Estado del Dispositivo

- Descripción general del dispositivo
- Mapa de ubicaciones
- Gestión de SIM
- Comandos

Descripción general del dispositivo

Abre un dispositivo desde **Panel de control** → **Dispositivos** haciendo clic en la fila del dispositivo. El título de la página muestra el **Modelo** del dispositivo (cuando está disponible) y el **Id** interno.

Datos históricos frente a la inscripción actual

Cuando un dispositivo tiene varias inscripciones, Cerberus Enterprise puede mostrar un registro histórico de solo lectura. En ese caso, la página muestra un banner de **Datos históricos** y un botón para volver a los datos de la inscripción actual.

Campos superiores

La sección superior resume la identidad del dispositivo, la asignación y el estado de gestión. Algunos campos son específicos de cada plataforma y solo aparecen para dispositivos Android o Apple.

- **Id** y **Modelo**: identificadores de solo lectura.
- **Usuario**: muestra el usuario asignado actualmente (si lo hay). Desde el menú del usuario puedes **Abrir usuario** o **Cambiar usuario**, o asignar un usuario cuando no hay ninguno.
- **Modo de gestión** y **Propiedad**: se muestran con información emergente en la interfaz.
- **Estado**: estado actual del dispositivo (con icono y detalles en la información emergente). Un dispositivo en modo perdido muestra **Perdido** tanto en Android como en Apple, y un banner en la parte superior de la página indica qué hacer a continuación.
- **Perfil ADE** (solo Apple): muestra el perfil Automated Device Enrollment asignado (si lo hay) y te permite abrirlo o cambiarlo.
- **Política**: muestra la política asignada y te permite abrirla o cambiarla, o asignar una cuando no hay ninguna.
- **Estado de cumplimiento de la política** (cuando se asigna una política): indica si el dispositivo cumple.
- **Versión de la política** (cuando se asigna una política): indica si el dispositivo tiene aplicada la última versión de la política.

- **App Cerberus Enterprise** (solo iPhone y iPad): el estado de la app Cerberus Enterprise que Cerberus instala en el dispositivo. **No disponible** (iOS o iPadOS anterior a 18.4, sin número de serie en un dispositivo de empresa, o sin una Managed Apple Account en un dispositivo personal); **Aún no disponible en dispositivos personales**; **Esperando la información del dispositivo**; **Esperando la licencia de usuario de la Managed Apple Account** (dispositivos personales, mientras Apple confirma la licencia); **No instalada** (la app no está en tu biblioteca de Apple Business o Apps and Books no está configurado, con un enlace a **Configuración de la cuenta**); **Instalada · Apps and Books requiere atención** (el token caducó o la app salió de tu biblioteca: la app permanece instalada); **Configuración no disponible**; **Instalando…** (si el dispositivo no envía ningún informe de estado durante 30 minutos, la información emergente sugiere comprobar que está en línea y reiniciarlo, lo que suele iniciar la instalación de nuevo); **Esperando la aprobación del usuario**; **El usuario lo rechazó** y **Error de instalación** (ambos con **Reintentar**, que vuelve a preguntar al dispositivo); **Instalada · esperando a que se inicie la app** (la app aún no se ha abierto); **Instalada · configuración no aceptada**; y, una vez que la app se ha registrado, su versión, su último contacto y si las notificaciones están activadas.
- **Inscrito el** y **Último informe de estado**: marcas de tiempo de la inscripción y del último estado notificado.
- **Inscripción anulada el**: se muestra cuando se ha anulado la inscripción del dispositivo.

> Algunos datos y paneles solo están disponibles cuando la categoría correspondiente está habilitada en la política del dispositivo. Para más información, lee las páginas **Notificación de estado** y **Ubicación y geocercas**.

Paneles

La página del dispositivo se organiza en secciones expandibles. Según la plataforma y el estado, puedes ver uno o varios de los siguientes paneles:

- **Mapa de ubicación**: un panel con pestañas que muestra el historial de **Ubicación** del dispositivo actual y, en dispositivos Android, iPhone y iPad, una pestaña **Geocercas** para las transiciones de geocercas.
- **Gestión de SIM**: EID del dispositivo y SIM y eSIM instaladas. En Android, también los comandos eSIM y su historial; en iPhone y iPad propiedad de la empresa con datos móviles, también la itinerancia de datos, el Punto de acceso personal y **Actualizar planes móviles**. Consulta la página dedicada de **gestión de SIM**.
- **Comandos**: envía comandos al dispositivo y consulta el historial de comandos (según la plataforma).
- **Postura de seguridad**: el estado de seguridad del dispositivo y sus riesgos. En Android también el veredicto de Play Integrity. Hasta que el dispositivo lo informe, dice **Sin**

especificar, o **Aún no se ha informado** en un dispositivo Android que no ha enviado ningún dato de seguridad.

