AnyDesk Colombia

Guia Completa de Acceso Remoto No Atendido con AnyDesk

TABLA DE CONTENIDO

¿Qué es el Acceso Remoto No Atendido?

Requisitos Previos

Configuración Paso a Paso en Windows y macOS

- Paso 1: Acceder a la configuración de acceso
- Paso 2: Establecer una contraseña
- Paso 3: Verificar la configuración

Configuración en Android

Cómo Conectarse a un Dispositivo con Acceso No Atendido

Funciones Avanzadas de Seguridad

- Guardar credenciales de acceso (Login automático)
- Restablecer tokens guardados
- Autenticación de Dos Factores (2FA)
- Bloquear solicitudes interactivas

Casos de Uso Reales

- 1. Soporte TI empresarial
- 2. Gestión de kioskos y POS
- 3. Trabajo híbrido

Solución de Problemas Comunes

- No puedo conectarme tras un reinicio
- La conexión se rechaza aunque la contraseña es correcta
- Android pide confirmación de grabación

Preguntas Frecuentes

- ¿Es necesario instalar AnyDesk para usar el acceso no atendido?
- ¿Pueden robar mi contraseña si acceden a mi AnyDesk?
- ¿Es seguro el acceso no atendido?
- ¿Funciona el acceso no atendido en Mac?

Conclusión

Articulo elaborado por el equipo de investigaciones de escritorioremoto.co.

Guía Completa de Acceso Remoto No Atendido con AnyDesk

El acceso remoto no atendido es una de las funcionalidades más potentes de AnyDesk. Permite controlar y gestionar dispositivos remotos sin que nadie esté físicamente presente para aceptar la conexión. En esta guía completa aprenderás qué es, cómo configurarlo paso a paso, y cómo aprovechar al máximo sus opciones de seguridad.

¿Qué es el Acceso Remoto No Atendido?

El acceso no atendido (Unattended Access) te permite conectarte a un dispositivo remoto en cualquier momento, sin necesidad de que alguien autorice la conexión desde el otro lado. Es la solución ideal para:

- **Trabajo remoto**: Acceder a tu ordenador de la oficina desde casa o cualquier ubicación
- **Mantenimiento de sistemas**: Actualizar software, instalar parches o resolver incidencias sin desplazamientos
- **Gestión de dispositivos no atendidos**: Kioskos, sistemas POS, señalización digital o servidores que funcionan 24/7
- **Operaciones entre zonas horarias**: Conectar con equipos en distintos países sin depender de horarios laborales
- **Conexión a dispositivos bloqueados**: Acceder a un sistema tras un reinicio o cuando nadie ha iniciado sesión

