SOPHOS

Security made simple.

Sophos Mobile Control
Technical Guide

Product version: 4
Document date: May 2014

Contents

1 About Sophos Mobile Control

Sophos Mobile Control is a device management solution for mobile devices. It allows configuration and software distribution as well as security settings and many other device management operations on mobile devices.

The Sophos Mobile Control system consists of a server and a client component which communicate through data connections and text messages.

Sophos Mobile Control currently supports the following mobile device platforms:

- Apple iOS
- Android
- Windows Phone 8
- Windows Mobile
- BlackBerry (through BlackBerry Enterprise Server)

  Note: For BlackBerry devices only the following functions are supported in the Sophos Mobile Control web interface: show devices in Sophos Mobile Control, Lock, Wipe, show software inventory, show device properties. The Self Service Portal does not support BlackBerry devices.

Sophos Mobile Security management through the Sophos Mobile Control web console is available as an optional module. Sophos Mobile Security is a security app for Android phones and tablets that protects devices from malicious apps and assists end users in detecting apps permissions that could be a security risk. In order to manage the Sophos Mobile Security app from Sophos Mobile Control, a license needs to be available and activated in the Sophos Mobile Control web console. For further information on managing Sophos Mobile Security through the web console, see the *Sophos Mobile Control administrator guide*. For further information on the Sophos Mobile Security app, see the *Sophos Mobile Security help*.

This manual describes the Sophos Mobile Control system's architecture and workflow.

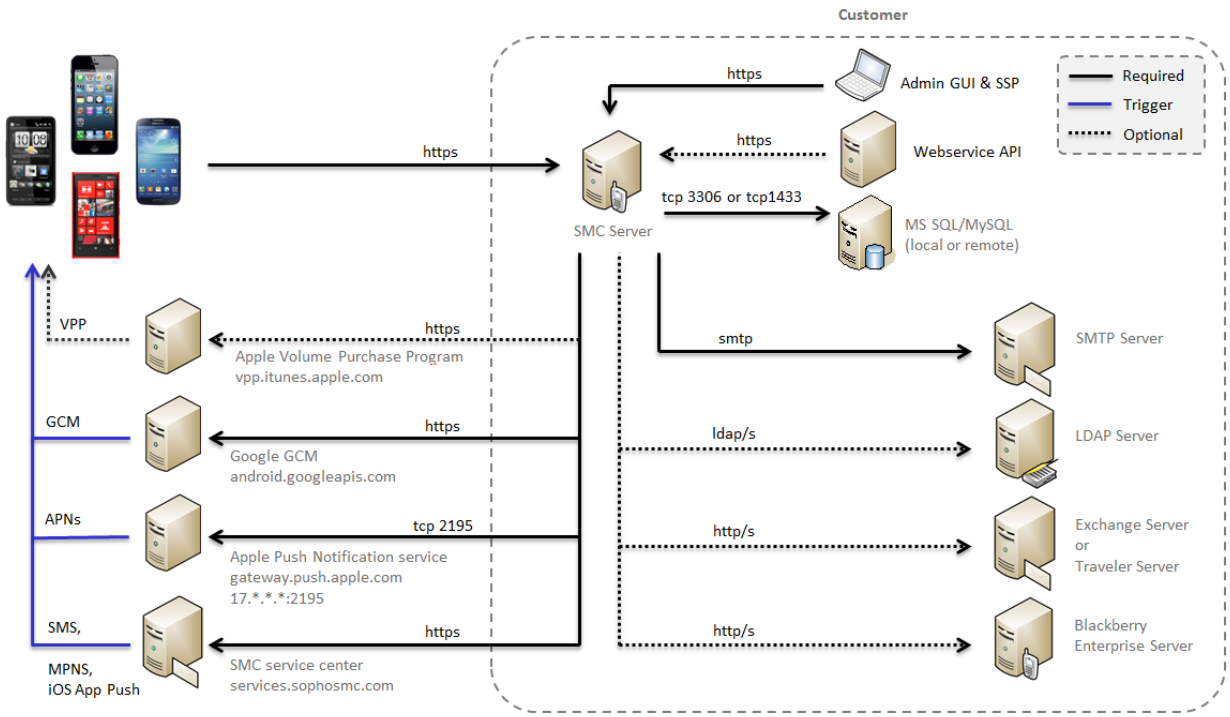
1.1 Terminology

Term or Abbreviation	Description
APNs	Apple Push Notification service
DB	Database
DMZ	Demilitarized Zone
DS	Data Synchronization

Term or Abbreviation	Description
EAS	Exchange ActiveSync
GCM	Google Cloud Messaging
IMEI	Unique serial number of a mobile device
IMSI	International Mobile Subscriber Identity
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MPNS	Microsoft Push Notification Service
OMA	Open Mobile Alliance
SMS	Short Message Service
SSP	Self Service Portal
SyncML	Synchronization Markup Language

