



# The Beginner's Guide to AirDroid Business

AirDroid Business MDM Solution for SMBs & Enterprises

# CONTENTS

## Part 1. Introducing AirDroid Business

- What is AirDroid Business? -----03
- Introducing Admin Console -----04  
(cloud-based Android remote control center)
- Introducing Desktop Client -----05  
(remote control, large file transfer, non-root set up)

## Part 2. What Can AirDroid Business Do?

- Remote Monitoring Templates -----06~07
- Alerts & Workflows -----08
- Reports -----09
- Member Management -----10
- Remote Device Management -----11  
(device group, remote access & control, batch mode, tags)
- Policy ----- 12
- Kiosk Mode ----- 12  
(device lockdown, single-app/multi-app mode)
- Application Management Services -----13  
(auto app updates, forced installation, staged rollout)
- Geofence -----13  
(location tracking, automated workflows)

## Part 3. MDM Solution for Industries

- Digital Signage -----14
- IT Service -----15
- Logistics -----16

- Part 4. How to Get Started -----17

# What is AirDroid Business?

AirDroid Business is an all-in-one **Android Mobile Device Management (MDM)** Solution that focuses heavily on remote Android device management. It is a mdm solution specifically designed for both small businesses and enterprises who need to manage more than 10 devices on a daily basis.

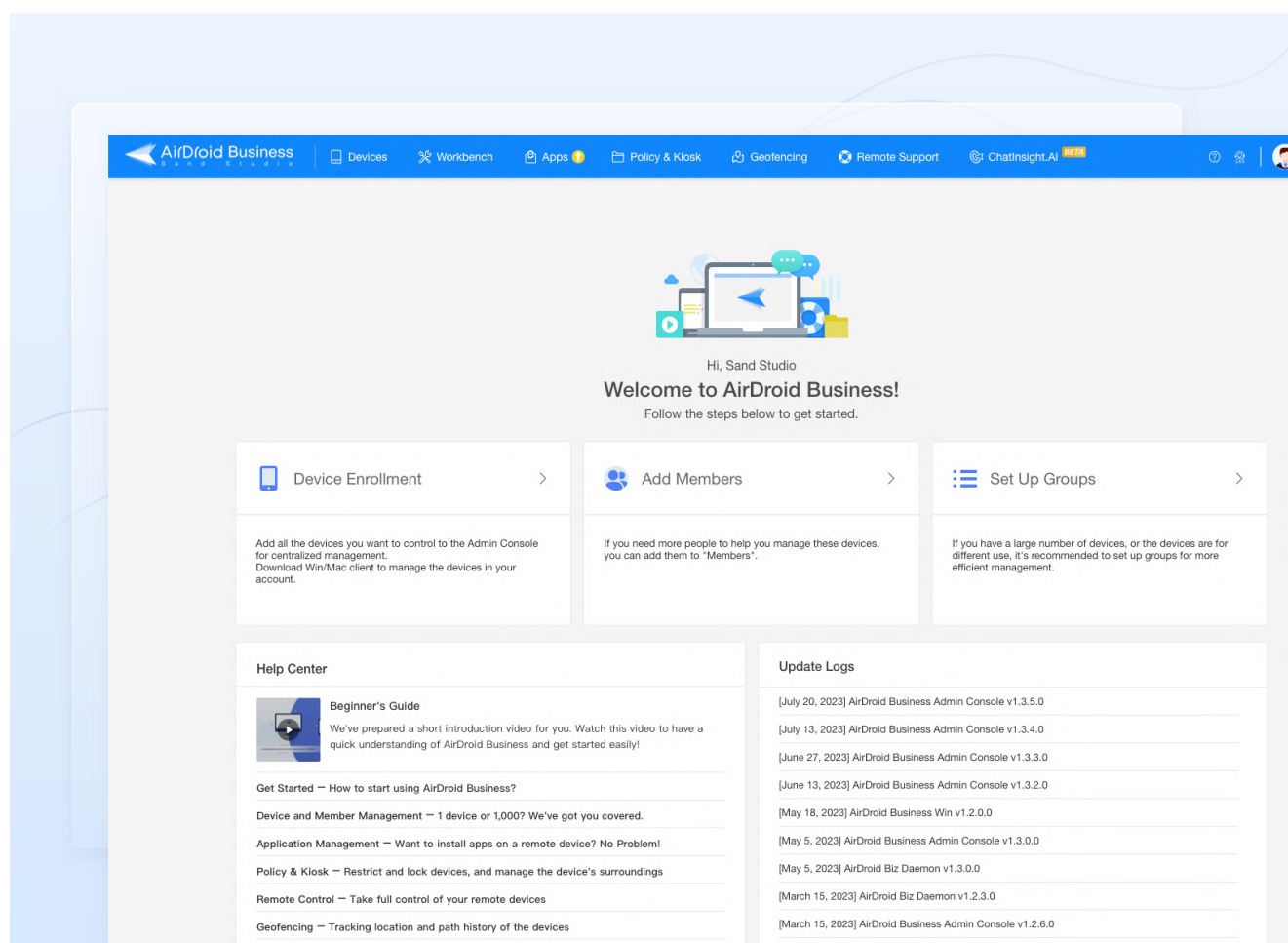
It helps business owners and IT professionals to remotely access, control, and manage both attended and unattended devices through a centralized approach. Stay up-to-date with your remote Android devices anytime anywhere. Identify potential system errors in advance and take actions to shorten troubleshooting time.



