

Sophos Mobile 8.1

Feature Matrix



	Deployment		Device Platform				
	Managed with Sophos Central	Installed On-Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Server							
Admin User Interface							
Easy-to-use web interface	✓	✓	✓	✓	✓	✓	✓
Flexible Dashboard with 29 different widgets	✓	✓	✓	✓	✓	✓	✓
Flexible filter mechanism	✓	✓	✓	✓	✓	✓	✓
Role-based access	✓	✓	✓	✓	✓	✓	✓
Multi-tenancy	✓	✓	✓	✓	✓	✓	✓
Sophos Central Partner Dashboard for Managed Service Providers	✓		✓	✓	✓	✓	✓
Communication from superadmin to all tenants (administration and self service portal UI)		✓	✓	✓	✓	✓	✓
Sophos technical notifications	✓	✓	✓	✓	✓	✓	✓
Sending of text messages (via APNs, GCM, Baidu, WNS)	✓	✓	✓	✓	✓	✓	✓
Customizable administrator UI branding	✓	✓	✓	✓	✓	✓	✓
Self Service Portal							
Register new device	✓	✓	✓	✓	✓	✓	✓
Device wipe	✓	✓	✓	✓	✓	✓	✓
Device lock	✓	✓	✓	✓	✓		✓
Device locate	✓	✓	✓	✓	✓	✓	
Passcode reset for Device, App Protection (Android), Sophos Container (iOS, Android)	✓	✓	✓	✓	✓	✓	
Trigger device check-in	✓	✓	✓	✓	✓	✓	✓
Decommission device (incl. corporate wipe on iOS, Samsung, LG, Sony, and Windows 10 Mobile)	✓	✓	✓	✓ ^{5,6,7}	✓	✓	✓
Delete decommissioned device from inventory	✓	✓	✓	✓	✓	✓	✓
Monitor device status and compliance information	✓	✓	✓	✓	✓	✓	✓
Show acceptable use policy with new device registration	✓	✓	✓	✓	✓	✓	✓
Display post-enrollment message	✓	✓	✓	✓	✓	✓	✓
Control registration by OS type	✓	✓	✓	✓	✓	✓	✓
Configure maximum number of devices per user	✓	✓	✓	✓	✓	✓	✓
Company-specific configuration of commands available to users	✓	✓	✓	✓	✓	✓	✓
Customizable branding	✓	✓	✓	✓	✓	✓	✓
User Directory and Management							
Comprehensive password policies	✓	✓	✓	✓	✓	✓	✓
Password recovery by the user	✓	✓	✓	✓	✓	✓	✓
Internal user directory including batch upload capability	✓	✓	✓	✓	✓	✓	✓
Microsoft ActiveDirectory integration	✓	✓	✓	✓	✓	✓	✓
Novell eDirectory integration		✓	✓	✓	✓	✓	✓
Lotus Notes Directory integration		✓	✓	✓	✓	✓	✓
Red Hat Directory integration		✓	✓	✓	✓	✓	✓
Zimbra Directory integration		✓	✓	✓	✓	✓	✓
Device compliance enforcement rules							
Group assignment or ownership-based compliance rules	✓	✓	✓	✓	✓	✓	✓
Compliance violations analytics	✓	✓	✓	✓	✓	✓	✓
Device under management	✓	✓	✓	✓	✓	✓	✓
Jailbreak or rooting detection	✓	✓	✓	✓	✓		✓
Encryption required	✓	✓	✓	✓	✓	✓	✓
Passcode required	✓	✓	✓	✓	✓	✓	✓
Minimum OS version required	✓	✓	✓	✓	✓	✓	✓
Maximum OS version allowed	✓	✓	✓	✓	✓	✓	✓
Last synchronization of the device	✓	✓	✓	✓	✓	✓	✓
Last synchronization of the Sophos Mobile Control app	✓	✓	✓	✓	✓		✓
Blacklisted apps	✓	✓	✓	✓			✓
Whitelisted apps	✓	✓	✓	✓			✓
Mandatory apps	✓	✓	✓	✓		✓	✓
Block installation from unknown sources (sideloading)	✓	✓	✓	✓			
Data roaming setting	✓	✓	✓	✓	✓		
USB debugging setting	✓	✓	✓	✓			
Sophos Mobile client version	✓	✓	✓	✓	✓		
Malware detection	✓	✓		✓ ⁴		✓ ⁸	
System Integrity Protection required	✓	✓					✓
Firewall required	✓	✓					✓
Suspicious apps detection	✓	✓		✓ ⁴			