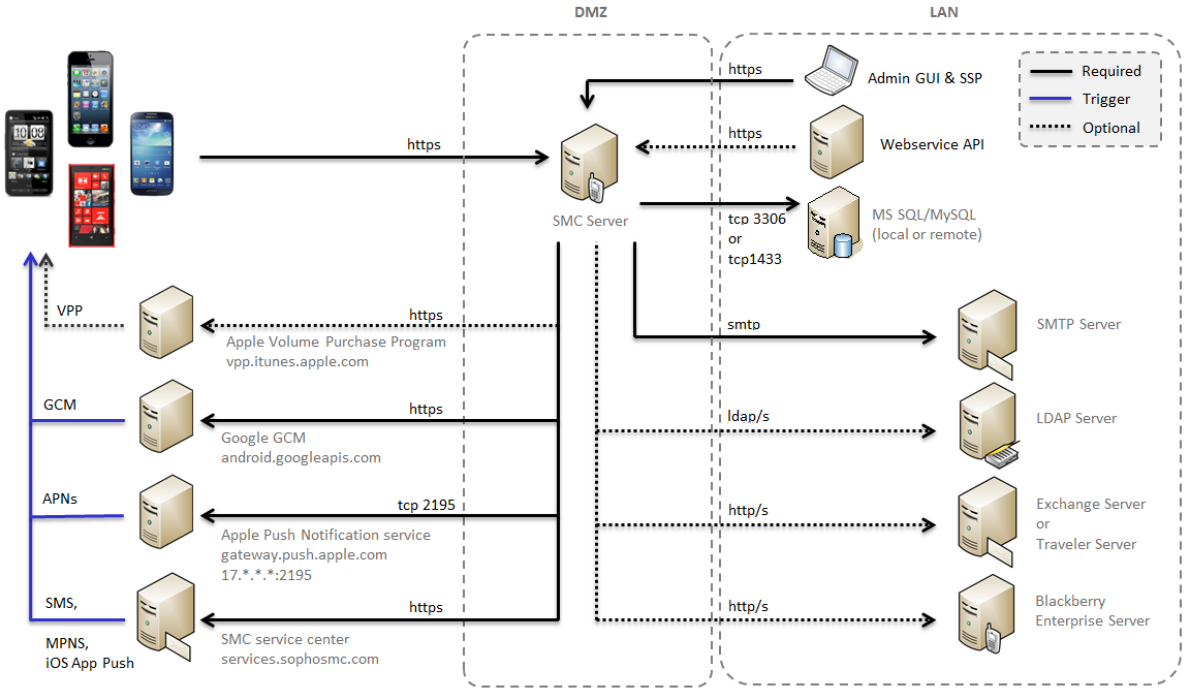
2 Integration

The following graphic shows how the Sophos Mobile Control server (SMC server) can be integrated into a company's infrastructure.



DMZ

The SMC Server can be installed in the DMZ (Demilitarized Zone) network segment.


DMZ
LAN
Required
Trigger
Optional
https
Admin GUI & SSP
https
Webservice API
https
SMC Server
tcp 3306
or
tcp1433
MS SQL/MySQL
(local or remote)
VPP
https
Apple Volume Purchase Program
vpp.itunes.apple.com
smtp
SMTP Server
GCM
https
Google GCM
android.googleapis.com
ldap/s
LDAP Server
APNs
tcp 2195
Apple Push Notification service
gateway.push.apple.com
17.*.*.*:2195
http/s
Exchange Server
or
Traveler Server
SMS,
MPNS,
iOS App Push
https
SMC service center
services.sophosmc.com
http/s
Blackberry
Enterprise Server

3 Architecture

3.1 Sophos Mobile Control Server

The core component of the system is the Sophos Mobile Control server.

- It is connected to the Internet.
- The administrator controls the server using the web interface.
- End users can register their devices by using the Self Service Portal.
- The mobile devices synchronize with the server through HTTPS.
- The server notifies iOS clients trough APNs, Android clients through SMS or GCM and Windows Mobile clients through SMS. Windows Phone 8 devices receive their tasks by connecting to the server in fixed intervals. Text messages and tile updates can be sent to Windows Phone 8 devices by MPNS.
- A database is used for storage. The database does not necessarily have to reside on the same machine.
- It supports multi-tenant setups to allow different customers on the same server.
- EAS integrated or standalone for email access. For the standalone variant HTTPS access to the SMC server is required.

The Sophos Mobile Control server has been developed for the Java enterprise environment (JEE). It installs and runs inside the well tested industry standard application server JBoss.

The default environment for the SMC server is Windows Server 2008. The server may be installed in virtualized environments.

3.1.1 Business logic

The Sophos Mobile Control server provides the business logic for the administration of data and the scheduler functionality. Every device management operation results in a task. These tasks are handled by the time driven scheduler. All tasks follow a well defined state process. The scheduler queries the database for tasks and handles the transition to the next state. This may for example result in a notification being sent or data being prepared for synchronization.

3.1.2 Web interface

3.1.2.1 Administration interface

The web interface is secured by a login and a session mechanism. You can implement password policies. Access control allows different user roles. The predefined roles are:

- Administrator
- User
- Helpdesk

These roles have different sets of access rights. Additional roles can be created. Each user can be assigned exactly one role.

