BizMobile Go! OS Comparison Table

as of November 2, 2020

No.	Service	Category	Functions	Use Cases	iOS	Android	Windows 10	macOS	Windows 10 IoT	Wear OS by Google
1	Standard	Hierarchical organization management	Organization and user management functions（Tree mode)	Unify management of all devices from multiple departments (branch offices) along with organization information	○	○	○	○	○	○
2			Access control (allow display and operation based on restrictions)	All the devices of multiple departments (branch offices) are unifiedly managed but they are operated by different organizations and operators with different roles	○	○	○	○	○	○
3			User Registration support (Auto registration from AAD)	Deploy store apps to Windows 10 device	—	—	○	—	—	—
4		Monitoring	Dashboard (Registration, Sync status and Transition)	Check dynamic management information of all device or per organization on a dashborad	○	○	○	○	○	○
5			Log management (Alarm, event, Command, and CSV export)	Operation logs and detected alarms from managed devices are managed by management screen and CSV outputs	○	○	○	○	○	○
6			E-mail notification (Specified Administrator)	Login to the management screen is unnecessary with notification mail to confirm the management status on the daily device management or alarm occurrence	○	○	○	○	○	○
7			Device information query	Collect device specific information such as UDID and dynamic information such as free storage spaces on the device	○	○	○	○	○	○
8			Query app info (managed、unmaneged)	Check the usage and update status by collecting the lsit of installed application on the device	○	○	○	○	○	○
9			Query status of app installations	Manage implementation status of deployed applications	○	×	×	×	×	×
10			Query Books info (managed, unmanaged)	Collect book information installed on the device	○	—	—	×	—	—
11			Query Apps lisence Info (lisence, number, etc)[per 5 min]	Automatically update and manage purchased application licenses	○	×	○	×	—	—
12		Device enrollment management	Device enrollment settings support (CSV import)	Enroll a large number of device information at once by CSV input	○	○	○	○	○	○
13			Device enrollment settings support (CSV export, CSV chenge, CSV import)	Output all enrolled devices in CSV files, edit and re-enter all at once	○	○	○	○	○	○
14			Delete deivce registration	Delete each device or all devices at once when those are no longer required for management after the model change	○	○	○	○	○	○
15			Device enrollment support (URL entry)	Enter the registration URL from the browser for those deivces that cannot receive mails	○	○	○	○	○	—
16			Device enrollment support (send E-mail with URL)	Automatically send mail including registration URL to device user	○	○	○	○	—	—
17			Device enrollment support (Check-in using QR code)	Read the registration URL using the camera on the device	○	○	○	○	—	—
18			Device enrollment support (Check-in using paring)	Enroll “Wear OS by Google” by connecting to Android device	—	—	—	—	—	○
19			Device enrollment automation(DEP, Zero-touch, Windows AutoPilot)	Automatically enroll device just by activating the deivce. Allow skipping some items at the activation	○[*3]	×	×	×	—	—
20		Remote commands	Synchronize	Collect information on the device and automatically perform filling the difference from the server setting when necessary	○	○	○	○	○	○
21			remote lock	Operator remotely lock the device with passcode to prevent the risk of information leakage when device is lost	○	○	○	○	—	○
22			remote wipe	Operator remotely perform factory reset the device to prevent the risk of information leakage when device is lost	○	○	○	○	○	○
23			remove passcode	Operator remotely reset the passcode when passcode set on the device is forgotten	○	○	—	—	—	○
24			reconfigure passcode	Operator remotely clear the current passcode and set the new passcode	—	○	—	—	—	—
25			withdraw	The corporate information deployed from MDM is deleted when managed device sataus is cancelled	○	○	—	○	—	○
26			Selective wipe (wipe only business-related data)	It is unpreferable to perform factory rest for BYOD devices so operator remotely delete only the corporate information when device is lost	○	○	○	○	△	○
27			remote reatart	Remotely reboot the device when required for applying specific profile restrictions	○[*1]	○[*2]	○	×	×	—
28			Admin Lock (Lost Mode, Fech Location)	Remotely lock the device which can only be unlocked by the operator to prevent unauthorized use of device user and risk of information leakage when device is lost. Obtain the location information when device is locked and able to search the device	○[*1]	○[*2]	×	×	×	—
29			OS auto-update(Feature update, Quality update, Driver update, etc)	Prevent vulnerabilities and compatibility with business application for the latest versions by allowing automatically perform OS updates that are often forgotten by device user	○[*1]	×	○	×	×	—
30			Detect and Restrict SIM Card change	Detect when SIM card was exchanged, such as suspected personal use of company-provided SIM card	○	○	—	—	×	—
31			Bypass Activation Lock	When changing the device user, avoid activation lock is applied by the previous user's Apple ID and the device is unable to use after being initialized	○[*1]	—	—	—	—	—