# Introducing Admin Console

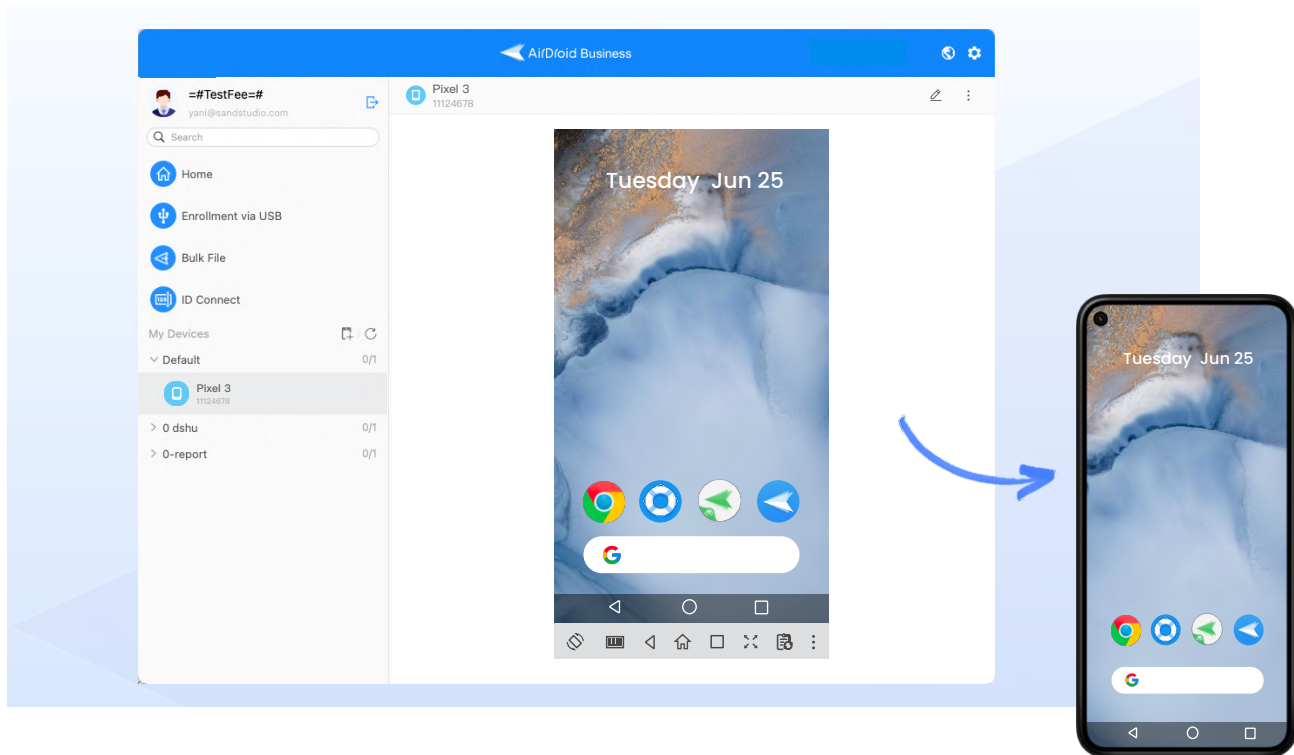
Admin Console is a cloud-based dashboard that allows IT managers or business owners to remotely access, control, and monitor their Android devices' real-time performances. After downloading Biz Daemon, the Android device management app onto the device that needs to be controlled, users will be able to view all the enrolled devices from monitoring templates and perform different remote device management tasks. These include locking devices into kiosks, remotely updating apps, and tracking device locations.

Alternatively, if you're looking to manage multiple users and devices, you can easily assign roles, permissions and categorize devices in groups. For enterprises looking for an Android MDM software, this member management feature can greatly reduce labor cost and IT workload.





# Introducing Desktop Client



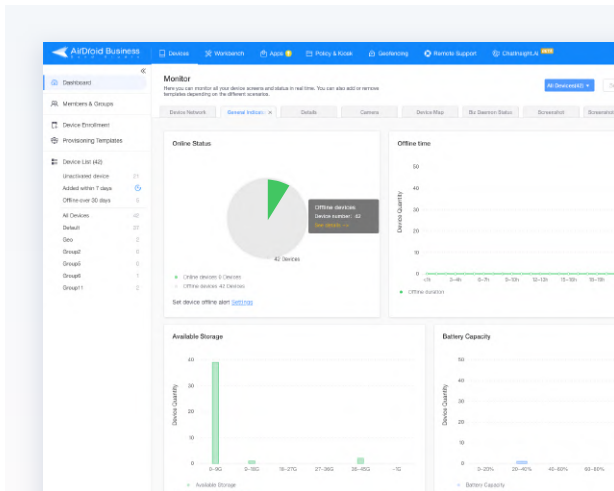
AirDroid Business Desktop Client works like an Android remote control center. This is where the majority of **unattended remote access and control** tasks happen! With Desktop Client, you'll be able to achieve:

- Access your remote camera
- Rotate your device's camera screen
- Switch to front camera
- Turn on the device's flashlight
- Refresh the camera screen
- Take screenshots of the remote camera
- Switch to full screen mode
- Modify screen display quality
- Record a video from your remote camera
- Turn on one-way audio to capture the surrounding sounds
- Use two-way file transfer
- Remotely view your device's screen
- Remotely record your device's screen
- Use remote keyboard
- Adjust your device's volume
- Power on and off
- Remotely lock or unlock your device's screen
- Remotely swipe up and down your device's screen
- Initiate voice calls during your remote control session

# Remote Monitoring Templates

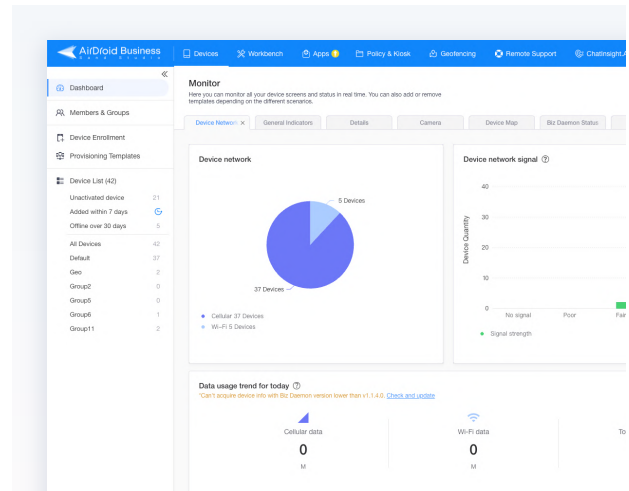
## Customized Monitoring Templates

Remotely monitor all your devices' real-time performances. Use 8 different monitoring templates to identify malfunction or hardware issues in advance.



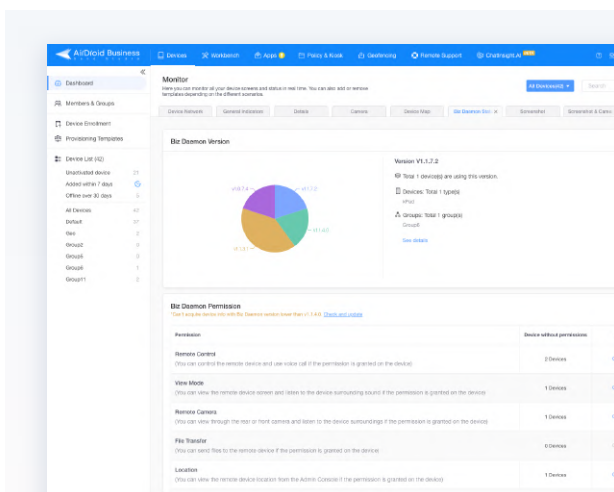
### General Indicators

Monitor your device's online status, offline time, available storage, battery capacity, charging status, and temperature



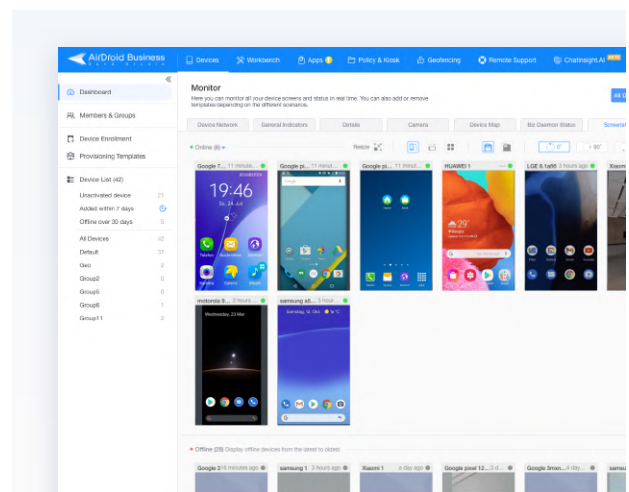
### Device Network

Monitor your device's network, signal strength, and data usage to avoid unnecessary and expensive data cost



### BizDaemon Status

Keep your bizDaemon version up-to-date and ensure all permissions are turned on for remote access and remote control



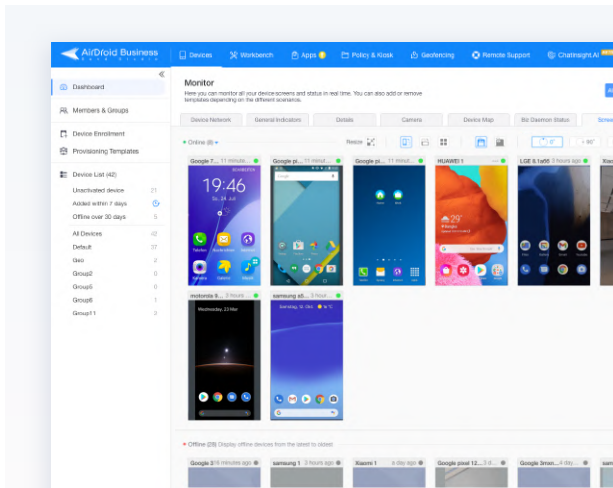
### Screenshot & Camera View

Monitor your device's screenshot and camera view simultaneously for streamlined operations and workflows

