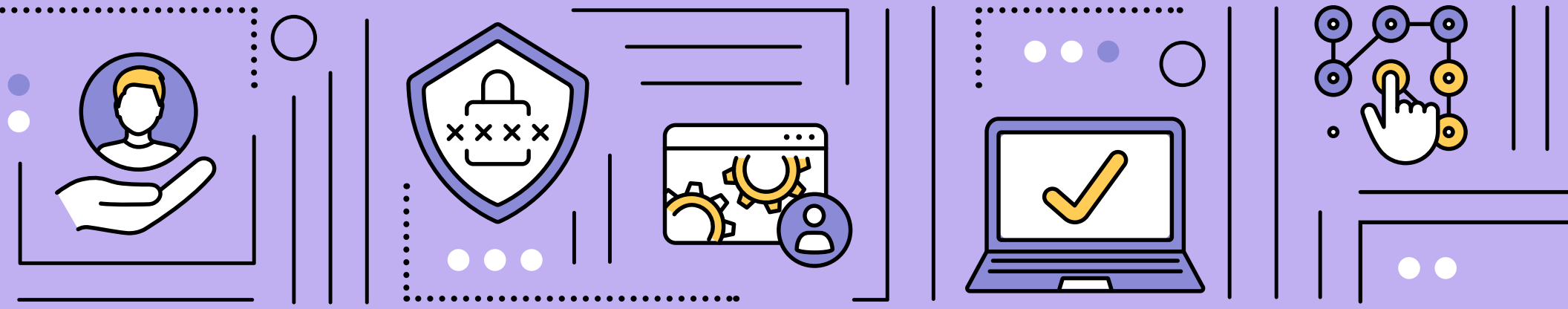
jamf

Apple Push-Benachrichtigung Service

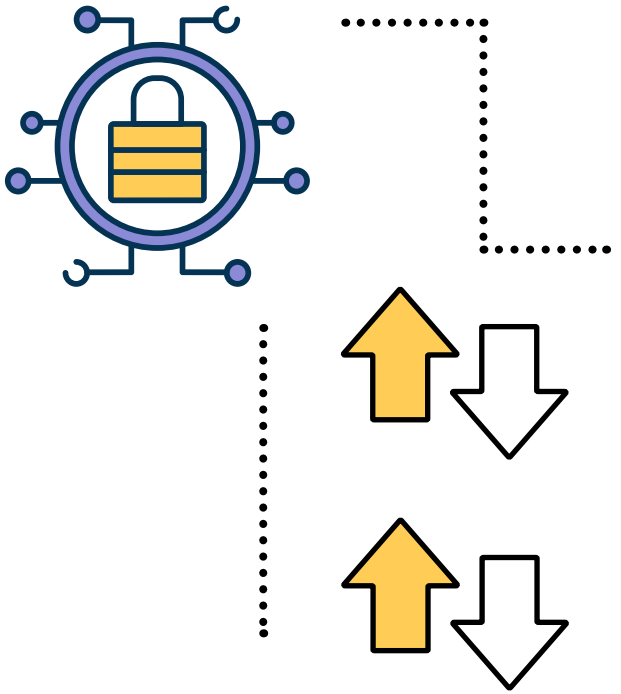
für Beginner



Die Verwaltung von Geräten im Apple-Ökosystem kann ein unkomplizierter Prozess sein, wenn es um grundlegende Verwaltungsbefehle geht.

Wenn Sie einen Computer aus der Ferne neu starten möchten, markieren Sie einfach den Datensatz des Geräts in Ihrer Lösung für das Mobile Device Management (MDM) und wählen Sie die Schaltfläche "Gerät neu starten", um den Befehl zu erteilen. Einfach, nicht wahr? Aber wie genau geschieht dieser Zauber?

Die Antwort auf diese Frage ist der Apple-Push-Benachrichtigungs-Service – oder kurz APNs – der als Dreh- und Angelpunkt für die Kommunikation zwischen dem Endgerät und dem MDM-Server dient. Dieses Thema wird in diesem Dokument behandelt, von den ersten Schritten zur Einrichtung bis zur zuverlässigen Sicherstellung der Betriebsbereitschaft des Benachrichtigungsdienstes.



