techstep

Techstep Essentials MDM

Functionality Matrix

Date: 09/06/2025

Contents

PUBLISHED BY:

Techstep Poland sp. z o.o.
Al. Grunwaldzka 50
80-241 Gdańsk

1. Legend

To get more information, please contact us at support@famoc.com.

Mark	Description
✓	Supported
×	Not supported by platform/OS/vendor

2. Management Modes

ANDROID	
Management mode	**Description**
BYOD	• Work profile on private device • Activation on already working device (doesn't require factory reset) • Personal and business data separation • No access to private part of the device • Work profile management • Available for Android 7 + devices
WPC (work profile on company owned devices)	• Work profile on corporate device • Activation on new device or after factory reset • Personal and business data separation • No access to private part of the device • Work profile management • Available for Android 11 + devices
COBO / fully managed	• Device owner • Activation on new device or after factory reset • Entire device for business data only • Management of the entire device • Available for Android 6 + devices
COSU / Dedicated device	• Device owner • Activation on new device or after factory reset • Entire device locked for dedicated purpose (single app mode or launcher mode) • Management of the entire device • Available for Android 8+ devices
iOS/iPadOS/macOS	
BYOD	• Activation on already working device (doesn't require factory reset) • Personal and business data separation • Business apps and accounts management • No access to private part of the device • Available for devices with iOS 13 +, macOS 10.15+
COBO / fully managed	• Supervised mode • Activation on new device or after factory reset • Entire device for business data only • Management of the entire device • Available for devices with iOS 13 +, macOS 10.14.4+
Normal	• Legacy mode for management of the entire device while maintaining privacy of the user • With every new iOS version, management options are limited in favor of BYOD and COBO modes • Available for devices with iOS 10 +
Dedicated device	• Single app mode using configuration • Basic lock down features

3. Main features

Features overview		
	Essentials MDM	**Essentials MDM with options**
Both hosted and on-site setup options	✓	✓
SSL certificate support (RSA, ECC)	✓	✓
Multiple server OS support	✗	✓
Multi-tenancy support	✓	✓
Multi-language support	✓	✓
Web-based User Interface	✓	✓
Advanced alert management	✓	✓
Two-factor authentication	✓	✓
Multiple user roles/permissions	✓	✓
Fail-over solution	✗	✓
Multi-OS Application Blacklist alerting	✓	✓
Secure proxy DMZ	✓	✓
Support for Exchange ActiveSync Proxy	✗	✓
Microsoft Certificate Authority support	✗	✓
Built-in Certificate Authority service	✓	✓
Status view of implemented policies with the update option	✓	✓
Custom branding	✓	✓
Custom language tools	✓	✓
Rule based security policies (time, location)	✓	✓
Car mode (security policies based on the device speed)	✓	✓
The ability to operate in a fully closed environment (without access to the Internet)	✓	✓
Managed device analytics	✓	✓
Shared device mode for Android devices	✓	✓
Defining and use of Smart Groups for devices	✓	✓
Protocol of transfer/withdrawal of fixed assets	✓	✓
Tree structure for device groups (up to 5 levels)	✓	✓
Service mode restoration in case of any issue with the device	✓	✓
Recovery mode in case of the lost connection to the server	✓	✓
Campaigns for operation scheduling	✓	✓
Remote Control for Android devices	✓	✓
Remote Control for Apple devices	✓	✓
Productivity apps	✗	✓
eSIM management	✓	✓
Continuous parameters reporting	✓	✓
Activity logs	✓	✓