# Remote Monitoring Templates

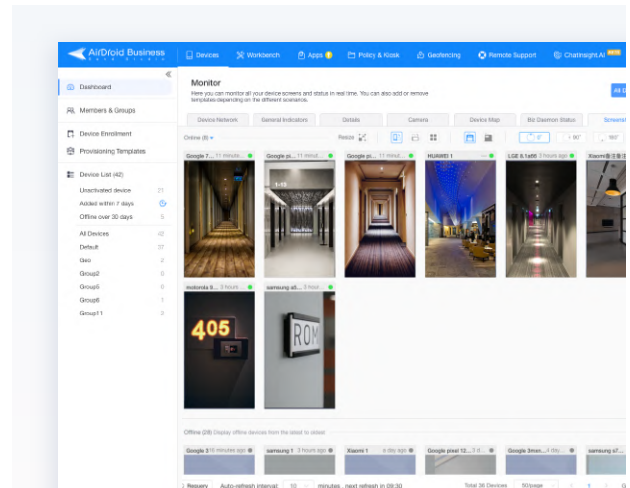
## Customized Monitoring Templates

Remotely monitor all your devices' real-time performances. Use 8 different monitoring templates to identify malfunction or hardware issues in advance.



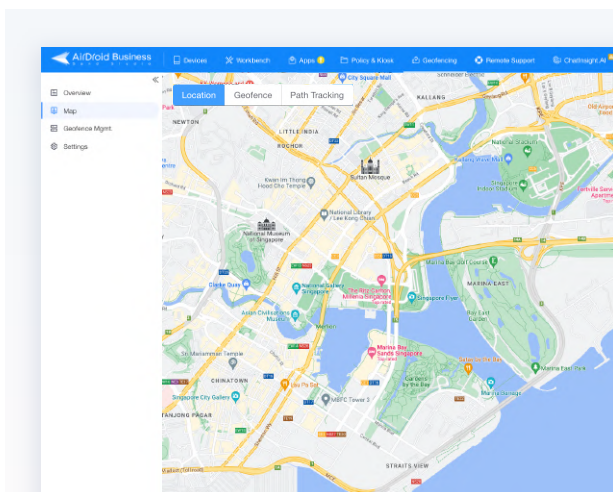
### Screenshot View

Monitor your device's screenshot to ensure your content is displaying properly



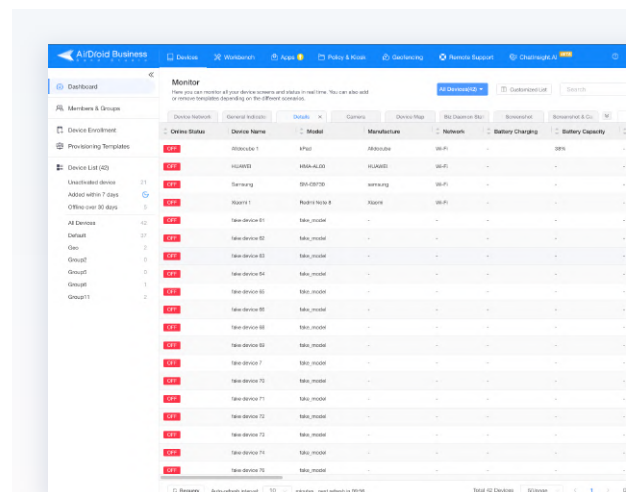
### Camera View

Check your device's camera view to monitor population and security of your device's surroundings



### Location Map

Locate all of your device's location in one view and identify abnormal device activities more efficiently



