AirDroid Business
Sand Studio

The Beginner's Guide to AirDroid Business

AirDroid Business MDM Solution for SMBs & Enterprises

CONTENTS

What is AirDroid Business?

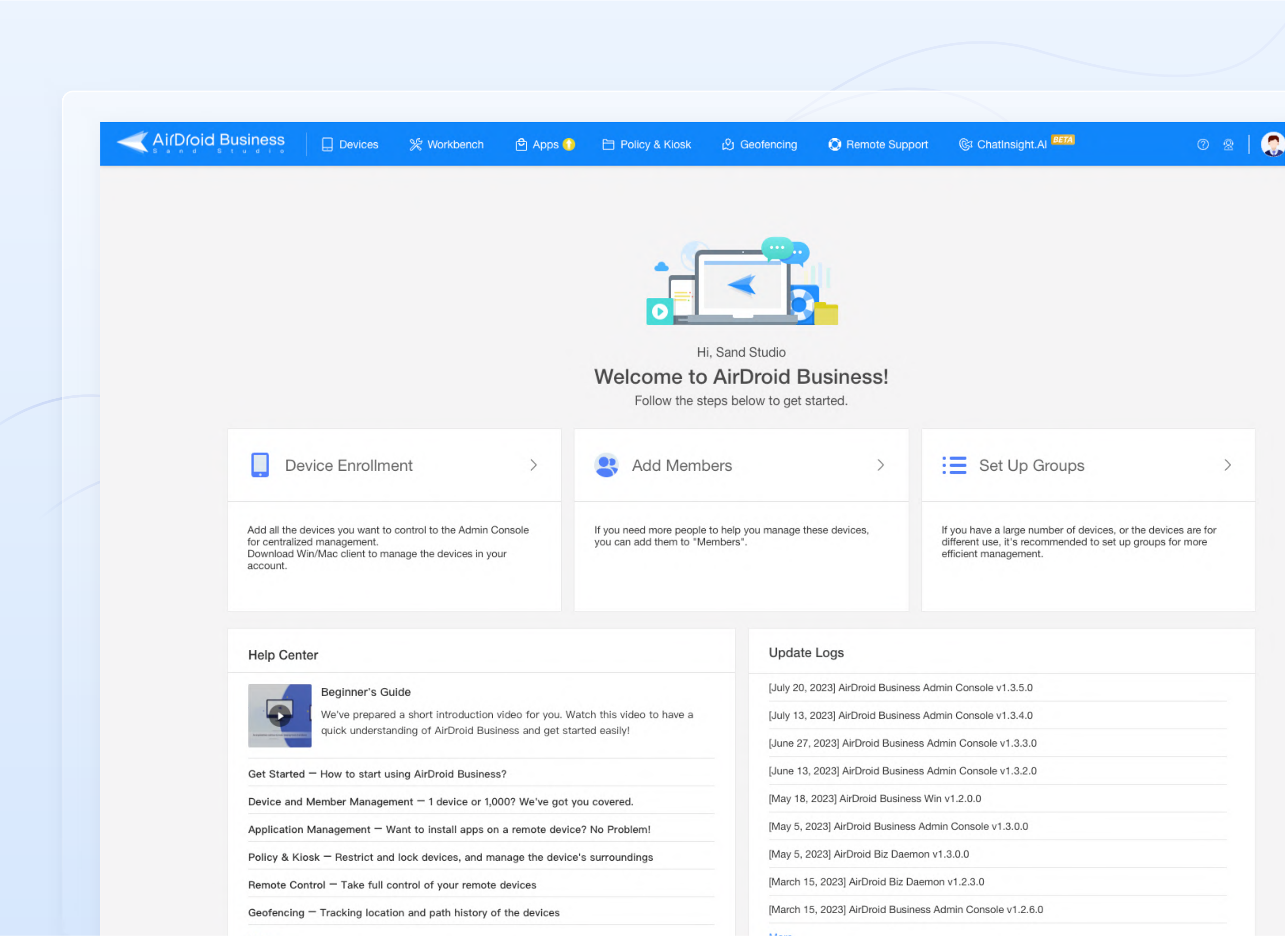
AirDroid Business is an all-in-one MDM Solution that focuses heavily on remote Android & Windows device management. It is a MDM solution specifically designed for both small businesses and enterprises who need to manage more than 10 devices on a daily basis.

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 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 devices' real-time performances. After downloading Biz Daemon, the device management app onto the Android or Windows 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 or Windows MDM software, this member management feature can greatly reduce labor cost and IT workload.



Hi, Sand Studio

Welcome to AirDroid Business!

Follow the steps below to get started.

Device Enrollment

Add all the devices you want to control to the Admin Console for centralized management.
Download Win/Mac client to manage the devices in your account.

Add Members

If you need more people to help you manage these devices, you can add them to "Members".

Set Up Groups

If you have a large number of devices, or the devices are for different use, it's recommended to set up groups for more efficient management.