4. Integrations

Integrations	Essentials MDM	Essentials MDM with options
Apple DEP and several VPP support	✓	✓
Apple APNs – push notifications	✓	✓
Exchange ActiveSync Control	✗	✓
Essentials MDM CA	✓	✓
Microsoft CA	✗	✓
Firebase Cloud Messaging API	✓	✓
Managed Google Play store	✓	✓
YubiKey	✗	✓
SAML protocol support	✓	✓
Samsung KNOX configurations and management	✓	✓
Samsung KNOX Service Plugin support	✓	✓
Essentials MDM Lite	✓	✓
Cisco Umbrella	✓	✓
Android Enterprise	✓	✓
Zebra StageNow support	✓	✓
Google zero-touch enrollment	✓	✓
Multi-user support on the Android platform	✓	✓
Cisco ISE	✓	✓
AD/LDAP	✓	✓
Microsoft Entra ID	✓	✓
Extreme Networks	✓	✓
Fully customizable Chrome browser	✓	✓
Essentials MDM tunnel VPN client integration	✗	✓
Knox Configure integration	✓	✓
Samsung Knox Mobile Enrollment support	✓	✓
IBM Verse	✓	✓
Syslog integrations	✓	✓
Checkpoint Harmony Mobile	✓	✓
Zimperium MTD	✓	✓
AppConfig support	✓	✓
AWS CDN integration	✓	✓
Zebra OEM configuration	✓	✓

5. Enrollment

Implementation of Techstep Essentials MDM system on devices - ENROLLMENT										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
Autoenrollment (Google zero-touch/ Apple DEP/ Samsung Knox Mobile enrollment)	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓
Use of Smart Groups for registration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
User enrollment:	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SMS enrollment	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓
Enrollment via the app from the application store	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
QR code enrollment	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓
SAML protocol enrollment	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓
Implementation via USB cable	✓	✗	✓	✗	✓	✗	✗	✗	✗	✓
Implementation via Android Management API	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Different policy applying based on the group assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

6. Device details information

Device details information										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
OS details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
List of apps installed on devices (range depends on the management mode)	✓	✓	✓	×	✓	✓	×	✓	✓	✓
Parameters of access points	✓	✓	✓	×	✓	✓	×	×	×	✓
Hardware parameters (RAM, screen resolution)	✓	✓	✓	×	✓	✓	×	×	×	✓
Memory details	✓	✓	✓	×	✓	✓	×	✓	×	✓
Details about Wi-Fi	✓	✓	✓	×	✓	✓	×	✓	×	✓
Device ID reporting (IMEI, serial number or UUID)	✓	✓	✓	×	✓	✓	×	✓	✓	✓
SIM/eSIM ID reporting: IMSI, serial number, EID	✓	✓	✓	×	✓	✓	×	✓	×	✓
Bluetooth registry information	✓	✓	✓	×	×	×	×	×	×	×
Memory card information	✓	✓	✓	×	×	×	×	×	×	✓
Operator detection	✓	✓	✓	×	✓	✓	×	×	×	✓
Location information	✓	✓	✓	×	✓	✓	×	✓	×	✓
Device administrators list	✓	✓	✓	×	×	×	×	×	×	×

Device accounts	✓	✓	✓	×	×	×	×	×	×	×
Custom fields	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Software updates	×	×	×	✓	✓	✓	✓	✓	✓	×
Certificates	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Device state	✓	✓	✓	✓	✓	✓	✓	✓	✓	×

7. Device state parameters

Device state parameters reporting										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	Work profile on private device	Work profile on corporate device	Device owner/ Fully managed device / Dedicated device	User enrollment	Supervised mode	Legacy mode	User enrollment	Supervised mode	Legacy mode	
Device Owner mode / Supervised mode	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Work profile status	✓	✓	✓	×	×	×	×	×	×	×
Encryption status	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Installation of applications from unknown sources	✓	✓	✓	×	×	×	×	×	×	×
Logging enabled	✓	✓	✓	×	×	×	×	×	×	×
App monitor service status	✓	✓	✓	×	×	×	×	×	×	×
Organization-owned device with work profile	✓	✓	✓	×	×	×	×	×	×	×
Suspended personal apps	✓	✓	✓	×	×	×	×	×	×	×
Development settings status	✓	✓	✓	×	×	×	×	×	×	×
Development mode change	✓	✓	✓	×	×	×	×	×	×	×
Auto time on device	✓	✓	✓	×	×	×	×	×	×	×
Auto time zone on device	✓	✓	✓	×	×	×	×	×	×	×
Jailbreak / Rooted	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Apple DEP device / KME device	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Lost mode	×	×	✓	×	✓	×	×	✓	×	×
App Store account	×	×	×	✓	✓	✓	✓	✓	✓	×

