SOPHOS

Security made simple.

# Sophos Mobile 9.0

## 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 33 different user-selectable 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 (classical AV plus maschine learning) | ✓ | ✓ | | ✓[4] | | ✓[8] | |
| System Integrity Protection required | ✓ | ✓ | | | | | ✓ |
| Firewall required | ✓ | ✓ | | | | | ✓ |
| Suspicious apps detection | ✓ | ✓ | | ✓[4] | | | |
| Sideloaded apps detection | ✓ | ✓ | ✓ | | | | |

© Copyright 2019. Sophos Ltd. All rights reserved.

| | Managed with Sophos Central | Installed On Premises | iOS | Android | Windows 10 Mobile | Windows 10 computers | macOS computers |
|---|---|---|---|---|---|---|---|
| Unmanaged configuration profile detection | ✓ | ✓ | ✓ | | | | |
| **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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Administrator guidance to resolve compliance issues | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| MitM attack detection | ✓ | ✓ | ✓[4] | ✓[4] | | | |
| **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 or Wireless, Cisco ISE, Check Point) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USSD code protection (e.g. *#2314#) | ✓ | ✓ | | ✓[4] | | | |
| Text message phishing detection | ✓ | ✓ | ✓ | | | | |
| Protection from malicous websites (web filtering) | ✓ | ✓ | ✓[2] | ✓[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 | ✓ | ✓ | ✓[2] | ✓[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) | ✓ | ✓ | ✓ | | | | ✓ |
| Android Zero-touch device enrollment | ✓ | ✓ | | ✓ | | | |
| Samsung Knox Mobile Enrollment | ✓ | ✓ | | ✓[5] | | | |
| 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 | ✓ | ✓ | ✓ | ✓ | ✓ | | |

© Copyright 2019. Sophos Ltd. All rights reserved.

| | Managed with Sophos Central | Installed On Premises | iOS | Android | Windows 10 Mobile | Windows 10 computers | macOS computers |
|---|---|---|---|---|---|---|---|
| Trigger device synchronization | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Co-branding of the Sophos Mobile Control app | | ✓ | ✓ | ✓ | ✓ | | |
| Show privacy information | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| **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 | ✓ | ✓ | | ✓ | ✓ | | |
| Block installation from unknown sources (sideloading) | ✓ | ✓ | | ✓[5,6,7] | | | |
| Block Wi-Fi | ✓ | ✓ | ✓[2] | ✓[1,5,6,7] | | | |
| Block Bluetooth | ✓ | ✓ | | ✓[1,5,6,7] | | ✓ | |
| Block data transfer via Bluetooth | ✓ | ✓ | | ✓[5] | ✓ | ✓ | |
| Block data transfer via NFC | ✓ | ✓ | | ✓[5,6,7] | ✓ | | |
| Block USB connections | ✓ | ✓ | | ✓[1,5,6,7] | ✓ | | |
| Block camera | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Protection of settings against modification/removal by the user | ✓ | ✓ | ✓ | ✓[1,5,6,7] | | ✓ | |
| 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 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] | | | | |
| 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] | | | |
| Prevent email forwarding | ✓ | ✓ | ✓ | | | | |
| S/MIME enforcement | ✓ | ✓ | ✓ | | | | |
| Support for SCEP certificate provisioning (incl. auto-renew) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Security (continued)** | | | | | | | |
| Allow/forbid AirDrop | ✓ | ✓ | ✓[2] | | | | |
| Allow/forbid single app mode (app lock or kiosk mode) | ✓ | ✓ | ✓[2] | ✓[5,6,7] | | | |

© Copyright 2019. Sophos Ltd. All rights reserved.

| | Managed with Sophos Central | Installed On Premises | iOS | Android | Windows 10 Mobile | Windows 10 computers | macOS computers |
|---|---|---|---|---|---|---|---|
| Allow/forbid iBooks store | ✓ | ✓ | ✓ | | | | |
| Allow/forbid explicit sexual content in iBooks store | ✓ | ✓ | ✓ | | | | |
| Allow/forbid iMessage | ✓ | ✓ | ✓ | | | | |
| Allow/forbid user to reset the device | ✓ | ✓ | | ✓ 1,5,6,7 | ✓ | | |
| Allow/forbid device unenrollment from MDM management | ✓ | ✓ | ✓ 2 | ✓ 5,6,7 | ✓ | ✓ | |
| Allow/forbid user to create screenshots | ✓ | ✓ | | ✓ 1,5,6,7 | ✓ | | |
| Allow/forbid user to use copy/paste | ✓ | ✓ | ✓ | ✓ 5,6,7 | ✓ | | |
| Filter access to web sites (blacklisting) or whitelist web sites with bookmarks | ✓ | ✓ | ✓ 2 | | | | ✓ |
| Delay or block OS upgrade | ✓ | ✓ | ✓ | ✓ 1,5,7 | | | ✓ |
| Allow/forbid password auto-fill | ✓ | ✓ | | | | | ✓ |
| Allow/forbid password sharing | ✓ | ✓ | | | | | ✓ |
| Allow/forbid password proximity requests | ✓ | ✓ | | | | | ✓ |
| Configure Device Guard settings | ✓ | ✓ | | | | ✓ | |
| **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 | ✓ | ✓ | ✓ | ✓ 1,5,6,7 | | | ✓ |
| 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 | ✓ | ✓ | ✓ | | | | ✓ |
| Firewall configuration | ✓ | ✓ | | | | | ✓ |
| Kernal Extension policy | ✓ | ✓ | | | | | ✓ |
| Kiosk Mode | ✓ | ✓ | ✓ | ✓ 1,5,6,7 | | | ✓ |
| App permissions | ✓ | ✓ | | ✓ 1 | | | |
| Enable iOS Lost Mode | ✓ | ✓ | ✓ | | | | |
| Configure Google Accounts | ✓ | ✓ | ✓ | | | | |
| Integrate with Duo Security | | ✓ | ✓ | ✓ | | | |
| Android enterprise: Configure password policy (workspace) | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure password policy (device) | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure restrictions | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure Wi-Fi | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure app protection | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure app control | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure app permissions | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Configure Exchange | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Install root certificate | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Install client certificate | ✓ | ✓ | | ✓ 1 | | | |
| Android enterprise: Install client certificate via SCEP | ✓ | ✓ | | ✓ 1 | | | |
| 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 | | | |
| Configure devices to use AirPrint printers | ✓ | ✓ | ✓ | | | | ✓ |
| **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 Teamviewer or 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 | | | |

© Copyright 2019. Sophos Ltd. All rights reserved.

| | Managed with Sophos Central | Installed On Premises | iOS | Android | Windows 10 Mobile | Windows 10 computers | macOS computers |
|---|---|---|---|---|---|---|---|
| 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] | | | |
| Unfied calendar view | ✓ | ✓ | ✓[4] | ✓[4] | | | |
| Anti-phishing protection for links in emails | ✓ | ✓ | ✓[4] | ✓[4] | | | |
| **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 secrely 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 | ✓ | ✓ | ✓ | ✓[1,5] | ✓ | | |
| 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) Support for Android Enterprise (former "Andriod for work")

(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

© Copyright 2019. Sophos Ltd. All rights reserved.