Acceso desatendido

TABLA DE CONTENIDO

- Configuración
  - Permisos (Versiones anteriores a AnyDesk 7)
  - Permisos (AnyDesk 7+)
- Configurar la autenticación de dos factores
- Habilitar el acceso desatendido
  - Inicio de sesión automático
  - Consideraciones de seguridad
  - Acceso desatendido exclusivo

El concepto de oficina en casa (home office) se está expandiendo rápidamente y los usuarios no siempre pueden depender de que una persona en el dispositivo remoto físico acepte su solicitud de conexión.

Además, en las pantallas de inicio de sesión como las de Windows y macOS, solo están disponibles los servicios en segundo plano, por lo que las ventanas basadas en GUI, como la Ventana de aceptación de AnyDesk, no pueden mostrarse.

Teniendo esto en cuenta, AnyDesk ofrece la posibilidad de conectarse a un dispositivo remoto mediante una contraseña, lo que evita la necesidad de que un usuario acepte la solicitud de conexión.

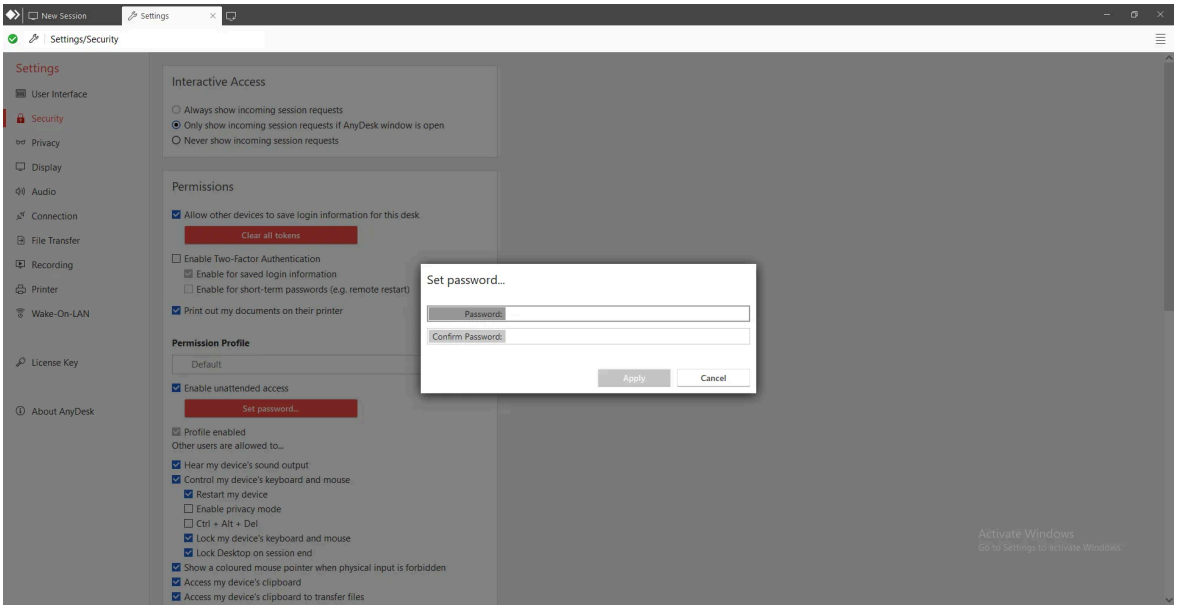
Nota: Aunque no es obligatorio, se recomienda encarecidamente instalar AnyDesk en el dispositivo donde se haya configurado el acceso desatendido. Esto garantiza la conectividad con el dispositivo incluso después de un reinicio del sistema o de haber cerrado la sesión de la cuenta.

Configuración

De forma predeterminada, el acceso desatendido está desactivado en el cliente AnyDesk y no permitirá conexiones desatendidas al dispositivo. En este caso, las solicitudes de conexión **deben ser aceptadas o rechazadas manualmente** utilizando la ventana de aceptación del cliente al que se conecta.