These are the most important components of the web interface:

- **Task view and archive**

  Used to monitor current and completed management operations including detailed status info.

- **Inventory**

  Used to administer registered devices and device groups.

- **Applications**

  Used to manage software packages and to (un-)install them on the devices.

- **Profiles**

  Used to create and apply configuration profiles for individual platforms.

- **Task bundles**

  Used to bundle several tasks for mobile devices in one transaction. All tasks necessary to have a device fully registered and running can be combined in a task bundle.

- **Command bundles**

  Used to define custom bundles of Sophos Mobile Control client commands to be transferred to the clients in a single task.

  Note: In the administrator web console, the **Command bundles** function is disabled by default. It can be enabled in the **Personal** tab of the **General settings** view. For further information, *see the Sophos Mobile Control administrator help*.

- **Backup**

  Used to configure data backups for Android and Windows Mobile devices. The backups handle SMS messages, bookmarks and user defined directory paths.

Note: In the administrator web console, the **Backup** function is disabled by default. It can be enabled in the **Personal** tab of the **General settings** view. For further information, *see the Sophos Mobile Control administrator help*.

- **Reports**

  Used to create device, app and compliance reports.

- **Compliance rules**

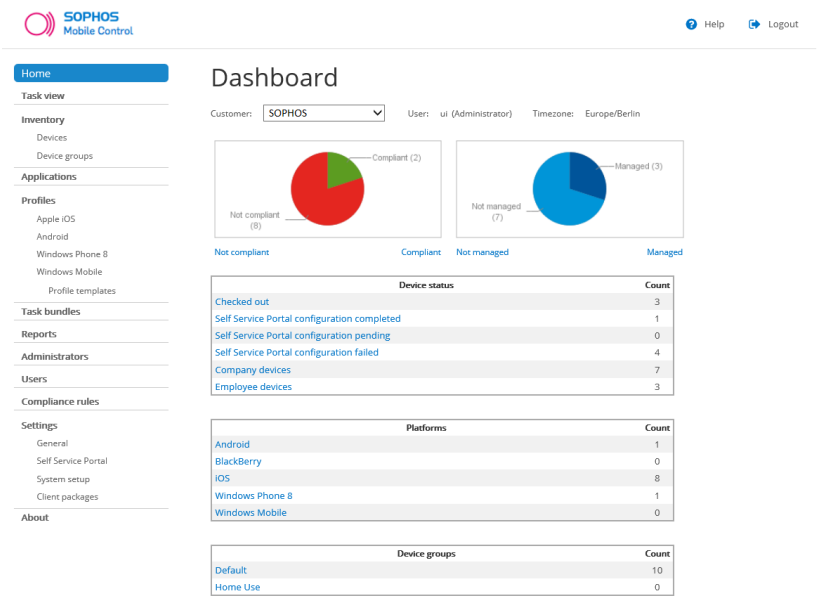
  Used to define compliance rules for individual platforms. You can define different compliance rules for different device groups and private or employee devices.

- **Settings**

  Used to define the following type of settings:

  - **General**
  - **Self Service Portal**
  - **System setup**
  - **Client packages**

Optional filters are available in many views of the web interface for restricting the number of items displayed. All kinds of operations follow the same wizard structure which makes it easy to work with the web interface.



For further information, see the *Sophos Mobile Control administrator guide*.

3.1.2.2 Super administrator interface

A super administrator has specific rights and tasks in Sophos Mobile Control administration. The first super administrator account is created during Sophos Mobile Control setup, see the *Sophos Mobile Control installation guide*. The super administrator is primarily used to set up and manage customers for device management.

As a super administrator you log on to the super administrator customer which is also created during Sophos Mobile Control configuration. The Sophos Mobile Control web console shows a specific view for the super administrator customer. This view is customized for super administrator tasks.

For further information, see the *Sophos Mobile Control super administrator guide*.

3.1.2.3 Self Service Portal

The Self Service Portal is secured by a login, session mechanism and a password policy. The account has to be set up by the administrator of the server and can be associated with any tenant. The Self Service Portal is designed for the end users of devices and enables them to perform the provisioning process and MDM client bootstrap process of the device by themselves. The end users are also allowed to perform tasks for their devices, for example remote lock or remote wipe. The tasks they can perform vary according to device type and configuration. As an administrator you can configure the Self Service Portal functions available to end users in the Sophos Mobile Control web console.

For further information on how to configure the Self Service Portal use for end users, see the *Sophos Mobile Control administrator guide*.

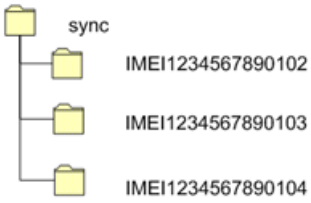
For further information on how to use the Self Service Portal as an end user, see the *Sophos Mobile Control user guides for Android, Apple iOS, Windows Phone 8 and Windows Mobile*.

3.1.3 Database

The database stores all data needed for the operation of Sophos Mobile Control. This includes device and application information. Sophos Mobile Control connects to the database through JDBC (Java database connectivity) drivers. The database does not have to be installed on the same machine as the Sophos Mobile Control server. For example, existing database clusters can be used.