Help Center

Beginner's Guide

We've prepared a short introduction video for you. Watch this video to have a quick understanding of AirDroid Business and get started easily!

Get Started — How to start using AirDroid Business?

Device and Member Management — 1 device or 1,000? We've got you covered.

Application Management — Want to install apps on a remote device? No Problem!

Policy & Kiosk — Restrict and lock devices, and manage the device's surroundings

Remote Control — Take full control of your remote devices

Geofencing — Tracking location and path history of the devices

Update Logs

[July 20, 2023] AirDroid Business Admin Console v1.3.5.0

[July 13, 2023] AirDroid Business Admin Console v1.3.4.0

[June 27, 2023] AirDroid Business Admin Console v1.3.3.0

[June 13, 2023] AirDroid Business Admin Console v1.3.2.0

[May 18, 2023] AirDroid Business Win v1.2.0.0

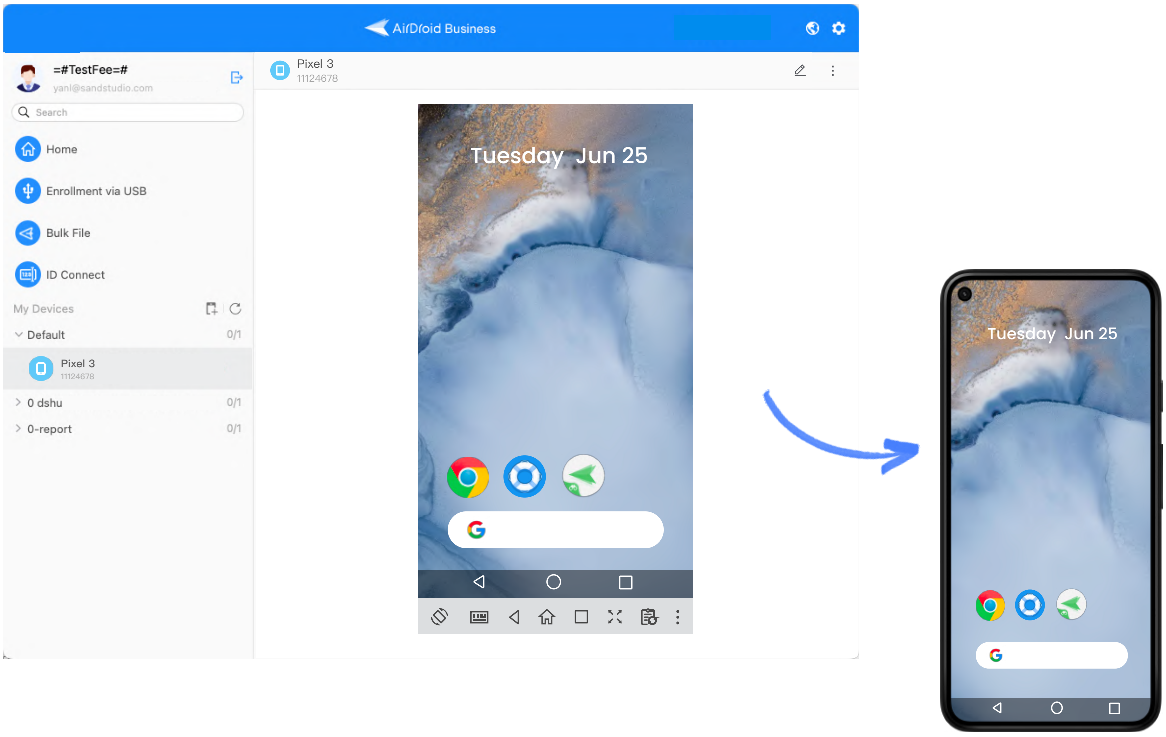
[May 5, 2023] AirDroid Business Admin Console v1.3.0.0

[May 5, 2023] AirDroid Biz Daemon v1.3.0.0

[March 15, 2023] AirDroid Biz Daemon v1.2.3.0

[March 15, 2023] AirDroid Business Admin Console v1.2.6.0

Introducing Desktop Client



AirDroid Business Desktop Client works like a device 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:

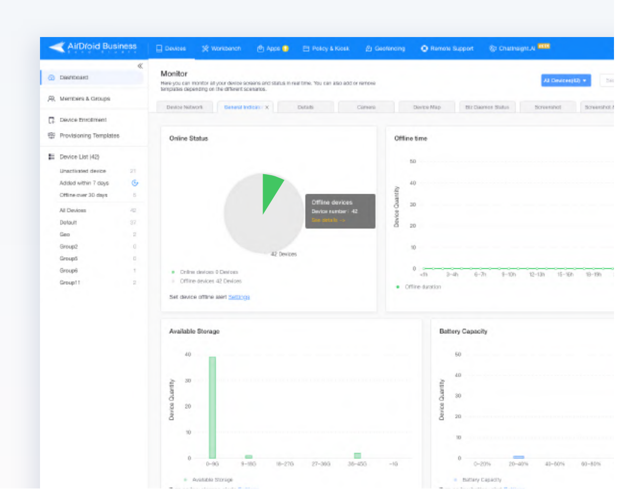
- Access your remote camera
- Rotate your device's camera screen
- Switch to front camera
- Turn on the device's flashlight
- Refresh the camera screen
- Take screenshots of the remote camera
- Switch to full screen mode
- Modify screen display quality
- Record a video from vour remote camera
- Turn 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 vour device's screen
- Initiate voice calls during your remote control session