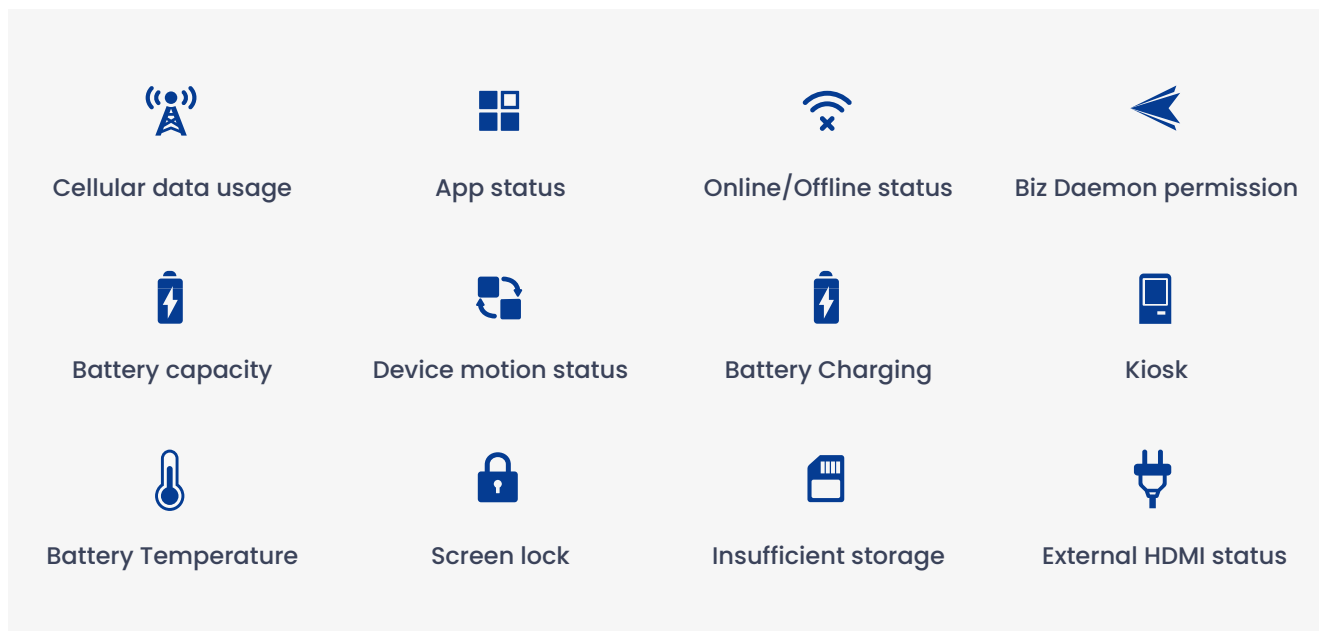
### Device Details

Obtain detailed performance information about your device, including network status, root status, device name, IMEI, model type, and more

# Alerts & Workflows

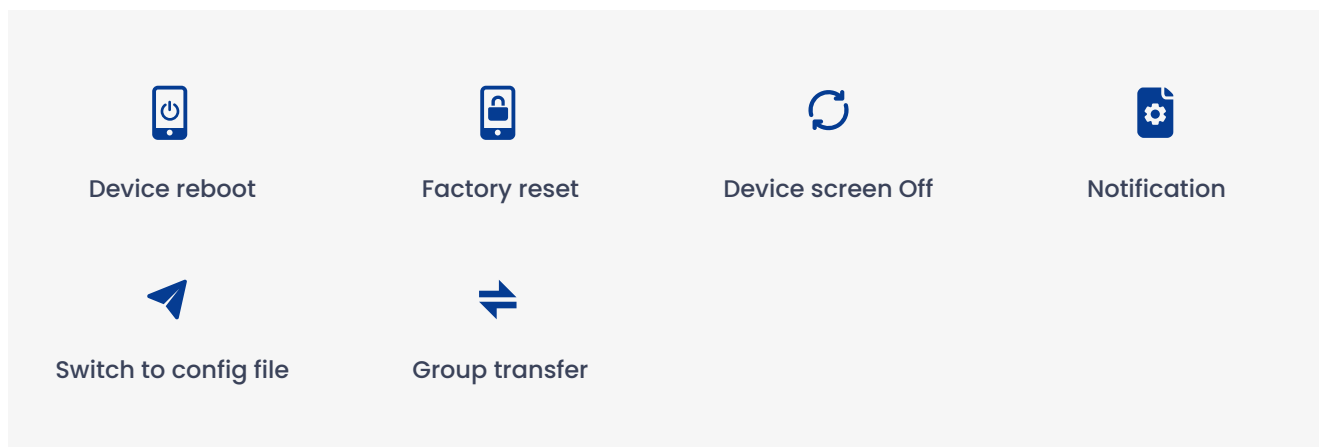
## Alerts

Set alerts for abnormal activities and shorten response time, thus improving production efficiency. There are 12 types of alerts to choose from:



## Workflows

Use in conjunction with Alerts/Geofence. Automatically execute various actions when there is irregular behaviour on your device that triggers your custom alert or scheduled task.



