Inscripción de Apple mediante cuenta

Con la inscripción mediante cuenta, los usuarios inscriben su iPhone, iPad o Mac iniciando sesión con su cuenta de trabajo (una **Managed Apple Account**, por ejemplo *name@company.com*) en los ajustes del dispositivo. No hay que descargar ningún perfil ni usar ningún código QR: Cerberus Enterprise encuentra al usuario, aplica la política y establece la propiedad por sí mismo.

Dos modos

- **User Enrollment** (dispositivos personales): solo se gestionan las apps, cuentas y datos de trabajo, en un área separada del dispositivo. Cerberus no puede ver los datos personales, borrar el dispositivo, localizarlo ni leer su número de serie. El dispositivo se establece como de propiedad personal. Requiere iOS y iPadOS 15 o macOS 14 o posterior.
- **Device Enrollment** (dispositivos de empresa que no están en Apple Business): se gestiona todo el dispositivo, como con una inscripción manual. Un Mac inscrito de esta forma está supervisado; un iPhone o iPad no lo está. El dispositivo se establece como propiedad de la empresa. Requiere iOS y iPadOS 17.1 o macOS 14.1 o posterior.

> Eliges el modo para iPhone y iPad y, por separado, para Mac: por ejemplo, User Enrollment para iPhone personales y Device Enrollment para Mac. Puedes cambiar la propiedad de un dispositivo más adelante en la página del dispositivo.

> La inscripción mediante cuenta está disponible cuando Apple Management (APNs) está configurado. Si aún no has completado la configuración de APNs, consulta **Configuración de Apple Management (APNs)**.

Configurar Apple Business

Los usuarios inician sesión con Managed Apple Accounts, que se crean en Apple Business. Antes de empezar:

1. **Verifica tu dominio** (por ejemplo, *company.com*) en Apple Business, en los dominios de tu organización.
2. **Crea las Managed Apple Accounts** de tus usuarios, o conecta Apple Business a Google Workspace o Microsoft Entra ID: entonces la cuenta de cada usuario es su dirección de correo de trabajo e inicia sesión con su contraseña.
3. Para User Enrollment, comprueba en los ajustes de gestión de acceso que las Managed Apple Accounts pueden iniciar sesión en **dispositivos personales**: cuando solo pueden iniciar sesión en dispositivos supervisados, User Enrollment falla.
4. Solo para la opción **Apple Business** que aparece más abajo: abre **Devices** → **Management Services** → **Default Device Assignment** (Edit) y elige el servicio de gestión de dispositivos Cerberus Enterprise para iPhone, iPad y Mac.

> Mantén el servicio de gestión de dispositivos Cerberus Enterprise y su token en Apple Business mientras los dispositivos estén inscritos con Managed Apple Accounts: eliminarlos puede hacer que las cuentas dejen de funcionar en los dispositivos.

Configurar Cerberus Enterprise

Abre la sección **Inscripción** del panel de control y selecciona la pestaña **Inicio de sesión con cuenta de Apple**. Una lista de comprobación en la parte superior muestra lo que aún falta. Solo los administradores pueden cambiar los ajustes.

- **Permitir la inscripción iniciando sesión con una cuenta de trabajo**: activa o desactiva la inscripción mediante cuenta para toda la organización.
- **Dominios**: los dominios de las cuentas de tus usuarios (por ejemplo, *company.com*), hasta 20. Solo pueden inscribirse las cuentas de estos dominios, y solo después de verificar el dominio (consulta más abajo).
- **iPhone y iPad** y **Mac**: Desactivado, User Enrollment o Device Enrollment para cada familia de dispositivos.
- **Política** de cada modo: se aplica a los dispositivos en cuanto se inscriben. Sin una política, los dispositivos se inscriben sin ella. Una política modificada se aplica a las siguientes inscripciones.
- **Usuarios**: *Solo usuarios existentes* (la dirección de correo de un usuario en Cerberus Enterprise debe coincidir con la cuenta introducida en el dispositivo) o *Crear un usuario para las cuentas de los dominios que no tengan uno*.