Remote Monitoring Templates

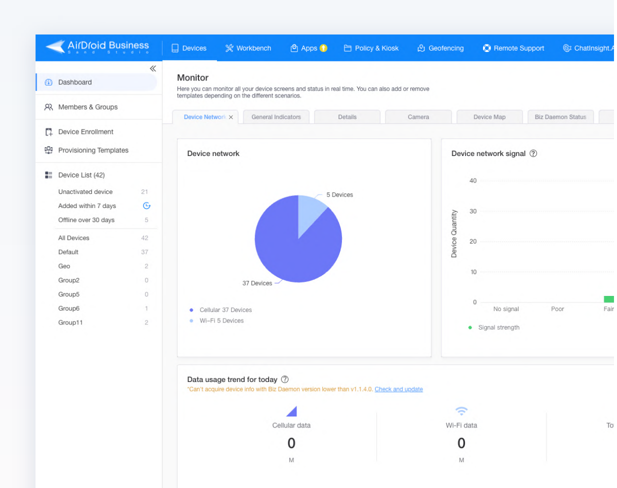
Customized Monitoring Templates

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



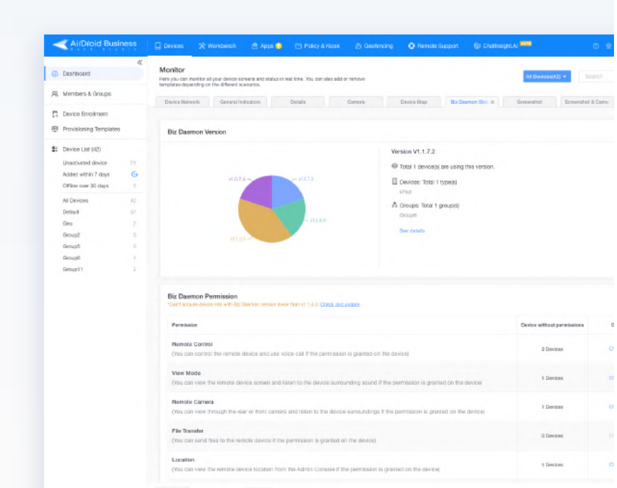
General Indicators

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



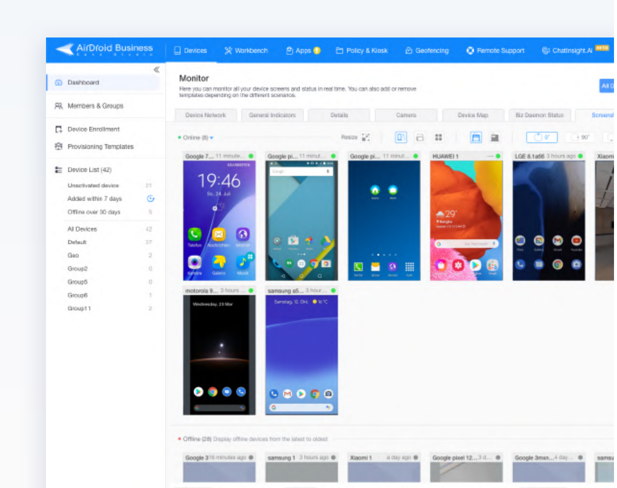
Device Network

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



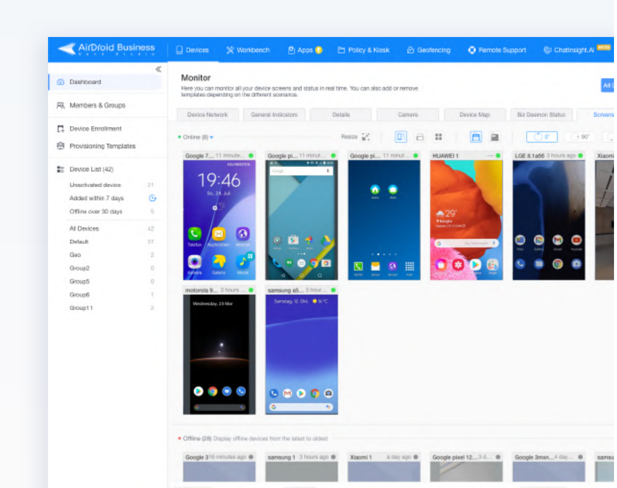
Screenshot & Camera View

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

Remote Monitoring Templates

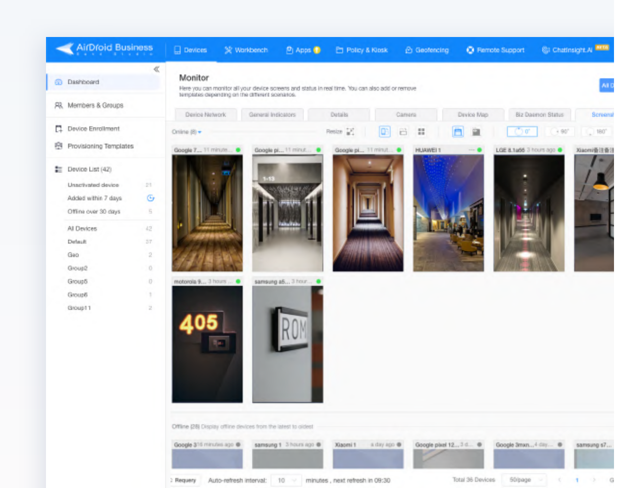
Customized Monitoring Templates

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



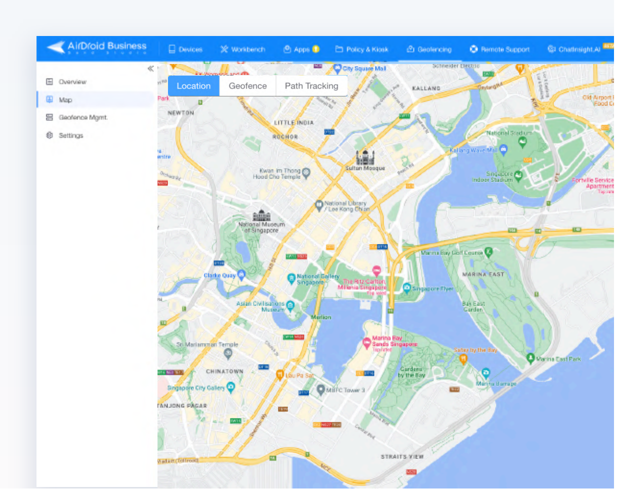
Screenshot View

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



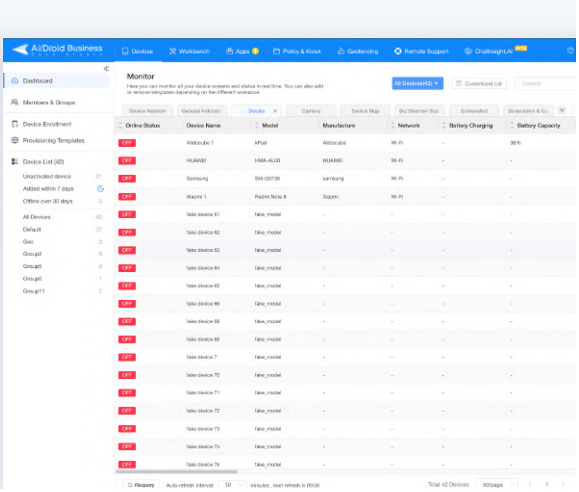
Camera View

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



Monitor

Here you can monitor all your device screens and status in real time. You can also add or remove templates depending on the different scenarios.

Online Status	Device Name	Model	Manufacture	Network	Battery Charging	Battery Capacity