Device network-tethered	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗
Diagnostic submission	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗
App analytics sharing	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗

8. Device features and restrictions

Device features and restrictions										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	Work profile on private device	Work profile on corporate device	Device owner/ Fully managed device / Dedicated device	User enrollment	Supervised mode	Legacy mode	User enrollment	Supervised mode	Legacy mode	
Camera lock (locked camera depends on the management mode)	×	×	✓	×	✓	✓	×	✓	✓	✓
Factory reset lock	×	×	✓	×	✓	✓	×	✓	×	✓
Unknown sources lock (range depends on the management mode)	✓	✓	✓	×	✓	✓	×	✓	×	✓
NFC lock	✓	✓	✓	×	×	×	×	×	×	✓
Memory card lock	×	×	✓	×	×	×	×	×	×	✓
Data transfer between private and work part lock	✓	✓	×	×	×	×	×	×	×	✓
Screen capture lock (range depends on the management mode)	✓	✓	✓	✓	✓	✓	×	×	×	✓
USB file manager lock	×	✓	✓	×	×	×	×	×	×	✓
Microphone lock	×	×	✓	×	×	×	×	×	×	✓
Cellular data lock	×	✓	✓	×	×	×	×	×	×	×
Cellular data lock in roaming	×	✓	✓	×	×	×	×	×	×	✓
GPS/location lock	✓	✓	✓	×	×	×	×	×	×	✓
Enable and maintain	×	×	✓	×	✓	×	×	×	×	×

GPS/location										
Developer options lock	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
USB debugging lock	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Web browser lock (range depends on the management mode)	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓
Microphone on/off	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓
Camera on/off (range depends on the management mode)	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓
Multi-window lock	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Safe/emergency mode lockout	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Certificate store access lock (scope depends on the management mode)	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Certificates installation	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
Possibility to send files to a device	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
Phone settings access lock	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
Copy/paste lock	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Possibility to define default applications for opening files of the following types: doc, xls, ppt, pdf	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓
Date and time settings change lock	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓
Manual accounts add lock (application store, email, exchange; range depends on the management mode)	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓

Enabling / disabling the option to restore a backup from a Google account	✓	✓	✓	×	×	×	×	×	×	×
Disabling Samsung Galaxy Store	×	×	✓	×	×	×	×	×	×	×
Remote reboot	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Disable content suggestions on your device	×	✓	✓	×	×	×	×	×	×	×
Disable content capture on the device	×	✓	✓	×	×	×	×	×	×	×
Disable SMS	×	✓	✓	×	×	×	×	×	×	✓
Turn off location sharing on your device	×	✓	×	×	×	×	×	×	×	✓
Service mode with additional pin code	×	✓	✓	×	×	×	×	×	×	×
Possibility to block outgoing calls	✓	✓	✓	×	×	×	×	×	×	×
Reporting user-triggered application uninstallation	✓	✓	✓	×	×	×	×	×	×	×
Invoking URL on a device	✓	✓	✓	×	×	×	×	×	×	×
Invoking intent on a device	✓	✓	✓	×	×	×	×	×	×	×
Force automatic date and time	×	×	✓	×	✓	×	×	×	×	×
Usage data monitoring, including:	✓	✓	✓	×	×	×	×	×	×	×
- Package data traffic using Wi-Fi	✓	✓	✓	×	×	×	×	×	×	×
- Package data traffic using GPRS	✓	✓	✓	×	×	×	×	×	×	×

- Reporting device state	✓	✓	✓	×	×	×	×	×	×	×
- Reporting screen unlock/lock time	✓	✓	✓	×	×	×	×	×	×	×
- Reporting application usage	✓	✓	✓	×	×	×	×	×	×	×
- Voice calls	×	×	✓	×	×	×	×	×	×	×
- SMS	×	×	✓	×	×	×	×	×	×	×
Prevent users from configuring credentials in the managed keystore	✓	✓	✓	×	×	×	×	×	×	×
Disable all keyguard shortcuts	×	×	✓	×	×	×	×	×	×	×
Disallow config default applications	✓	✓	✓	×	×	×	×	×	×	×
Device screen brightness control	✓	✓	✓	×	×	×	×	×	×	×

