Some Help With

AnyDesk On-Premises

TABLE OF CONTENT

Benefits of using AnyDesk On-Premises

- Control who can connect
- Use without internet
- Limit client usage on your network
- Full control of your data

> **License:** Ultimate

The AnyDesk On-Premises lets you host your own AnyDesk appliance server on your internal network, using either physical or virtual hardware. This gives you full control over your Remote Desktop environment.

> 🦉 You can find a step-by-step Installation Guide in **my.anydesk II**.

> 💡 **NOTE**
>
> The **Automatically register the client to the Address Book** feature is not yet supported for On-Premises AnyDesk clients due to system limitations. This feature is under development.

Benefits of using AnyDesk On-Premises

Control who can connect

Only custom AnyDesk clients created in your **my.anydesk** portal can connect to each other. Standard AnyDesk clients from our website or custom clients from other organizations cannot connect to your environment, as only your clients are aware of your appliance server.

 © 2026 www.somehelpwith.com

For additional security, you can use a third-party VPN together with your on-premises setup. Hosting the appliance server in a DMZ and restricting access to internal IP addresses ensures that only devices connected via VPN can reach the server. This way, only devices on your internal network, or devices connected through VPN, can reach the server. External clients without VPN access won't be able to find or connect to it.

Use without internet

The cloud version of AnyDesk requires internet access to find client information and initiate sessions from the global AnyDesk database.

With the on-premises setup, this is not required. As long as both devices can connect to your local server, they can start a remote session, even without an internet connection.

You can also make your appliance server available online if you configure your appliance server to be publicly accessible over the internet. This allows your custom clients to connect from different locations over the internet.

Limit client usage on your network

Organizations with strict security requirements can enforce the use of only pre-configured AnyDesk clients. You can block access to AnyDesk cloud servers using your firewall:

- Block access to AnyDesk cloud network addresses in your firewall.
- Deploy only on-premises clients across your internal devices.

This prevents standard AnyDesk clients from working on your network. Your pre-configured on-premises clients will still work, as they connect only to your own server.

Full control of your data

By hosting the AnyDesk appliance server and its associated database on your infrastructure, you maintain full control over your data. This includes:

- Managing or deleting Session History for compliance or internal policy requirements.
- Controlling access based on IP address.

This capability supports data privacy regulations and allows organizations to implement customized data retention and security policies.

A self-hosted version of AnyDesk running on your own in-house virtual servers. All data remains within your company network and can be self-managed by your own IT team. It offers a high-level of security

and data protection.

The ability to access and control a device from a different location using AnyDesk, facilitating remote support and work.

A guide that provides step-by-step instructions on how to install and set up AnyDesk.

A feature that lets you save and organize your contacts, which you can group using tags, for quick and easy access to remote devices.

A built-in feature that creates a secure, private connection between local and remote devices. It enhances security by linking only the two devices directly, without allowing access to other devices on either network.

A record of all remote sessions conducted using AnyDesk, including details such as duration and participants.