3.1.4 File system

The Sophos Mobile Control server's central synchronization directory includes a directory named after the serial number for each registered device. These IMEI directories are synchronized with the corresponding devices.



3.2 Client overview

Sophos Mobile Control supports the native Sophos Mobile Control clients and the Apple MDM clients.

3.2.1 Apple iOS and Windows Phone 8 MDM Clients

The Sophos Mobile Control server can control devices that feature the built-in Apple iOS and Windows Phone 8 MDM client. On the end user device, first the Apple iOS or Windows Phone 8 MDM profile has to be installed followed by the Sophos Mobile Control app.

The Windows Phone 8 MDM Client is part of the System Settings of a Windows Phone 8 device. MDM can only be configured through this client. Manual synchronization processes with the server can only be triggered through the device.

3.2.2 Sophos Mobile Control client

The Sophos Mobile Control client is a piece of software that resides on the mobile device. It is available for a number of different operating systems and versions.

Note: Due to the natures of different operating systems not every feature is available on every platform.

The client receives the command to synchronize with the server to receive tasks. It also monitors specific actions of the device and reports them to the server (for example software installations by the user). The following sections explain the most important modules.

Note: For Windows Phone 8 devices, different scenarios apply. The Sophos Mobile Control Windows Phone 8 client synchronizes with the server in regular intervals, for example to load compliance violations and support information. Messages can be sent through MPNS. They are only received and displayed if the app is open on the device or if the user has tapped on the toast notification for incoming messages.

3.2.2.1 SMS recognizer

The recognizer monitors the device's messaging inbox for the trigger SMS sent by the server. The mechanism used depends on the operating system of the device. The trigger SMS is not visible to the user.

3.2.2.2 Command dispatcher

This module dispatches incoming commands to the corresponding modules. The use of this dispatcher module makes the client flexible and allows extensions to be added easily.

3.2.2.3 Synchronization module

This essential module handles all synchronization processes with the server. Synchronization processes are carried out using the OMA DS protocol which is implemented in this module.

3.2.2.4 Installation module

This module handles the installation and removal of software packages. Depending on the device's operating system, the module allows different ways of installing software (silent/non-silent). It also adds the processes of the software installed to the white list.

3.2.2.5 Process module

This module monitors the processes running on the device and ensures that no processes are started which are not white-listed in the configuration. By default, all operating system processes and processes installed by Sophos Mobile Control are white-listed.

4 Workflow

4.1 Data synchronization

Data synchronization is the basic method of transferring data between Sophos Mobile Control Server and Client. The OMA DS (former SyncML DS) protocol is used for synchronization.

For Windows Phone 8 OMA DM is used. The Windows Phone 8 Client uses XMLComm and PropComm.

4.1.1 Trigger

Synchronization is either triggered by a command of the administrator followed by an SMS, GCM or APNs message of the Sophos Mobile Control server, or as a result of a user-initiated action on the device. By default synchronization is also triggered automatically for iOS devices 24 hours after the last synchronization process. For other platforms this is controlled by the client.

Note: For Windows Phone 8 devices synchronization cannot be triggered automatically. The devices connect to the server in a defined interval. This interval can be defined once per enrollment. You define the interval in the Sophos Mobile Control web console in the **Windows Phone client** tab of the **General Settings** view. For further information, *see the Sophos Mobile Control administrator help*. If you need to change the interval afterwards, you need to deregister the device, specify the new interval and enroll it again.

Synchronization processes triggered by the client may be caused by the following actions:

- An application is being installed or uninstalled on the device.
- The client has not contacted the server for a certain period of time.

The Sophos Mobile Control server sends SMS, GCM or APNs messages to trigger synchronization processes to the Sophos Mobile Control client for each management task the administrator defines, for example:

- (Un-)installation of software packages
- Security policy changes
- Process white list changes

Note: For Windows Phone 8 devices, synchronization may be triggered by sending an MPNS message, if the user taps the toast notification and starts the app. Otherwise, synchronization cannot be triggered automatically.

4.1.2 Execution

Data synchronization consists of a common balancing of files in directories as is usual in current synchronization proceedings. Files from certain directories are compared between server and client. Server and client remember the directory structure after each synchronization process. Each client has a separate synchronization directory on the server.

4.1.3 Synchronization

This is a typical management operation workflow:

1. The device is monitored for an incoming message containing a trigger word. (The SMS, GCM and APNs messages are retrieved before the device's messaging application notifies the user.)
2. After parsing the message the contained command is executed. (In most cases this is a synchronization process.)
3. During synchronization, the management operations to be performed are transferred to the client. Software packages that are to be installed are also transferred to the client.
4. The client executes the commands.
5. The client lists concerned are refreshed (software list, process list).
6. The client generates a result file including success or detailed error information.
7. The result and the modified lists are transferred to the server.