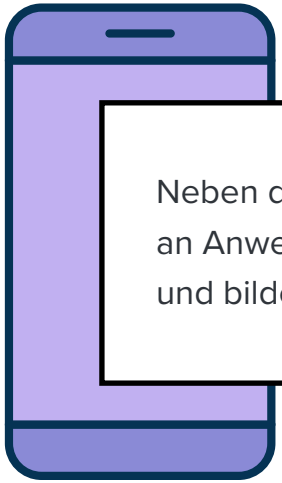
In diesem E-Book wird behandelt:

- Was APNs macht und wie dieser Service funktioniert
- Warum APNs für die Geräteverwaltung entscheidend sind
- Bewährte Verfahren zur Aufrechterhaltung der vollen Funktionalität von APNs

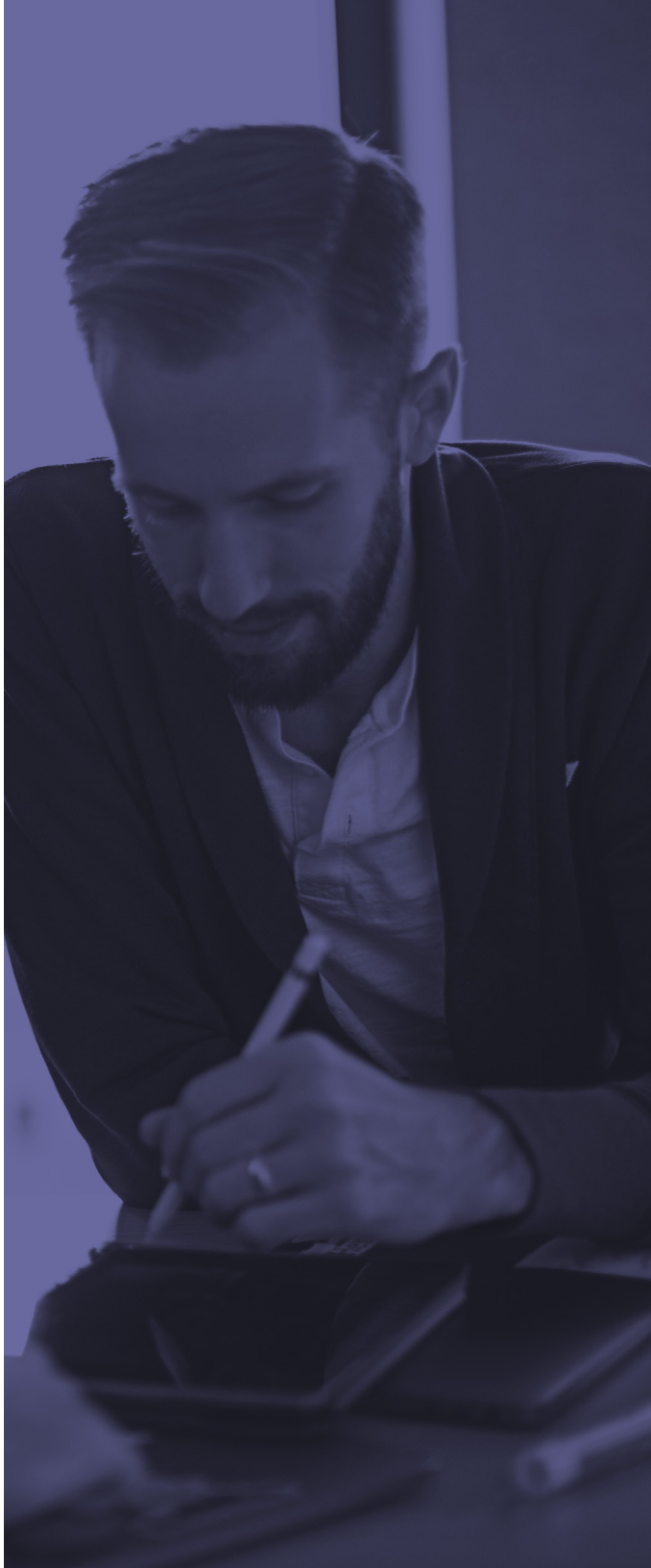
APNs 101

Laut Apple sind "lokale und Push-Benachrichtigungen hervorragend geeignet, um Nutzer mit aktuellen und relevanten Inhalten auf dem Laufenden zu halten, unabhängig davon, ob Ihre App im Hintergrund läuft oder inaktiv ist. Benachrichtigungen können eine Nachricht anzeigen, einen charakteristischen Ton abspielen oder ein Abzeichen auf Ihrem App-Symbol aktualisieren."

APNs sind im Wesentlichen die Übermittlungsmethode für Mitteilungen, die an Apps gesendet werden. Diese Benachrichtigungen senden Aktualisierungen an die Benutzer*innen und informieren sie über Änderungen im Zustand der App oder des Systems. Wenn zum Beispiel eine neue E-Mail in Ihrem Posteingang ankommt, zeigt der E-Mail-Server diese Änderung an und nutzt APNs, um den Endbenutzer über die App auf seinem Apple-Gerät zu informieren, dass eine neue Nachricht eingegangen ist.