	Managed with Sophos Central	Installed On-Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Device compliance enforcement rules (continued)							
Potentially unwanted apps detection	✓	✓		✓ ⁴			
Last malware scan	✓	✓		✓ ⁴		✓ ⁸	
Locate for Sophos Mobile Control app enabled	✓	✓	✓	✓	✓		
Compliance rule templates for HIPAA and PCI	✓	✓	✓	✓	✓	✓	✓
Security							
Encrypted connection to web interface	✓	✓	✓	✓	✓	✓	✓
Encrypted communication with devices	✓	✓	✓	✓	✓	✓	✓
Control email access by compliance state [Exchange gateway, Office 365 access control]	✓	✓	✓	✓	✓	✓	✓
2FA device authentication at the Exchange gateway (password, certificate)	✓	✓	✓	✓	✓	✓	✓
Define allowed email clients at the Exchange gateway	✓	✓	✓	✓	✓	✓	✓
Control network access by compliance [Generic NAC interface, Sophos UTM, Cisco ISE, Check Point]	✓	✓	✓	✓	✓	✓	✓
USSD code protection (e.g. *#2314#)	✓	✓		✓ ⁴			
Spam call protection	✓	✓		✓ ⁴			
Protection from malicious websites [web filtering]	✓	✓		✓ ⁴			
Protect corporate apps with additional authentication [App Protection]	✓	✓		✓ ⁴			
Web productivity filtering by 14 categories + allow/deny lists by IP address, DNS name and IP range	✓	✓		✓ ⁴			
Manage and store passwords using KeePass format	✓	✓		✓ ⁴			
Inventory							
Device groups	✓	✓	✓	✓	✓	✓	✓
User-oriented device view	✓	✓	✓	✓	✓	✓	✓
Automatic transfer of unique device ID (IMEI, MEID, UDID) and further device data	✓	✓	✓	✓	✓	✓	✓
Automatic OS version detection	✓	✓	✓	✓	✓	✓	✓
Automatic device model resolution into a user-friendly name	✓	✓	✓	✓	✓	✓	✓
Use actual device name for device inventory	✓	✓	✓	✓	✓	✓	✓
Marker for company-owned and privately-owned devices	✓	✓	✓	✓	✓	✓	✓
Customer defined device properties with template support	✓	✓	✓	✓	✓	✓	✓
Import/export of device information	✓	✓	✓	✓	✓	✓	✓
Savable extended filters for devices	✓	✓	✓	✓	✓	✓	✓
Provisioning / Device enrollment							
Device management (MDM) enrollment	✓	✓	✓	✓	✓	✓	✓
Container-only Management enrollment	✓	✓	✓	✓	✓	✓	✓
Device enrollment wizard for admins	✓	✓	✓	✓	✓	✓	✓
Device enrollment by emails	✓	✓	✓	✓	✓	✓	✓
Online registration from the device	✓	✓	✓	✓	✓	✓	✓
Bulk provisioning [by email]		✓	✓	✓	✓	✓	✓
Apple Configurator deployment		✓	✓				
Apple DEP enrollment [Device Enrollment Program]	✓	✓	✓				
Admin enrollment w/o installed app [no iTunes account required]	✓	✓	✓				✓
Definition of standard rollout packages for personal or corporate devices	✓	✓	✓	✓	✓	✓	✓
Automatic assignment of initial policies and groups based on user directory group membership	✓	✓	✓	✓	✓	✓	✓
Enrollment using provisioning package files (*.ppkg)	✓	✓			✓	✓	
Task management							
Scheduled task generation	✓	✓	✓	✓	✓	✓	✓
Tasks can be generated for single devices or groups	✓	✓	✓	✓	✓	✓	✓
Detailed status tracking for each task	✓	✓	✓	✓	✓	✓	✓
Intelligent strategies for task repetition	✓	✓	✓	✓	✓	✓	✓
Reporting							
Export inventory using applied filters	✓	✓	✓	✓	✓	✓	✓
Export all reports as XLS or CSV	✓	✓	✓	✓	✓	✓	✓
Compliance log of all administrator activities	✓	✓	✓	✓	✓	✓	✓
Detailed Alert log	✓	✓	✓	✓	✓	✓	✓
Malware reports [2 different reports]	✓	✓	✓	✓	✓	✓	✓
Compliance violation reports [2 different reports]	✓	✓	✓	✓	✓	✓	✓
Device reports [9 different reports]	✓	✓	✓	✓	✓	✓	✓
App reports [8 different reports]	✓	✓	✓	✓	✓	✓	✓
Certificate reports [2 different reports]	✓	✓	✓	✓	✓	✓	✓
Programming interface (API)							
Web service [REST] API for device information and provisioning from 3rd party systems		✓	✓	✓	✓	✓	✓
Devices							
Sophos Mobile Control app functionality							
Enterprise App Store	✓	✓	✓	✓	✓		
Show compliance violations (including help for the enduser to fix reported compliance issues)	✓	✓	✓	✓	✓		
Show server messages	✓	✓	✓	✓	✓		
Show technical contact	✓	✓	✓	✓	✓		
Trigger device synchronization	✓	✓	✓	✓	✓		
Co-branding of the Sophos Mobile Control app		✓	✓	✓	✓		
Show privacy information	✓	✓	✓	✓	✓		

