Security made simple.

Sophos Mobile 7

Feature Matrix

	Deployment		Device Platform			
	Managed with Sophos Central	Installed On Premise	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Server						
Admin User Interface						
Easy-to-use web interface	✓	✓	✓	✓	✓	✓
Flexible Dashboard with 23 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 login screen 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)	✓	✓	✓	✓[5,8,9]	✓	✓
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 login screen 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 SMC app	✓	✓	✓	✓	✓	
Blacklisted apps	✓	✓	✓	✓		
Whitelisted apps	✓	✓	✓	✓		
Mandatory apps	✓	✓	✓	✓		
Block installation from unknown sources (sideloading)	✓	✓		✓		
Data roaming setting	✓	✓	✓	✓	✓	
USB debugging setting	✓	✓		✓		
SMC client version	✓	✓	✓	✓	✓	
Malware detection	✓	✓		✓[4]		✓[10]
Suspicious apps detection	✓	✓		✓[4]		

	Managed with Sophos Central	Installed On Premise	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Device compliance enforcement rules (cont'd)						
Potentially unwanted apps detection	✓	✓		✓[4]		
Last malware scan	✓	✓		✓[4]		✓[10]
Locate for SMC 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 protection (call, SMS, MMS)	✓	✓		✓[4]		
Protection from malicous 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]		
Inventory						
Device groups	✓	✓	✓	✓	✓	✓
User oriented view on devices	✓	✓	✓	✓	✓	✓
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 real device name as name in the inventory	✓	✓	✓			
Marker for company-owned and privately-owned devices	✓	✓	✓	✓	✓	✓
Customer defined device properties with template support	✓	✓	✓	✓	✓	✓
Import/export of device information	✓	✓	✓	✓	✓	✓
Provisioning / Device enrollment						
Device enrollment wizard for admins	✓	✓	✓	✓	✓	✓
By email	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓
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						
Inventory export with applied filters	✓	✓	✓	✓	✓	✓
Export of all tables in the system as XLS or CSV	✓	✓	✓	✓	✓	✓
Malware reports (2 different reports)	✓	✓	✓	✓	✓	✓
Compliance log of all administrator activities	✓	✓	✓	✓	✓	✓
Compliance violation reports (2 different reports)	✓	✓	✓	✓	✓	✓
Device reports (10 different reports)	✓	✓	✓	✓	✓	✓
App reports (6 different reports)	✓	✓	✓	✓	✓	✓
Programming interface (API)						
Web service (REST) API for device information and provisioning from 3rd party systems	✓	✓	✓	✓	✓	✓
Devices						
SMC 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 SMC app		✓	✓	✓	✓	
Show privacy information	✓	✓	✓	✓	✓	

	Managed with Sophos Central	Installed On Premise	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Mobile 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	✓	✓		✓[5,8,9]		
Remote configuration of company apps (managed settings)	✓	✓	✓[2]			
Block specific apps from running (app blocker)	✓	✓	✓[2]	✓	✓	
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 length of the password	✓	✓	✓	✓	✓	
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	✓	✓			✓	✓
Activation/deactivation of device data encryption	✓	✓		✓	✓	
Block installation from unknown sources (sideloading)	✓	✓		✓[5]		
Block Wi-Fi	✓	✓	✓[2]	✓[5,8,9]		
Block Bluetooth	✓	✓		✓[5]		✓
Block data transfer via Bluetooth	✓	✓		✓[6]	✓	✓
Block data transfer via NFC	✓	✓		✓[6]	✓	
Block USB connections	✓	✓			✓	
Block camera	✓	✓	✓	✓[5]	✓	✓
Protection of settings against modification/removal by the user	✓	✓	✓			✓
Allow/forbid use of iTunes Store / Google Play / Windows Store	✓	✓	✓	✓[8]	✓	
Allow/forbid use of YouTube app	✓	✓	✓			
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 Copy to Clipboard	✓	✓		✓[5]		
Allow/forbid manual Wi-Fi configuration	✓	✓		✓[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	✓	✓	✓			✓
Configuration of profile lifetime	✓	✓	✓			
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]			

	Managed with Sophos Central	Installed On Premise	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
Security (cont'd)						
Allow/forbid AirDrop	✓	✓	✓ [2]			
Allow/forbid single app mode (app lock or kiosk mode)	✓	✓	✓ [2]	✓ [5,8,9]		
Allow/forbid iBooks store	✓	✓	✓			
Allow/forbid explicit sexual content in iBooks store	✓	✓	✓			
Allow/forbid iMessage	✓	✓	✓			
Allow/forbid user to reset the device	✓	✓		✓ [5,8,9]	✓	
Allow/forbid device unenrollment from MDM management	✓	✓		✓ [5,8,9]	✓	✓
Allow/forbid user to create screenshots	✓	✓			✓	
Allow/forbid user to use copy/paste	✓	✓			✓	
Filter access to web sites (blacklisting) or whitelist web sites with bookmarks	✓	✓	✓ [2]			
Block OS upgrade	✓	✓		✓ [5]		
Device configuration						
Microsoft Exchange settings for email	✓	✓	✓	✓ [5,8,9]	✓	✓
IMAP or POP settings for email	✓	✓	✓			
LDAP, CardDAV and CalDAV settings	✓	✓	✓			
Configuration of access points	✓	✓	✓	✓		
Proxy settings	✓	✓	✓			
Wi-Fi settings	✓	✓	✓	✓	✓	✓
VPN settings	✓	✓	✓	✓ [5]		
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)	✓	✓	✓			
Automatically receive Wi-Fi and VPN settings from Sophos UTM appliances	✓	✓	✓	✓		
Managed domains	✓	✓	✓			
Android enterprise ("Android for Work"): Configure password policy	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Configure restrictions	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Configure app protection	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Configure app control	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Configure app permissions	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Configure Exchange	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Install root certificate	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Install client certificate	✓	✓		✓ [11]		
Android enterprise ("Android for Work"): Install client certificate via SCEP	✓	✓		✓ [11]		
Samsung Knox: Container handling (create, lock, decommission)	✓	✓		✓ [6]		
Samsung Knox: Configure restrictions	✓	✓		✓ [6]		
Samsung Knox: Configure Exchange	✓	✓		✓ [6]		
Samsung Knox: Manage container password	✓	✓		✓ [6]		
Samsung Knox: Allow/block data and file sync between Knox Workspace and personal area	✓	✓		✓ [6]		
Samsung Knox: Allow/block Iris authentication for Knox Workspace	✓	✓		✓ [6]		
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]		✓ [10]
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]		
Show event details	✓	✓	✓ [4]	✓ [4]		
Export contacts to device	✓	✓	✓ [4]	✓ [4]		
Define out of office message in the email app	✓	✓	✓ [4]	✓ [4]		
Unfied calendar view	✓	✓	✓ [4]	✓ [4]		
Anti-phishing protection for links in emails	✓	✓	✓ [4]	✓ [4]		

	Managed with Sophos Central	Installed On Premise	Apple iOS	Android	Windows 10 Mobile	Windows 10 Desktop
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]		
Mobile Content Management (with Sophos Secure Workspace app)						
Publish documents from SMC 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]		
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]	✓	
Disable voice while roaming	✓	✓	✓	✓[5]		
Control sync while roaming	✓	✓		✓[5]		
Configure APN or Carrier settings	✓	✓	✓	✓		
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 and optionally an installation of a plug-in

[6] Samsung Knox V2.1 or higher

[7] Deleted

[8] Required Sony extended MDM API enabled device

[9] Requires LG GATE enabled device

[10] With Windows Defender

[11] Android for Work