> La cuenta introducida en el dispositivo se compara con el campo **Managed Apple Account** de los usuarios y, después, con su dirección de correo. El código siempre se envía a la dirección de correo del usuario. Una Managed Apple Account asignada a un usuario puede inscribirse aunque su dominio no esté verificado en Cerberus, por ejemplo una cuenta del dominio reservado *org.appleid.com* de Apple Business. Con la detección de servicios de

Apple Business, los usuarios siempre introducen su Managed Apple Account.

Verificar los dominios

Después de guardar los ajustes, la sección **Verificación de dominio** muestra un registro TXT para cada dominio. Añádelo al DNS del dominio y, a continuación, haz clic en **Verificar**. Los cambios de DNS pueden tardar algún tiempo en ser visibles. Un dominio verificado sigue verificado: puedes eliminar el registro después. Los usuarios de un dominio que no esté verificado no pueden inscribirse.

Detección de servicios: cómo encuentran los dispositivos Cerberus Enterprise

Cuando un usuario inicia sesión, el dispositivo pregunta al dominio de la cuenta (por ejemplo, *https://company.com*) qué servidor lo gestiona. Configura al menos una de estas tres opciones. La sección **Detección de servicios** de la pestaña muestra la URL de detección de tu organización y el texto exacto que hay que copiar para cada opción.

Opción 1: Apple Business (recomendada)

Haz clic en **Registrar en Apple Business**: Cerberus Enterprise almacena su URL de detección en tu organización de Apple Business y no hay que publicar nada en tus dominios. **Comprobar en Apple Business** muestra la URL que tiene ahora Apple Business, y **Eliminar de Apple Business** la elimina.

- Requiere iOS y iPadOS 18.2 o macOS 15.2 o posterior. Los dispositivos más antiguos necesitan la opción 2 o 3.
- Requiere Apple Business conectado en Cerberus Enterprise (token de servicio de Automated Device Enrollment) y la asignación predeterminada de dispositivos descrita anteriormente.
- El dispositivo pregunta a Apple Business solo cuando tu dominio no responde: la dirección *https://company.com/.well-known/com.apple.remotemanagement* no debe existir (un error como "not found"). Si tu sitio web responde con una página web, los dispositivos se detienen ahí. Usa **Comprobar configuración** para ver qué responde.

> Apple Business guarda una sola URL de detección por organización: al registrarla, todas las Managed Apple Accounts de la organización se dirigen a esta organización de Cerberus Enterprise. No la registres desde dos organizaciones de Cerberus Enterprise que usen la misma organización de Apple Business.

Opción 2: redirección desde tu sitio web

En el servidor web de cada dominio, redirige */.well-known/com.apple.remotemanagement* a la URL de detección de tu organización, **conservando la cadena de consulta** (que contiene la cuenta introducida por el usuario). Esto funciona con todas las versiones del sistema operativo compatibles con la inscripción mediante cuenta, y el modo puede ser distinto para iPhone y Mac. Copia el texto para Apache o nginx de la pestaña; tiene este aspecto, con la clave de tu organización:

Apache (.htaccess o host virtual):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

En otros servidores web o servicios (IIS, Cloudflare, paneles de control de alojamiento), crea una regla de redirección (302) desde la misma ruta a la URL de detección con la opción que conserva o reenvía la cadena de consulta.

Opción 3: archivo estático en tu sitio web

Si no puedes añadir una redirección, publica un archivo en *https://company.com/.well-known/com.apple.remotemanagement* (sin extensión de archivo), servido con *Content-Type: application/json*. Copia su contenido de la pestaña. Un archivo estático no puede elegir el modo por dispositivo: usa el mismo modo para iPhone, iPad y Mac. Para User Enrollment, tiene este aspecto:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/byod"}]}
```

y para Device Enrollment:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/adde"}]}
```

> El modo del archivo también debe ser el modo establecido en la pestaña para la familia de dispositivos; de lo contrario, se rechaza la inscripción.