Neben der Bereitstellung von Informations-Updates zu Änderungen an Anwendungen arbeiten APNs auch mit MDM-Diensten zusammen und bilden den Grundstein für die Fernverwaltung von Geräten.



Kommunikation ist der Schlüssel

Wie in der modernen Computerlandschaft, in der Kommunikation das Lebenselixier der weltweiten Produktivität ist, ist dies auch ein zentraler Punkt, um Anwendungen auf Apple-Geräten auf dem neuesten Stand zu halten, Benutzer über wichtige Nachrichten zu informieren und sicherzustellen, dass die Geräte sowohl im MDM registriert sind als auch mit den Konfigurationsprofilen und Sicherheitsrichtlinien konform bleiben.

Denn ohne diese integrale Komponente wird die Verbindung zwischen den Endgeräten und dem MDM-Server, der sie verwaltet, unterbrochen. Dies führt zu einem direkten Verlust der Kommunikation mit dem Endgerät und macht die Geräte somit für die IT-Abteilung unbrauchbar.

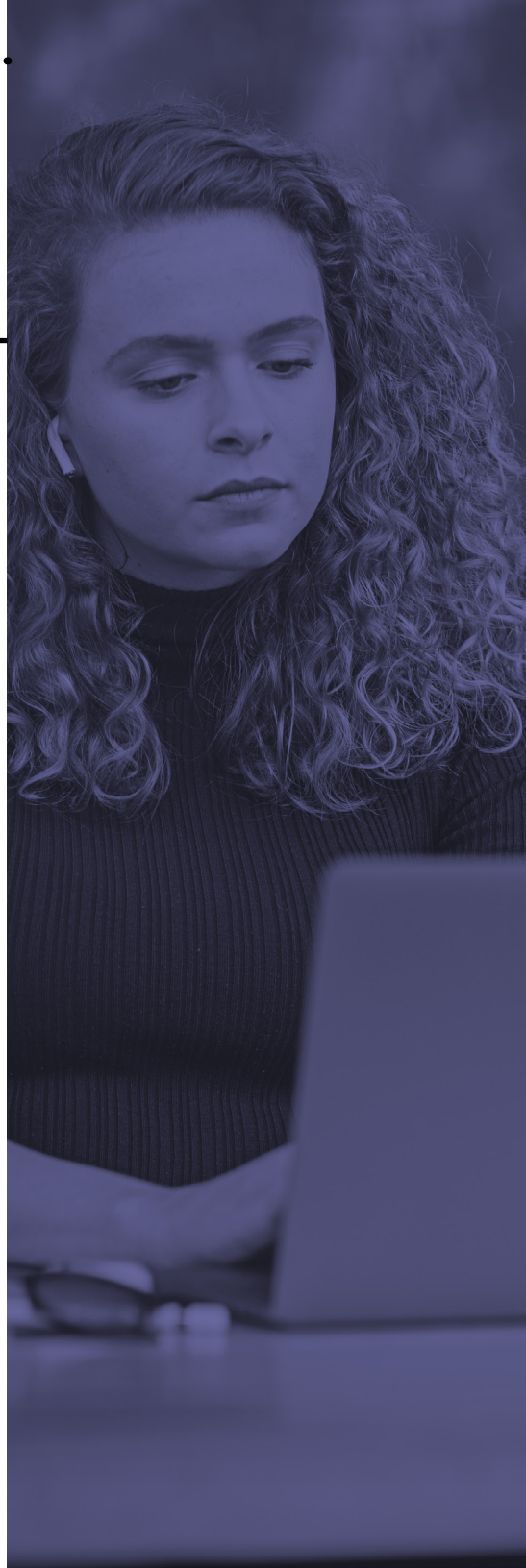
Es ist wichtig zu beachten, dass trotz des Verlusts der Verwaltungsfunktion alle Anwendungen oder Konfigurationen, die bereitgestellt wurden, intakt bleiben, die Geräte selbst jedoch – zusammen mit allen Anwendungen und Konfigurationen – nicht aktualisiert werden, bis die Verbindung zu APNs wiederhergestellt ist.

Wie APNs funktionieren

Sie denken jetzt vielleicht, dass hier beschrieben wird, was APNs sind und warum sie so wichtig sind, aber wie genau funktionieren sie? Eigentlich ist es ganz einfach, wie das folgende Diagramm zeigt.

