Descripción de los ID de Apple Gestionados para empresas

Cuando usas productos Apple en tu organización, es importante saber cómo funcionan los ID de Apple Gestionados con los servicios que puedan necesitar los empleados. Los ID de Apple Gestionados son cuentas diseñadas específicamente para las empresas que permiten el acceso a los principales servicios de Apple.

Las organizaciones pueden usar Apple Business Manager para crear automáticamente ID de Apple Gestionados. De este modo, los empleados pueden colaborar con apps y servicios de Apple, y también acceder a los datos de trabajo en las apps gestionadas que usan iCloud Drive. Mediante la autenticación federada, estas cuentas usan las mismas credenciales que la infraestructura existente que posee y gestiona cada organización.

¿Qué son los ID de Apple Gestionados?

Al igual que cualquier ID de Apple, los ID de Apple Gestionados se usan para personalizar un dispositivo. También se utilizan para acceder a apps y servicios de Apple, y para que los equipos de TI puedan acceder a Apple Business Manager. A diferencia de los ID de Apple, la propiedad y gestión de los ID de Apple Gestionados corresponde a la propia empresa, incluido el restablecimiento de contraseña y la administración basada en funciones.

Apple Business Manager permite crear fácilmente un ID de Apple Gestionado único para cada empleado de una organización. Gracias a la integración con Microsoft Azure Active Directory, las empresas pueden proporcionar ID de Apple Gestionados a los empleados usando las credenciales corporativas que ya tienen.

Los ID de Apple Gestionados se pueden compaginar con un ID de Apple personal en los dispositivos propiedad de los empleados cuando las organizaciones usan la inscripción de usuarios en iOS, iPadOS y macOS Catalina. Opcionalmente, los ID de Apple Gestionados se pueden usar en cualquier dispositivo como el ID de Apple principal (y único). Los ID de Apple Gestionados también tienen acceso a iCloud en la web después de iniciar sesión por primera vez en un dispositivo Apple.

No hay ningún requisito técnico para implantar dispositivos con un ID de Apple. Los dispositivos Apple se pueden gestionar y las apps se pueden distribuir a los dispositivos sin usar un ID de Apple. Consulta los servicios que ofrecerá tu organización y determina la mejor forma de hacer la transición a los ID de Apple Gestionados. Como los ID de Apple Gestionados solo están pensados para el uso empresarial, algunas prestaciones están desactivadas para proteger a la organización.

Prestaciones para organizaciones

- **Acceso a los servicios de Apple.** Los empleados pueden usar los servicios de Apple, como iCloud y la colaboración con iWork y Notas. El correo electrónico está desactivado, y el uso de FaceTime o iMessage solo está disponible cuando un ID de Apple Gestionado es el único ID de Apple de un dispositivo.
- **Consulta de cuentas de usuario.** Permite que los empleados busquen información de contacto de otros usuarios en tu organización de Apple Business Manager. De este modo, les resultará más sencillo colaborar entre ellos en las apps.
- **Creación optimizada de cuentas.** Con Apple Business Manager, las cuentas se crean automáticamente la primera vez que los empleados inician sesión en un dispositivo Apple.
- **Autenticación federada.** Los administradores pueden conectar Apple Business Manager con Microsoft Azure Active Directory para que sus empleados tengan sus cuentas preparadas automáticamente usando las credenciales de empresa que ya tienen.
- **Funciones y privilegios.** Los administradores pueden crear y asignar funciones y privilegios para que los equipos de TI utilicen diferentes prestaciones en Apple Business Manager.
- **Privacidad y seguridad integradas.** Los ID de Apple Gestionados emplean las mismas protecciones de cifrado de datos que los ID de Apple estándar, y no se les puede aplicar publicidad segmentada en la plataforma de anuncios de Apple. El comercio está desactivado, así como el acceso a servicios como Apple Pay y Wallet. La prestación Buscar está desactivada porque las organizaciones pueden usar el Modo Perdido con la gestión de dispositivos móviles (Mobile Device Management, MDM).

Autenticación federada

Con la autenticación federada, puedes conectar Apple Business Manager con Microsoft Azure Active Directory (Azure AD) para que los empleados puedan usar sus nombres de usuario y contraseñas existentes como ID de Apple Gestionados.

Microsoft Azure AD es el proveedor de identidades e incluye los nombres de usuario y contraseñas de las cuentas que quieras usar con Apple Business Manager.

Al integrarse con Microsoft Azure AD, los ID de Apple Gestionados siguen exactamente las mismas políticas de contraseña, ya que se federan con las credenciales existentes.

Los ID de Apple Gestionados se crean automáticamente cuando los usuarios inician sesión en su dispositivo Apple, por lo que los administradores de TI no tendrán que dedicarse a crearlos de antemano.

A partir de ahí, los empleados pueden utilizar sus credenciales de Azure AD existentes para acceder a servicios de Apple, como iCloud Drive, Notas, Recordatorios y las prestaciones de colaboración.

Como la organización ya gestiona la identidad, todas las políticas y restablecimientos de contraseñas son manejados por la organización o el usuario en Microsoft Azure AD.

Requisitos para la autenticación federada

- **Microsoft Azure Active Directory.** Da los primeros pasos con la autenticación federada si ya estás usando esto.
- **Versión local de Active Directory.** Debes realizar algunos pasos adicionales de configuración para la sincronización con Azure AD. Microsoft ofrece documentación y una herramienta de sincronización en el enlace mostrado abajo.

Cómo configurar la autenticación federada

1. **Verifica un dominio con Apple**. Inicia sesión en Apple Business Manager como Administrador o Gestor de Personas y añade el/los dominio/s que quieres federar.
2. **Conecta con Microsoft Azure Active Directory y concede acceso para Apple Business Manager.** Usa una cuenta de Administrador Global o Administrador de Aplicaciones para iniciar sesión en Azure AD y acepta permisos para que Apple Business Manager pueda leer perfiles de usuario.
3. **Comprueba la propiedad del dominio con Microsoft Azure Active Directory.** Una vez establecida la confianza, continúa el proceso de comprobación de dominio/s. Desde Apple Business Manager, inicia sesión en Microsoft Azure AD con una cuenta que termine con el dominio que quieres federar. Este paso comprueba la configuración del dominio y constata la propiedad.
4. **Comprueba si hay conflictos entre dominios.** Apple Business Manager verificará si hay posibles conflictos con cualquier ID de Apple existente dentro de tu/s dominio/s. Pueden ser ID de Apple personales o ID de Apple Gestionados configurados por otra organización que usa el mismo dominio.
5. **Inicia la resolución de conflictos entre dominios**. Si Apple Business Manager detecta un ID de Apple personal en el/los dominio/s que quieres federar, estos usuarios serán notificados y tendrán que cambiar las direcciones de correo electrónico de sus ID de Apple. Las compras y los datos seguirán estando asociados al ID de Apple personal de cada usuario.
6. **Migra las cuentas preexistentes.** Si ya tienes ID de Apple Gestionados, puedes realizar su migración a la autenticación federada. Para ello, modifica sus detalles de modo que coincidan con el dominio federado y nombre de usuario adecuados.

Recursos

- Guía de primeros pasos — Apple Business Manager
- Guía del usuario de Apple Business Manager
- Más información sobre cómo crear ID de Apple Gestionados en Apple Business Manager
- Introducción a la autenticación vinculada en Apple Business Manager
- Más información sobre los conflictos con ID de Apple existentes
- Más información sobre la integración de dominios locales de Active Directory con Azure Active Directory