AirDroid Business Policy & Restriction Settings

Category	Feature	Description
features only work when AirDroid Biz Daemon has the Device Owner permission on the device. Learn More		
- PASSWORD SETTINGS -		
Password Configurations		Create your device password based on your password preferences: • **Passwords meet complexity requirements:** Unlock the device by entering the password that complies with the rules you've set up. • **Force password configuration:** Unlock the device by entering the password you configured. • **Password Removal** ⚠ Devices enrolled through Android Enterprise or Zero Touch DO NOT support Force Password Configuration and Password Removal.
Password Rules	Password Complexity Setup	Establish the rules for the password to unlock the device screen. ⚠ Certain devices with Android 7.0, 7.1.1 and 7.1.2 may not take effect due to system issues.
	Minimum Password Length	Set up the minimum length requirements for your passwords; ranging from 4 numbers to 16.
	Maximum Number of Failed Attempts	If the number of password attempts exceeds the configuration number, the device will be restored to its factory settings; supports the number of attempts ranging from 4 to 16.
	Password Valid Period	Set a valid period for your passwords. You need to reset them after the expiration.
	Maximum number of reused passwords	Set the maximum number of times a password can be reused.
	Smart Lock	Users can bypass the password prompt on the device lock screen by configuring trust agents such as On-Body Detection, Trusted Device, etc. ⚠ Support devices with Android 5.0 and above. ⚠ Devices enrolled through Android Enterprise or Zero Touch are not supported. * This setting is renamed "Extended Unlock" for Android 14 and above devices.

Create Password	Forced Lock Screen Password	Users cannot change the password that has been configured. ⚠ The devices with Android 7.0 or above will need to gain Device Owner permission to take effect. ⚠ 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.
Remove Password	Password Removal	The existing password will be removed and users cannot set a new password. ⚠ The devices with Android 7.0 or above will need to gain Device Owner permission to take effect. ⚠ For devices with Android 11 and above, if a password already exists, you need to enter the old password on the device first before the removal of the password can take effect.
- APPLICATION SETTINGS -		
App Policy	App Blocklist	Apps added to the blocklist will be prohibited and cannot be used on the device.
	App Allowlist	Only apps in the allowlist can be used on the device.
- RESTRICTION SETTINGS -		
Device Functions	Camera	Allow or disable users to turn on the camera. ⚠ Support devices with Android 5.0 and above.
	Lockscreen Camera	Allow or disable users to enable the camera from the lock screen. * This will affect screenshot-related features, such as screenshots and remote controls on Dashboard. ⚠ Support devices with Android 5.0 and above.
	Microphone	Allow or disable users to enable the camera from the lock screen. ⚠ Support devices with Android 5.0 and above.
	Mandatory Storage Encryption	Apply forced encryption to the data stored on the device.
	System Update	Allow or disable users to configure updates based on their preferences when the system updates are available. Functions include: • **Auto update:** Enabling this setting will install any system updates automatically and reboot the device without asking permission from the user. • **Defer update:** This option will defer system updates for up to 30 days.

Device Functions	System Update	• **Windowed update:** This option allows you to set a maintenance time window to push out updates; insert a start and end time of the maintenance window. This ensures that the updates will be done during offbusiness hours. ⚠ Support devices with Android 6.0 and above.
Safety	Factory Reset	Allow or disable device users to initiate a factory reset; however, this does not apply to a hard reset (factory reset with hard keys). ⚠ Support devices with Android 5.0 and above.
	Factory Reset Protect	Add and select the only Google email address your devices can log in to after being factory reset. ⚠ Support devices with Android 11 and above. ⚠ This feature is unavailable for devices enrolled through Zero Touch.
	Login in Safe Mode	Allow or disable users to use safe mode to log in to the device. ⚠ Support devices with Android 7.0 and above.
	Developer Mode	Allow or disable users to access Developer mode. ⚠ Support devices with Android 5.0 and above.
	USB debugging	Allow or disable users to connect USB to enable USB debugging. ⚠ Support devices with Android 5.0 and above. ⚠ Devices enrolled through Android Enterprise or Zero Touch are not supported.
	Custom Compliance Settings	When enabled, you can customize compliance settings. The device will prioritize the compliance rules you customize. * The device will be marked as "non-compliant" when the device does not comply with the password rule in [Password]-[Rules for creating passwords]. * You can set the actions-'Disable device' or 'Erase device' - to be performed on non-compliant devices and the ececution time. ⚠ Support devices with Android 7.0 and above.
Sync & Transfer	USB file transfer	Allow or disable users to use USB to transfer files between the device and the computer. ⚠ Support devices with Android 7.0 and above.
	USB external device	Allow or disable users to connect SD cards and other devices via USB. ⚠ Support devices with Android 5.0 and above.