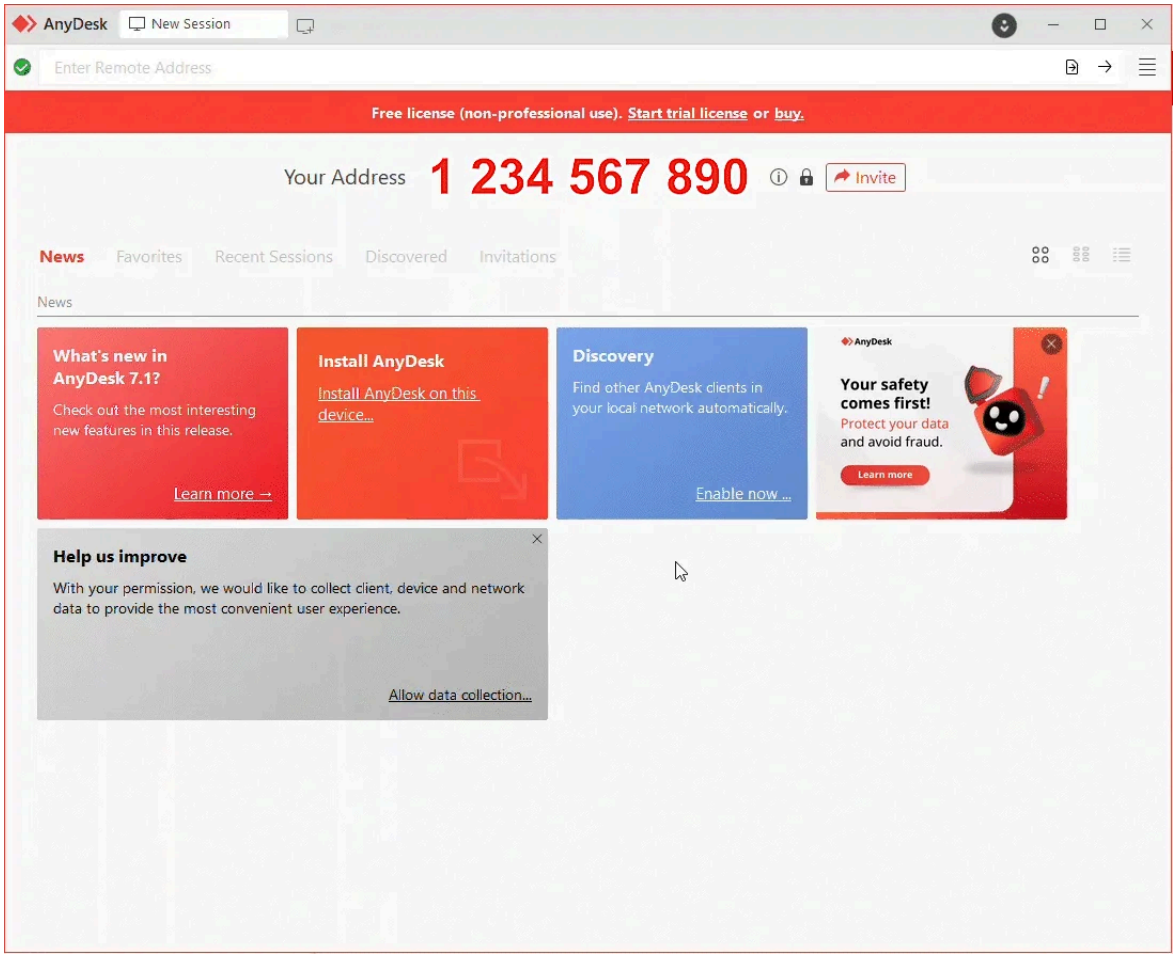


Diagrama conceptual de acceso remoto local vs remoto

A diferencia de una conexión interactiva normal —donde alguien debe aceptar manualmente la solicitud de conexión— el acceso no atendido utiliza una contraseña preconfigurada para autenticar la sesión de forma automática y segura.

Requisitos Previos

Antes de configurar el acceso no atendido, asegúrate de cumplir estos requisitos:

1. **AnyDesk instalado** en el dispositivo remoto (el que vas a controlar). Puedes descargarlo desde anydesk.com/downloads.
2. **AnyDesk instalado o en modo portable** en el dispositivo local (desde donde te conectas).
3. **Conexión a internet** en ambos dispositivos.

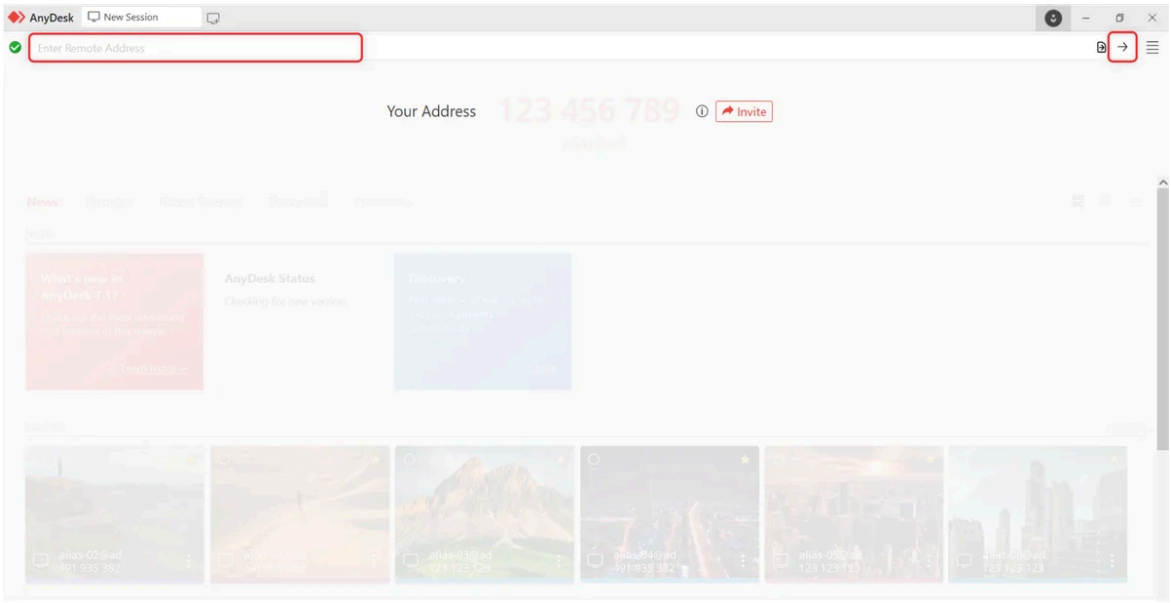
> **Importante:** Aunque AnyDesk puede funcionar como aplicación portable, se recomienda instalarlo en el dispositivo remoto para garantizar que el acceso no atendido siga activo tras un reinicio del sistema.

