Aprovisionamiento de Dispositivos - Android

Dispositivos compatibles

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

Para una mejor experiencia de usuario, le recomendamos utilizar dispositivos que cumplan con los requisitos de dispositivos recomendados de Android Enterprise.

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

Cerberus Enterprise es compatible tanto con dispositivos propiedad de la empresa como con dispositivos personales, y ofrece dos modos de gestión: propietario del dispositivo y propietario del perfil.

Los dispositivos de propiedad personal pueden gestionarse a través de un **perfil de trabajo**. Esto permite una solución BYOD (Bring Your Own Device) manteniendo los datos y las aplicaciones laborales de los empleados separados de los datos y las aplicaciones personales, mejorando tanto la seguridad como la privacidad. Esta opción es adecuada para dispositivos que ya son propiedad de los empleados y que desea inscribir en su organización para uso laboral.

Dispositivos propiedad de la empresa también pueden ser gestionados a través de un perfil de trabajo, pero también puede optar por la opción de **gestión completa**, que permite un control más estricto sobre el dispositivo. Los dispositivos propiedad de la empresa con un perfil de trabajo son adecuados cuando proporciona dispositivos corporativos a los empleados para el trabajo, al tiempo que permite el uso personal. Los dispositivos con gestión completa son más adecuados para dispositivos que deben utilizarse únicamente para el trabajo, o para **dispositivos dedicados** (COSU, dispositivos de uso único propiedad de la empresa), como quioscos.

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

Tokens de inscripción

Cerberus Enterprise utiliza tokens de inscripción para iniciar el proceso de inscripción (configuración) de dispositivos Android. El token que seleccione define la política inicial aplicada a los dispositivos inscritos e influye en los modos de configuración permitidos.

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

¿Dónde encontrar los tokens de inscripción?

En el panel, abra **Tokens de inscripción**. Dependiendo de la configuración de su cuenta, la página puede mostrar varias pestañas (tokens de Android, registro con Google, registro manual de Apple y registro automático de dispositivos de Apple).

> Si su entorno Android Enterprise está respaldado por un dominio administrado de Google (Google Workspace), el panel también puede mostrar una pestaña de **Autenticación mediante la inscripción de Google**. Para obtener detalles sobre cómo habilitarla y usarla, consulte **Autenticación mediante la inscripción de Google**.

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 con los detalles del token.

Columnas

- **Id**: identificador interno de token.
- **Estado**: **Disponible**, **Utilizado** (token de un solo uso ya utilizado) o **Vencido**.
- **Vencimiento**: fecha y hora de vencimiento, o **Nunca**.
- **Política**: la política asignada al token (la información sobre herramientas también muestra el ID de la política).
- **Uso personal**: Permitido / No permitido / Dispositivo dedicado.
- **Usos permitidos**: Uso múltiple o solo una vez.

- **Usuario**: usuario opcional, preasignado a los dispositivos inscritos con el token.

Acciones

- Cada fila tiene una acción de eliminación (**Eliminar token de inscripción**). La eliminación está deshabilitada cuando la licencia ha expirado.
- La tabla admite la selección de múltiples filas: puede activar el modo de selección, seleccionar varios tokens y eliminarlos con **Eliminar tokens seleccionados**.
- Utilice la acción "Actualizar" para volver a cargar la lista. La tabla se divide en páginas (10/25/50 elementos por página).

Cree un nuevo token de inscripción

En la pestaña de tokens de Android, haga clic en **Nuevo token de inscripción**. para abrir la página de creación del token. Si su licencia ha expirado, el botón de creación está deshabilitado.

Opciones de token

1. Política

Requerido.. La política se aplica automáticamente a todos los dispositivos inscritos utilizando este token. Seleccione una de sus **políticas de Android**. Si aún no tiene ninguna política, cree una primero.

2. Usuario

Opcional. Si se establece, 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 de propiedad de la empresa para uso laboral y personal.
- **No permitidos**: adecuados para dispositivos propiedad de la empresa, destinados únicamente al uso laboral (administración completa).
- **Dispositivo dedicado**: adecuado para dispositivos tipo quiosco o dispositivos dedicados (el dispositivo no está asociado a un usuario específico).

4. Usos permitidos

Selecciona si el token puede usarse varias veces (**Varias veces**) o solo una vez (**Solo una vez**).

5. Vencimiento

Seleccione la unidad de vencimiento (**Minutos**, **Horas**, **Días**, o **Nunca**). Cuando no se establece en "Nunca", ingrese el valor de vencimiento. El rango permitido depende de la unidad seleccionada y puede llegar hasta 10,000 días.