	Managed with Sophos Central	Installed On-Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Application management							
Installing apps (with or without user interaction, including managed apps on iOS)	✓	✓	✓	✓	✓	✓	
Uninstalling apps (with or without user interaction)	✓	✓	✓	✓		✓	
List of all installed apps	✓	✓	✓	✓		✓	✓
Support for Apple Volume Purchasing Program [VPP]	✓	✓	✓				
Allow/forbid installation of apps	✓	✓	✓	✓	✓	✓	
Block app deinstallation	✓	✓		✓ 5,6,7			
Remote configuration of company apps (managed settings)	✓	✓	✓ ²				
Block specific apps from running (app blocker)	✓	✓	✓ ²	✓	✓	✓	
Manage and configure Microsoft Office 365 apps	✓	✓	✓	✓			
Security							
Jailbreak (iOS)/Rooting (Android) detection	✓	✓	✓	✓			
Tamper detection	✓	✓	✓	✓	✓		
Anti-theft protection: Remote wipe	✓	✓	✓	✓	✓	✓	✓
Anti-theft protection: Remote lock	✓	✓	✓	✓	✓		✓
Anti-theft protection: Device locate	✓	✓	✓	✓	✓	✓	
Enforce password strength and complexity	✓	✓	✓	✓	✓	✓	✓
Inactivity time (time in minutes until password is required)	✓	✓	✓	✓	✓	✓	✓
Maximum number of attempts until the device will be reset	✓	✓	✓	✓	✓	✓	✓
Minimum password length	✓	✓	✓	✓	✓	✓	✓
Password history	✓	✓	✓	✓	✓	✓	✓
Password expiration time	✓	✓	✓	✓	✓	✓	✓
Minimum length of lower/upper case, non-letter or symbol characters in the passcode	✓	✓	✓	✓	✓		✓
Passcode reset (unlock)/administrator defines new passcode	✓	✓	✓	✓	✓		
Activation lock bypass	✓	✓	✓ ²				
Activation of storage encryption	✓	✓	✓ ³	✓	✓		
Access to the memory card can be prohibited	✓	✓		✓ 5,6,7	✓	✓	
Activation/deactivation of device data encryption	✓	✓		✓ 5,6,7	✓		
Block installation from unknown sources (sideloading)	✓	✓		✓ 5,6,7,9			
Block Wi-Fi	✓	✓	✓ ²	✓ 5,6,7,9			
Block Bluetooth	✓	✓		✓ 5,6,7,9		✓	
Block data transfer via Bluetooth	✓	✓		✓ ⁵	✓	✓	
Block data transfer via NFC	✓	✓		✓ 5,6,7	✓		
Block USB connections	✓	✓		✓ 5,6,7,9	✓		
Block camera	✓	✓	✓	✓	✓	✓	✓
Protection of settings against modification/removal by the user	✓	✓	✓	✓ 5,6,7,9		✓	
Allow/forbid use of iTunes Store / Google Play / Windows Store	✓	✓	✓	✓ 5,6,7	✓		
Allow/forbid use of Browser	✓	✓	✓	✓	✓		
Allow/forbid explicit content	✓	✓	✓				
Allow/forbid camera on lock screen	✓	✓		✓			
Allow/forbid widgets on lock screen	✓	✓		✓			
Prevent email forwarding	✓	✓	✓				
S/MIME enforcement	✓	✓	✓				
Allow/forbid 3rd party app usage of email	✓	✓	✓				
Allow/forbid iCloud autosync	✓	✓	✓				
Allow/forbid manual Wi-Fi configuration	✓	✓	✓ ²	✓ ⁵			
Allow/forbid to send crash data to Apple / Google / Samsung / Microsoft (Telemetry)	✓	✓	✓	✓ ⁵	✓	✓	
Allow/forbid certificates from untrusted sources	✓	✓	✓		✓		
Allow/forbid WiFi auto-connect	✓	✓	✓			✓	
Allow/forbid shared photo stream	✓	✓	✓				✓
Allow/forbid Apple Wallet/Passbook on lock screen	✓	✓	✓				
Allow/forbid device act as hotspot	✓	✓	✓			✓	✓
Allow/forbid recent contacts to sync	✓	✓	✓				
Allow/forbid Siri (iOS) or Cortana (Microsoft)	✓	✓	✓		✓	✓	
Allow/forbid Siri to query content from the web	✓	✓	✓ ²				
Support for SCEP certificate provisioning	✓	✓	✓	✓	✓		✓
Allow/forbid "Open with..." functionality to share data between managed and unmanaged apps	✓	✓	✓				
Allow/forbid fingerprint reader (Touch ID) to unlock device	✓	✓	✓	✓			✓
Allow/forbid account modification	✓	✓	✓ ²				
Allow/forbid modification of cellular data usage per app	✓	✓	✓ ²				
Allow/forbid Control Center on lock screen	✓	✓	✓				
Allow/forbid Notification Center on lock screen	✓	✓	✓		✓		
Allow/forbid Today view on lock screen	✓	✓	✓				
Allow/forbid over-the-air PKI updates	✓	✓	✓				
Allow/forbid find my friends modification	✓	✓	✓ ²				
Allow/forbid host pairing	✓	✓	✓ ²				
Allow/forbid iris scan authentication	✓	✓		✓ ⁵			