Configuración Paso a Paso en Windows y macOS

Paso 1: Acceder a la configuración de acceso

En el dispositivo remoto (al que quieres conectarte sin supervisión):

1. Abre la aplicación **AnyDesk**.
2. Ve a **Settings** > **Access** (Configuración > Acceso).
3. Busca la sección **Unattended Access** (Acceso no atendido).



Interfaz principal de AnyDesk con menú de configuración visible

Paso 2: Establecer una contraseña

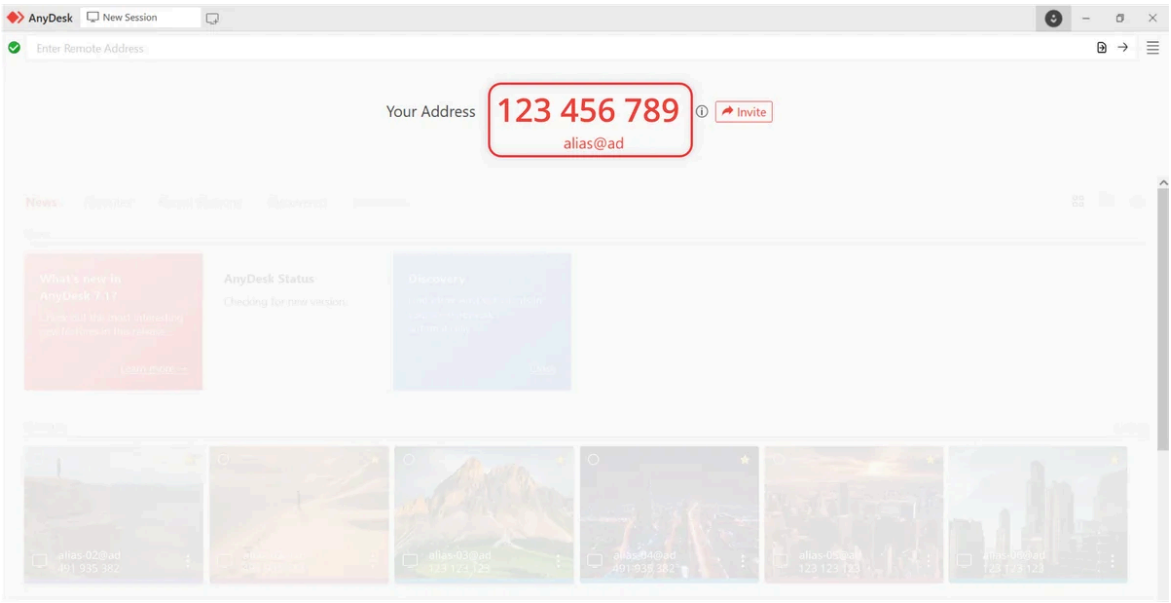
1. En la sección Unattended Access, haz clic en **Set password** (Establecer contraseña).
2. Crea una contraseña segura que cumpla estos criterios:
   - Mínimo **8 caracteres** (se recomiendan 12 o más)
   - Combina **letras, números y símbolos**
   - Evita patrones simples o repetitivos
3. Haz clic en **Apply** para guardar.