9. App management features

App management features										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
Application distribution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application removal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application list reporting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application reputation status/control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application password policy	×	×	✓	×	×	×	✓	✓	✓	✓
Application allow/deny policy	×	×	✓	×	✓	✓	×	×	×	×
Remote application start	✓	✓	✓	×	×	×	×	×	×	×
Corporate AppStore	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application permission control	✓	✓	✓	×	×	×	×	✓	×	×
Application installation from defined network (e.g. corporate Wi-Fi)	✓	✓	✓	×	×	×	✓	✓	✓	✓
User installation blocked	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
Installation blocked from unknown sources	✓	✓	✓	✓	✓	✓	×	×	×	×
Force the use of Google Play Protect	✓	✓	✓	×	×	×	×	×	×	×
Clear application data	✓	✓	✓	×	×	×	×	×	×	×
Notification handling on managed apps	×	×	×	✓	✓	✓	×	✓	×	×

Don't allow data sharing from unmanaged apps	✓	✓	✓	✓	✓	✓	×	×	×	×
Disallow assist content	✓	✓	✓	×	×	×	×	×	×	×

10. Security

Security										
Functionality	Android			iOS / iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	NORMAL
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
Remote lock	✓	✓	✓	×	✓	×	×	✓	✓	✓
Remotely restore the device to factory settings	×	✓	✓	×	✓	×	×	✓	✓	✓
Corporate data wipe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Restore device to factory settings when there is no SIM card or it is replaced	×	✓	✓	×	×	×	×	×	×	✓
Corporate data wipe when there is no SIM card or it is replaced	×	✓	✓	×	×	×	×	×	×	×
Wipe on root/jailbreak detection	×	×	✓	×	✓	✓	×	×	×	×
Factory Reset/ Activation Protection (FRP)	×	✓	✓	×	✓	×	×	×	×	×
Auto-lock policy	✓	✓	✓	×	✓	✓	×	✓	×	✓
Password policies	✓	✓	✓	×	✓	✓	×	✓	✓	✓
Wipe on X password attempts	✓	✓	✓	×	✓	✓	×	✓	✓	✓
SIM change reporting	✓	✓	✓	×	✓	✓	×	×	×	✓
Anti-virus application management	✓	✓	✓	×	×	×	×	×	×	×
Phone memory encryption	✓	✓	✓	×	✓	✓	×	✓	✓	✓
Installation restrictions	✓	✓	✓	×	✓	✓	×	✓	×	✓

Blocking the uninstallation of the application	✓	✓	✓	✓	✓	✓	×	✓	×	✓
Device reboot	×	×	✓	×	✓	✓	×	✓	×	×
Device shutdown	×	×	✓	×	✓	✓	×	✓	×	×
Selective data wipe	×	×	✓	×	✓	✓	×	✓	×	×
Block data transfer between private and business applications	✓	✓	×	×	✓	✓	×	×	×	×
Screen lock during enrollment for the time of uploading all elements of the policy.	×	×	✓	×	×	×	×	×	×	×
Disable the ability to connect external physical media	×	✓	✓	×	×	×	×	×	×	×
Content protection policy	✓	✓	✓	×	×	×	×	×	×	×
Disallow user from creating private profile	✓	✓	×	×	×	×	×	×	×	×

11. Operating system version control

Operating system version control										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
User update lock	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓
Remote installation of the update	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗
Update installation delay	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗
Force update installation	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗

12. Network settings

Network settings										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	
Additional mode description	*Work profile on private device*	*Work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	
Access point (APN) configuration	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓
WLAN configuration	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
WLAN EAP-TLS configuration	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
Managed networks change lock	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Wi-Fi tethering lock	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
USB tethering lock	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Manual Wi-Fi configuration lock	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓
Internet sharing lock	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
VPN configuration	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓
VPN configuration with YubiKey hardware tokens authorization	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Firewall configuration	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗
Keep Wi-Fi on in sleep mode	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Prevent Wi-Fi from being turned off	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
Bluetooth lock	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓
Disable Network Settings Reset	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗

Disable VPN settings	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Block private DNS settings	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Block cell broadcast config	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Disallow cellular 2G	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Disallow Ultra-Wideband(UWB)	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
NFC lock	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Disallow eSIM	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Disallow change of Wi-Fi state	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗

13. Remote support

Remote support										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	
Additional mode description	Work profile on private device	Work profile on corporate device	Device owner/ Fully managed device / Dedicated device	User enrollment	Supervised mode	Legacy mode	User enrollment	Supervised mode	Legacy mode	
Remote access - view only mode	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remote access to screen and keyboard: → All Android devices (Accessibility service needed for devices other than listed HERE) → macOS	✓	✓	✓	×	×	×	✓	✓	✓	✓
Visual remote file browsing (operations, upload, download, run etc.)	✓	✓	✓	×	×	×	×	×	×	✓
Chat option during the remote session	×	×	×	✓	✓	✓	✓	✓	✓	×

14. Other features

Other features										
Functionality	Android			iOS/iPadOS			macOS			Windows 8.1/10
MANAGEMENT MODE	BYOD	WPC	COBO	BYOD	COBO	NORMAL	BYOD	COBO	NORMAL	
Additional mode description	*Work profile on*	*Work profile on corporate device*	*Device owner/ Fully managed device*	*User enrollment*	*Supervised mode*	*Legacy mode*	*User enrollment*	*Supervised mode*	*Legacy mode*	

	private device									
Security policies: - Time - Location - speed (car mode) - block connection to the network based on MCC/MNC code	×	×	✓	×	×	×	×	×	×	✓
Message to user	✓	✓	✓	×	✓	✓	×	×	×	×
Secure SSL connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data encryption	✓	✓	✓	×	✓	✓	×	✓	✓	✓
Business phonebook	✓	✓	✓	✓	✓	✓	×	×	×	×
Sound settings	✓	✓	✓	×	×	×	×	×	×	✓
Wallpaper settings	×	×	✓	×	✓	×	×	×	×	✓
Encrypted DNS settings	×	×	×	×	✓	×	×	✓	×	×
Upload file	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Extensible single sign-on	×	×	×	×	✓	×	×	✓	×	×
Set device language	×	×	✓	×	×	×	×	×	×	×
Execute command	×	×	✓	×	×	×	×	✓	×	×

15. COSU mode (kiosk mode) for dedicated devices

COSU mode (kiosk mode) possibilities - all of the above and below:		
Functionality	Android	iOS/iPadOS
MANAGEMENT MODE	COSU	COBO
Additional mode description	*Dedicated device*	*Supervised mode*
One app mode	✓	✓
Many apps mode (Launcher start screen)	✓	✗
Upload the wallpaper to the home screen	✓	✗
Upload the wallpaper to the lock screen	✓	✓
Status bar visibility	✓	✗
Customizable logo and message text on the lock screen	✓	✗
Custom settings bar	✓	✗
Wi-Fi option	✓	✗
Bluetooth option	✓	✗
Restart device option	✓	✗
Brightness option	✓	✗
Torch option	✓	✗
Volume change option	✓	✗
Customizable grid / list	✓	✗
Zoom mode	✓	✗
Customizable app background	✓	✗
Customizable header with logo	✓	✗
Device info page with up to 8 custom fields	✓	✗
Optional support button with possibility to make a call	✓	✗
Possibility to add different views of the same application (ActivityName)	✓	✗
Possibility to define default applications for opening files of the following types: doc, xls, ppt, pdf	✓	✗
Volume change control	✓	✓
Keyboard protection	✓	✗
Power button lock	✓	✓
Home button lock	✓	✗
Recent apps button Lock	✓	✗
Notifications lock	✓	✓
Display of system information on the status bar lock	✓	✓
Touch screen lock	✗	✓
Screen rotation lock	✓	✓
Service mode with an additional PIN code to disable KIOSK mode	✓	✗
Widgets support	✓	✗
Webclip support	✓	✗