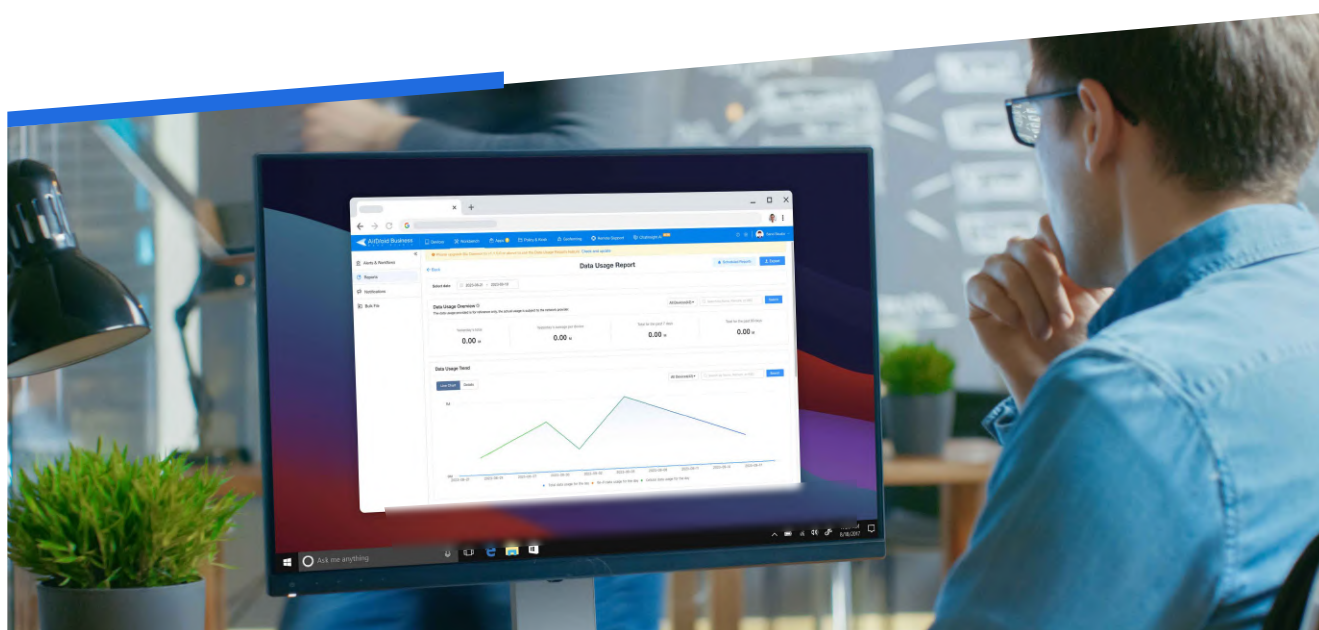


## 9 Types of Reports to Choose from

Get a granular look of your device performances in one screen view

### Data usage

- Overview: Historic statistics dated back to one year
- Data Trending Chart: Divided by WiFi and cellular usage
- Top 10 Consuming Apps: Identify abnormal app activities



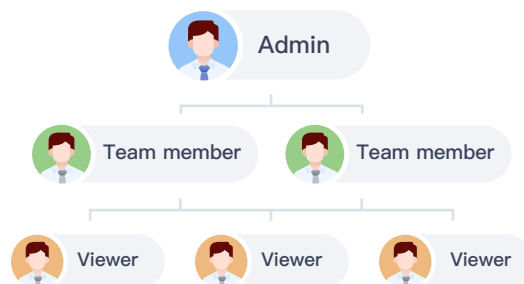
- Device list with detailed info
- Admin & member account activity logs
- Application versions
- Device Availability
- Device health indicators (coming soon)
- Screen-on time (coming soon)
- Remote connection history (coming soon)
- SIM card status (coming soon)

# Member Management

Assign different roles and device permission to your team to further protect your device's data security.

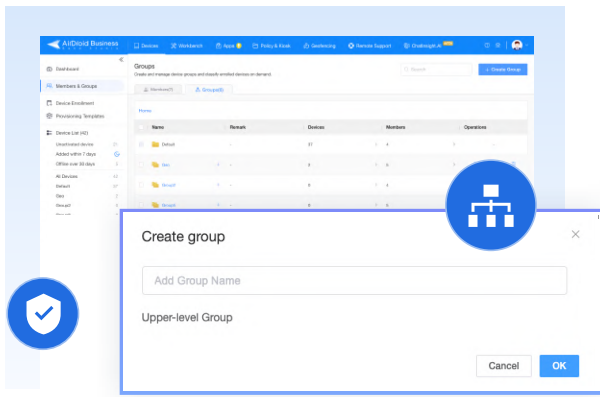
There are three different roles to assign:

- **Admin:** An Admin has full accessibility to manage and control all enrolled devices in Admin Console
- **Team member:** A Team member can only access and manage devices assigned to him/her by Admins
- **Viewer:** A Viewer has limited access to assigned devices during specific time frames. They can only use "Remote Camera" and "Remote View" Mode



Roles/Accessibility	Admin	Team Member	Viewer
Access to Devices	✓	○	○
Remote View	✓	○	○
Remote Camera	✓	○	○
Remote Control	✓	○	✗
Invite Members	✓	✗	✗

✓ Full access    ○ Limited access    ✗ No access



## Device Grouping

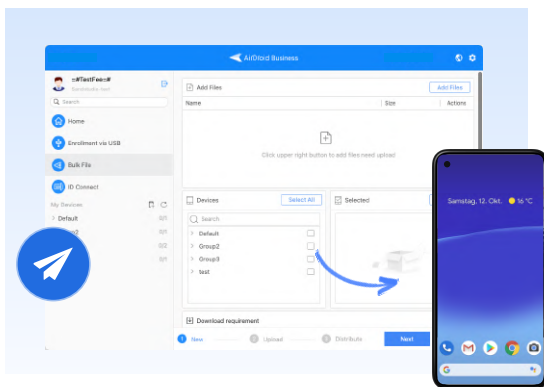
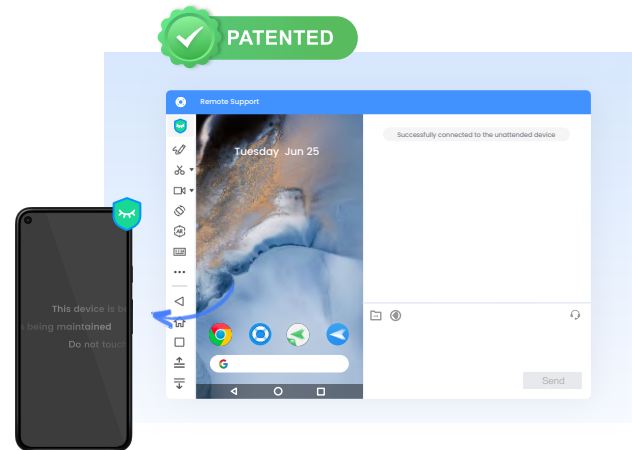
Categorize your devices in groups according to different business types or clients.

- Prevent data breach across different users
- Efficiently manage your team and devices internationally

## Unattended Remote access and control

Remotely access and control unattended Android devices from your desktop.