> **Seguridad crítica:** Cualquier persona que tenga tu contraseña y tu AnyDesk ID podría acceder a tu dispositivo. Utiliza una contraseña robusta y única. Considera habilitar autenticación de dos factores (2FA) para una protección adicional.

Paso 3: Verificar la configuración

Una vez establecida la contraseña, el acceso no atendido queda activado. Para comprobarlo:

1. Anota el **AnyDesk ID** del dispositivo remoto (visible en la pantalla principal).
2. Desde otro dispositivo, introduce ese ID en el campo de conexión.
3. Cuando se solicite, introduce la contraseña que acabas de configurar.
4. La conexión debería establecerse automáticamente sin necesidad de aprobación manual.

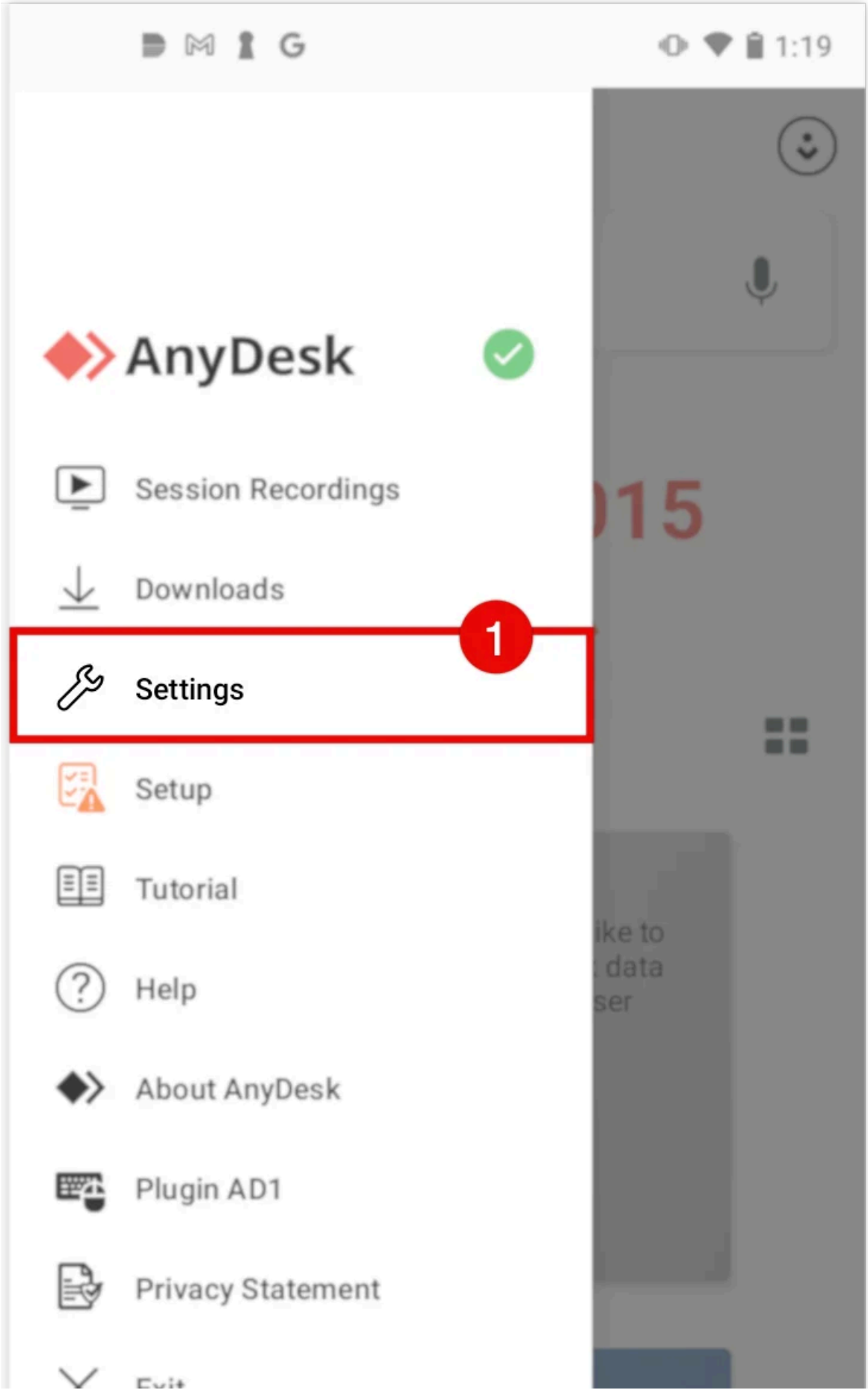


Campo de dirección remota con AnyDesk ID visible

Configuración en Android

El acceso no atendido en dispositivos Android tiene un flujo ligeramente diferente:

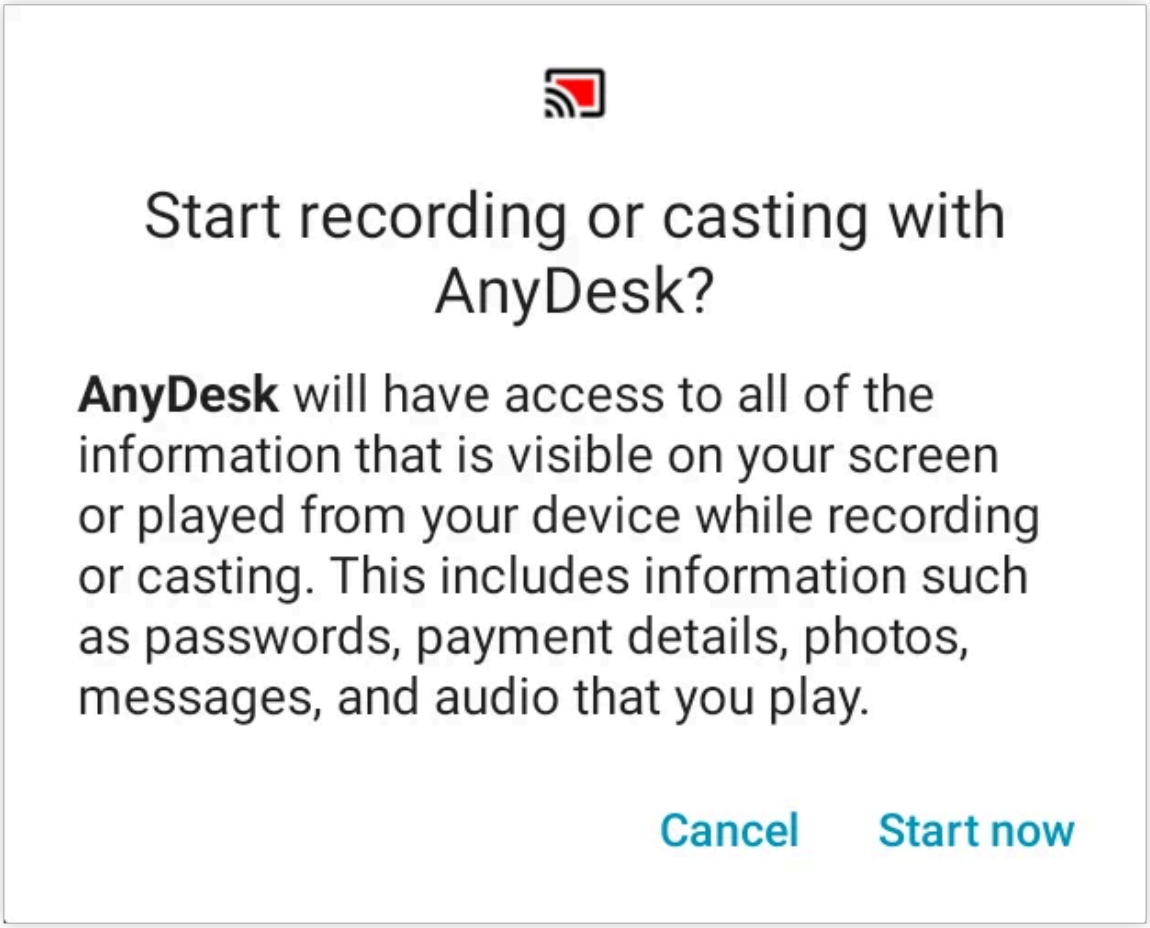
1. Abre AnyDesk en el dispositivo Android remoto.
2. Toca el icono de menú y ve a **Settings** > **Permissions** > **Permission Profiles**.
3. Selecciona **Unattended Access** en la lista.
4. Activa **Enable unattended access** y establece una contraseña segura.


