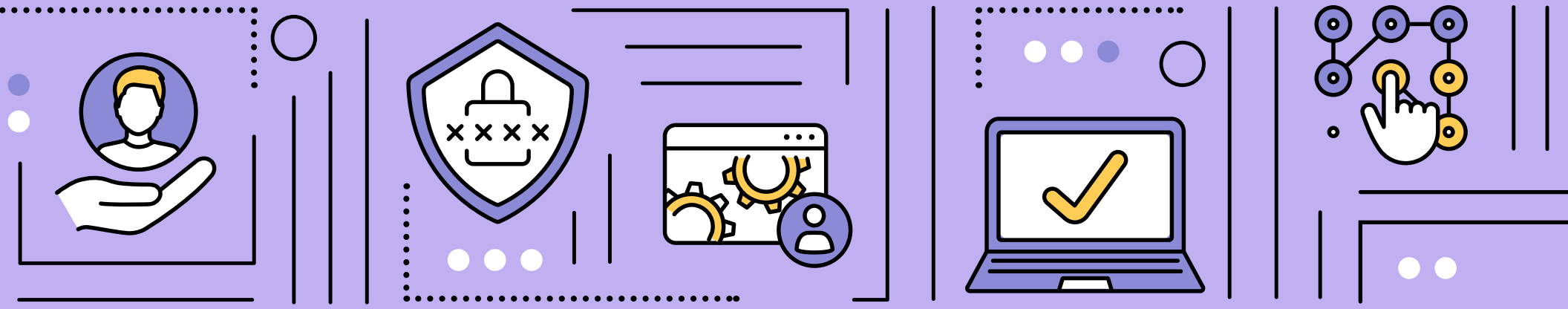
jamf

Servicio de notificación push de Apple

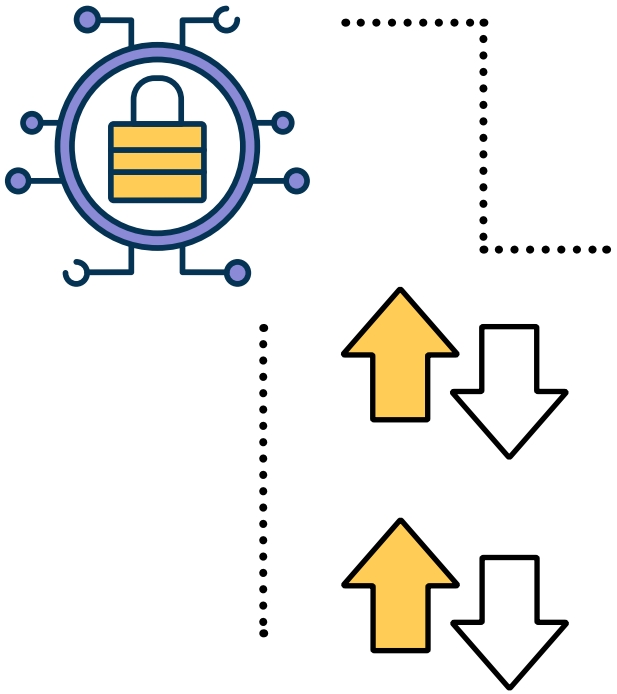
para principiantes



La administración de dispositivos en el ecosistema Apple puede ser un proceso sencillo cuando se trata de comandos de administración básicos.

Si desea reiniciar un equipo a distancia, sólo tiene que resaltar el registro del dispositivo en su solución de administración de dispositivos móviles (MDM) y seleccionar el botón "Reiniciar dispositivo" para emitir la orden. Fácil, ¿verdad? Pero, ¿cómo se produce exactamente esa magia?

La respuesta a esta pregunta es el servicio de notificaciones push de Apple —o APN, para abreviar—, que sirve de eje para la comunicación entre la terminal y el servidor MDM. Este será el tema que se tratará en este documento, desde los pasos iniciales para la configuración hasta asegurar con confianza que el servicio de notificación sigue siendo operativo.