Los ajustes de acceso desatendido se encuentran en *Settings* > *Security* > *Unattended Access* para las versiones de AnyDesk que no son de Windows o para las versiones de AnyDesk para Windows anteriores a AnyDesk 7.

Para AnyDesk 7 para Windows y versiones más recientes, el acceso desatendido se puede habilitar en *Settings* > *Security* > *Permissions* > **Permission Profile** de forma individual para cada perfil.



Permisos (Versiones anteriores a AnyDesk 7)

Override standard permissions (Anular los permisos estándar): Cuando esta opción está desactivada, se utilizan en su lugar los permisos de “Settings” > “Security” > “Standard Permissions of Remote Users”.

Permitir al usuario que se conecta:

- Escuchar la salida de sonido de mi ordenador.
- Controlar el teclado y el ratón de mi ordenador.
- Acceder al portapapeles de mi ordenador.
- Acceder al portapapeles de mi ordenador para transferir archivos.

- Bloquear el teclado y el ratón de mi ordenador.
- Reiniciar mi ordenador.
- Utilizar el Administrador de archivos.
- Bloquear la cuenta al finalizar la sesión.
- Solicitar información del sistema.
- Imprimir mis documentos en su impresora (Consulte Impresión remota).
- Dibujar en la pantalla del ordenador (Consulte Pizarra).
- Crear túneles TCP (Consulte Túnel TCP).
- Habilitar el modo de privacidad (Consulte Privacidad de pantalla).
- Mostrar un puntero de ratón de color cuando el usuario que se conecta no tiene permiso para controlar mi dispositivo.

Permisos (AnyDesk 7+)

Consulte Perfiles de permisos.

Configurar la autenticación de dos factores

> 💡 **NOTA**
>
> Necesitará una aplicación de autenticación que admita contraseñas de un solo uso basadas en el tiempo (TOTP).

AnyDesk ofrece autenticación de dos factores (2FA) para el acceso remoto a dispositivos sin que haya nadie presente físicamente (acceso desatendido).

Se recomiendan las siguientes aplicaciones de autenticación para su uso con AnyDesk:

- Google Authenticator
- Microsoft Authenticator
- FreeOTP

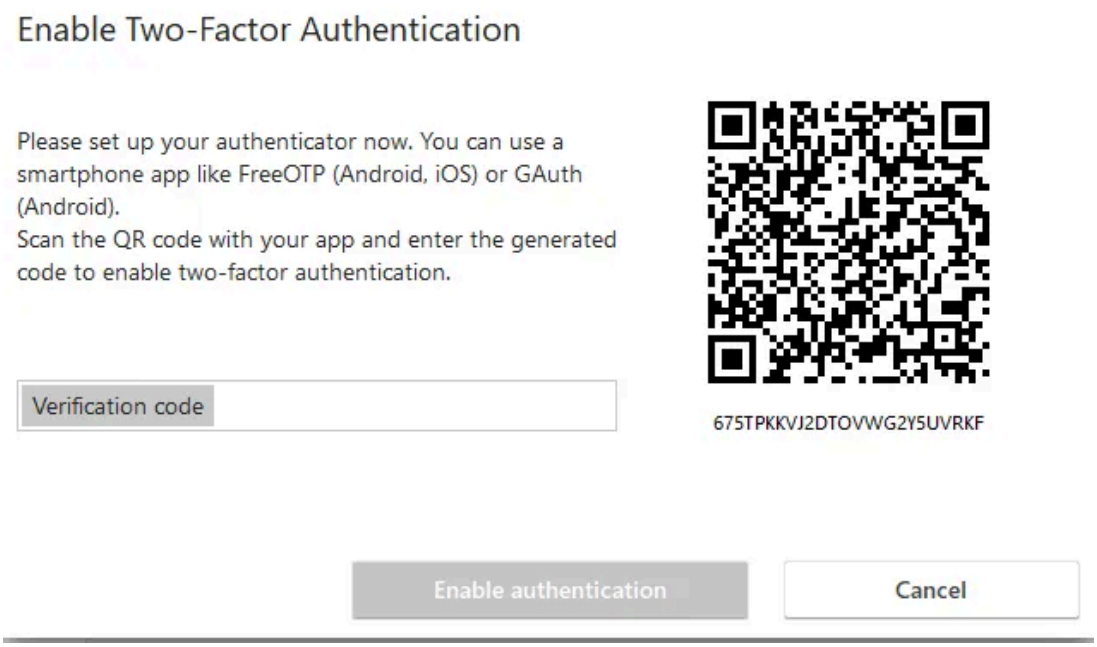
Para habilitar la verificación 2FA para las conexiones de acceso desatendido a su cliente, siga estos pasos:

