Aprovisionamiento de Dispositivos - Android

- Dispositivos compatibles
- Tokens de inscripción
- Dispositivos de propiedad personal
- Dispositivos propiedad de la empresa para uso laboral y personal
- Dispositivos propiedad de la empresa solo para uso laboral
- Zero-touch
- Autenticación con Google para la inscripción

Dispositivos compatibles

En general, cualquier dispositivo con Android 6 o posterior y Google Play Services es compatible con Cerberus Enterprise.

Para una mejor experiencia de usuario, te recomendamos usar dispositivos que cumplan los requisitos de Android Enterprise Recommended.

> Algunas funciones están limitadas a versiones específicas de Android o pueden comportarse de forma distinta según la versión del sistema operativo. Para obtener más información sobre una función específica, consulta la sección Políticas de la documentación.

Cerberus Enterprise admite tanto dispositivos propiedad de la empresa como de propiedad personal, y dos modos de gestión: propietario del dispositivo y propietario del perfil.

Los dispositivos de propiedad personal se pueden gestionar mediante un **perfil de trabajo**. Esto permite una solución BYOD al mantener los datos y las apps de trabajo de los empleados separados de los datos y las apps personales, mejorando tanto la seguridad como la privacidad. Esta opción es adecuada para dispositivos que ya son propiedad de los empleados y que quieres inscribir en tu organización para uso laboral.

Los dispositivos propiedad de la empresa también se pueden gestionar mediante un perfil de trabajo, pero también puedes elegir la opción **totalmente gestionado**, que permite un control más estricto del dispositivo. Los dispositivos propiedad de la empresa con un perfil de trabajo son adecuados cuando proporcionas dispositivos corporativos a los empleados para el trabajo, sin dejar de permitir el uso personal. Los dispositivos totalmente gestionados son más adecuados para dispositivos que deben usarse solo para el trabajo, o para **dispositivos dedicados** (COSU, corporate-owned single-use), como los kioscos.

Para obtener más información sobre el aprovisionamiento de dispositivos, consulta la página Descripción general del aprovisionamiento de dispositivos.

Tokens de inscripción

Cerberus Enterprise usa tokens de inscripción para iniciar el proceso de inscripción (aprovisionamiento) de dispositivos Android. El token que selecciones define la política inicial aplicada a los dispositivos inscritos e influye en qué modos de aprovisionamiento se permiten.

> La pestaña de tokens de inscripción de Android solo está disponible después de completar **Configuración de Android Management**.

Dónde encontrar los tokens de inscripción

En el panel de control, abre **Tokens de inscripción**. Según la configuración de tu cuenta, la página puede mostrar varias pestañas (tokens de Android, inscripción con inicio de sesión de Google, inscripción manual de Apple e Inscripción automática de dispositivos de Apple).

> Si tu empresa de Android está respaldada por un dominio de Google gestionado (Google Workspace), el panel de control también puede mostrar una pestaña **Authenticate Using Google Enrollment**. Para obtener detalles sobre cómo habilitarla y usarla, consulta **Authenticate Using Google enrollment**.

Lista de tokens de inscripción (Android)

La pestaña de tokens de Android muestra una tabla con todos los tokens. Al hacer clic en una fila se abre la página de detalles del token.

Columnas

- **Estado**: **Activo** (los dispositivos pueden inscribirse con el token), **Caducado** (ha pasado la fecha de vencimiento) o **Agotado** (un token de un solo uso que ya se utilizó).
- **Política**: la política asignada al token (la información sobre herramientas muestra el id de la política). **Política eliminada** significa que la política se eliminó después de crear el token.
- **Usuario**: usuario opcional asignado previamente a los dispositivos inscritos con el token. **Usuario eliminado** significa que el usuario se eliminó después de crear el token.
- **Inscripciones**: cuántos dispositivos se inscribieron con el token, mostrado como **n / 1** en un token de un solo uso.
- **Uso personal**: Permitido / No permitido / Dispositivo dedicado.
- **Creado**: cuándo se creó el token. La tabla muestra primero los tokens más recientes.
- **Caducidad**: fecha y hora de caducidad, o **Nunca**.
- **Código de inscripción**: el código del token, el que escribes en el dispositivo cuando lo inscribes sin un código QR.