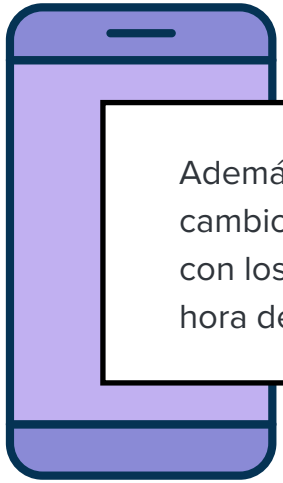
En este e-book se trata el tema:

- Qué hace las APN y cómo funciona este servicio
- Por qué las APN son cruciales para la administración de dispositivos
- Mejores prácticas para mantener las APN en pleno funcionamiento

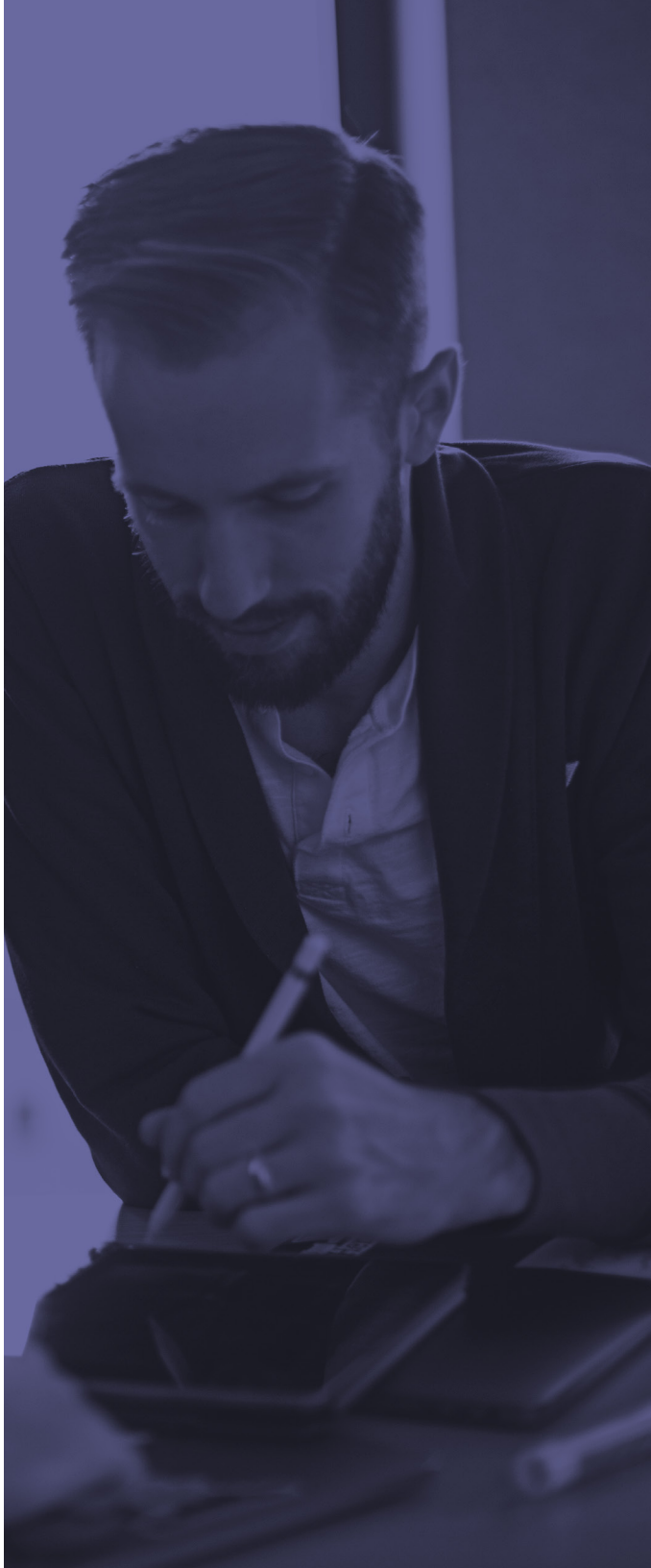
APN 101

Según Apple, "las notificaciones locales y push son estupendas para mantener a los usuarios informados con contenido oportuno y relevante, tanto si tu app está funcionando en segundo plano como si está inactiva. Las notificaciones pueden mostrar un mensaje, reproducir un sonido distintivo o actualizar una insignia en el icono de tu app".