1. Abra el cliente AnyDesk, haga clic en

   en la esquina superior derecha y seleccione **Settings**.

2. En **Settings**, navegue hasta **Access** y, en la sección **Unattended Access**, marque la casilla **Enable Two-Factor Authentication**.
3. Aparecerá un aviso donde podrá escanear el código QR o pegar la clave en uno de nuestros autenticadores recomendados.



4. Introduzca el código de autorización de su autenticador y haga clic en **Enable authorization**.

🚨 Si introduce el código de autenticación correcto pero el botón **Enable authorization** sigue apareciendo en gris, asegúrese de que la hora tanto en el autenticador como en el dispositivo AnyDesk esté sincronizada. Dado que los códigos se basan en el tiempo, fallarán si las horas no están alineadas.

Establecer una sesión

Al conectarse a un cliente AnyDesk con la autenticación de dos factores (2FA) habilitada, se le pedirá que introduzca un código de autorización de 6 dígitos de su aplicación de autenticación inmediatamente después de enviar la contraseña de acceso desatendido (ya sea manual o automáticamente).



Ajustes

Reconocemos la importancia de la autenticación de dos factores (2FA) para mejorar la seguridad. Sin embargo, también somos conscientes de que la 2FA puede no ser necesaria para muchos usuarios después de la verificación inicial.

Para solucionar esto, AnyDesk ofrece dos opciones para que los administradores permitan a los usuarios que se conectan omitir la verificación 2FA:

1. **Inicio de sesión automático**: Si la casilla **Enable for saved login information** está desactivada, AnyDesk no pedirá el código de verificación 2FA cuando un usuario se conecte utilizando el token de inicio de sesión automático.
2. **Contraseñas a corto plazo**: Si la casilla **Enable for short-term passwords (e.g., remote restart)** está desactivada, AnyDesk no pedirá el código de verificación 2FA al reconectar automáticamente una sesión, como durante un Reinicio remoto.

Al personalizar estos ajustes, los administradores pueden agilizar la experiencia del usuario manteniendo las medidas de seguridad adecuadas.

Habilitar el acceso desatendido

Al activar “Enable Unattended Access”, aparecerá un mensaje donde el usuario puede establecer la contraseña utilizada para el acceso desatendido. Se puede cambiar una contraseña existente haciendo clic en “Set password for unattended access”.

Restricciones de la contraseña:

- Al menos 8 caracteres.
- Al menos suficientemente segura (sin caracteres que se repitan constantemente o contraseñas identificables básicas, por ejemplo, “contraseña”).
- **Recomendado:** Una mezcla de letras, números y símbolos.

