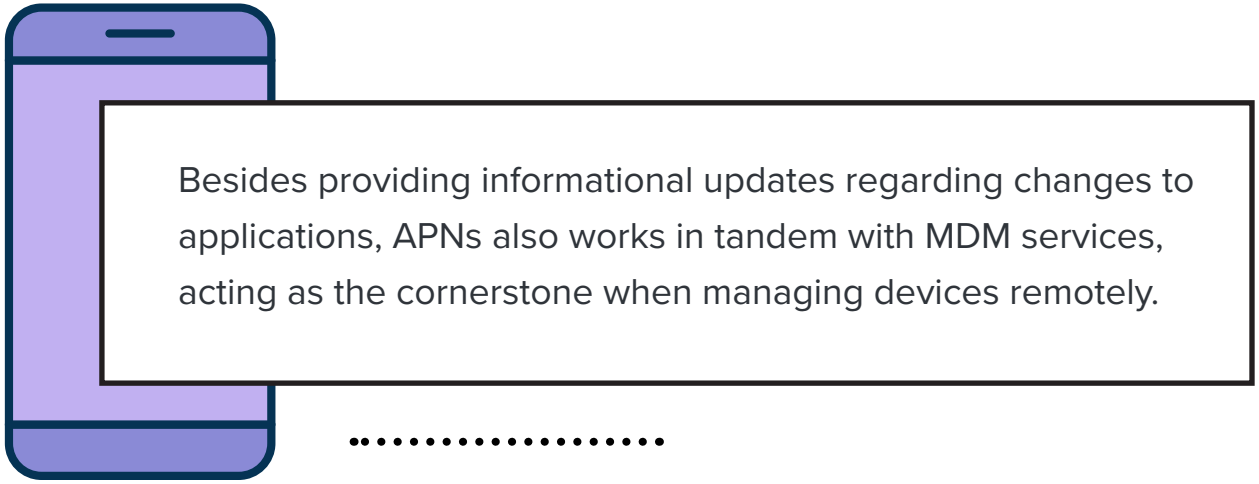
Covered in this e-book:

- What APNs does and how this service works
- Why APNs is crucial to device management
- Best practices to keep APNs fully functional