BizMobile Go! OS Comparison Table

as of November 2, 2020

No.	Service	Category	Functions	Use Cases	iOS	Android	Windows 10	macOS	Windows 10 IoT	Wear OS by Google
32	Standard	Application management	Apps registration support (In-house Apps with version management)	Manage the version along with the release notes when registering the In-House application to be deployed	○	○	○	×	×	○
33			Apps registration support (Store Apps name search)	Easily search with application name when registering the Store application to be deployed	○	○	×	×	×	○
34			Apps registration support (VPP Store Apps auto registration)	Automatically register purcased licensed applications	○*3	×	×	×	×	×
35			Deployment apps support (required user's operation)	For BYOD device, deploy the application only when accepted by the device user	○	○	—	—	×	○
36			Deployment apps support (not required user's operation)	Install applications without any operation by device user	○*1	○	○	×	×	—
37			Detection of blocked applications (whitelists, blacklists)	Detect applications that is not permitted are installed	○	○	×	○	×	○
38			Notification of blocked applications (Alart, Notification E-mail)	Confirm the status with notification mail when applications that is not permitted are installed	○	○	×	○	×	○
39			Deployment Apps support (When Store Apps are updated, Store apps on the deveice are automatically updated)	Always update deployed applications to the latest version	○	×	×	×	×	×
40			Deployment Apps support (change from unmanaged apps to managed apps)	Put the device under MDM management without re-installing the installed application when introducing MDM to the device that has already been used	○	×	×	×	×	×
41			Configuration Apps support (get max 255 character by MDM)[need Apps treatment]	Allow log-in permissions in application and enable / disable specific functions for those devices registered in MDM	○	○	×	×	×	—
42		Contents management	Registration Books support (iBooks form, ePub form, PDF form)[iBook Store available]	Register the book to be deployed	○	—	—	—	—	—
43			Deployment Books support (when books changed, deploy the books automatically)[not only PDF]	Deploy manuals and conference materials at once to iBooks application without any operation by device users. Deleting is also possible	○	—	—	—	—	—
44		Profiles management	Restrict unmanaged app installation	Prohibit installing the apps which is not deployed via MDM	○*1	○ *2	—	—	—	—
45			Batch distribution (certificates authenticated with password)	Deploy authentication certificates at once (different authentication certificates can be deployed at once for each device)	○	×	○	×	×	—
46			Deploy provisioning profile support (per Apps)	Deploy provisioning profile and extend the certificate expiration without updating the In-House application	○	—	—	—	—	—
47			Enforce passcode policy (for local lock & wipe)	Force stronger passcode policy on device	○	○	○	○	×	○
48			Disable cameras	Prohibit the use of camera	○	○	○	×	○	—
49			Disable USB connection	Prevent data leakage by prohibiting connection with PC	○*1	○ *2	○	×	○	—
50			Restrict device backup feature	Prohibit iCloud backup while using Apple ID	○	—	—	×	—	—
51			Disable or Enable Bluetooth/Tethering/Roaming	Specify enable/disable on bluetooth / personal hotspot / data roaming	○*1	○ *2	○	×	—	—
52			Restrictions for school usage	Restrict functions unnecessary for class use such as displaying of predictive text keyboard	○*1	—	—	×	—	—
53			Disable device settings change（Account setting, Network setting)	Deploy corporate mail accounts from MDM and prohibit the use of personal mail accounts	○*1	○	○	×	○	—
54			Restrict file transferring	Prohibit sending and receiving of files between personal application (non-managed application) and business application (managed application)	○	○	○	×	○	—
55			Restrict notifications on lock screen	Prevent notification being displayed on the lock screen	○*1	○ *2	—	×	—	—
56			Parental Controls	Restrict target age of available applications	○	—	—	×	—	—
57			Restrict app usage (Black list / White list)	Restrict usage by hiding pre-installed applications	○*1	○ *2	×	×	×	—
58			Global HTTP proxy	Monitors communication by letting all HTTP communication of the device go through specified proxy	○*1	○ *2	—	—	—	—
59			Content Filter	Filter access in Safari and prohibit any access to unauthorized destinations	○*1	—	—	—	—	—
60			Wi-Fi	Deploy Wi-Fi access information at once. Prevent password leakage by not requiring password and displayed on the device	○	○	○	—	○	○
61			CardDAV server	Deploy settings for using contacts managed by the company	○	—	—	—	—	—
62			LDAP server	Deploy settings for accessing to LDAP server	○	—	—	—	—	—
63			APN	Deploy APN settings necessary for SIM usage	○	—	—	—	—	—
64			Web Clips	Display URL shortcut icons used for business on home screen	○	—	—	—	—	—
65			Mail account	Deploy mail account settings	○	—	—	—	—	—
66			Exchange ActiveSync	Deploy settings for connecting to Exchange Active Sync server	○	—	○	—	—	—
67			VPN	Deploy VPN settings	○	—	○	—	○	—
68			Per-App VPN	Deploy VPN settings that automatically connects only when specified application is launched	○	×	×	×	×	—
69			Force an OS software update delay	Prevent up to 90 days of OS updates by device users in accordance with the business application updates	○*1	×	○	×	×	—
70			Notifications per apps	Specify ON / OFF of notification for each application	○*1	—	—	—	—	—
71			Set Wallpaper, Device name	Set business logo on wallpaper and unify the look as business-dedicated devices	○*1	×	—	×	—	—

