



PRIVACY. SECURITY. DISCRETION.

SECURE REMOTE ACCESS

ANYDESK ON THE GO

Use a travel device to reach a more capable computer while keeping sensitive work and files on the remote system.

SET UP BOTH DEVICES

REMOTE

Install AnyDesk. Set a unique 12+ character Unattended Access password, enable 2FA, allowlist the travel device, and allow Privacy Mode.

TRAVEL

Install the official app, add the remote ID or Alias, keep automatic login off, and test the connection before travel.

CONNECT & USE

1 Unlock travel device • 2 Enter AnyDesk password + 2FA
3 Enter remote OS PIN • 4 Enable Privacy Mode • 5
Disconnect + lock

THREE LAYERS OF SECURITY

THREE LOCKS. THREE SECRETS.

A stolen or exposed travel device should not be enough to open the remote computer.

1 Travel Device PIN

UNLOCK THE TRAVEL DEVICE

Use a unique 6+ digit PIN or passcode. Enable device encryption and a short auto-lock. Biometrics may add convenience, but the PIN remains the primary barrier.

2 AnyDesk Access PIN

UNATTENDED ACCESS PASSWORD

AnyDesk calls this the Unattended Access password. Use a different 12+ character passphrase, enable 2FA, and do not save the login token.

3 Remote Device PIN

UNLOCK THE REMOTE COMPUTER

After AnyDesk connects, enter a separate operating-system PIN or password. Never reuse the travel-device PIN or AnyDesk passphrase.

THREE BARRIERS



ONE PRINCIPLE

Keep every credential different. Store recovery details in a password manager, not on the travel device.

SECURE BY DESIGN

ANYDESK SECURITY

Use the controls below to reduce exposure before, during and after every remote session.

ENCRYPTION & IDENTITY

- TLS/AEAD encrypted sessions
- Connection fingerprint view
- Salted password hashing
- Optional two-factor auth
- Device-specific login tokens

PRIVACY

- Privacy Mode blanks display
- Blocks local input and audio
- Does not erase OS history

SESSION CONTENT

- Session content not retained
- Local recording if enabled
- Connection metadata exists

ACCESS CONTROL

- Allowlist trusted AnyDesk IDs
- Unattended Access only
- Least-privilege permissions

NETWORK

- Private two-endpoint VPN
- Supported clients only

DATA CONTROL

- Disable clipboard sync
- Disable file transfer/recording

IMPORTANT

- No remote LAN or internet routing

KEEP THE WORK REMOTE

Keep transfer, clipboard and recording off; avoid screenshots.

Sensitive files stay on the remote computer.

Privacy Mode may be limited during login, UAC or other protected screens. Confirm the remote display is hidden.

RED.ONE • RED-ONE.INFO



PRIVACY. SECURITY. DISCRETION.

STEP 1 • PREPARE

SET UP THE REMOTE DEVICE

Complete these steps on the PC or Mac you plan to leave powered, awake and online.

INSTALL & IDENTIFY

ALL DEVICES Create a free AnyDesk account and install the official app on the remote computer and each travel device. Record the remote ID or Alias.

REMOTE Settings > Access: set a unique 12+ character password; enable 2FA and Privacy Mode. Leave AnyDesk open, signed in and minimized.

ADDITIONAL SECURITY: APPROVED ADDRESSES ONLY

On the **remote computer**, open AnyDesk Settings > Security > Access Control List (menu names vary by version). Enable the option to restrict incoming access to listed addresses.

Add each approved travel device's **AnyDesk ID or Alias**. These are AnyDesk addresses, not email or IP addresses. Only listed devices can connect; all others are blocked. Use exact entries, without wildcards.

Before travel, test an approved device and confirm an unlisted device is blocked. Keep your password and 2FA enabled.

PREVENT SAVED LOGINS

Turn off "Allow other computers to save login information" and clear old tokens.

STEP 2 • KEEP IT REACHABLE

POWER & LID SETTINGS

The remote computer must stay powered, awake and connected while you are away.

1 Windows PC

PLUGGED-IN POWER

Settings > System > Power & battery: set sleep to Never. For simplest testing, set display off to Never. On a laptop, set the plugged-in lid action to Do nothing.

2 Mac

POWER + AWAKE

Battery > Options: turn on 'Prevent automatic sleeping on power adapter when the display is off.' Keep the Mac connected to power.

3 Lid & Final Test

DO NOT ASSUME CLOSED = AWAKE

Windows: close only after choosing Do nothing. MacBook: leave open unless a powered external-display setup is tested. Test AnyDesk from another network.

STEP 3 • CONNECT & CONTROL

REMOTE IN. WORK. LOCK.

Run one complete practice session before travel, using a different network.

CONNECT

- Unlock travel device
- Open AnyDesk + choose ID
- Enter access password + 2FA
- Enter remote OS PIN
- Confirm remote desktop

APPLE OPTION

- Place iPhone near powered Mac
- Same Apple Account + 2FA
- Wi-Fi and Bluetooth on

IPHONE MIRRORING

- Open the app on the Mac
- Complete first-use prompts

WORK

- Control the PC or Mac
- Display > Privacy Mode
- Keep files on remote device

REQUIREMENTS

- macOS 15+ / iOS 18+
- Compatible Mac + supported region

FINISH

- Lock remote computer
- End session; lock travel device

NOTE

- iPhone Mirroring unavailable in EU

CONTROL THE IPHONE THROUGH THE MAC

From the AnyDesk session, open iPhone Mirroring on the remote Mac.

The nearby iPhone stays locked while you interact with it.

Privacy Mode needs permission on both ends and may drop at login, UAC, lock or other protected screens.

RED.ONE • RED-ONE.INFO

POWERED & AWAKE → VISIBLE IN ANYDESK

A dark display is fine; sleep is not. Keep Wi-Fi or Ethernet reliable.