Opciones de aprovisionamiento (solo código QR)

Estas opciones adicionales están integradas en el código QR y se aplican durante el aprovisionamiento de dispositivos gestionados, inscritos mediante la lectura del 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

Utiliza esto para permitir que un dispositivo se conecte automáticamente a Wi-Fi durante la configuración, para que pueda descargar e inicializar la aplicación de gestión. Los campos disponibles incluyen **SSID**, **SSID oculto**, **Seguridad**, y (cuando sea necesario) **Contraseña**.

También puede configurar un proxy HTTP (**Proxy**) y, según el modo, establecer **Servidor**/**Puerto**, **URI PAC** y **Servidor de bypass del proxy**.

Otras opciones

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

Detalles del token de inscripción

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

- **Estado**, **Vencimiento**, **Uso**, **Uso personal**, y **Usos permitidos**.
- **Token**: el valor 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 utiliza para inscribir dispositivos administrados.

> Para obtener instrucciones detalladas sobre el proceso de configuración, siga las guías de incorporación para Android: **Dispositivos propiedad del usuario**, **Dispositivos**

propiedad de la empresa para uso laboral y personal, **Dispositivos propiedad de la empresa para uso laboral exclusivo**, y **Configuración automática**.

Dispositivos propiedad del usuario

Los dispositivos propiedad de los empleados pueden configurarse con un **perfil de trabajo**. Un perfil de trabajo proporciona un espacio independiente para aplicaciones y datos laborales, separado de las aplicaciones y datos personales. La mayoría de las políticas de administración de aplicaciones, datos y otros aspectos se aplican únicamente al perfil de trabajo, mientras que las aplicaciones y los datos personales de los empleados permanecen privados.
Para configurar un perfil de trabajo en un dispositivo de uso personal, utilice uno de los siguientes métodos de configuración (asegúrese de que el token de inscripción tenga ***Uso personal*** establecido en **Permitido**):

Enlace del token de registro

Versión de Android
6.0+

Puede proporcionar la URL de registro a los usuarios finales. Cuando un usuario final abra el enlace desde su dispositivo, se le guiará a través de 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:

1. Ve a *Configuración > Google > Configuración y restauración*.
2. Toque "*Configurar su perfil de trabajo*".

Estos pasos inician un asistente de configuración que descarga *Política de Dispositivo Android* en el dispositivo. A continuación, se le pedirá al usuario que escanee un código QR o que introduzca manualmente un token de registro 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, el usuario puede descargar la aplicación <x id="START_EMPHASISED_TEXT" ctype="x-em" equiv-text=""/>Política del Dispositivo

Android<x id="CLOSE_EMPHASISED_TEXT" ctype="x-em" equiv-text=""/> desde Google Play Store. Una vez instalada la aplicación, se le pedirá al usuario que escanee un código QR o que introduzca manualmente un token de registro para completar la configuración del perfil de trabajo.

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 trabajo como para uso personal. En los dispositivos propiedad de la empresa con perfiles de trabajo:

- La mayoría de las políticas de aplicaciones, datos y otras configuraciones se aplican únicamente al perfil de trabajo.
- Los perfiles personales de los empleados permanecen privados. Sin embargo, las empresas pueden aplicar ciertas políticas a nivel del dispositivo y políticas de uso personal.
- Las empresas pueden utilizar el *ámbito de bloqueo* para aplicar acciones de cumplimiento a todo el dispositivo o solo a su perfil de trabajo.
- La eliminación 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, utilice uno de los siguientes métodos de aprovisionamiento (asegúrese de que el token de inscripción tenga el **uso personal** configurado como **Permitido**):

Método de 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 lugar. Esto activa el dispositivo para que solicite al usuario que escanee un código QR.

Dispositivos propiedad de la empresa, solo para uso laboral

La gestión completa del dispositivo es adecuada para dispositivos propiedad de la empresa destinados exclusivamente para uso laboral. Las empresas pueden gestionar todas las aplicaciones del dispositivo e implementar todas las políticas y comandos de la API de administración de Android.
También es posible restringir un dispositivo (a través de la configuración) para que solo ejecute una aplicación o un conjunto limitado de aplicaciones, con el fin de cumplir un propósito o caso de uso específico. Este subconjunto de dispositivos completamente administrados se denomina **dispositivos dedicados**.
Para configurar la administración completa en un dispositivo propiedad de la empresa, utilice uno de los siguientes métodos de configuración (asegúrese de que el token de inscripción tenga **Uso personal** establecido en **No permitido**):

Método de 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 lugar. Esto activa el dispositivo para que solicite al usuario que escanee un código QR.