OFF	Alldocube 1	iPad	Alldocube	Wi-Fi	-	38%
OFF	HUAWEI	HMA-AL00	HUAWEI	Wi-Fi	-	-
OFF	Samsung	SM-G9730	samsung	Wi-Fi	-	-
OFF	Xiaomi 1	Redmi Note 8	Xiaomi	Wi-Fi	-	-
OFF	fake device 61	fake_model	-	-	-	-
OFF	fake device 62	fake_model	-	-	-	-
OFF	fake device 63	fake_model	-	-	-	-
OFF	fake device 64	fake_model	-	-	-	-
OFF	fake device 65	fake_model	-	-	-	-
OFF	fake device 66	fake_model	-	-	-	-
OFF	fake device 68	fake_model	-	-	-	-
OFF	fake device 69	fake_model	-	-	-	-
OFF	fake device 7	fake_model	-	-	-	-
OFF	fake device 70	fake_model	-	-	-	-
OFF	fake device 71	fake_model	-	-	-	-
OFF	fake device 72	fake_model	-	-	-	-
OFF	fake device 73	fake_model	-	-	-	-
OFF	fake device 74	fake_model	-	-	-	-
OFF	fake device 76	fake_model	-	-	-	-

Requery Auto-refresh interval 10 minutes , next refresh in 09:56 Total 42 Devices 50/page 1

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:

- Cellular data usage
- App status
- Online/Offline status
- Biz Daemon permission
- Battery capacity
- Device motion status
- Battery Charging
- Kiosk
- Battery Temperature
- Screen lock
- Insufficient storage
- External HDMI status

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.

