Some Help With

Unattended access

TABLE OF CONTENT

- Setup
- Permissions (Pre-AnyDesk 7)
- Permissions (AnyDesk 7+)
- Set up two-factor authentication
- Enabling Unattended Access
- Automatic Login
- Security Considerations
- Exclusive Unattended Access

The home office idea is rapidly expanding and users cannot always rely on a user on the physical remote device to accept their connection request.

Furthermore, on login screens such as those on Windows and macOS, only background services are available so that GUI-based windows such as AnyDesk's Accept Window cannot be displayed.

With this in mind, AnyDesk provides the ability to connect to a remote device using a password which bypasses the need for a user to accept the connection request.

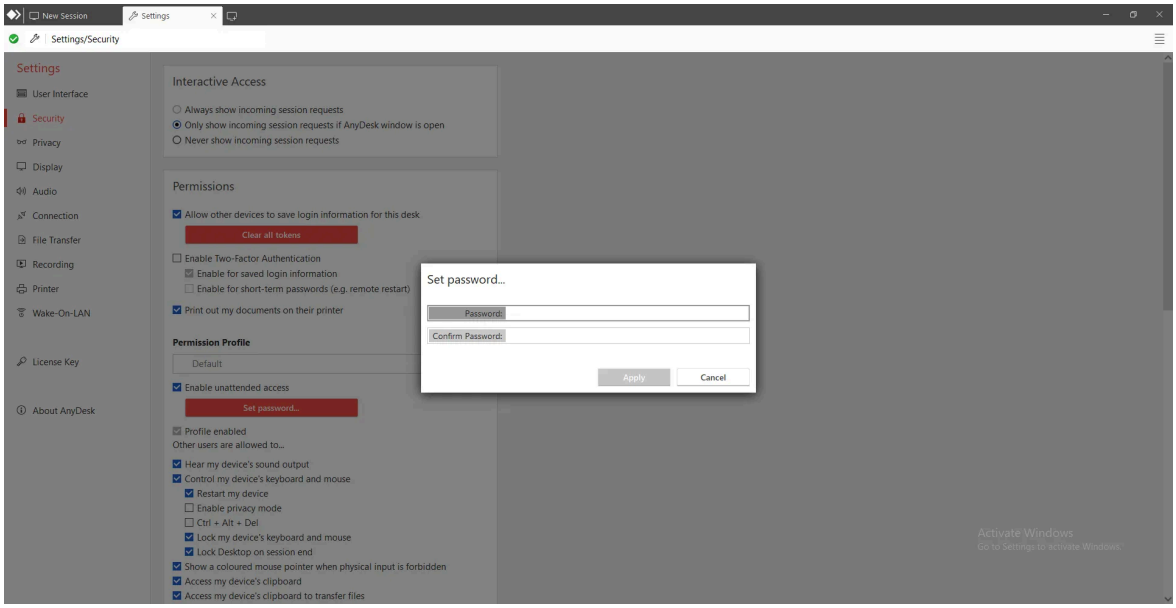
Note: While not required, it is highly recommended that AnyDesk is installed on the device where Unattended Access has been configured. This ensures connectivity with the device even after a system restart or the account has been logged out of.

Setup

By default, Unattended Access is disabled on the AnyDesk client and will not allow unattended connections to the device. In this case, connection requests **need to be manually accepted or rejected** using the Accept Window of the client being connected to.

Unattended Access settings can be found in *Settings* > *Security* > *Unattended Access* for non-Windows versions of AnyDesk or versions of AnyDesk for Windows before AnyDesk 7.

For AnyDesk 7 for Windows and newer, Unattended Access can be enabled in *Settings* > *Security* > *Permissions* > *Permission Profile* on a per profile basis.



VirtualBoxVM_wGgBAsjpbU

Permissions (Pre-AnyDesk 7)

Override standard permissions: When disabled, the permissions from “Settings” > “Security” > “Standard Permissions of Remote Users” are used instead.

Allow the connecting user to:

- Hear my computer’s sound output
- Control my computer’s keyboard and mouse
- Access my computer’s clipboard
- Access my computer’s clipboard to transfer files
- Lock my computer’s keyboard and mouse
- Restart my computer
- Use the File Manager
- Lock account on session end
- Request system information
- Print out my documents on their printer (See Remote Print)
- Draw on computer’s screen (See Whiteboard)
- Create TCP tunnels (See TCP-Tunneling)

- Enable privacy mode (See Screen Privacy)
- Show a colored mouse pointer when the connecting user does not have permission to control my device

Back to top

Permissions (AnyDesk 7+)

Please see Permission Profiles.