- **Por qué el dispositivo no cumple**: se muestra solo cuando el dispositivo no cumple, con un icono de alerta rojo; ábrelo para ver los motivos. En Android enumera los ajustes de política que no cumplen; en Apple también indica si una regla de cumplimiento bloqueó el dispositivo.
- **Estado del dispositivo** (solo Apple): versión del sistema operativo, progreso de la actualización de software, código de acceso, FileVault, batería y cuentas notificados por el dispositivo, y las actualizaciones del sistema disponibles para él. Consulta la página de **Comandos**.
- **Aplicaciones** (Android): apps instaladas y sus comentarios e informes de errores.
- **Aplicaciones** (solo Apple): las apps instaladas por la política, las apps instaladas con comandos y las apps instaladas por el usuario, con su estado de instalación, errores y acciones (reintentar, eliminar). En Mac también enumera los paquetes instalados por la política, con su estado y **Instalar de nuevo**; los paquetes instalados como apps gestionadas tienen una etiqueta **Gestionada**, y una nota indica cuándo se instaló un paquete sin gestión y por qué, o cuándo no se encontró su app una hora después de la descarga. En iPhone y iPad, la app Cerberus Enterprise tiene la etiqueta **Instalada por Cerberus**; no aparece en el filtro **Política**. Una app cuya configuración gestionada no aceptó el dispositivo tiene la etiqueta **Configuración no aceptada**. En iPhone y iPad personales (inscripción de usuario), una línea muestra la Managed Apple Account cuyos usuarios licencian las apps del App Store que se usan, las apps que esperan su licencia muestran **Esperando una licencia de usuario** o **Error de licencia de usuario**, una app cuyo aviso de instalación canceló el usuario muestra **Esperando la aprobación del usuario para la instalación**, y **Solicitar de nuevo** vuelve a pedir la licencia a Apple o muestra de nuevo el aviso. Consulta la página de **Comandos**.
- **Perfiles, certificados y seguridad** (solo Apple): perfiles de configuración, certificados y estado de seguridad notificados por el dispositivo.
- **Cambios de inventario** (solo Apple): una cronología de las apps, perfiles y certificados instalados, eliminados o actualizados en el dispositivo, con búsqueda y filtros por tipo y cambio. Consulta la página de **Comandos**.
- **Usuarios de iPad compartido** y **Usuarios de Mac** (solo Apple): los usuarios de un iPad compartido y los usuarios de un Mac. Consulta la página **Comandos**.
- **Informes de estado**: datos adicionales notificados por el dispositivo, que se muestran como un árbol de categorías y valores.
- **Historial de inscripciones**: inscripciones anteriores de este mismo dispositivo físico, que se muestran como una lista.

Pestañas del panel de ubicación

El panel **Mapa de ubicación** usa pestañas para mantener separados el historial de ubicación y las transiciones de geovalla.

- **Ubicación**: muestra filtros de historial, una búsqueda por intervalo de fechas, marcadores de ubicación, el círculo de precisión y los controles de seguimiento en vivo del dispositivo actual.
- **Geocercas** (Android, iPhone y iPad): muestra el historial de transiciones de geocercas en un mapa dedicado, con filtros de periodo, una opción para mostrar geocercas archivadas y una lista lateral de transiciones. En iPhone y iPad, una línea de estado también indica cuándo no puede funcionar la geolocalización por geocercas en el dispositivo.

Para conocer el comportamiento completo de estas pestañas, consulta **Mapa de ubicación**.

Acciones

En la parte inferior de la página puedes actualizar los datos y realizar acciones según la plataforma, el estado del dispositivo y el estado de la licencia.