Wie Sie sehen, ist der Anbieter in diesem Fall der Entwickler oder Service, der eine ständige Verbindung zur Cloud der Push-Benachrichtigungsdienste von Apple unterhält, die als eine Art Proxy für Apple-Geräte fungiert. Die ursprüngliche Nachricht wird vom MDM-Anbieter an die APNs gesendet, die wiederum die Nachricht an das Gerät selbst weiterleiten, wo sie von der App verarbeitet wird und schließlich die Benachrichtigung an die Endbenutzer*innen übermittelt.

Das obige Beispiel beschreibt zwar den Prozess im Allgemeinen, geht aber nicht vollständig darauf ein, wie ein Verwaltungssystem wie Jamf ihn zur Verwaltung von Geräten nutzt. In diesem Fall meldet sich die IT-Abteilung bei der Jamf-Konsole (Jamf Pro, Jamf School oder Jamf Now) an und wählt die Befehle aus, die sie bereitstellen möchte, nachdem sie das/die gewünschte(n) Gerät(e) identifiziert hat. In einem Verwaltungsszenario enthält das von Jamf gesendete Befehls- oder Konfigurationsprofil eine Nutzlast, die den oder die spezifischen Befehle angibt, die auf dem oder den Zielgeräten verarbeitet werden sollen. Die Benachrichtigung wird an APNs gesendet und dann an das/die Gerät(e) im Geltungsbereich weitergeleitet. Sobald sie bei dem/den Zielgerät(en) ankommen, werden die Befehle vom Betriebssystem verarbeitet und wie vorgesehen ausgeführt.



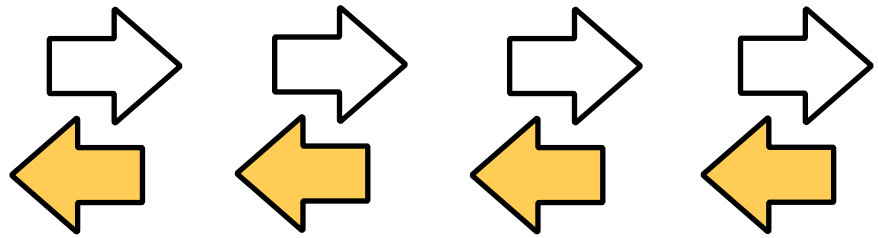
Aufrechterhaltung des APNs-Flusses

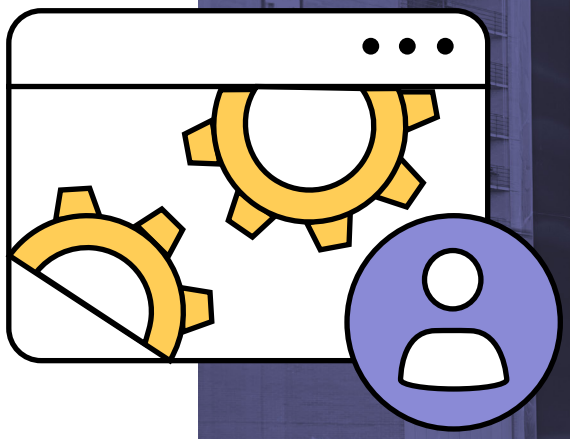
Mit dem Wissen über die Funktionsweise von APNs und dem Verständnis für deren Bedeutung liegt der Schwerpunkt nun auf der Aufrechterhaltung des ordnungsgemäßen Funktionierens des Dienstes, um etwaige Probleme, einschließlich Unterbrechungen der Verwaltungsdienste, zu minimieren.

Zunächst einmal ist bei der **Erstellung eines Push-Zertifikats** – das erforderlich ist, um den Service Ihres Anbieters in der APNs Cloud von Apple einzurichten – eine Apple-ID erforderlich. Dies ist notwendig, um ein Zertifikat zu erstellen, das mit der Verwendung von APNs durch Ihr Unternehmen verknüpft ist. Unabhängig davon, ob das Unternehmen ihre eigene App, ihren eigenen Service hostet oder die App/den Service eines anderen Unternehmens nutzt – jedes Unternehmen muss sein eigenes Push-Zertifikat bei APNs registrieren lassen.

> Es ist wichtig, dass dieser Account privat und mit einem sicheren Passwort geschützt bleibt. Wenn dieses Konto kompromittiert oder das/die generierte(n) Zertifikat(e) in irgendeiner Weise verändert wird/werden, kann dies dazu führen, dass die Funktionalität von Anwendungen und Diensten, die auf APNs angewiesen sind, unterbrochen wird – dies schließt alle von MDM verwalteten Geräte ein. Eine weitere Sicherheitsüberlegung ist die Aktivierung der Zwei-Faktor-Authentifizierung (2FA), um die Möglichkeit zu minimieren, dass die Apple-IDs in die Hände von unbefugten Benutzer*innen gelangen.