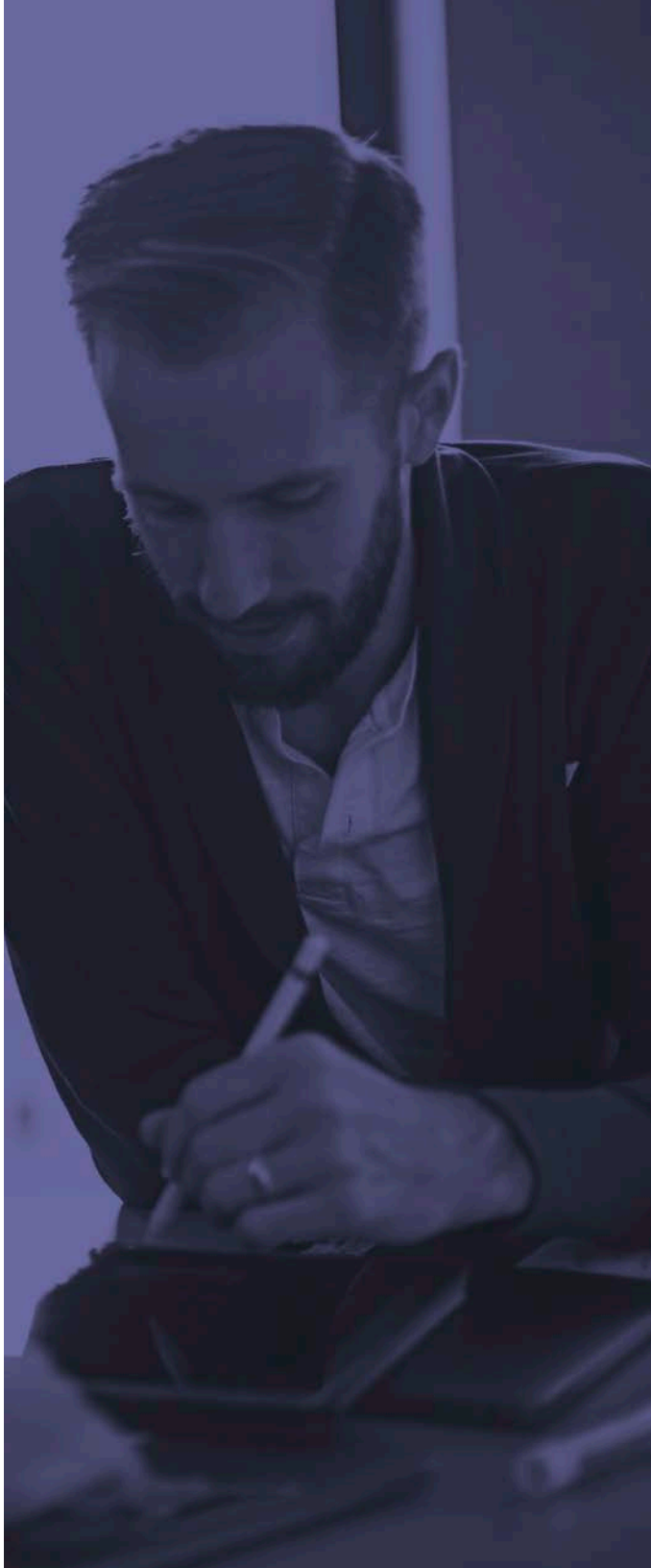
APNs 101

According to Apple, “Local and push notifications are great for keeping users informed with timely and relevant content, whether your app is running in the background or inactive. Notifications can display a message, play a distinctive sound, or update a badge on your app icon.”

In essence, APNs is the delivery method for communications sent to apps. These notifications provide updates to the user, informing them of changes in state of the app or system. For example, when a new email message arrives in your inbox, the email server denotes this change and promptly uses APNs to alert the end user via the app on their Apple device that a new message has been received.



Besides providing informational updates regarding changes to applications, APNs also works in tandem with MDM services, acting as the cornerstone when managing devices remotely.



Communication is key

Mirroring the modern computing landscape where communication is the lifeblood of productivity worldwide, it too is a core tenet to keeping applications updated on Apple devices, notifying users of important messages, and ensuring devices are both enrolled in MDM and remain compliant with configuration profiles and security policies.

The fact is that without this integral component in place, the link between endpoints and the MDM server that manages them will be severed. This results in a direct loss of communication with the endpoint, and thus, renders devices unmanageable by IT.

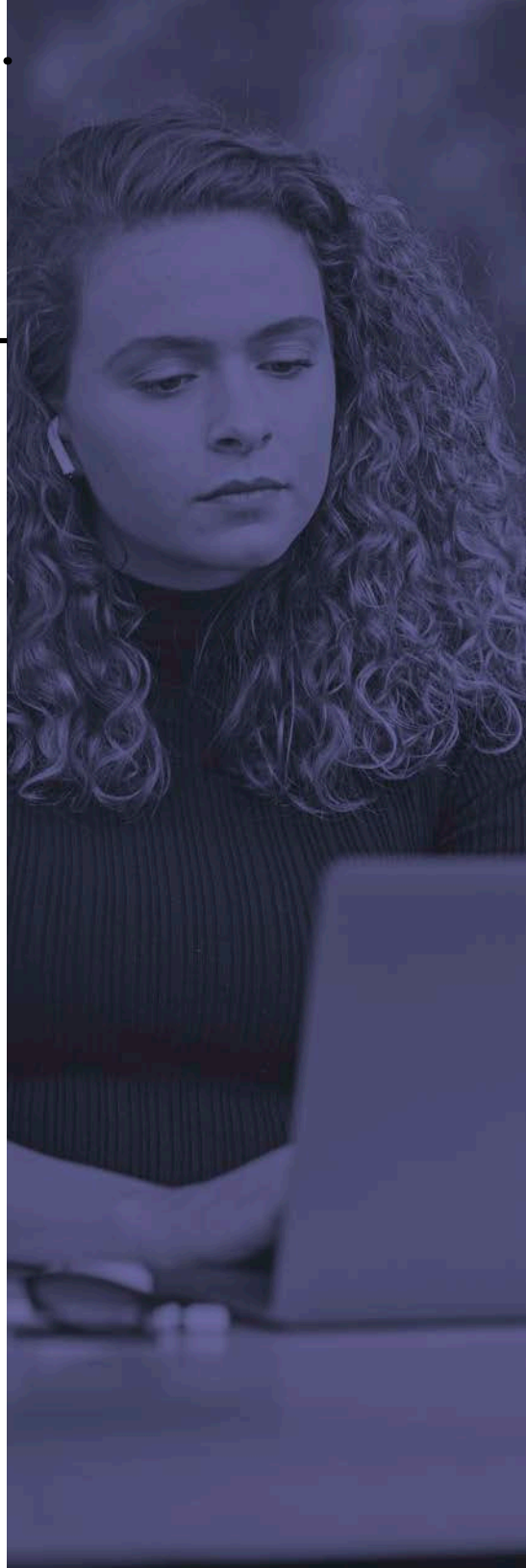
> It's important to note that despite the loss of management capability, any apps or configurations that have been deployed will remain intact, however the devices themselves – along with all apps and configurations – will not update until the connection to APNs is restored.