Comprobar configuración

En **Comprobar configuración**, elige un dominio y un dispositivo (iPhone o Mac) y haz clic en **Comprobar**: Cerberus Enterprise pregunta al dominio lo mismo que preguntaría un dispositivo y muestra la respuesta, cada redirección y un veredicto. Que el dominio apunte a Cerberus Enterprise significa que las opciones 2 o 3 funcionan; una respuesta de error (como "not found") es correcta para la opción 1; una página web o un archivo que apunte a otro sitio detiene los dispositivos. La comprobación también avisa cuando una redirección pierde la cadena de consulta o el archivo no se sirve como *application/json*.

Clave de inscripción

Las URL de detección e inscripción contienen una clave de tu organización. Si las URL se publicaron por error, haz clic en **Regenerar clave**: las URL antiguas dejan de funcionar de inmediato, así que actualiza las redirecciones y los archivos estáticos de tus sitios web. Cerberus Enterprise registra la nueva URL en Apple Business por sí mismo cuando se usa la opción 1.

Cómo se inscriben los usuarios

1. iPhone y iPad: abre *Configuración → General → VPN y gestión de dispositivos → Iniciar sesión en la cuenta de trabajo o centro educativo*. Mac: *Configuración del Sistema → General → Gestión de dispositivos → Iniciar sesión* (en macOS 14: *Privacidad y seguridad → Perfiles → Iniciar sesión*).
2. Introduce la Managed Apple Account o la dirección de correo de trabajo del usuario en Cerberus (por ejemplo, *name@company.com*). Cuando la Managed Apple Account del usuario es distinta de la introducida, el dispositivo pide entonces iniciar sesión con esa cuenta.
3. Se abre una página de Cerberus Enterprise: toca *Enviar el código* e introduce el código de 6 dígitos recibido por correo electrónico. El código caduca a los 10 minutos; tras 5 códigos incorrectos, el usuario debe cerrar la página e iniciar sesión de nuevo.
4. Inicia sesión con la contraseña de la Managed Apple Account (o con la página de inicio de sesión de la empresa cuando Apple Business está conectado a Google Workspace o

Microsoft Entra ID) y, a continuación, permite la gestión del dispositivo.

> Las cuentas que no pueden inscribirse (dominio no verificado, ningún usuario coincidente cuando los usuarios no se crean automáticamente, varios usuarios con la misma dirección de correo) ven "Esta cuenta no está configurada para la inscripción. Contacta con tu administrador de TI." Los eventos están en los registros del sistema del panel de control.

Después de la inscripción

- La página del dispositivo muestra la **Managed Apple Account** usada para inscribirse y el tipo de inscripción (User Enrollment o Account-driven Device Enrollment). En la lista de dispositivos, los dispositivos con User Enrollment muestran "User Enrollment".
- En los dispositivos con User Enrollment, los comandos y ajustes de política que Apple no permite (borrar, ubicación, modo perdido, actualizaciones del sistema operativo, muchas restricciones) no se ofrecen ni se envían. Las apps del App Store de la política usan una licencia de usuario en lugar de una licencia de dispositivo (consulta **Apps en dispositivos personales** más abajo).
- En los dispositivos con User Enrollment, los clips web aparecen en la pantalla de inicio pero no se enumeran en *Ajustes → General → VPN y gestión de dispositivos*.
- El certificado MDM de estos dispositivos no se renueva automáticamente y **Return to Service** no está disponible: antes de que caduque el certificado MDM (un año después de la inscripción; consulta la página del dispositivo), pide al usuario que vuelva a inscribir el dispositivo.
- Para dejar la gestión, el usuario cierra la sesión de la cuenta de trabajo en el mismo lugar de los ajustes, o tú anulas la inscripción del dispositivo desde Cerberus Enterprise. Con User Enrollment solo se eliminan las apps, cuentas y datos de trabajo; los datos personales se conservan. Un dispositivo que se vuelve a inscribir aparece como un dispositivo nuevo.