16. Additional management and security features depending on the manufacturer of Android devices

Samsung			
Functionality	Android		
MANAGEMENT MODE	BYOD	WPC	COBO
Additional mode description	*Features available in work profile on private device*	*Features available in work profile on corporate device*	*Device owner/ Fully managed device / Dedicated device*
Block incoming calls	✗	✗	✓
Block incoming SMS messages	✗	✗	✓
Block incoming MMS messages	✗	✗	✓
Voice recording lock in recording apps	✗	✗	✓
Block of individual Bluetooth interface profiles (A2DP, AVRCP, HFP, HSP, PBAP, SPP, file transfer)	✗	✗	✓
Task manager lock	✗	✗	✓
NFC lock	✗	✗	✓
Block airplane mode	✗	✓	✓
Multi-window lock	✗	✗	✓
Remote access to screen and keyboard	✓	✓	✓
SIM card pin code management	✗	✗	✓
Common Criteria mode activation	✗	✗	✓
Support for a dedicated access point (Enterprise billing)	✓	✓	✓
Samsung Knox Service Plugin support, including:	✓	✓	✓
- Separate applications policy	✗	✗	✓
- Advanced DeX mode settings	✗	✗	✓
- Advanced VPN configuration	✓	✓	✓
- Advanced firewall configuration	✓	✓	✓
- Force specified language of the device menu	✗	✗	✓
- Configuration of the SIM card in the second slot	✗	✗	✓
- Adjust the availability of items in device settings	✗	✗	✓
- Possibility to name the work profile and private part	✓	✓	✗

Zebra	
Functionality	Android
MANAGEMENT MODE	COBO
Additional mode description	*Device owner/ Fully managed device / Dedicated device*
Advanced operating system version management - Zebra LifeGuard	✓
Support for advanced Zebra StageNow configurations	✓
Zebra OEMConfig powered by MX support, including:	✓
RFID settings	✓
Scanner settings	✓
Advanced camera settings	✓
DataWedge feature	✓
Advanced Bluetooth configuration	✓
Operating system version management	✓
File management	✓
Advanced customization of the visual elements of the device	✓
Adjust the availability of items in device settings	✓
Sound settings	✓
Manage the automatic start of the device	✓

Honeywell	
Functionality	Android
MANAGEMENT MODE	COBO
Additional mode description	*Device owner/ Fully managed device / Dedicated device*
Honeywell OEMConfig, including:	✓
Advanced network settings	✓
Scanner settings	✓
Peripherals settings (e.g. Defroster, Dock, Heater, Touch)	✓
Operating system version management	✓
Sensor settings	✓
Printing settings	✓
Sound settings	✓
Manage the automatic start of the device	✓

17. Additional management and security features depending on the Apple platform (iOS/macOS/tvOS)

Apple					
Functionality	iOS			macOS	tvOS
MANAGEMENT MODE	BYOD	COBO	NORMAL		
Additional mode description	*User enrollment*	*Supervised mode*	*Legacy mode*		
Network policy					
Turn off cellular plan modification	×	✓	×	×	×
Block background downloads when roaming	×	✓	✓	×	×
Block voice dialing if device is password locked	×	✓	✓	×	×
Block cellular data modification for apps	×	✓	×	×	×
Disable host pairing	×	✓	×	×	×
Disable eSIM settings modification	×	✓	×	×	×
Preserve eSIM while erasing the device	×	✓	×	×	×
Prevent the transfer of an eSIM to a different device	×	✓	✓	×	×
Hardware Policy					
Disable remote screen viewing by the Classroom app	×	✓	✓	✓	×
Prevent Siri from querying user-generated content from the web	×	✓	×	×	×
Disable automatic keyboard correction	×	✓	×	×	×
Disable incoming AirPlay requests	×	✓	×	×	×
Disable biometric modification	×	✓	×	×	×
Forced biometric timeout	×	×	×	✓	×
Disable keyboard shortcuts	×	✓	×	×	×
Disable spell check on keyboard	×	✓	×	×	×
Block Photo Stream	×	✓	✓	×	×
Block the creation of untrusted TLS connections	×	✓	✓	×	×
Don't allow certificate trust database update	×	✓	✓	×	×
Disable modification of notification settings	×	✓	×	×	×
Turn off pairing watches	×	✓	×	×	×
Disable password modification	×	✓	×	✓	×
Block device name modification	×	✓	×	×	✓
Disable diagnostic data transfer modification	×	✓	×	×	×

