Some Help With

Ultimate Guide to Two-Factor Authentication with AnyDesk: Setup, Best Practices, and Use Cases

TABLE OF CONTENT

- Client
- my.AnyDesk.com
- Recommended authenticator apps
- Use Cases

Two-Factor Authentication

Table of Contents

Client	my.AnyDesk.com	Recommended authenticator apps	Use Cases

AnyDesk offers Two-Factor Authentication (2FA) for unattended access connections to a specific AnyDesk client as well as for access to the MyAnyDesk customer portal.

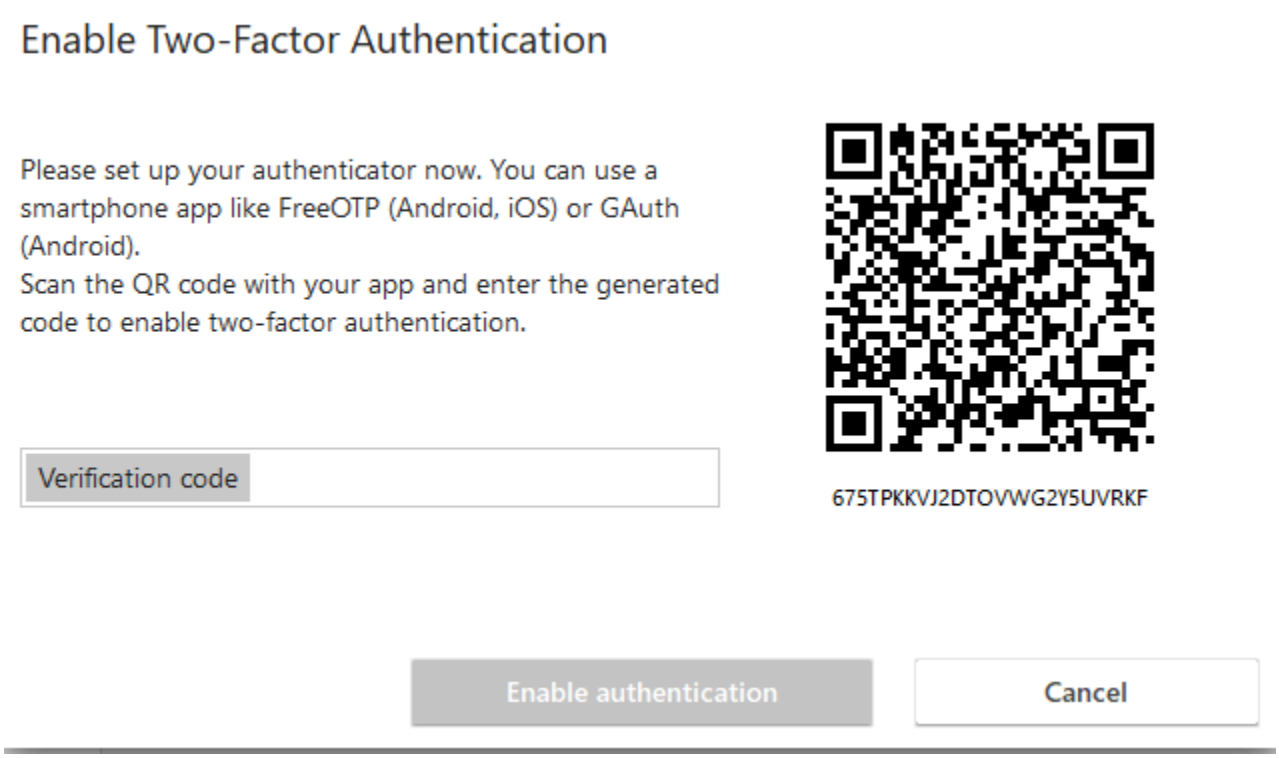
Note: The use of this feature requires an authentication app that supports “time-based one-time passwords” (TOTP).

Client

To require a 2FA verification code when connecting to your client using Unattended Access, follow these steps:

 © 2026 www.somehelpw

Setup



1. Enable “Enable Two-Factor Authentication” in *Settings* > *Security* > *Permissions*.
2. A prompt will appear where the user can scan the QR-Code or paste the key into one of our recommended authenticators.
3. Enter the authorization code from the authenticator and click “Enable authorization”.

Warning:

If the correct authentication code is given but the “Enable authorization” button remains grayed out, please make sure that the times on both authenticator and AnyDesk device are synchronized. As the verification codes are time-based, they will not authenticate if the times are asynchronous.

Establishing a session



 © 2026 www.somehelpw

When connecting to an AnyDesk client with 2FA enabled, a 6-digit authorization key from the authenticator is requested directly after the unattended access password is manually or automatically submitted.

Settings

While AnyDesk understands the necessity for 2FA and the level of security that it brings, we also understand that this level of authentication is unnecessary for many after the initial verification stage. Therefore, AnyDesk offers two situations where the administrator of the client can allow connecting users to skip the 2FA verification:

1. Automatic Login - If “Enable for saved login information” is **unticked**, then AnyDesk **will not** ask for the 2FA verification code when the connecting user is establishing a session using the Automatic Login token.
2. Short-term passwords - If “Enable for short-term passwords (e.g. remote restart” is **unticked**, then AnyDesk **will not** ask for the 2FA verification code when automatically reconnecting the session. For example, in the case of Remote Restart.

Back to Top

my.AnyDesk.com

Two-Factor authentication for MyAnyDesk can be activated in *Settings* > *General* > *Two-factor authentication* of your MyAnyDesk customer portal.

Warning:

Print or save the recovery key in a secure location in order to restore access to your account when needed.
DO NOT PROCEED WITHOUT SAVING OR PRINTING THE RECOVERY KEY.
The recovery key cannot be retrieved or reset.

In the event that you lose access to your authentication device and do not have access to the recovery key, please contact AnyDesk Technical Support.

Back to Top

Recommended authenticator apps

The following authenticator apps are tested and recommended for use with AnyDesk:

- Google Authenticator

- Microsoft Authenticator
- FreeOTP

Back to Top

Use Cases

Home Office

Set up a company mobile phone, tablet, or PC with 2FA for unique access so that only your employee can access the office computer.

Additionally, you can set up multiple authentication devices by scanning the same QR code with more than one authenticator.

Limit Access

Limit the access to selected devices like your servers to only the person that has the authentication device.

Back to Top

 © 2026 www.somehelpw