Comandos

La página del dispositivo proporciona un panel **Comandos** para enviar comandos remotos a un dispositivo gestionado. Los comandos disponibles dependen de la plataforma (Android o Apple) y del estado del dispositivo.

Los comandos solo se pueden enviar a un dispositivo que esté inscrito actualmente. En un dispositivo con la inscripción anulada, en un dispositivo ADE que aún no se ha inscrito y en el historial de una inscripción anterior, el panel solo muestra el historial de comandos.

> Si el dispositivo no está conectado en este momento, el comando se entregará y ejecutará en cuanto se conecte a Internet. En los comandos de Android puedes establecer el parámetro **Validez** para determinar cuánto tiempo sigue siendo válido un comando no entregado.

Comandos de Android (AMAPI)

En los dispositivos Android, el panel Comandos incluye un campo **Validez** (valor + unidad) y un selector **Comando**. Algunos comandos requieren parámetros adicionales, que aparecen dinámicamente al seleccionar el comando.

Parámetros comunes

- **Validez**: cuánto tiempo es válido el comando si no se puede ejecutar de inmediato.
- **Comando**: elige qué acción enviar al dispositivo.

Comandos sin campos adicionales

- **Bloquear dispositivo**: bloquea el dispositivo.
- **Reiniciar dispositivo**: reinicia el dispositivo. Requiere Android 7.0 o posterior.
- **Desactivar modo perdido**: saca el dispositivo del modo perdido.
- **Retirar la propiedad**: elimina el perfil de trabajo y todas las políticas de un dispositivo propiedad de la empresa con Android 8.0 o posterior, y lo deja para uso personal. Las apps y los datos del perfil personal se conservan. El dispositivo se elimina del servidor después de confirmar el comando. Esto no se puede deshacer.

Comandos con campos adicionales

- **Restablecer contraseña**: requiere **Nueva contraseña** y **Confirmar nueva contraseña**. Los interruptores opcionales incluyen **Bloquear ahora**, **Requerir entrada** y **No solicitar credenciales al arrancar**.
- **Borrar datos de la app**: requiere el **nombre del paquete** de destino.
- **Activar modo perdido**: requiere un **Mensaje de modo perdido** y admite campos de contacto opcionales (dirección postal, organización, número de teléfono, correo electrónico). Cuando el dispositivo lo informa, su estado pasa a ser **Perdido**, la página del dispositivo muestra un banner y este comando se oculta hasta que se desactiva el modo perdido.
- **Borrar dispositivo**: admite un **Mensaje con el motivo del borrado** (se muestra a los usuarios en dispositivos personales) e indicadores de borrado opcionales, incluido **Borrar eSIM**.

> Los comandos de eSIM (**Añadir eSIM**, **Quitar eSIM**, **Solicitar EID**) están disponibles en el panel específico **Gestión de SIM**.

Historial de comandos

Debajo de los controles de envío, el panel de control muestra una tabla de historial de comandos. La tabla se puede ordenar y admite paginación. Algunas filas se pueden expandir para ver parámetros adicionales o detalles de ejecución.

Columnas del historial de Android

- **Fecha de creación**
- **Comando**
- **Validez**
- **Estado**
- **Error**
- **Fecha de ejecución**

Comandos de Apple (MDM)

En los dispositivos Apple, el panel Comandos ofrece un selector **Comando**. Algunos comandos requieren datos adicionales. Al igual que en Android, debajo se muestra una tabla de historial de comandos.

Comandos con campos adicionales

- **Instalar app**: requiere el **ID del paquete** de la aplicación.
- **Enviar notificación**: requiere un **Mensaje de notificación** (longitud máxima de 200 caracteres).

En iPhone y iPad, **Enviar notificación** y el seguimiento en vivo llegan al dispositivo a través de la app **Cerberus Enterprise**: están desactivados hasta que la app está instalada y se ha registrado para recibir notificaciones (consulta el campo **App Cerberus Enterprise**). Al iniciar el seguimiento en vivo se muestra «Solicitud de seguimiento en vivo enviada al dispositivo»: el seguimiento empieza cuando el dispositivo envía su primera ubicación. iOS puede retrasar la solicitud o no entregarla, por ejemplo en el modo de bajo consumo o sin conexión de red: si no llega ninguna ubicación en 2 minutos, pide al usuario que abra la app una vez. Cuando una solicitud falla, el mensaje indica el motivo, por ejemplo que la app aún no se ha registrado, que falta la clave de notificación del servidor o que el token de notificación del dispositivo ya no es válido.