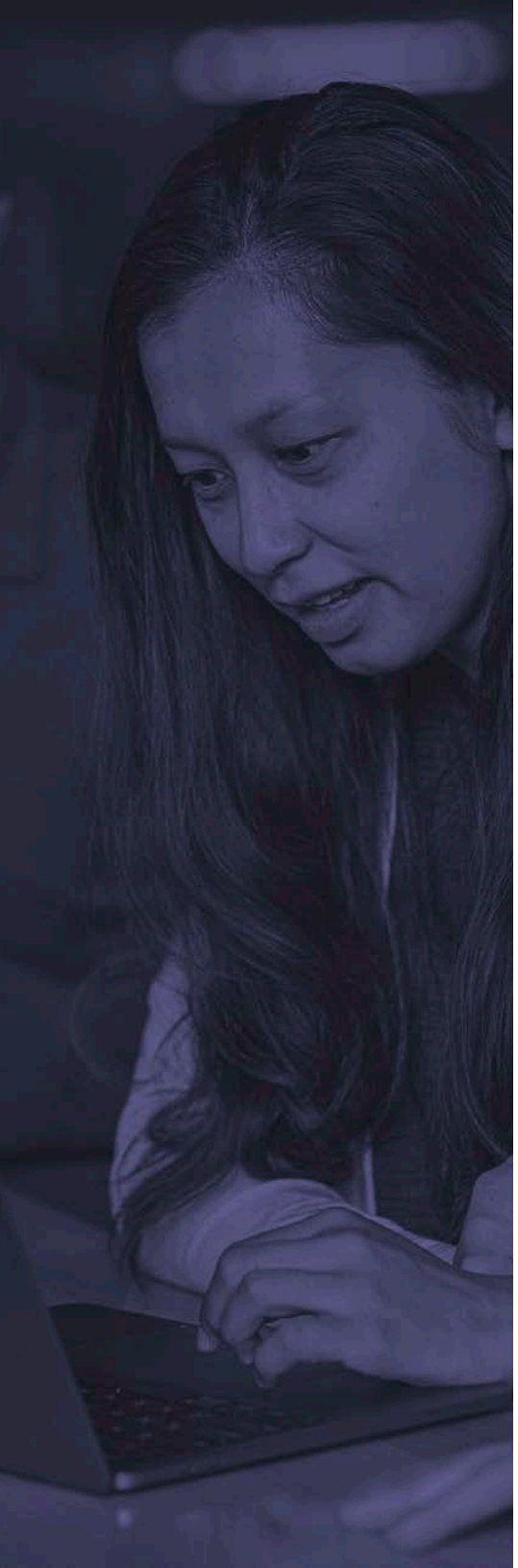
How APNs works

So, you might be thinking this covers what APNs is and why it's so important, but how exactly does it work? Actually, it's quite simple as illustrated in the diagram below.