	Managed with Sophos Central	Installed On-Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Security (continued)							
Allow/forbid AirDrop	✓	✓	✓ ²				
Allow/forbid single app mode (app lock or kiosk mode)	✓	✓	✓ ²	✓ ^{5,6,7}			
Allow/forbid iBooks store	✓	✓	✓				
Allow/forbid explicit sexual content in iBooks store	✓	✓	✓				
Allow/forbid iMessage	✓	✓	✓				
Allow/forbid user to reset the device	✓	✓		✓ ^{5,6,7,9}	✓		
Allow/forbid device unenrollment from MDM management	✓	✓	✓ ²	✓ ^{5,6,7}	✓	✓	
Allow/forbid user to create screenshots	✓	✓		✓ ^{5,6,7,9}	✓		
Allow/forbid user to use copy/paste	✓	✓	✓	✓ ^{5,6,7}	✓		
Filter access to web sites (blacklisting) or whitelist web sites with bookmarks	✓	✓	✓ ²				✓
Block OS upgrade	✓	✓		✓ ^{5,7,9}			
Device configuration							
Microsoft Exchange settings for email	✓	✓	✓	✓ ^{5,6,7}	✓	✓	✓
IMAP or POP settings for email	✓	✓	✓		✓		✓
LDAP, CardDAV and CalDAV settings	✓	✓	✓				✓
Configuration of access points	✓	✓	✓	✓			
Proxy settings	✓	✓	✓	✓			✓
Wi-Fi settings	✓	✓	✓		✓	✓	✓
VPN settings	✓	✓	✓	✓ ^{5,6,7}			✓
Install root certificates	✓	✓	✓	✓ ⁵	✓	✓	✓
Install client certificates	✓	✓	✓	✓	✓		✓
Per app VPN	✓	✓	✓				
Single sign-on (SSO) for 3rd party apps (app protection) and company webpages	✓	✓	✓	✓			✓
Distribution of bookmarks (Web Clips)	✓	✓	✓				✓
Force iOS update on supervised devices (and display pending iOS updates)	✓	✓	✓ ²				
Configure the iOS lock screen and home screen	✓	✓	✓ ²				
Automatically receive Wi-Fi and VPN settings from Sophos UTM appliances	✓	✓		✓			
Managed domains	✓	✓	✓				✓
Kiosk Mode	✓	✓	✓	✓ ^{5,6,7,9}			
App permissions	✓	✓		✓ ⁹			
Enable iOS Lost Mode	✓	✓	✓				
Configure Google Accounts	✓	✓	✓				
Integrate with Duo Security	✓	✓	✓	✓			
Android enterprise: Configure password policy (workspace)	✓	✓		✓ ⁹			
Android enterprise: Configure password policy (device)	✓	✓		✓ ⁹			