Acciones del dispositivo

Solo se muestran los comandos compatibles con el dispositivo: algunos requieren un iPhone o iPad supervisado y otros no están disponibles en un Mac. Los que interrumpen el uso piden confirmación.

- **Bloquear dispositivo**: bloquea la pantalla, con un mensaje y un número de teléfono opcionales. Un Mac se reinicia y se bloquea con un PIN de seis dígitos, que se muestra una vez después de enviar el comando y en los detalles del comando. El iPhone muestra el título «iPhone perdido» encima de tu mensaje, aunque este comando no activa el modo perdido.
- **Activar modo perdido** (iPhone y iPad supervisados): bloquea el dispositivo y muestra tu mensaje, número de teléfono y nota al pie en la pantalla de bloqueo. Mientras el modo perdido está activo, la página muestra un banner y los comandos **Localizar dispositivo** (la ubicación aparece en el mapa de ubicaciones), **Reproducir sonido** y **Desactivar modo perdido**.
- El dispositivo avisa a quien lo tenga de que se ha localizado: después de **Localizar dispositivo**, la pantalla de bloqueo muestra **iPhone localizado** con la hora y el nombre del servidor que recibió la ubicación, y un botón **Continuar**. iOS muestra este aviso y no se puede desactivar.
- **Borrar código de acceso**: elimina el código de acceso de un iPhone o iPad, por ejemplo cuando el usuario lo ha olvidado. Si la política exige un código de acceso, se pide al usuario que establezca uno nuevo.
- **Actualizar información del dispositivo**: pide al dispositivo su información (supervisión, versión del sistema operativo, estado de seguridad, certificado MDM) y su inventario.
- **Configuración del dispositivo**: abre una ventana para cambiar el nombre del dispositivo, el nombre de host de un Mac, Bluetooth, la itinerancia de datos, el punto de

acceso personal, la zona horaria, el fondo de pantalla, si se permite el Bloqueo de activación y, en un iPad compartido, su configuración (consulta más abajo). Solo se envían los ajustes que cambias; los que el dispositivo no admite se desactivan con el motivo. Un dispositivo puede confirmar la itinerancia de datos o el punto de acceso personal sin aplicarlos (por ejemplo, cuando el plan de la SIM no incluye el punto de acceso personal), así que Cerberus Enterprise los vuelve a leer unos 30 segundos después y escribe una advertencia en los registros del sistema si no han cambiado.

- **Reiniciar dispositivo** y **Apagar dispositivo**: reinician o apagan el dispositivo de inmediato, tras una confirmación.
- **Borrar dispositivo**: borra todo el contenido y los ajustes y elimina el dispositivo de la gestión. En iPhone y iPad puedes conservar el plan de datos eSIM y omitir la configuración por proximidad; un Mac recibe un PIN de seis dígitos.
- **Devolver al servicio** (opción de **Borrar dispositivo**, iPhone y iPad con iOS 17 o posterior): tras el borrado, el dispositivo se configura de nuevo por sí solo, sin que nadie lo toque, y se inscribe otra vez con su política, usuario y propiedad actuales. Elige una red Wi-Fi de la política del dispositivo para la configuración, a menos que el dispositivo tenga Ethernet o datos móviles: solo se pueden usar redes personales (con contraseña y sin certificados), porque el dispositivo aún no tiene usuario ni certificado. El Bloqueo de activación debe estar desactivado.
- **Actualizar planes móviles** (iPhone y iPad con conectividad móvil, iOS 13 o posterior, no User Enrollment): introduce la **URL del servidor eSIM del operador** indicada por el operador (una dirección https://, un nombre de host o un código de activación LPA, del que solo se usa el servidor) y el dispositivo descarga los planes eSIM que el operador vinculó a su EID. El EID del dispositivo se muestra debajo del campo para enviarlo al operador. Consulta la página **Gestión de SIM**.
- **Conservar el plan de datos eSIM** desactivado elimina todas las eSIM con el borrado. La restricción de política **Conservar la eSIM al borrar el dispositivo** (dispositivos supervisados, iOS 17.2 o posterior) se aplica a los borrados iniciados en el dispositivo (demasiados intentos fallidos de código de acceso, Borrar todo el contenido y los ajustes): Apple no documenta su efecto en este comando.
- **Cerrar sesión del usuario** (iPad compartido): cierra la sesión del usuario actual y vuelve a la pantalla de inicio de sesión. Los datos que aún no se han sincronizado con iCloud permanecen en el iPad.

iPad compartido

Un iPad compartido lo usan varias personas, cada una con su propia cuenta de Apple gestionada, o invitados con sesiones temporales. Se configura con un perfil de ADE que habilita el iPad compartido (consulta la página **Apple Automated Device Enrollment**), y su campo **Tipo de inscripción** muestra **iPad compartido**.