Back to top

Set up two-factor authentication

> 💡 **NOTE**
>
> You will need an authentication app that supports time-based one-time passwords (TOTP).

AnyDesk provides Two-Factor Authentication (2FA) for remote access to devices without someone physically present (unattended access).

The following authenticator apps are recommended for use with AnyDesk:

- Google Authenticator
- Microsoft Authenticator
- FreeOTP

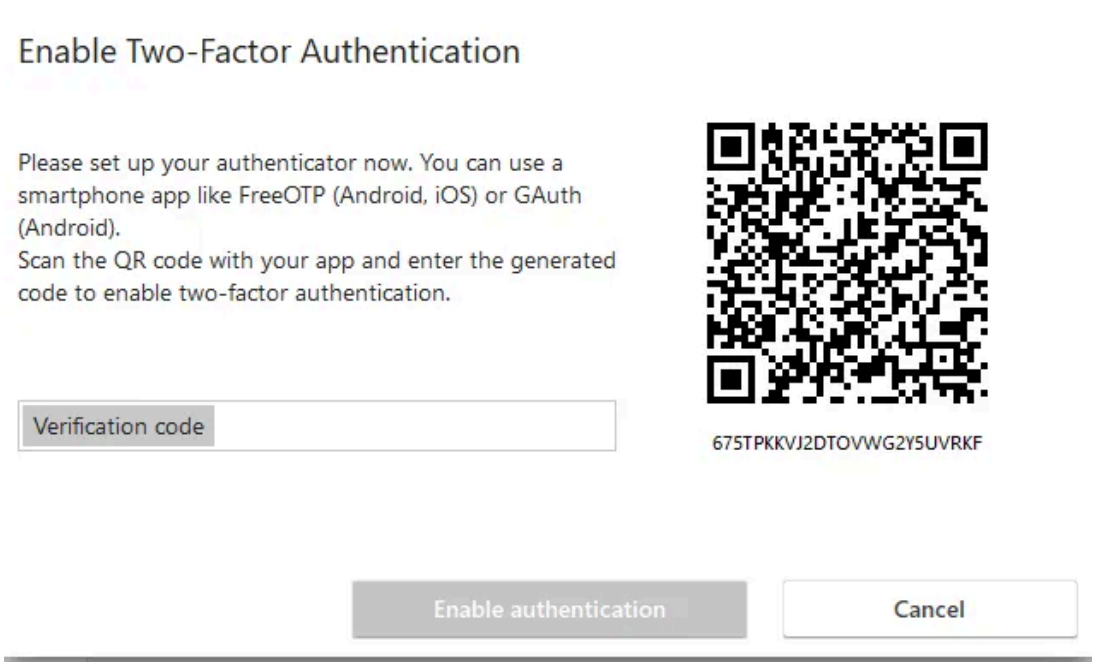
To enable 2FA verification for Unattended Access connections to your client, complete the following steps:

1. Open AnyDesk client, in the upper-right corner, click

   image.png

   and select **Settings**.
2. In **Settings**, navigate to **Access** and in the **Unattended Access** section, select the **Enable Two-Factor Authentication** checkbox.
3. A prompt will appear where you can scan the QR-Code or paste the key into one of our recommended authenticators.



VirtualBoxVM_ruFnNywIpQ

4. Enter the authorization code from the authenticator and click **Enable authorization**.

🚨 If the correct authentication code is entered but the **Enable authorization** button is still grayed out, ensure the time on both the authenticator and the AnyDesk device is synchronized. Since the codes are time-based, they will fail if the times are not aligned.

Establishing a session

When connecting to an AnyDesk client with two-factor authentication (2FA) enabled, you will be prompted to enter a 6-digit authorization code from your authenticator app immediately after submitting the unattended access password, whether manually or automatically.



VirtualBoxVM_J7Vpls2g94

Settings

We recognize the importance of two-factor authentication (2FA) for enhancing security. However, we also acknowledge that 2FA may not be necessary for many users after the initial verification.