1:19
AnyDesk
Session Recordings
Downloads
1
Settings
Setup
Tutorial
Help
About AnyDesk
Plugin AD1
Privacy Statement



Menú de configuración de AnyDesk en Android con opciones de permisos

> **Limitación en Android 10+:** En versiones de Android 10 y superiores, el sistema puede mostrar un mensaje de confirmación de grabación de pantalla que debe aceptarse manualmente en el dispositivo, incluso con el acceso no atendido configurado. Esto es una restricción del sistema operativo, no de AnyDesk.



Diálogo de permiso de grabación de pantalla en Android

Cómo Conectarse a un Dispositivo con Acceso No Atendido

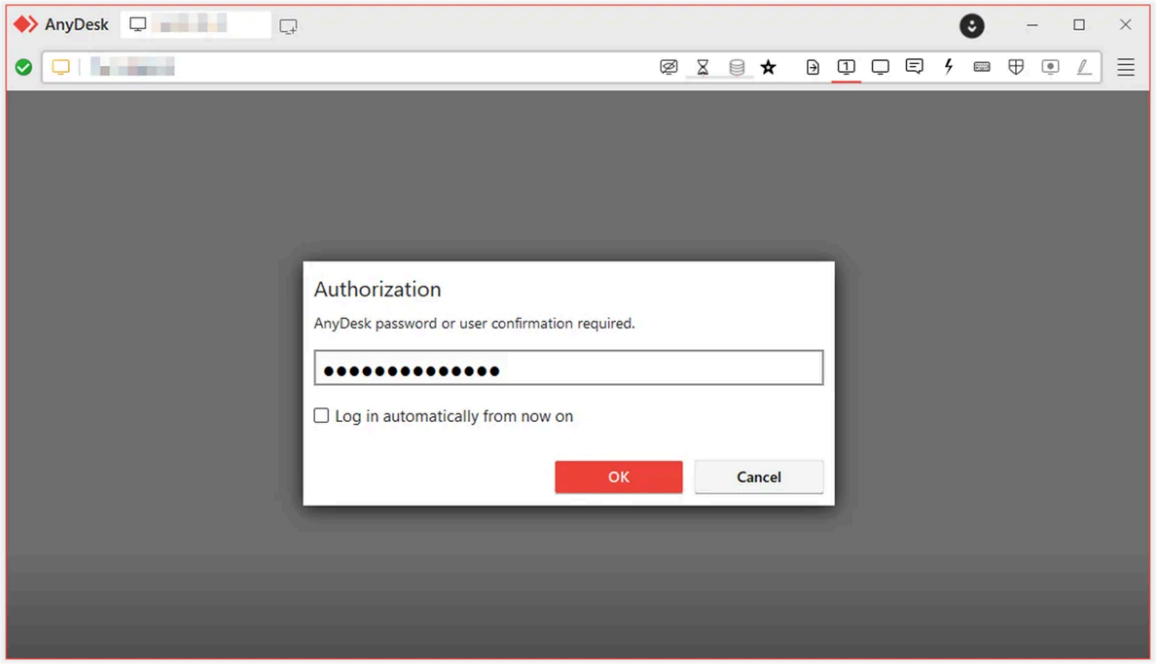
Una vez configurado, conectarse es sencillo:

1. Abre AnyDesk en tu dispositivo local.
2. Introduce el **AnyDesk ID** o **Alias** del dispositivo remoto en el campo “Remote Address”.
3. Pulsa el botón de conexión o presiona **Enter**.



Campo para introducir el AnyDesk ID con botón de conexión

4. Cuando se solicite, introduce la **contraseña de acceso no atendido**.



Diálogo de autenticación solicitando contraseña de AnyDesk

5. La sesión se inicia automáticamente y verás el escritorio remoto.

Si la autenticación es correcta, tendrás control completo del dispositivo remoto: mover el ratón, usar el teclado, transferir archivos y ejecutar aplicaciones, todo como si estuvieras frente a la pantalla.