- **Usuarios del iPad compartido**: los usuarios del iPad, con el usuario que ha iniciado sesión, el almacenamiento que usan y si algunos datos aún no se han sincronizado con iCloud. Usa **Actualizar** para volver a pedir la lista al iPad. Se puede eliminar un usuario

junto con sus datos, excepto el usuario que ha iniciado sesión (cierra su sesión primero); **Eliminar todos los usuarios** requiere iPadOS 14 o posterior. Cuando los datos aún no se han sincronizado, la confirmación advierte de que se perderán.
- **Ajustes del dispositivo**: el almacenamiento de cada usuario, el número de usuarios previsto, el tiempo de inactividad tras el cual se cierran las sesiones de usuarios e invitados, solo sesiones de invitado, los dominios de cuenta de Apple gestionada sugeridos en la pantalla de inicio de sesión, cuántos días puede iniciar sesión un usuario sin comprobar la contraseña en línea y omitir la configuración de idioma y región para los usuarios nuevos. Los campos vacíos conservan su valor actual; los ajustes que necesitan un iPadOS más reciente aparecen deshabilitados.

Usuarios de Mac

En un Mac, el panel **Usuarios de Mac** muestra los usuarios inscritos en la gestión, normalmente el usuario que inscribió el Mac. Las cuentas de la política se instalan en sus sesiones. Para cada usuario se muestra cuándo se inscribió, el último informe de su sesión y el estado de las cuentas: **Al día**, **Esperando al usuario** (el Mac las instala cuando el usuario ha iniciado sesión), **No aplicadas** con los motivos indicados por el Mac, o **Sin cuentas** cuando la política no tiene ninguna. Usa **Recargar** para volver a leer la lista.

Bloqueo de activación

El campo **Bloqueo de activación** muestra si el Bloqueo de activación está activado. Cuando está activado, un dispositivo borrado solo se puede configurar de nuevo con la cuenta de Apple del usuario o con el código de omisión del dispositivo. Los dispositivos supervisados activan el Bloqueo de activación solo si se permite en **Ajustes del dispositivo**. Cerberus Enterprise pide el código de omisión a los dispositivos supervisados y lo guarda: usa **Mostrar código de omisión** en el menú del campo para verlo (solo pueden los administradores, y cada visualización queda registrada en el registro del sistema) y, después, introdúcelo como contraseña en la pantalla de Bloqueo de activación del dispositivo, dejando la cuenta de Apple vacía.

Bloqueo de recuperación y contraseña de firmware (Mac)

Un Mac con Apple silicon muestra el campo **Bloqueo de recuperación**, y un Mac con Intel el campo **Contraseña de firmware**. Ambos protegen el Mac al arrancar: con el Bloqueo de recuperación, recoveryOS pide la contraseña; con una contraseña de firmware, el Mac la pide para arrancar desde otro disco o desde recuperación. El campo muestra si el Mac informa de una contraseña y, en su información sobre herramientas, cuándo la guardó Cerberus Enterprise y cuándo se verificó por última vez.

- **Establecer o cambiar contraseña**: Cerberus Enterprise genera una contraseña de 20 letras que están en las mismas teclas con cualquier distribución de teclado, o un administrador escribe una (de 8 a 64 caracteres sin acentos; los demás roles solo pueden generar una, porque no pueden ver las contraseñas guardadas). La contraseña se guarda cifrada antes de enviarse y sustituye a la guardada solo cuando el Mac la confirma. Si el Mac ya tiene una contraseña establecida fuera de Cerberus Enterprise, escríbela como contraseña actual: se usa una vez y no se guarda.
- **Verificar contraseña**: pregunta al Mac si la contraseña guardada es correcta. El resultado aparece en la información sobre herramientas y en el registro del sistema.
- **Mostrar contraseña**: solo los administradores pueden ver la contraseña guardada, y cada visualización queda registrada en el registro del sistema. Las contraseñas generadas se muestran en grupos de cuatro letras: escríbelas sin espacios.
- **Borrar contraseña**: elimina la contraseña del Mac.