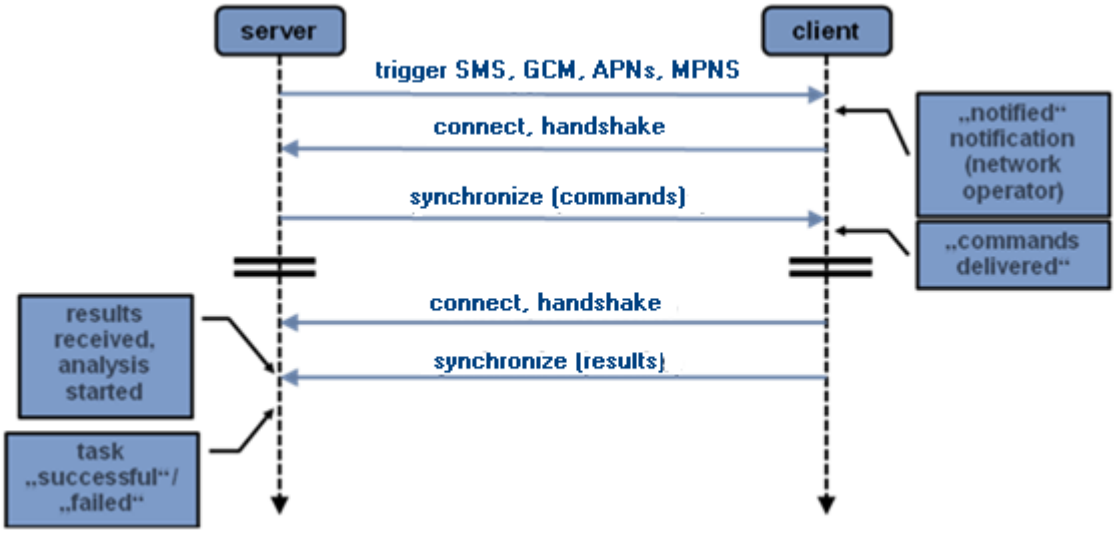
This mechanism forms the fixed frame for every management operation process mentioned.

4.2 Installation and usage of the Sophos Mobile Control client

For installing a Sophos Mobile Control client on a mobile device, synchronization cannot be used, because the client has not been installed yet. For bootstrap, a standard mechanism has to be used that works on every supported device. This is based on the dispatch of a link that points to an installation file for the corresponding operating system. The file type and/or MIME type are known to the device as an installable application or for iOS devices as a base profile. The user has to open the link and accept installation.

After client installation specific information of the device is collected and sent to the server during the first synchronization process.

The client can now be controlled via Sophos Mobile Control server to carry out the management operations and report results.



4.2.1 Installation and usage on Windows Phone 8 devices

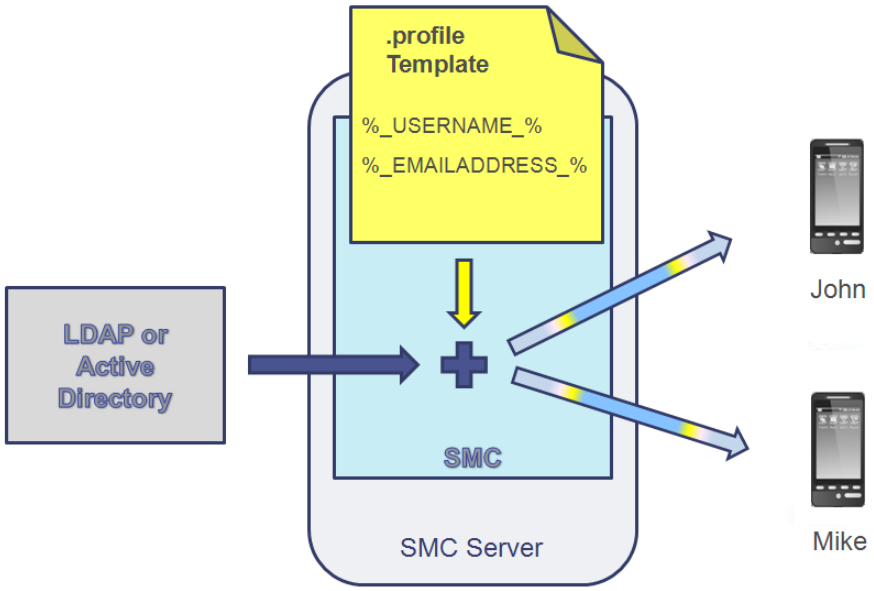
For Windows Phone 8 devices a different scenario applies to the installation and usage of the Sophos Mobile Control client.

For setting up Sophos Mobile Control on a Windows Phone 8 device, the Self Service Portal provides all relevant information to the user. The user has to specify the relevant information on the device under **Company apps**. For a detailed description of the setup process, see the *Sophos Mobile Control user guide for Windows Phone 8*.

After Sophos Mobile Control has been set up on a Windows Phone 8 device, it receives its tasks by connecting to the server in fixed intervals.

5 Directory Access

Sophos Mobile Control allows the customization of generic configuration profiles with user-specific data retrieved from Directories via LDAP (Lightweight Directory Access Protocol) as supported by Microsoft Active Directory and Lotus Domino. The generic profile may contain placeholders which are replaced by user data at the time of task execution. Using directory access it is possible to have just one generic profile (which is easy to maintain) and have it personalized for each device. This minimizes the necessary user input on the target device.