> Justo después de la inscripción, algunos perfiles de la política (certificados, redes Wi-Fi, clips web) pueden notificarse como fallidos con un error desconocido, y el dispositivo puede mostrarse como **No cumple** durante un tiempo. El dispositivo lo vuelve a intentar por sí mismo y se instalan al cabo de un rato, sin necesidad de hacer nada. No vuelvas a guardar la política ni inscribas de nuevo el dispositivo por este motivo.

Apps en dispositivos personales

Los iPhone y iPad inscritos con User Enrollment no tienen número de serie, por lo que Apps and Books no puede darles una licencia de dispositivo. En su lugar, Cerberus Enterprise da a las apps

del App Store de su política una **licencia de usuario**: la licencia va a la Managed Apple Account que ha iniciado sesión en el dispositivo. Nada cambia en la política: la misma política sirve para dispositivos de empresa y personales, y Cerberus elige el tipo de licencia para cada dispositivo.

- **Automático**: en la primera inscripción, Cerberus registra la Managed Apple Account en Apps and Books y luego pide a Apple una licencia de cada app del App Store de la política. Las apps gratuitas también necesitan una licencia; Apple les da licencias ilimitadas. Una app de pago usa una licencia por Managed Apple Account, compartida por todos los dispositivos personales de esa cuenta.
- **Misma organización**: las Managed Apple Accounts y el token de Apps and Books de Cerberus Enterprise deben pertenecer a la misma organización de Apple Business, y las apps deben estar en la biblioteca de la ubicación del token.
- **Primero la licencia**: una app se envía al dispositivo solo después de que Apple confirme su licencia, normalmente en unos minutos. Hasta entonces, el panel **Aplicaciones** del dispositivo la muestra como **Esperando una licencia de usuario**, con el motivo.
- **Indicación de instalación**: los dispositivos personales nunca están supervisados, así que iOS pregunta al usuario antes de instalar cada app, incluida la app **Cerberus Enterprise**, que Cerberus también instala en estos dispositivos (**Instalar** o **Cancelar**); no hace falta iniciar sesión en ninguna Apple Account. Si el usuario cancela, la app muestra **Esperando la aprobación del usuario para la instalación**: usa **Solicitar de nuevo** en la página del dispositivo para volver a mostrar la indicación. Las apps instaladas como **Obligatoria** no las puede eliminar el usuario.
- **Apps instaladas antes de la inscripción**: Apple no permite que la organización se haga cargo de una app que el usuario instaló personalmente en un dispositivo inscrito con User Enrollment. Pide al usuario que elimine su propia copia antes de la inscripción, o elimínala y luego usa **Solicitar de nuevo** en la página del dispositivo: la organización instala entonces la copia gestionada.
- **Dejar la gestión**: cuando se anula la inscripción del dispositivo, iOS elimina las apps gestionadas y sus datos. Una licencia se libera cuando ya no la necesita ningún otro dispositivo inscrito de la misma Managed Apple Account, por ejemplo cuando la app sale de la política o se anula la inscripción del último dispositivo; las licencias que ya no necesita nadie se liberan con la comprobación diaria en el plazo de un día.

> Cuando Apple no puede asignar una licencia, por ejemplo porque una app de pago se ha quedado sin licencias, la app muestra **Error de licencia de usuario** con el mensaje de Apple. Añade licencias en Apple Business y luego usa **Solicitar de nuevo** en la página del dispositivo; Cerberus también lo vuelve a intentar por sí mismo en la comprobación diaria. La línea situada encima de la lista de apps muestra la Managed Apple Account y el estado de su usuario de Apps and Books; el mismo estado está en la página del usuario.

> Las licencias de usuario solo se usan en iPhone y iPad: en los Mac registrados con Inscripción de usuario no se instalan las apps del App Store de la política. Los libros y las cuentas de Apple personales no son compatibles.

Revision #7
Created 2026-11-10 15:15:04 UTC by Admin
Updated 2026-11-12 09:54:47 UTC by Admin