Un Mac con Intel se reinicia para aplicar un cambio de contraseña de firmware: hasta entonces se sigue necesitando la contraseña anterior (Mostrar contraseña la muestra) y no se puede enviar otro cambio. Apple además acepta solo un comando de contraseña de firmware cada 30 segundos. Las contraseñas se ocultan en el historial de comandos.

Cuando un Mac deja la gestión (se anula su inscripción, lo elimina el usuario o se borra), macOS elimina el Bloqueo de recuperación por sí mismo y Cerberus Enterprise descarta la contraseña de Bloqueo de recuperación guardada; hace lo mismo cuando el Mac informa de que no tiene Bloqueo de recuperación, por ejemplo después de volver a inscribirse. Cuando anulas la inscripción de un Mac (o eliminas su política), primero se borra la contraseña de firmware guardada, el Mac se reinicia y luego deja la gestión. Si el borrado falla, el Mac deja la gestión de todos modos y la contraseña sigue guardada para que puedas verla. Un Mac eliminado de la gestión por el usuario, o borrado, conserva su contraseña de firmware: Cerberus Enterprise también la conserva. Al eliminar el registro del dispositivo se elimina la contraseña guardada, por lo que se te pide confirmarlo primero: anota la contraseña, porque sin ella solo Apple puede eliminarla.

FileVault (Mac)

El campo **FileVault** muestra si el disco del Mac está cifrado y, en su información sobre herramientas, si Cerberus Enterprise almacena su clave de recuperación personal. Un Mac envía la clave cuando FileVault está activado después de recibir el ajuste de FileVault de su política (consulta la página **macOS** de las políticas de Apple).

- **Mostrar clave de recuperación**: solo los administradores pueden ver la clave, y cada visualización queda registrada en el registro del sistema. Úsala en la ventana de inicio de sesión del Mac para restablecer la contraseña del usuario, o en recuperación para desbloquear el disco. Sigue disponible después de que el Mac deje la gestión; al eliminar el registro del dispositivo se elimina.
- **Cambiar clave de recuperación**: el Mac sustituye su clave de recuperación personal y envía la nueva cifrada; la clave anterior deja de funcionar. Solo es posible cuando la clave

guardada se puede leer: el Mac está desbloqueado con ella y no se necesita la contraseña de ningún usuario. La clave guardada se oculta en el historial de comandos y se elimina del servidor en cuanto el Mac responde (o tras 7 días sin respuesta).

Bootstrap Token (Mac)

Un Mac con macOS 10.15 o posterior envía su **Bootstrap Token** al servidor de gestión cuando inicia sesión un usuario con un token seguro. El servidor lo guarda y solo se lo devuelve a ese Mac, que lo usa para dar un token seguro a los usuarios nuevos y, en un Mac con Apple silicon, para instalar actualizaciones de software y aprobar extensiones del kernel sin pedir la contraseña de administrador. Nadie puede ver el token, ni en el panel de control ni en ningún otro sitio. El campo **Bootstrap Token** muestra su estado:

- **En custodia**: el servidor tiene el token; la información sobre herramientas muestra cuándo lo envió el Mac.
- **En custodia anteriormente**: el token almacenado se envió antes de la última inscripción o de la última renovación del certificado MDM del Mac. Tras una renovación, esto es lo esperado: el token se conserva y el Mac no lo vuelve a enviar. Tras una nueva inscripción puede que ya no sea válido: ejecuta `sudo profiles install -type bootstraptoken` en Terminal en el Mac.
- **Sin custodia**: el Mac aún no ha enviado un token. Para enviarlo ahora, un administrador del Mac ejecuta `sudo profiles install -type bootstraptoken` en Terminal (`sudo profiles status -type bootstraptoken` muestra si está en custodia).

La información sobre herramientas también indica si el Mac permite el token para la autenticación. Los Mac configurados con Automated Device Enrollment lo permiten automáticamente; en otros Mac con Apple silicon, un usuario puede permitirlo en la Utilidad de seguridad de inicio en recoveryOS. Los Mac con Intel no pueden usar el token para la autenticación (**Not supported**), pero un token en custodia sigue dando un token seguro a los usuarios nuevos. Cada vez que un Mac envía, elimina o solicita su token, queda registrado en el registro del sistema.

Estado del dispositivo y actualizaciones del sistema operativo

El panel **Estado del dispositivo** muestra lo que el dispositivo informa sobre sí mismo: la versión y compilación del sistema operativo, el progreso de una actualización de software (versión pendiente, fecha límite, qué la inició, fallos), si hay un código de acceso establecido y cumple la política, FileVault en un Mac, el estado de la batería y las cuentas configuradas en el dispositivo.