Note: Placeholders must be entered in upper case.

Directory access can also be used for the Self Service Portal login. In this case you can log in to the Self Service Portal with the relevant domain user, if the user is a member of the Self Service Portal group. You can use an existing LDAP group as the Self Service Portal Group. You can also create a new group and assign the relevant users to it. Otherwise internal user management must be used.

6 Microsoft Exchange ActiveSync Proxy

With the module EAS Proxy, Sophos Mobile Control provides a means for filtering incoming ActiveSync traffic as used by Microsoft Exchange and Lotus Traveler for iOS and Samsung SAFE devices. For Android and Windows Mobile devices a Traveler client is available that uses its own protocol. This protocol is only supported by the external EAS Proxy. For further information, see the *Sophos Mobile Control installation guide*. The component is installed as the ActiveSync endpoint known by the mobile devices. It only forwards traffic to the Exchange server, if the device is known in Sophos Mobile Control and matches the required policies. This guarantees higher security as the Exchange server does not need to be accessible from the Internet and only authorized (correctly configured, for example passcode guidelines) devices can access it. Access to Exchange can also be blocked for specific devices through the web interface.

The EAS Proxy component is part of the Sophos Mobile Control Server. For specific scenarios it is also available as a standalone component. The EAS Proxy is automatically installed with Sophos Mobile Control. Sophos Mobile Control also offers a separate installer for an external EAS Proxy (for example for load balancing or processing Lotus Notes traffic).

The standalone variant communicates by web interface (HTTPS) with the Sophos Mobile Control Server. If you use Sophos Mobile Control as a service, the EAS Proxy server is therefore suitable for installation in your own environment.

For further information, refer to the *Sophos Mobile Control installation guide*.

7 Security

7.1 Web interface

The web interface is secured by SSL (HTTPS). The default certificate uses 128 bit encryption. If necessary, stronger encryption certificates can be used. Users have to identify themselves by entering customer name, user name and user password to log in to the system's web interface. Optionally you can secure access to the Self Service Portal or the web console with an IP range whitelist.

7.2 SMS trigger

The SMS messages used to trigger the Sophos Mobile Control client are encrypted and protected against replay attacks on other devices. This is achieved by including the device's IMEI in the encryption key.

7.3 Data synchronization

Synchronization is generally encrypted with a standard SSL/HTTPS connection and a server certificate.

The Sophos Mobile Control client authenticates at the server by user name (IMEI) and an individual password. This ensures that foreign clients cannot synchronize with the Sophos Mobile Control server. The Sophos Mobile Control client does not accept any incoming connections. As the connections are always initiated by the Sophos Mobile Control client, it is ensured that no foreign server can synchronize with the client.

8 Sophos Mobile Control feature matrix

The following matrix shows the Sophos Mobile Control features available per device type.

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
SERVER					
Admin user interface					
Easy-to-use web interface	✓	✓	✓	✓	✓
Dashboard	✓	✓	✓	✓	✓
Flexible filter mechanism	✓	✓	✓	✓	✓
Role-based access	✓	✓	✓	✓	✓
Multitenancy	✓	✓	✓	✓	✓
Sending of text messages (via APNs, GCM, MPS, SMS)	✓	✓	✓	✓	✓
Self Service Portal					
Register new device	✓	✓	✗	✓	✓
Device wipe	✓	✓	✗	✓	✓
Device lock	✓	✓	✗	✗	✗
Device locate	✓	✓	✗	✗	✓
Passcode reset	✓	✓	✗	✗	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Synchronize device	✓	✓	✗	✓	✗
Decommission device from management (incl. corporate wipe on iOS, Samsung SAFE, Windows Phone 8)	✓	✓	✗	✗	✓
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	✓	✓	✗	✓	✓
User management					
Comprehensive password policies	✓	✓	✓	✓	✓
Password recovery by the user	✓	✓	✓	✓	✓
Internal user directory	✓	✓	✓	✓	✓

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Microsoft ActiveDirectory integration	✓	✓	✓	✓	✓
Novell eDirectory integration	✓	✓	✓	✓	✓
Lotus Notes Directory integration	✓	✓	✓	✓	✓
Device compliance enforcement rules					
Group assignment or ownership-based compliance rules	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Mandatory apps	✓	✓	✓	✓	✗
Block installation from non-Google markets	✗	✓	✗	✗	✗
Data roaming setting	✓	✓	✗	✗	✗
USB Debugging setting	✗	✓	✗	✗	✗
SMC client version	✓	✓	✗	✓	✓
Malware detection	✗	✓ (4)	✗	✗	✗
Suspicious apps detection	✗	✓ (4)	✗	✗	✗
Potentially unwanted apps detection	✗	✓ (4)	✗	✗	✗
Last malware scan	✗	✓ (4)	✗	✗	✗
Locate for SMC app enabled	✓	✓	✗	✗	✓
Security					
Encrypted connection to web interface	✓	✓	✓	✓	✓
Encrypted communication with devices	✓	✓	✓	✓	✓
Trusted Devices (Exchange ActiveSync Proxy)	✓	✓	✗	✓	✓
Control networ access by compliance state (NAC interface)	✓	✓	✓	✓	✓