Acciones

- Cada fila tiene una acción de eliminación (**Eliminar token de inscripción**). La eliminación está deshabilitada cuando la licencia ha caducado.
- La tabla admite la selección de varias filas: puedes habilitar el modo de selección, seleccionar varios tokens y eliminarlos con **Eliminar tokens seleccionados**.
- Usa la acción de actualizar para volver a cargar la lista. La tabla está paginada (10/25/50 elementos por página).

Crear un nuevo token de inscripción

En la pestaña de tokens de Android, haz clic en **Nuevo token de inscripción** para abrir la página de creación de tokens. Si tu licencia ha caducado, el botón de creación está deshabilitado.

Opciones del token

1. Política

Obligatorio. La política que se aplica automáticamente a todos los dispositivos inscritos con este token. Selecciona una de tus **políticas de Android**. Si aún no tienes ninguna política, crea una primero.

2. Usuario

Opcional. Si se configura, los dispositivos recién inscritos se asocian automáticamente a este usuario.

3. Uso personal

Controla si se permite el uso personal en un dispositivo aprovisionado con este token de inscripción:

- **Permitido**: adecuado para dispositivos de propiedad personal (perfil de trabajo) y dispositivos propiedad de la empresa para uso laboral y personal.
- **No permitido**: adecuado para dispositivos propiedad de la empresa solo para uso laboral (totalmente gestionados).
- **Dispositivo dedicado**: adecuado para dispositivos de kiosco o dedicados (el dispositivo no está asociado a un único usuario).

4. Usos permitidos

Selecciona si el token se puede usar varias veces (**Múltiples**) o solo una vez (**Solo una vez**).

5. Caducidad

Selecciona la unidad de caducidad (**Minutos**, **Horas**, **Días** o **Nunca**). Cuando no se configure como Nunca, introduce el valor de caducidad. El intervalo permitido depende de la unidad seleccionada y puede llegar hasta 10.000 días.

6. Autenticación de Google

Controla si el usuario debe autenticarse con una cuenta de Google durante la inscripción del dispositivo:

- **Sin especificar**: se usa la configuración de autenticación de Google de nivel de empresa para determinar si el usuario debe autenticarse con Google durante la inscripción.
- **Opcional**: el usuario puede optar por omitir la autenticación de Google durante la inscripción.
- **Obligatorio**: el usuario debe autenticarse con una cuenta de Google para continuar con la inscripción.

Cuando se selecciona **Obligatorio**, aparece un campo opcional **Correo de la cuenta requerida**. Si se configura, el usuario debe autenticarse con esa cuenta de Google específica durante la inscripción.

Opciones de aprovisionamiento (solo código QR)

Estas opciones adicionales se incorporan en el código QR y se aplican durante el aprovisionamiento de dispositivos totalmente gestionados inscritos escaneando el código QR. No se aplican a perfiles de trabajo ni a dispositivos inscritos mediante la URL de inscripción o el token.

Configuración de Wi-Fi

Usa esta opción para que un dispositivo se conecte automáticamente a Wi-Fi durante el aprovisionamiento, de modo que pueda descargar e inicializar la app de gestión. Los campos disponibles incluyen **SSID**, **SSID oculto**, **Seguridad** y (cuando sea necesario) **Frase de contraseña**.

También puedes configurar un proxy HTTP (**Proxy**) y, según el modo, establecer **Host**/**Puerto**, **PAC URI** y **Host de omisión del proxy**.

Otras opciones

Las opciones adicionales incluyen **Configuración regional**, **Zona horaria** y **Omitir cifrado**.