Android enterprise: Configure restrictions	✓	✓		✓ ⁹			
Android enterprise: Configure Wi-Fi	✓	✓		✓ ⁹			
Android enterprise: Configure app protection	✓	✓		✓ ⁹			
Android enterprise: Configure app control	✓	✓		✓ ⁹			
Android enterprise: Configure app permissions	✓	✓		✓ ⁹			
Android enterprise: Configure Exchange	✓	✓		✓ ⁹			
Android enterprise: Install root certificate	✓	✓		✓ ⁹			
Android enterprise: Install client certificate	✓	✓		✓ ⁹			
Android enterprise: Install client certificate via SCEP	✓	✓		✓ ⁹			
Samsung Knox: Container handling (create, lock, decommission)	✓	✓		✓ ⁵			
Samsung Knox: Configure restrictions	✓	✓		✓ ⁵			
Samsung Knox: Configure Exchange	✓	✓		✓ ⁵			
Samsung Knox: Manage container password	✓	✓		✓ ⁵			
Samsung Knox: Allow/block data and file sync between Knox Workspace and personal area	✓	✓		✓ ⁵			
Samsung Knox: Allow/block Iris scan authentication for Knox Workspace	✓	✓		✓ ⁵			
Device information							
Internal memory utilization (free/used)	✓	✓	✓				✓
Battery charge level	✓	✓	✓	✓			
IMSI (unique identification number) of SIM card	✓	✓	✓	✓	✓		
Currently used cellular network	✓	✓	✓	✓			
Roaming mode	✓	✓	✓	✓	✓		
OS version	✓	✓	✓	✓	✓	✓	✓
List of installed profiles	✓	✓	✓	✓	✓	✓	✓
List of installed certificates	✓	✓	✓		✓	✓	✓
Malware detected on device	✓	✓		✓ ⁴		✓ ⁸	
Remote screen sharing (requires AirPlay device)	✓	✓	✓				
Secure Email (with Sophos Secure Email app)							
Exchange email	✓	✓	✓ ⁴	✓ ⁴			
Exchange contacts	✓	✓	✓ ⁴	✓ ⁴			
Exchange calendar	✓	✓	✓ ⁴	✓ ⁴			
Geo-fencing / Time-fencing / Wi-Fi fencing	✓	✓	✓ ⁴	✓ ⁴			
Control cut and copy	✓	✓	✓ ⁴	✓ ⁴			
Control screenshot	✓	✓		✓ ⁴			
Show event details	✓	✓	✓ ⁴	✓ ⁴			
Export contacts to device	✓	✓	✓ ⁴	✓ ⁴			
Define out of office message in the email app	✓	✓	✓ ⁴	✓ ⁴			
Unified calendar view	✓	✓	✓ ⁴	✓ ⁴			
Anti-phishing protection for links in emails	✓	✓	✓ ⁴	✓ ⁴			