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Trigger malware scan on device	✗	✓ (4)	✗	✗	✗
USSD code protection (for example *#2314#)	✗	✓ (4)	✗	✗	✗
Spam protection (call, SMS, MMS)	✗	✓ (4)	✗	✗	✗
Protection from malicious websites (web filtering)	✗	✓ (4)	✗	✗	✗
Inventory					
Easy to handle with device templates	✓	✓	✓	✓	✓
Grouping devices	✓	✓	✓	✓	✓
Automatic transfer of unique device ID (IMEI, MEID, UDID) and further device data	✓	✓	✓	✓	✓
Automatic OS version detection	✓	✓	✓	✓	✓
Marker for company-owned and privately owned devices	✓	✓	✓	✓	✓
Import/export of device information	✓	✓	✓	✓	✓
Provisioning					
By SMS	✓	✓	✗	✓	✗
By email	✓	✓	✗	✗	✓

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Online registration from the device	✓	✓	✗	✗	✓
Bulk provisioning (by SMS or email)	✓	✓	✗	✓	✓
Definition of standard rollout packages	✓	✓	✗	✓	✓
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 filters	✓	✓	✓	✓	✓
Graphical report of device inventory state	✓	✓	✓	✓	✓
Compliance violation report (2 different kinds)	✓	✓	✓	✓	✓
Device reports (7 different kinds)	✓	✓	✓	✓	✓
App reports (6 different kinds)	✓	✓	✓	✓	✓

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
DEVICES					
SMC app functionality					
Enterprise App Store (required and recommended apps)	✓	✓	✗	✗	✓
Show compliance violations	✓	✓	✗	✗	✓
Show SMC messages	✓	✓	✗	✗	✓
Show technical contact	✓	✓	✗	✗	✓
Trigger device synchronization	✓	✓	✗	✗	✓
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	✓	✓	✓	✓	✗
Block user-initiated installing or uninstalling of apps	✗	✗	✗	✓	✗
Support for Apple Volume Purchasing Program (VPP) both voucher-based and license-based	✓	✗	✗	✗	✗
Allow forbid installation of apps	✓	✗	✗	✓	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Remote configuration of company apps (managed settings)	✓ (10)	✗	✗	✗	✗
Security					
Jailbreak (iOS)/Rooting (Android) detection	✓	✓	✗	✗	✗
Changes of SIM cards are identified and send to the administrator including the new telephone number	n/a	✓	✗	✓	✗
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 up to the query of the password)	✓	✓	✗	✓	✓
Maximum number of attempts until the device will be reset	✓	✓	✗	✓	✓
Minimum length of the password	✓	✓	✗	✓	✓
Password history	✓	✓ (2)	✗	✓	✓
Password expiration time	✗	✓ (2)	✗	✓	✓