- Remotely view your device's screen
- Remotely lock or reset devices
- Remotely update or uninstall apps



## Batch Mode

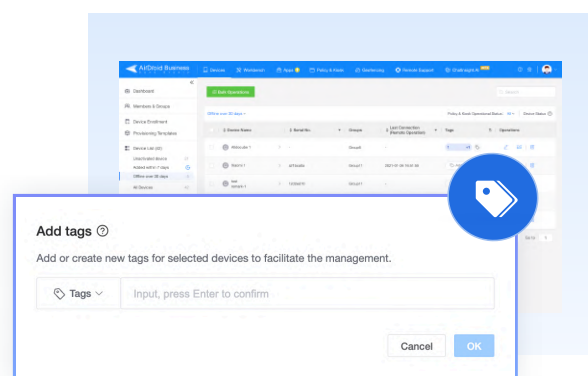
Easily transfer and delete files across multiple devices all at once.

- Push group notifications to specific devices or device groups

## Tags

You can add tags to your devices for better management.

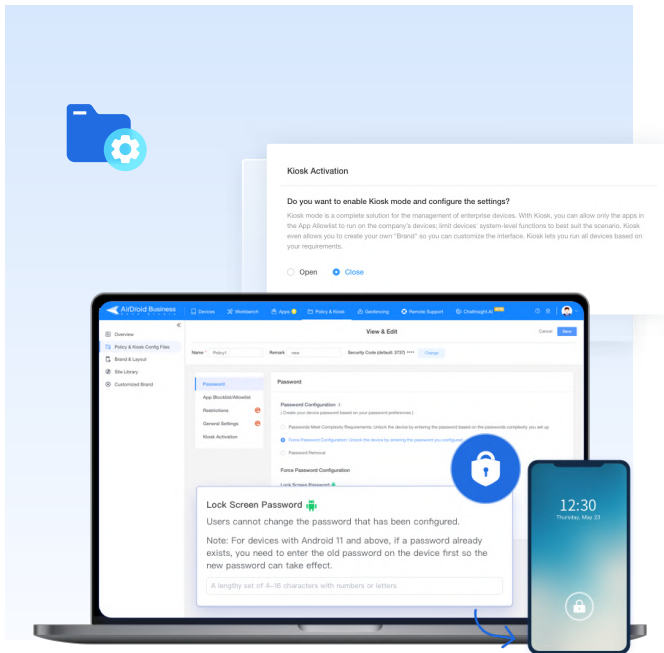
- Tagging enables easy identification of devices within the console
- Using the filter to view the relevant list of devices that have added tags



## Policy

Policy offers a broad array of settings that enable you to impose restrictions on managed devices, enhancing your company's security and safeguarding its data.

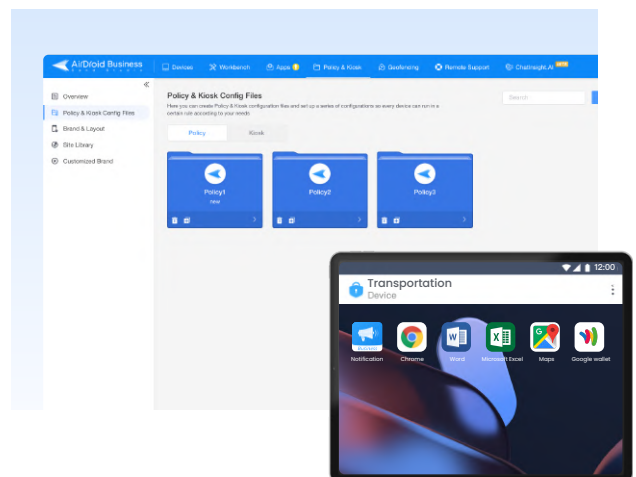
- Password management: password complexity set up, force password configuration, or password removal
- App allowlist/blocklist: allow only trusted apps to be run/block certain apps from being installed or used on managed devices
- Device restrictions: Functionality limits (sound/video recording, prevent screen capture), Safety (factory reset, FRP, developer mode, safe mode, USB connection), Compliance management, Apps(allow unknown sources/uninstall app, app permission settings), Tethering(disable hotspots, etc)
- General settings: APN, VPN, credential, device language, time zone
- Kiosk activation: enable/disable kiosk mode
- Calls: setting SIM card binding, allowed numbers, and importing contacts.



## Kiosk Mode

Kiosk Mode is a device lockdown mechanism that limits your users usage with Android devices or tablets. You can:

- Lock apps into single-app/multi-app mode
- Block websites or lockdown browser
- Limit device peripheral settings(WiFi, Hotspot, 4G, etc.)
- Customize the interface of your device for brand identity

