Configurar firewalls para AnyDesk

TABLA DE CONTENIDO

Puertos requeridos

Dominios en lista blanca

Configuración del Firewall de Windows

Permitiendo manualmente AnyDesk a través del firewall

Configuración de firewall de hardware o empresa

En algunos entornos, las configuraciones de firewall pueden bloquear a AnyDesk para crear o mantener conexiones remotas.

Este artículo explica qué puertos y direcciones deben estar abiertos o en lista blanca para asegurar el uso ininterrumpido de AnyDesk.

Puertos requeridos

Para conectarse exitosamente, AnyDesk usa los siguientes puertos TCP y UDP:

- **Puertos TCP:** 80, 443 y 6568

> 💡 **NOTA**
>
> Al menos uno de estos puertos debe estar abierto para crear una conexión remota.

- **Puertos UDP:** 50001–50003
  - Usados por la función **Discovery** de AnyDesk para identificar dispositivos en la red local.
  - El tráfico de Discovery se envía a la **dirección IP:** 239.255.102.18 (multicast).

Dominios en lista blanca

Si está usando un firewall o solución de filtrado de tráfico, recomendamos poner en lista blanca el siguiente dominio para evitar problemas de conexión:

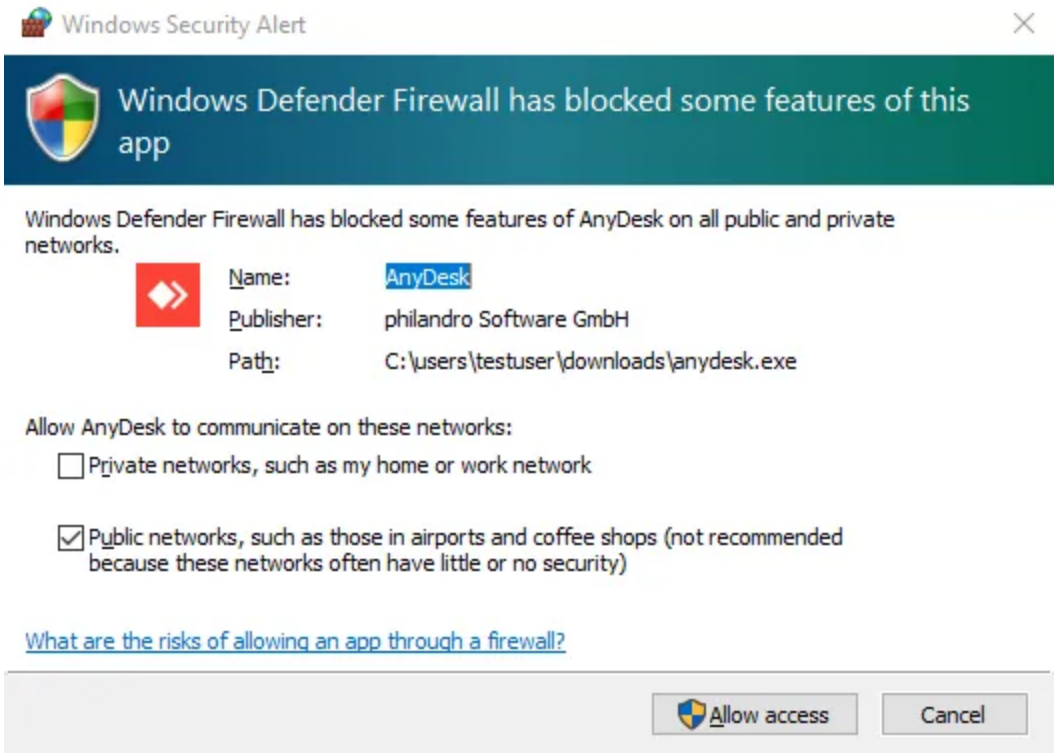
- `*.net.anydesk.com`

Esto asegura que el cliente AnyDesk pueda alcanzar nuestros servidores e iniciar o mantener sesiones remotas.

Configuración del Firewall de Windows

Cuando ejecuta AnyDesk en **modo portátil** (desinstalado), la primera vez que intenta conectarse, el **Firewall de Windows Defender** le preguntará si permitir AnyDesk a través del firewall.

- Haga clic en **Permitir acceso** para dejar pasar AnyDesk a través del firewall. Esto otorga los permisos necesarios para conexiones directas.