Detalles del token de inscripción

Cuando abres un token, la página de detalles muestra la configuración del token y la información de uso:

- **Estado**, **Caducidad**, **Uso**, **Uso personal**, **Usos permitidos** y (cuando se configura) **Autenticación de Google** con el **Correo de la cuenta requerida** opcional.
- **Token**: el valor sin formato del token de inscripción (se puede copiar).
- **URL de inscripción**: una URL de inscripción de Google Android Enterprise (se puede copiar y enviar por correo electrónico).
- **Código QR**: se muestra en el lado derecho de la página y se usa para inscribir dispositivos totalmente gestionados.

> Para conocer los procedimientos de aprovisionamiento paso a paso, sigue las guías de inscripción de Android: **Dispositivos de propiedad personal**, **Dispositivos propiedad de la empresa para uso laboral y personal**, **Dispositivos propiedad de la empresa solo para uso laboral** y **Zero-touch**.

Dispositivos de propiedad personal

Los dispositivos propiedad de los empleados se pueden configurar con un **perfil de trabajo**. Un perfil de trabajo proporciona un espacio independiente para las apps y los datos de trabajo, separado de las apps y los datos personales. La mayoría de las políticas de apps, datos y otras gestiones se aplican solo al perfil de trabajo, mientras que las apps y los datos personales de los empleados siguen siendo privados.
Para configurar un perfil de trabajo en un dispositivo de propiedad personal, usa uno de los siguientes métodos de aprovisionamiento (asegúrate de que el token de inscripción tenga ***Uso personal*** configurado como **Permitido**):

Enlace del token de inscripción

Versión de Android
6.0+

Puedes proporcionar la URL de inscripción a los usuarios finales. Cuando un usuario final abre el enlace desde su dispositivo, se le guía por la configuración del perfil de trabajo.

Añadir perfil de trabajo desde "*Configuración*"

Versión de Android
6.0+

Para configurar un perfil de trabajo en su dispositivo, un usuario puede abrir la app ***Configuración*** del dispositivo y usar la barra de búsqueda para encontrar y tocar la opción ***Configurar tu perfil de trabajo***.

Si la búsqueda no da resultados, la ubicación de esta opción puede variar. Estas son algunas posibilidades:

- *Configuración -> Servicios y preferencias de Google -> Todos los servicios -> Configurar tu perfil de trabajo*.
- *Configuración -> Google -> Configurar y restaurar -> Configurar tu perfil de trabajo*.

Estos pasos inician un asistente de configuración que descarga *Android Device Policy* en el dispositivo. A continuación, se pedirá al usuario que escanee un código QR o introduzca manualmente un token de inscripción para completar la configuración del perfil de trabajo.

Descargar Android Device Policy

Versión de Android
6.0+

Para configurar un perfil de trabajo en su dispositivo, un usuario puede descargar Android Device Policy desde Google Play Store. Una vez instalada la app, se pedirá al usuario que escanee un código QR o introduzca manualmente un token de inscripción para completar la configuración del perfil de trabajo.

iPhone y iPad personales

Los iPhone y iPad personales (y los Mac) se inscriben con **User Enrollment** de Apple: el usuario inicia sesión con su Managed Apple Account en los ajustes del dispositivo, y solo se gestionan las apps, cuentas y datos de trabajo. En iPhone y iPad, las apps del App Store de la política y la app **Cerberus Enterprise** se instalan con una licencia de usuario de esa cuenta. La ubicación de los dispositivos personales se recopila solo si su política activa **Ubicación y geovallas en dispositivos personales** y el usuario lo permite. Consulta **Inscripción mediante cuenta de Apple**.