As you can see, the provider in this case is the developer or service that maintains a constant connection to Apple's Push Notification Services cloud, which acts as a proxy of sorts to Apple devices. The initial message is sent by the MDM provider to APNs, which in turn, forwards the message to the device itself where it is processed by the app, ultimately delivering the notification to the end user.

While the above example describes the process in general, it does not fully address how a management system, like Jamf, uses it to manage devices. In this case, IT would login to the Jamf console (Jamf Pro, Jamf School or Jamf Now) and select which commands they wish to deploy after identifying the device(s) they wish to target. In a management scenario, the command or configuration profile that is sent from Jamf contains a payload specifying the specific command(s) to be processed on the targeted device(s). The notification is sent to APNs, then routed to the device(s) in scope. Once they arrive at the target device(s), the command(s) are processed by the operating system and executed, as intended.





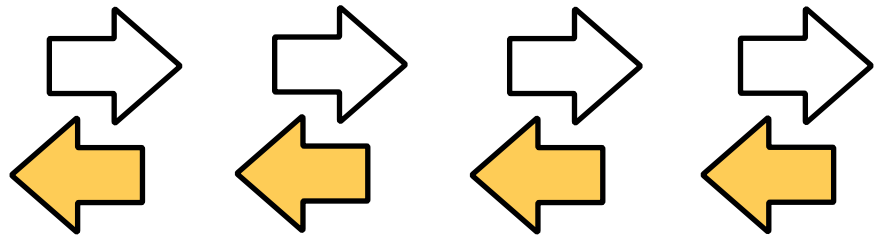
Maintaining the APNs flow

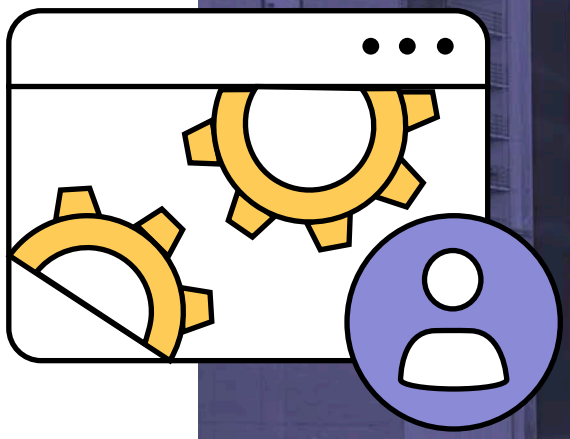
Armed with the knowledge of how APNs works and understanding how important it is, the focus now becomes keeping the service functioning properly to minimize any issues, including interruptions to management services.

The first thing to point out is when **creating a push certificate** – which is required to establish your providers service within Apple's cloud – an Apple ID is required. This is necessary to generate a certificate which is linked to your organization's usage of APNs. Regardless of whether the organization is hosting their own app, service or using another company's app/service – each one must have their own push certificate registered with APNs.