- Device reboot
- Factory reset
- Device screen Off
- Notification
- Switch to config file
- Group transfer

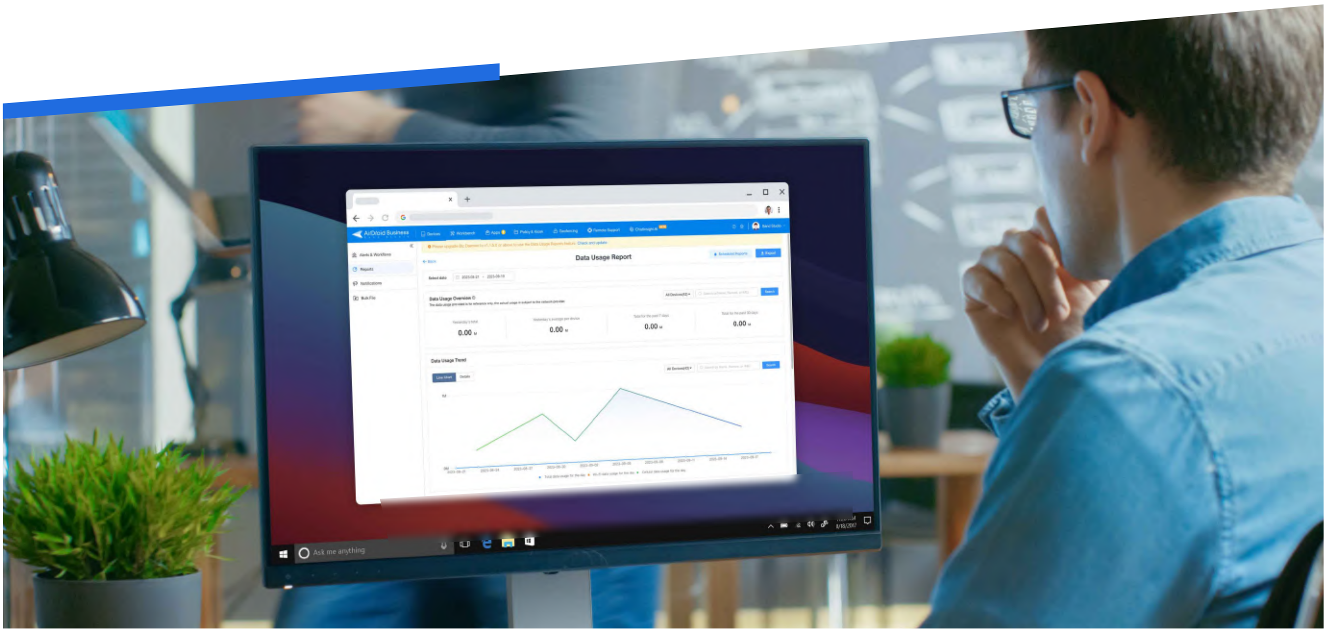
Reporting

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



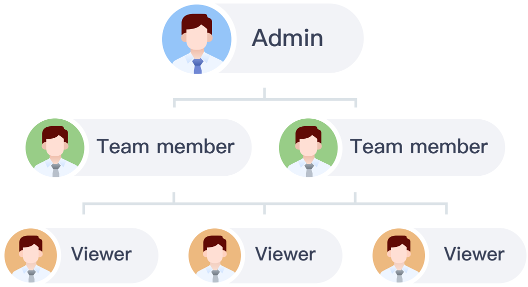
- Device list with detailed info
- Admin & member account activity logs
- Application versions
- Device Availability
- Screen-on time
- Remote connection history
- Device health indicators (coming soon)
- SIM card status (coming soon)

Member Management

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

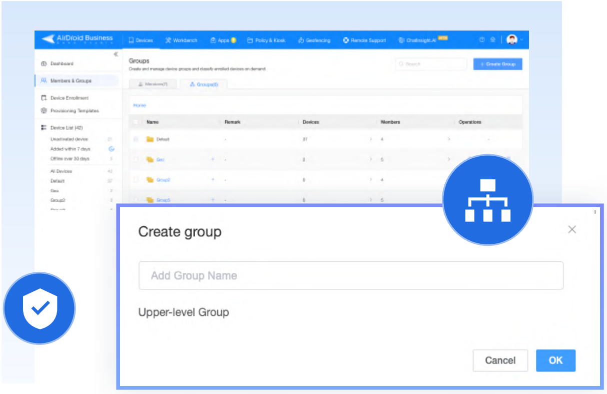
There are three different roles to assign:

- **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



Create group

Add Group Name

Upper-level Group

Device Grouping

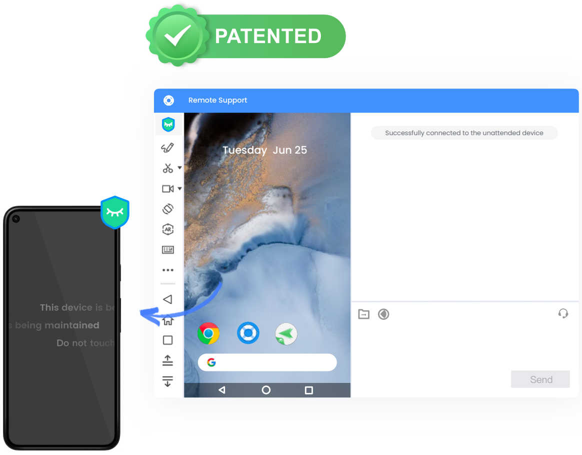
Categorize your devices in groups according to different business types or clients.

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

Unattended Remote access and control

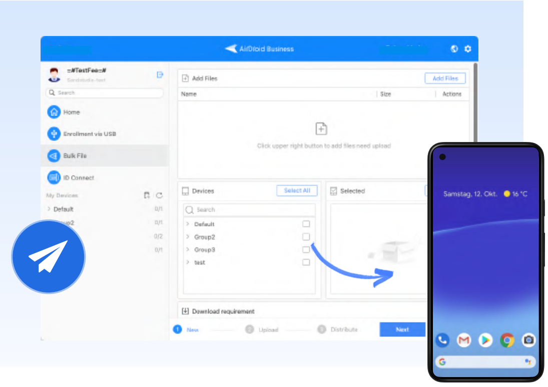
Remotely access and control unattended Android devices from your desktop.

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



Successfully connected to the unattended device

This device is being maintained
Do not touch



Click upper right button to add files need upload

Batch Mode

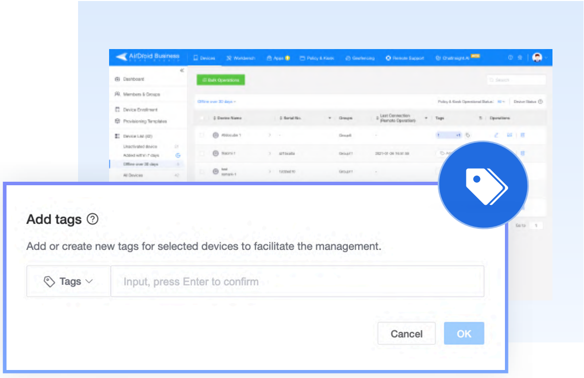
Easily transfer and delete files across multiple devices all at once.

- Push group notifications to specific devices or device groups

Tags

You can add tags to your devices for better management.

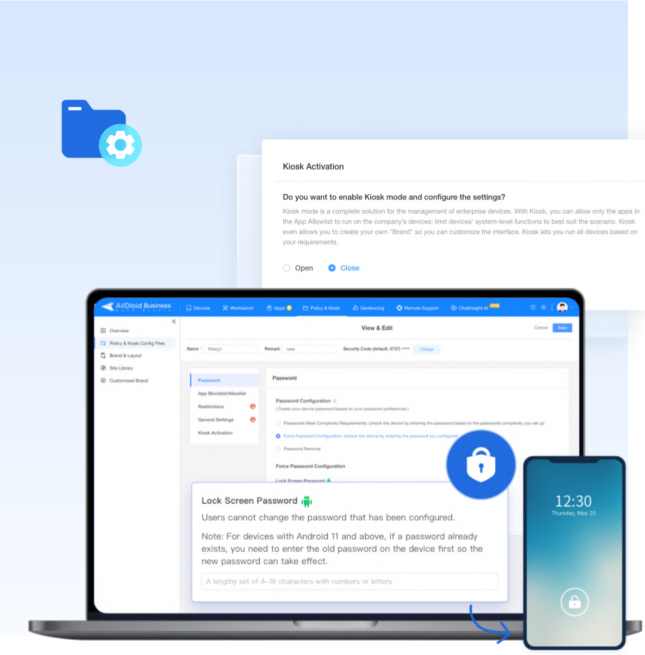
- Tagging enables easy identification of devices within the console
- Using the filter to view the relevant list of devices that have added tags



Add tags ⓘ

Add or create new tags for selected devices to facilitate the management.

Tags ⌵ Input, press Enter to confirm



Kiosk Activation

Do you want to enable Kiosk mode and configure the settings?

Kiosk mode is a complete solution for the management of enterprise devices. With Kiosk, you can allow only the apps in the App Allowlist to run on the company's devices; limit devices' system-level functions to best suit the scenario. Kiosk even allows you to create your own "Brand" so you can customize the interface. Kiosk lets you run all devices based on your requirements.