BizMobile Go! OS Comparison Table

as of November 2, 2020

No.	Service	Category	Functions	Use Cases	iOS	Android	Windows 10	macOS	Windows 10 IoT	Wear OS by Google
72	Standard	Profiles management	Home screen layout (Web clips can be specified)	Reduces the burden on supporting device users by specifying and fixing the application placement on the home screen	○[*1]	×	—	—	—	—
73			Single App Mode（Kiosk Mode）	Always launch specified application such as application used for taking orders at the restaurant and use it as business-dedicated device	○[*1]	○[*2]	△	×	×	—
74			Mulutiple App Mode（Kiosk Mode）	Display specific app icons designated by operator on home screen	○[*1]	○[*2]	—	×	×	—
75			Custom profiles	For each set values on the profile, specify different values for each targeted device by variables and deploy it at once	○	×	○	×	○	—
76			Others	Quickly correspond to profile functions provided by each OS	○	○	○	○	○	○
77	Options	Messages	Collect/display location information with OpenStreetMap	Confirm the daily location history of the device users (Able to hide the information of off-duty hours)	○	○	×	×	×	—
78			Simultaneous message notification (read status can be monitored)	Send messages to all managed devices, urging to delete application when prohibited application is installed.	○	○	×	×	×	—
79			Jailbreak notification (for jailbreaking, rooting)	Detect jailbreak devices that is not appropriate for business use	○	○	×	×	×	—
80		Personal	Personal UI (for Self Service)	When the device is lost, the user can send remote command to the device by using browser without contacting the administrator	○	○	○	×	×	—
81		AppCatalog	Deployment Apps with BizGo!Catalog (VPP, CustomB2B, In-House)	Provide recommended applications that can optionally be installed without requiring Apple ID through the BizGo! Catalog application and display them per categories with paid/free flags	○[*3]	×	×	×	×	—
82		Device Exchange	Device exchange service (automatic transfer of configuration to new device and subsequent reset of the old device)	Reduce administrator's operations at the time of changing old to new devices	○	○	○	○	○	—
83		Remote Control	Remotely view and control a device by administrator's PC	Reduce on-site support or collecting devices thanks to remote control including remote operation thourgh administrator's PC	—	○	—	—	—	—
84		Custom browser	Provide a secure browser which can access to only specified URL	Prevent the device user from accessing to web sites for personal usage	×	○	×	×	—	—
85		SMS check-in	Device enrollment support (send SMS with URL)	Automatically send mail including registration URL to device user	○	○	—	—	—	—
86		Geofence	Automatic template switching triggered by getting in and out of geofence	Switch templates automatically by detection of getting in and out of designated area (e.g.: Hide business apps outside office area)	○	—	—	—	—	—
87		User Survey	Survey for device user	Deliver and collect questionnaires for each managed devices through the survey app (e.g.: Inventory clearance through the survey for device owner)	○	—	—	—	—	—
88		Time-based Policy Management	Automatic template switching by designated schedule	Switch templates automatically on designated schedule basis so that devices can be optimized depending on each schedule (e.g.: Hide business apps after business hours to prevent overtime working)	○	○	○	—	—	—

[*1] Supervised mode required

[*2] Device Owner mode required

[*3] Availability of Apple DEP and VPP depends on countries due to Apple's policy.