- **Actualizar datos**: vuelve a cargar el registro del dispositivo.
- **Deshabilitar dispositivo** / **Habilitar dispositivo** (solo Android): disponible en los estados compatibles.
- **Anular la inscripción del dispositivo**: elimina la gestión del dispositivo. El comportamiento exacto depende de la plataforma y la propiedad (por ejemplo, Android puede borrar un perfil de trabajo o restablecer los valores de fábrica).
- **Eliminar dispositivo**: disponible cuando el dispositivo ya tiene la inscripción anulada y su registro se puede eliminar.

Mapa de ubicaciones

Esta página documenta las herramientas de ubicación específicas del dispositivo disponibles en **Vista general del dispositivo**. El panel contiene una pestaña **Ubicación** para el historial de posiciones y, en dispositivos Android, iPhones y iPads, una pestaña **Geovalla** para las transiciones de geovalla.

Requisitos previos

En Android, los datos de ubicación del dispositivo se muestran solo cuando la notificación de ubicación está habilitada en la política del dispositivo. Para habilitarla, abre la política y activa **Ubicación y geocercas** → **Notificar ubicación**. Para más detalles, consulta **Ubicación y geocercas**.

En iPhone y iPad, la ubicación procede de la app Cerberus Enterprise, una vez que el usuario lo permite, o del comando **Localizar dispositivo** mientras el dispositivo está en modo perdido. Los Mac y otros dispositivos Apple no informan de su ubicación.

> En los dispositivos que no están totalmente gestionados, los datos de ubicación pueden depender de que la app Cerberus Enterprise tenga los permisos de ubicación necesarios y de que los servicios de ubicación estén habilitados en el dispositivo.

> En los dispositivos personales (User Enrollment), la ubicación y las geovallas están disponibles solo cuando la política de Apple tiene la opción **Ubicación y geovallas en dispositivos personales** activada y solo si el usuario permite la ubicación para la app Cerberus Enterprise. De lo contrario, la página de su dispositivo no muestra las acciones de ubicación ni el seguimiento en tiempo real. El modo perdido nunca está disponible en dispositivos personales.

> Para consultar el mapa global de varios dispositivos disponible en el panel de control, consulta **Mapa de ubicaciones del panel de control**.

Estado de carga y sin datos

- Mientras se cargan los datos de ubicación, el panel muestra una superposición de carga en el mapa.
- Si el dispositivo no tiene datos de ubicación disponibles, el panel muestra un mensaje que indica **No hay datos de ubicación disponibles**. En Android añade un recordatorio para habilitar el informe de ubicación en la política asignada, cuando está desactivado. En Apple indica de dónde procede la ubicación, o que este tipo de dispositivo no la informa.
- Si hay un filtro de fecha activo y ninguna muestra coincide, el panel muestra **No hay datos disponibles en el intervalo de fechas seleccionado**.

Pestaña Ubicación

Abre la pestaña **Ubicación** para consultar el historial de un solo dispositivo. Los filtros disponibles incluyen la última ubicación conocida, intervalos de historial recientes, un intervalo de fechas personalizado y el seguimiento en tiempo real.

- **Última**: muestra la última ubicación conocida.
- **Hoy**, **Últimos 7 días** y **Últimos 30 días**: muestran las ubicaciones registradas durante el periodo seleccionado.
- **Buscar**: te permite elegir un intervalo de fechas personalizado.
- **En directo**: inicia o detiene el seguimiento en tiempo real del dispositivo actual.

> Las ubicaciones se conservan durante **90 días**: las más antiguas se eliminan automáticamente cada noche. La última ubicación de cada dispositivo inscrito se conserva siempre, por lo que el dispositivo sigue en los mapas aunque no haya enviado su ubicación desde hace mucho tiempo. En los dispositivos eliminados y las inscripciones anteriores, se eliminan todas las ubicaciones de más de 90 días. Por este motivo, el intervalo de fechas del filtro **Buscar** no puede empezar hace más de 90 días.

Detalles del marcador

Cuando haces clic en un marcador de ubicación, se abre una ventana de información con:

- La marca de tiempo del registro de ubicación.
- La **precisión** notificada (en metros).
- La **velocidad** notificada, cuando el dispositivo la proporciona.
- El **rumbo** o la orientación notificados, cuando el dispositivo los proporciona.

Círculo de precisión

Cuando la ventana de información está abierta, se muestra un círculo de precisión alrededor del marcador. El radio del círculo corresponde a la precisión notificada (en metros). Al cerrar la ventana de información se oculta el círculo.