Método de identificación del perfil de configuración (DPC)

Versión de Android
5.1+

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

1. Siga el asistente de configuración en un dispositivo nuevo o restablecido de fábrica.
2. Ingrese los detalles de acceso de Wi-Fi para conectar el dispositivo a Internet.
3. Cuando se le solicite iniciar sesión, ingrese **afw#setup**, lo que descargará la política del dispositivo Android.
4. Escanee un código QR o introduzca manualmente un token de inscripción para configurar el dispositivo.

Configuración automática

Los administradores de TI pueden aprovisionar dispositivos propiedad de la empresa utilizando el método de inscripción sin intervención, que se describe en Inscripción sin intervención para administradores de TI. Cuando un dispositivo se enciende por primera vez, se configura automáticamente con los ajustes definidos por el administrador de TI.

Los administradores de TI pueden preconfigurar los dispositivos adquiridos de proveedores autorizados y gestionarlos a través del panel de control de Cerberus Enterprise. Para vincular su cuenta de Zero-touch, vaya a la sección **Zero-touch** en el panel de control y siga las instrucciones.

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

Autentícate utilizando la inscripción con Google

Autentícate utilizando la inscripción con Google (también conocida como **Autenticación de Google para la inscripción**), lo que permite a los usuarios autenticarse con su cuenta de Google Workspace durante la inscripción del dispositivo Android.

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

¿Dónde encontrarlo?

En el panel, abra **Tokens de inscripción** y seleccione la pestaña **Autenticar con la inscripción de Google**. La pestaña se muestra solo cuando la administración de Android está configurada y la integración de Google Workspace está disponible para su empresa.

Habilite (o deshabilite) la autenticación con Google

La autenticación con Google está habilitada desde la **consola de administración de Google**. Después de cambiar la configuración, regrese a Cerberus Enterprise y utilice **Actualizar estado** para recargar la configuración actual.

1. Inicie sesión en su **consola de administración de Google** con una cuenta de administrador.
2. Abra **Dispositivos**.
3. Vaya a **Dispositivos móviles y terminales** → **Configuración** → **Integraciones de terceros**.
4. Encuentre la **integración de Android EMM** para Cerberus Enterprise y ábrala.
5. Haz clic en **Administrar proveedores EMM**.
6. Active **Autenticar con Google** para habilitar o deshabilitar la autenticación con Google para el registro.
7. Haz clic en **Guardar**.
8. Vuelva al panel de control de Cerberus Enterprise y haga clic en **Actualizar estado** en la pestaña **Autenticación con Google**.

Token de registro para la autenticación con Google

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

Opciones principales

- **Permitir uso personal**: controla si el token puede registrar dispositivos para uso laboral y personal (escenarios de perfil de trabajo) o solo para uso laboral (escenarios de gestión completa/dedicado).
- **Política predeterminada alternativa**: la política que se aplica cuando el usuario que se está inscribiendo no tiene asignada una política predeterminada específica de Google Authentication.

Interacción con la política

La configuración de la política **Autenticación en la 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 la Consola de administración de Google **Autenticar con Google** y el tipo de token de inscripción aún pueden requerir autenticación.

Para dispositivos ya registrados, esta política solo se aplica si el dispositivo está gestionado mediante una cuenta de Google Play corporativa (es decir, registrado sin **autenticación mediante Google**).

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

Registrar un dispositivo

Durante el registro, se solicita al usuario que se autentique con su cuenta de Google Workspace. Después de un registro exitoso, el dispositivo se asocia con el usuario autenticado.

Perfil de trabajo (dispositivos de uso personal)

- Comparte la **URL de inscripción** con el usuario. Cuando el usuario la abre en su dispositivo Android, se le guiará a través de la configuración del perfil de trabajo y la autenticación de Google.
- Alternativamente, el usuario puede iniciar desde la configuración de Android y seleccionar el flujo de configuración del perfil de trabajo, luego escanear el código QR o ingresar el token de inscripción cuando se le solicite.

Dispositivos propiedad de la empresa

- **Método de código QR**: en un dispositivo nuevo o restablecido de fábrica, toca la pantalla varias veces en el mismo lugar hasta que aparezca la solicitud de código QR, luego escanea el código QR que se muestra en el panel.
- **Método de identificación del perfil de dispositivo (DPC)** (cuando el escaneo de códigos QR no está disponible): siga el asistente de configuración, conéctese a Wi-Fi y, cuando se le solicite, ingrese **afw#setup** y continúe escaneando el código QR o ingresando el token de inscripción. Cuando se le solicite, autentíquese con la cuenta de Google Workspace.

Para obtener información sobre los procedimientos generales de configuración de dispositivos Android (perfil de trabajo frente a dispositivos totalmente administrados), consulte las páginas de registro estándar de Android en este manual.