	Managed with Sophos Central	Installed On-Premises	iOS	Android	Windows 10 Mobile	Windows 10 computers	macOS computers
Corporate Browser (with Sophos Secure Workspace)							
Browsing restricted to predefined corporate domains	✓	✓	✓ ⁴	✓ ⁴			
Preconfigured corporate bookmarks	✓	✓	✓ ⁴	✓ ⁴			
Password manager	✓	✓	✓ ⁴	✓ ⁴			
Client or user certificates to authenticate against corporate websites	✓	✓	✓ ⁴	✓ ⁴			
Root certificates	✓	✓	✓ ⁴	✓ ⁴			
Restricted cut, copy, and paste	✓	✓	✓ ⁴	✓ ⁴			
Content Management (with Sophos Secure Workspace app)							
Publish documents from Sophos Mobile server	✓	✓	✓ ⁴	✓ ⁴			
Geo-fencing / Time-fencing / Wi-Fi fencing	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Dropbox	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Google Drive	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Microsoft OneDrive personal and business	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Box	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Telekom MagentaCloud	✓	✓	✓ ⁴	✓ ⁴			
Content storage: Egnyte	✓	✓	✓ ⁴	✓ ⁴			
Content storage: OwnCloud	✓	✓	✓ ⁴	✓ ⁴			
Content storage: WebDAV (for example Windows Server, Strato Hi-Drive, etc.)	✓	✓	✓ ⁴	✓ ⁴			
User authentication	✓	✓	✓ ⁴	✓ ⁴			
FIPS 140-2 encryption with AES256	✓	✓	✓ ⁴	✓ ⁴			
DLP setting: Allow offline viewing	✓	✓	✓ ⁴	✓ ⁴			
DLP setting: Allow copy to clipboard	✓	✓	✓ ⁴	✓ ⁴			
DLP setting: Allow emailing in encrypted form	✓	✓	✓ ⁴	✓ ⁴			
DLP setting: Allow "open with" unencrypted, including emailing unencrypted	✓	✓	✓ ⁴	✓ ⁴			
Add files from mail or download to content app	✓	✓	✓ ⁴	✓ ⁴			
Select existing encryption key or create new user key		✓	✓ ⁴	✓ ⁴			
Integrated with SafeGuard Encryption for Cloud Storage		✓	✓ ⁴	✓ ⁴			
Shared keyring with Sophos SafeGuard		✓	✓ ⁴	✓ ⁴			
Lock container access on non-compliant devices	✓	✓	✓ ⁴	✓ ⁴			
Request call home based on time or by unlock count	✓	✓	✓ ⁴	✓ ⁴			
Edit or create Word, Excel, PowerPoint, and text format files	✓	✓	✓ ⁴	✓ ⁴			
Annotate PDF files	✓	✓	✓ ⁴	✓ ⁴			
Fill PDF forms	✓	✓	✓ ⁴	✓ ⁴			
View SafeGuard format password-protected HTML5 files	✓	✓	✓ ⁴	✓ ⁴			
Share documents as password-protected HTML5 files	✓	✓	✓ ⁴	✓ ⁴			
Anti-phishing protection for links in documents	✓	✓	✓ ⁴	✓ ⁴			
"View with Secure Workspace" access to encrypted documents from other apps	✓	✓	✓ ⁴	✓ ⁴			
Unlock app via fingerprint reader	✓	✓	✓ ⁴	✓ ⁴			
View, manage, and create Zip and 7z compressed archives	✓	✓	✓ ⁴	✓ ⁴			
Manage and store passwords secretly using KeePass format	✓	✓	✓ ⁴	✓ ⁴			
Mobile SDK (to be embedded in apps)							
App expiration date	✓	✓	✓ ⁴	✓ ⁴			
App embedded EULA	✓	✓	✓ ⁴	✓ ⁴			
App password (with SSO across all SDK-enabled apps)	✓	✓	✓ ⁴	✓ ⁴			
Geo-fencing of the app	✓	✓	✓ ⁴	✓ ⁴			
Time-fencing of the app	✓	✓	✓ ⁴	✓ ⁴			
Block app start on jailbroken or rooted devices	✓	✓	✓ ⁴	✓ ⁴			
Make Wi-Fi network mandatory for app usage	✓	✓	✓ ⁴	✓ ⁴			
Make available corporate Wi-Fi mandatory for app usage	✓	✓	✓ ⁴	✓ ⁴			
Telecom Cost Control							
Disable data while roaming	✓	✓	✓	✓ ^{5,9}	✓		
Disable voice while roaming	✓	✓	✓	✓ ⁵			
Control sync while roaming	✓	✓	✓	✓ ⁵			
Configure APN or Carrier settings	✓	✓	✓	✓			
Define data usage upper limit per device	✓	✓	✓	✓			
Compare data usage against limit	✓	✓	✓	✓			
Per app network usage rules	✓	✓	✓				

[1] Deleted

[2] Requires a supervised device

[3] By setting a pin or passcode

[4] Requires a Mobile Advanced or Central Mobile Advanced license

[5] Requires a device compatible with Samsung Knox Standard V2.1 or higher

[6] Required Sony extended MDM API enabled device

[7] Requires LG GATE enabled device

[8] With Windows Defender

[9] Android Enterprise ("Android for Work")