La lista **Actualizaciones disponibles** muestra las actualizaciones del sistema operativo que el dispositivo puede instalar, recopiladas durante la inscripción y semanalmente. Usa **Buscar actualizaciones** para solicitarlas ahora, y **Instalar** para instalar una actualización de inmediato

(el dispositivo se reinicia, tras una confirmación) o solo descargarla y dejar que el usuario la instale. Esto funciona en iPhone y iPad supervisados y en Mac, hasta iOS, iPadOS y macOS 26: en versiones posteriores y para actualizar muchos dispositivos, usa las actualizaciones obligatorias de la política (consulta la página **Actualizaciones de software** de las políticas de Apple).

Un Mac con Apple silicon instala una actualización sin pedir la contraseña de administrador solo cuando permite su Bootstrap Token para la autenticación y el token está en custodia (consulta Bootstrap Token más arriba). De lo contrario, la confirmación indica que puede que un usuario tenga que introducir una contraseña de administrador antes de que se instale la actualización.

Aplicaciones e inventario

El panel **Aplicaciones** muestra todas las apps del dispositivo en una tabla. El dispositivo informa en tiempo real del estado de instalación de las apps instaladas por la política o con un comando; las versiones, los tamaños y las apps instaladas por el usuario proceden de la última lista de apps, recopilada en la inscripción y semanalmente. Usa **Preguntar al dispositivo** para solicitarla ahora.

- **Gestión**: **Política** para las apps instaladas por la política del dispositivo, **Gestionada** para las apps instaladas con un comando como **Instalar app**, **No gestionada** para las instaladas por el usuario. La app Cerberus Enterprise tiene la etiqueta **Instalada por Cerberus**.
- **Requiere atención**: apps que no se pudieron instalar, que el usuario rechazó o eliminó, o que esperan al usuario. Abre una fila para ver el error; las apps de política que fallaron se pueden volver a instalar con el botón de reintentar. No se cuentan las apps integradas ni las apps del App Store que el dispositivo indica como no validadas.
- **Eliminar app**: las apps gestionadas se pueden eliminar, junto con sus datos. Para eliminar una app instalada por la política, elimínala de la política. La política también envía este comando por sí misma cuando se elimina de la política un paquete de Mac instalado como app gestionada.

El panel **Perfiles, certificados y seguridad** muestra los perfiles de configuración, los certificados y el estado de seguridad (código de acceso, cifrado, FileVault y firewall en un Mac) indicados por el dispositivo.

> En los dispositivos de propiedad personal no se recopilan las apps instaladas por el usuario y solo se muestran los perfiles y certificados gestionados por Cerberus Enterprise.

El panel **Cambios de inventario** muestra qué cambió entre dos listas enviadas por el dispositivo: apps instaladas, eliminadas o actualizadas (con la versión anterior y la nueva), perfiles instalados, eliminados o actualizados y certificados añadidos o eliminados. Un cambio se detecta cuando el dispositivo envía una lista nueva, semanalmente para apps y perfiles y a diario para certificados, o cuando usas **Preguntar al dispositivo**: la fecha mostrada es cuando se detectó; el cambio se produjo entre la lista anterior y esa. La primera lista de un dispositivo, y la primera después de una nueva inscripción o un cambio de propiedad, solo se registra como punto de partida. Busca por

nombre o identificador y filtra por tipo y cambio. Los cambios se conservan durante 365 días.

> Cuando una actualización del sistema operativo sustituye muchas apps de Apple a la vez, se muestran como una sola línea (por ejemplo, "23 apps de Apple actualizadas") que puedes expandir. La renovación del certificado MDM se muestra como **Certificado MDM renovado** . En los dispositivos de propiedad personal solo se muestran los cambios de los elementos gestionados por Cerberus Enterprise.

Columnas del historial de Apple

- **Fecha de creación**
- **Comando**
- **Estado**: **Enviado** (esperando al dispositivo, se entrega en cuanto se conecta), **Correcto**, **Respondido** (abre la fila para ver el resultado), **Esperando al dispositivo** (el dispositivo no puede ejecutar el comando en este momento), **Error** (abre la fila para ver el motivo) o **Cancelado** (se vació la cola de comandos del dispositivo, por ejemplo cuando volvió a inscribirse).
- **Fecha de ejecución**

Actualizar

Usa la acción de actualizar del panel Comandos para volver a cargar el historial de comandos.

Revision #60
Created 2025-12-17 09:33:25 UTC by Admin
Updated 2026-11-12 09:54:38 UTC by Admin