Seguimiento en vivo

En la vista del historial del dispositivo, seleccionar el filtro **En vivo** inicia una solicitud de seguimiento en tiempo real para ese dispositivo concreto. Cerberus Enterprise pide confirmación antes de iniciar la solicitud.

- El seguimiento en vivo se ejecuta durante un máximo de **15 minutos**.
- Mientras el seguimiento en vivo está activo, los dispositivos Android muestran una notificación y los iPhone y iPad muestran el indicador de ubicación.
- Mientras el seguimiento en vivo está activo, el panel sigue actualizando la última ubicación y el indicador de en vivo permanece visible.
- Si seleccionas de nuevo el filtro En vivo, puedes detener el seguimiento en vivo antes de que termine el tiempo de espera.
- En **iPhone y iPad**, el seguimiento en vivo funciona a través de la app Cerberus Enterprise, con el acceso a la ubicación configurado en **Siempre**. La solicitud normalmente activa la app aunque no esté abierta, y la app envía entonces las ubicaciones durante toda la sesión. iOS no garantiza estas solicitudes: puede retrasarlas o no entregarlas, por ejemplo en el modo de bajo consumo o sin conexión de red. Si no llega ninguna ubicación en 2 minutos, el panel de control cancela la solicitud: pide al usuario que abra la app una vez y vuelve a intentarlo.

Pestaña Geocercas

En dispositivos Android, iPhone y iPad, la segunda pestaña muestra las transiciones de geocercas generadas a partir de las geocercas definidas en la política asignada.

- El mapa muestra las áreas de geocercas actuales junto con los puntos de transición registrados.
- La lista de transiciones de la derecha te permite inspeccionar los eventos de **entrada** y **salida**.
- Los filtros disponibles son **Hoy**, **Últimos 7 días**, **Últimos 30 días** y una búsqueda personalizada por intervalo de fechas.
- **Incluir archivadas** también muestra las transiciones relacionadas con definiciones de geocercas antiguas que ya no están presentes en la política actual.
- Las transiciones de geocercas se conservan durante **90 días** y las más antiguas se eliminan automáticamente cada noche, por lo que la búsqueda con un intervalo de fechas personalizado no puede empezar hace más de 90 días.

En iPhone y iPad, cuando la política tiene geocercas activas, una línea de estado en la parte superior de la pestaña muestra si la geolocalización por geocercas funciona en el dispositivo. Te indica cuándo no puede funcionar: la app Cerberus Enterprise no ha contactado con el servidor o debe actualizarse, el acceso a la ubicación no está configurado en **Siempre**, **Ubicación precisa** o **Actualización en segundo plano** está desactivado, **Modo de bajo consumo** estaba activado cuando la app notificó por última vez su configuración (los eventos y cambios de geocercas pueden entonces retrasarse horas), o la app aún no ha aplicado las últimas geocercas. Cuando todo funciona, muestra cuántas geocercas monitoriza la app.

Detalles de la transición de geocerca

Al seleccionar una transición, se abren sus detalles en el mapa y se resalta la entrada correspondiente de la lista. Cuando están disponibles, Cerberus Enterprise también muestra las coordenadas del dispositivo y la precisión notificada para esa transición.

Gestión de SIM

La página del dispositivo proporciona un panel **Gestión de SIM**. En dispositivos Android gestiona las SIM y los perfiles eSIM instalados en el dispositivo, añade o elimina perfiles eSIM y muestra el historial de los comandos eSIM enviados al dispositivo. En iPhone y iPad con datos móviles propiedad de la empresa muestra las SIM y los planes eSIM notificados por el dispositivo y permite que el dispositivo descargue los planes eSIM preparados por el operador: consulta **iPhone y iPad** más abajo.

> Los dispositivos totalmente gestionados notifican la información de SIM cuando el informe de **Información de red** está habilitado en la política del dispositivo (Cerberus Enterprise siempre habilita esta opción). Consulta la página de **Informes de estado**.

EID del dispositivo

El EID (eUICC Identifier) identifica el hardware eSIM del dispositivo. Los operadores lo usan para vincular perfiles eSIM al dispositivo, por lo que obtenerlo suele ser el primer paso de un flujo de aprovisionamiento de eSIM.