○ Open ● Close

View & Edit

Remark: new

Security Code (default: 3737) ****

Password Configuration

(Create your device password based on your password preferences)

○ Passwords Meet Complexity Requirements: Unlock the device by entering the password based on the passwords complexity you set up

● Force Password Configuration: Unlock the device by entering the password you configured

○ Password Removal

Force Password Configuration

Lock Screen Password

Users cannot change the password that has been configured.

Note: For devices with Android 11 and above, if a password already exists, you need to enter the old password on the device first so the new password can take effect.

A lengthy set of 4–16 characters with numbers or letters

Policy

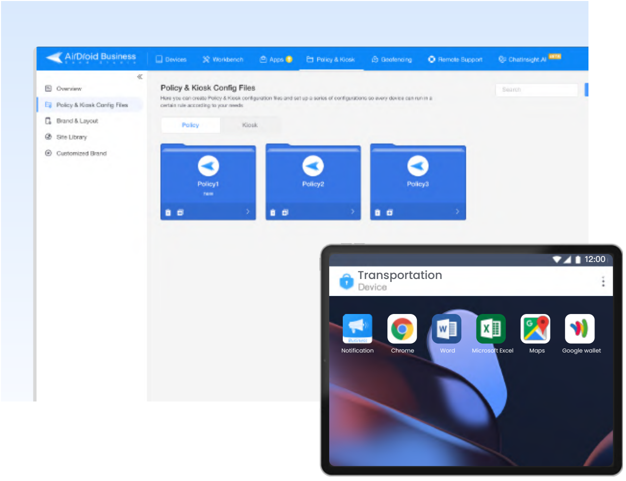
Policy offers a broad array of settings that enable you to impose restrictions on managed devices, enhancing your company's security and safeguarding its data.

- **Password management:** password complexity setup, 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
- **OEM Configuration:** Remotely configure Samsung device-specific settings by adjusting KSP(Knox Service Plugin) configurations and distributing them to devices. Enforce more granular control on Samsung devices.
- **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 the managed devices.

- Lock apps into single-app/multi-app mode
- Block websites or lockdown browser
- Customize the interface of your device for brand identity



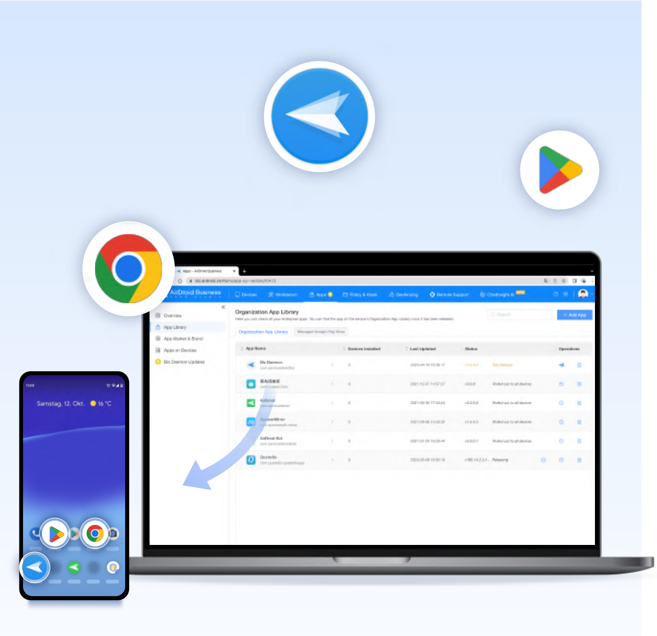
Policy & Kiosk Config Files

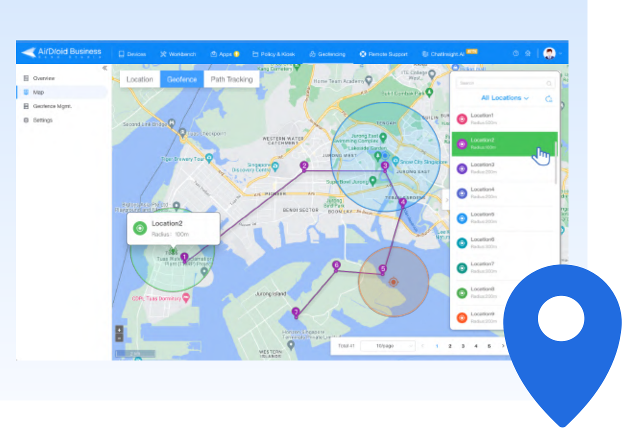
Here you can create Policy & Kiosk configuration files and set up a series of configurations so every device can run in a certain rule according to your needs

Application Management Services(AMS)

AMS offers flexible methods for businesses to remotely update, install, or uninstall apps on managed 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 installor 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