Users and Accounts	Allow adding/ deleting accounts	Allow or disable users to add/delete accounts for devices. ⚠ Support devices with Android 5.0 and above.
	Allow adding/ deleting Google accounts	Allow or disable users to add/delete accounts for devices ⚠ Support devices with Android 5.0 and above.
Apps	Allow unknown sources	Once disabled, users are not allowed to install any apps from unknown sources*. However, you still can distribute and install apps via AMS. * Apps from unknown sources: apps coming from a third-party source or an APK file. ⚠ Support devices with Android 7.0 and above.
	Uninstall app	Allow or disable users to uninstall apps on the devices. ⚠ Support devices with Android 7.0 and above.
	App Permissions Management	You can set a default runtime permission for apps here. When the apps on your devices request permissions, they will respond according to your customized permission rules. ⚠ Support devices with Android 6.0 and above.
	In-App Browser	Allow or disable users' access to websites within applications. You can configure to allow/disallow specified applications from using "In-App Browser" functionality. ⚠ Support devices with Android 6.0 and above.
Network & Roaming	Airplane mode	Allow or disable users to activate airplane mode. ⚠ Support devices with Android 9.0 and above.
	Wi-Fi Status	You can choose whether to keep your device's Wi-Fi ON/OFF. * If you choose to keep your device's Wi-Fi off, it will be completely disconnected from the internet until connecting it to an Ethernet cable or inserting a SIM card. ⚠ Devices enrolled through Android Enterprise or Zero Touch on Android 10.0 and above are not supported
	Select Wi-Fi Settings	You can choose to add multiple Wi-Fi networks to your settings, and select a maximum of six between these Wi-Fi networks. By default, the system connects to the Wi-Fi networks in the order you select. ⚠ Devices enrolled through Android Enterprise or Zero Touch on Android 10.0 and above are not supported
	Delete the Wi-Fi settings applied on the devices	When this option is enabled, unselecting or switching Wi-Fi settings will delete the Wi-Fi settings applied on the devices. ⚠ Devices enrolled through Android Enterprise or Zero Touch on Android 10.0 and above are not supported

Device Connectivity	Android Beam	Allow or disable users to use the Android Beam feature. ⚠ Support devices with Android 5.1 and above.
	Bluetooth	Bluetooth Status. Allows options: Keep Enabled/Keep Disables. ⚠ Devices enrolled in Android Enterprise or Zero Touch on Android 13.0 and above are not supported
Tethering	Network Sharing	Allow or disable users to share the network, such as Hotspot/ Bluetooth/USB. ⚠ Support devices with Android 5.0 and above.
	Hotspot	You can choose to add multiple hotspot options to your settings. This will allow you to choose and switch between the options you've added and apply to your device. ⚠ Only available for Android 8.0 and lower.
Notifications	Do Not Disturb Settings	Allow users to configure Do Not Disturb Settings. Users can adjust it to Keep Enabled or Keep Disabled. ⚠ Available to devices running Android 6.0 and above ⚠ Devices enrolled through Android Enterprise or Zero Touch are not supported. ⚠ The notification permission must be granted for the Biz Daemon on devices.
Calls	SIM Card Binding Settings	Activating this will bind the device to the specified ICCID(s). Please navigate to Device List to set the ICCID(s). The device can use any SIM card to make calls if not set. ⚠ The devices with Android 10.0 and above need Device Owner permission to take effect. ⚠ Requires phone permission granted to the device's Biz Daemon.
	Allowed Numbers	If no allowed number is set, the device can receive and make any calls. To customize the phone allowlist for each device, select Restrict incoming calls/Restrict outgoing calls and then set it in Device List. ⚠ The feature is only effective when the device is granted permissions for Phone and Call Log. ⚠ Certain devices with Android 10.0 and above require the Device Owner permission for this feature.
	Contacts	After the contacts are sent, the contacts on the device will be updated with the ones that were sent.
Location	Location Settings	The GPS Status of the device can be configured when this option is enabled.