Dispositivos propiedad de la empresa para uso laboral y personal

Configurar un dispositivo propiedad de la empresa con un **perfil de trabajo** permite usar el dispositivo tanto para el trabajo como para uso personal. En los dispositivos propiedad de la empresa con perfiles de trabajo:

- La mayoría de las políticas de apps, datos y otras gestiones se aplican solo al perfil de trabajo.
- Los perfiles personales de los empleados siguen siendo privados. Sin embargo, las empresas pueden aplicar determinadas políticas para todo el dispositivo y políticas de uso personal.
- Las empresas pueden usar *Block scope* para aplicar acciones de cumplimiento en todo un dispositivo o solo en su perfil de trabajo.
- La anulación de la inscripción del dispositivo y los comandos del dispositivo se aplican a todo el dispositivo.

Para configurar un dispositivo propiedad de la empresa con un perfil de trabajo, usa uno de los siguientes métodos de aprovisionamiento (asegúrate de que el token de inscripción tenga **Uso personal** configurado como **Permitido**):

Método del código QR

Versión de Android
8.0+

En un dispositivo nuevo o restablecido de fábrica, el usuario (normalmente un administrador de TI) toca la pantalla seis veces en el mismo punto. Esto hace que el dispositivo solicite al usuario escanear un código QR.

Dispositivos propiedad de la empresa solo para uso laboral

Gestión completa del dispositivo es adecuada para dispositivos propiedad de la empresa destinados exclusivamente a fines laborales. Las empresas pueden gestionar todas las apps del dispositivo y aplicar toda la gama de políticas y comandos de Android Management API.
También es posible bloquear un dispositivo (mediante una política) a una sola app o a un pequeño conjunto de apps para un propósito o caso de uso concreto. Este subconjunto de dispositivos totalmente gestionados se denomina **dispositivos dedicados**.
Para configurar la gestión completa en un dispositivo propiedad de la empresa, usa uno de los siguientes métodos de aprovisionamiento (asegúrate de que el token de inscripción tenga **Uso personal** configurado como **No permitido**):

Método del código QR

Versión de Android
7.0+

En un dispositivo nuevo o restablecido de fábrica, el usuario (normalmente un administrador de TI) toca la pantalla seis veces en el mismo punto. Esto hace que el dispositivo solicite al usuario escanear un código QR.

Método del identificador DPC

Versión de Android
5.1+

Si Android Device Policy no se puede añadir mediante un código QR, un usuario o administrador de TI puede seguir estos pasos para aprovisionar un dispositivo totalmente gestionado o dedicado:

1. Sigue el asistente de configuración en un dispositivo nuevo o restablecido de fábrica.
2. Introduce los datos de inicio de sesión de Wi-Fi para conectar el dispositivo a internet.
3. Cuando se te pida iniciar sesión, introduce **afw#setup**, lo que descarga Android Device Policy.
4. Escanea un código QR o introduce manualmente un token de inscripción para aprovisionar el dispositivo.

Zero-touch

Los administradores de TI pueden aprovisionar dispositivos propiedad de la empresa con el método de inscripción Zero-touch, descrito en Zero-touch enrollment for IT admins. Cuando se enciende un dispositivo por primera vez, se le aplican automáticamente los ajustes definidos por el administrador de TI.

Los administradores de TI pueden preconfigurar dispositivos comprados a revendedores autorizados y gestionarlos mediante el panel de control de Cerberus Enterprise. Para vincular tu cuenta de Zero-touch, ve a la sección **Zero-touch** del panel de control y sigue las instrucciones.

Versión de Android	Perfil de trabajo	Dispositivo totalmente gestionado	Dispositivo dedicado
8.0+ (Pixel 7.1+)	✓	✓	✓

Autenticación con Google para la inscripción

Authenticate Using Google enrollment (también denominada **Google Authentication for Enrollment**) permite a los usuarios autenticarse con su cuenta de Google Workspace durante la inscripción de dispositivos Android.

> Esta función solo está disponible para empresas de Android respaldadas por un dominio de Google gestionado (Google Workspace).