Precaución:

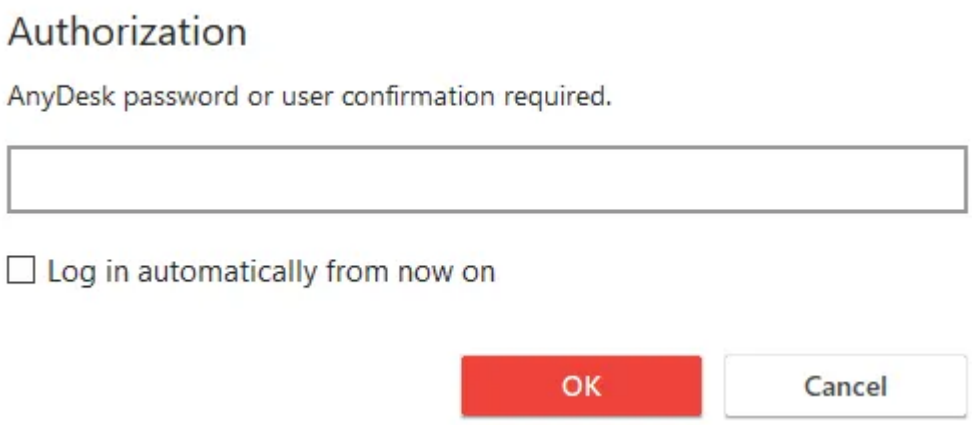
La contraseña debe ser muy segura. Cualquier persona que conozca la contraseña y su ID de AnyDesk puede tener acceso total a su ordenador dependiendo de los permisos disponibles. Se recomienda encarecidamente una contraseña que supere al menos los 12 caracteres.

AnyDesk también admite la autenticación de dos factores para obtener la mejor seguridad.

Compruebe siempre por partida doble cuando un tercero se ponga en contacto con usted y le pida su dirección de AnyDesk. Nosotros (**AnyDesk Software**) **nunca** le pediremos su contraseña, y las empresas legítimas nunca se pondrán en contacto con usted sin que usted haya iniciado la comunicación primero. En caso de que busque la ayuda de un servicio de reparación de PC, asegúrese de conocer al proveedor.

Inicio de sesión automático

Activar “Allow other computers to save login information for this computer” (Permitir que otros ordenadores guarden la información de inicio de sesión de este equipo) permitirá que los usuarios que se conecten al cliente mediante acceso desatendido seleccionen “Login automatically from now on” (Iniciar sesión automáticamente a partir de ahora).



Cuando se selecciona esta opción y la contraseña de acceso desatendido es correcta, el cliente que se conecta recibirá un token del cliente AnyDesk remoto. Con este token, las futuras conexiones desde ese cliente al cliente remoto permitirán que sus solicitudes se acepten automáticamente sin necesidad de escribir la contraseña de acceso desatendido para las sesiones posteriores.

Restablecer el token

El token se puede restablecer desde el dispositivo remoto seleccionando “Clear all tokens” (Borrar todos los tokens) o cambiando la contraseña de acceso desatendido.

Restablecer el token obligará a todos los usuarios de acceso desatendido a introducir manualmente la contraseña de acceso desatendido de nuevo.

Puede desactivar la función que permite guardar la información de inicio de sesión (la contraseña) desmarcando “Allow other computers to save login information for this computer”. Tenga en cuenta que los tokens ya existentes seguirán funcionando, pero no se generarán tokens nuevos.

Consideraciones de seguridad

- Esta función no guarda la contraseña en sí. En su lugar, la máquina remota genera un token específico. **Este token solo puede ser utilizado por el cliente autorizado.** Un cliente solo puede obtener la autorización si se introdujo la contraseña correcta.
- Incluso si alguien tiene acceso total a su cliente que tiene esta función habilitada, no hay forma de obtener su contraseña en texto claro.
- Cambiar la contraseña por la misma contraseña también invalidará todos los tokens. Esto es útil si ha introducido la contraseña en el cliente en el pasado, pero el propietario del cliente no conoce la contraseña.

Acceso desatendido exclusivo

Para forzar al cliente AnyDesk a que solo sea accesible mediante la contraseña de acceso desatendido, se puede activar “Never show incoming session requests” (No mostrar nunca las solicitudes de sesión entrantes) en *Settings* > *Security* > **Interactive Access**.