Date & Time	Time Zone	You can set and lock the time zone of a device. ⚠ Devices with Android 8.0 and 8.1 are not supported. ⚠ The devices with Android 9.0 or above will need to gain Device Owner permission to take effect. ⚠ Devices enrolled through Android Enterprise or Zero Touch on Android 9.0 and above are not supported.
	Change Date/Time	Allow users to modify the time and date settings on the device. ⚠ Support devices with Android 9.0 and above.
Display	Screen Timeout	Use this setting to keep the device awake, or set the duration of idle time before the device gets put to sleep. Options include 15s, 30s, 1 min, 2 min, 5 min, 10 min, 30 min, or Keep Awake.
	Allow to adjust Screen Timeout	Allow or disable users to adjust device screen timeout.
	Allow to adjust Screen Brightness	Allow users to change the screen brightness from the notification center.
	Screen Brightness	You can set the device screen to a fixed brightness.
Others	Disable Power Menu	Disable power menu options when long pressing the "Power" button, this will hide the Power Off menu when users press on the Power button. * This does not disable the Power Off function completely, the menu is only hidden. ⚠ It may not take effect after setting on some of the devices with Android 9.0 and above.
- GENERAL SETTINGS -		
General Settings	APN settings	Select and configure the APN settings for the device. ⚠ Support devices with Android 9.0 and above. ⚠ Devices enrolled through Android Enterprise or Zero Touch are not supported.
	VPN settings	Select the VPN for the "Always-on VPN" feature * You must install the VPN you selected, and the VPN must support the always-on feature (ensure all connections automatically route through the VPN). Your device will be connected to a regular Internet connection if there is an issue with the VPN. ⚠ Support devices with Android 10.0 and above.
		Lock down VPN Enable to force your devices to only connect to the Internet through the selected VPN. ⚠ Support devices with Android 10.0 and above.

General Settings	Credential settings	Add and select the credential to be installed for safer access to the organization's data from managed devices. * To install credentials on devices running Android 9 and above, please go to [Password] - [Password Configuration] to set a password first before issuing a credential. ⚠ Support devices with Android 7.0 and above. ⚠ This feature is unavailable for Android 7.0 devices enrolled through Android Enterprise or Zero Touch.
	Device Language	Select the desired language for the device. * Language change goes into effect immediately with the devices enrolled only by "Enrollment via USB". For other enrollment methods, please reboot the devices to take effect after the language setting. * Your devices must support the language you've set to, otherwise the settings will not take effect. ⚠ Support devices with Android 7.0 and above.
	Volume	You can choose to lock your device's **ringer**, **media**, and/or **alarm volumes** at a set range.
	Power Settings	Configure the power settings of a device when it is connected to a power source through a USB cable.options include: • **Power on the device when it is connected to a charger block**: When enabled, powered-off devices are automatically powered on when connecting to a charger block. ⚠ Supports Samsung devices running Knox 2.6 or higher • **Power off the device when it is disconnected from a charger block**: When enabled, powered-on devices connected to a charger block are automatically powered off when disconnecting from the block. ⚠ Supports Samsung devices running Knox 2.8 or higher ⚠ Devices enrolled through Android Enterprise, Zero Touch, or Samsung Knox Mobile Enrollment are not supported
	Wallpaper	You can customize the device's appearance by setting wallpaper on the home screen.
OEM Config		OEMConfig is a customizable configuration that can be applied to devices of various brands, enabling them to operate according to your requirements.
- KIOSK SETTINGS -		
Kiosk Mode Activation		Once Kiosk Mode is enabled, you can add applications to whitelist, control the system settings of the device, specify the exclusive brand and UI design for Kiosk, etc., so that your devices can operate according to your business requirements.
	Kiosk app allowlist	App Allowlist lets you select the apps that can be used in Kiosk Mode. Other apps will then be hidden.

Kiosk Browser		The below Kiosk Browser settings will only take effect when the Kiosk Mode is activated on the device.
	Website allowlist	Website Allowlist secures the website access under Kiosk mode. You can limit users to access the below websites only. Websites that are not on the list cannot be accessed. Kiosk Browser will be auto-activated once the site is added below. (Kiosk Browser icon will automatically show up on the main screen during Kiosk mode): • **Allow alert dialog:** Allow JavaScript alert dialogs on this website; otherwise, they will be blocked. • **Allow autofill:** allow the website to automatically fill in form field data. ⚠ Only available for devices under Android 8.0. • **Allow users to zoom website:** Allow users to zoom in and out on a webpage. • **Check existing file:** before downloading, check if the file already exists in the device; if so, the file will not be downloaded. • **Auto refresh:** If there is no operation during the set time, the web page will auto-refresh. • **Location access:** Allow websites to access the device location. Enable this option to auto grant permissions to the websites. Please enable this option only to the websites you trust. Users will receive pop-up asking for permission when it is disabled. • **Device file access:** Allow the websites to access the device files such as photos, videos and etc. Please enable this option only to the websites you trust. Users will receive pop-up asking for permission when it is disabled. • **Display desktop version as priority:** Open this URL in the desktop version site as priority. • **Text size:** Set the text size of the website (10 - 71px). • **Always start from the set page:** Every time the user taps the shortcut, it starts from the first page. * Website Allowlist only takes effect in Kiosk Browser.
	Browser Settings	Provides a variety of configuration options for you to customize your Kiosk Browser's policy and restrictions to your business needs; options include: • **Display URL bar:** Display and allow the user to navigate with the URL bar, but the input address will still be limited by the allowlist. • **Allow multiple tabs to be opened:** Allow users to open links in a new tab. • **Allow "Print" option:** Show or hide the "Print" button. ⚠ The button will be hidden for devices below Android 4.4 due to OS restrictions. • **Allow desktop website:** Allow users to switch between the desktop and the mobile websites. • **Auto page adjustment:** Adjust the web page automatically based on device screen size.