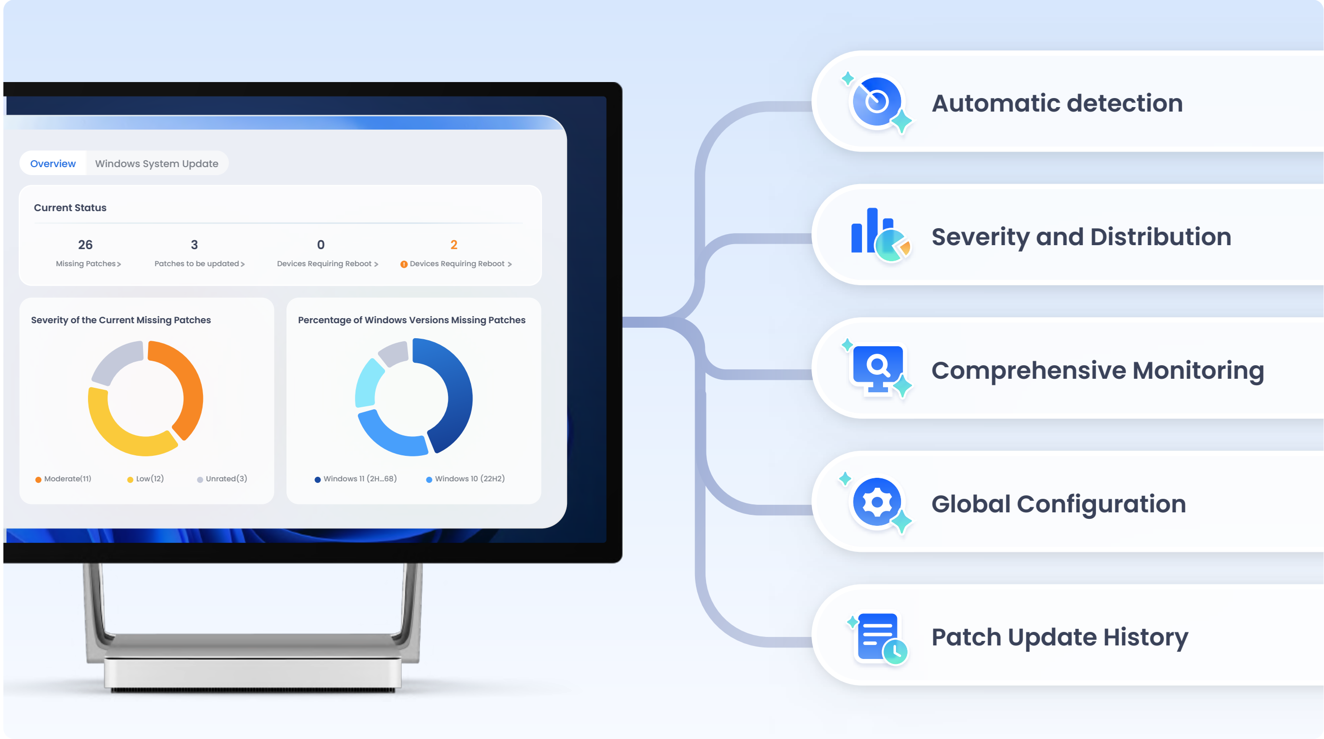
Let our consultants give you the best guidance based on your requirements.

CONTACT US

Patch Management

Patch Management feature allows IT administrators to monitor patches and deploy necessary updates from a single dashboard to ensure system security.

- **Automated Patch Detection:** Automatically detect system vulnerabilities, identifying missing, pending updates, devices pending reboot, and failed patches.
- **Severity and Distribution:** Analyze the severity levels of missing patches through charts and view their distribution across devices.
- **Comprehensive Monitoring:** Monitor patch updates across all Windows devices through device and update dimensions.
- **Global Configuration:** Configure global update rules, including synchronization intervals, installation timing, and reboot settings.
- **Patch Update History:** Review patch update history for each device.



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

MDM Solution for Industries

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 theircustomers. Now, if today they decided to update their in-house apps and apply these changes inevery digital signage they've deploved 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.

MDM Solution for Industries

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.

MDM Solution for Industries

Logistics

Remotely lock devices from frequentuser 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

interactive SOLUTIONS · Aura · the discount Vending store · esoftwaresolutions · VisionFund · TRANSTIRA LOGISTICS & TRANSPORT

Review Recognitions

Top 50 IT Management Products BEST SOFTWARE AWARDS 2024

SPRING 2025 Grid Leader

SPRING 2025 Momentum Leader

SPRING 2025 Best Support

SPRING 2025 Best Relationship

SPRING 2025 Easiest To Use

SOURCEFORGE Top Performer Winter 2024

Slashdot Users Love Us 2024

crozdesk TRUSTED VENDOR HIGH MARKET PRESENCE 2024

crozdesk QUALITY CHOICE TOP RANKED SOLUTION 2024

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

Sales inquiry: sales@airdroid.com

Customer Support: success@airdroid.com

SCAN ME

AirDroid and its related products are developed by Sand Studio. They are not sponsored, endorsed, or approved by, or affiliated or associated with Google LLC, its Android trademarks, or its Android offerings