Eine entscheidende Komponente zur Aufrechterhaltung des Datenflusses ist der Netzwerkverkehr, der in das und aus dem Netzwerk fließt. Dieser Datenfluss wird häufig – manchmal stark – durch den Einsatz von Firewall-Anwendungen reguliert, um unerwünschten Datenverkehr herauszufiltern und das Netz und seine Nutzer zu schützen. Nun, APNs sind auf Netzwerk-Ports angewiesen, damit die Benachrichtigungsdaten korrekt weitergeleitet werden. Obwohl der größte Teil dieses Datenverkehrs über den TCP-Port 5223 läuft (und bei Bedarf auf den TCP-Port 443 ausweicht), nutzt Apple auch die TCP-Ports 2195-2197. Wenn Sie also mit ihrem Sicherheitsadministrator sicherstellen, dass **diese Ports offen sind**, wird dies den Datenverkehr erheblich erleichtern und Kommunikationsfehler und den Verlust von Services verringern.





Dieser Profi-Tipp betrifft die rechtzeitige Erneuerung der von den APNs verwendeten Zertifikate. Es kann nicht genug betont werden, wie wichtig es für das ordnungsgemäße Funktionieren der Meldungen ist. Indem die Zertifikate auf dem neuesten Stand gehalten werden, unterbrechen APNs niemals ihre Verbindung mit dem MDM-Server oder den Endgeräten, wodurch die Verwaltbarkeit der Geräte erhalten bleibt.

Was passiert aber, wenn die Verbindung zu den APNs unterbrochen wird?

In diesem Fall behalten die Endpunkte alle Einstellungen und Anwendungen, die vor dem Trennen der Verbindung für sie bereitgestellt wurden, die Verwaltbarkeit ab diesem Zeitpunkt geht jedoch verloren. Es sind keine Verwaltungsbefehle, kein Onboarding neuer Geräte und keine Bereitstellung vorhandener Geräte möglich. Kurz gesagt, es werden keine Änderungen vom MDM-Anbieter an die Endgeräte übertragen. Da die zweiseitige Verbindung zwischen MDM-Anbieter und Endgerät verloren geht, muss ein neues APNs-Zertifikat erstellt werden, um die Konnektivität wieder zu gewährleisten. Durch die Einführung eines neuen Zertifikats müssen alle Geräte manuell beim MDM-Anbieter neu registriert (und im Falle von iOS-Geräten gelöscht) werden.

Sowohl Apple als auch Jamf sind hervorragend darin, die IT-Abteilung an Verlängerungsfristen zu erinnern – sowohl per E-Mail als auch in der Jamf-Konsole – sodass genügend Zeit vor Ablauf der Frist für die Verlängerung bleibt. Jamf Pro führt die IT-Abteilung sogar durch den gesamten Prozess (auch durch die Teile, die innerhalb des Apple-Portals stattfinden) und bietet eine Hash-Prüfung, um zu verifizieren, dass das erneuerte Zertifikat dasselbe Konto verwendet wie das, das bei der Erstellung verwendet wurde. So wird die Integrität des Vertrauens zwischen MDM und APNs sichergestellt. Außerdem kann die IT-Abteilung durch diese integrierte Sicherheitsprüfung sicherstellen, dass die APNs mit dem richtigen Konto verknüpft sind und nicht missbraucht werden.

Schließlich kann die IT-Abteilung über dasselbe Apple-Portal auch ungenutzte oder abgelaufene Zertifikate widerrufen, indem sie einfach den betreffenden Datensatz ausfindig macht und auf die Schaltfläche "Widerrufen" daneben klickt und dann die Änderung bestätigt. Dies ist ein wichtiger Schritt bei der Änderung von Zertifikaten oder der Einführung neuer Zertifikate. Durch den Widerruf von veralteten Zertifikaten wird sichergestellt, dass sie nicht wiederverwendet oder, schlimmer noch, in ein anderes System hochgeladen werden können, um Geräte zu kompromittieren, die noch unter dem früheren APN-Zertifikat verwaltet werden.

Testen Sie die APNs-Workflows noch heute mit Jamf.

Unabhängig von Ihrer Umgebung bietet Jamf eine auf Ihre Bedürfnisse zugeschnittene Lösung zur Verwaltung mobiler Geräte. Erfahren Sie mehr über die **Verwaltung von Mobilgeräten** ,und wenn Sie bereit sind, können Sie mit einer kostenlosen Testversion starten.

Los geht's

Oder wenden Sie sich noch heute an Ihren bevorzugten Händler für Apple-Hardware.