Kiosk Browser	Browser Settings	• **Always use incognito mode:** Once the user exits the browser, no data such as account password or private information left in forms will be saved. Text autofill will be disabled when this mode is turned on. • **Auto-clear cache:** Kiosk Browser cache will be cleared periodically. • **Disable back button:** The device back button will be disabled during the use of Kiosk Browser; however, users can still tap the back icon (←) on the web page. * The following settings only take effect in the Kiosk Browser. Please DO NOT add other browsers to the app allowlist.
Brand	Brand	You can select a brand you created in "Brand & Layout" to apply to your devices. This will show the corresponding wallpaper, icon size, and color when the device is under Kiosk Mode. If no brand is preselected, the device will be applied with the default interface.
Kiosk Launcher		In the Kiosk settings, you can set the single app mode, home screen and notification center in Kiosk mode according to your needs. It helps you limit user behavior on the device and provide a controlled environment.
Kiosk Launcher	Single-app Mode	You can force one application from your set of apps to run consistently, or relaunch after a time delay: • **Select an app:** You can select a default app to run. • **Delay app relaunch:** You can enter a wait time (in seconds) for the delay to relaunch the app after exiting. • **Keep running:** If you select this option and wish to exit Single-app mode later, you will need to go to the Admin Console to exit the device from Kiosk Mode.
	Home Screen	• **Use system status bar:** Allow or disable the system status bar. ⚠ Device with Android 8.0 or above can only use system default ⚠ For devices with Android 9.0 and above that AirDroid Biz Daemon has Device Owner permission. Users can access the default Notification Center after this option is enabled (go to [Kiosk Restriction]-[Other settings] to ensure the home key is enabled). • **Hide the navigation bar of the bottom screen:** The navigation bar will be hidden. • **Full-screen mode:** The device will switch to full-screen mode by hiding the navigation and status bar. • **View and switch apps:** Enable this feature to allow users to access recently used apps via floating buttons on device screens when the devices' built-in Recent Keys are disabled. * Once the full-screen mode is activated, the bottom navigation bar and the keyboard will be hidden. Swipe up from the bottom of your device to unhide if needed. All app notifications will not be displayed at the top status bar after this option is enabled.

	Notification center	By default, the default notification center is closed when the device is in the Kiosk Mode. Enabling this option allows the user to have a notification center with quick features of your choice: • **Auto-rotate:** Allow users to change the orientation of the device from the notification center. • **Flashlight:** Allow users to turn ON/OFF the flashlight from the notification center. • **View and switch apps:** Allow users to view and switch between running applications. • **Clear app cache:** Allow users to clear cache from apps, enhancing phone performance by releasing system resources. ⚠ Due to varying system or app restrictions, some apps may restart automatically. • **Allow USB notification (Beta):** Enabling this option will show the USB connection notifications. ⚠ This may not work on some devices. • **Choose notification center position:** You can choose to show it from the screen top, bottom, left or right side to access notification center. ⚠ Support devices with Android 8.0 and above.
	Display	Allow users to customize scrolling text (e.g., notifications, fault alerts) to display during device alerts or when something needs special attention.
Kiosk Restrictions		You can choose to enable Kiosk mode and configure the its device settings here.
	Cellular Data	Allow or disable users to access "Cellular Data" when in Kiosk Mode.
	Wi-Fi	Allow or disable users to access "Wi-Fi" setting when in Kiosk Mode.
	Hotspot	Allow or disable users to turn hotspot on/off when in Kiosk mode. ⚠ Only available for Android 8.0 and lower.
	Bluetooth	Allow or disable users to access the "Bluetooth" settings in Kiosk mode.
	APN Settings	Allow users to access the "APN" settings in Kiosk mode ⚠ Devices enrolled through Android Enterprise or Zero Touch are not supported.

Kiosk Restrictions	Display	• **Lock display orientation (tablets only):** This will allow you to lock your device screen in either landscape or portrait mode. Please note that the rotation button in the notification center will be invalid after lockdown. • **Check screen size to detect tablet form-factor:** If enabled, the device screen size (width and height) will be checked to determine if the device is a tablet and if it supports orientation-related features. * This may cause some large-screen Phone/Phablets to be detected as a tablet and start supporting orientation.
	Time Zone	Allow users to access the "Time Zone" option on the upper right menu when in Kiosk Mode. ⚠ Only available for Android 8.0 and lower.
	Other Settings	• **Home key:** Allow or disable users to use Home key in Kiosk mode. • **Recent Key:** Allow or disable users to use Recent key in Kiosk mode. ⚠ Support devices with Android 9.0 and above.