En esencia, los APN son el método de entrega de las comunicaciones enviadas a las apps. Estas notificaciones proporcionan actualizaciones al usuario, informándole de los cambios en el estado de la app o del sistema. Por ejemplo, cuando llega un nuevo mensaje de correo electrónico a su bandeja de entrada, el servidor de correo electrónico de detecta este cambio y utiliza rápidamente las APN para alertar al usuario final a través de la app de su dispositivo Apple de que se ha recibido un nuevo mensaje.



Además de proporcionar actualizaciones informativas sobre los cambios en las aplicaciones, las APN también trabajan en conjunto con los servicios de MDM, actuando como la piedra angular a la hora de gestionar dispositivos de forma remota.



La comunicación es la clave

Reflejar el panorama informático moderno, en el que la comunicación es la esencia de la productividad en todo el mundo, también es un principio fundamental para mantener las aplicaciones actualizadas en los dispositivos Apple, notificar a los usuarios los mensajes importantes y garantizar que los dispositivos estén inscritos en la MDM y sigan cumpliendo los perfiles de configuración y las políticas de seguridad.

El hecho es que sin este componente integral en funcionamiento, el vínculo entre las terminales y el servidor MDM que las administra se cortará. Esto provoca una pérdida directa de la comunicación con la terminal y, por tanto, impide que los dispositivos sean administrados por el departamento de IT.

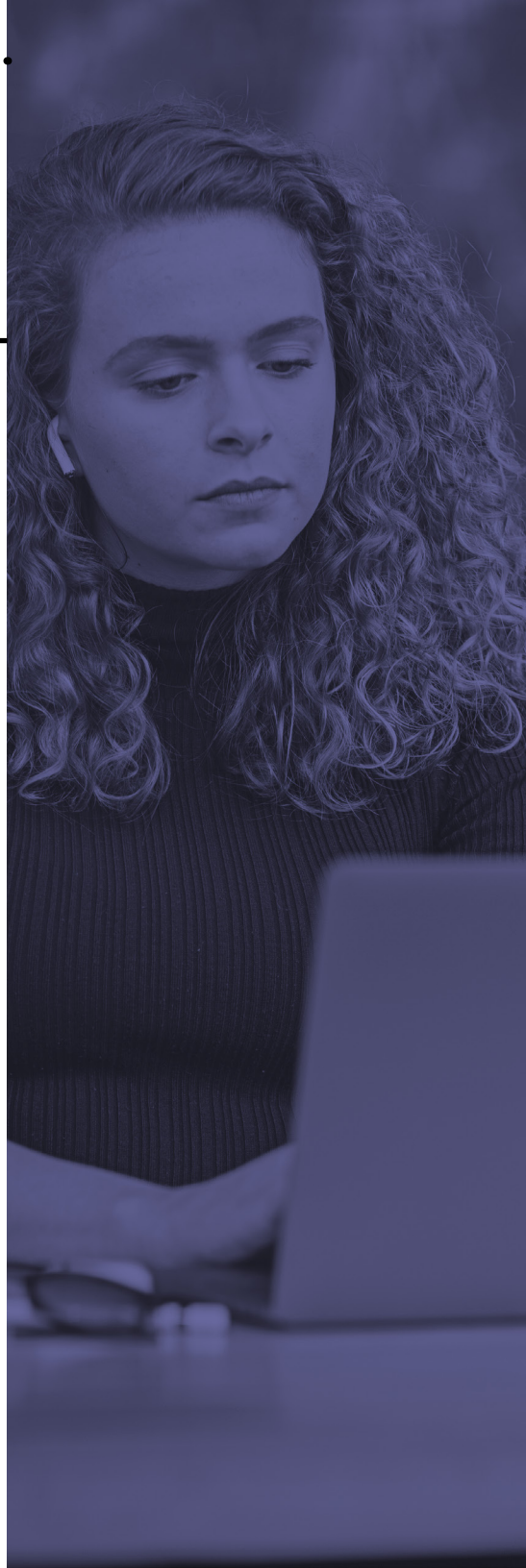
Es importante tener en cuenta que, a pesar de la pérdida de la capacidad de administración, cualquier app o configuración que se haya implementado permanecerá intacta; sin embargo, los propios dispositivos —junto con todas las apps y configuraciones— no se actualizarán hasta que se restablezca la conexión con las APN.