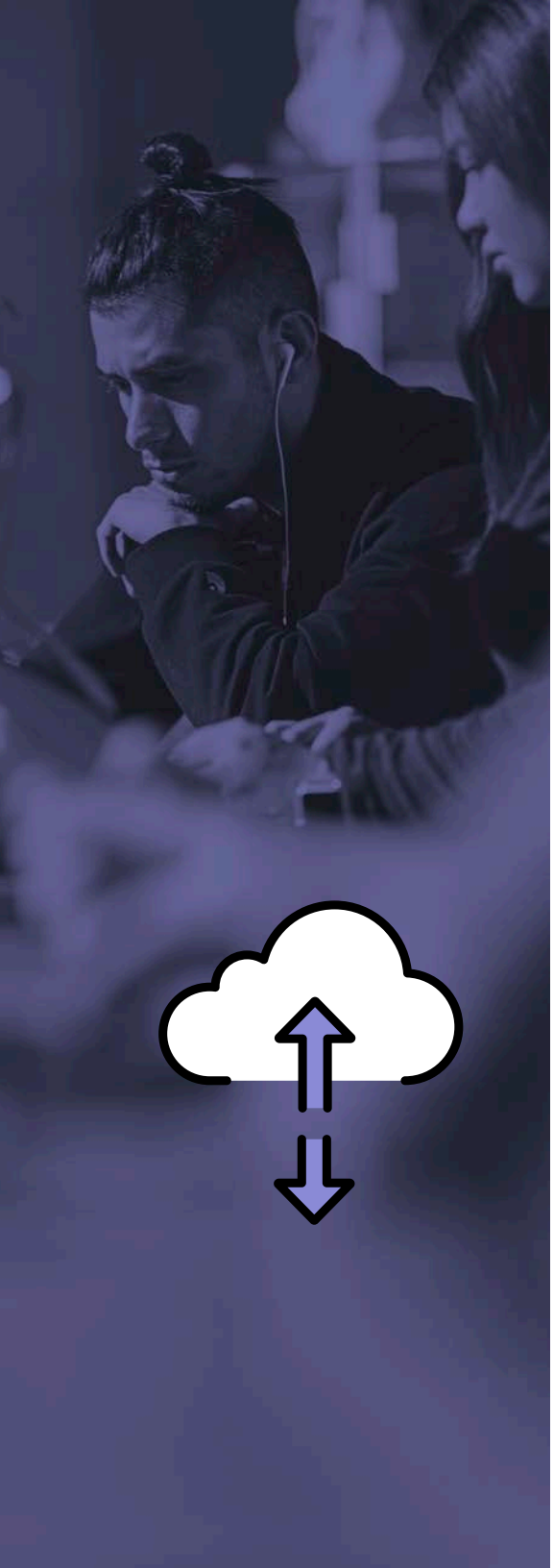
> It's important to keep this account private and secured using a strong password. If this account were to become compromised or the certificate(s) generated modified in any way, it can have the effect of breaking functionality for apps and services relying on APNs – this includes any devices managed by MDM. Another security consideration is to enable two-factor authentication (2FA) to further minimize the possibility of the Apple ID falling into the hands of unauthorized users.

A crucial component of maintaining the flow is the network traffic that flows to and from the network. This flow is often regulated – sometimes heavily – through the use of Firewall appliances to filter out any unwanted traffic to protect the network and its users. Well, APNs relies on network ports to keep notification data routed correctly. Though most of this traffic points to TCP port 5223 (with fail-over duties falling to TCP port 443, if necessary), Apple also utilizes TCP ports 2195-2197, as well, so verifying with your security administrator that **these ports are open** will aid the traffic immensely and cut down on communication errors and loss of services.





This pro tip involves the timely renewal of certificates used by APNs. It cannot be underscored enough just how imperative it is to keeping notifications functioning properly. By keeping certificates up-to-date, APNs will never break its connection with the MDM server or endpoints, maintaining device manageability.



But what happens if the connection to APNs is severed?

If this occurs, the endpoints will still retain all of the settings and apps deployed to them prior to the connection being severed, however, manageability from that point forward will be lost. No management commands, no onboarding of new devices or provisioning existing devices will be possible. In short, no changes will be pushed from the MDM provider to the endpoints. Since the two-way connection between MDM provider and endpoint will be lost, it will require a new APNs certificate to be created to secure connections once again, and by introducing a new certificate, it will require all devices to be manually re-enrolled (and wiped in the case of iOS-based devices) with the MDM provider.

Both Apple and Jamf are excellent when it comes to reminding IT about renewal deadlines too – both via email and in the Jamf console – providing ample time before expiration to renew. Jamf Pro even walks IT through the process (even the parts that take place within Apple's portal) and provides a hash check to verify that the renewed certificate uses the same account as the one used during its creation, providing integrity for the trust established between MDM and APNs. Also, it assures IT that APNs is linked to the correct account and not being hijacked with this built-in security check.

Lastly, from within the same Apple portal IT can also revoke unused or expired certificates as well, simply by locating the record in question and clicking the revoke button next to it, then confirming the change. This is an important step when changing certificates or implementing new ones. Revoking any deprecated ones will ensure they cannot be reused or worse, uploaded to another system to compromise devices that are still managed under the previous APNs certificate.

Put the APNs workflows to the test with Jamf today.

Regardless of your environment, Jamf offers a mobile device management solution tailored to your needs. Learn more about **mobile device management** and when you're ready, get started with a free trial.

Get Started

Or contact your preferred reseller of Apple hardware today.