Some Help With

Configure firewalls for AnyDesk

TABLE OF CONTENT

Required ports

Whitelist domains

Windows Firewall Configuration

    Manually allowing AnyDesk through the firewall

Hardware or company firewall configuration

In some environments, firewall configurations may block AnyDesk from creating or maintaining remote connections.

This article explains which ports and addresses must be open or whitelisted to ensure uninterrupted use of AnyDesk.

Required ports

To connect successfully, AnyDesk uses the following TCP and UDP ports:

- **TCP ports:** 80, 443, and 6568

  > 💡 **NOTE**
  >
  > At least one of these ports must be open to create a remote connection.

- **UDP ports:** 50001–50003
  - Used by AnyDesk's **Discovery** feature to identify devices on the local network.
  - Discovery traffic is sent to **IP address:** 239.255.102.18 (multicast).

Whitelist domains

If you are using a firewall or traffic filtering solution, we recommend whitelisting the following domain to avoid connection issues:

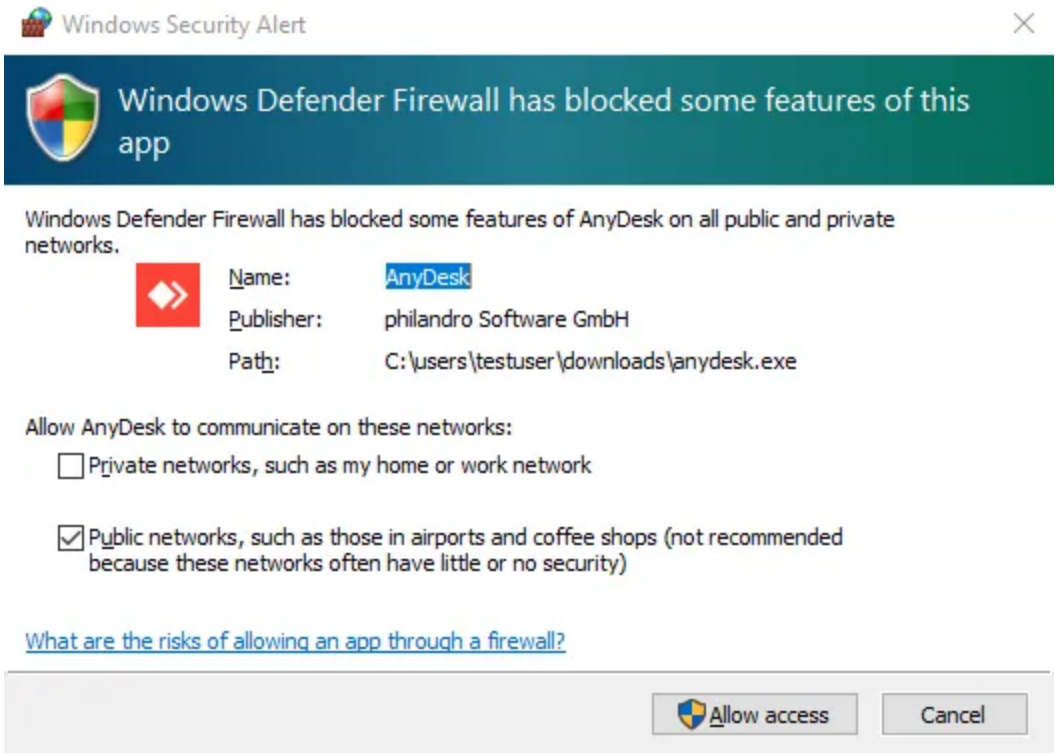
- `*.net.anydesk.com`

This ensures that the AnyDesk client can reach our servers and initiate or maintain remote sessions.

Windows Firewall Configuration

When you run AnyDesk in **portable mode** (uninstalled), the first time you try to connect, **Windows Defender Firewall** will ask whether to allow AnyDesk through the firewall.

- Click **Allow access** to let AnyDesk through the firewall. This grants the required permissions for direct connections.