Funciones Avanzadas de Seguridad

Guardar credenciales de acceso (Login automático)

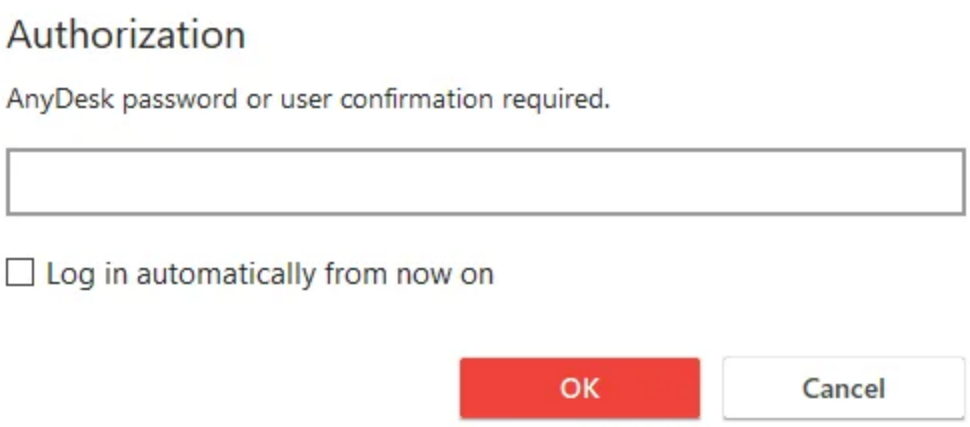
AnyDesk permite guardar la contraseña en el dispositivo local para no tener que introducirla en cada conexión. Para activarlo:

En el dispositivo remoto:

1. Ve a **Settings > Access > Unattended Access**.
2. Marca la casilla **Allow other computers to save login information for this computer**.

En el dispositivo local:

- Al introducir la contraseña correctamente, aparecerá la opción **Log in automatically from now on**.
- Márcala para guardar un token de autenticación.



Diálogo de acceso con opción de inicio de sesión automático

> **Cómo funciona:** AnyDesk no almacena la contraseña. En su lugar, genera un **token único** tras la autenticación correcta. Este token es específico del dispositivo y no puede extraerse en texto plano. Cambiar la contraseña (incluso al mismo valor) invalida todos los tokens emitidos.

Restablecer tokens guardados

Para revocar accesos guardados:

- **Borrar todos los tokens**: Ve a Settings > Access > Unattended Access y selecciona **Clear all tokens**.
- **Cambiar la contraseña**: Automáticamente invalida todos los tokens existentes.
- **Desactivar el guardado**: Desmarca la casilla “Allow other computers to save login information”. Los tokens ya emitidos seguirán siendo válidos hasta que se borren manualmente.

Autenticación de Dos Factores (2FA)

Para máxima seguridad, AnyDesk soporta 2FA en conexiones no atendidas:

1. En el dispositivo remoto, ve a **Settings > Access > Unattended Access**.

2. Marca **Enable Two-Factor Authentication**.
3. Escanea el código QR con una app autenticadora (Google Authenticator, Microsoft Authenticator, FreeOTP).
4. Introduce el código de 6 dígitos para confirmar.

A partir de ese momento, cualquier conexión no atendida requerirá:

- La **contraseña** de acceso no atendido
- Un **código de 6 dígitos** de la app autenticadora

> **Sincronización de tiempo:** Si el botón “Enable authorization” aparece grisado tras introducir el código correcto, verifica que la hora del dispositivo y la app autenticadora estén sincronizadas. Los códigos 2FA dependen del tiempo exacto.

Opciones para omitir 2FA

Los administradores pueden configurar excepciones para 2FA:

- **Login automático**: Si se desmarca “Enable for saved login information”, no se pedirá 2FA cuando se use un token de acceso guardado.
- **Contraseñas temporales**: Si se desmarca “Enable for short-term passwords”, no se pedirá 2FA en reconexiones automáticas tras un reinicio remoto.