Cómo funcionan las APN

Así que tal vez piense que esto cubre lo que son las APN y por qué son tan importantes, pero ¿cómo funcionan exactamente? En realidad, es bastante sencillo, como se ilustra en el siguiente diagrama.

Como puede ver, en este caso el proveedor es el desarrollador o el servicio que mantiene una conexión constante con la nube de servicios de notificaciones push de Apple, que actúa como una especie de proxy para los dispositivos Apple. El mensaje inicial es enviado por el proveedor de MDM a las APN que, a su vez, reenvían el mensaje al propio dispositivo donde es procesado por la app, entregando finalmente la notificación al usuario final.

Aunque el ejemplo anterior describe el proceso en general, no aborda completamente cómo un sistema de administración, como Jamf, lo utiliza para administrar dispositivos. En este caso, IT se conectaría a la consola de Jamf (Jamf Pro, Jamf School o Jamf Now) y seleccionaría los comandos que desea implementar después de identificar el o los dispositivos a los que desea dirigirse. En un escenario de administración, el comando o el perfil de configuración que se envía desde Jamf contiene una carga útil que especifica el comando o comandos específicos que se van a procesar en el o los dispositivos de destino. La notificación se envía a las APN y, a continuación, se dirige al dispositivo o dispositivos en cuestión. Una vez que llegan al o a los dispositivos de destino, el o los comandos son procesados por el sistema operativo y ejecutados según lo previsto.



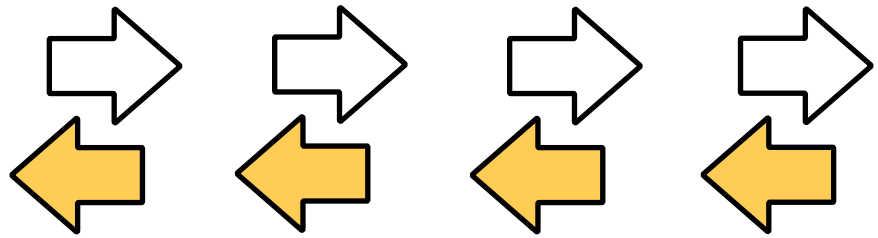
Conservación del flujo de las APN

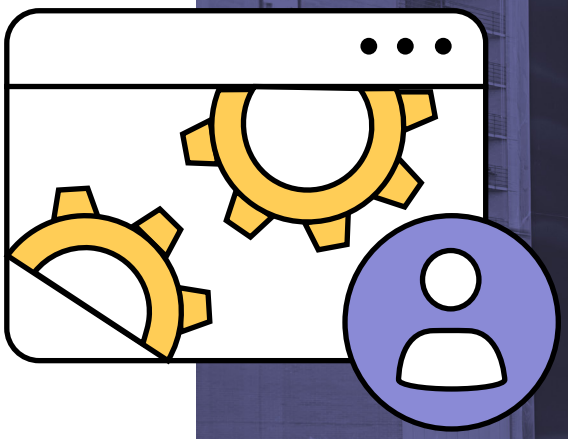
Al conocer el funcionamiento de las APN y comprender su importancia, ahora el objetivo es mantener el servicio en buen estado para minimizar cualquier problema, incluidas las interrupciones de los servicios de administración.

Lo primero que hay que señalar es que a la hora de **crear un certificado push** —que es necesario para establecer el servicio de sus proveedores dentro de la nube de APN de Apple— se necesita una ID de Apple. Esto es necesario para generar un certificado que esté vinculado al uso de las APN por parte de su organización. Sin importar si la organización aloja su propia app, servicio o utiliza la app/servicio de otra empresa, cada una debe tener su propio certificado push registrado con las APN.