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Minimum length of lower/upper case, non-letter or symbol characters in the passcode	✗	✓ (2)	✗	✗	✗
Password reset (unlock)/administrator defines new password	✓	✓	✓	✗	✗
Activation of storage encryption	✓ (3)	✓ (2)	✗	✗	✗
Access to the memory card can be prohibited	✗	✗	✗	✓	✓
Activation, deactivation or enforcement of memory card encryption	✗	✗	✗	✓	✗
Activation or deactivation of device data encryption	✗	✗	✗	✓	✗
Blocking installation from non Google Play markets	✗	✓ (5)	✗	✗	✗
Blocking of WiFi	✗	✓ (5)	✗	✓	✗
Blocking of Bluetooth	✗	✓ (5)	✗	✓	✗
Blocking of data transfer via Bluetooth	✗	✗	✗	✓	✗
Blocking of data transfer via Infrared	✗	✗	✗	✓	✗
Blocking of wired ActiveSync connections	✗	✗	✗	✓	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Blocking of camera	✓	✓ (5), (7)	✗	✓	✗
Protection of settings against modification/removal by the user	✓	✗	✗	✓	✗
Allow or forbid use of iTunes Store/Google Play/Windows Store	✓	✓ (5)	✗	✗	✗
Allow or forbid use of YouTube app	✓	✗	✗	✓	✗
Allow or forbid use of Browser	✓	✓ (5)	✗	✓	✗
Allow or forbid explicit content	✓	✗	✗	✗	✗
Allow/forbid camera on lock screen	✗	✓ (7)	✗	✗	✗
Allow/forbid widgets on lock screen	✗	✓ (7)	✗	✗	✗
Prevent email forwarding	✓ (1)	✗	✗	✗	✗
S/MIME enforcement	✓ (1)	✗	✗	✗	✗
Allow or forbid 3rd party app usage of email	✓ (1)	✗	✗	✗	✗
Allow or forbid iCloud autosync	✓ (1)	✗	✗	✗	✗
Allow or forbid to send crashed data to Apple / Google / Samsung / Microsoft	✓ (1)	✓ (5)	✗	✗	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Allow or forbid certificates from non-trusted sources	✓ (1)	✗	✗	✗	✗
Allow/forbid WiFi auto-connect	✓ (1)	✗	✗	✗	✗
Allow or forbid shared photo stream	✓ (6)	✗	✗	✗	✗
Allow or forbid Passbook on lock screen	✓ (6)	✗	✗	✗	✗
Allow/forbid synchronization while roaming	✗	✓ (5)	✗	✗	✗
Allow/forbid mobile data connection while roaming	✗	✓ (5)	✗	✗	✗
Allow/forbid voice calls while roaming	✗	✓ (5)	✗	✗	✗
Configuration of profile lifetime	✓ (6)	✗	✗	✗	✗
Allow/forbid device to act as a hotspot	✓ (10)	✗	✗	✗	✗
Allow/forbid recent contacts to sync	✓ (6)	✗	✗	✗	✗
Allow/forbid Siri	✓ (1)	✗	✗	✗	✗
Allow/forbid Siri querying content from the web	✓ (11)	✗	✗	✗	✗
Support for SCEP certificate provisioning	✓ (9)	✗	✗	✗	✗
Allow/forbid "Open with" functionality to share data between	✓ (10)	✗	✗	✗	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
managed and unmanaged apps.					
Allow/forbid fingerprint reader (Touch ID) for unlocking device	✔ (10)	✘	✘	✘	✘
Allow/forbid account modification	✔ (11)	✘	✘	✘	✘
Allow/forbid modification of cellular data usage per app	✔ (11)	✘	✘	✘	✘
Allow/forbid Control Center on lock screen	✔ (10)	✘	✘	✘	✘
Allow/forbid Notification Center on lock screen	✔ (10)	✘	✘	✘	✘
Allow/forbid Today view on lock screen	✔ (10)	✘	✘	✘	✘
Allow/forbid over-the-air PKI updates	✔ (10)	✘	✘	✘	✘
Allow/forbid find my friends modification	✔ (11)	✘	✘	✘	✘
Allow/forbid host pairing	✔ (11)	✘	✘	✘	✘
Allow/forbid AirDrop	✔ (11)	✘	✘	✘	✘
Allow/forbid single app mode (app lock or kiosk mode)	✔ (11)	✘	✘	✘	✘
Allow/forbid iBooks store	✔ (10)	✘	✘	✘	✘

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Allow/forbid explicit sexual content in iBooks store	✓	✗	✗	✗	✗
Allow/forbid iMessage	✓ (10)	✗	✗	✗	✗
Filter access to websites (blacklisting) or whitelist websites by bookmarks	✓ (11)	✗	✗	✗	✗
Device configuration					
Blocking of configuration areas	✗	✗	✗	✓	✗
Microsoft Exchange settings for email	✓	✓ (5, 12)	✗	✓	✓
IMAP or POP settings for email	✓	✗	✗	✓	✗
LDAP and CalDAV settings	✓	✗	✗	✗	✗
Add, delete or change registry data	✗	✗	✗	✓	✗
Configuration of energy options	✗	✗	✗	✓	✗
Configuration of access points	✓	✓	✗	✓	✗
Proxy settings	✓	✗	✗	✓	✗
WiFi settings	✓	✓	✗	✓	✗
VPN settings	✓	✓ (5)	✗	✓	✗
Per app VPN	✓ (10)	✗	✗	✗	✗

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Distribution of bookmarks	✗	✗	✗	✓	✗
Single sign on (SSO) for 3rd party apps (app protectoin and company webpages (iOS 7 only)	✓ (10)	✓	✗	✗	✗
Device information					
Internal memory utilization (free/used)	✓	✗	✓	✓	✗
Memory card 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)	✗	✗	✗
Remote screen sharing (requires AirPlay device)	✓ (10)	✗	✗	✗	✗
Cost minimization					

Feature	iOS	Android	BlackBerry	Windows Mobile	Windows Phone 8
Control of the monthly used data traffic (WiFi, GSM/3G, roaming)	✗	✓	✗	✓	✗
Backup/Restore					
Files and directories	✗	✓ (9)	✗	✓ (9)	✗
Browser bookmarks	✗	✓ (9)	✗	✓ (9)	✗
SMS	✗	✓ (9)	✗	✓ (9)	✗

1. Requires iOS 5 or higher.
2. Requires Android 3.0 or higher.
3. By setting a PIN or passcode.
4. In combination with Sophos Mobile Security Enterprise.
5. Requires a Samsung SAFE compatible device and installation of the SAFE plugin.
6. Requires iOS 6 or higher.
7. Requires Android 4 or higher.
8. Blackberry is only supported for on-premise installations.
9. Only available for on-premise installations, not for the Software as a Service version.
10. Requires iOS 7 or higher.
11. Requires iOS 7 and a supervised device.
12. Requires Touchdown mail client on the device.

9 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *http://community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *http://www.sophos.com/en-us/support/documentation.aspx*.
- Download the product documentation at .
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

10 Legal notices