Bloquear solicitudes interactivas

Para máxima seguridad, puedes configurar el dispositivo remoto para que **solo** acepte conexiones no atendidas y rechace todas las solicitudes interactivas:

1. Ve a **Settings > Security > Interactive Access**.
2. Selecciona **Never show incoming session requests**.

De este modo, nadie podrá solicitar una conexión interactiva. Solo quien tenga la contraseña de acceso no atendido podrá conectarse.

Casos de Uso Reales

1. Soporte TI empresarial

Un equipo de soporte puede gestionar cientos de equipos de empleados sin necesidad de que estén presentes. Configurando acceso no atendido en todos los equipos corporativos, el equipo TI puede:

- Resolver incidencias fuera del horario laboral
- Instalar actualizaciones de software de forma masiva
- Realizar auditorías de seguridad periódicas

2. Gestión de kioskos y POS

Los quioscos digitales, cajas registradoras y sistemas de señalización suelen estar en ubicaciones remotas y sin personal técnico. Con acceso no atendido:

- Reiniciar sistemas bloqueados de forma remota
- Actualizar contenido digital sin desplazamientos
- Monitorizar el estado del sistema

3. Trabajo híbrido

Acceder al ordenador de la oficina desde casa con la misma experiencia que si estuvieras sentado frente a él. Archivos, aplicaciones y configuraciones permanecen accesibles en todo momento.

Solución de Problemas Comunes

No puedo conectarme tras un reinicio

Causa: AnyDesk no está instalado como servicio o no está configurado para iniciarse con el sistema.

Solución: Instala AnyDesk (no uses la versión portable) y verifica que la opción de inicio automático esté activada en Settings > Privacy > Start AnyDesk with Windows.

La conexión se rechaza aunque la contraseña es correcta

Causa posible: 2FA está activado y no se está introduciendo el código, o el token guardado ha sido invalidado.

Solución: Verifica si 2FA está activo. Si es así, necesitas el código de la app autenticadora. Si el token fue invalidado (por cambio de contraseña), introduce la contraseña manualmente.

Android pide confirmación de grabación

Causa: Restricción de Android 10+ que requiere confirmación manual para grabar la pantalla.

Solución: Alguien debe aceptar el diálogo de grabación en el dispositivo Android. No hay forma de evitarlo por restricciones del sistema operativo.

Preguntas Frecuentes

¿Es necesario instalar AnyDesk para usar el acceso no atendido?

No es estrictamente necesario, pero **sí muy recomendable**. La versión portable funciona, pero tras un reinicio del sistema, AnyDesk no se iniciará automáticamente y el acceso no atendido no estará disponible hasta que alguien abra la aplicación.

¿Pueden robar mi contraseña si acceden a mi AnyDesk?

No. AnyDesk no almacena la contraseña en texto plano. Cuando se guarda el login, se genera un token criptográfico vinculado al dispositivo específico. Aunque alguien acceda al archivo de configuración, no podrá extraer la contraseña.

¿Es seguro el acceso no atendido?

Sí, siempre que sigas las buenas prácticas:

- Usa contraseñas de al menos 12 caracteres
- Habilita 2FA cuando sea posible
- Cambia la contraseña periódicamente
- Restringe el acceso interactivo si no lo necesitas
- Solo guarda tokens en dispositivos de confianza

¿Funciona el acceso no atendido en Mac?

Sí, el acceso no atendido funciona en Windows, macOS y Linux. En macOS, es posible que necesites conceder permisos adicionales de accesibilidad y grabación de pantalla en System Settings > Privacy & Security.

Conclusión

El acceso remoto no atendido de AnyDesk es una herramienta esencial para cualquier profesional que necesite gestionar dispositivos remotos de forma eficiente. Con una configuración adecuada y las medidas de seguridad recomendadas, puedes mantener acceso 24/7 a tus sistemas sin comprometer la seguridad.

La combinación de contraseña robusta, autenticación de dos factores y gestión de tokens proporciona un nivel de seguridad adecuado para entornos empresariales. Solo recuerda instalar AnyDesk (no usar portable) en los dispositivos remotos para garantizar la conectividad tras reinicios.

¿Listo para configurar tu primer acceso no atendido? Descarga AnyDesk desde anydesk.com/es/downloads y sigue los pasos de esta guía.