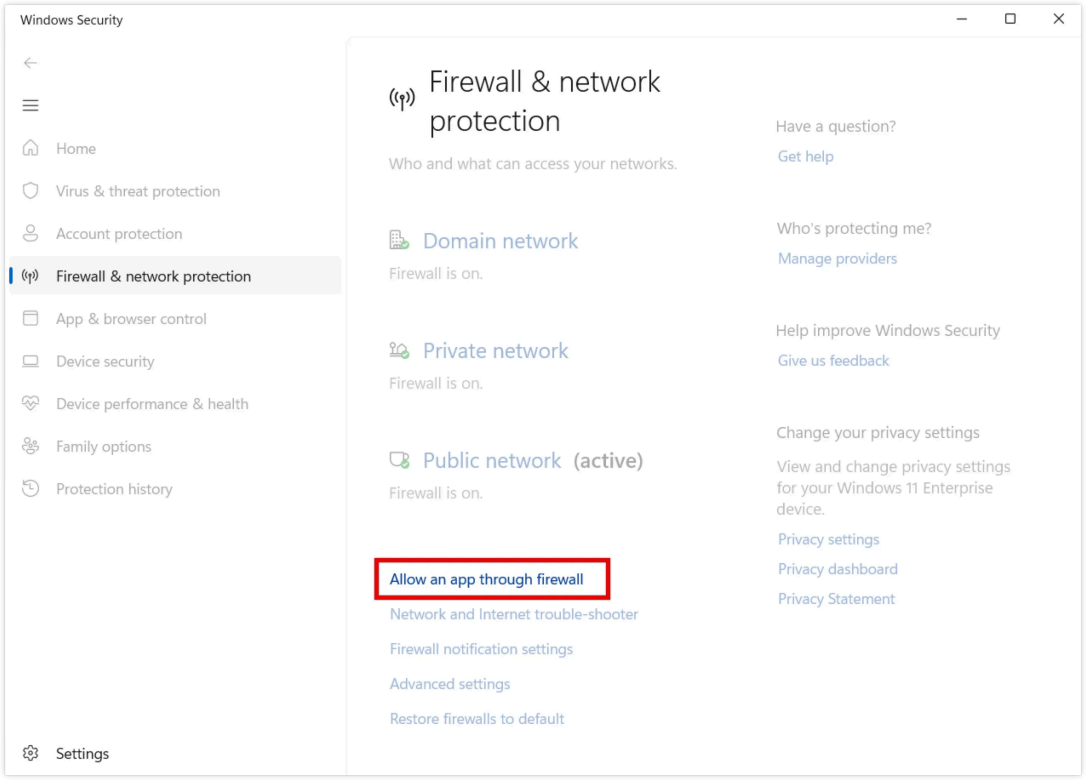


> 💡 **NOTE**
>
> If you're using a Custom Client, you can turn on the **Disable TCP listen port** toggle in the Custom . This blocks incoming TCP connections and prevents the **Windows Firewall** prompt.

Manually allowing AnyDesk through the firewall

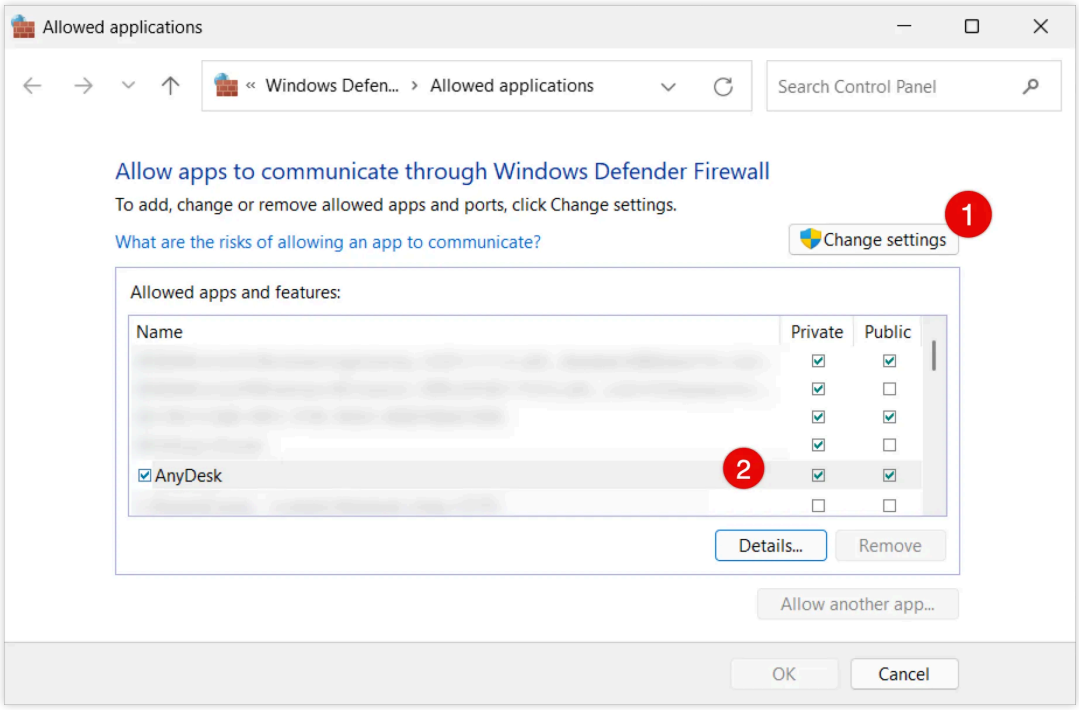
If you previously denied the firewall prompt, follow these steps to manually grant access:

1. Open **Windows Settings**.
2. Navigate to **Privacy & security** > **Windows Security**.
3. Click **Firewall & network protection**.
4. On the opened window, select **Allow an app through firewall**.



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

5. Click **Change settings**, locate **AnyDesk** and select both checkboxes (*Private* and *Public*).



Windows Defender Firewall settings

Hardware or company firewall configuration

If your network uses a hardware-based or enterprise firewall (e.g., a router or gateway device), additional configuration may be required. AnyDesk must be excluded from network-level security scans that interfere with encrypted traffic, such as:

- **HTTPS scanning**
- **Deep packet inspection (DPI)**

These scans can disrupt AnyDesk's TLS encryption and may cause sessions to disconnect unexpectedly.

> 💡 **NOTE**
>
> The exact name and behavior of these settings depend on the vendor. Refer to your firewall documentation to configure exceptions or bypass rules for `*.net.anydesk.com`.

Settings that determine how network traffic is managed and filtered, which can affect the ability of AnyDesk to establish connections.

A tailored version of AnyDesk that can be configured for specific organizational needs, including branding and functionality.