- **Dispositivos propiedad de la empresa** (Android 13 o posterior): el EID se notifica automáticamente con el estado del dispositivo y no se requiere la interacción del usuario.
- **Dispositivos de propiedad personal** (Android 13 o posterior): usa el botón **Solicitar EID**. El usuario verá una notificación en el dispositivo que le pedirá compartir el EID, y podrá aprobar o rechazar la solicitud. El EID solo se muestra si el usuario aprueba. Mientras la solicitud está pendiente, el botón permanece deshabilitado.

> Al enviar una solicitud de EID se muestra primero un diálogo de confirmación, porque el usuario verá una notificación en el dispositivo.

SIM instaladas

La tabla de **SIM instaladas** enumera las SIM conocidas actualmente para el dispositivo, incluidas las SIM físicas y los perfiles eSIM. En dispositivos de propiedad personal, los perfiles eSIM instalados con el comando **Añadir eSIM** se muestran aunque el dispositivo no notifique información de SIM.

- **Operador**: el nombre del operador asociado a la SIM (cuando se notifica).
- **Número de teléfono**: el número de teléfono asociado a la SIM (cuando se notifica).
- **ICCID**: el identificador de tarjeta de circuito integrado de la SIM.
- **Estado de activación**: si la eSIM está activada o no. Solo se notifica para eSIM en Android 15 o posterior.
- **Modo de configuración**: si el administrador o el usuario configuró la eSIM. Solo se notifica para eSIM en Android 15 o posterior.
- **Tipo de SIM**: muestra si el dispositivo notifica la entrada como eSIM.

> Las eSIM con un comando de eliminación en curso o ejecutado (no fallido) muestran un estado de activación temporal **Eliminando**. La entrada desaparece de la lista cuando el dispositivo notifica la lista de SIM actualizada. Mientras hay una eliminación en curso, el botón de eliminar no está disponible para evitar enviar el mismo comando dos veces.

Eliminar eSIM

Usa el botón de eliminar junto a una eSIM instalada para quitar su perfil del dispositivo. Un diálogo de confirmación te pide que confirmes el ICCID de la eSIM que se va a eliminar antes de enviar el comando. La eliminación de una eSIM es compatible con Android 15 o posterior.

Añadir eSIM

La sección **Añadir eSIM** instala un nuevo perfil eSIM en el dispositivo (compatible con Android 15 o posterior). Requiere:

- **Validez**: cuánto tiempo es válido el comando si no se puede ejecutar de inmediato.
- **Código de activación**: el código de activación del perfil eSIM, proporcionado por el operador. Puedes introducir el código completo, o solo la dirección SM-DP+ para que el dispositivo descubra un perfil que el operador ya haya vinculado a su EID.
- **Estado de activación**: si el perfil eSIM debe activarse automáticamente después de la descarga, o dejarse sin activar para que el usuario lo active manualmente.

Historial de comandos

Debajo de la sección Añadir eSIM, el panel muestra el historial de los comandos eSIM enviados al dispositivo: **Añadir eSIM**, **Eliminar eSIM** y **Solicitar EID**. La tabla se puede ordenar y admite paginación. Algunas filas se pueden expandir para ver los parámetros del comando (por ejemplo, el código de activación o el ICCID) y el estado de ejecución, incluidos los detalles del error de eSIM cuando una operación falla en el dispositivo.

- **Fecha de creación**
- **Comando**
- **Validez**
- **Estado**
- **Error**: muestra el estado de error de eSIM (por ejemplo, *El usuario lo denegó*, *Código de activación no válido* o *ICCID no encontrado*) cuando la ejecución del comando lo notifica.
- **Fecha de ejecución**

Borrar eSIM al borrar y anular la inscripción

Cuando borras el dispositivo desde el panel de comandos, la marca **Borrar eSIM** controla si los perfiles eSIM se eliminan con el borrado. En dispositivos de propiedad personal con un perfil de trabajo, esta marca está habilitada de forma predeterminada (las eSIM gestionadas se eliminan, las eSIM de propiedad personal no se ven afectadas). La misma marca está disponible en el diálogo de confirmación **Anular la inscripción del dispositivo**.

iPhone y iPad

El panel se muestra para iPhone y para iPad que hayan notificado datos móviles (un iPad solo Wi-Fi no tiene), solo cuando el dispositivo es propiedad de la empresa y no es una inscripción de usuario. La información móvil se solicita al dispositivo junto con la información del dispositivo: en la inscripción, cada día, con **Actualizar información del dispositivo**, cuando su propiedad pasa a ser de la empresa y unos minutos después de **Actualizar planes móviles**.