To address this, AnyDesk provides two options for administrators to allow connecting users to skip 2FA verification:

1. **Automatic Login**: If the **Enable for saved login information** checkbox is unticked, AnyDesk will not ask for the 2FA verification code when a user connects using the Automatic Login token.
2. **Short-term Passwords**: If the **Enable for short-term passwords (e.g., remote restart)** checkbox is unticked, AnyDesk will not ask the 2FA verification code when automatically reconnecting a session, such as during a Remote Restart.

By customizing these settings, administrators can streamline the user experience while maintaining appropriate security measures.

Enabling Unattended Access

By enabling “Enable Unattended Access”, a prompt will appear where the user can set the password used for Unattended Access. An existing password can be changed by clicking “Set password for unattended access”.

Password Constraints:

- At least 8 characters.
- At least sufficiently safe (no consistently repeating characters or basic identifiable passwords (e.g. “password”)).
- **Recommended:** A mix of letters, numbers, and symbols.

Caution:

The password should be very secure. Anyone who knows the password and your AnyDesk ID can potentially have full access to your computer depending on the available permissions. A password that exceeds at least 12 characters is highly recommended.

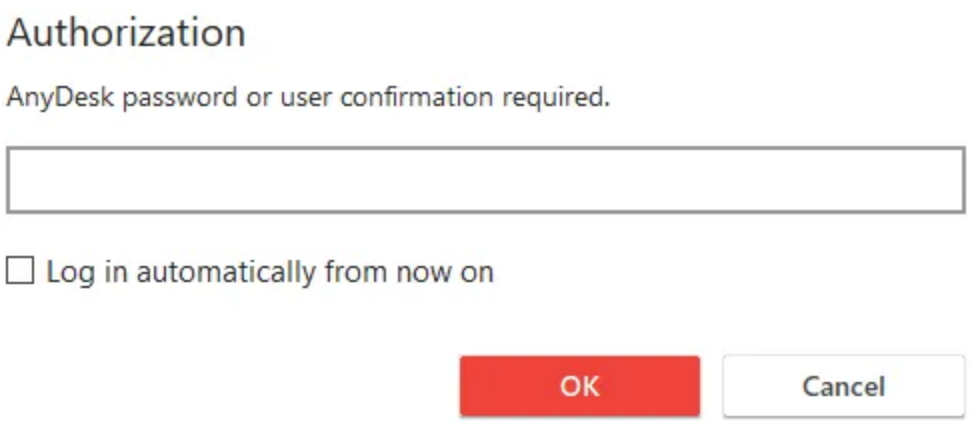
AnyDesk also supports Two-Factor Authentication for the best security.

Always double-check when a third-party contacts you and demands your AnyDesk Address. We (**AnyDesk Software**) will **never**ask for your password and legitimate companies will never contact you

without you having initiated the communication first. In case you are seeking the help of a PC repair service, please make sure you know the vendor.

Automatic Login

Enabling “Allow other computers to save login information for this computer” will allow users connecting to the client via Unattended Access to select “Login automatically from now on”.



VirtualBoxVM_AtUalU6jye

When this option is selected and the Unattended Access password is correct, the connecting client will receive a token from the remote AnyDesk client. With this token, future connections from the connecting client to the remote client will allow the connecting client to have his requests accepted automatically without the need of typing the Unattended Access password for subsequent sessions.

Resetting the Token

The token can be reset by the remote device by selecting “Clear all tokens”, or changing the unattended access password.

Resetting the token will force all Unattended Access users to manually type in the Unattended Access password again.

You can disable the feature to allow login information (the password) by unticking “Allow other computers to save login information for this computer”. Please note that already existing tokens will remain functional, but no new tokens will be generated.

Security Considerations

- This feature does not save the password itself. Instead, the remote machine generates a specific token. **This token can only be used by the authorized client.** A client can only get

authorization if the correct password was entered.

- Even if someone has full access to your client that has this feature enabled, there is no way to gain access to your password in cleartext.
- Changing the password to the same password will also invalidate all tokens. This is useful if you have entered the password on the client in the past, but the owner of the client does not know the password.

Exclusive Unattended Access

To force the AnyDesk client to only be accessible using the Unattended Access password, “Never show incoming session requests” can be enabled in *Settings* > *Security* > *Interactive Access*.