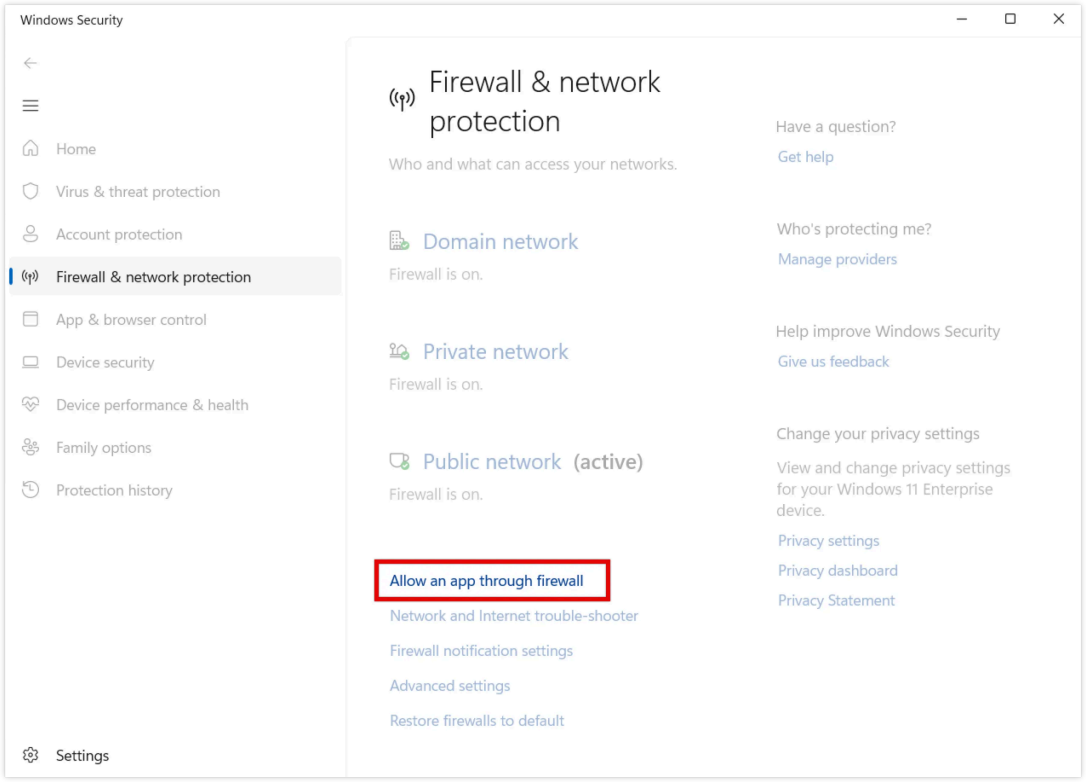


> 💡 **NOTA**
>
> Si está usando un Cliente Personalizado, puede activar el interruptor **Disable TCP listen port** en el Cliente Personalizado. Esto bloquea las conexiones TCP entrantes y previene el aviso del **Firewall de Windows**.

Permitiendo manualmente AnyDesk a través del firewall

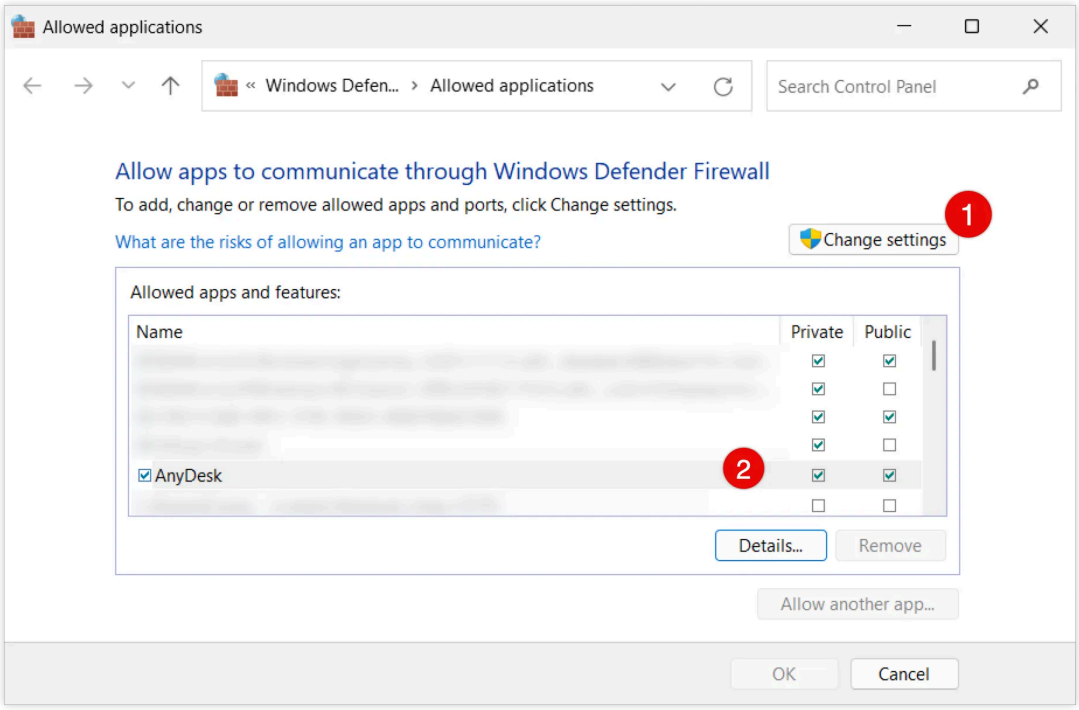
Si previamente denegó el aviso del firewall, siga estos pasos para otorgar acceso manualmente:

1. Abra **Configuración de Windows**.
2. Navegue a **Privacidad y seguridad** > **Seguridad de Windows**.
3. Haga clic en **Firewall y protección de red**.
4. En la ventana abierta, seleccione **Permitir una aplicación a través del firewall**.



Windows Security settings showing firewall options and allowing apps through the firewall.

5. Haga clic en **Cambiar configuración**, localice **AnyDesk** y seleccione ambas casillas (*Privada* y *Pública*).



Configuración de firewall de hardware o empresa

Si su red usa un firewall basado en hardware o empresarial (ej., un router o dispositivo de puerta de enlace), puede requerirse configuración adicional. AnyDesk debe ser excluido de escaneos de seguridad a nivel de red que interfieran con el tráfico cifrado, tales como:

- **Escaneo HTTPS**
- **Inspección profunda de paquetes (DPI)**

Estos escaneos pueden interrumpir el cifrado TLS de AnyDesk y pueden causar que las sesiones se desconecten inesperadamente.

> 💡 **NOTA**
>
> El nombre exacto y comportamiento de estas configuraciones dependen del proveedor. Consulte la documentación de su firewall para configurar excepciones o reglas de bypass para `*.net.anydesk.com`.

Configuraciones que determinan cómo se gestiona y filtra el tráfico de red, lo que puede afectar la capacidad de AnyDesk para establecer conexiones.

Una versión a medida de AnyDesk que se puede configurar para necesidades organizacionales específicas, incluyendo marca y funcionalidad.