Disable dictation	✗	✓	✗	✓	✗
Turn off screen time	✗	✓	✗	✗	✗
Disable wallpaper modification	✗	✓	✗	✓	✗
Force assistant profanity filter	✗	✓	✗	✓	✗
Allow devices to be booted into recovery by an unpaired device	✗	✓	✗	✗	✗
Enable USB accessories while device is locked	✗	✓	✗	✗	✗
Disable the prompt to setup new nearby devices	✗	✓	✗	✗	✗
Disable AirPrint	✗	✓	✗	✗	✗
Disable saving of AirPrint credentials on iCloud	✗	✓	✗	✗	✗
Require trusted certificates for TLS printing communication	✗	✓	✗	✗	✗
Disable iBeacon discovery of AirPrint printers	✗	✓	✗	✗	✗
Disallow macOS auto unlock	✗	✓	✗	✓	✗
Disallow macOS cloud desktop and document services	✗	✗	✗	✓	✗
Prevent Touch ID from unlocking a device	✗	✓	✓	✓	✗
Disallow content caching	✗	✗	✗	✓	✗
Disable QuickPath keyboard	✗	✓	✗	✗	✗
Prevent device from sleeping	✗	✗	✗	✗	✓
Disable Siri	✓	✓	✓	✗	✗
Disable Siri when device is locked	✓	✓	✓	✗	✗
Disable connections to Siri servers for the purposes of dictation	✓	✓	✓	✗	✗
Disable connections to Siri servers for the purposes of translation		✓	✓	✗	✗
Disable automatically submitting diagnostic reports to Apple	✓	✓	✓	✓	✗
Disable Control Center from appearing on the Lock screen	✓	✓	✓	✗	✗
Disable notifications history view on the lock screen	✓	✓	✓	✗	✗
Disable today notifications history view on the lock screen	✓	✓	✓	✗	✗
Disable managed applications to use the iCloud	✓	✓	✓	✗	✗
Force devices receiving AirPlay requests from this device to use a pairing pass	✓	✓	✓	✗	✗
Force encrypted backup	✓	✓	✓	✗	✗
Force wrist detection on Apple Watch	✓	✓	✓	✗	✗