- **EID del dispositivo**: el EID notificado con las SIM, con un botón para copiarlo para el operador. Si el dispositivo no lo notifica, el usuario lo encuentra en Ajustes > General > Información.
- **Notificado**, **Itinerancia de datos**, **Punto de acceso personal** y **Firmware del módem**: cuándo respondió el dispositivo y el estado que notificó. La itinerancia de datos y el Punto de acceso personal se pueden cambiar con **Ajustes del dispositivo** en el panel de comandos, que también muestra el estado actual.
- **SIM**: una fila por cada SIM o plan eSIM (los dispositivos con SIM dual tienen dos), con la ranura tal como la notifica el dispositivo, su etiqueta y su tipo (**eSIM** cuando el dispositivo notifica el EID con ella, **tarjeta SIM** en caso contrario), el operador (el operador de origen en una información emergente cuando el dispositivo está en itinerancia en otra red), el número de teléfono, el ICCID, el EID, el IMEI, la SIM usada para datos y para llamadas, y la itinerancia. Una ranura eSIM sin plan se muestra atenuada como **Sin plan**.
- **Este dispositivo no notificó ninguna SIM** significa que el dispositivo respondió sin ninguna SIM; **Aún no hay información móvil** significa que todavía no ha respondido:

usa **Actualizar información del dispositivo**.

> Los números de teléfono, el ICCID, el IMEI y el EID identifican a la persona y a la línea: nunca se solicitan a dispositivos de propiedad personal ni a inscripciones de usuario. Cuando un dispositivo pasa a ser de propiedad personal, la información se elimina de inmediato y se oculta en los resultados de los antiguos comandos de información del dispositivo del historial de comandos. No se exporta ni se escribe en los registros del sistema.

Actualizar planes móviles

iPhone y iPad no pueden instalar una eSIM a partir de un código de activación. El operador vincula (reserva) el plan eSIM al EID del dispositivo en su servidor eSIM (SM-DP+) y te da la dirección de ese servidor; **Actualizar planes móviles** pide entonces al dispositivo que descargue los planes que le esperan. El botón **Actualizar planes móviles** del panel selecciona el comando en el panel de comandos, donde introduces la **URL del servidor eSIM del operador**:

- **Una dirección https://**, que se envía tal cual. No se aceptan direcciones con http://, con un nombre de usuario o contraseña, o con una parte #.
- **Un nombre de host**, por ejemplo *smdp.carrier.example*, que se envía como https://smdp.carrier.example.
- **Un código de activación LPA** (LPA:1$server$code, el texto de un código QR de eSIM): solo se usa el servidor, porque el comando no puede transportar el código. El operador debe vincular el plan al EID del dispositivo; de lo contrario, el dispositivo no encuentra nada que descargar.

El dispositivo instala y activa el plan sin preguntar al usuario, también cuando no está supervisado. El éxito en el historial de comandos significa que el dispositivo aceptó la solicitud, no que se haya instalado un plan: la instalación puede tardar hasta tres minutos, y Cerberus Enterprise vuelve a solicitar las SIM al dispositivo unos tres minutos después, de modo que el nuevo plan aparece en el panel. Los errores 36001 (el dispositivo no pudo acceder a su sistema móvil), 36002 (sin compatibilidad con eSIM) y 36003 (sistema móvil ocupado, inténtalo de nuevo más tarde) se explican en los registros del sistema. Un plan descargado una vez no se puede volver a descargar: si la instalación falla, contacta con el operador. El comando también está disponible para varios dispositivos a la vez en el menú **Acciones para dispositivos Apple** de la página Dispositivos.

Lo que Apple no permite

- **Añadir eSIM** desde un código de activación: no es posible; usa **Actualizar planes móviles** con un plan vinculado al EID.
- **Eliminar eSIM**: una eSIM no se puede eliminar de forma remota una a una. Si borras el dispositivo con **Conservar el plan de datos eSIM** desactivado, se eliminan todas las eSIM. Para detener un solo plan, pide al operador que lo desactive: el plan permanece en el dispositivo pero no puede conectarse.

- **Solicitar EID**: no es necesario; el EID viene con las SIM de los dispositivos propiedad de la empresa.
- Los **Mac** no tienen gestión de datos móviles ni de eSIM.

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.