Dónde encontrarlo

En el panel de control, abre **Tokens de inscripción** y selecciona la pestaña **Authenticate Using Google Enrollment**. La pestaña solo se muestra cuando Android Management está configurado y la integración con Google Workspace está disponible para tu empresa.

Habilitar (o deshabilitar) la autenticación de Google

La autenticación de Google se habilita desde la **Google Admin console**. Después de cambiar la configuración, vuelve a Cerberus Enterprise y usa **Actualizar estado** para recargar la configuración actual.

1. Inicia sesión en la **Google Admin console** con una cuenta de administrador.
2. Abre **Dispositivos**.
3. Ve a **Dispositivos móviles y endpoints** → **Configuración** → **Integraciones de terceros**.
4. Busca la **integración de Android EMM** de Cerberus Enterprise y ábrela.
5. Haz clic en **Gestionar proveedores EMM**.
6. Activa o desactiva **Authenticate Using Google** para habilitar o deshabilitar la autenticación de Google para la inscripción.

7. Haz clic en **Guardar**.
8. Vuelve al panel de control de Cerberus Enterprise y haz clic en **Actualizar estado** en la pestaña **Authenticate Using Google Enrollment**.

Token de inscripción de autenticación de Google

Cuando la autenticación de Google está habilitada, el panel de control muestra un token de inscripción dedicado para este modo de inscripción. La página puede mostrar un **código QR**, un valor de **token de inscripción** y una **URL de inscripción** (se puede copiar y enviar por correo electrónico).

Opciones clave

- **Permitir uso personal**: controla si el token puede inscribir dispositivos para uso laboral y personal (escenarios de perfil de trabajo) o solo para uso laboral (escenarios totalmente gestionados o dedicados).
- **Política predeterminada de reserva**: la política que se aplica cuando el usuario que se inscribe no tiene asignada una política predeterminada específica de autenticación de Google.

Interacción con las políticas

La configuración de política **Autenticación de configuración de la cuenta de trabajo** (workAccountSetupConfig.authenticationType) controla cómo se autentican los usuarios durante la configuración de la cuenta de trabajo, pero la configuración de Google Admin Console **Authenticate Using Google** y el tipo de token de inscripción aún pueden exigir autenticación.

En los dispositivos ya inscritos, esta política solo se aplica si el dispositivo está gestionado por una cuenta de Google Play gestionada (es decir, inscrito sin **Authenticate Using Google Enrollment**).

> Algunas acciones (por ejemplo, cambiar las opciones del token) pueden estar deshabilitadas cuando la licencia ha caducado.

Inscribir un dispositivo

Durante la inscripción, se pide al usuario que se autentique con su cuenta de Google Workspace. Después de una inscripción correcta, el dispositivo se asocia al usuario autenticado.

Perfil de trabajo (dispositivos de propiedad personal)

- Comparte la **URL de inscripción** con el usuario. Cuando el usuario la abre en su dispositivo Android, se le guía por la configuración del perfil de trabajo y la autenticación de Google.
- Como alternativa, el usuario puede empezar desde los Ajustes de Android y elegir el flujo de configuración del perfil de trabajo, luego escanear el código QR o introducir el token de inscripción cuando se le solicite.

Dispositivos propiedad de la empresa

- **Método del código QR**: en un dispositivo nuevo o restablecido de fábrica, toca la pantalla varias veces en el mismo punto hasta que aparezca la solicitud del código QR, luego escanea el código QR que se muestra en el panel de control.
- **Método del identificador DPC** (cuando el escaneo de QR no esté disponible): sigue el asistente de configuración, conéctate a Wi-Fi y, cuando se te pida iniciar sesión, introduce **afw#setup** y continúa escaneando el código QR o introduciendo el token de inscripción. Cuando se te solicite, autentícate con la cuenta de Google Workspace.

Para consultar los procedimientos generales de aprovisionamiento de Android (perfil de trabajo frente a totalmente gestionado), consulta las páginas estándar de inscripción de Android de este manual.