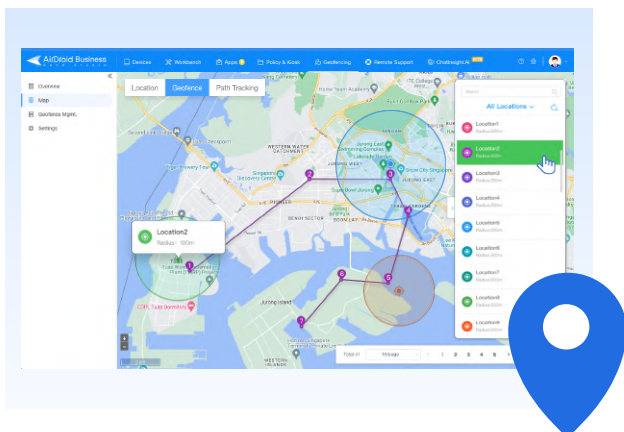
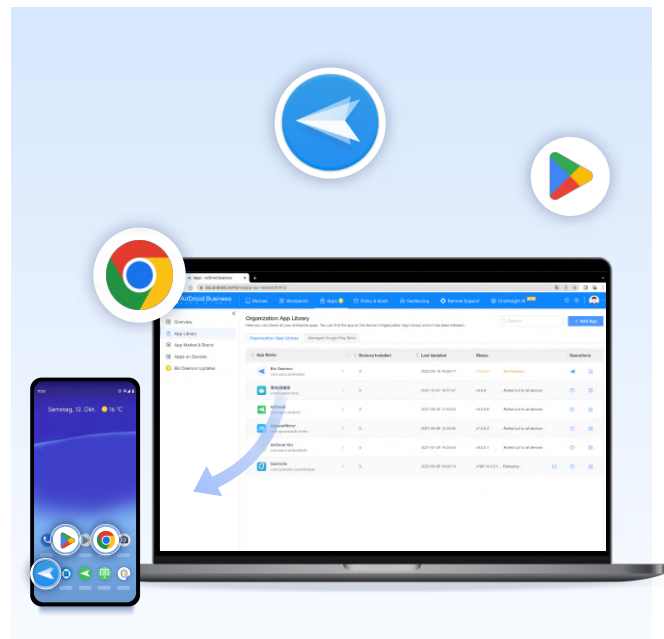




## Application Management Services(AMS)

AMS offers flexible methods for businesses to remotely update, install, or uninstall apps on Android devices. You can use:

- Google Play Store – Manage apps on your corporate-owned GMS devices
- Enterprise app store – Create your own app library for internal use
- Staged Rollouts–Update apps by percentage, locations or device groups to prevent total breakdown
- Test Release–Run tests before publish official updates to avoid unexpected errors
- Scheduled Release–Schedule specific time for app updates to avoid business hours
- Forced Installation–Remotely install or replace broken apps without manual intervention



## Geofence

Geofence allows businesses to track all of the deployed devices for higher productivity and efficiency. You can:

- Track the device's location
- Track the device's path history
- Create digital geofence and workflows
- Set up notifications when workflows are triggered

## Try it for free

Get your 14-day free trial now. No credit card or setup fees needed.

[SIGN UP HERE](#)

## Get the help you need

Let our consultants give you the best guidance based on your requirements.

[CONTACT US](#)



## Digital Signage

"Remotely auto update and uninstall apps without manual interference"

### Scenario

Hotel California introduces digital display boards in their lobby and reception area. They use digital signage to showcase their hotels, special offers and events. They even created their own hotel booking app to engage more with their customers. Now, if today they decided to update their in-house apps and apply these changes in every digital signage they've deployed across the whole country, how can they accomplish this?

### Solution

With basic remote control and AMS, businesses can easily update/uninstall apps or reboot unattended Android devices in a less costly way.

### Other industries

Airlines and Airports, Casinos, Restaurants, Healthcare, Education, Banking, and more.



## IT Services

"Remotely view, control , and troubleshoot unlimited devices more efficiently"

### Scenario

FutureTech Inc. is an IT company that offers software services to SafeAlways Insurance. SafeAlways distributes Android tablets to their sales so they can showcase their products to their customers and close deals more efficiently. When FutureTech published a new app version on SafeAlways' Android tablets, there was an error message. And now IT support agents want to replace broken apps on all the unattended devices, how can this be done?

### Solution

An IT professional at FutureTech navigates to AMS and then App Library. He selects the App and device group, then runs Forced Installation to replace the broken apps on all unattended devices from SafeAlways right away.

(Note: For GMS devices, the IT professional can also push the apps silently via the Managed Google Play Store)

IT professionals can further use Kiosk Mode to lockdown specific applications on devices, and even configure Wi-Fi settings to reduce workload and improve productivity.



## Logistics

Remotely lock devices from frequent user misuse and data cost

### Scenario

Evergreen Logistics dispatched several Android tablets to their drivers and doesn't want employees to use other non-work related apps and websites. How should the company prevent these device misuse from happening so frequently?

### Solution

By using Kiosk Mode, businesses can lockdown applications on their Android tablets. Drivers are only allowed to use company-owned apps at work. Additionally, owners can block websites such as YouTube and Facebook on the tablets so drivers won't be able to access these pages and waste unnecessary data cost. This way, even your employee with zero IT background won't have any trouble using the device at work.

With the growing demands for touchless delivery, many logistics companies are now implementing mobile device management solutions to minimize IT workload and save operational costs.



## Our Customers



## Follow the steps below to start using AirDroid Business

- 1 Get your 14-day FREE Trial [HERE](#) (No credit card required).
- 2 Verify your email address
- 3 Complete your device enrollment

\*If you don't find our welcome letter in your inbox, remember to check your Spam or Trash folder.

\*Please note it's NECESSARY to complete binding your devices before you can start remotely managing your devices.

### ? Resources

- [How to enroll my devices?](#)
- [AirDroid Business Help Center](#)

Website: [www.airdroid.com/business](http://www.airdroid.com/business)

Sales inquiry: [sales@airdroid.com](mailto:sales@airdroid.com)

Customer Support: [success@airdroid.com](mailto:success@airdroid.com)



SCAN ME