Es importante mantener esta cuenta privada y segura utilizando una contraseña fuerte. Si esta cuenta se viera comprometida o los certificados generados fueran modificados de alguna manera, podría tener el efecto de romper la funcionalidad de las apps y servicios que dependen de las APN, y esto incluye cualquier dispositivo administrado por MDM. Otra consideración de seguridad es habilitar la autenticación de dos factores (2FA) para minimizar aún más la posibilidad de que el ID de Apple caiga en manos de usuarios no autorizados.

Un componente crucial para mantener el flujo es el tráfico de red que fluye hacia y desde la red. A menudo, este flujo se regula — a veces fuertemente — mediante el uso de dispositivos de firewall para filtrar cualquier tráfico no deseado con el fin de proteger la red y a sus usuarios. Pues bien, las APN dependen de los puertos de red para que los datos de las notificaciones se enruten correctamente. Aunque la mayor parte de este tráfico apunta al puerto TCP 5223 (con funciones de conmutación por error que recaen en el puerto TCP 443, si es necesario), Apple también utiliza los puertos TCP 2195-2197, por lo que verificar con su administrador de seguridad que **estos puertos están abiertos** ayudará enormemente al tráfico y se reducirán los errores de comunicación y la pérdida de servicios.





Este consejo profesional se refiere a la renovación oportuna de los certificados utilizados por las APN. Nunca se insistirá lo suficiente en lo importante que es mantener el buen funcionamiento de las notificaciones. Al mantener los certificados actualizados, las APN nunca interrumpirán su conexión con el servidor MDM o las terminales, manteniendo la capacidad de administración de los dispositivos.

Pero, ¿qué pasaría si se cortara la conexión con las APN?

Si esto ocurre, las terminales seguirán conservando todas las configuraciones y apps implementadas en ellas antes de que se interrumpiera la conexión; sin embargo, se perderá la posibilidad de administrarlas a partir de ese momento. No se dispondrá de comandos de administración, no se podrán incorporar nuevos dispositivos ni aprovisionar los existentes. En resumen, no se transmitirá ningún cambio desde el proveedor de MDM a las terminales. Dado que se perderá la conexión bidireccional entre el proveedor de MDM y la terminal, será necesario crear un nuevo certificado de las APN para volver a asegurar las conexiones y, al introducir un nuevo certificado, será necesario volver a inscribir manualmente todos los dispositivos (y borrarlos en el caso de los dispositivos basados en iOS) con el proveedor de MDM.

Tanto Apple como Jamf son excelentes a la hora de recordar a IT los plazos de renovación también, tanto por correo electrónico como en la consola de Jamf, proporcionando tiempo suficiente antes de su vencimiento para renovarlos. Jamf Pro incluso guía a IT a través del proceso (incluso en las fases que tienen lugar dentro del portal de Apple) y proporciona una comprobación hash para verificar que el certificado renovado usa la misma cuenta que la utilizada durante su creación, proporcionando integridad a la confianza establecida entre la MDM y las APN. Además, asegura a IT que las APN están vinculadas a la cuenta correcta y no están siendo secuestradas con esta verificación de seguridad incorporada.

Por último, desde el mismo portal de Apple, IT también puede revocar los certificados no utilizados o caducados, simplemente localizando el registro en cuestión y haciendo clic en el botón de revocación que se encuentra junto a él, para luego confirmar el cambio. Este es un paso importante cuando se cambian los certificados o se implementan otros nuevos. La revocación de los obsoletos asegurará que no puedan ser reutilizados o, peor aún, subidos a otro sistema para comprometer los dispositivos que aún se administran bajo el certificado de las APN anteriores.

Ponga a prueba los flujos de trabajo de las APN con Jamf hoy mismo.

Independientemente de su entorno, Jamf ofrece una solución de administración de dispositivos móviles adaptada a sus necesidades. Obtenga más información sobre **administración de dispositivos móviles** y cuando esté listo, comience con una prueba gratuita.

Empiece

O comuníquese con su distribuidor preferido de productos Apple hoy mismo.