Disable auto-dim on iPad devices with OLED displays	✗	✓	✗	✗	✗
Disallow iPhone mirroring	✗	✓	✓	✓	✗
Disable writing tools	✗	✓	✓	✓	✗
Installer Policy					
Disable App Store	✗	✓	✗	✗	✗
Prohibit the user from installing configuration profiles interactively and certificates	✗	✓	✗	✗	✗
Application limitations					
Block iCloud Private Relay	✗	✓	✗	✓	✗
Turn off iTunes	✗	✓	✗	✗	✗
Force user to enter iTunes password for every transaction	✗	✓	✓	✗	✗
Disable changes in Find My Friends	✗	✓	✗	✗	✗
Block trusting corporate apps	✗	✓	✓	✗	✗
Block in-app purchases	✗	✓	✓	✗	✗
Block Passbook Notifications on Lock Screen	✗	✓	✓	✗	✗
Enforce limited ad tracking	✗	✓	✓	✗	✗
Disable AutoFill in Safari	✗	✓	✗	✓	✗
Disable JavaScript in Safari	✗	✓	✓	✗	✗
Block Popups in Safari	✗	✓	✓	✗	✗
Cookie management accepted by Safari	✗	✓	✓	✗	✗
Disable game center	✗	✓	✗	✓	✗
Disable adding friends to Game Center	✗	✓	✗	✓	✗
Block multiplayer games	✗	✓	✗	✓	✗
Disable App Removal	✗	✓	✗	✗	✗
Prevent apps purchased on another device from automatically downloading	✗	✓	✗	✗	✗
Remove the BookStore tab from the Books app	✗	✓	✗	✓	✗
Disable downloading of Apple Books media tagged as erotic	✗	✓	✓	✓	✓
Turn off iMessage	✗	✓	✗	✗	✗
Hide uncensored music or videos purchased from the iTunes Store	✗	✓	✗	✓	✓
Disable connecting to network drives in the Files app	✗	✓	✗	✗	✗
Disable connecting to any connected USB devices in the Files app	✗	✓	✗	✗	✗
Disable the News app	✗	✓	✗	✗	✗
Disable podcasts	✗	✓	✗	✓	✗
Turn off Apple Music Radio	✗	✓	✗	✗	✗
Disable Shared Photo Stream	✗	✓	✓	✗	✗

Hide FaceTime App	×	✓	×	×	×
Force auto-join Classroom classes	×	✓	×	✓	×
Require permission to leave Classroom	×	✓	×	✓	×
Force self-lock apps and devices in Classroom	×	✓	×	✓	×
Force uninvited screen observation in Classroom	×	✓	×	✓	×
Disable AirDrop	×	✓	×	×	×
Do not allow to share managed documents using AirDrop	✓	✓	✓	×	×
Disable passwords sharing with Airdrop Passwords feature	×	✓	×	✓	×
Disable autofill passwords in apps	×	✓	×	✓	×
Do not request passwords from nearby devices	×	✓	×	✓	✓
Authenticate Face ID/Touch ID before allowing autofill passwords or credit card information	×	✓	×	×	×
Disable iCloud Photo Library	×	✓	✓	✓	×
Disable document syncing to iCloud	×	✓		✓	×
Disable iCloud keychain synchronization	×	✓	×	✓	×
Disable macOS iCloud Boookmark sync	×	×	×	✓	×
Disable macOS iCloud Mail services	×	×	×	✓	×
Disable macOS iCloud Calendar services	×	×	×	✓	×
Disable macOS iCloud Reminder services	×	×	×	✓	×
Disable macOS iCloud Address Book services	×	×	×	✓	×
Disable macOS iCloud Notes services	×	×	×	✓	×
Disable iTunes application file sharing services	×	×	×	✓	×
Disable returning Internet search results by Spotlight	×	✓	×	✓	×
Disable pairing of Apple TV with the Remote app or Control Center widget	×	×	×	×	✓
Max level of movie content allowed on the device	×	✓	✓	×	✓
Max level of TV content allowed on the device	×	✓	✓	×	✓
Max level of app content allowed on the device	×	✓	✓	×	✓
Disable Find My Device in the Find My app	×	✓	×	×	×
Disable Find My Friends in the Find My app	×	✓	×	×	×

Disable activity continuation	×	✓	✓	✓	×
Disable accounts modification on Apple devices	×	✓	×	×	×
Allow use of TLS 1.0/1.1 in Safari	×	✓	✓	✓	×
Prevent a user from adding any App Clips	×	✓	×	×	×
Limit Apple personalized advertising	×	✓	✓	×	×
Disable app uninstallation	✓	✓	✓	×	✓
Disable enterprise apps trust		✓	✓	×	×
Enables Safari fraud warning	✓	✓	✓	×	×
Prevent installation of apps from the alternative application stores	×	✓	×	×	×
Disallow web app distribution	×	✓	✓	×	×
Disallow to create new Genmoji	×	✓	✓	×	×
Disallow Image Playground	×	✓	✓	✓	×
Disallow Image Wand	×	✓	✓	×	×
Prevent the system from generating text in the user's handwriting	×	✓	✓	×	×